VMware AirWatch Integration with F5 Guide

Enabling secure connections between mobile applications and your backend resources

Workspace ONE UEM v9.6

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

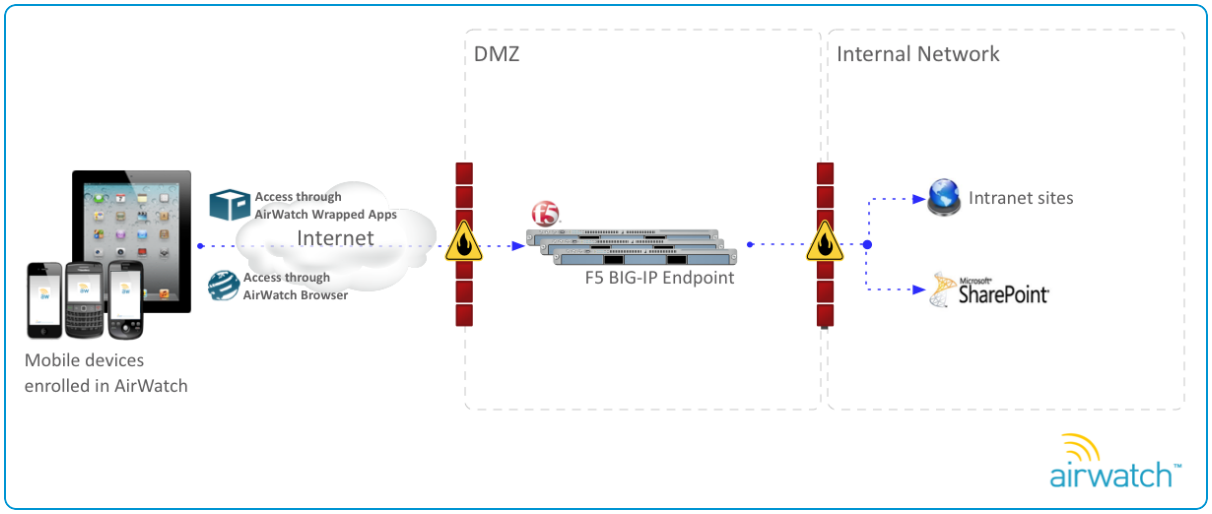
Table of Contents

Chapter 1:
Overview

Introduction to F5 Integration

This document provides an overview of the integration between AirWatch and various F5 components, such as the BIG-IP Access Policy Manager (APM) and SSL VPN Edge Client. The integration capabilities allow a device to have seamless access to web services behind the firewall by defining specific policies that allow secure connections through the F5. This connectivity only allows compliant and managed devices to access resources using the F5, and it selectively allows access by explicitly defining which apps have access to specific intranet sites once authenticated. The tunneling is integrated with the VMware Content Locker for access to SharePoint and other file shares, the VMware Browser for intranet site access, the AirWatch Inbox for email access, and the AirWatch SDK and App Wrapping to allow any internally developed apps to access backend services.

The following network diagram below is one example of how F5 BIG-IP can facilitate AppTunnel within an AirWatch mobile device deployment.



Setup and configuration depends on your specific network and security requirements. AirWatch recommends contacting your F5 administrator or vendor support representative for best practices and setup instructions for your specific F5 architecture.

In This Guide

- Before You Begin – This section covers topics and prerequisites you should familiarize yourself with so you can get the most out of using this guide.
- Enabling App Tunneling using F5's Access Policy Manager – Enable app tunneling for AirWatch apps and wrapped apps using your F5 APM.
- Enabling Secure Connections using F5's SSL VPN Edge Client – Enable secure connections through VPN using your F5 SSL VPN Edge Client.

Before You Begin

Before integrating AirWatch with your F5, you should consider the following prerequisites, requirements, supporting materials, and helpful suggestions from the AirWatch team. Familiarizing yourself with the information available in this section helps prepare you for integrating AirWatch with your F5.

Getting Started

This guide covers two separate scenarios:

- Using app tunneling using your F5 APM to establish a secure connection between AirWatch applications or wrapped apps and your backend resources.
- Using a VPN profile to establish a secure connection using your F5 SSL VPN Edge Client between managed applications and your backend resources.

The approach you take will most likely depend on the existing F5 infrastructure your organization has in place.

The following requirements, steps, and procedures are used to configure your F5 for the most basic access. This is but one of many potential configurations, and AirWatch does not recommend it for production use.. Please refer to your F5 documentation and support for detailed information on securing access to your internal resources.

Chapter 2:
Enabling App Tunneling using F5's Access Policy Manager

To enable app tunneling for AirWatch apps and wrapped apps, you must ensure your F5 is configured properly and enabled in the AirWatch Console for integration. You can then associate either a Default or Shared application profile with your applications.

Configuring Your F5

The following requirements, steps, and procedures are used to configure your F5 for the most basic access. This is but one of many potential configurations, and AirWatch does not recommend it for production use. Please refer to your F5 documentation and support for detailed information on securing access to your internal resources.

Prerequisites

- 11.x Big-IP LTM and APM.
- AirWatch v6.5 and higher.
- Knowledge of network and F5 configuration.
- Basic network configuration completed on the F5 server.
- An F5 SSL profile configured.
- A preconfigured AAA server in F5.

The following is a list of Virtual Server configuration settings that will are set automatically when using the Configuration Wizard process described below:

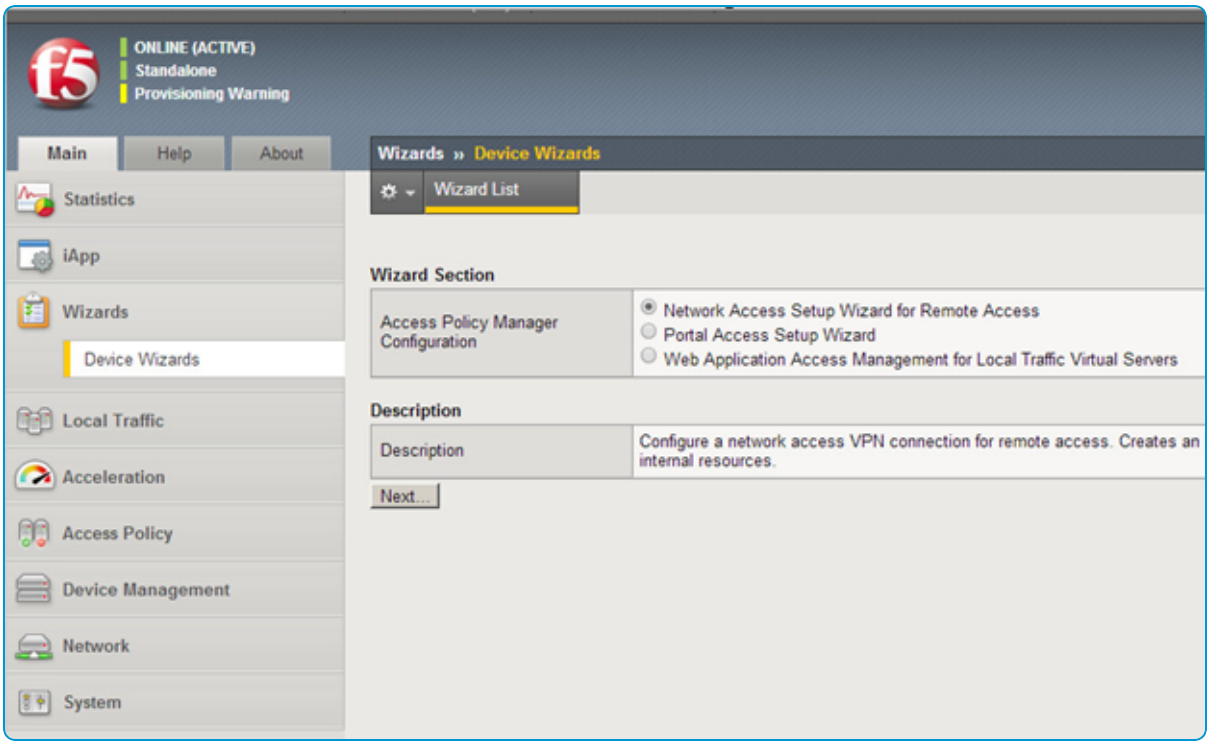
- HTTP, Access Policy and Connectivity profiles assigned, as well as an IP lease pool.
- VDI and Java support are enabled.
- No Source Address Translation.
- If you use the Device Wizard to configure Network Access, the only changes you need to make are configuring your SSL Client Profile and enabling VDI and Java Support in the Advanced settings for the Virtual Server.

The Access Policy can be customized to meet your needs. For example, the most basic is with AD or LDAP integration. The Virtual Server can be configured to require client certificates, which can be issued to the device when the application is launched. The following steps were used to configure full network access for the AirWatch Managed Browser.

