VMware Tunnel Guide for Windows

Installing 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

Copyright © 2018 VMware, Inc. All rights reserved.

Copyright © 2018 VMware, Inc. All rights reserved.

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 9.

2. Configure your server with the appropriate network rules.

   See VMware Tunnel Installation Preparation Overview on page 14.

3. Configure VMware Tunnel settings in the AirWatch Console.

   See Configure VMware Tunnel Proxy (Legacy MAG) on page 21.

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 25.

5. Run the installer you downloaded post-configuration on your VMware Tunnel server.

   See Install the AirWatch Tunnel Relay Server (Windows) on page 27 or Install the AirWatch Tunnel – Basic (Windows) on page 37.

Copyright © 2018 VMware, Inc. All rights reserved.

Chapter 1: Overview

Copyright © 2018 VMware, Inc. All rights reserved.

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.

Whether it is for a global sales staff member, a traveling executive, or any other employee trying to access the company intranet from outside of the office, mobile access to enterprise resources is becoming a necessity in today's work environments. This access extends to far more than just corporate email access. Your employees may require access to:

- Corporate intranet sites to keep up with internal announcements and collaborate with other employees.
- Other internal resources to gather Business Intelligence (BI) data, provide secure transactions, or fetch the most recent corporate updates from mobile applications.

The VMware Tunnel makes it possible to meet all the requirements of employee access and IT security by providing a secure and effective method for individual applications to access corporate resources.

By serving as a relay between your mobile devices and enterprise systems, the VMware Tunnel authenticates and encrypts traffic from individual applications on compliant devices to the back-end systems they are trying to reach.

Use the VMware Tunnel to access the following internal resources over HTTP(S):

- Internal Web sites and Web applications through VMware Browser.
- Any other enterprise system accessible over HTTP(S) from your business applications through AirWatch App Wrapping.

The VMware Tunnel also helps to enable BYOD in your organization. By separating access between personal and business applications and data on your device, a device can be thought of as having two owners: an employee with business needs and an ordinary user with personal needs. The VMware Tunnel allows business applications to access your enterprise systems over HTTP(S) but keep end-user personal applications segregated by preventing enterprise access.

Because the VMware Tunnel is architected as part of AirWatch Enterprise Mobility Management (EMM), administrators can view an intuitive and action-oriented display of mobile access information directly from the AirWatch Console. System administrators are put in the position of managing proactively instead of reactively by easily identifying at-risk devices and managing exceptions.

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.

Copyright © 2018 VMware, Inc. All rights reserved.

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.
- **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.

Copyright © 2018 VMware, Inc. All rights reserved.

Chapter 2:
Architecture and Security

Copyright © 2018 VMware, Inc. All rights reserved.

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 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.

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 SaaS Deployments Architecture

SaaS deployments support basic and relay-endpoint configurations. In a SaaS deployment, AirWatch hosts certain components, such as the Console and API servers, in the cloud.

The following diagrams illustrates both the basic and relay-endpoint deployment models. For more information about the traffic between components, see the Network Requirements part of the VMware Tunnel System Requirements section.

Basic Endpoint Workflow

1. The AirWatch Cloud communicates with end-user devices to perform initial device enrollment, which includes creating and delivering certificates.
2. The VMware Tunnel server retrieves the certificates used for authentication from the AirWatch Cloud. It also communicates with the AirWatch API for initialization.
3. End users access internal websites through the proxy component over port 2020 by default.
4. The VMware Tunnel server communicates with your internal servers to retrieve the resources end users are trying to access.

Relay-Endpoint Workflow

1. The AirWatch Cloud communicates with end-user devices to perform initial device enrollment, which includes creating and delivering certificates.
2. The VMware Tunnel Relay server retrieves the certificates used for authentication from the AirWatch Cloud. It also communicates with the AirWatch API for initialization.
3. End users access internal websites through the proxy component over port 2020 by default.
4. The VMware Tunnel Relay server fields the request and forward it to the VMware Tunnel endpoint server over port 2010 by default.
5. The VMware Tunnel server communicates with your internal servers to retrieve the resources end users are trying to access.

Copyright © 2018 VMware, Inc. All rights reserved.

VMware Tunnel On-Premises Deployments

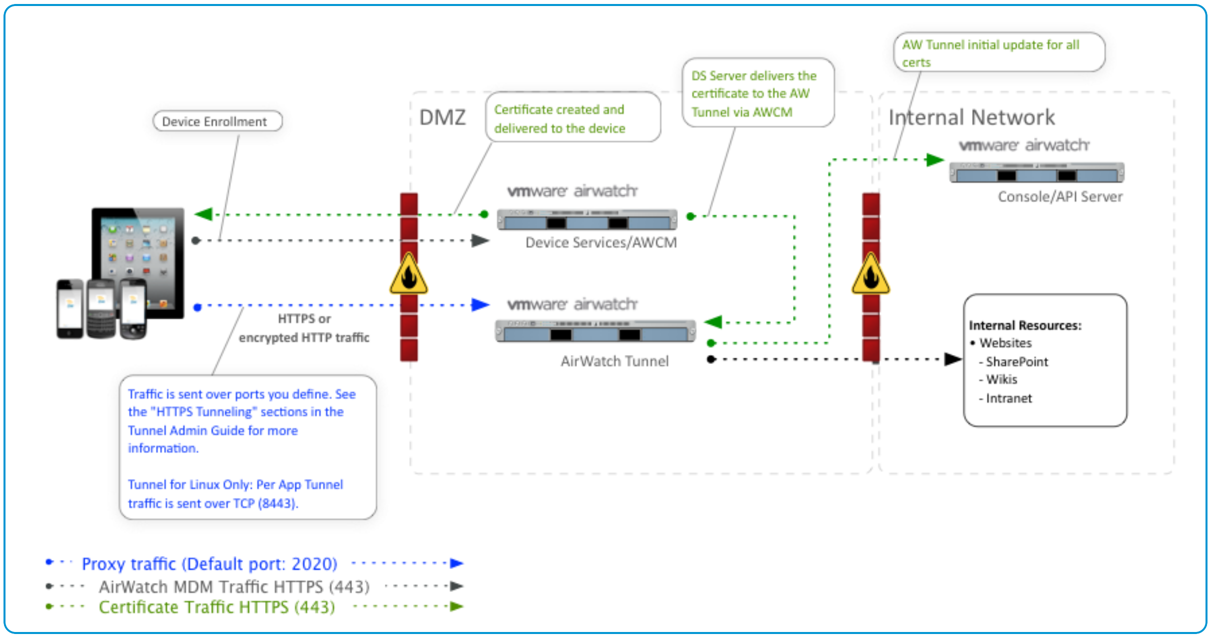
On-premises deployments support basic and relay-endpoint configurations. In this configuration, your organization hosts all AirWatch components and servers on its internal networks.

Basic Endpoint

In a basic endpoint deployment, the VMware Tunnel is behind a WAF and resides on an internal network. The traffic from your managed devices is sent securely over an HTTP or HTTPS transport and its message level is signed using unique X.509 certificates. All deployment configurations support load balancing and reverse proxy.

- For VMware Tunnel Proxy for Windows, basic endpoint can apply to the Proxy component.

These components can be installed on shared or dedicated servers. The following image shows a single server for all components.

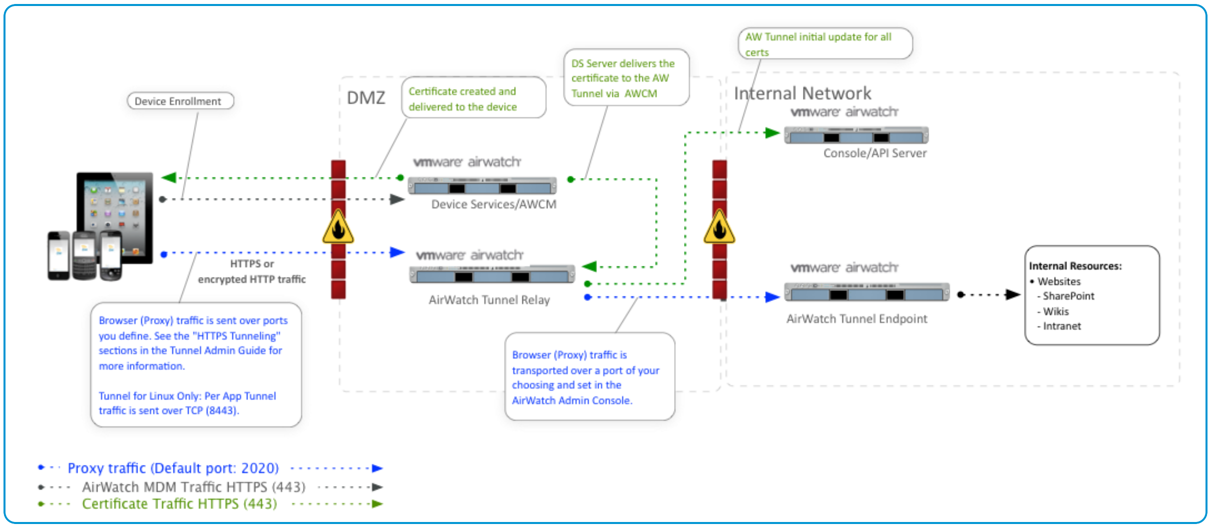

AW Tunnel initial update for all certs
DS Server delivers the certificate to the AW Tunnel via AWCM
Certificate created and delivered to the device
Device Enrollment
DMZ
Internal Network
vmware airwatch
Console/API Server
vmware airwatch
Device Services/AWCM
vmware airwatch
AirWatch Tunnel
HTTPS or encrypted HTTP traffic
Internal Resources:
• Websites
- SharePoint
- Wikis
- Intranet
Traffic is sent over ports you define. See the "HTTPS Tunneling" sections in the Tunnel Admin Guide for more information.
Tunnel for Linux Only: Per App Tunnel traffic is sent over TCP (8443).
Proxy traffic (Default port: 2020)
AirWatch MDM Traffic HTTPS (443)
Certificate Traffic HTTPS (443)

Relay-Endpoint

In a multiple network zones deployment, the VMware Tunnel is used in an on-premises (non-SaaS) environment to integrate with internal systems from a DMZ server connection. All deployment configurations support load balancing and reverse proxy.

- For VMware Tunnel Proxy for Windows, basic endpoint can apply to the Proxy component.

Copyright © 2018 VMware, Inc. All rights reserved.


Device Enrollment
DMZ
Certificate created and delivered to the device
DS Server delivers the certificate to the AW Tunnel via AWCM
AW Tunnel initial update for all certs
Internal Network
vmware airwatch
Console/API Server
vmware airwatch
Device Services/AWCM
vmware airwatch
AirWatch Tunnel Relay
HTTPS or encrypted HTTP traffic
vmware airwatch
AirWatch Tunnel Endpoint
Internal Resources:
• Websites
- SharePoint
- Wikis
- Intranet
Browser (Proxy) traffic is sent over ports you define. See the "HTTPS Tunneling" sections in the Tunnel Admin Guide for more information.
Tunnel for Linux Only: Per App Tunnel traffic is sent over TCP (8443).
Browser (Proxy) traffic is transported over a port of your choosing and set in the AirWatch Admin Console.
Proxy traffic (Default port: 2020)
AirWatch MDM Traffic HTTPS (443)
Certificate Traffic HTTPS (443)

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.

Copyright © 2018 VMware, Inc. All rights reserved.

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 51.

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.
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.
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.

Copyright © 2018 VMware, Inc. All rights reserved.

Chapter 3:
Installation Preparation

Copyright © 2018 VMware, Inc. All rights reserved.

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, seeIntroduction 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".

