

VMware Tunnel Guide

Deploying the VMware Tunnel for your AirWatch environment

AirWatch v9.3

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

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

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

Table of Contents

| | |
|--|-----------|
| VMware Tunnel Quick Start | 4 |
| Chapter 1: Overview | 5 |
| Introduction to VMware Tunnel | 6 |
| VMware Tunnel Technologies and Features | 7 |
| VMware Tunnel Terminology | 7 |
| Chapter 2: Architecture and Security | 9 |
| VMware Tunnel Architecture and Security Overview | 10 |
| VMware Tunnel Deployment Model Overview | 10 |
| Per-App Tunnel Architecture and Security | 13 |
| Proxy (SDK/Browser) Architecture and Security | 13 |
| VMware Tunnel Security and Certificates | 14 |
| Chapter 3: Installation Preparation | 16 |
| VMware Tunnel Installation Preparation Overview | 17 |
| Prepare for a Tunnel Installation | 17 |
| VMware Tunnel Virtual Appliance System Requirements | 18 |
| Chapter 4: Tunnel Configuration | 24 |
| VMware Tunnel Configuration Overview | 25 |
| Configure VMware Tunnel | 25 |
| Configure Advanced Settings for VMware Tunnel | 29 |
| Chapter 5: VMware Tunnel installation on Unified Access Gateway | 32 |
| Virtual Appliance Installation Overview | 33 |
| PowerShell Virtual Appliance Deployment | 37 |
| Chapter 6: VMware Tunnel Management | 46 |
| VMware Tunnel Management Overview | 47 |
| Configure VMware Browser for VMware Tunnel | 47 |
| Per-App Tunneling Overview | 48 |

| | |
|--|-----------|
| Upgrade the VMware Tunnel Virtual Appliance | 55 |
| Upgrade Java for Tunnel Proxy Component | 56 |
| Network Traffic Rules for Per-App Tunnel | 56 |
| VMware Tunnel Access Logs and Syslog Integration | 60 |
| VMware Tunnel SSL Offloading | 61 |
| Kerberos KDC Proxy Support | 63 |
| VMware Tunnel Outbound Proxy Overview | 65 |
| RSA Adaptive Authentication for VMware Tunnel | 69 |
| Appendix: VMware Tunnel Troubleshooting | 71 |
| Per-App Tunnel | 71 |
| Proxy | 72 |
| Tunnel_Snap Troubleshooting Utility | 73 |
| Chapter 7: Tunnel Server Installer Method | 75 |
| VMware Tunnel Linux Installer Overview | 76 |
| VMware Tunnel for Linux System Requirements | 76 |
| Manual Installation of Packages | 80 |
| VMware Tunnel Multi-tier Installation Overview | 81 |
| Basic (Endpoint only) Install Overview | 87 |
| Uninstall the VMware Tunnel | 90 |
| Upgrade the VMware Tunnel for Linux | 90 |
| Accessing Other Documents | 91 |

VMware Tunnel Quick Start

Deploying the VMware Tunnel for your AirWatch environment involves setting up the initial hardware, configuring the server information and app settings in the AirWatch Console, downloading an installer file, and running the installer on your VMware Tunnel server.

Use the following basic steps to deploy VMware Tunnel.

1. Review the different supported architectures of VMware Tunnel and determine which deployment model you plan to use.
See [VMware Tunnel Architecture and Security Overview on page 10](#).
2. Configure your server with the appropriate network rules.
See [VMware Tunnel Installation Preparation Overview on page 17](#).
3. Configure VMware Tunnel settings in the AirWatch Console.
See [VMware Tunnel Configuration Overview on page 25](#).
4. (Optional) Configure various VMware Tunnel functionality within the AirWatch Console, depending on your use cases.
See [Configure VMware Browser for VMware Tunnel on page 47](#) and [Per-App Tunneling Overview on page 48](#).
5. Deploy the VMware Tunnel virtual appliance.
See [VMware Tunnel Virtual Appliance System Requirements on page 18](#). If you want to use the Linux installer, see [VMware Tunnel Linux Installer Overview on page 76](#).
6. Run the installer you downloaded post-configuration on your VMware Tunnel server.

Chapter 1:

Overview

| | |
|---|---|
| Introduction to VMware Tunnel | 6 |
| VMware Tunnel Technologies and Features | 7 |
| VMware Tunnel Terminology | 7 |

Introduction to VMware Tunnel

The VMware Tunnel provides a secure and effective method for individual applications to access corporate resources. The VMware Tunnel authenticates and encrypts traffic from individual applications on compliant devices to the back-end system they are trying to reach.

Tunnel Basics

The 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. To accomplish this authentication and encryption, the VMware tunnel uses unique certificates. For more information, see [VMware Tunnel Technologies and Features on page 7](#)

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 [VMware Tunnel Terminology on page 7](#).

The VMware Tunnel consists of two major components, the Per-App Tunnel and the Proxy components. You must stand up a Linux server or deploy the virtual appliance to use the Per-App Tunnel component. VMware Tunnel offers two architecture models for deployment: single-tier and multi-tier. Both configurations support load-balancing for high availability. The proxy component supports SSL offloading, while Per-App Tunneling cannot be SSL offloaded. For more information on deployment models and components, see [VMware Tunnel Architecture and Security Overview on page 10](#).

Installation Preparation

Before you can install or deploy the VMware Tunnel, you must ensure you meet the requirements. The VMware Tunnel requires specific hardware, software, and network requirements to function properly. For more information, see [VMware Tunnel Installation Preparation Overview on page 17](#).

Configuration

The configuration wizard for the VMware Tunnel provides step-by-step configuration. The settings configured in the wizard are used by the virtual appliance to configure a newly deployed VMware Tunnel. The settings are also packaged into the installer for using the alternate installer method for deploying the VMware Tunnel. For more information, see [VMware Tunnel Configuration Overview on page 25](#).

Virtual Appliance Installation (Preferred Method)

After configuring your VMware Tunnel settings, deploy VMware Tunnel as a virtual appliance to simplify the installation process. AirWatch supports installation using either VMware vSphere web client or PowerShell scripting. The virtual appliance method uses the VMware Unified Access Gateway appliance to deploy the VMware Tunnel. For more information on this installation method, see [Virtual Appliance Installation Overview on page 33](#).

VMware Tunnel Server Installation (Alternate Installer Method)

Instead of using the virtual appliance method, you can use the Linux and Windows installer to install the VMware Tunnel onto the corresponding server. This installer method requires additional work as the installer must be run on each server used in your deployment. Note that the Windows installer does not support the Per-App Tunnel functionality and other features. For more information, see [VMware Tunnel Linux Installer Overview on page 76](#).

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. The additional functionality allows you to maintain and manage your VMware Tunnel deployment. For more information, see [VMware Tunnel Management Overview on page 47](#).

VMware Tunnel Troubleshooting

The VMware Tunnel supports troubleshooting logs to aid in diagnosing issues in your deployment. For more information, see [VMware Tunnel Troubleshooting on page 71](#).

VMware Tunnel Technologies and Features

The VMware Tunnel uses unique certificates for authentication and encryption between end-user applications and the VMware Tunnel.

App Certificate Authentication and Encryption

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

Per-App Tunnel

See [Per-App Tunneling Overview on page 48](#)

Secure Internal Browsing

By using the VMware Tunnel with VMware Browser, you can provide secure internal browsing to any intranet site and Web application that resides within your network. Because VMware Browser has been architected with application tunneling capabilities, all it takes to enable mobile access to your internal Web sites is to enable a setting from the AirWatch Console. By doing so, VMware Browser establishes a trust with VMware Tunnel using an AirWatch-issued certificate and accesses internal Web sites 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.

VMware Tunnel Terminology

VMware Tunnel consists of two major components that are referenced frequently throughout this document. Understanding the functionality that these components reference will aid your comprehension of this product.

Tunnel Components and Functionality

- **VMware Tunnel** – An AirWatch product offering secure connections to internal resources through enabled mobile applications. It comprises two components: Proxy and Per-App Tunnel.
 - **Proxy** – The component that handles securing traffic between an end-user device and a Web site through the VMware Browser mobile application. VMware Tunnel Proxy is also available on Windows. To use an internal application with VMware Tunnel Proxy, then ensure the AirWatch SDK is embedded in your application, which gives you tunneling capabilities with this component.
 - **Per-App Tunnel** – The component that enables Per-App Tunneling functionality for iOS, macOS, Android, and Windows devices for your internal and managed public apps through the VMware Tunnel mobile app. Per-App Tunnel is only available for the VMware Tunnel for Linux.
- **Virtual Appliance** – A virtual appliance is a preconfigured virtual machine that is ready to run on a hypervisor such as VMware vSphere. Deploy VMware Tunnel as a virtual appliance through either the vSphere Web client or using a PowerShell script. Virtual appliances do not require specific hardware or software as they are self-contained and configure the proper hardware requirements upon deployment.
- **App tunnel / app tunneling** – 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 Web site or file server.

On premises and SaaS

Note the following distinction between on-premises and SaaS deployments:

- **On premises** refers to AirWatch deployments where your organization hosts all AirWatch components and servers on its internal networks.
- **SaaS** refers to AirWatch deployments where AirWatch hosts certain AirWatch components, such as the Console and API servers, in the cloud.

Chapter 2:

Architecture and Security

| | |
|--|----|
| VMware Tunnel Architecture and Security Overview | 10 |
| VMware Tunnel Deployment Model Overview | 10 |
| Per-App Tunnel Architecture and Security | 13 |
| Proxy (SDK/Browser) Architecture and Security | 13 |
| VMware Tunnel Security and Certificates | 14 |

VMware Tunnel Architecture and Security Overview

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.

VMware Tunnel offers two architecture models for deployment: single-tier and multi-tier. Both configurations support load-balancing for high availability. The proxy component supports SSL offloading, while Per-App Tunneling cannot be SSL-offloaded.

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 Per-App Tunnel provides most of the same functionality of the Proxy component without the need for additional configuration that Proxy requires.

VMware Tunnel installs as a virtual appliance using VMware vSphere. This deployment method simplifies configuration, installation, maintenance, and upgrades. After configuring VMware Tunnel in the AirWatch Console, download and install the .ova file using VMware vSphere.

VMware Tunnel Deployment Model Overview

The VMware Tunnel supports deploying a single-tier model and a multi-tier model. Use the deployment model that best fits your needs.

Both SaaS and on-premises AirWatch environments support the single-tier and multi-tier models. The VMware Tunnel must have a publicly accessible endpoint for devices to connect to when making a request.

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

Multi-tier networks have separation between servers with firewalls between the tier. Typical AirWatch 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, AirWatch 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.

VMware Tunnel Basic Endpoint Deployment Model

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

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

The basic endpoint Tunnel server communicates with API and AWCM to receive a whitelist of clients allowed to access VMware Tunnel. Both proxy and Per-App Tunnel components support using an outbound proxy to communicate with API/AWCM in this deployment model. When a device connects to VMware Tunnel, it is authenticated based on unique

X.509 certificates issued by AirWatch. Once a device is authenticated, the VMware Tunnel (basic endpoint) forwards the request to the internal network.

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

Cascade Mode Deployment

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

Only the Per-App Tunnel component supports the cascade deployment model. Cascade mode supports a relay-endpoint service if you use the Per-app component and the proxy component in combination. If you use only the proxy component, you must use the Relay-Endpoint model. For more information, see [Relay-Endpoint Deployment Mode on page 12](#).

