BIG-IP APM and F5 Access for macOS

Version 1.0.0

Table of Contents

BIG-IP APM and F5 Access for macOS

In September 2017, Apple posted the release of F5 Access for macOS version 1.0.0. Users should download this new version from the macOS app store.

Requirements for F5 Access for macOS

F5 Access for macOS 1.0.0 has the following minimum software requirements:

- macOS 10.12.2 or later
- BIG-IP v13.0 or later

F5 Access for macOS general information

General F5 Access Information

F5 Access for macOS provides Layer 3 network access for the BIG-IP APM module. The F5 Access for macOS SSL VPN application complements the existing Edge Client VPN product line, addressing similar use-case and deployment scenarios.

F5 Access for macOS incorporates Apple's new Network Extension Framework. This change creates some major architectural shifts in the new F5 Access VPN application. As a result, there are currently feature differences between F5 Access and Edge Client for macOS.

Note: *Users can install and use both F5 Access and Edge Client for macOS on the same system.*

F5 Access for macOS supports certification authentication (CA), but with some caveats. When you use non-official certificates, by default, all non-officially signed server certificates are rejected. If you install your own CA, you must set the system keychain settings to **Always Trust**.

Note: *F5 Access for macOS is hosted in the Apple App Store, instead of on a BIG-IP system.*

F5 Access for macOS has two components:

- **App Extension**: built on the Network Extension framework to provide traffic tunneling.
- **F5 Access Container App**: handles configuration management and state monitoring.

Supported Authentication Modes

Native

Native authentication mode is the default mode that the administrator can use to set the user logon by using username+password, optional client certificate, or both. Interactive authentication, including SAML and external logon pages, are not supported in this mode. Native mode does not require user interaction if all the credentials are previously saved.

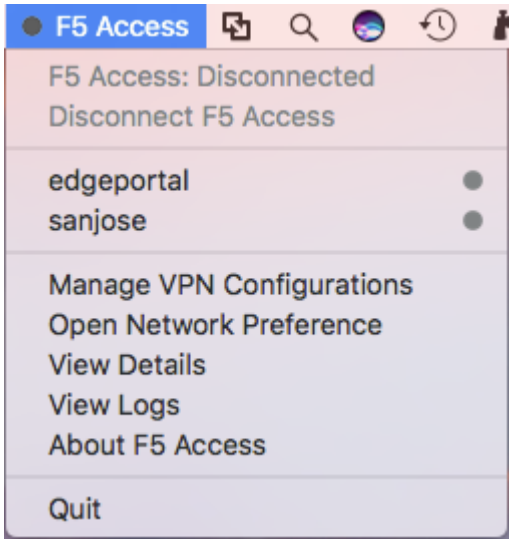
Web

Web-based Authentication is not supported in the initial release

Note: *Client certificate authentication in required mode is not supported in this release.*

About the F5 Access for macOS container app

Container app interface



After F5 Access for macOS is installed, the container app is available from the macOS menu bar.

The following functions and status items can be viewed and accessed from the container app:

- **Connection status**: Shows the status of F5 Access, and the status of configured connections. Users can disconnect from here when the status is `Connected`.
- **List of VPN configurations**: Shows the current configured VPN connections. The user can click a configuration to connect. Clicking another VPN configuration when connected causes the connection to switch VPN configurations.
- **Manage VPN Configurations**: Allows the user to add, edit, and remove VPN configurations. Note that configurations managed by a Mobile Device Manager (MDM) cannot be edited or removed by the user.
- **Open Network Preference**: Opens the network settings in the System Preferences app.
- **View Details**: Displays the connection details window.
- **View Logs**: Views the F5 Access logs. This can be useful for troubleshooting.
- **About F5 Access**: Shows information about the installed version of F5 Access
- **Quit**: Quits the container app. Note that this does not terminate the VPN connection.

Creating a VPN configuration from Container app

You create a configuration to establish a VPN connection to access network resources.