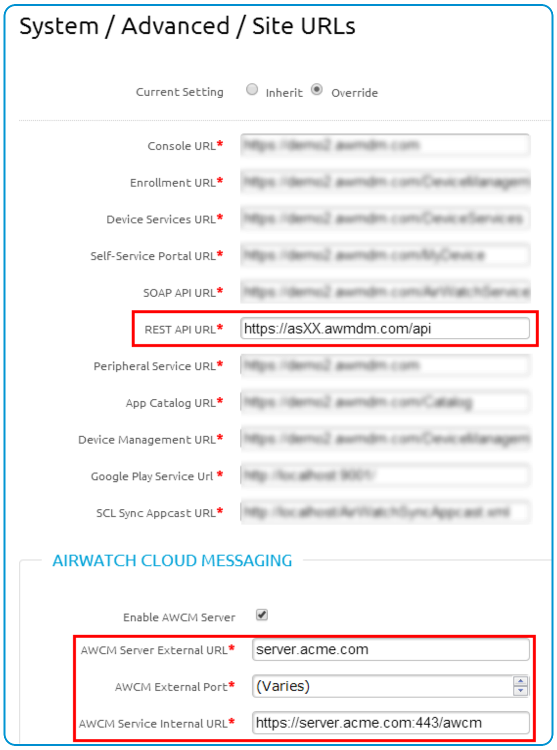
   Saas customers must contact AirWatch support to get their REST API URL.

   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.

Copyright © 2018 VMware, Inc. All rights reserved.



System / Advanced / Site URLs

Current Setting ○ Inherit ● Override

Console URL* [redacted]

Enrollment URL* [redacted]

Device Services URL* [redacted]

Self-Service Portal URL* [redacted]

SOAP API URL* [redacted]

REST API URL* https://asXX.awmdm.com/api

Peripheral Service URL* [redacted]

App Catalog URL* [redacted]

Device Management URL* [redacted]

Google Play Service Url * [redacted]

SCL Sync Appcast URL* [redacted]

AIRWATCH CLOUD MESSAGING

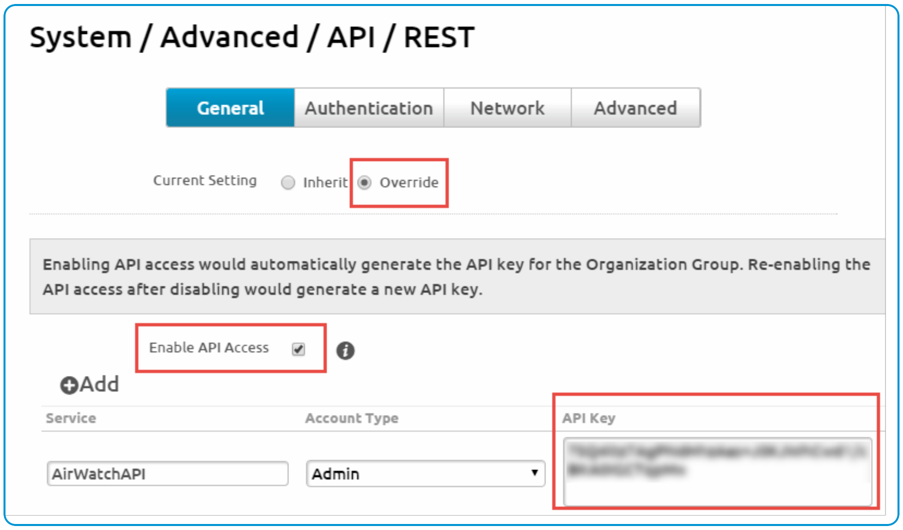
Enable AWCM Server ☑

AWCM Server External URL* server.acme.com

AWCM External Port* (Varies)

AWCM Service Internal URL* https://server.acme.com:443/awcm

3. Select **Save**.
4. Navigate to **Groups & Settings** > **All Settings** > **System** > **Advanced** > **API** > **REST API** and select the **Override** radio button.



System / Advanced / API / REST

Current Setting ○ Inherit ● Override

Enabling API access would automatically generate the API key for the Organization Group. Re-enabling the API access after disabling would generate a new API key.

Enable API Access ☑

Service	Account Type	API Key
AirWatchAPI	Admin	[redacted]

5. Ensure that the **Enable API Access** check box is selected and an API Key is displayed in the text box.
6. Select **Save**.

VMware Tunnel System Requirements (Windows)

To deploy VMware Tunnel for Windows, ensure your system meetings the requirements.

Copyright © 2018 VMware, Inc. All rights reserved.

Hardware Requirements

Use the following requirements as a basis for creating your VMware Tunnel server, which can be a VM or physical server (64-bit).

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)	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. CPU Cores should each be 2.0 GHz or higher. An Intel processor is required.

**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	
Windows Server 2008 R2 or Windows Server 2012 or Windows Server 2012 R2		
Install 64-bit Java Runtime Environment version 7 or greater	Do not pre-install Java, the Tunnel installer automatically installs **Note:** Ensure that 32-bit Java is not installed.	
Internally registered DNS record	Register the VMware Tunnel Proxy relay (If Relay-Endpoint) or register the VMware Tunnel Proxy Endpoint (If Endpoint only)	
Externally registered DNS record	Register the VMware Tunnel Proxy relay (If Relay-Endpoint) or register the VMware Tunnel Proxy Endpoint (If Endpoint only)	
(Optional) SSL Certificate from a trusted third party with Subject or Subject Alternative name of DNS	If you opt not to use the AirWatch certificates that are automatically generated by default as part of your Tunnel configuration, then you can use a public SSL certificate. Ensure that the full chain of certificates is present when you upload the certificate in the AirWatch Console. Ensure that the SSL certificate is trusted by all device types being used. (that is, not all Comodo certificates are natively trusted by Android). If VMware Tunnel is already installed and running and your SSL certificate expires, then you must reupload the renewed SSL certificate and redownload and rerun the installer.	

Copyright © 2018 VMware, Inc. All rights reserved.

Requirement	Notes	
Ensure that the AWCM SSL certificates Intermediate and Root CA certificate are in the Java CA Keystore on the VMware Tunnel Proxy server	Use the Command Line Utility on the VMware Tunnel Proxy server to enter the following: keytool -list -v -keystore $JAVA_HOME\jre \lib\security\cacerts OR Use the GUI tool (free) here: http://portecle.sourceforge.net/	

General Requirements for VMware Tunnel

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

Requirement	Notes	
Ensure that you have remote access to the servers that AirWatch is installed on	Set up Remote Desktop Connection Manager for multiple server management, installer can be downloaded from https://www.microsoft.com/en-us/download/details.aspx?id=44989	
Installation of Notepad++ (Recommended)	Installer can be downloaded from http://download.tuxfamily.org/notepadplus/6.5.1/npp.6.5.1.Installer.exe	

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* by default	Once VMware Tunnel Proxy starts correctly, it listens on the HTTPS port by default. To make sure, you can open a browser and check the following: **https://<AirWatch_Tunnel_Proxy_Host>:<port>** – Verify you see an untrusted certificate screen unless there is a trusted SSL certificate and in that case you see *407 MAG Authentication Failed!*	1
VMware Tunnel Proxy – Basic-Endpoint Configuration					
VMware Tunnel Proxy	AirWatch Cloud Messaging Server**	HTTPS	**SaaS:** 443 **On Prem:** 2001 or a port you configure	Verify by entering **https://<AWCM URL>:<port>/awcm/status** in browser and ensure that there is no certificate trust error	2

Copyright © 2018 VMware, Inc. All rights reserved.

Source Component	Destination Component	Protocol	Port	Verification	Note
VMware Tunnel Proxy	Internal Web sites / Web apps	HTTP or HTTPS	80 or 443		4
VMware Tunnel Proxy	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	Verify by entering **https://APIServerUrl/API/help** in browser. If you are prompted for credentials, enter AirWatch admin credentials and an API help page displays.	5
Console Server	VMware Tunnel Proxy	HTTPS	**On-Prem:** 2020	Verify after installation using telnet command from the console server to the Tunnel Proxy on port 2020 (On-Premesis only).	6
VMware Tunnel Proxy – Relay-Endpoint Configuration					
VMware Tunnel Proxy Relay	AirWatch Cloud Messaging Server**	HTTP or HTTPS	**SaaS:** 443 **On Prem:** 2001 or a port you configure	Verify by entering **https://<AWCM URL>:<port>/awcm/status** in browser and ensure that there is no certificate trust error	2
VMware Tunnel Proxy Relay	VMware Tunnel Proxy Endpoint	HTTPS	2010*	Telnet from VMware Tunnel Proxy Relay to the VMware Tunnel Proxy Endpoint server on port	3
VMware Tunnel Proxy Endpoint	Internal Web sites / Web apps	HTTP or HTTPS	80 or 443		4
VMware Tunnel Proxy 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	**SaaS:** 443 **On-Prem:** 80 or 443	Verify by entering **https://APIServerUrl/API/help** in browser. If you are prompted for credentials, enter AirWatch admin credentials and an API help page displays.	5

Copyright © 2018 VMware, Inc. All rights reserved.

Source Component	Destination Component	Protocol	Port	Verification	Note
Console Server	VMware Tunnel Proxy	HTTPS	**On-Prem:** 2020	Verify after installation using telnet command from the console server to the Tunnel Proxy on port 2020 (On-Premesis only).	6

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

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

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

Copyright © 2018 VMware, Inc. All rights reserved.

Chapter 4:
Tunnel Configuration

Copyright © 2018 VMware, Inc. All rights reserved.

VMware Tunnel Configuration Overview

After completing the steps in the VMware Tunnel Installation Preparation Overview on page 14, 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 to use VMware Tunnel. Doing so ensures all HTTP(S) traffic for the specified applications is routed through the VMware Tunnel.

Configure VMware Tunnel Proxy (Legacy MAG)

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, 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**.

   If this is your first time configuring VMware Tunnel Proxy, then select **Configure** and follow the configuration wizard screens. Otherwise, select the **Override** radio button, ensure the **Enable VMware Tunnel** check box is selected, and then select **Configure** to configure the following settings.

2. On the **Configuration Type** screen, enable the **Proxy** component only, because Per-App Tunnel is not available for a VMware Tunnel for Windows deployment. In the drop-down menu that displays, select whether you are configuring a **Relay-Endpoint** or **Basic** deployment. Select the information icon to view 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	This text box only displays if you select Relay-Endpoint as your configuration type. Enter the relay server host name, for example, awtunnel.acmemdm.com.

Copyright © 2018 VMware, Inc. All rights reserved.

Setting	Description
Endpoint Host Name	The name given to the server where the VMware Tunnel Proxy is installed. If you plan to install the VMware Tunnel Proxy on an SSL offloaded server, enter the name of that server in place of the **Host Name**. When entering the **Host Name**, do not include a protocol such as http://, https://, etc.
Relay Port (HTTPS)	The port number automatically assigned for HTTPS communication with the VMware Tunnel Proxy. The default value is 2020.
Relay-Endpoint Port	This text box only displays if you select Relay-Endpoint as your configuration type. This value is the port used for traffic between the VMware Tunnel Proxy relay and VMware Tunnel Proxy endpoint. The default value is 2010.
Use Kerberos Proxy	Enable Kerberos proxy support to allow access to Kerberos authentication, typically only available inside the corporate network, 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 46. The Endpoint server must be on the same domain as KDC for the Kerberos Proxy to communicate successfully with the KDC.
Realm	This text box only displays if you enable **Use Kerberos Proxy**. Enter the domain of the KDC server.

5. Select **Next**.

6. On the **SSL** screen, configure the following settings.

   - **Use Public SSL Certificate –** Select the **Use Public SSL Certificate** check box if you are using third-party public SSL certificates for encryption between wrapped apps, VMware Browser, or SDK-enabled apps and the VMware Tunnel Proxy. Select **Upload** to browse for and upload your certificate file (.pfx or .p12). This file must contain both your public and private key pair.