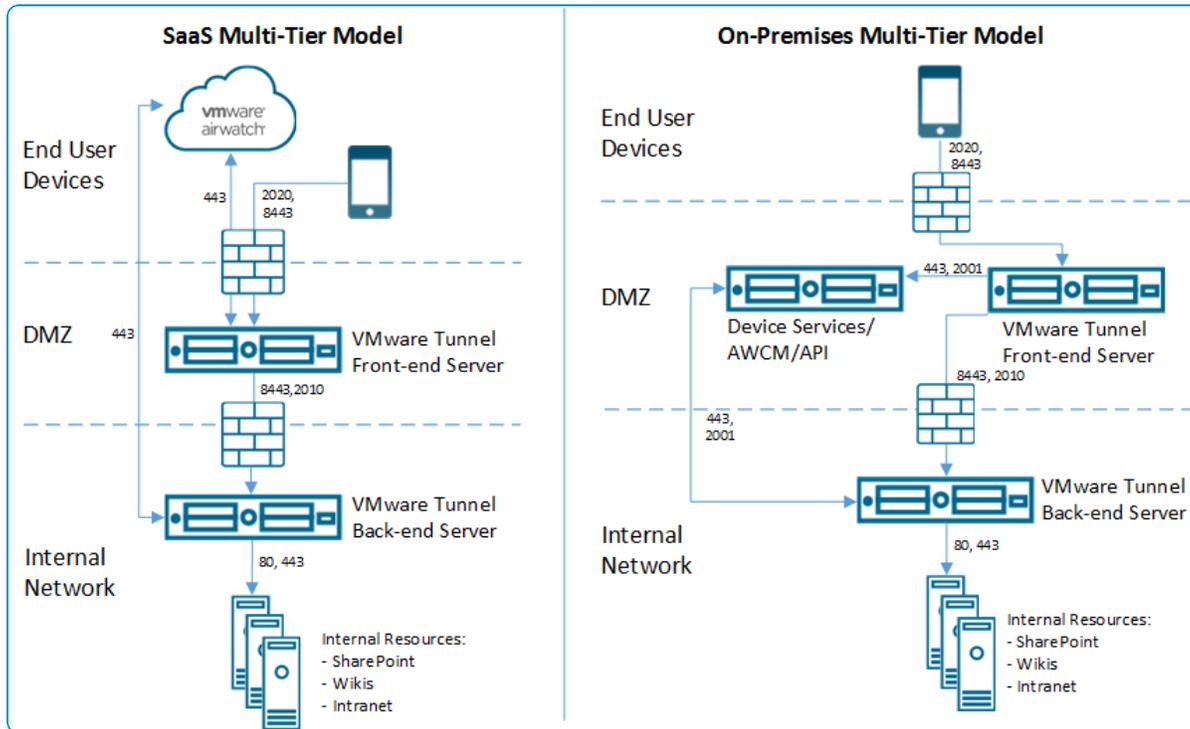
Devices access the front-end server for cascade mode using a configured hostname over configured ports. The default port for accessing the front-end server is port 8443. The back-end server for cascade mode is installed in the internal network hosting your intranet sites and web applications. This deployment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

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

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

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

Both the front-end and back-end servers communicate with the AirWatch API server and AWCM. The API server delivers the VMware Tunnel configuration and the AWCM delivers device authentication, whitelisting, and traffic rules. The front-end and back-end server communicates with API/AWCM through direct TLS connections unless you enable outbound proxy calls. Use this connection if the front-end server cannot reach the API/AWCM servers. If enabled, front-end servers connect through the back-end server to the API/AWCM servers. This traffic, and the back-end traffic, route using server-side traffic rules. For more information, see [Network Traffic Rules for Per-App Tunnel on page 56](#)



Relay-Endpoint Deployment Mode

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 cascade mode deployment. For more information, see [Cascade Mode Deployment on page 11](#).

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 can be resolved by the relay server. This deployment model separates the publicly available server from the server that connects directly to internal resources, providing an added layer of security.

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

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

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

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

VMware Tunnel Load Balancing

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

The Per-App Tunnel component requires authentication of each client after a connection is established. Once connected, a session is created for the client and stored in memory. The same session is then used for each piece of client data so the data can be encrypted and decrypted using the same key. When designing a load balancing solution, the load balancer must be configured with IP/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 DNS round robin, which means the client can select a different server for each connection.

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

For more information on load balancing with Unified Access Gateway appliances, see the Unified Access Gateway Documentation Center: <https://www.vmware.com/support/pubs/access-point-pubs.html>.

Per-App Tunnel Architecture and Security

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

Proxy (SDK/Browser) Architecture and Security

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 high value causes extra memory to be allocated for this operation. AirWatch 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.

VMware Tunnel Security and Certificates

VMware Tunnel uses certificates to authenticate communication among the AirWatch Console, VMware Tunnel, and end-user devices. The following workflows show the initial setup process and how certificates are generated and provisioned.

Initial Setup Workflow

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

Any additional VMware Tunnel servers set up in the same AirWatch 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 AirWatch Recommended Architecture Guide**, available on [Accessing Other Documents on page 91](#).

Certificate Integration Cycle

4. AirWatch generates Device Root Certificates that are unique to every instance during the installation process.

For Proxy: The Device Root Certificate is used to generate client certificates for each of the applications and devices.

For Per-App Tunnel: The Device Root Certificate is used to generate client certificates for each of the devices.
5. **For Proxy:** The certificate an application uses to authenticate with the VMware Tunnel is only provided after the application attempts to authenticate with the AirWatch enrollment credentials for the first time.

For Per-App Tunnel: The certificate is generated at the time of profile delivery.
6. VMware Tunnel gets the chain during installation. The VMware Tunnel installer is dynamically packaged and picks these certificates at the time of download.
7. Communication between the VMware Tunnel and device-side applications (includes VMware Browser and wrapped applications using app tunneling) is secured by using the identity certificates generated during installation. These identity certs are child certificates of the Secure Channel Root certificate.
8. 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*.

9. VMware Tunnel maintains a list of devices and certificates and only authenticates communication if it sees a certificate it recognizes.
X.509 (version 3) digitally signed client certificates are used for authentication.

Chapter 3:

Installation Preparation

| | |
|---|----|
| VMware Tunnel Installation Preparation Overview | 17 |
| Prepare for a Tunnel Installation | 17 |
| VMware Tunnel Virtual Appliance System Requirements | 18 |

VMware Tunnel Installation Preparation Overview

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

Before deploying the VMware Tunnel, you must enable API access so the virtual appliance can deploy.

Consider reviewing the network requirements of the VMware Tunnel with your network admins. If the requirements are not met, issues can arise with your VMware Tunnel deployment.

Prepare for a Tunnel Installation

Ensure your AirWatch environment is prepared for an VMware Tunnel installation before attempting to configure or install the product. Before you begin installing VMware Tunnel, ensure that API and AWCM are installed correctly, running, and communicating with AirWatch without any errors.

For more information about configuring AWCM, see [Introduction to AWCM](#) on page 1.

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.

1. Navigate to **Groups & Settings > All Settings > System > Advanced > Site URLs** in the AirWatch Console.
2. Validate the following URLs in Site URLs:
 - REST API URL** – Enter in the format of "https://<url>/api".
SaaS customers must contact AirWatch support to get their REST API URL.
 - AWCM Server External URL** – Enter in the format of "server.acme.com" and do not include a protocol such as https.
 - AWCM Service Internal URL** – Enter in the format of "https://server.acme.com".

For on-premises customers, the default port for AWCM is 2001. For SaaS customers, AWCM and API use port 443.

 Are you migrating from a Linux server to the virtual appliance? Follow the AirWatch migration flow for migrating to the virtual appliance. For more information, see <https://support.air-watch.com/articles/115001666308>.

Hypervisor Requirements

The VMware Unified Access Gateway, the virtual appliance 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 OVF.

Supported Hypervisors

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

Software Requirement

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

Hardware Requirements for VMware Tunnel

The OVF package for the VMware 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** to change the default settings as needed.

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

| 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 log file size based on your log use and requirements for storing logs. | | | | |

Network Requirements for VMware Tunnel

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

| Source Component | Destination Component | Protocol | Port | Verification | Note |
|---|--|---------------------|---|--|------|
| Devices (from Internet and Wi-Fi) | VMware Tunnel Proxy | HTTPS | 2020* | After installation, run the following command to validate: <pre>netstat -tlnp grep [Port]</pre> | 1 |
| Devices (from Internet and Wi-Fi) | VMware Tunnel Per-App Tunnel | TCP | 8443* | After installation, run the following command to validate: <pre>netstat -tlnp grep [Port]</pre> | 1 |
| Admin Device (from Internet and Wi-Fi) | VMware Tunnel admin UI | HTTPS | 9443 | | |
| VMware Tunnel – Basic-Endpoint Configuration | | | | | |
| VMware Tunnel | AirWatch Cloud Messaging Server** | HTTPS | SaaS: 443 On-Prem: 2001* | <pre>curl -Ivv https://<AWCM URL>:<port>/awcm/status.</pre> The expected response is HTTP 200 – OK. | 2 |
| VMware Tunnel | AirWatch REST API Endpoint SaaS: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com On-Prem: Most commonly your DS or Console server | HTTP or HTTPS | SaaS: 443 On-Prem: 80 or 443 | <pre>curl -Ivv https://<API URL>/api/mdm/ping</pre> The expected response is HTTP 401 – unauthorized. | 5 |
| VMware Tunnel | Internal resources | HTTP, HTTPS, or TCP | 80, 443, Any TCP | Confirm that the VMware Tunnel can access internal resources over the required port. | 4 |

| Source Component | Destination Component | Protocol | Port | Verification | Note |
|--|--|----------|--|---|------|
| VMware Tunnel | Syslog Server | UDP | 514* | | |
| VMware Tunnel — Cascade Configuration | | | | | |
| VMware Tunnel Front-End | AirWatch Cloud Messaging Server** | TLS v1.2 | SaaS: 443 On-Prem: :2001* | Verify by using wget to https://<AWCM URL>:<port>/awcm/status and ensuring you receive an HTTP 200 response. | 2 |
| VMware Tunnel Front-End | VMware Tunnel Back-End | TLS v1.2 | 8443* | Telnet from VMware Tunnel Front-End to the VMware Tunnel Back-End server on port | 3 |
| VMware Tunnel Back-End | AirWatch Cloud Messaging Server** | TLS v1.2 | SaaS: 443 On-Prem: :2001* | Verify by using wget to https://<AWCM URL>:<port>/awcm/status and ensuring you receive an HTTP 200 response. | 2 |
| VMware Tunnel Back-End | Internal Web sites / Web apps | TCP | 80 or 443 | | 4 |
| VMware Tunnel Back-End | Internal resources | TCP | 80, 443, Any TCP | | 4 |
| VMware Tunnel Front-End and Back-End | AirWatch REST API Endpoint SaaS: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com On-Prem: Most commonly your DS or Console server | TLS v1.2 | 80 or 443 | <pre>curl -Ivv https://<API URL>/api/mdm/ping</pre> The expected response is HTTP 401 – unauthorized. | 5 |

| Source Component | Destination Component | Protocol | Port | Verification | Note |
|---|--|---------------------|---|---|------|
| VMware Tunnel – Relay-Endpoint Configuration | | | | | |
| VMware Tunnel Relay | AirWatch Cloud Messaging Server** | HTTP or HTTPS | SaaS: 443 On-Prem: 2001* | <pre>curl -Ivv https://<AWCM URL>:<port>/awcm/status.</pre> <p>The expected response is HTTP 200 – OK.</p> | 2 |
| VMware Tunnel Endpoint and Relay | AirWatch REST API Endpoint SaaS: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com On-Prem: Most commonly your DS or Console server | HTTP or HTTPS | 80 or 443 | <pre>curl -Ivv https://<API URL>/api/help</pre> <p>The expected response is HTTP 401 – unauthorized.</p> <p>The VMware Tunnel Endpoint requires access to the REST API Endpoint only during initial deployment.</p> | 5 |
| VMware Tunnel Relay | VMware Tunnel Endpoint | HTTPS | 2010* | Telnet from VMware Tunnel Relay to the VMware Tunnel Endpoint server on port | 3 |
| VMware Tunnel Endpoint | Internal resources | HTTP, HTTPS, or TCP | 80, 443, Any TCP | Confirm that the VMware Tunnel can access internal resources over the required port. | 4 |
| VMware Tunnel | Syslog Server | UDP | 514* | | |

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

** For SaaS customers who need to whitelist outbound communication, please refer to the following AirWatch Knowledge Base article for a list of up-to-date IP ranges AirWatch currently owns: <https://support.airwatch.com/articles/115001662168>.