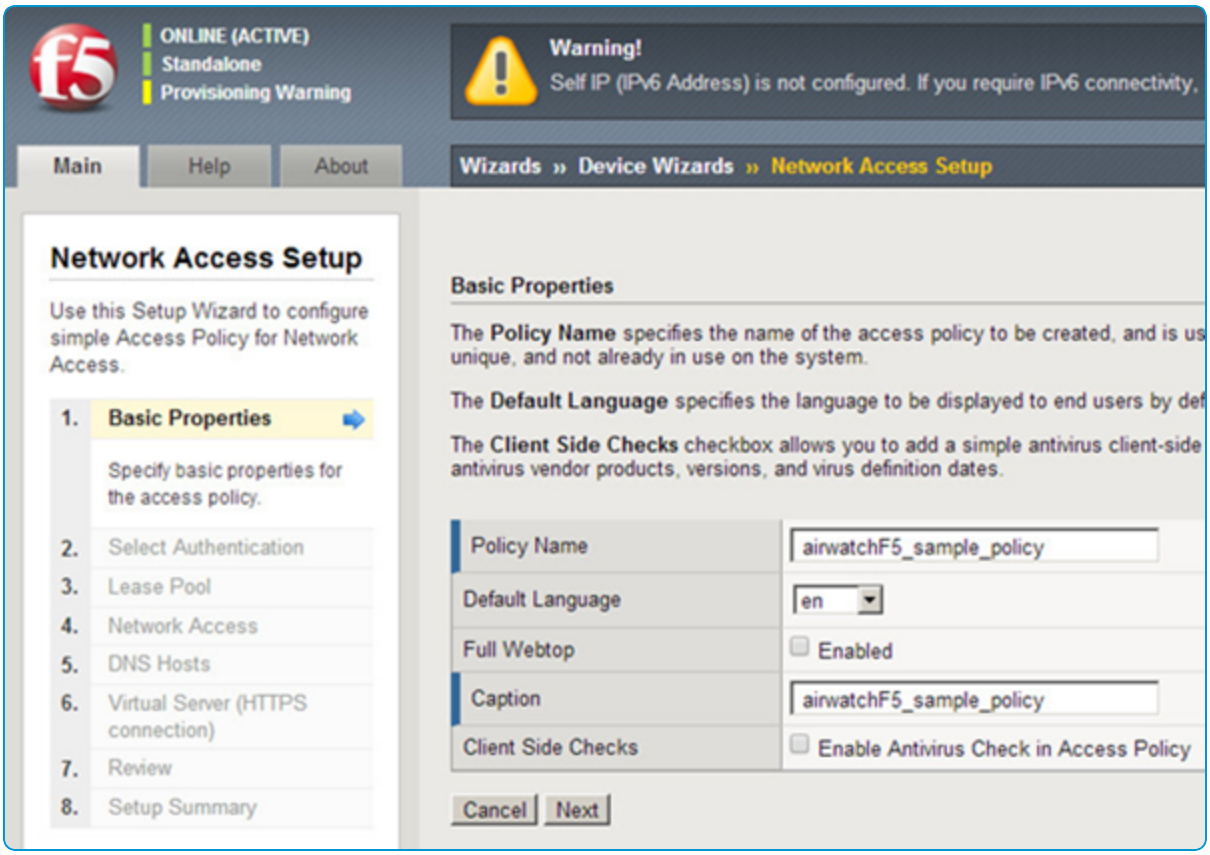
Configuring the F5

The following requirements, steps, and procedures are used to configure your F5 for the most basic access. This is but one of many potential configurations, and AirWatch does not recommend it for production use. Please refer to your F5 documentation and support for detailed information on securing access to your internal resources.

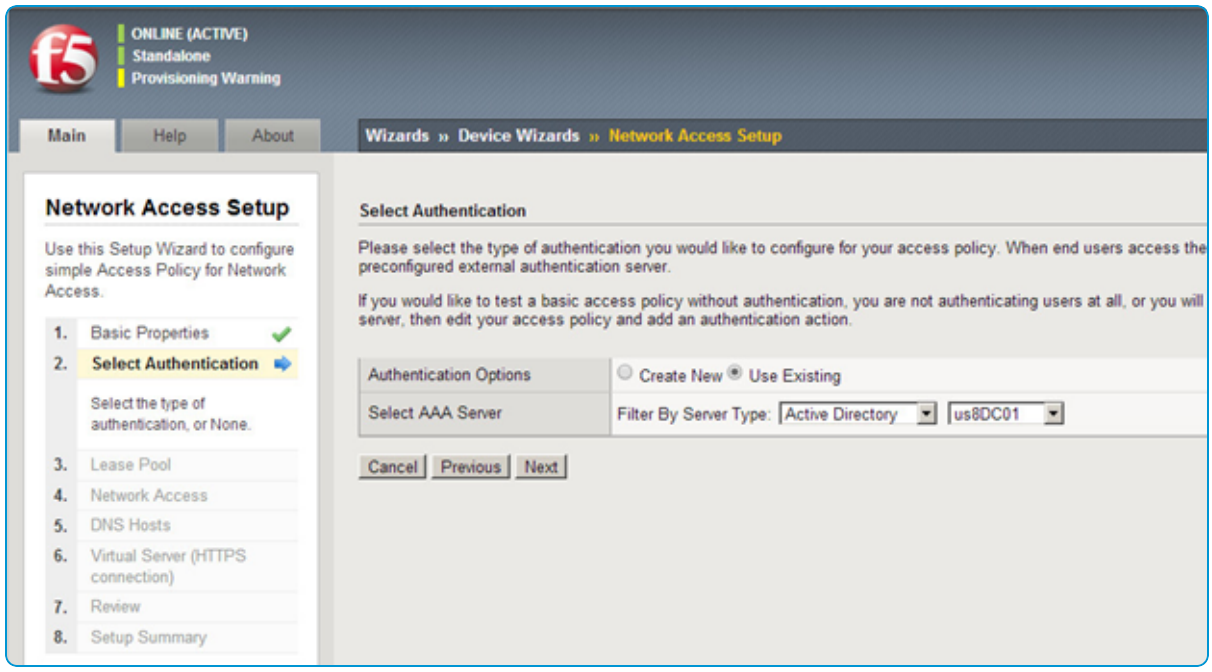
1. Start the Device Wizard, select **Network Access**, and then select **Next**.



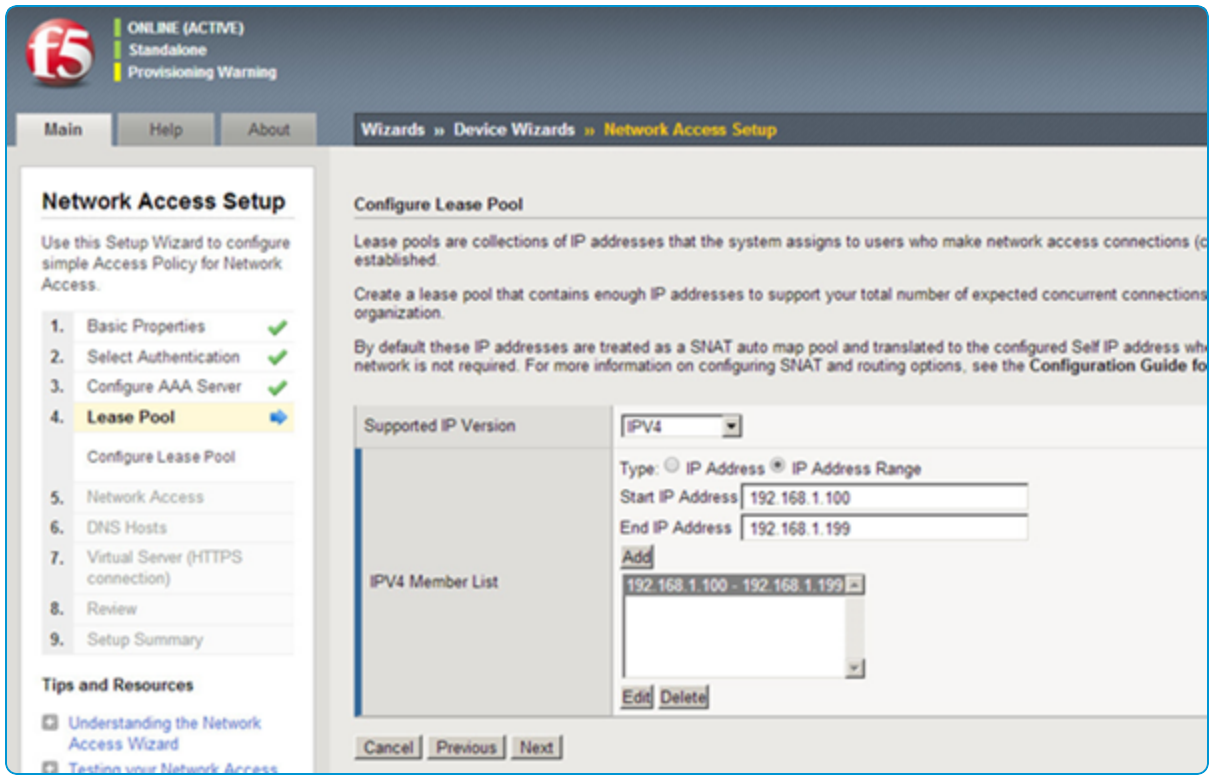
2. Name your policy and then uncheck **Enable Antivirus Check in Access Policy**. Select **Next**.