7. Select **Next**.

8. On the **Authentication** screen, configure the following settings.

   - **Proxy Authentication –** Select whether to use an enterprise Certificate Authority (CA) in place of AirWatch issued certificates for authentication between wrapped apps, VMware Browser, or SDK-enabled apps and the VMware Tunnel Proxy.

     - Select **Default** to use AirWatch issued certificates.

     - Select **Enterprise CA** to display drop-down menus for your certificate authority and certificate template that you have configured in AirWatch. Also upload your root certificate of your CA.

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

       For more information about integrating with your certificate provider, see the Certificate Management documentation for your CA, available on AirWatch Resources in the Certificate Management section.

9. Select **Next**.

10. On the **Miscellaneous** screen, you can configure whether to enable access logs for the Proxy component.

Copyright © 2018 VMware, Inc. All rights reserved.

You must enable this log before you install the VMware Tunnel Proxy. For more information on these settings, refer to the Access Logs and Syslog Integration and Configuring Advanced Settings sections.

11. Review the summary of your VMware Tunnel Proxy configuration and select **Save**. You are navigated back to the VMware Tunnel Proxy configuration page.
12. If you plan to install the VMware Tunnel Proxy on an SSL offloaded server, select **Export VMware Tunnel Certificate** from the AirWatch Console once the certificate has been generated. Then, import the certificate on the server performing SSL offload. (This server can be a load balancer or reverse proxy.)
13. Select the **General** tab and then select the **Download Windows Installer** hyperlink. This button downloads a single EXE file used for installation of both a relay server and endpoint.

    If you want to enable Access Logs using syslog, then you must enable this feature through the **Advanced** tab before you download and run the installer. See Access Logs and Syslog Integration for more information.
14. Enter and confirm a certificate password and then select **Download**.

    The VMware Tunnel Proxy password must contain a minimum of six characters and is used during installation.
15. Select **Save**.
16. Continue with the steps for VMware Tunnel Proxy (Legacy MAG) Installation for a Relay-Endpoint Configuration on Windows or VMware Tunnel Proxy (Legacy MAG) Installation for a Basic (Endpoint only) Configuration on Windows, 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 49.
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.

Copyright © 2018 VMware, Inc. All rights reserved.

Setting	Description
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.
Access Logs	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. 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. There is no correlation between this syslog integration and the integration accessed on **Groups & Settings > All Settings > System > Enterprise Integration > Syslog.** 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.
Syslog Hostname	Enter the URL of your syslog host. This setting displays after you enable Access Logs.
Port	Enter the port over which you want to communicate with the syslog host. This setting displays after you enable Access Logs.
API and AWCM outbound calls via proxy	Enable this option if the communication for initialization between the VMware Tunnel and AirWatch API or AWCM is through an outbound proxy.
Show detailed errors	Enable this option to ensure client applications (for example, VMware Browser) are informed when the VMware Tunnel fails to authenticate a device.
Log Level	Set the appropriate logging level, which determines how much data is reported to the LOG files.

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

Copyright © 2018 VMware, Inc. All rights reserved.

4. 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.

5. Select **Save**.

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.

Copyright © 2018 VMware, Inc. All rights reserved.

Chapter 5: Installation for Relay-Endpoint Configurations

Copyright © 2018 VMware, Inc. All rights reserved.

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.

Install the AirWatch Tunnel Relay Server (Windows)

After ensuring that your servers meets all the proper requirements, configuring VMware Tunnel settings in the AirWatch Console, and downloading the installer to your Windows 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.

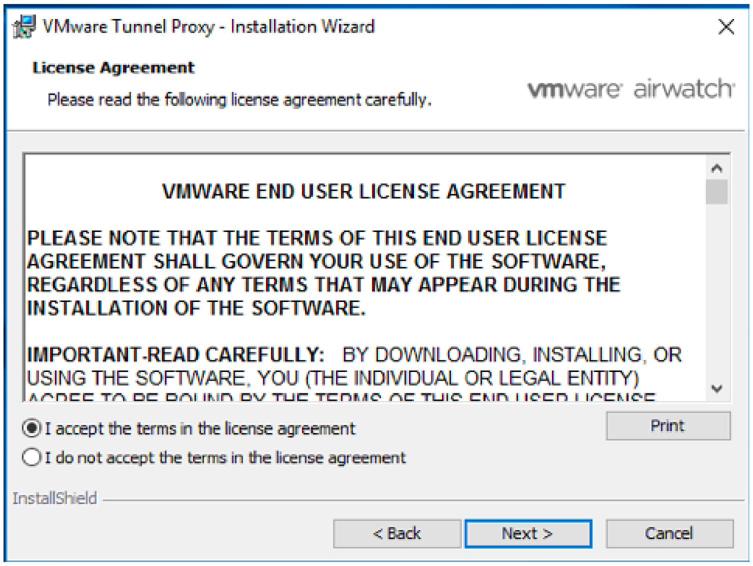
Procedure

Perform the following steps on the relay server:

1. Open the installer executable on the Relay VMware Tunnel Proxy server and then select **Next**. For Relay-Endpoint configurations, you must perform VMware Tunnel Proxy installation on both the Relay and Endpoint servers. The steps listed here assume that you are first installing it on the Relay server.

   If a previous version of VMware Tunnel Proxy is installed, the installer auto-detects it and offers the option to upgrade to the latest version.

2. Accept the End User License Agreement and then select **Next**.



VMware Tunnel Proxy - Installation Wizard

License Agreement

Please read the following license agreement carefully.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

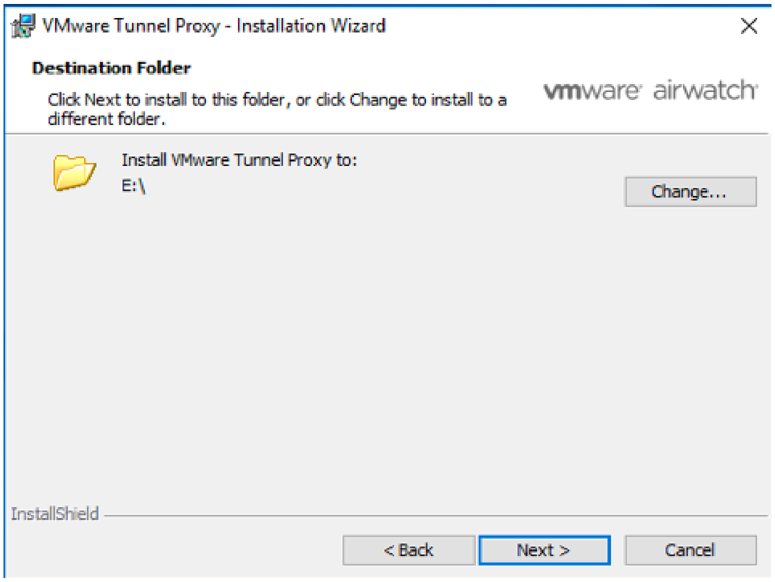
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

3. Specify the destination for the downloaded VMware Tunnel Proxy installation files and then select **Next**.

Copyright © 2018 VMware, Inc. All rights reserved.

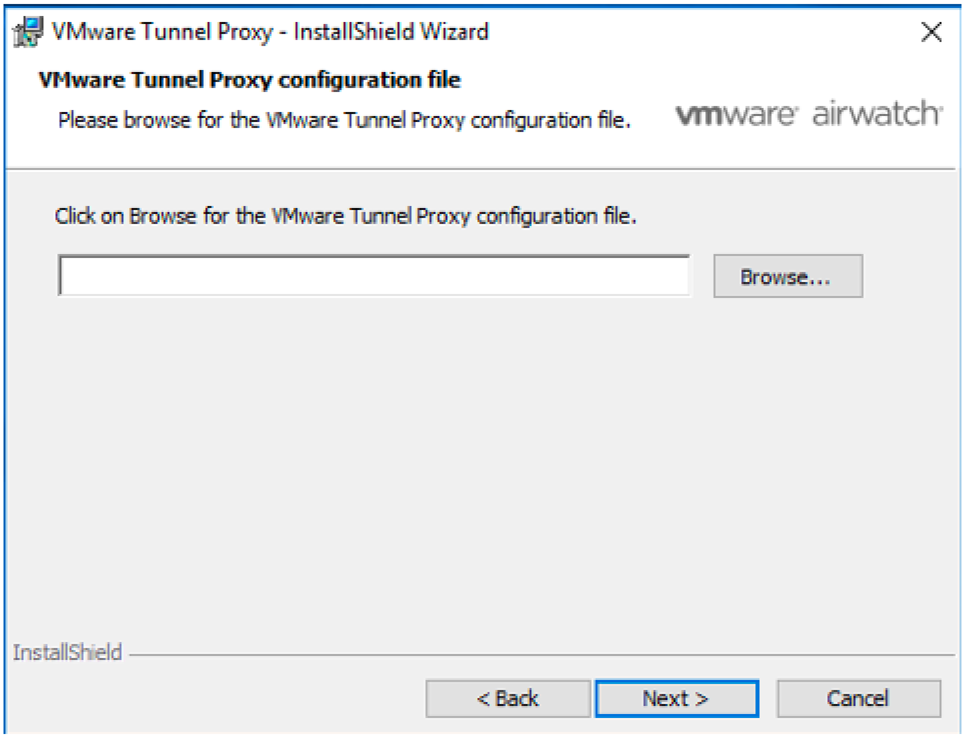

VMware Tunnel Proxy - Installation Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install VMware Tunnel Proxy to:
E:\

4. Select **Browse** and select the config.xml file downloaded from the AirWatch Console.


VMware Tunnel Proxy - InstallShield Wizard

VMware Tunnel Proxy configuration file

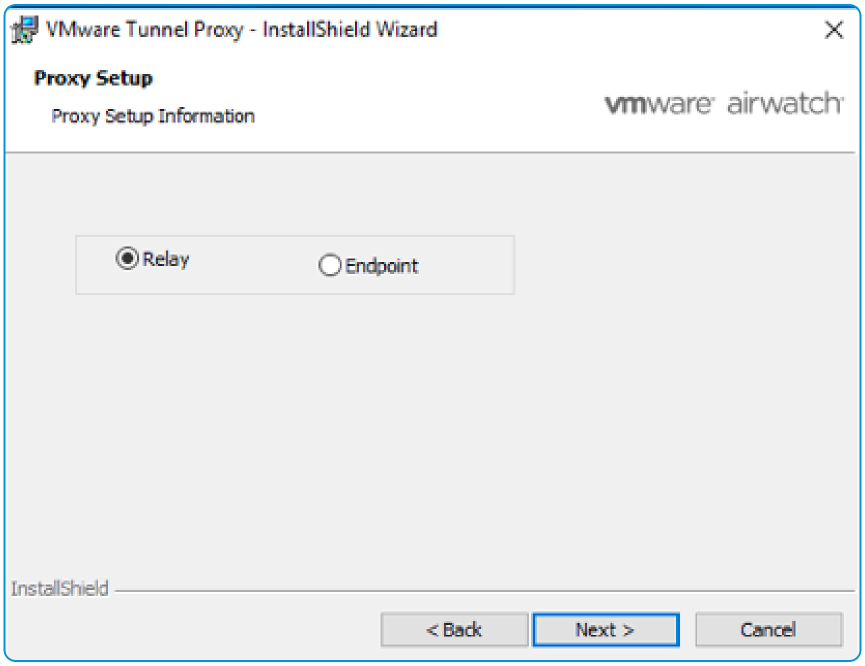
Please browse for the VMware Tunnel Proxy configuration file.

Click on Browse for the VMware Tunnel Proxy configuration file.

Then select **Next**.

5. Select the **Relay** button to install VMware Tunnel Proxy on the Relay server.

Copyright © 2018 VMware, Inc. All rights reserved.