1. Devices connect to the public DNS configured for VMware Tunnel over the specified port.
2. For the VMware Tunnel to query the AirWatch 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.

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 are all on the same subnet.
- With two network interfaces, external traffic is on one subnet, and internal and management traffic are on another subnet.
- Using three network interfaces is the most secure option. With a third NIC, external, internal, and management traffic all have their own subnets.

Chapter 4:

Tunnel Configuration

| | |
|---|----|
| VMware Tunnel Configuration Overview | 25 |
| Configure VMware Tunnel | 25 |
| Configure Advanced Settings for VMware Tunnel | 29 |

VMware Tunnel Configuration Overview

After completing the steps in the [VMware Tunnel Installation Preparation Overview on page 17](#), you can configure VMware Tunnel settings per your deployment's configuration and functionality needs in the AirWatch Console.

Configure the VMware Tunnel installer in the AirWatch Console under **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel**. The wizard walks you through the installer configuration step-by-step. The options configured in the wizard are packaged in the installer, which you can download from the AirWatch 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 deploy the VMware Tunnel, you need the details of the server where you plan to install. Before configuration, determine the deployment model, one or more hostnames and ports, and which features of VMware Tunnel to implement, such as access log integration, NSX integration, SSL offloading, enterprise certificate authority integration, and so on. Because the wizard dynamically displays the appropriate options based on your selections, the configuration screens may display different text boxes and options.

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

Configure VMware Tunnel

To configure the VMware Tunnel, you need the details of the server where you plan to install. Know whether or not you plan to use certain features, such as syslog integration, NSX integration, SSL offloading, and so on, since these features are enabled during configuration.

To configure the VMware Tunnel, perform the following steps:

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

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

| Setting | Description |
|---|--|
| PROXY (APP WRAPPING / BROWSER / SDK) CONFIGURATION | |
| Relay Host Name | (Relay-Endpoint Only). Enter the FQDN of the public host name for the Tunnel relay server, for example, tunnel.acmemdm.com. This hostname must be publicly available as it is the DNS that devices connect to from the Internet. |
| Endpoint Host Name | The internal DNS of the Tunnel endpoint server. This value is the hostname that the relay server connects to on the relay-endpoint port. If you plan to install the VMware Tunnel on an SSL offloaded server, enter the name of that server in place of the Host Name . When you enter the Host Name , do not include a protocol, such as http://, https://, etc. |
| Relay Port (HTTPS) | The proxy service is installed on this port. Devices connect to the <relayhostname>:<port> to use the VMware Tunnel proxy feature. The default value is 2020. |
| Relay-Endpoint Port | (Relay-Endpoint only). This value is the port used for communication between the VMware Tunnel relay and VMware Tunnel endpoint. The default value is 2010. If you are using a combination of Proxy and Per-App Tunnel, the relay endpoint installs as part of the Front-End Server for Cascade mode. The ports should be different values. |
| Advanced Proxy Configuration Details | |
| Use Kerberos Proxy | Enable Kerberos proxy support to allow access to Kerberos authentication for your target back end Web services. This feature does not currently support Kerberos Constrained Delegation (KCD). For more information, see Kerberos KDC Proxy Support on page 63 . The Endpoint server must be on the same domain as KDC for the Kerberos Proxy to communicate successfully with the KDC. |
| Realm | Enter the domain of the KDC server. This text box only displays if you enable Use Kerberos Proxy . |
| PER - APP TUNNELING CONFIGURATION | |
| Basic Mode | |
| Hostname | Enter the FQDN of the public host name for the Tunnel server, for example, tunnel.acmemdm.com. This hostname must be publicly available as it is the DNS that devices connect to from the Internet. |
| Port | Enter the port number assigned for communication with the VMware Tunnel component. The default value is 8443. |
| Cascade Mode | |
| Front-end Hostname | Enter the FQDN of the public host name for the Tunnel relay server, for example, tunnel.acmemdm.com. This hostname must be publicly available as it is the DNS that devices connect to from the Internet. |
| Front-end Port | Enter the port number assigned for communication with the VMware Tunnel component. The default value is 8443. |

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

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

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

- Select **Next**.
- On the **Authentication** screen, configure the following settings to select the certificates that devices use to authenticate to the VMware Tunnel.
 - Proxy Authentication / Per-App Tunnel Authentication** – By default, all the components use AirWatch issued certificates. To use Enterprise CA certificates for client-server authentication, select the Enterprise CA option.
 - Select **Default** to use AirWatch issued certificates. The default AirWatch issued client certificate does not

automatically renew. To renew these certificates, re-publish the VPN profile to devices that have an expiring or expired client certificate. View the certificate status for a device by navigating to **Devices > Device Details > More > Certificates**.

- Select **Enterprise CA** in place of AirWatch-issued certificates for authentication between the VMware Browser, Per-App Tunnel-enabled apps, or SDK-enabled apps and the VMware Tunnel requires that a certificate authority and certificate template are set up in your AirWatch environment before configuring VMware Tunnel.
 - Select the certificate authority and certificate template that are used to request a certificate from the CA.
 - Upload the full chain of the public key of your certificate authority to the configuration wizard.

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

Certificates auto-renew based on your CA template settings.

9. Select **Next**.
10. On the **Profile Association** screen, you can optionally create a new iOS or Android VPN profile or select an existing one. For a device to take advantage of Per-App Tunnel functionality, it must be issued with a device profile with a VPN payload configured that uses VMware Tunnel as the VPN provider. These profiles can also be created after the VMware Tunnel configuration is complete.

Select the platform, then select whether to **Create New Profile** or **Use Existing**. The **Create New Profile** option creates a device profile in **Devices > Profiles > List View**. This profile is assigned to the organization group where you configure VMware Tunnel and the deployment type is set to On Demand. If you choose to create one or more profiles now, refer to the **Configuring Per-App Tunneling with VMware Tunnel** section of the **VMware Tunnel Admin Guide** for more details.

The profile is only created with this step – you still must publish it manually. By default any profiles you create on this screen are assigned to all devices at the current organization group. You can edit these profiles manually after completing VMware Tunnel configuration.

11. Select **Next**.
12. On the **Miscellaneous** screen, you can enable access logs for the proxy or Per-App Tunnel components. If you intend to use this feature you must configure it now as part of the configuration, as it cannot be enabled later without reconfiguring Tunnel and rerunning the installer. For more information on these settings, see [VMware Tunnel Access Logs and Syslog Integration on page 60](#) and [Configure Advanced Settings for VMware Tunnel on page 29](#).
For Per-App Tunneling, you can also configure NSX Communication, which is the integration between AirWatch and VMware NSX to achieve micro-segmentation. For more information on this integration, refer to the **VMware AirWatch and VMware NSX Integration Guide**.
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. If you plan to use SSL offloading for the VMware Tunnel proxy component, select the Advanced tab on the Tunnel Configuration screen and select **Export Proxy Certificate**. Then, import this certificate on the server performing SSL offloading. (This server can be a load balancer or reverse proxy.)
15. Select the **General** tab and then select the **Download Virtual Appliance** hyperlink. This button downloads the OVA file used for deploying VMware Tunnel on to relays and endpoints. The download file also includes the PowerShell

script and .ini template file for the PowerShell deployment method.

For legacy installer methods, select Download Linux Installer. This button downloads a single TAR file used for deploying the relay and endpoints. You must also confirm a certificate password that is used during installation. The password must contain a minimum of six characters.

16. Select **Save**.

Continue with the steps to [Deploy VMware Tunnel using vSphere on page 33](#) or [PowerShell Virtual Appliance Deployment on page 37](#), depending on the deployment method you use.

For legacy deployment methods, continue with the steps for [Install the AirWatch Tunnel Front-End Server\(Linux\) on page 81](#) or [Install the AirWatch Tunnel Back-End Server \(Linux\) on page 84](#), depending on the configuration that you selected.

Configure Advanced Settings for VMware Tunnel

The Advanced settings tab lets you configure more settings that are optional for an VMware Tunnel deployment. Except where noted, you can configure these settings before or after installation.

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

| Setting | Description |
|--------------------------------------|---|
| RSA Adaptive Auth Integration | Enable this setting if you want to integrate the Proxy component with RSA authentication for comprehensive Web browsing security. Select to enable the following adaptive authentication settings. For more information, see RSA Adaptive Authentication for VMware Tunnel on page 69 . |
| 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. |

| Setting | Description |
|--|---|
| Access Logs | <p>Enable this setting to tell VMware Tunnel Proxy component to write access logs to syslog for any of your own purposes. These logs are not stored locally. They are pushed to the syslog host over the port you define. Communication to the syslog server occurs over UDP, so ensure that UDP traffic is allowed over this port.</p> <p>If you are using a relay-endpoint deployment model, the relay writes the access logs. If you are using an basic endpoint deployment model, the endpoint writes the access logs.</p> <p>There is no correlation between this syslog integration and the integration accessed on Groups & Settings > All Settings > System > Enterprise Integration > Syslog.</p> <p>You must enable this feature before you install any of the components. Any changes you make to the access logs configuration on the AirWatch Console require reinstallation of the VMware Tunnel server.</p> |
| Syslog Hostname | <p>Enter the URL of your syslog host.</p> <p>This setting displays after you enable Access Logs.</p> |
| Port | <p>Enter the port over which you want to communicate with the syslog host.</p> <p>This setting displays after you enable Access Logs.</p> |
| API and AWCM outbound calls via proxy | <p>Enable this option if the communication for initialization between the VMware Tunnel and AirWatch API or AWCM is through an outbound proxy.</p> |
| Show detailed errors | <p>Enable this option to ensure client applications (for example, VMware Browser) are informed when the VMware Tunnel fails to authenticate a device.</p> |
| Log Level | <p>Set the appropriate logging level, which determines how much data is reported to the LOG files.</p> |

3. If applicable, configure the following Kerberos Proxy settings, which display only if you select **Use Kerberos Proxy** during the VMware Tunnel configuration. If the realm info you entered during configuration does not work properly, you can enter the KDC IP address here, which overrides the information that you provided during configuration. You must reinstall the VMware Tunnel after changing these settings. A restart does not work.

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

4. If applicable, configure the following Per-App Tunneling settings.

Any changes to the Per-App Tunneling settings after installation of the VMware Tunnel server do not require restarting/reinstallation of the service. Changes automatically apply to the server.

| Setting | Description |
|--|---|
| Access Logs | <p>Enable this setting to enable the 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.</p> <p>There is no correlation between this syslog integration and the integration accessed on Groups & Settings > All Settings > System > Enterprise Integration > Syslog.</p> <p>You must enable this feature as part of VMware Tunnel configuration before you install any of the components.</p> |
| Syslog Hostname | <p>Enter the URL of your syslog host.</p> <p>This setting displays after you enable Access Logs.</p> |
| Port | <p>Enter the Port over which you want to communicate with the syslog host.</p> <p>This setting displays after you enable Access Logs.</p> |
| API and AWCM outbound calls via proxy | <p>Enable this option if the communication for initialization between the VMware Tunnel and AirWatch API or AWCM is through an outbound proxy.</p> |

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

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

6. Select **Save**.

Chapter 5:

VMware Tunnel installation on Unified Access Gateway

| | |
|---|----|
| Virtual Appliance Installation Overview | 33 |
| PowerShell Virtual Appliance Deployment | 37 |

Virtual Appliance Installation Overview

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.

VMware Unified Access Gateway is a secure virtual appliance that ensures the only traffic entering the corporate data center is traffic on behalf of a strongly authenticated remote user. VMware Tunnel uses the Unified Access Gateway platform to deploy as a virtual appliance.