3. Select your AAA server, fill out relevant information, and select **Next**. If you do not have a AAA server configured, you may **Create a New AAA server** here or select **No Authentication**. Refer to the help tab and your F5 documentation for more information.

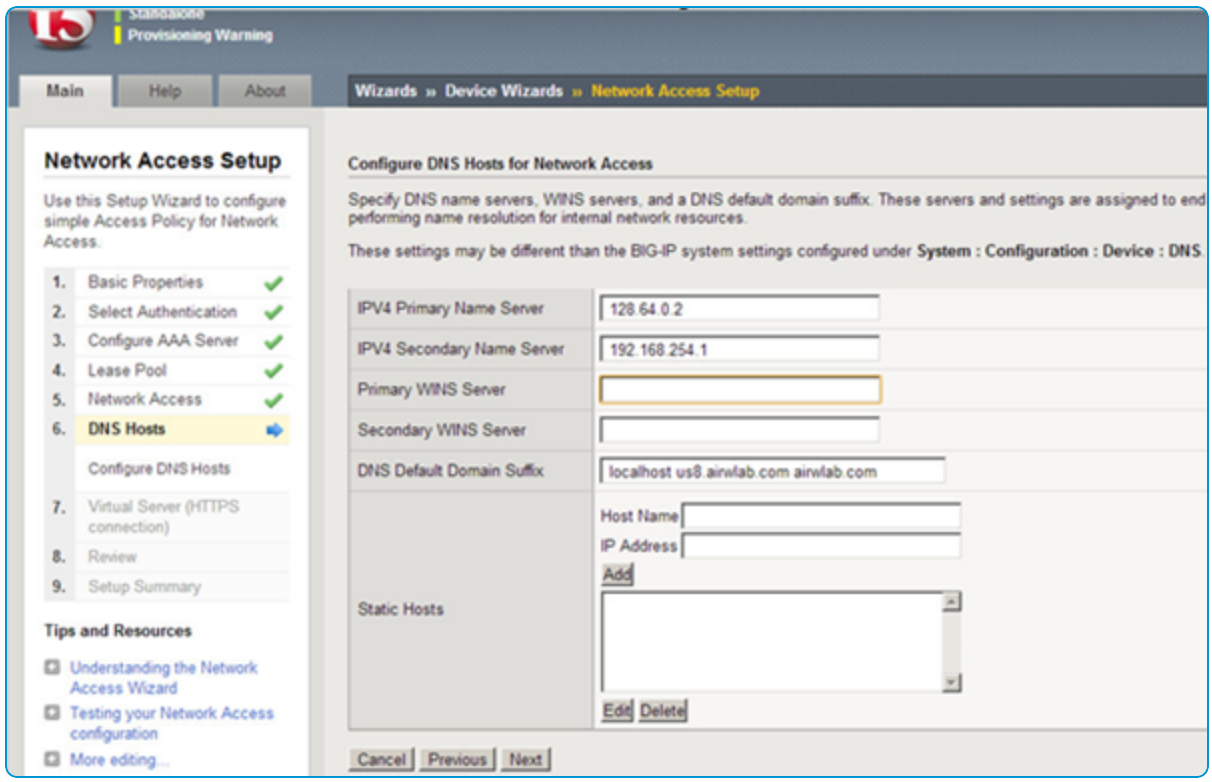


4. Configure an IP lease pool for connected devices. Take into account how many connections you may have at any given time. You need an IP for each device connected. This IP is released to the pool when the connection is terminated.

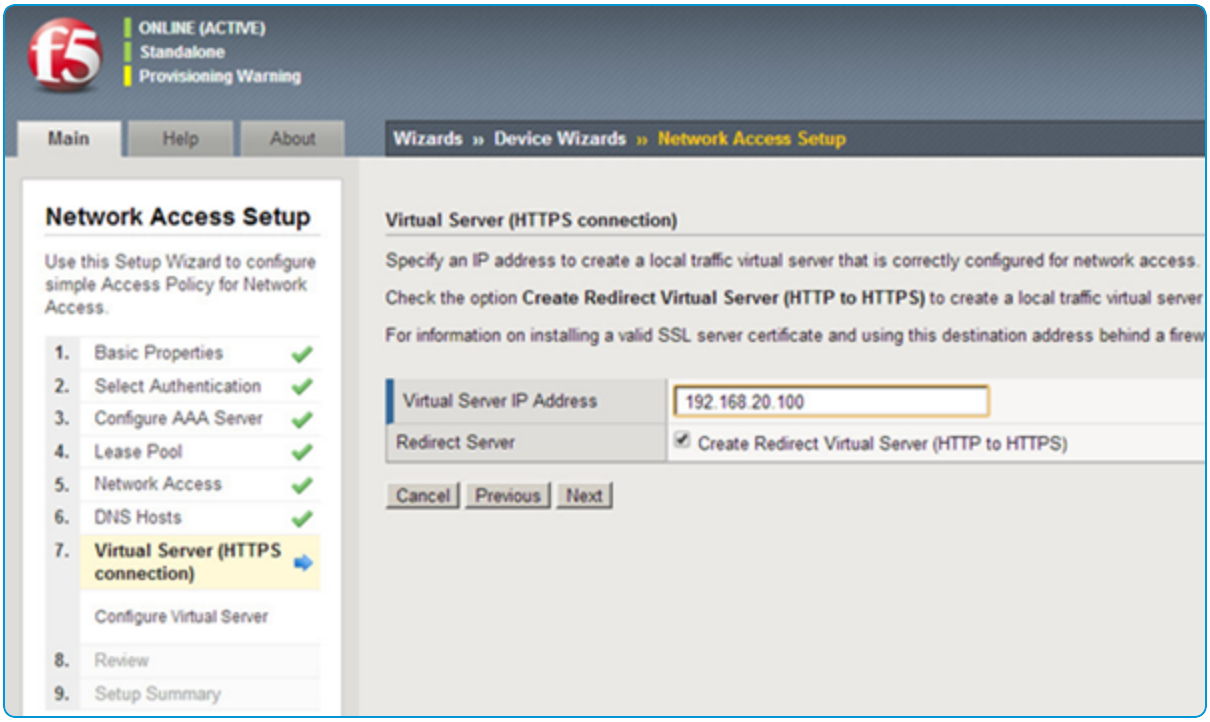


5. Select **Network Access** settings. For this example, no changes are needed to the default settings.

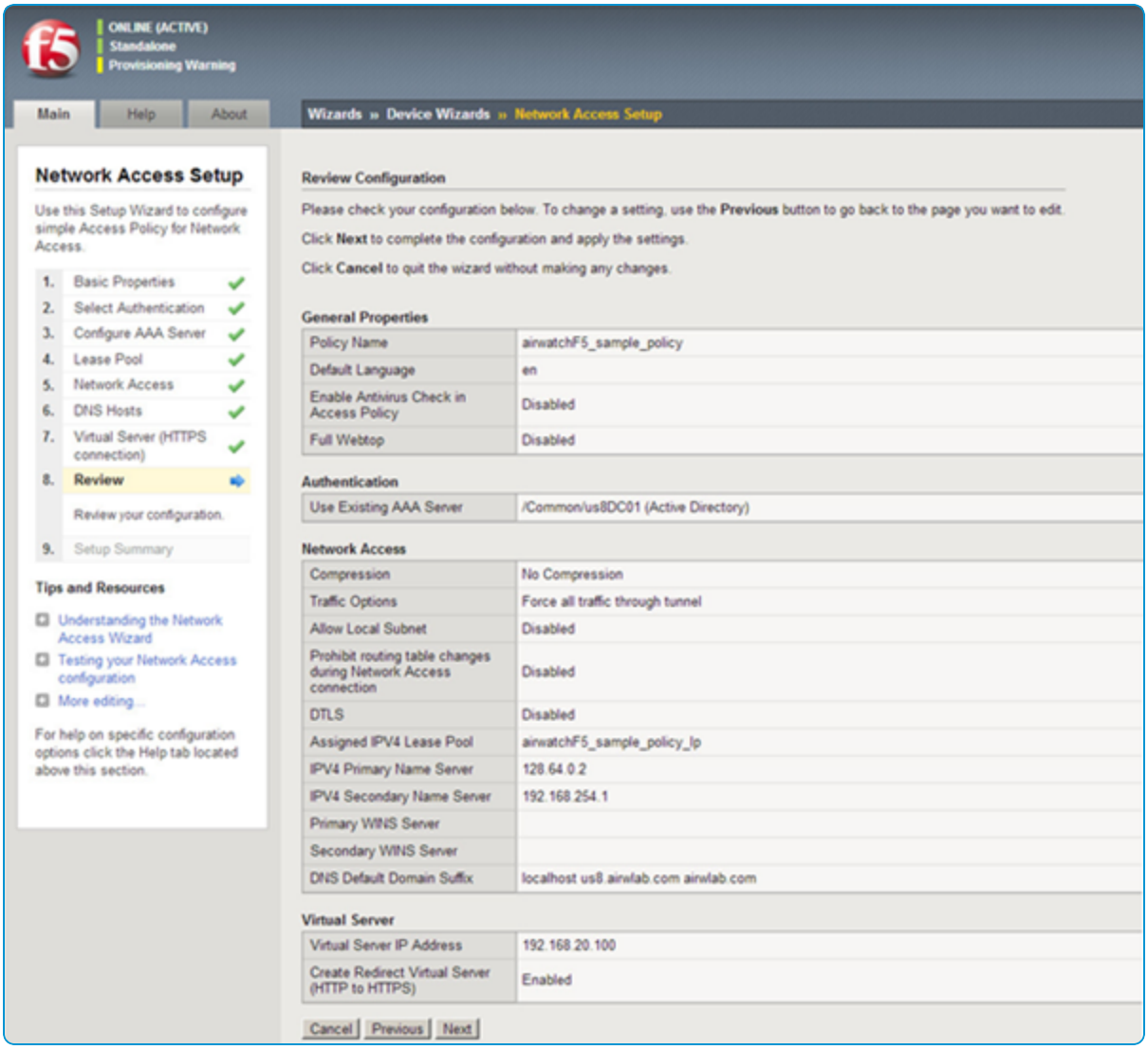
6. Configure DNS settings for your Network Access settings. You can configure static hosts in addition to or in replacement of adding a DNS.