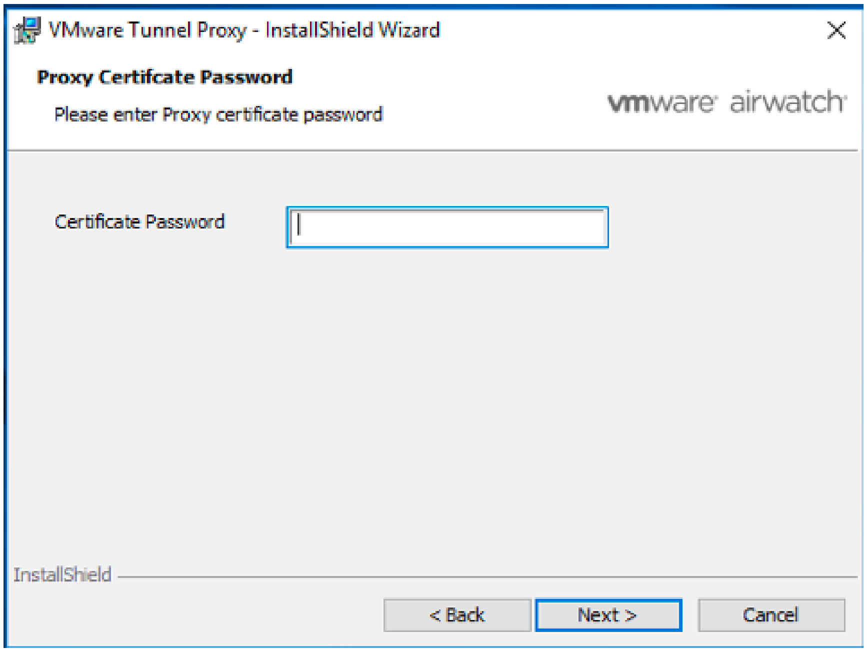

VMware Tunnel Proxy - InstallShield Wizard

Proxy Setup

Proxy Setup Information

● Relay ○ Endpoint

6. Enter the Certificate Password you created in the AirWatch Console and then select **Next**.


VMware Tunnel Proxy - InstallShield Wizard

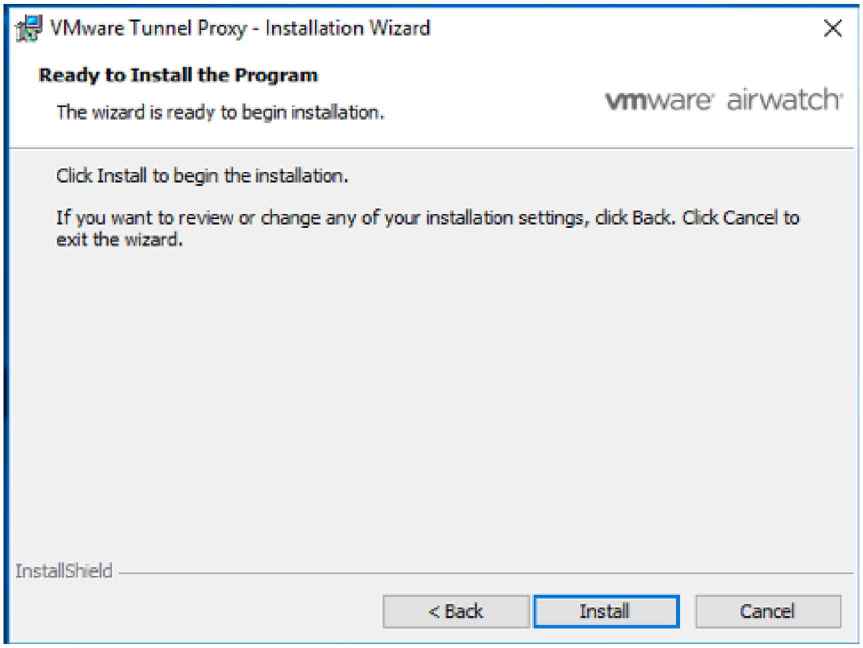
Proxy Certifcate Password

Please enter Proxy certificate password

Certificate Password

7. Click **Install** to begin VMware Tunnel Proxy installation on the server.

Copyright © 2018 VMware, Inc. All rights reserved.



VMware Tunnel Proxy - Installation Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

8. Click **Finish** to close the installer.

To complete your installation, perform the steps for Install the AirWatch Tunnel Endpoint Server (Windows) on page 30.

Install the AirWatch Tunnel Endpoint Server (Windows)

In Relay-Endpoint configurations, you install the endpoint server after installing the relay server. If you have not already, perform the steps under Install the AirWatch Tunnel Relay Server (Windows) on page 27.

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

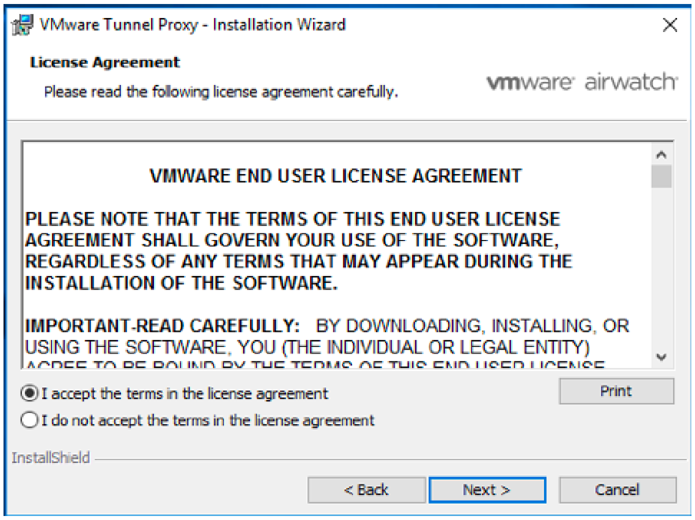
Perform the following steps on the endpoint server:

1. Open the installer executable on the Endpoint VMware Tunnel Proxy server and then select **Next**.

   If a previous version of VMware Tunnel Proxy is installed, the installer auto-detects it and offers the option to upgrade to the latest version.

2. Accept the End User License Agreement and then select **Next**.

Copyright © 2018 VMware, Inc. All rights reserved.



VMware Tunnel Proxy - Installation Wizard

License Agreement

Please read the following license agreement carefully.

VMWARE END USER LICENSE AGREEMENT

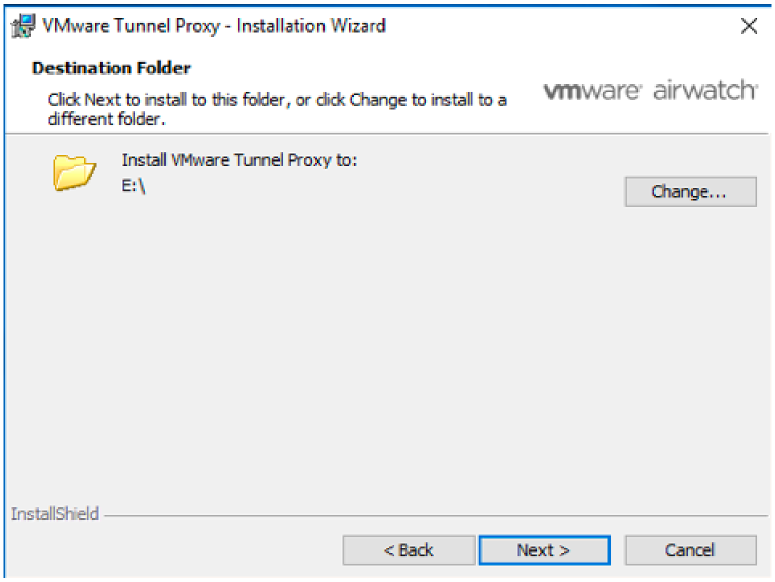
PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

3. Specify the destination for the downloaded installation files and then select **Next**.



VMware Tunnel Proxy - Installation Wizard

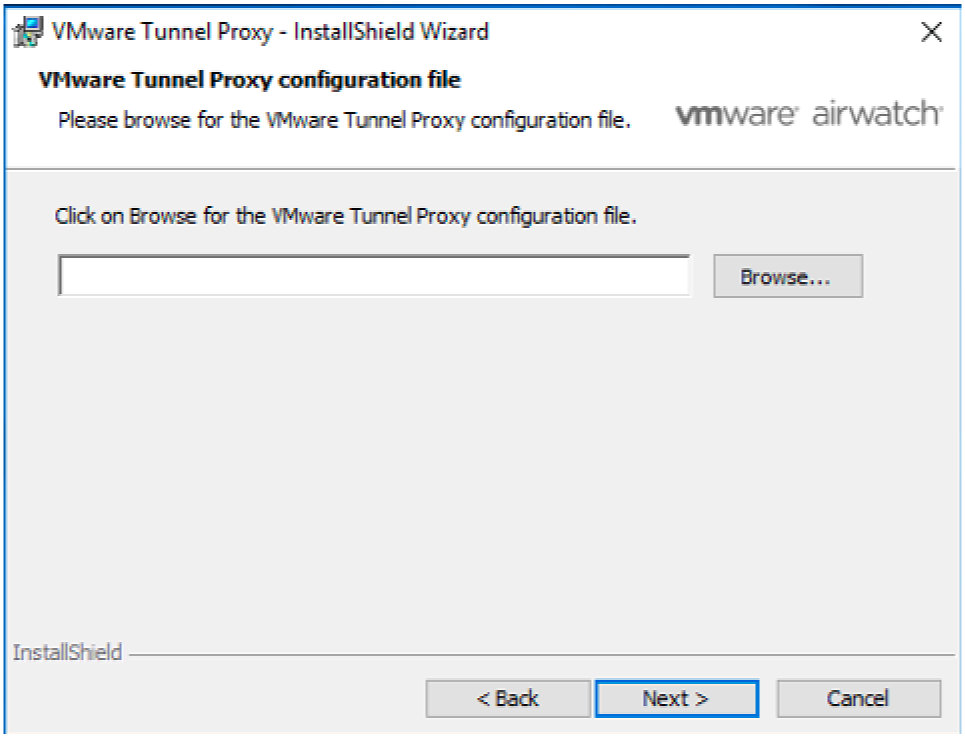
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install VMware Tunnel Proxy to:
E:\

4. Select **Browse** and select the config.xml file downloaded from the AirWatch Console.

Copyright © 2018 VMware, Inc. All rights reserved.



VMware Tunnel Proxy - InstallShield Wizard

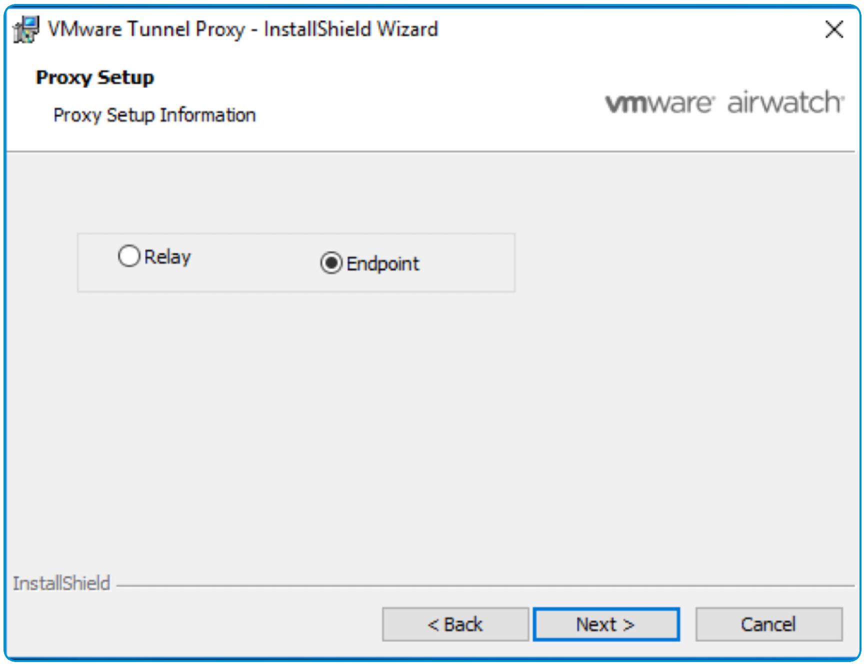
VMware Tunnel Proxy configuration file

Please browse for the VMware Tunnel Proxy configuration file.