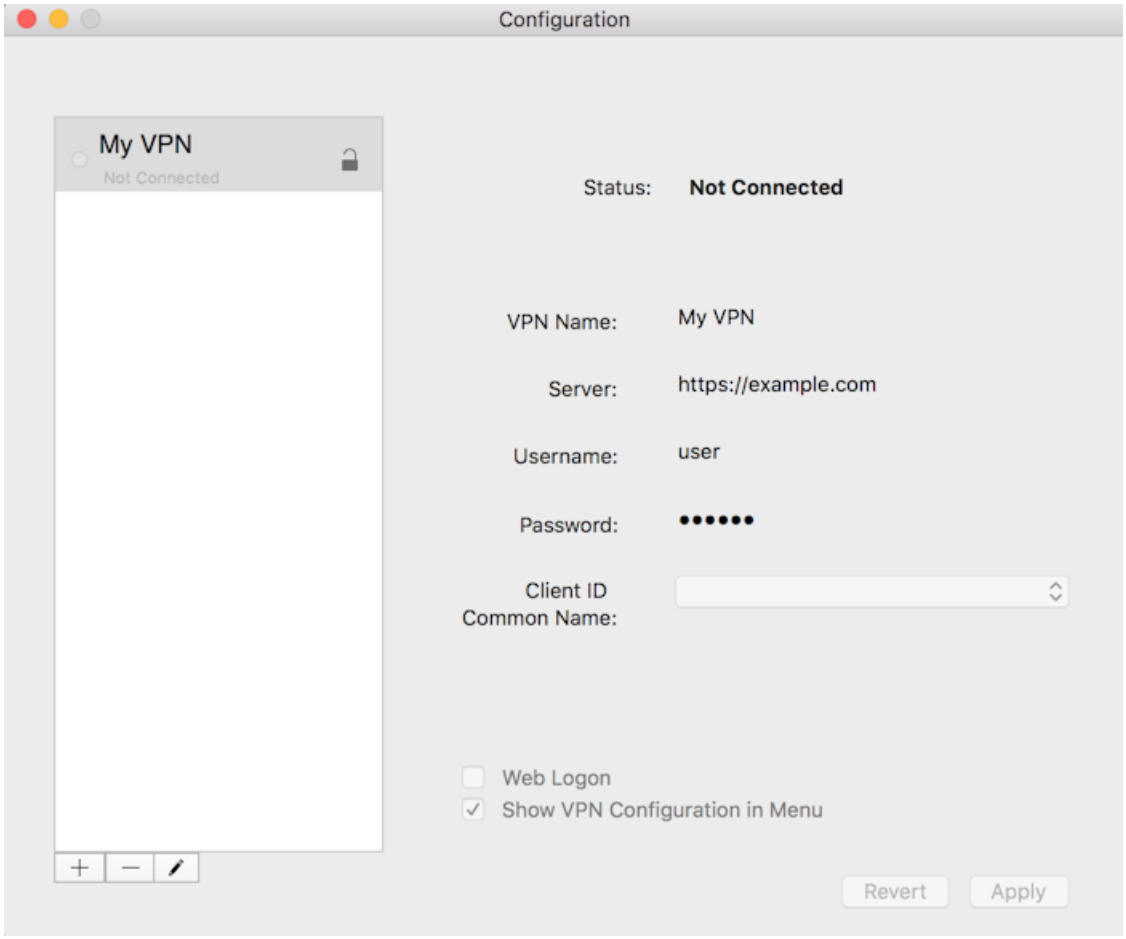
Note: *You can install a VPN profile in plist format by double-clicking it.*

1. From the F5 Container App click **Manage VPN Configurations**.
2. Click + to add a configuration.
3. In the **VPN Name** field, type a VPN name.
4. In the **Server** field, type the server address.

5. In the **Username** field, type the username.
6. In the **Password** field, type the password.
7. In the **Client ID Common Name** field, select a common name for the client certificate.
8. To show the VPN status in the F5 Container App menu, click **Show VPN Status in Menu bar**.
9. Click **Apply**.

The VPN configuration is created. Start the VPN connection by selecting the configuration name from the F5 Container App menu.