7. Select an IP for your Virtual Server. This is suggested to be an IP on the External F5 network. Refer to your F5 documentation for more information.

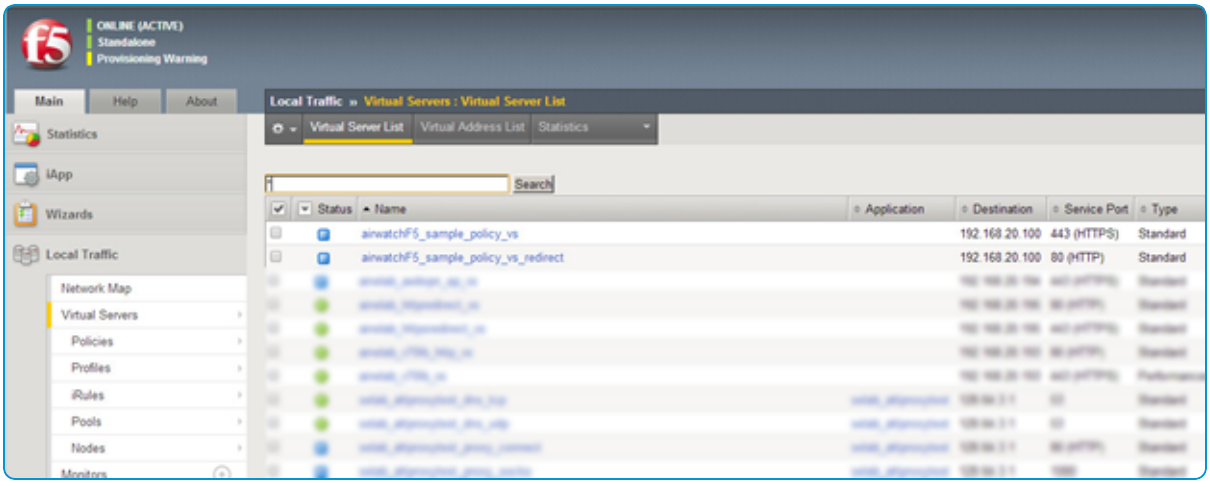


8. Review your settings and select **Next**.

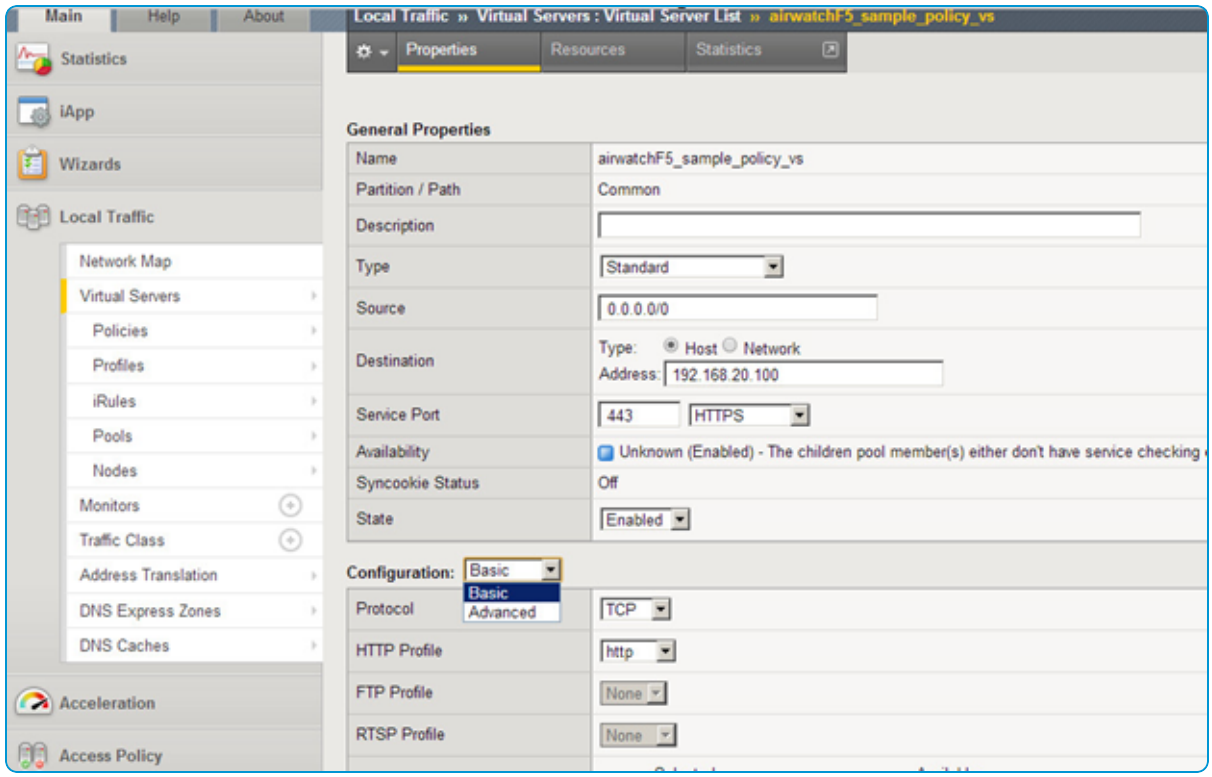


9. Follow the onscreen instructions and select **Finished** when you are satisfied that the settings are correct.

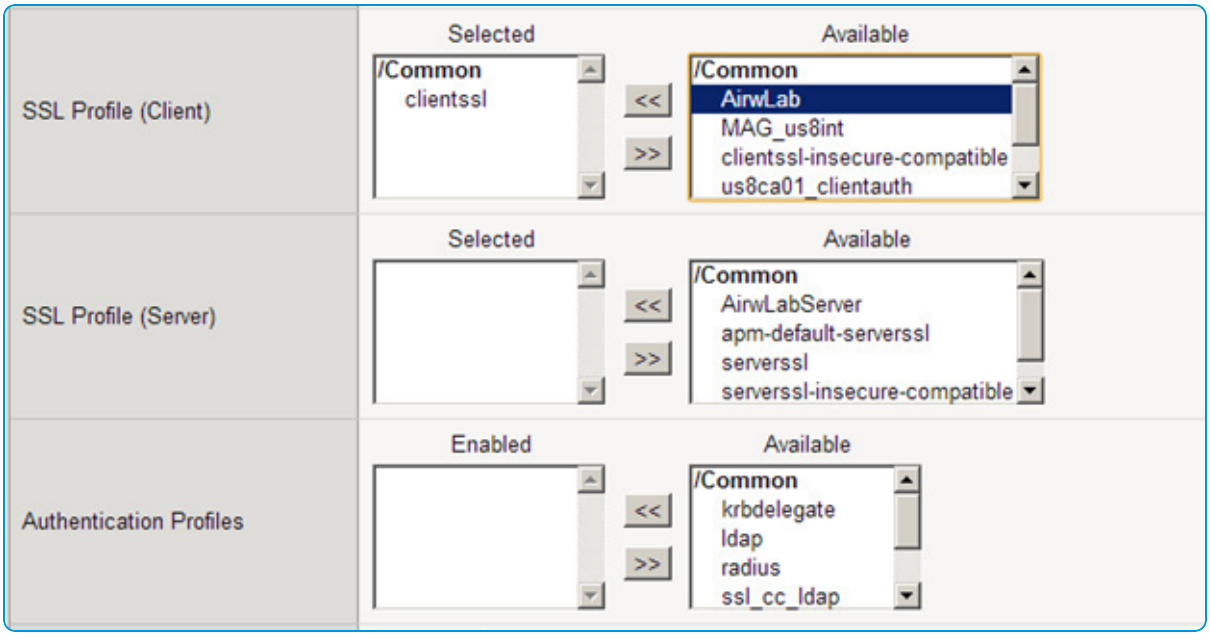
10. Select **Local Traffic > Virtual Servers** and then select the virtual server that was created to listen on 443.