Click on Browse for the VMware Tunnel Proxy configuration file.

Then select **Next**.

5. Select the **Endpoint** button to install VMware Tunnel Proxy on the Endpoint server.



VMware Tunnel Proxy - InstallShield Wizard

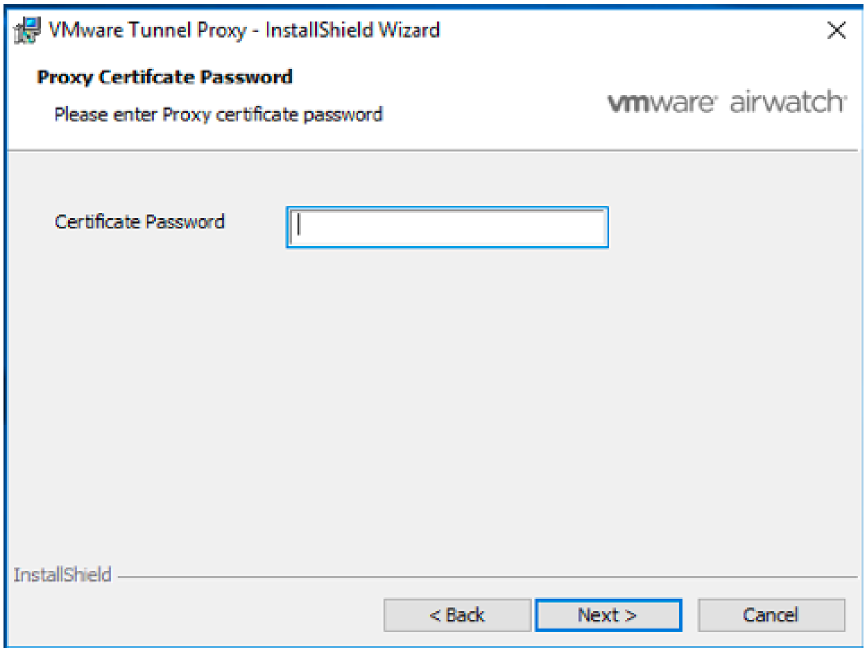
Proxy Setup

Proxy Setup Information

○ Relay ● Endpoint

6. Enter the Certificate Password you created in the AirWatch Console and then select **Next**.

Copyright © 2018 VMware, Inc. All rights reserved.



VMware Tunnel Proxy - InstallShield Wizard

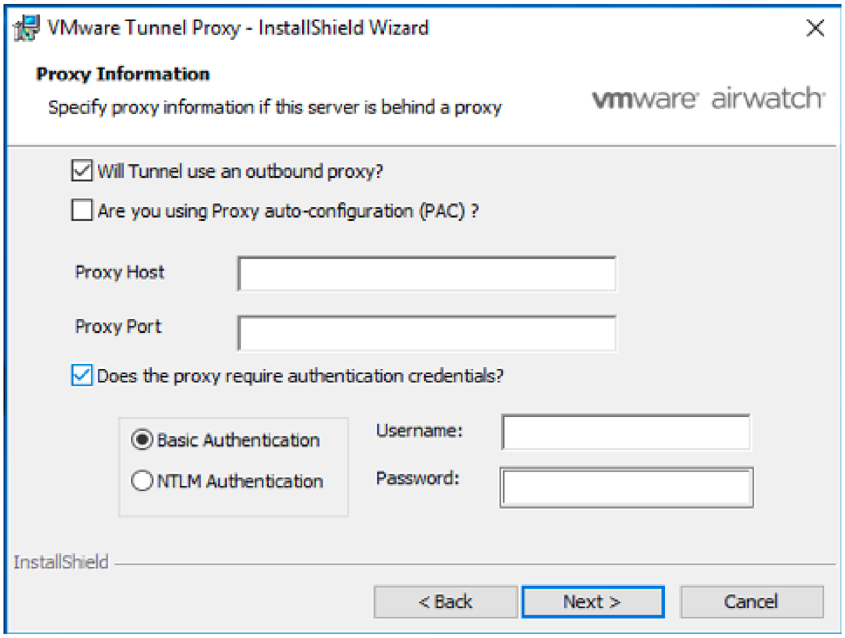
Proxy Certifcate Password

Please enter Proxy certificate password

Certificate Password

7. Select the check box to indicate if VMware Tunnel Proxy uses an outbound proxy. If so, enter the address of the **Proxy Host** and **Proxy Port** number to be used for communication. If the proxy requires authentication, first select the **Does the proxy require authentication credentials?** checkbox, then select whether it uses **Basic** or **NTLM** authentication, then specify the **Username** and **Password** credentials.

   For more information about using outbound proxies, see VMware Tunnel Outbound Proxy Overview on page 49.



VMware Tunnel Proxy - InstallShield Wizard

Proxy Information

Specify proxy information if this server is behind a proxy

☑ Will Tunnel use an outbound proxy?

□ Are you using Proxy auto-configuration (PAC) ?

Proxy Host

Proxy Port

☑ Does the proxy require authentication credentials?

● Basic Authentication

○ NTLM Authentication

Username:

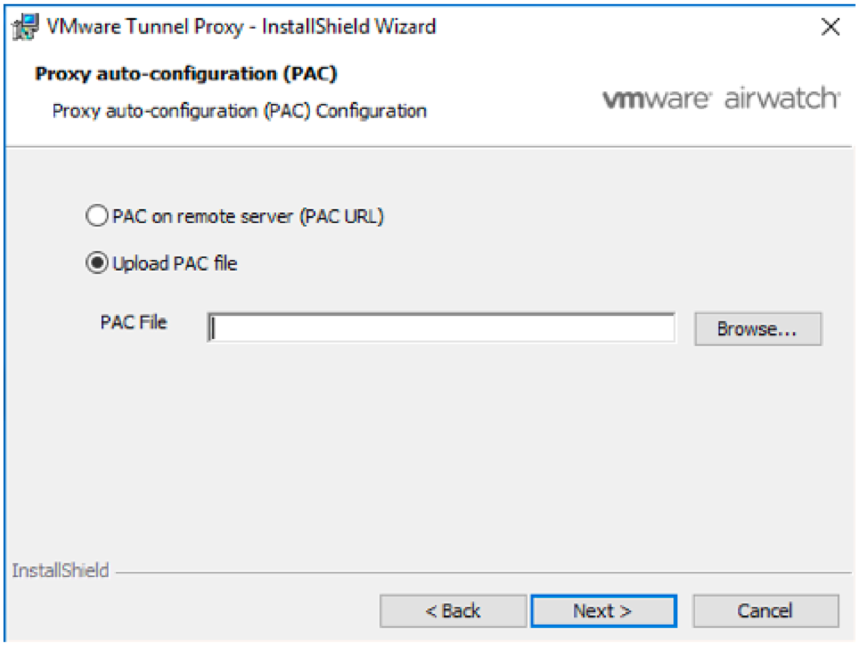
Password:

8. Specify whether you are using **Proxy auto-configuration (PAC)** files as part of your installation. A PAC file is a set of rules that a browser checks to determine where traffic gets routed. For VMware Tunnel Proxy, traffic is checked against the PAC file to determine if it has to go through an outbound proxy. If you have authentication for PAC files, then the VMware Tunnel Proxy must know the user name and password of the proxy. You can reference a **PAC file on a remote server** by providing the PAC URL or **Upload a PAC file** directly.

Copyright © 2018 VMware, Inc. All rights reserved.

> **Note:** If you are accessing outbound proxies through the VMware Tunnel Proxy that use a PAC file and also require authentication, then refer to Enable Outbound Proxy for VMware Tunnel Proxy for Windows on page 49.

When you are finished, select **Next**.



VMware Tunnel Proxy - InstallShield Wizard

Proxy auto-configuration (PAC)

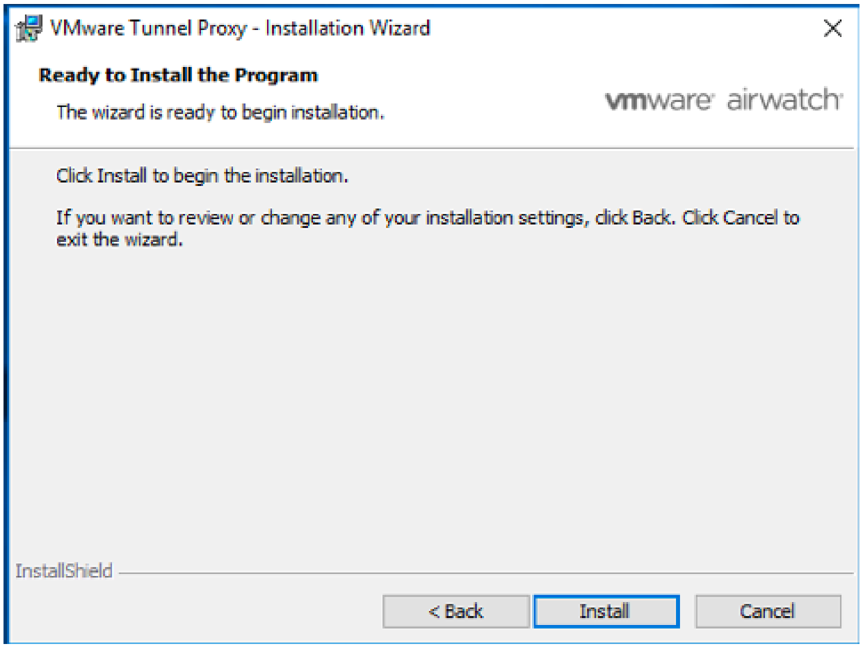
Proxy auto-configuration (PAC) Configuration

○ PAC on remote server (PAC URL)

● Upload PAC file

PAC File

9. Click **Install** to begin installation on the server.



VMware Tunnel Proxy - Installation Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

10. Click **Finish** to close the installer.

Verify Your VMware Tunnel Installation

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

Copyright © 2018 VMware, Inc. All rights reserved.

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.

Copyright © 2018 VMware, Inc. All rights reserved.

Chapter 6: Installation for Basic (Endpoint only) Configurations

Copyright © 2018 VMware, Inc. All rights reserved.

Install the AirWatch Tunnel – Basic (Windows)

After ensuring that your server meets all the proper requirements, configuring VMware Tunnel settings in the AirWatch Console, and downloading the installer to your Windows 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.