As a virtual appliance, VMware Tunnel does not require extensive pre-installation configuration of hardware and software. The hardware and software requirements are automatically configured as the virtual appliance deploys. Deploy Unified Access Gateway appliance through either the VMware vSphere web client and Unified Access Gateway Admin UI method or the PowerShell script method.

The vSphere web client deployment method allows you to deploy the virtual appliance through vSphere and then configure your custom settings in an admin UI. The PowerShell script deployment method automates the settings based on the pre-configured script. The PowerShell script method calls the API server before running so you get a quick validation of the entered information before deploying the virtual appliance. Consider using the PowerShell method for the best deployment experience.

Note: VMware Tunnel deploys using a hardened, VMware appliance. For more information on the hardening of this appliance, see the [Deploying and Configuring Access Point](https://www.vmware.com/support/pubs/access-point-pubs.html) guide on <https://www.vmware.com/support/pubs/access-point-pubs.html>.

Deploy VMware Tunnel using vSphere

After configuring the VMware Tunnel in the AirWatch Console and downloading the VMware Unified Access Gateway OVA file, use VMware vSphere to install the virtual appliance onto your server. The virtual appliance simplifies installation of the VMware Tunnel.

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

Requirements

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

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

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

Procedure

1. Log in to the vSphere Web client.
2. Navigate to VMs and Templates.
3. Select the folder where you want to deploy the virtual appliance OVA file. Right-click the file and select **Deploy OVF Template**.
4. Select the OVA file on your local machine or enter the URL for the OVA file. Click **Next**.
5. Review the template details and select **Next**.
6. Enter a unique **Name** for the deployment then select the folder or data center to hold the OVA file and select **Next**.
7. Select the number of Network Interface Controllers (NICs) you want to associate with the appliance for your deployment configuration. Click **Next**.

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

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

<https://www.vmware.com/support/pubs/access-point-pubs.html>.

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

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

When finished, select **Next**.

10. Configure the **Network Mapping** settings.
Enter the vSphere network names. A vSphere Network Protocol Profile must be associated with every referenced network name.
The network profiles determine the IP protocol, DNS servers, gateway, and IPv4 subnet mask. If these are values are empty, you must enter the values.
When finished, select **Next**.
11. Configure the **Properties** settings. These settings include the **Network Properties** and the **Password Options**.
 - Customize the **Network Properties** as they relate to your VMware Tunnel network configuration.
 - Customize the **Password Options**.
 - Configure the password for the root user of the VM.
 - Configure the password for the REST API access.
The REST API password is the password for the admin UI. You must follow the password requirements:

- The password must be 8 characters long.
- The password must contain at least one special character which includes: !@#\$*()
- The password must contain at least one lowercase character.
- The password must contain at least one uppercase character.

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

When finished, select **Next**.

12. Review the OVA settings and select the **Power on after deployment**.
13. Select **Finish** to deploy the virtual appliance.

To complete the configuration of the VMware Tunnel, you must log into the virtual appliance admin UI to customize your settings.

Configure VMware Tunnel Settings

After deploying the VMware Tunnel on the VMware Unified Access Gateway appliance, 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 virtual appliance.

To configure the VMware Tunnel settings:

1. Navigate to the URL of your virtual appliance 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 **Per-App Tunnel and Proxy Settings**, select the settings icon () to configure your VMware Tunnel deployment.
7. Customize the **AirWatch Properties**:

| Settings | Descriptions |
|---|--|
| Enable Per-App Tunnel and Proxy Settings | Set to Yes to use the configured VMware Tunnel settings. After configuration, setting this option to No does not disable the VMware Tunnel. |

| Settings | Descriptions |
|---------------------------------|---|
| API Server URL | Enter the URL to your AirWatch API server. The appliance contacts the AirWatch API server to fetch your VMware Tunnel configuration. For example, https://asXXX.example.com. |
| API Server Username | Enter the user name of an AirWatch Admin user account. You must have Console Administrator privileges at a minimum. |
| API Server Password | Enter the password of an AirWatch 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. |
| AirWatch Server Hostname | Enter the hostname for your VMware Tunnel configuration. The hostname must match the hostname entered in the VMware Tunnel configuration wizard. The virtual appliance 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 AirWatch Outbound Proxy Settings if you use an outbound proxy to make the initial call to the API server:

| Settings | Description |
|------------------------------------|---|
| Outbound Proxy Host | Enter the outbound proxy hostname. |
| Outbound Proxy Port | Enter the outbound proxy port. |
| Outbound Proxy User | Enter the user name if your proxy requires authentication. |
| Outbound Proxy Password | Enter the password for your outbound proxy if your proxy requires authentication. |
| NTLM Authentication | Enable if your proxy requires NTLM authentication. |
| Use for VMware Tunnel Proxy | Enable to use these proxy settings as the outbound proxy for your VMware Tunnel deployment. |
| Host Entries | Enter the host entries for the server. You can enter multiple host entries separated by commas. They must follow this format: IP address hostname hostname alias (optional). For example, 10.192.168.1 example1.com, 10.192.167.2 example2.com. Use this option if your DNS is not publicly available or accessible from the DMZ. |

| Settings | Description |
|-----------------------------|---|
| 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. |

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

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

PowerShell Virtual Appliance Deployment

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.

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), AirWatch Administrator, optional outbound proxy password, and vCenter. Each password is then validated so you can easily troubleshoot why the deployment failed.

PowerShell enables you to deploy multiple instances of VMware Tunnel quickly and easily. Use the same .ini template to run the script multiple times.

Configure the vSphere .INI Template

After configuring the VMware Tunnel in the AirWatch Console and downloading the OVA file, configure the vSphere template.ini file with your virtual appliance settings. The PowerShell script uses the template to configure your virtual appliance deployment.



Watch a tutorial video explaining how to deploy the VMware Tunnel virtual appliance using PowerShell: <https://support.air-watch.com/articles/115001666428>.

To configure the template.ini:

- Download the Unified Access Gateway Using vSphere ZIP from AirWatch Resources (<https://resources.air-watch.com/view/sbfsfykltppqfxhvg9tpty/en>).
- Unzip the file and locate the template.ini file.
- Right click the file and select **Open With**. Select notepad or your preferred file editor.
- Configure the template.ini settings:

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

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

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

Configure the Hyper-V .INI Template

After configuring the VMware Tunnel in the AirWatch Console, download and configure the Hyper-V template.ini file with your virtual appliance settings. The PowerShell script uses the template to configure your virtual appliance deployment.



Watch a tutorial video explaining how to deploy the VMware Tunnel virtual appliance using PowerShell: <https://support.air-watch.com/articles/115001666428>.

To configure the template.ini:

1. Download the Unified Access Gateway Using Hyper-V ZIP from AirWatch Resources (<https://resources.air-watch.com/view/dyw27fqmg4gw7ptpvdhp>).
2. Unzip the file and locate the template.ini file.
3. Right click the file and select **Open With**. Select notepad or your preferred file editor.
4. Configure the template.ini settings:

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

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

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

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

Run the VMware Tunnel PowerShell Script

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

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

Prerequisites

- Windows administrator privileges
- PowerShell 4

The PowerShell script runs on Windows 8.1 or later machines or Windows Server 2008 R2 or later. The machine can also be a vCenter Server running on Windows or a separate Windows machine.
- VMware OVF Tool 4.1 (available on my.vmware.com)
- VMware-ClientIntegrationPlugin (available on my.vmware.com)
- Configured .ini template file to pass the configuration values to the appliance (part of the OVA download package available on AirWatch Resources at <https://resources.air-watch.com/view/sbfsfykltpqfxhvg9tpty/en>)
- PowerShell script to configure the appliance (part of the OVA download package available on AirWatch Resources at <https://resources.air-watch.com/view/sbfsfykltpqfxhvg9tpty/en>)
- Communication between the Windows machine used to deploy the OVA and your vSphere instance

Supported Hypervisors

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

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

Procedure

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

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

Example:

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

4. Enter the password for each prompt:

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

After entering each password, PowerShell validates the entered password.

Once all passwords are entered, the virtual appliance 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 virtual appliance name must be different each time you deploy through PowerShell.

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

Chapter 6:

VMware Tunnel Management

| | |
|--|----|
| VMware Tunnel Management Overview | 47 |
| Configure VMware Browser for VMware Tunnel | 47 |
| Per-App Tunneling Overview | 48 |
| Upgrade the VMware Tunnel Virtual Appliance | 55 |
| Upgrade Java for Tunnel Proxy Component | 56 |
| Network Traffic Rules for Per-App Tunnel | 56 |
| VMware Tunnel Access Logs and Syslog Integration | 60 |
| VMware Tunnel SSL Offloading | 61 |
| Kerberos KDC Proxy Support | 63 |
| VMware Tunnel Outbound Proxy Overview | 65 |
| RSA Adaptive Authentication for VMware Tunnel | 69 |

VMware Tunnel Management Overview

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

The additional functionality allows you to maintain and manage your VMware Tunnel deployment. The network traffic rules control access to your internal resources by restricting traffic sent from apps or to specified domains. You can also configure the outbound proxy during installation to control traffic to and from your network. The Kerberos KDC Proxy limits access to devices with correct authentication. Use RSA authentication to control access to internal resources through two-factor authentication. SSL offloading, supported by the Proxy component only, eases the burden of encrypting and decrypting traffic from the VMware Tunnel server.

The access logs and syslog integration provides detailed logs for troubleshooting.

Configure VMware Browser for VMware Tunnel

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

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

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

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. If a URL that is about to be invoked contains a domain that matches the list in the settings, this URL request goes through the VMware Tunnel. If the URL domain does not match the domain in the list, it goes directly to the Internet. Leave the text box empty to send all requests through the VMware Tunnel.
4. Select **Save**.
5. Ensure the VMware Browser is using the Shared SDK profiles for iOS and Android by navigating to **Groups & Settings > All Settings > Apps > VMware Browser** and selecting them under **SDK Profile**.

Caveats and Known Limitations

- For VMware Tunnel, the current authentication scheme requires the use of a chunk aggregator of fixed size. A low value puts restrictions on the amount of data that is sent from the devices in a single HTTP request. By contrast, a high value causes extra memory to be allocated for this operation. AirWatch 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.

Per-App Tunneling Overview

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

This alternative solution is different from app tunneling with app wrapping because it supports both TCP and HTTP(S) traffic. It works for both public and internally developed apps. However, for internal apps, the VMware Tunnel app acts as an alternative option only if the sole requirement is tunneling into the internal network. Otherwise, you must use app wrapping to take advantage of features including integrated authentication, geofencing, offline access control, and so on.

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

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

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

Note: VMware Tunnel does not support Per-App VPN functionality for macOS devices. You can restrict access to domains through the Safari Domains feature of the Network Traffic rules. For more information, see [Network Traffic Rules for Per-App Tunnel on page 56](#).

Additional Details

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

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

Configure Per-App Tunnel Profile for iOS

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

In addition to the steps below, you can also configure Per-App Tunnel profiles within the VMware Tunnel configuration wizard when configuring other VMware Tunnel settings.

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

What to do next

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

Configure Per-App Tunnel Profile for Android

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

In addition to the steps below, you can also add a Per-App Tunnel profile within the VMware Tunnel configuration wizard when configuring other VMware Tunnel settings.

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.
These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
3. Select the **VPN** payload from the list.
4. Enter a **Connection Name** and select **VMware Tunnel** as the **Connection Type**.
The **Server** text box populates automatically with your VMware Tunnel component server URL. If this component is not configured, you see a message and hyperlink to the system settings page where you can configure it.
5. Select **Save & Publish**.

What to do next

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

Configure Per-App Tunnel Profile for Windows

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

In addition to the steps below, you can also add a Per-App Tunnel profile within the VMware Tunnel configuration wizard when configuring other VMware Tunnel settings.