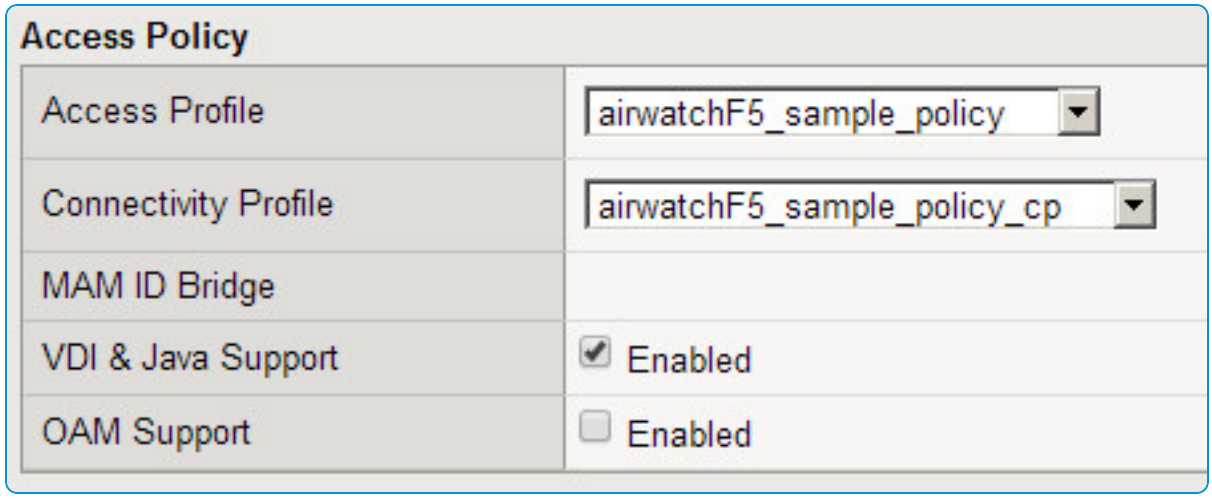
11. Select **Advanced** in the **Configuration** drop-down menu.



12. Review your SSL profile and ensure the appropriate profile is selected. For more information on SSL profiles, refer to your F5 documentation.



13. In the **Access Policy** settings, enable **VDI & Java Support**.



14. Select **Update** at the end of the configuration page. You have now configured the F5 to accept client connections.

You need to configure a DNS entry that points to the IP of the Virtual Server you selected in step 7. This is the DNS name you use when configuring F5Integration in the AirWatch Console. Ensure you have a service account that can be authenticated by the AAA server you configured in step 3. Complete integration by following the instructions for configuring F5 Integration in the AirWatch Console. You also need to make sure that the AppTunnel settings are configured to use the F5.

Enabling F5 in the AirWatch Console

The next step for enabling F5 integration with your AirWatch environment is to enable it in the AirWatch Console and enter your F5 server details. This can be done at any organization group to support multi-tenancy.

You must have the correct permissions to configure F5 Settings in Enterprise Integration. If this option does not display when you select the link, ensure you have full administrative permissions.

To enable F5 integration, perform the following step-by-step instructions:

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Proxies and Tunnels.**
2. Select **Add**, then select **App Tunnel** as the **Function** and **F5 Proxy** as the **Type**. Provide a **Name** and **Description**.
3. Enter the **Proxy Server** and **Proxy Port** information of your F5 server.

   The **Proxy Server** is the external DNS name that resolves to the IP address of your F5.

   The **Proxy Port** is the port selected when configuring the Virtual Server.
4. Select an **Authentication Mode.** This should reflect the settings made on the F5 Access Policy. If you were to use the configuration settings in the previous section as an example, then this would be a username and password that can authenticate to your AAA server.
   - **Username / Password and Certificate** – Use both username and password credentials and a certificate for authentication.
   - **Username / Password** – Use only a username and password combination for authentication.
   - **Certificates** – Use only a certificate for authentication.

     For more information, see Authentication.
5. Select whether to use an **SSO Identity** or **Service Account** if you included Username / Password in the Authentication Mode. If you select Service Account, enter your username and password credentials.

   For more information, see Authentication.
6. Select whether to use a **Defined Certificate Authority** that you configured in the AirWatch Console or **Upload** to upload a certificate if you selected either **Username/Password and Certificate** or just **Certificates** as the Authentication Mode.
7. Select **Save** when you are done.

Now that you have defined your F5 server within the AirWatch Console, you can use it to enable app tunneling for the applications below.

Authentication

The AirWatch Console enables you to leverage either single factor or two factor authentication. For single factor authentication, you can use any one of the following:

- **Certificate-based –** Issue a certificate through an integrated certificate authority. Select or upload a certificate authority on the F5 system settings page in the **Credential Source** drop-down list, then specify the **Certificate Authority** and **Certificate Template**.

  Certificates are especially useful because they can be revoked for noncompliant devices, which ensures unauthorized users cannot successfully authenticate using only their credentials, which may still be valid.

- **SSO Identity –** Allow end users to use the same SSO credentials (for example, directory service credentials) that they use to access AirWatch apps.

  Enable Single Sign On by navigating to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**. For more information about this feature, please see the **VMware AirWatch Mobile Application Management Guide**.

- **Service Account –** Enter the service account credentials of the F5 server you configured. With this method, all users use the same service account to authenticate. This lets you prevent users from accessing the VPN from other clients and ensures the credentials are kept private.

Enforce two-factor authentication by combining either SSO Identity or a Service Account with certificates.

Configuring AirWatch Applications to Use App Tunneling

Now that you have configured your F5 and enabled it in the AirWatch Console, you have to tell the applications to use the F5 for their network traffic. You can do this for the VMware Browser and wrapped applications.

VMware Browser

Configuring the VMware Browser with app tunnel settings allows the Browser to redirect all or some traffic through your F5 Proxy. The Browser supports the Kerberos and NTLM authentication types without any additional console settings changes. You can enable split tunneling by predefining domains. Predefined domains go through the F5 while other domains route directly to the Internet. Entering no domains, while enabling app tunneling, causes all requests to go through the F5.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Select **Enabled** for the **App Tunnel** field to indicate to the VMware Browser that web traffic needs to be channeled through a proxy server.
3. Select **F5 Proxy** as the **App Tunnel Mode**.
4. Ensure your F5 settings are populated.
5. Alternatively, select **Configure F5 Settings** if you have not previously implemented F5. This link redirects you to F5 configurations so that the app tunnel can function properly.

   You must have the correct permissions to configure F5 Settings in Enterprise Integration. If this option does not display when you select the link, ensure you have full administrative permissions.
6. Optionally, enable the split F5 Tunnel for devices by entering URLs into the **Apply Proxy to these Domains Only** textbox. 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 F5. If the URL does not match the URL Prefix in the list, it should go directly to the Internet. Leave the text box empty to send all requests through the F5.
7. Ensure you have configured the VMware Browser to use these settings by navigating to **Groups & Settings > All Settings > Apps > VMware Browser** and selecting **Default** as the **Application Profile**.

Wrapped Applications

You can take advantage of AirWatch's advanced management capabilities to bring application security and configuration to the next level. Advanced application management provides you with AirWatch App Wrapping, which you can use to add rich features and security – including app tunneling – directly to your own enterprise applications. You can do this in one of two ways: By creating an app wrapping profile that is shared across all applications or by creating a custom app wrapping profile that applies to a specific application. With either method you can configure app tunnel settings that allow the applications to access internal resources through your F5 Proxy.

For the first "Default" type you can configure settings as part of an Android Default Settings or iOS Default Settings SDK profile, which you can then apply to all applications set up at a particular organization group or below. This is performed by navigating to **Groups & Settings > All Settings > Apps > Settings and Policies**. This lets you use a single point of configuration for all of your apps in a particular OG or child groups. In terms of app tunneling, any application using this Default profile would use the app tunnel for its network communication. For the second "Custom" type you can configure profiles that you can apply to specific app wrapped applications. These offer granular control for specific applications and override the Default Settings profiles. In terms of app tunneling, only those wrapped apps utilizing this Custom profile would use the app tunnel for their network communication.

Both methods are outlined below.