Creating the Configuration and the Configuration in the Container App menu



Editing a VPN configuration from Container app

You can edit or delete a configuration from the Container app after you have created it.

1. From the F5 Container App click **Manage VPN Configurations**.
2. Click the name of a VPN configuration.
3. To edit the configuration, click the pencil icon.
4. To delete the configuration, click the minus icon.

Creating a VPN configuration from a plist file

You create a configuration to establish a VPN connection to access network resources.

Important: *You cannot edit or delete a VPN configuration created with a plist file from the VPN configurations dialog.*

Double-click a plist file to install the VPN.

The VPN configuration is created. Start the VPN connection by selecting the configuration name from the F5 Container App menu.

Example plist VPN configuration file

Includes a sample plist file for VPN configuration.

VPN configuration with plist example

The following example uses sample data only. For your own configuration, items like the `PayloadDisplayName`, `Payload UUID`, username, password and certificate information must be customized to your network and installation.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
            <key>IPv4</key>
            <dict>
                <key>OverridePrimary</key>
                <integer>0</integer>
            </dict>
            <key>PayloadDescription</key>
           <string>Configures VPN settings, including authentication.</string>

            <key>PayloadDisplayName</key>
            <string>VPN (test_vpn_config)</string>
            <key>PayloadIdentifier</key>
            <string>com.f5.access.macos.vpn.profile</string>
            <key>PayloadOrganization</key>
            <string></string>
            <key>PayloadType</key>
            <string>com.apple.vpn.managed</string>
```

```
            <key>PayloadUUID</key>
            <string>3A0ED411-G45D-4551-AE35-650CE54B08D5</string>
            <key>PayloadVersion</key>
            <integer>1</integer>
            <key>Proxies</key>
            <dict/>
            <key>UserDefinedName</key>
            <string>test_vpn_config</string>
            <key>VPN</key>
            <dict>
                <key>AuthName</key>
                <string>username</string>
                <key>AuthPassword</key>
                <string>password</string>
                <key>AuthenticationMethod</key>
                <string>Certificate</string>
                    <key>PayloadCertificateUUID</key>
                    <string>CF12345D-E819-4521-88DE-2AEB6E1DC3D8</string>
                <key>RemoteAddress</key>
                <string>https://selfip.example.com</string>
                <key>ProviderType</key>
                    <string>packet-tunnel</string>
                    <key>ProviderBundleIdentifier</key>
                    <string>com.f5.access.macos.PacketTunnel</string>
            </dict>
            <key>VPNSubType</key>
            <string>com.f5.access.macos</string>
            <key>VPNType</key>
            <string>VPN</string>
            <key>VendorConfig</key>
            <dict/>
        </dict>
        <dict>
                <key>Password</key>
                <string>123456</string>
                <key>PayloadCertificateFileName</key>
                <string>identity.p12</string>
                <key>PayloadContent</key>
                <data>
MIIJCQIBAzCCCM8GCSqGSIb3DQEHAaCCCMAEggi8MIIIuDCCA28GCSqGSIb3DQEHBqCCA2AwggNcAgEA
MIIDVQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQIzdOkMx7b/skCAggAgIIDKNjtUzTS2/diyoiU
ArGTs6vaAcb6PW7bjR/5gObmwV+NHT4BVqGVfm9L+F7zkhgtSx/gTVISOLphruYjSdpiqVN8IVcL6uVR
... (etc...)
           </data>
            <key>PayloadDescription</key>
            <string>Provides device authentication (certificate or
identity).</string>
            <key>PayloadDisplayName</key>
            <string>identity.p12</string>
            <key>PayloadIdentifier</key>
            <string>com.f5.access.macos.vpn.credential</string>
            <key>PayloadOrganization</key>
            <string/>
            <key>PayloadType</key>
            <string>com.apple.security.pkcs12</string>
            <key>PayloadUUID</key>
            <string>C9BF4927-E819-4521-88DE-2AEB6E1DC3D8</string>
            <key>PayloadVersion</key>
            <integer>1</integer>
           </dict>
    </array>
    <key>PayloadDescription</key>
    <string>f5 mac tunnel test</string>
    <key>PayloadDisplayName</key>
    <string>mac_vpn_mdm_profile</string>
    <key>PayloadIdentifier</key>
    <string>com.f5.access.macos.vpn.profile</string>
    <key>PayloadOrganization</key>
    <string></string>
```