1. Navigate to **Devices > Profiles > List View > Add** and select **Windows**. Then select **Windows Desktop** and **User**.
2. Configure the profile's **General** settings.
These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
3. Select the **VPN** payload from the list.
4. Enter a **Connection Name** and select **VMware Tunnel** as the **Connection Type**.
The **Server** text box populates automatically with your VMware Tunnel component server URL. If this component is not configured, you see a message and hyperlink to the system settings page where you can configure it.
5. Configure the **Per App VPN** rules.
6. Select **Add New Domain** to add all domains you want resolved through the VMware Tunnel server.
7. Select **Save & Publish**.

Configure Per-App Tunnel Profile for Windows

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

In addition to the steps below, you can also add a Per-App Tunnel profile within the VMware Tunnel configuration wizard when configuring other VMware Tunnel settings.

1. Navigate to **Devices > Profiles > List View > Add** and select **Windows**. Then select **Windows Desktop** and **User**.
2. Configure the profile's **General** settings.
These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
3. Select the **VPN** payload from the list.
4. Enter a **Connection Name** and select **VMware Tunnel** as the **Connection Type**.
The **Server** text box populates automatically with your VMware Tunnel component server URL. If this component is not configured, you see a message and hyperlink to the system settings page where you can configure it.
5. Configure the **Per App VPN** rules.
6. Select **Add New Domain** to add all domains you want resolved through the VMware Tunnel server.
7. Select **Save & Publish**.

Configure Per-App Tunnel Profile for macOS

Configure Per-App Tunnel for macOS 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.

If configure network traffic rules for Per-App Tunnel for macOS, AirWatch disables any configured Safari domains in existing macOS VPN profiles.

In addition to the steps below, you can also add a Per-App Tunnel profile within the VMware Tunnel configuration wizard when configuring other VMware Tunnel settings.

1. Navigate to **Devices > Profiles > List View > Add** and select **macOS**. Then select **User**.
2. Configure the profile's **General** settings.
These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
3. Select the **VPN** payload from the list.
4. Enter a **Connection Name** and select **VMware Tunnel** as the **Connection Type**.
The **Server** text box populates automatically with your VMware Tunnel component server URL. If this component is not configured, you see a message and hyperlink to the system settings page where you can configure it.
5. Select **Save & Publish**.

To configure the Safari domains, see [Network Traffic Rules for Per-App Tunnel on page 56](#).

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.

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.

For additional instructions on adding or editing apps, please see the **VMware AirWatch Mobile Application Management Guide**, available on [AirWatch Resources](#).

This workflow only applies to Android and iOS devices.

Configure Internal Apps to Use Per App Profile

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

1. Navigate to **Apps & Books > Applications > Native**.
2. Select the **Internal** tab.

3. Select **Add Application** and add an app.
4. Select **Save & Assign** to move to the Assignment page.
5. Select **Add Assignment** and select **Per-App VPN Profile** in the **Advanced** section.
6. **Save & Publish** the app.

For additional instructions on adding or editing apps, please see the **VMware AirWatch Mobile Application Management Guide**, available on [AirWatch Resources](#).

This workflow only applies to Android and iOS devices.

Access the VMware Tunnel App for iOS

The VMware Tunnel application for iOS lets end users access internal corporate Web resources and sites through managed public and internal applications. The legacy VMware Tunnel application for iOS does not support the same functionality as the VMware Tunnel application.

Requirements

- VMware Tunnel application for iOS
 - iOS 9.3+
 - AirWatch v9.0+

Using the VMware Tunnel App

Your end users must download and install the VMware Tunnel application from the iOS App Store.

Important: The VMware Tunnel app must be present on devices before assigning the VPN profile. For more information on migrating to the VMware Tunnel app, see <https://support.air-watch.com/articles/115004308288>.

Access the AirWatch Tunnel App for iOS

The AirWatch Tunnel application for iOS lets end users access internal corporate Web resources and sites through managed public and internal applications.

The AirWatch Tunnel App for iOS is a legacy app. For the most up-to-date functionality, use the VMware Tunnel app for iOS. For more information, see [Access the VMware Tunnel App for iOS on page 52](#).

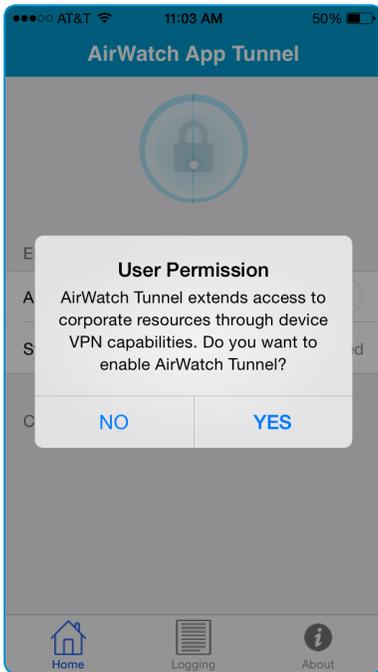
Note: AirWatch Tunnel for iOS does not currently support UDP traffic.

Requirements

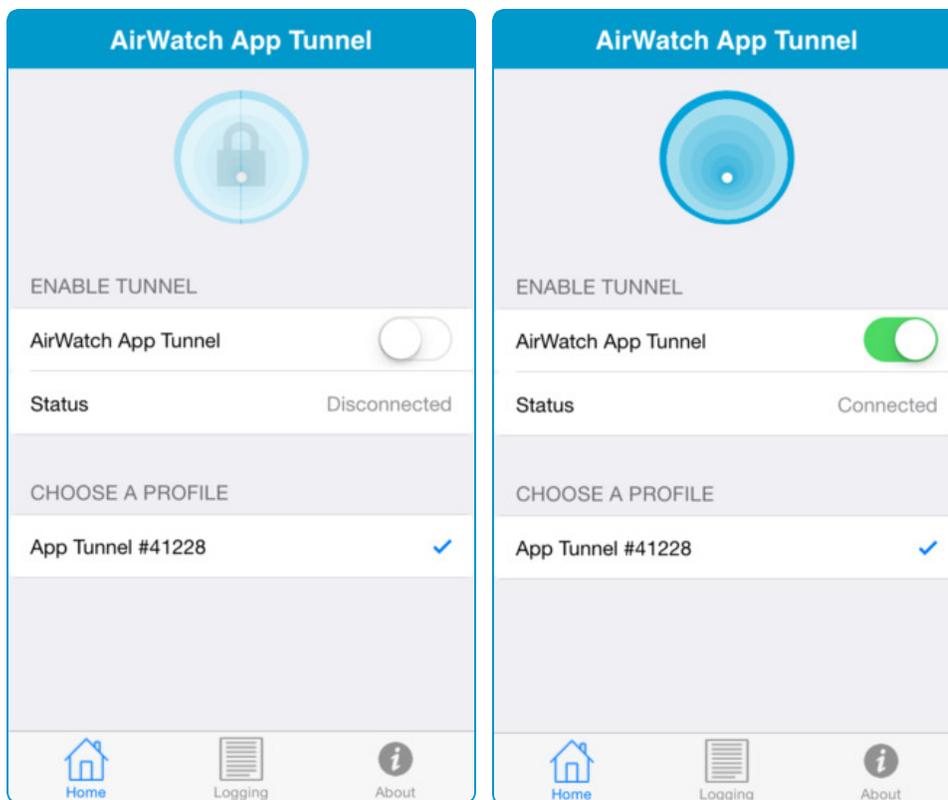
- iOS 8.0+
- Ensure you are on the latest AirWatch version for optimal functionality.

Using the App

Your end users must download and install the AirWatch Tunnel application from the iOS App Store. After installing it, end users have to run it at least once and accept the User Permission prompt.



The AirWatch Tunnel displays as **Connected** whenever an end user opens a managed app that you configured to use the App Tunnel profile or a Safari domain that you set to connect automatically.



Access the VMware Tunnel App for Android

The VMware Tunnel application for Android lets end users access internal corporate Web resources and sites through managed public and internal applications.

Requirements

- Android Agent v5.3+
- Android 4.4+
- Ensure you are on the latest AirWatch version for optimal functionality.

Important: If you are using Per-App Tunnel with Android devices in cascade mode, then ensure that your internal DNS is exposed to the VMware Tunnel front-end server in the DMZ.

For basic endpoint setups, ensure that your internal DNS is exposed to the VMware Tunnel server in the DMZ.

For more information, see the knowledge base article, [Configure Per-App Tunnel DNS entries for Android and Windows 10 devices](https://support.air-watch.com/articles/115001666168) (<https://support.air-watch.com/articles/115001666168>).

Using the App

Your end users must download and install the VMware Tunnel application from the Play Store. After installing it, end users have to run it at least once and accept the connection request.

The VMware Tunnel displays as **Connected** whenever an end user opens a managed app that you configured to use the App Tunnel profile or a domain that you set to connect automatically.

Note: The key icon in the notification center displays on the device because there is an application installed that uses the Per App VPN functionality. This icon does not indicate an active connection or session with the VMware Tunnel server. The key icon displays even if you are not actively browsing.

 Certain Android devices allow end users to disable the VPN on an OS level. This prevents the VMware Tunnel from working on the device. For information on how to correct the issue, see <https://support.air-watch.com/articles/115001666348>

Access the VMware Tunnel App for Windows 10

The VMware Tunnel application for Windows 10 lets end users access internal corporate Web resources and sites through configured applications.

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

Requirements

- Windows 10 Build 14393+
- AirWatch v8.4.8+

Using the App

Your end users must download and install the VMware Tunnel application from the Windows Store. End users must accept an alert dialog the first time they launch an app that triggers the VMware Tunnel app.

When using Windows 10 devices, ensure that your DNS server does not use 192.168.x.x IP as this address is used by the VMware Tunnel Server to assign the IPs to clients (mobile devices). This setting is a configurable setting in server.conf.

The VMware Tunnel displays as **Connected** whenever an end user opens a managed app that you configured to use the App Tunnel profile.

Access the VMware Tunnel App for macOS

The VMware Tunnel application for macOS lets end users access internal corporate Web resources and sites through Safari domains

Requirements

- macOS 10.12+
- AirWatch v9.1+

Using the App

Your end users must download and install the VMware Tunnel application from the App Store.

Upgrade the VMware Tunnel Virtual Appliance

VMware Tunnel is backwards compatible with updated versions of the AirWatch Console. Upgrade the VMware Tunnel product whenever you perform any major version upgrades.

Upgrade Using vSphere

1. Access the admin UI for your VMware Tunnel.
2. Select **Configure Manually**.
3. Scroll down to the bottom and select **Export Unified Access Gateway Settings**.
4. Download the new OVA package from AirWatch Resources (<https://resources.air-watch.com/view/sbfsfykltppqfxhvg9tpy/en>).
5. Deploy the new OVA in place of the existing OVA. Follow the steps you used before. See [Deploy VMware Tunnel using vSphere on page 33](#) for more information.
6. Instead of manually configuring the settings, select **Import Settings**.
7. Browse for the downloaded export JSON file.
8. Select **Import**.

The Unified Access Gateway appliance supports a Zero Downtime Upgrade process. For more information, see the Unified Access Gateway Documentation Center: <https://www.vmware.com/support/pubs/access-point-pubs.html>.

Upgrade Using PowerShell Script

1. Download the new OVA package from AirWatch Resources (<https://resources.air-watch.com/view/sbfsfykltppqfxhvg9tpy/en>).

2. Use the same .ini template from your previous deployment with the PowerShell script.
3. Follow the steps you use before. See [Run the VMware Tunnel PowerShell Script on page 43](#) for more information.

Upgrade Java for Tunnel Proxy Component

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

To upgrade Java without reinstalling Tunnel Proxy:

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

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

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

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

5. Restart the Tunnel Proxy service.

Network Traffic Rules for 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 component of VMware Tunnel, create device traffic rules to control how devices handle traffic from specified applications and server traffic rules to manage network traffic when you have third-party proxies configured.