Configure an App Tunnel with a Default Profile

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Enable **App Tunnel** to allow the application to travel through your F5 proxy. The settings automatically use the F5 server details you provided under **System > Enterprise Integration > F5 Integration**.
3. Enter domains to route through the app tunnel. All traffic not listed here goes directly to the Internet. If nothing is listed here, all traffic is directed through the app tunnel.
4. Select **Save** to save the settings.
5. Upload an internal application or edit an existing one. Under the **Wrapping** tab, select **Enable App Wrapping** and select the Default profile (either Android Default Settings or iOS Default Settings).
6. Select **Save & Publish**.

Any internal applications you wrap with the app wrapping profile now use your F5 proxy for their network traffic.

Configure an App Tunnel with a Custom Profile

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Profiles**. Select **Add Profile** and select **App Wrapping Profile**, then the applicable platform.
2. Enter information on the **General** tab as necessary, such as the name of the profile.
3. Select the **Proxy** tab and **Enable App Tunnel** to allow the application to travel through your F5 proxy. The settings automatically use the F5 server details you provided.
4. Enter domains to route through the app tunnel. All traffic not listed here goes directly to the Internet. If nothing is listed here, all traffic is directed through the app tunnel.
5. Select **Save** to save the settings.
6. Upload an internal application or edit an existing one. Under the **Wrapping** tab, select **Enable App Wrapping** and

select the custom profile you created.

7. Select **Save & Publish**.

Any internal applications you wrap with the app wrapping profile now use your F5 proxy for their network traffic.

Chapter 3:
Enabling Secure Connections using F5's SSL VPN Edge Client

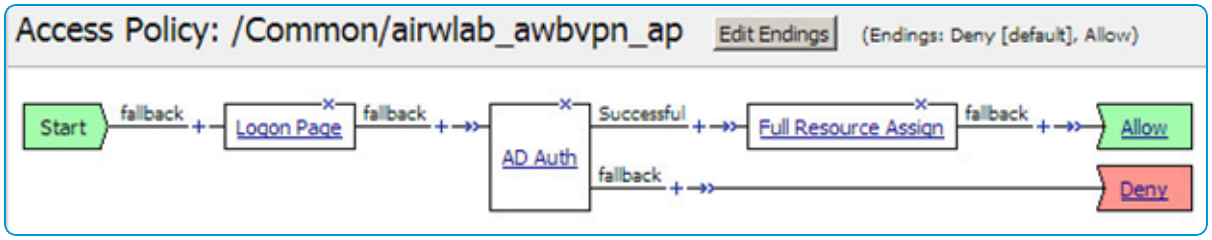
This section describes the different types of VPN configuration profile that you can configure through AirWatch for F5's SSL VPN Edge Client. The Edge Client enables mobile devices to access internal resources through F5's Big-IP Access Policy Manager (APM), Edge Gateway or FirePass solutions. AirWatch allows for easy configuration of some important data loss prevention features available in the Edge Client, such as on-demand VPN with certificate authentication. For iOS 7 users you can enable Per-App VPN, which forces selected applications to connect through your corporate VPN.

Configuring Your F5

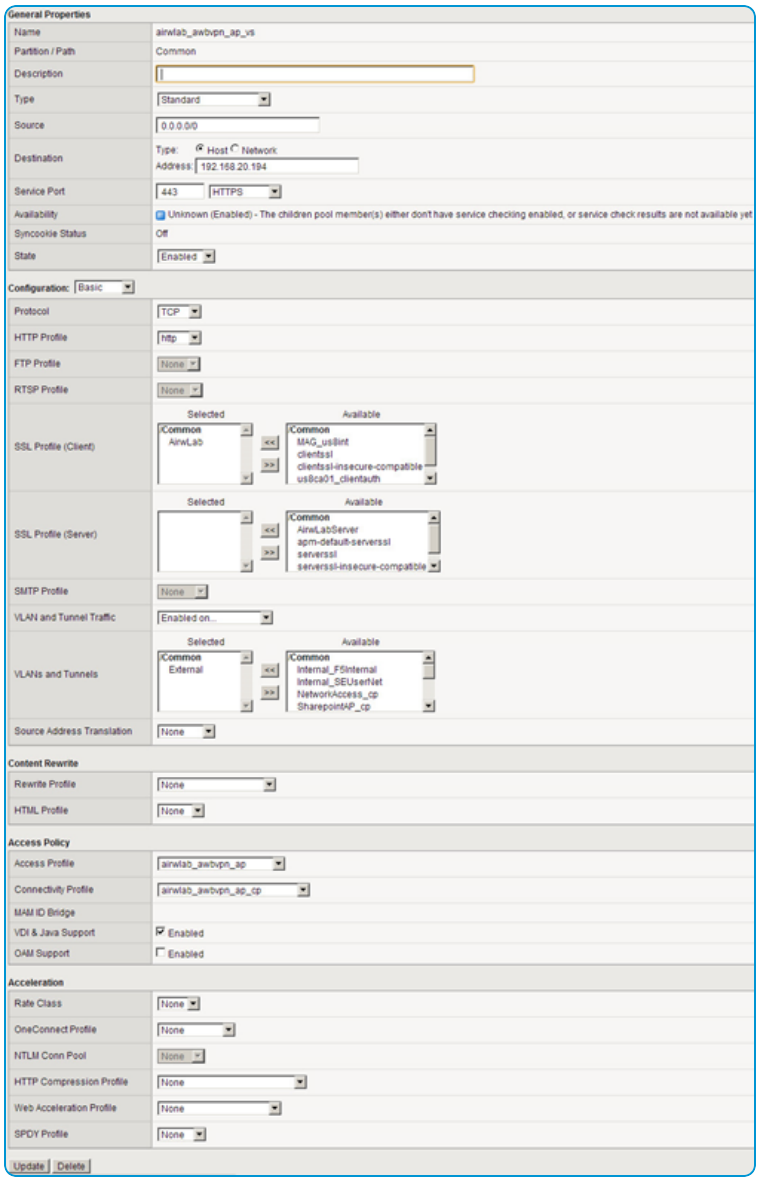
For the Edge Client to work correctly it needs to connect to a support F5 VPN appliance solution. In this case we use the Access Policy Manager (APM). APM includes configuration wizards that guide you through the configuration of all the necessary base components to provide VPN access to the Edge Client. This should result in a newly created Virtual Server with an associated Access Policy.

Important: The following requirements, steps and procedures are used to configure your F5 for the most basic access. This is one of many potential configurations, and AirWatch does not recommend it for production use.. Please refer to your F5 documentation and support for detailed information on securing access to your internal resources.