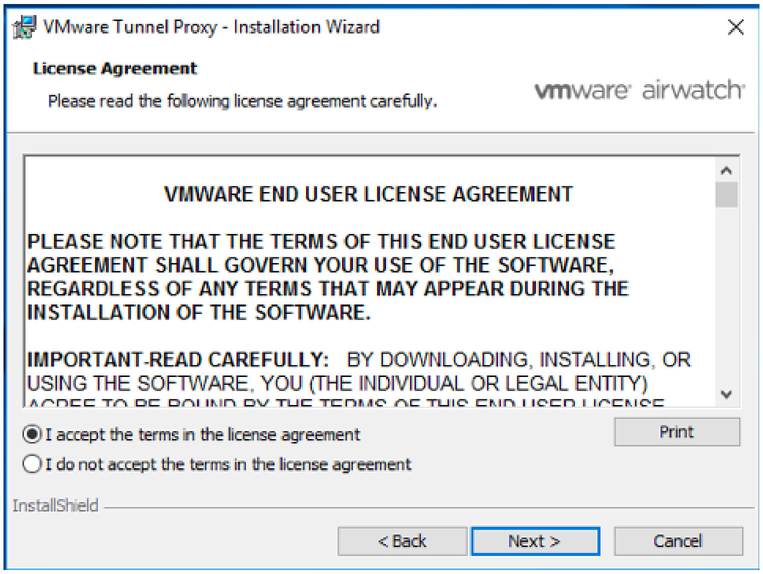
Procedure

Perform the following steps on your single VMware Tunnel server:

1. Open the installer executable on the Endpoint VMware Tunnel Proxy server and then select **Next**.

   If a previous version of VMware Tunnel Proxy is installed, the installer auto-detects it and offers the option to upgrade to the latest version.

2. Accept the End User License Agreement and then select **Next**.



VMware Tunnel Proxy - Installation Wizard

License Agreement

Please read the following license agreement carefully.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

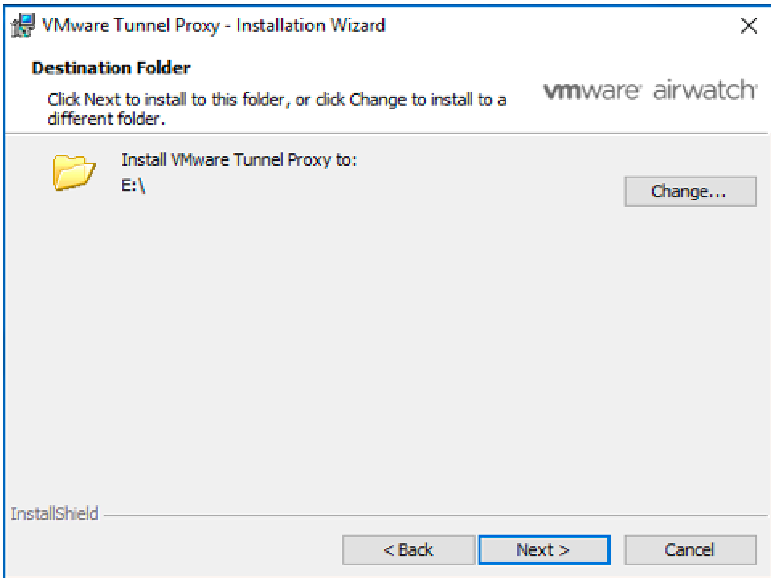
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

3. Specify the destination for the downloaded VMware Tunnel Proxy installation files and then select **Next**.

Copyright © 2018 VMware, Inc. All rights reserved.

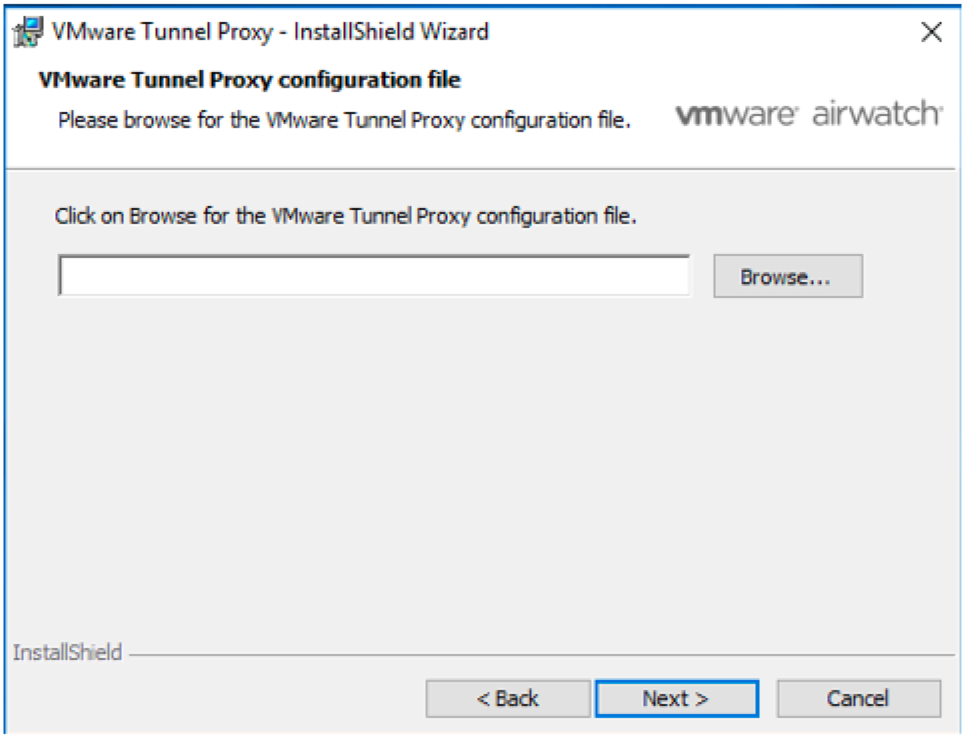

VMware Tunnel Proxy - Installation Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install VMware Tunnel Proxy to:
E:\

4. Select **Browse** and select the config.xml file downloaded from the AirWatch Console.


VMware Tunnel Proxy - InstallShield Wizard

VMware Tunnel Proxy configuration file

Please browse for the VMware Tunnel Proxy configuration file.

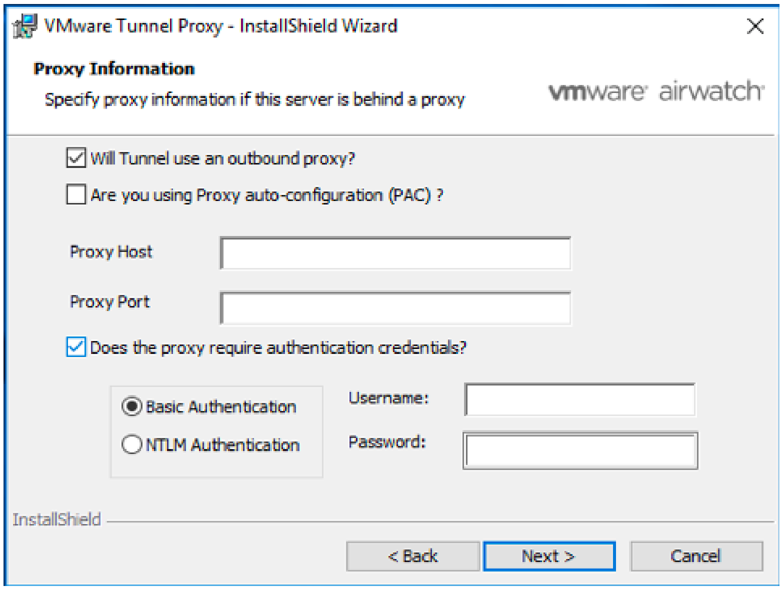
Click on Browse for the VMware Tunnel Proxy configuration file.

Then select **Next**.

5. Select the check box to indicate if VMware Tunnel Proxy uses an outbound proxy. If so, enter the address of the **Proxy Host** and **Proxy Port** number to be used for communication. If the proxy requires authentication, first select the **Does the proxy require authentication credentials?** checkbox, then select whether it uses **Basic** or **NTLM** authentication, then specify the **Username** and **Password** credentials.

   For more information about using outbound proxies, see VMware Tunnel Outbound Proxy Overview on page 49.

Copyright © 2018 VMware, Inc. All rights reserved.



VMware Tunnel Proxy - InstallShield Wizard

Proxy Information

Specify proxy information if this server is behind a proxy

☑ Will Tunnel use an outbound proxy?

□ Are you using Proxy auto-configuration (PAC) ?

Proxy Host

Proxy Port

☑ Does the proxy require authentication credentials?

● Basic Authentication

○ NTLM Authentication

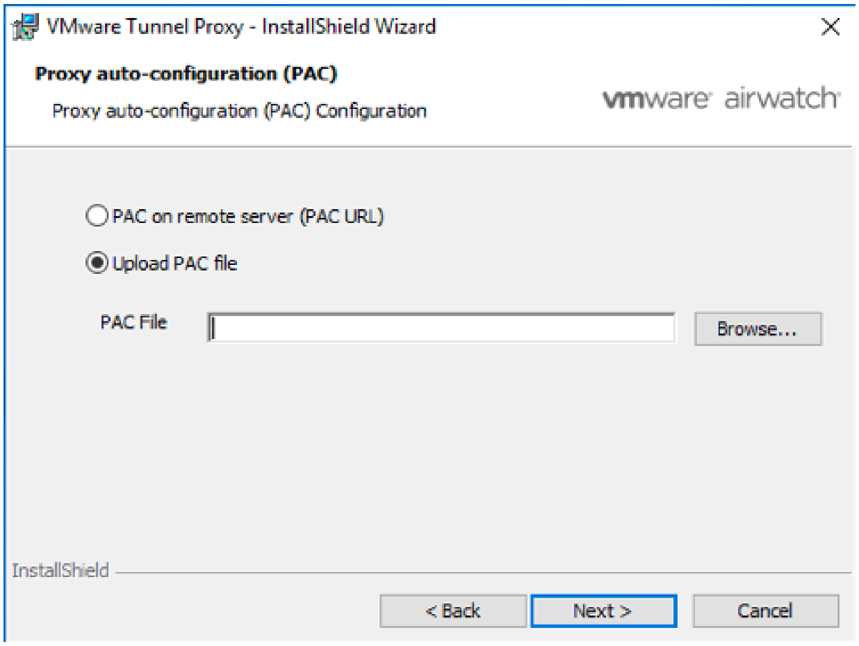
Username:

Password:

6. Specify whether you are using **Proxy auto-configuration (PAC)** files as part of your VMware Tunnel Proxy installation. A PAC file is a set of rules that a browser checks to determine where traffic gets routed. For VMware Tunnel Proxy, traffic is checked against the PAC file to determine if it has to go through an outbound proxy. If you have authentication for PAC files, then the VMware Tunnel Proxy must know the user name and password of the proxy. You can reference a **PAC file on a remote server** by providing the PAC URL or **Upload a PAC file** directly.

   > **Note:** If you are accessing outbound proxies through the VMware Tunnel Proxy that use a PAC file and also require authentication, then refer to Enable Outbound Proxy for VMware Tunnel Proxy for Windows on page 49.

   When you are finished, select **Next**.



VMware Tunnel Proxy - InstallShield Wizard

Proxy auto-configuration (PAC)

Proxy auto-configuration (PAC) Configuration

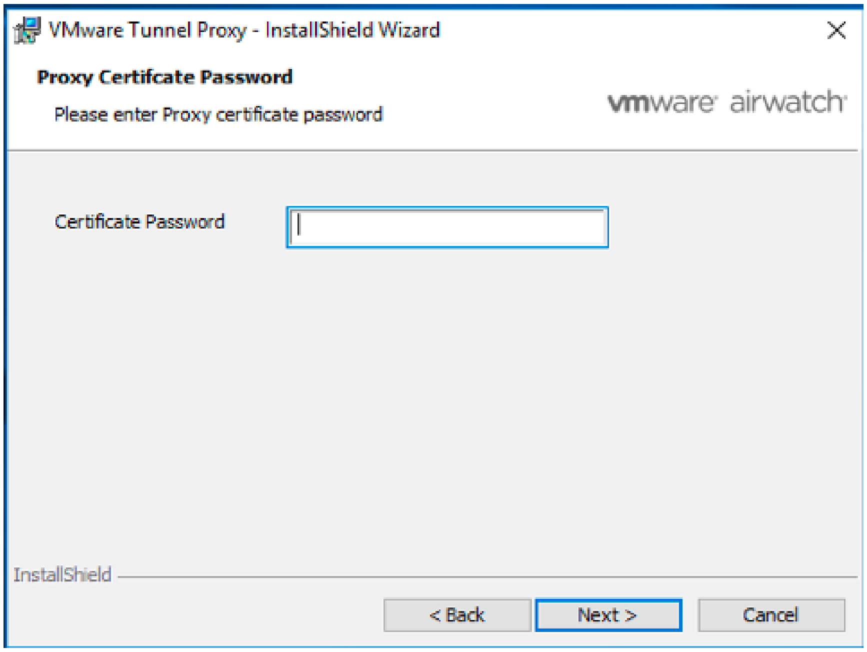
○ PAC on remote server (PAC URL)

● Upload PAC file

PAC File

7. Enter the Certificate Password you created in the AirWatch Console and then select **Next**.

Copyright © 2018 VMware, Inc. All rights reserved.