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

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

Supported Platforms

VMware Tunnel supports Network Traffic rules for the following platforms:

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

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

 Looking for information on Single Sign-On? For information on implementing Android mobile single sign-on for Workspace ONE, see the Workspace ONE Quick Start Guide, available at https://docs.vmware.com/en/VMware-Identity-Manager/3.2/ws1_quickconfiguration.pdf.

Create Device Traffic Rules

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

 Watch a tutorial video explaining how to create device traffic rules: <https://support.airwatch.com/articles/115001666388>.

Prerequisites

- Configured VMware Tunnel with the Per-App Tunnel component enabled.
- For iOS and Android, applies to mobile applications configured for Per App VPN for VMware Tunnel. See [Configure Public Apps to Use Per App Profile on page 51](#) for more information.

Procedure

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Network Traffic Rules**.
2. Configure the Device Traffic Rules settings:

| Settings | Descriptions |
|-----------------------|--|
| Default Action | <p>This rule is automatically configured and applies to all applications except Safari.</p> <p>The default action is always applied last.</p> <ul style="list-style-type: none"> • Tunnel – All apps, except Safari, on the device configured for Per App VPN send network traffic through the tunnel. For example, set the Default Action to Tunnel to ensure all configured apps without a defined traffic rule use the VMware Tunnel for internal communications. • Block – Blocks all apps, except Safari, on the device configured for Per App VPN from sending network traffic. For example, set the Default Action to Block to ensure that all configured apps without a defined traffic rule cannot send any network traffic regardless of destination. • Bypass – All apps, except Safari, on the device configured for Per App VPN bypass the tunnel and connect to the Internet directly. For example, set the Default Action to Bypass to ensure all configured apps without a defined traffic rule bypass the VMware Tunnel to access their destination directly. |
| Add | Select Add to create a rule. |
| Rank | <p>Select the up or down arrows to rearrange the ranking of your network traffic rules. You can also select-and-drag the rule.</p> <p>The up and down arrows only display when you have more than one rule created.</p> |
| Application | <p>Select Add to add a triggering application for the network rule.</p> <p>This drop-down menu is populated with applications with Per App VPN enabled and Safari for macOS.</p> <p>If you configure rules for the Safari app for macOS, the traffic rules override and disable any domain rules configured in existing profiles.</p> |
| Action | <p>Select the action from the drop-down menu that the VMware Tunnel app applies to all network traffic from the triggering app when the app starts.</p> <ul style="list-style-type: none"> • Tunnel – Sends app network traffic for specified domains through the tunnel to your internal network • Block – Blocks all traffic sent to specified domains. • Bypass – Bypasses the VMware Tunnel so the app attempts to access specified domains directly. • Proxy – Redirect traffic to the specified HTTPS proxy for the listed domains. The proxy must be HTTPS and must follow the correct format: <code>https://example.com:port</code> |

| Settings | Descriptions |
|-----------------------------|---|
| Destination Hostname | <p>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.</p> <p>Use a comma (,) to distinguish between hostnames.</p> <p>You may use wildcard characters for your hostnames. Wildcards must follow the format:</p> <ul style="list-style-type: none"> • *.<domain>.* • *<domain>.* • *.* — You cannot use this wildcard for Safari domain rules. • * — You cannot use this wildcard for Safari domain rules. |

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

Create Server Traffic Rules

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

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

To configure server traffic rules:

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

| Settings | Descriptions |
|-----------------------|--|
| Outbound Proxy | |
| Add | Select to add a third-party outbound proxy. You may add additional outbound proxies by selecting Add again. |
| Hostname | Enter the proxy hostname. |
| Port | Enter the port the third-party proxy uses to listen to the VMware Tunnel |
| Authentication | Select the proxy authentication method used. Selecting Basic or Ntlm displays the Credential text box. |
| Credentials | Enter the Username and Password for proxy authentication. |
| Network Rules | |
| Add | Select to add a server traffic rule. |

| Settings | Descriptions |
|-----------------------|--|
| Destination | <p>Enter the destination hostname that triggers the traffic rule.</p> <p>Rules for a Windows 10 device must use IP address as the hostname. Windows 10 devices support using the following wildcards:</p> <ul style="list-style-type: none"> • 10.10.* • 10.10.0.0/16 <p>If you are entering multiple hostnames, separate them by commas. You can use regular expressions in the hostname.</p> |
| Action | <p>Select the action that the VMware Tunnel applies to server traffic for the destination hostname.</p> <ul style="list-style-type: none"> • Bypass – Bypass the proxy and send all traffic directly to the destination hostname. • Proxy – Send server traffic through the outbound proxy. <p>Selecting Proxy displays the Outbound Proxy menu.</p> |
| Outbound Proxy | <p>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.</p> <p>The proxies that populate this menu are those proxies added in the Outbound Proxy Settings section.</p> |

3. (Optional) Add any additional server traffic rules.
4. Select **Save** to save your changes.
5. Select **Publish Rules** to update send the rules to your VMware Tunnel server and auto-configure the servers to use these rules.

Consider checking that your proxies are active and functional before publishing rules.

VMware Tunnel Access Logs and Syslog Integration

AirWatch supports access logs and syslog integration for the Proxy and 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.

The endpoint server writes the access logs. In cascade mode, the back-end server writes the access logs.

For instructions on enabling access log and syslog integration, see [Configure Advanced Settings for VMware Tunnel on page 29](#).

Using a Linux Server to act as a Syslog Host

Most Linux servers by default have support for syslog. To enable a Linux server to act as syslog host, navigate to `rsyslog.conf`:

```
vi /etc/rsyslog.conf
```

Uncomment the features under UDP syslog reception:

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

To view the logs, enter the following command:

```
tail -f /var/log/messages | grep <rsyslog_dent>
```

Make sure UDP port 514 is open routing to the syslog server:

```
-A INPUT -p udp -m udp -dport 514 -j ACCEPT
```

VMware Tunnel SSL Offloading

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

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

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

You can perform SSL offloading with products such as F5's BIG-IP Local Traffic Manager (LTM), or Microsoft's Unified Access Gateway (UAG), 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 AirWatch console for the Tunnel Proxy must be imported to the SSL Termination Proxy.

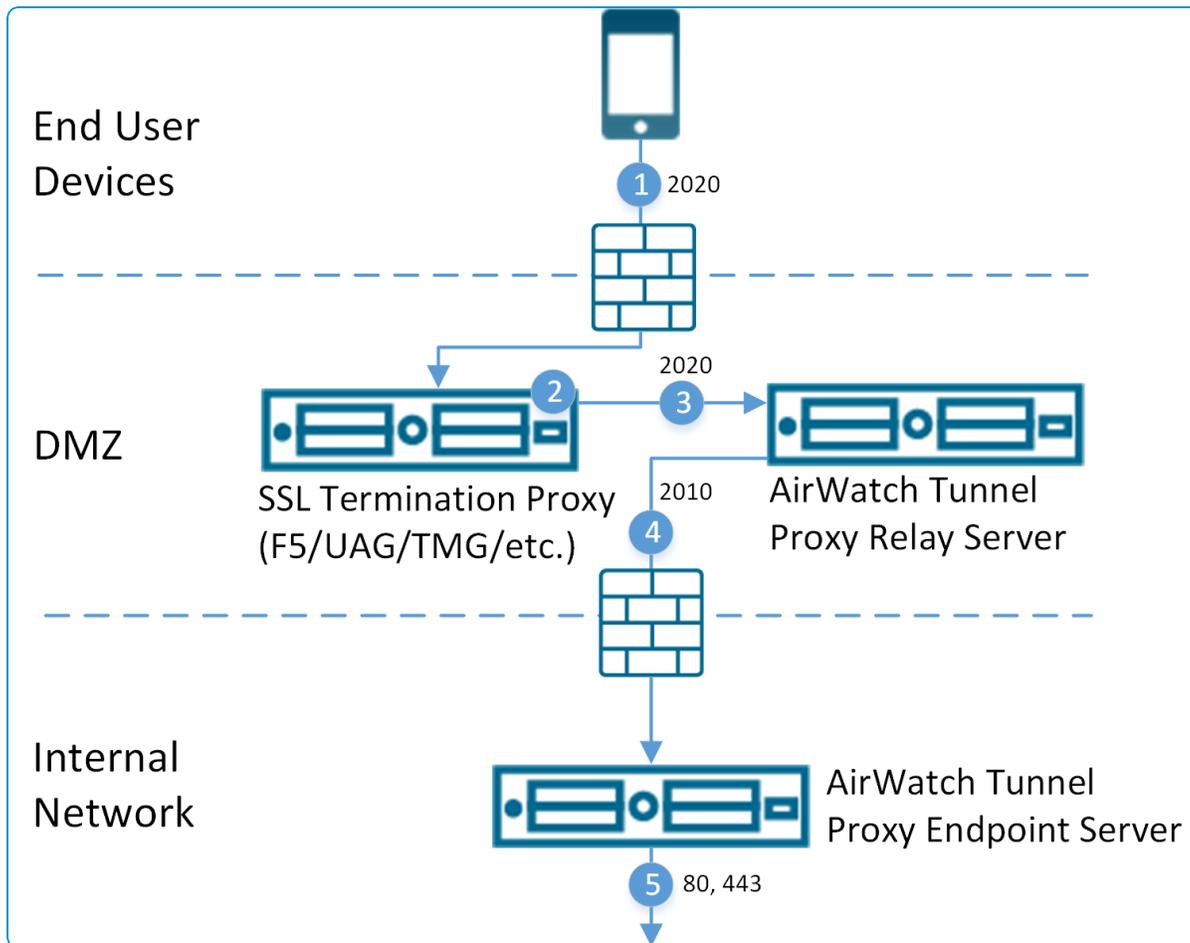
Ensure settings are configured properly in the AirWatch console, VMware Tunnel server, and your SSL Off loading solution in order to successfully implement SSL Offloading for the Tunnel Proxy.

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 an AirWatch Certificate and not a public SSL certificate, then you can export the SSL certificate from the AirWatch 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 an AirWatch SDK-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 AirWatch 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 an AirWatch Certificate and not a public SSL certificate, then you can export the SSL certificate from the AirWatch 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 AirWatch 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.

Kerberos KDC Proxy Support

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

AirWatch KKDCP acts as a proxy to your internal KDC server. AirWatch-enrolled and compliant devices with a valid AirWatch 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.

For HTTPS sites, VMware Browser for Android supports Kerberos authentication only when the site also has NTLM authentication enabled. This requirement is because the Android WebView, on which the VMware Browser is built, does not support Kerberos authentication natively.

HTTP Sites do not require NTLM authentication as the VMware Tunnel can perform Kerberos authentication without NTLM being enabled.

Currently, this functionality is only supported with the VMware Browser v2.5 and higher for Android.

Enable Kerberos Proxy Settings

Enable [Kerberos KDC Proxy Support on page 63](#) during your initial VMware Tunnel configuration. AirWatch KKDCP acts as a proxy to your internal KDC server.

To enable Kerberos proxy settings:

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

Mobile Access Gateway Configuration

Configuration Type > **Details** > Authentication > Summary

Configuration requires an on-premise installation of the MAG server. Upon successfully completing the configuration, you will be able to download the installer for the MAG application

APP WRAPPING / BROWSER / SDK CONFIGURATION

Endpoint Host Name*

Default HTTP Port*

Default HTTPS Port*

Use Kerberos Proxy ⓘ

Realm ⓘ

2. If the Realm is not reachable, then you can configure the **KDC server IP** on the **Advanced** settings tab in system settings.