Access Flow for a Basic Access Policy



Sample Virtual Server Configuration

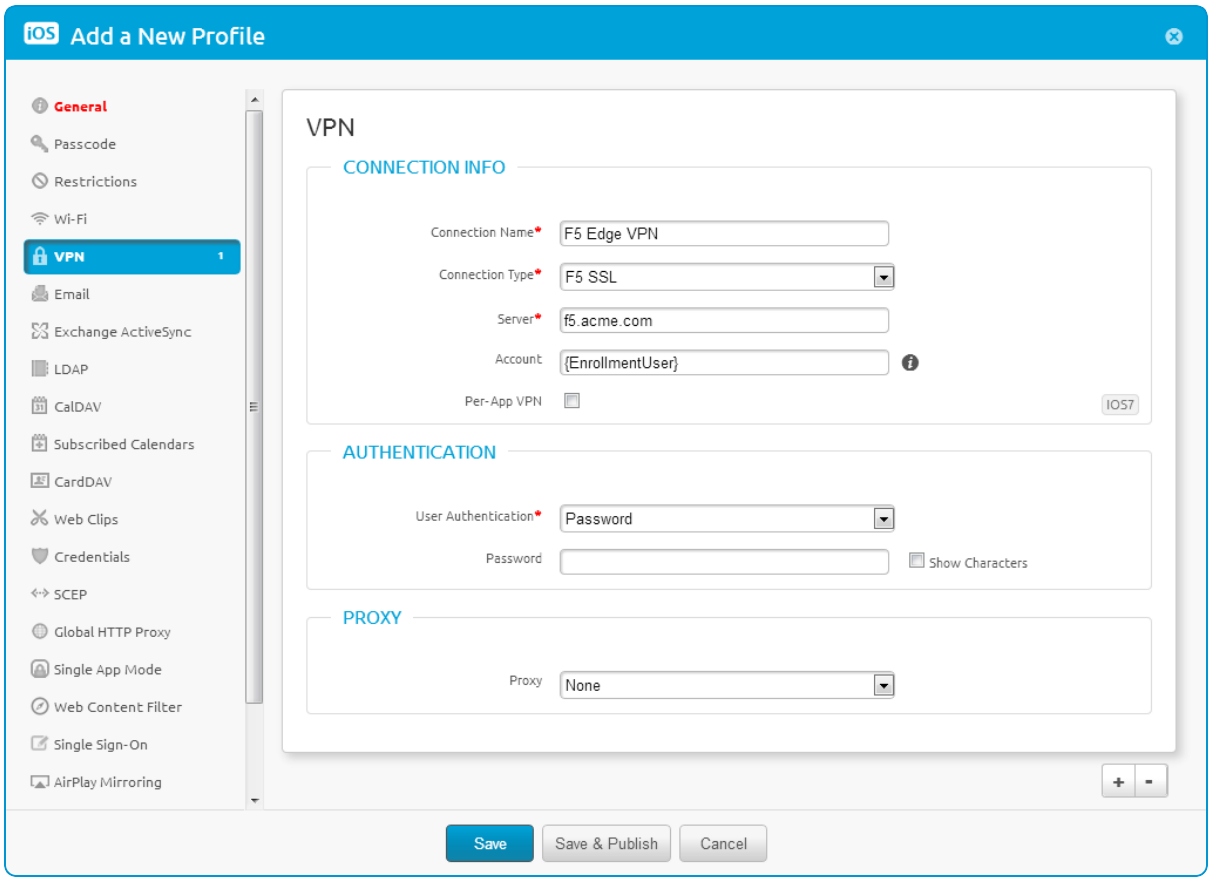


VPN Comparison Matrix

	Use if you want to...	Requires...
Base VPN Profile	Create a VPN profile that applies to all network traffic on Android and iOS devices	
VPN On-Demand Profile	Create a VPN profile that automatically initiates a VPN connection whenever applications navigate to any of the domains you specify.	iOS
Per-App VPN Profile	Create a VPN profile that lets you specify which specific managed applications can utilize the VPN connection.	iOS 7+

Configuring a Base VPN Profile for the Edge Client

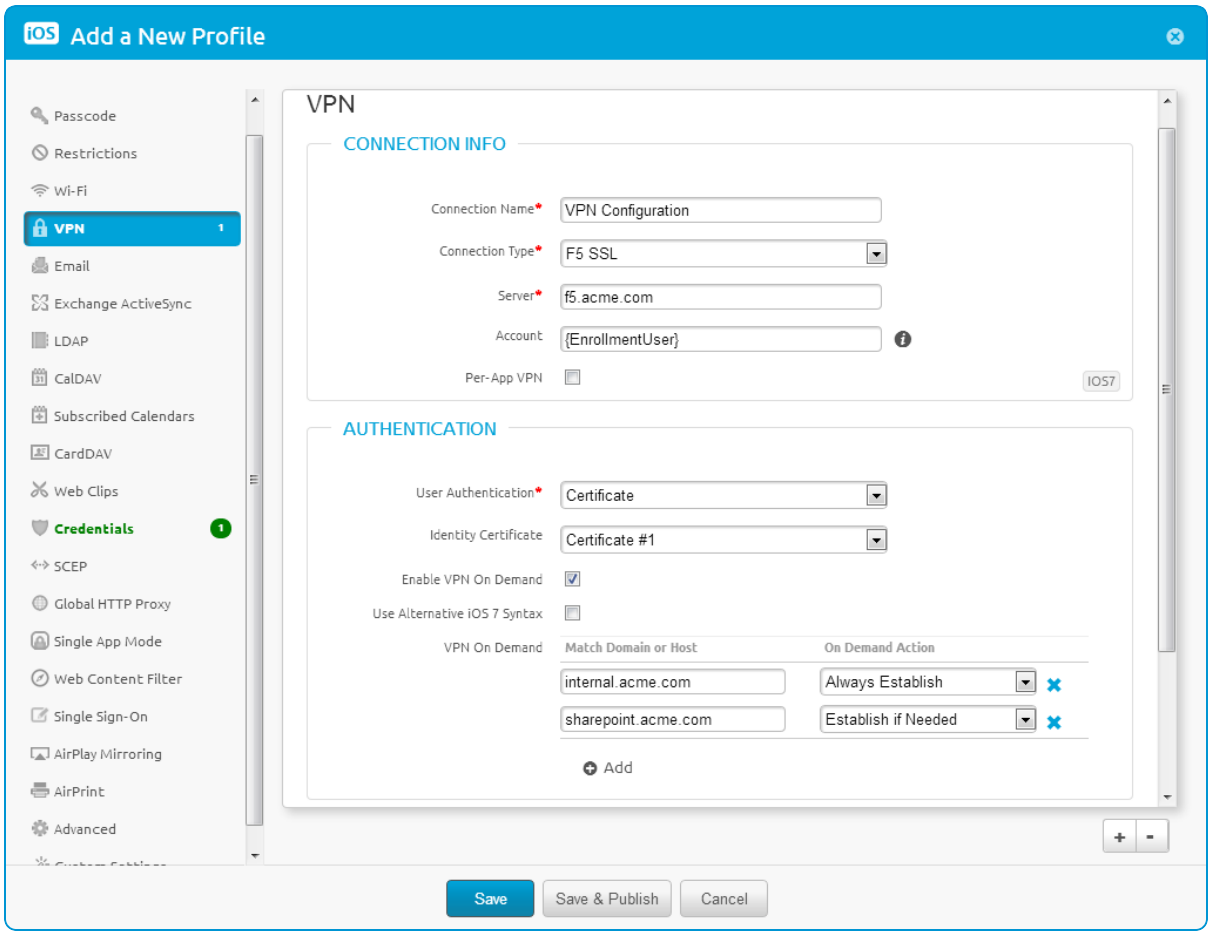
Create a base VPN profile for Android or iOS devices that applies to all network traffic.



1. Navigate to **Devices > Profiles > List View** and **Add** a new profile for iOS or Android.
2. Select the **VPN** payload and select on **Configure** to add a new payload.
3. Customize the **Connection Name** as it will appear on the Edge Client.
4. Select **F5 SSL** as the **Connection Type**.
5. Provide the **Server** address to which the Edge Client will connect.
6. Specify a user **Account** or lookup-value from in the user field.
7. Enter **Authentication** details. By default the authentication type is set to **Password**. If left empty, the end user is prompted for a password when initiating the connection.
8. Enter **Proxy** details, if applicable.
9. Select **Save & Publish**.

Configuring VPN On-Demand for iOS Devices

The VPN On-Demand feature for iOS devices allows applications to automatically initiate a VPN connection using the Edge Client whenever those applications navigate to any of the domains you specify in the VPN profile.



1. Create a new base VPN profile.
2. Add a **Credential** payload to the profile.

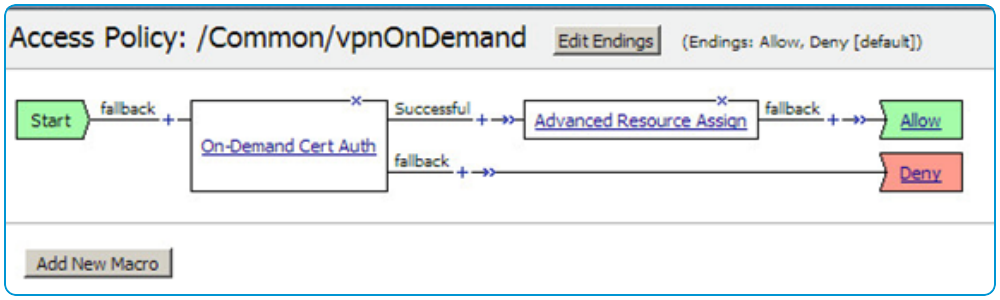
   You can upload an individual certificate or use a defined certificate authority to request independent certificates for each user.
3. In the **VPN** payload, change the **User Authentication** type to **Certificate**.
4. Select the corresponding **Identity Certificate** from the drop-down menu.
5. Select Enable **VPN On-Demand**.
6. Specify the domains or subdomains that should trigger the VPN connection. *.com is not an accepted entry.
   a. internal.com = *.internal.com
   b. subdomain.internal.com = *.subdomain.internal.com

7. Select the **On-Demand** action for each domain specified in the payload:
   a. **Establish if Needed –** The VPN connection initiates only if the specified page cannot be reached directly.
   b. **Always Establish –** The VPN connection is established regardless of whether the page can be accessed directly or not.
   c. **Never Establish –** The VPN connection is not established.
8. Select **Save & Publish**.

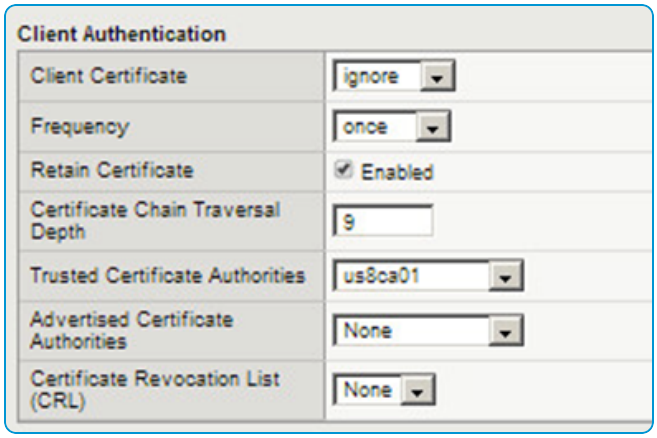
Notes

- The access policy and SSL profile associated with the Virtual Server need to be to modified accordingly to support On-Demand Certificate Authentication.