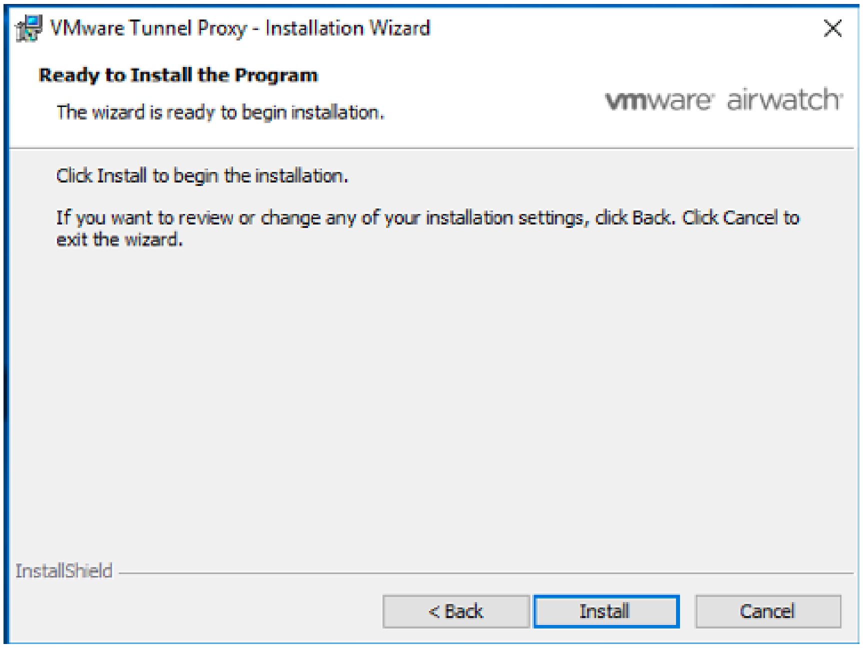

VMware Tunnel Proxy - InstallShield Wizard

Proxy Certifcate Password

Please enter Proxy certificate password

Certificate Password

8. Click **Install** to begin VMware Tunnel Proxy installation on the server.


VMware Tunnel Proxy - Installation Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

9. Click **Finish** to close the VMware Tunnel Proxy installer.

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

Copyright © 2018 VMware, Inc. All rights reserved.

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.

Copyright © 2018 VMware, Inc. All rights reserved.

Chapter 7:
VMware Tunnel Management

Copyright © 2018 VMware, Inc. All rights reserved.

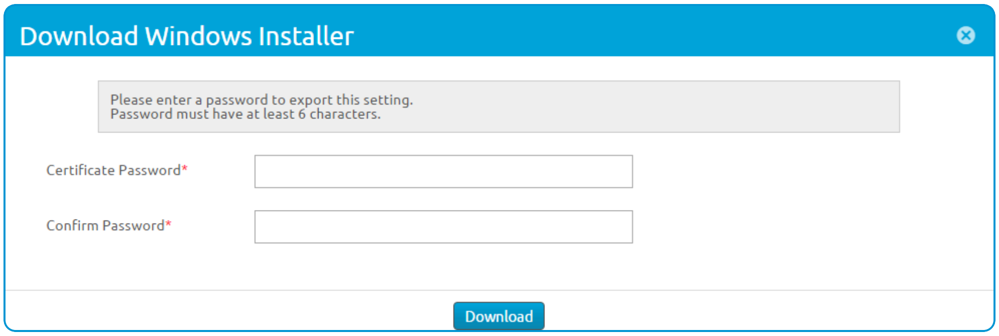
Upgrade the VMware Tunnel Proxy for Windows Component

To upgrade, simply download and run the installer again using the same procedures outlined previously in this document, depending on your configuration setup. Any custom changes you made to configuration files after the original installation may be lost, so you may want to make backups of these files to reference later.

KB Note: To update Java on the Windows server hosting your Tunnel Proxy component without reinstalling the Tunnel Proxy, see the Knowledge Base article available here: https://support.air-watch.com/articles/115001675388.

To upgrade the component:

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 Windows Installer** hyperlink.
3. Enter and confirm a certificate password and then select **Download**.



Download Windows Installer

Please enter a password to export this setting.
Password must have at least 6 characters.

Certificate Password*

Confirm Password*

The VMware Tunnel Proxy password must contain a minimum of six characters.

4. Continue with the steps for Install the AirWatch Tunnel Relay Server (Windows) on page 27 or Install the AirWatch Tunnel – Basic (Windows) on page 37.

VMware Tunnel Access Logs and Syslog Integration

AirWatch supports access logs and syslog integration for the VMware Tunnel Proxy (Legacy MAG) component. 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.

For instructions on enabling access log and syslog integration, seeConfigure Advanced Settings for VMware Tunnel on page 23.

Important: You must enable access logs 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.

Copyright © 2018 VMware, Inc. All rights reserved.

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.

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.

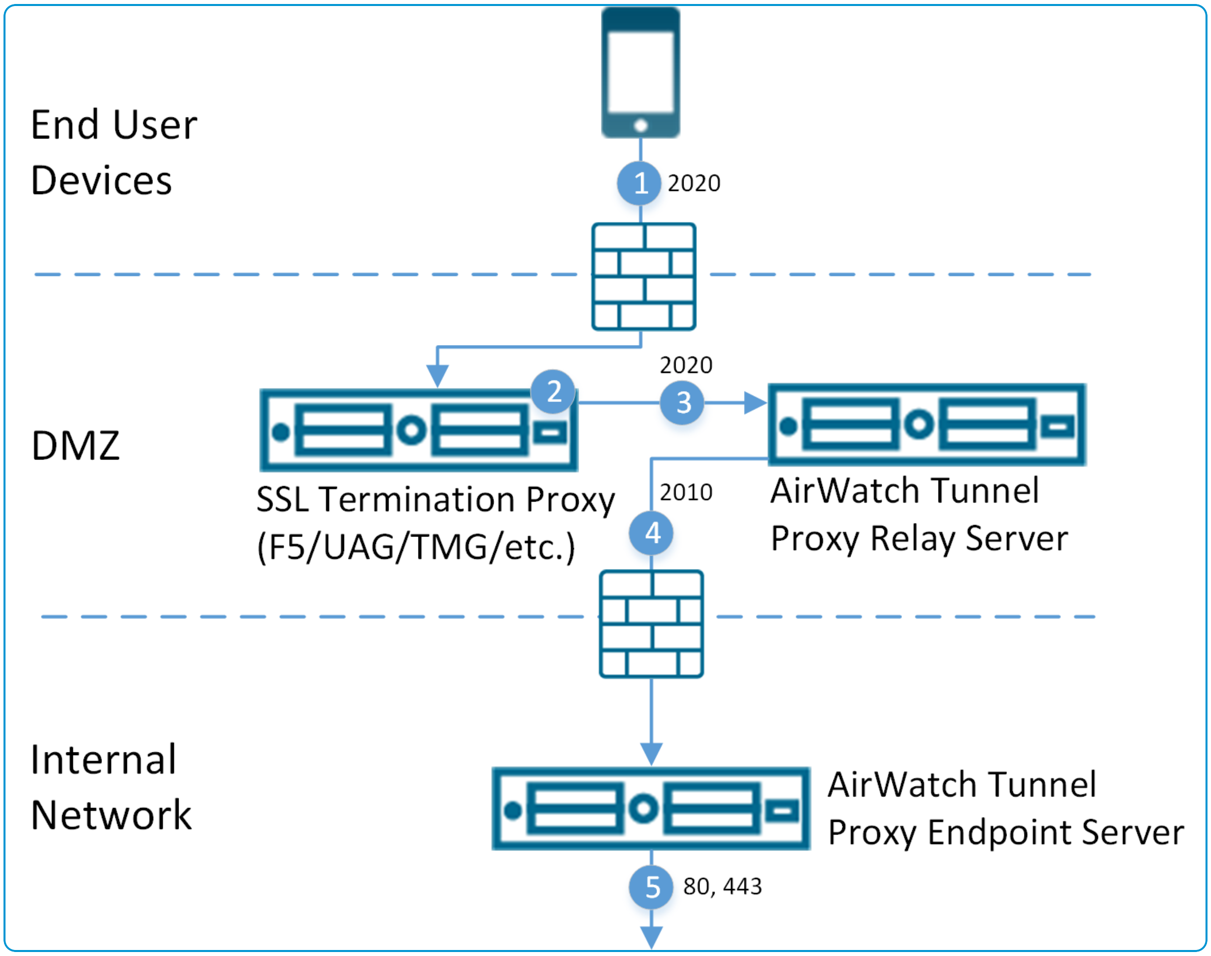
Copyright © 2018 VMware, Inc. All rights reserved.

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.


End User Devices
1
2020
DMZ
2
2020
3
SSL Termination Proxy (F5/UAG/TMG/etc.)
2010
4
AirWatch Tunnel Proxy Relay Server
Internal Network
AirWatch Tunnel Proxy Endpoint Server
5
80, 443

> **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.

Copyright © 2018 VMware, Inc. All rights reserved.

- 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.

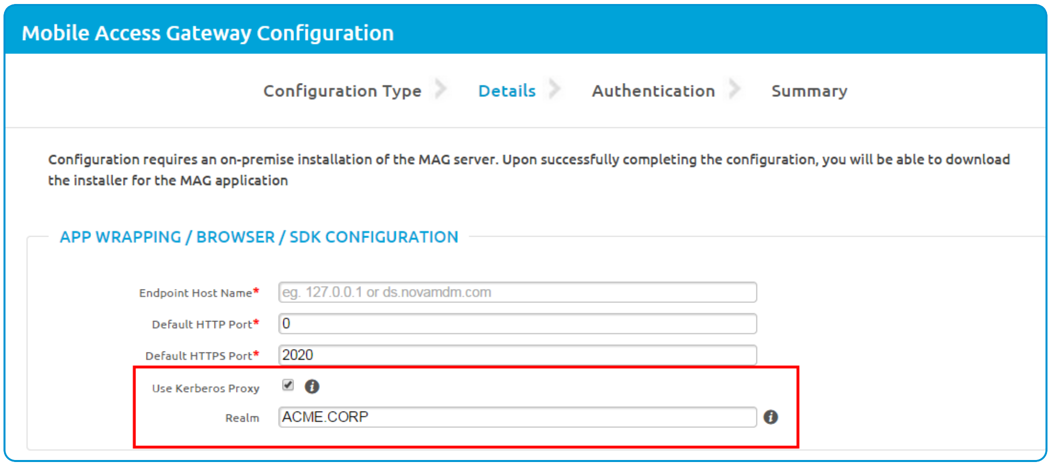
Enable Kerberos Proxy Settings

Enable Kerberos KDC Proxy Support on page 46 during your initial VMware Tunnel configuration. AirWatch KKDCP acts as a proxy to your internal KDC server.

To enable Kerberos proxy settings:

Copyright © 2018 VMware, Inc. All rights reserved.