AirWatch Certificate

Thumbprint : C0DF30FE0637989BBB1DA05B469DAA875A769E

Expires on: 10/23/2034

Generating new certificates will require you to rerun the installer

KERBEROS PROXY

KDC Server IP

Kerberos Proxy Port

PER-APP VPN

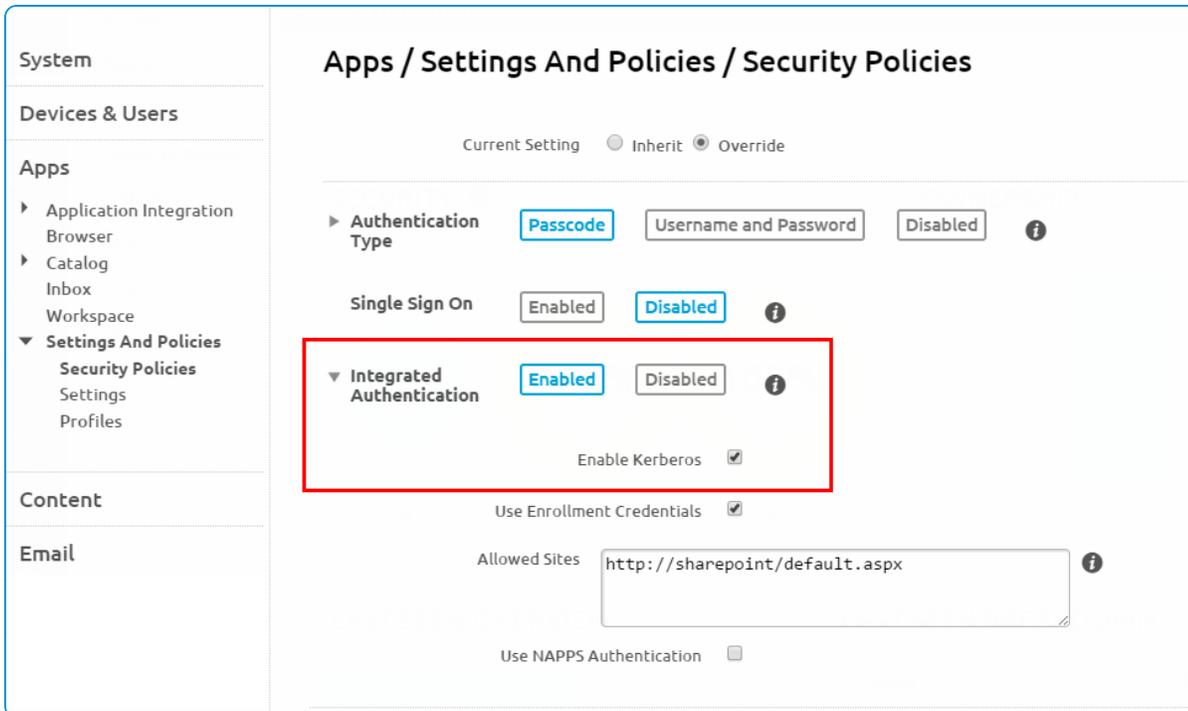
Log Level

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

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

3. Save the settings and download the installer to install VMware Tunnel Proxy.
4. Enable Kerberos from the SDK settings in the AirWatch Console so the requesting application is aware of the KDC.

Navigate to **Groups & Settings > All Settings > Apps > Settings And Policies** and select **Security Policies**. Under Integrated Authentication, select **Enable Kerberos**. Save the settings.



Accessing Logs

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

```
{
  "kdcServer": "internal-dc01.internal.local.:88",
  "kdcAccessible": true
}
```

VMware Tunnel Outbound Proxy Overview

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, AirWatch supports outbound proxies for the two VMware Tunnel components: Proxy and Per-App Tunnel.

Outbound Proxy for the Proxy Component

Configure an outbound proxy for the VMware Tunnel Proxy component to control the flow of traffic within your network. The following table illustrates outbound proxy support for the VMware Tunnel Proxy component on Linux:

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

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

Outbound Proxy with Authentication

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

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

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

PAC Files and Multiple Outbound Proxies

A PAC file is a set of rules that a browser checks against to determine where traffic is routed. If you want to use a proxy auto configuration (PAC) file, then provide the path to the PAC file location when prompted during Tunnel installation. If you want to use a PAC file for an outbound proxy that requires authentication, or if you want to use multiple proxies with different hostnames, or if some proxies require authentication (basic/NTLM) and some do not, then refer to [Use the Proxy Tool for PAC Files and Multiple Outbound Proxies \(Proxy Component\) on page 66](#).

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

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

To use the tool, perform the following steps:

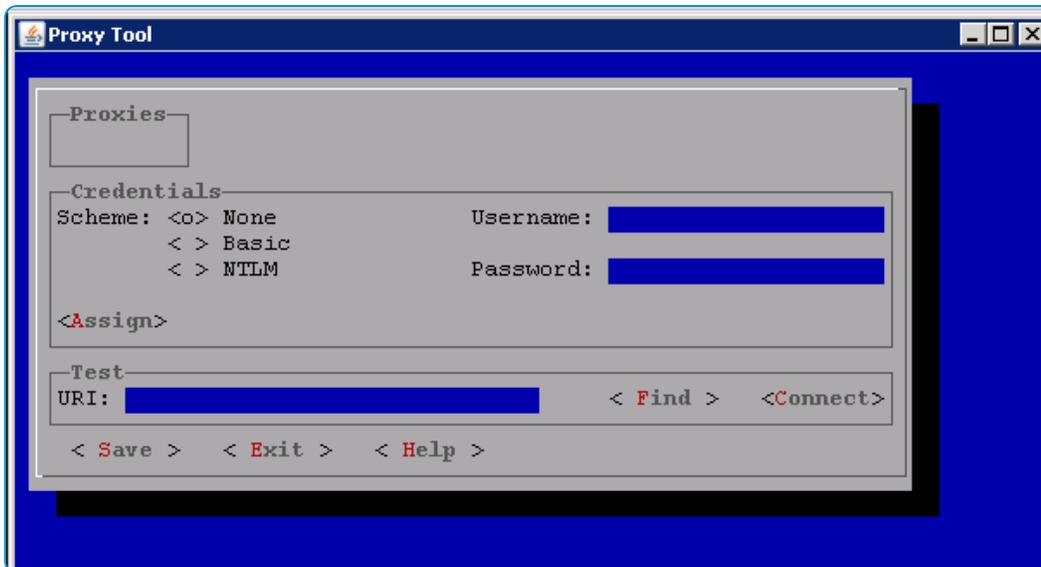
1. Within Linux CLI mode, navigate to `/opt/vmware/tunnel/proxy/tools`.
2. Convert the proxy tool to an executable by using the following command:

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

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

```
sudo sh Proxytools.sh
```

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



5. Select **Save**.

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

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

VMware Tunnel Proxy Tools

The Proxy Tool is an application you can run to configure multiple outbound proxies for the VMware Tunnel. For more information, see [Use the Proxy Tool for PAC Files and Multiple Outbound Proxies \(Proxy Component\) on page 66](#).

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.

Outbound Proxy for the Per-App Tunnel Component

Configure an outbound proxy for the VMware Tunnel Per-App Tunnel component to control the flow of traffic within your network.

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

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

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

Configure the rules for sending traffic to your outbound proxies using the server traffic rules. For more information, see [Create Server Traffic Rules on page 59](#).

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

VMware Tunnel PAC Utility

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

The PAC utility is packed with the VMware Tunnel installer bundle available on AirWatch Resources. Install the PAC utility on any Linux server such as your VMware Tunnel server. Installation requires extracting the PAC utility and running the install script.

The PAC Utility only supports Linux servers currently.

The PAC utility does not support the following rules:

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

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

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

RSA Adaptive Authentication for VMware Tunnel

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.

Step-Up Authentication Workflow

There are two main workflows to consider when using step-up authentication with this integration:

- 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 AirWatch 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 already set their SecurID PIN.

Users who have already 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).

Requirements

- 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.
- RSA Adaptive Authentication information configured in the AirWatch Console.
 - In the AirWatch Console, you must enter some 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. For more details on these settings, see [Configure Advanced Settings for VMware Tunnel on page 29](#).

Client Compatibility

- AirWatch iOS Browser v4.5+
AirWatch Android Browser v3.1+
- AirWatch iOS SDK v5.5+
- AirWatch Android SDK v15.11+

Appendix:

VMware Tunnel Troubleshooting

If you encounter issues with your VMware Tunnel deployment, the component logs allow you to diagnose issues. These logs are useful when contacting AirWatch Support.

To simplify troubleshooting your VMware Tunnel deployment, consider using the `tunnel_snap` utility. For more information, see [Tunnel_Snap Troubleshooting Utility on page 73](#).

Per-App Tunnel

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

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

Change Log Level

Change the log level to meet your troubleshooting need.

To change the log level:

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

Enabling Debug in rsyslog:

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

Virtual Appliance Logs

You can access the VMware Tunnel logs from the virtual appliance by accessing a specific URL based on your deployment. Enter the URL into a browser to download a ZIP file that contains your logs.

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

Commands

Virtual Appliance

```
systemctl start vpnd - Starts the service.
systemctl stop vpnd - Stops the service.
systemctl restart vpnd - Restarts the service.
```

CentOS/RHEL 6.x:

```
service vpnd start - Starts the service.
service vpnd stop - Stop the service.
service vpnd restart - Restarts the service.
```

CentOS/RHEL 7.x:

```
systemctl start vpnd - Starts the service.
systemctl stop vpnd - Stops the service.
systemctl restart vpnd - Restarts the service.
```

Proxy

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

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

Virtual Appliance Logs

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

Commands

Proxy – Any CentOS/RHEL version/Virtual Appliance:

```
sudo service proxy start - Starts the service.
sudo service proxy stop - Stops the service.
sudo service proxy restart - Restarts the service.
sudo service proxy status - Shows the status of the service.
```

Change Proxy Log Level

You can change the log levels for the Proxy component in the AirWatch Console by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration > Advanced**. In cases where

communication breaks between the VMware Tunnel and AWCM or API, you can still change the log level with the following steps:

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

Tunnel_Snap Troubleshooting Utility

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

The utility captures data from the following files:

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

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

Run the utility in the following folder:

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

Use the following command to run the utility:

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

The utility collects the diagnostic data in:

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

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

Chapter 7:

Tunnel Server Installer Method

| | |
|--|----|
| VMware Tunnel Linux Installer Overview | 76 |
| VMware Tunnel for Linux System Requirements | 76 |
| Manual Installation of Packages | 80 |
| VMware Tunnel Multi-tier Installation Overview | 81 |
| Basic (Endpoint only) Install Overview | 87 |
| Uninstall the VMware Tunnel | 90 |
| Upgrade the VMware Tunnel for Linux | 90 |

VMware Tunnel Linux Installer Overview

For customers who do not want to use the AirWatch virtual appliance deployment, AirWatch offers the Linux installer so you can configure, download, and install VMware Tunnel onto a server.

The Linux installer has different prerequisites than the virtual appliance method. To run the Linux installer, you must meet specific hardware, software, and general requirements before you can begin installation. Using the virtual appliance simplifies the requirements and installation process.

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

VMware Tunnel for Linux System Requirements

To deploy VMware Tunnel for Linux, ensure that your system meets the requirements.