Sample On-Demand Certificate Authentication Access Policy



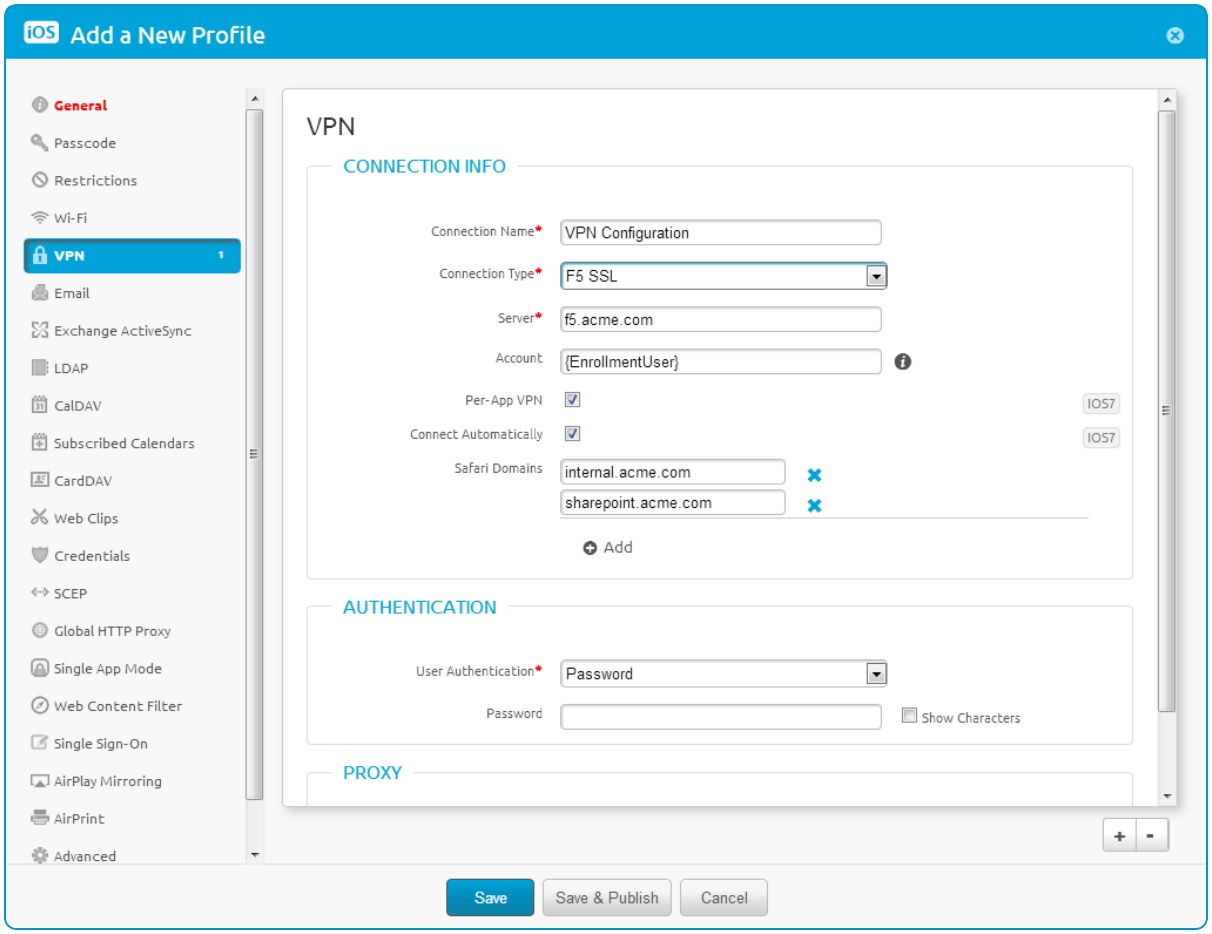
SSL Profile Settings for On-Demand Certificate Authentication



- If using On-Demand Certificate Authentication, make sure client authentication is enabled with **Client Certificate** set to **Ignore**.

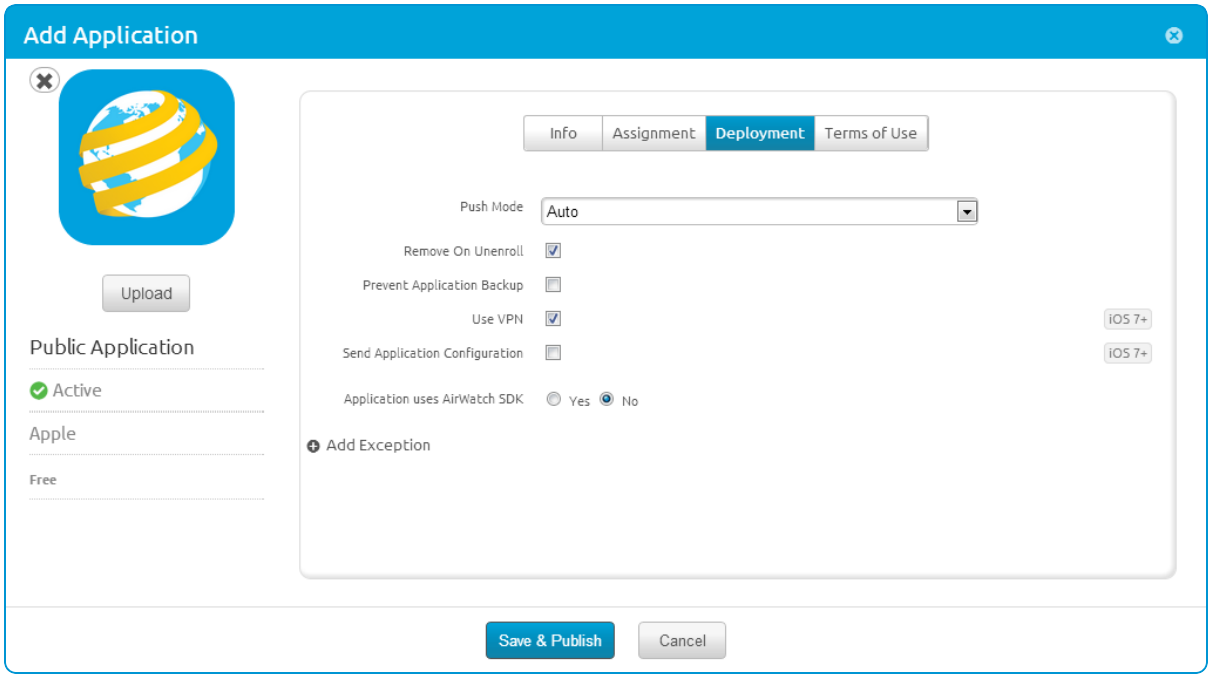
Configuring Per-App VPN for iOS 7 Devices

The Per-App VPN feature, which is available for iOS 7 devices, allows you to specify which managed applications can utilize the VPN connection. Managed applications are those you push specifically to devices using the AirWatch Console.



1. Create a new base VPN profile.
2. Select **Per-App VPN**.
3. Enter whitelisted domains for Safari, if applicable. Since Safari is not a managed application, this is the location in the AirWatch Console where you specify the domains that should use Per-App VPN.
4. Select **Save & Publish**.

Now that you have created and published the Per-App VPN profile, you need to specify which managed applications can use this VPN connection.

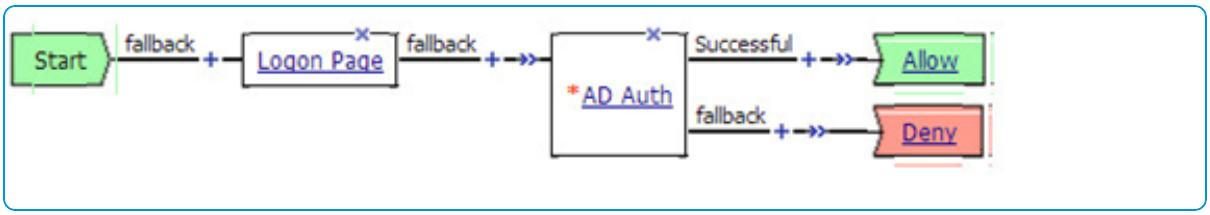


1. Navigate to **Apps & Books > Applications > Native**. The applications page displays.
2. **Add** an application from either the **Internal** or **Public** tabs.

   For more information about how to add an application, refer to the **VMware AirWatch Mobile Application Management Guide**.
3. In the **Deployment** tab, select **Use VPN**.
4. Select **Save & Publish**. Note that this re-pushes the application to all applicable devices, so you should schedule accordingly and notify end users.

Notes

- Applications with the **Use VPN** option enabled requires an active VPN connection for Internet access.
- The Access Policy and Virtual Server need to be modified to support Per-App VPN.



  In this case, there should be no Resource Assignment within the policy.
- Verify that VDI & Java Support is enabled within the Virtual Server settings.