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



Mobile Access Gateway Configuration

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* eg. 127.0.0.1 or ds.novamdm.com

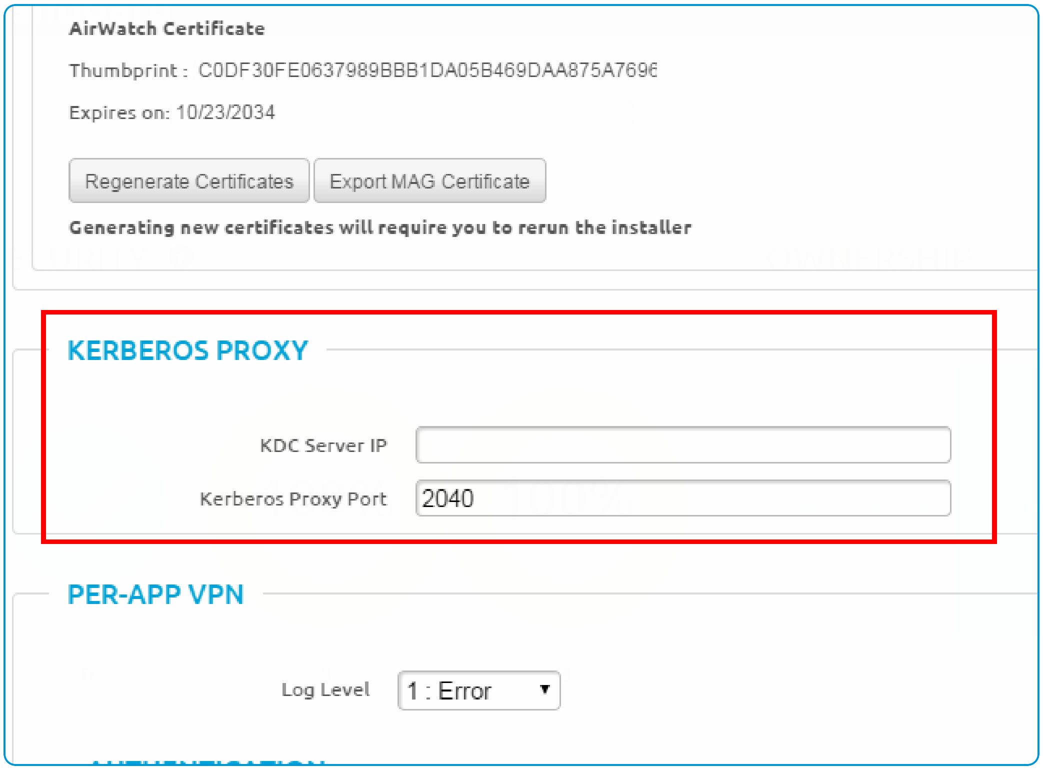
Default HTTP Port* 0

Default HTTPS Port* 2020

Use Kerberos Proxy ☑

Realm ACME.CORP

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 : C0DF30FE0637989BBB1DA05B469DAA875A7696

Expires on: 10/23/2034

Generating new certificates will require you to rerun the installer

KERBEROS PROXY

KDC Server IP

Kerberos Proxy Port 2040

PER-APP VPN

Log Level 1 : Error

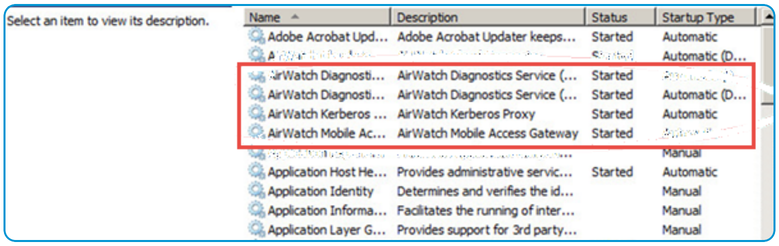
Only add the IP if the Realm is not reachable, as it takes precedence over the Realm value entered in the configuration.

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.

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

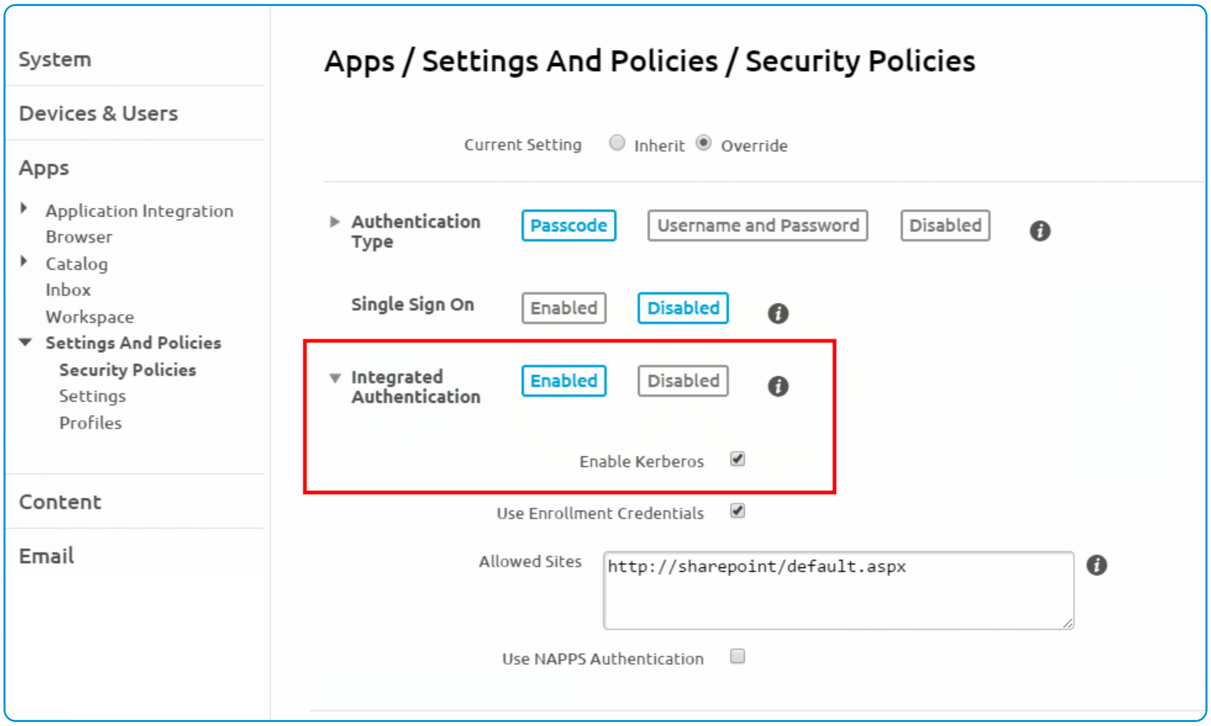
Copyright © 2018 VMware, Inc. All rights reserved.



Select an item to view its description.

Name	Description	Status	Startup Type
Adobe Acrobat Upd...	Adobe Acrobat Updater keeps...	Started	Automatic
A[illegible]	[illegible]	Started	Automatic (D...
AirWatch Diagnosti...	AirWatch Diagnostics Service (...	Started	[illegible]
AirWatch Diagnosti...	AirWatch Diagnostics Service (...	Started	Automatic (D...
AirWatch Kerberos ...	AirWatch Kerberos Proxy	Started	Automatic
AirWatch Mobile Ac...	AirWatch Mobile Access Gateway	Started	[illegible]
[illegible]	[illegible]		Manual
Application Host He...	Provides administrative servic...	Started	Automatic
Application Identity	Determines and verifies the id...		Manual
Application Informa...	Facilitates the running of inter...		Manual
Application Layer G...	Provides support for 3rd party...		Manual

4. Enable Kerberos from the SDK settings in the AirWatch Console so the requesting application is aware of the KKDCP. Navigate to **Groups & Settings > All Settings > Apps > Settings And Policies** and select **Security Policies**. Under Integrated Authentication, select **Enable Kerberos**. Save the settings.



Apps / Settings And Policies / Security Policies

Current Setting ○ Inherit ● Override

Authentication Type: **Passcode** | Username and Password | Disabled

Single Sign On: Enabled | **Disabled**

Integrated Authentication: **Enabled** | Disabled

Enable Kerberos ☑

Use Enrollment Credentials ☑

Allowed Sites: http://sharepoint/default.aspx

Use NAPPS Authentication ☐

Accessing Logs

The path for KKDCP logs for VMware Tunnel Proxy for Windows is: **\AirWatch\Logs\MobileAccessGateway**

To make sure the AirWatch KKDCP server is up and running, access the following URL in your browser from the server where KKDCP is installed: **http://localhost:2040/kerberosproxy/status**

If the proxy server is working as expected then the browser returns the following response:

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

Copyright © 2018 VMware, Inc. All rights reserved.

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.

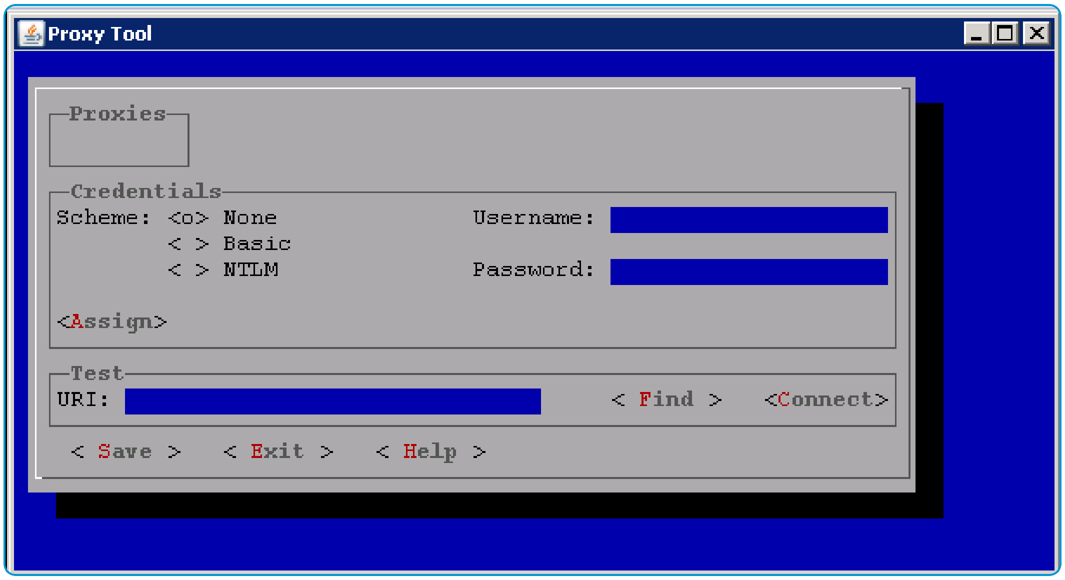
It is not mandatory to use outbound proxies with VMware Tunnel, but your organization may choose to deploy them behind one or more VMware Tunnel servers based on recommendations from your security and network teams. For VMware Tunnel on Windows, AirWatch supports outbound proxies for the Proxy component.

Enable Outbound Proxy for VMware Tunnel Proxy for Windows

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. In Windows Explorer, navigate to **\AirWatch\tunnelproxy\tools\proxytool\proxytool.bat**.
2. Run **proxy-tools**. The Proxy Tool dialog box displays.
3. 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.



```
Proxy Tool

Proxies

Credentials
Scheme: <o> None                Username:
        < > Basic
        < > NTLM                Password:

<Assign>

Test
URI:                              < Find >     <Connect>

 < Save >    < Exit >    < Help >
```

4. Select **Save**.

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 23.

Client Compatibility

- AirWatch iOS Browser v4.5+

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

Copyright © 2018 VMware, Inc. All rights reserved.

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.

Copyright © 2018 VMware, Inc. All rights reserved.