Use the following requirements as a basis for creating your VMware Tunnel server.

| Requirement | | | | |
|--|--|---|---|---|
| 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, AirWatch recommends deploying at least 2 load-balanced servers with 2 CPU Cores each regardless of number of devices for uptime and performance purposes. | | | | |
| **About 10 GB is for a typical deployment. Log file size should be scaled based on your log usage and requirements for storing logs. | | | | |

Software Requirements for VMware Tunnel

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

| Requirement | Notes |
|---|-----------------------|
| Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7 | (Recommended UI-less) |

| Requirement | Notes |
|---|---|
| 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 | AirWatch 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 AirWatch 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. |

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

General Requirements for VMware Tunnel

Ensure your VMware Tunnel is set up with the following general requirements to ensure a successful installation.

| Requirement | Notes |
|--|--|
| SSH access to Linux Servers available to AirWatch and Administrator rights | |
| Administrator account with root privileges to the server | It is required that the root account has full permissions to write files. If using an account other than root, the account MUST have sudo access with the same privilege as root. Admin accounts must have write and run permissions for the /opt/*, /tmp/*, and /etc/* directories. If this condition is not met, the installation is likely to fail. Once installation is complete, restrictions can be put into place for these account types. If you are installing as an account other than root, ensure that the root user is not removed from the sudoers file on the Tunnel server. |
| VMware Tunnel has outbound Internet access | The VMware Tunnel installer automatically downloads required packages if it is connected to the Internet. If your server is offline or has restricted outbound access, then see Manual Installation of Packages on page 80 . |
| IPv6 enabled locally | IPv6 must be enabled locally on the Tunnel server hosting Per-App Tunnel. AirWatch requires it to be enabled for the Per-App Tunnel service to run successfully. |

Network Requirements for VMware Tunnel

For configuring the ports listed below, all 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 -tln https://<AirWatch_Tunnel_Host>:<port> | 1 |
| Devices (from Internet and Wi-Fi) | VMware Tunnel Per-App Tunnel | TCP | 8443* (for Per-App Tunnel) | | 1 |
| VMware Tunnel – Basic Endpoint Configuration | | | | | |
| VMware Tunnel | AirWatch Cloud Messaging Server** | HTTPS | SaaS: 443 On-Prem: 2001* | Verify by using wget to https://<AWCM URL>:<port>/awcm/status and ensuring you receive an HTTP 200 response. | 2 |
| VMware Tunnel | Internal Web sites / Web apps | HTTP or HTTPS | 80 or 443 | | 4 |
| VMware Tunnel | Internal resources | HTTP, HTTPS, or TCP | 80, 443, Any TCP | | 4 |
| VMware Tunnel | AirWatch REST API Endpoint SaaS: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com On-Prem: Most commonly your DS or Console server | HTTP or HTTPS | SaaS: 443 On-Prem: 80 or 443 | <pre>curl -Iv https://<API URL>/api/mdm/ping</pre> The expected response is HTTP 401 – unauthorized. | 5 |

| Source Component | Destination Component | Protocol | Port | Verification | Note |
|---|--|---------------|---|---|------|
| VMware Tunnel — Cascade Configuration | | | | | |
| VMware Tunnel Front-End | AirWatch Cloud Messaging Server** | TLS v1.2 | SaaS: 443 On-Prem: 2001* | Verify by using wget to https://<AWCM URL>:<port>/awcm/status and ensuring you receive an HTTP 200 response. | 2 |
| VMware Tunnel Front-End | VMware Tunnel Back-End | TLS v1.2 | 8443* | Telnet from VMware Tunnel Front-End to the VMware Tunnel Back-End server on port | 3 |
| VMware Tunnel Back-End | AirWatch Cloud Messaging Server** | TLS v1.2 | SaaS: 443 On-Prem: 2001* | Verify by using wget to https://<AWCM URL>:<port>/awcm/status and ensuring you receive an HTTP 200 response. | 2 |
| VMware Tunnel Back-End | Internal Web sites / Web apps | TCP | 80 or 443 | | 4 |
| VMware Tunnel Back-End | Internal resources | TCP | 80, 443, Any TCP | | 4 |
| VMware Tunnel Front-End and Back-End | AirWatch REST API Endpoint SaaS: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com On-Prem: Most commonly your DS or Console server | TLS v1.2 | 80 or 443 | <pre>curl -Ivv https://<API URL>/api/mdm/ping</pre> The expected response is HTTP 401 – unauthorized. | 5 |
| VMware Tunnel – Relay Endpoint Configuration | | | | | |
| VMware Tunnel Relay | AirWatch Cloud Messaging Server** | HTTP or HTTPS | SaaS: 443 On-Prem: 2001* | Verify by using wget to https://<AWCM URL>:<port>/awcm/status and ensuring you receive an HTTP 200 response. | 2 |
| VMware Tunnel Relay | VMware Tunnel Endpoint | HTTPS | 2010* | Telnet from VMware Tunnel Relay to the VMware Tunnel Endpoint server on port | 3 |

| Source Component | Destination Component | Protocol | Port | Verification | Note |
|----------------------------------|--|---------------------|------------------|--|------|
| 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 | AirWatch REST API Endpoint SaaS: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com On-Prem: Most commonly your DS or Console server | HTTP or HTTPS | 80 or 443 | <pre>curl -Ivv https://<API URL>/api/mdm/ping</pre> <p>The expected response is HTTP 401 – unauthorized.</p> | 5 |

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

** For SaaS customers who need to whitelist outbound communication, please refer to the following AirWatch Knowledge Base article for a list of up-to-date IP ranges AirWatch currently owns: <https://support.airwatch.com/articles/115001662168>.

1. For devices attempting to access internal resources.
2. For the VMware Tunnel to query the AirWatch 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.

Manual Installation of Packages

The VMware Tunnel Linux installer automatically downloads required packages if 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.

| Package | Command |
|---------|---|
| Openssl | <code>sudo yum -y install openssl</code> |
| Haveged | <code>sudo yum -y install haveged*</code> |
| Nscd | <code>sudo yum -y install nscd</code> |
| Json-c | <code>sudo yum -y install json-c</code> |

| Package | Command |
|---------|---|
| libxml2 | <code>sudo yum -y install libxml2</code> |
| log4cpp | <code>sudo yum -y install log4cpp*</code> |

* For CentOS/RHEL 7.x systems, you may require installing the epel-release rpm to install these packages through yum.

VMware Tunnel Multi-tier Installation Overview

During VMware Tunnel configuration, you specify whether you are installing in a multi-tier or single-tier configuration. Use the following instructions for multi-tier configurations.

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 AirWatch Tunnel Front-End Server(Linux)

After ensuring that your servers meets all the proper requirements, configuring VMware Tunnel settings in the AirWatch Console, and downloading the installer to your Linux server, you can run the installer to enable the service.

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

Prerequisites

- Download the installer and transfer to the server. The link in the AirWatch Console directs you to AirWatch 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` file from the AirWatch Console and transfer to the server.

Procedure

Perform the following steps on the front-end server:

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

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

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

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

Launching installer...

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

Preparing CONSOLE Mode Installation..

=====
Introduction
=====

InstallAnywhere will guide you through the installation of AirWatch Tunnel.

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

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

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

PRESS <ENTER> TO CONTINUE:
```

Press **Enter**.

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

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

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

Select the installation type: █
```

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

```

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

Please Review the Following Before Continuing:

Product Name:
  VMware Tunnel

Product Features:
  VMware Per-App Tunnel,
  VMware Proxy

PRESS <ENTER> TO CONTINUE: █

```

Press **Enter**.

Continue to Step 5.

- Option 2: 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 AirWatch Console.

Continue to Step 5.

5. Enter Relay or Front as the configuration type for VMware Tunnel Setup.
6. Enter Y to grant the installer firewall permissions needed for VMware Tunnel.

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

7. Review and verify the summary information.

```

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

Please Review the Following Before Continuing:

Product Name:
  VMware Tunnel

Install Folder:
  /opt/vmware/tunnel

Product Features:
  VMware Per-App Tunnel,
  VMware Proxy

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

PRESS <ENTER> TO CONTINUE: █

```

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

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

To complete your installation, see [Install the AirWatch Tunnel Back-End Server \(Linux\) on page 84](#).

Install the AirWatch Tunnel Back-End Server (Linux)

In multi-tier configurations, you install the back-end server after installing the front-end server. If you have not already, perform the steps described in [Install the AirWatch Tunnel Front-End Server\(Linux\) on page 81](#).

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

Prerequisites

- Download the installer onto the server. The link in the AirWatch Console directs you to AirWatch Resources to download the installer.
- Download the config.xml file from the AirWatch Console onto the server.

Procedure

Perform the following steps on the endpoint server:

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

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

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

```

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

Launching installer...

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

Preparing CONSOLE Mode Installation...

=====
Introduction
=====

InstallAnywhere will guide you through the installation of AirWatch Tunnel.

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

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

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

PRESS <ENTER> TO CONTINUE:

```

Press **Enter**.

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

```

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

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

Select the installation type: █

```

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

Press **Enter**.

Continue to Step 5.

- Option 2: Import Config.xml file
 - a. Select the components you want to install.
 - b. Enter the file path of the configuration file.
 - c. Enter the VMware Tunnel certificate password as entered in the AirWatch Console.

Continue to Step 5.

5. Enter **Endpoint** or **Back** as the configuration type for VMware Tunnel Setup.
6. Enter **Y** or **N** for whether you want to use an outbound proxy as part of your VMware Tunnel configuration. This option only displays if you are installing the Proxy component.
7. Enter **Y** to grant the installer firewall permissions needed for VMware Tunnel.

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

8. Review and verify the summary information.

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

Please Review the Following Before Continuing:

Product Name:
  VMware Tunnel

Install Folder:
  /opt/vmware/tunnel

Product Features:
  VMware Per-App Tunnel,
  VMware Proxy

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

PRESS <ENTER> TO CONTINUE: █
```

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

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

Verify Your VMware Tunnel Installation

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

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

Proxy component.

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

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

Basic (Endpoint only) Install Overview

During VMware Tunnel configuration, you specify whether you are installing in a multi-tier or single-tier configuration. Use the following instructions for single-tier configurations. During installation, you specify whether you are installing proxy, Per-App Tunnel, or both.

Install the VMware Tunnel – Basic (Linux)

After ensuring that your server meets all the proper requirements, configuring VMware Tunnel settings in the AirWatch 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 AirWatch Console directs you to AirWatch Resources to download the installer.
- Download the config.xml file from the AirWatch Console onto the server.

Procedure

Perform the following steps on your single VMware Tunnel server:

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

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

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

```

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

Launching installer...

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

Preparing CONSOLE Mode Installation...

=====
Introduction
=====

InstallAnywhere will guide you through the installation of AirWatch Tunnel.

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

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

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

PRESS <ENTER> TO CONTINUE:

```

Press **Enter**.

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

```

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

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

Select the installation type: █

```

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

Press **Enter**.

Continue to Step 5.

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

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

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

6. Review and verify the summary information.

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

Please Review the Following Before Continuing:

Product Name:
  VMware Tunnel

Install Folder:
  /opt/vmware/tunnel

Product Features:
  VMware Per-App Tunnel,
  VMware Proxy

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

PRESS <ENTER> TO CONTINUE: █
```

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

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

Verify Your VMware Tunnel Installation

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

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

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

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

Uninstall the VMware Tunnel

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

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

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

2. Execute **Uninstall_Tunnel**.

```
sudo ./Uninstall_Tunnel
```

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

Upgrade the VMware Tunnel for Linux

VMware Tunnel is backwards compatible with updated versions of the AirWatch Console. Upgrade the VMware Tunnel product whenever you perform any major version upgrades.

To upgrade an existing VMware Tunnel, download the latest version of the installer from the AirWatch Console. Load the installer onto one or more VMware Tunnel servers and run the installer following the same procedures outlined in the installation chapters of this document 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 may want to reference after the upgrade and create a snapshot of each VMware Tunnel server before the upgrade.

To upgrade VMware Tunnel:

1. Log in to the AirWatch 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 AirWatch Resources to download the installer.
3. Create a directory for the Tunnel installer and copy the `VMwareTunnel.bin` file to this location.
4. Continue with the steps for [Install the AirWatch Tunnel Front-End Server\(Linux\) on page 81](#) or [Install the AirWatch Tunnel Back-End Server \(Linux\) on page 84](#).

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

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm and search for the document you need. Each release-specific document has a link to its PDF copy on AirWatch Resources.

Alternatively, you can navigate to AirWatch Resources on myAirWatch (resources.air-watch.com) and search. When searching for documentation on Resources, be sure to select your AirWatch version. You can use the filters to sort by PDF file type and AirWatch v9.3.