```
    <key>PayloadRemovalDisallowed</key>
    <false/>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>A6F83919-B570-41FE-A84F-52DAC24838D8</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
</dict>
</plist>
```

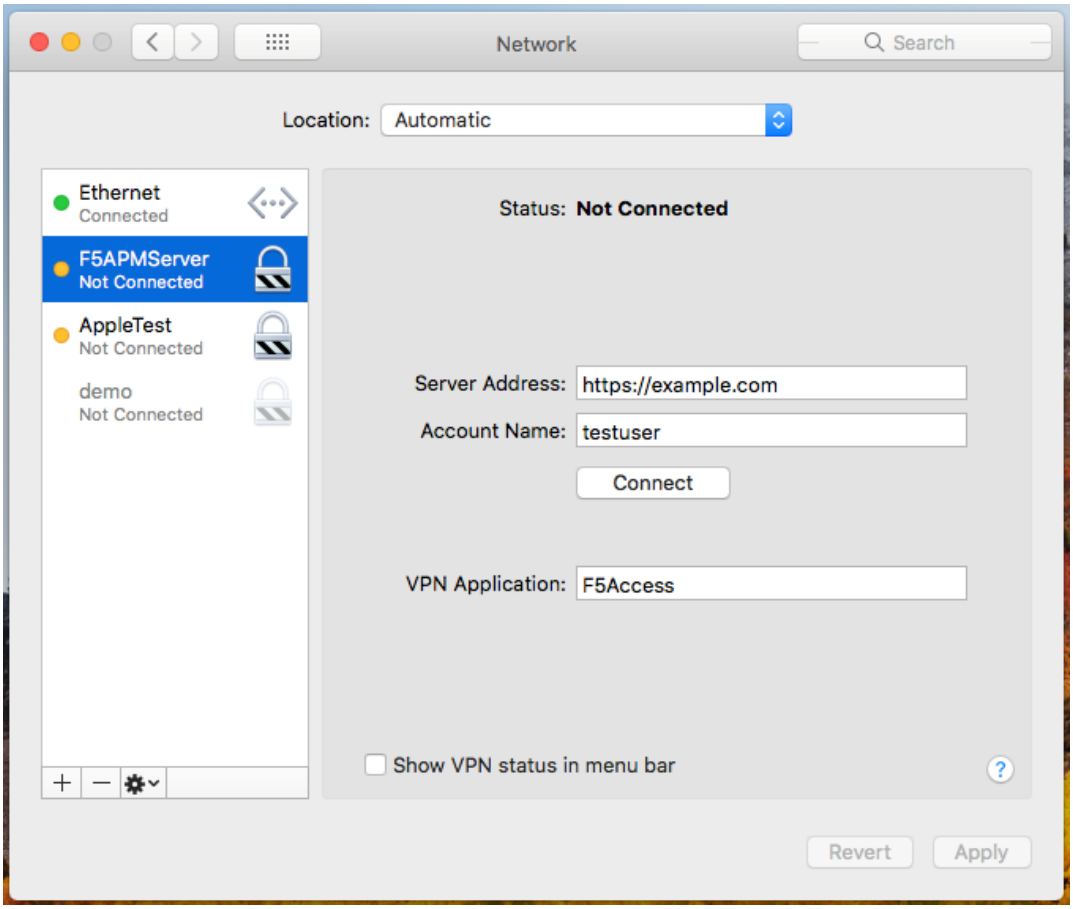
Starting a connection manually

Starting a connection on F5 Access for macOS requires a configured BIG-IP Network Access access policy to which you can connect. All configurations created from the Container app are also available in the **System Preference > Network** panel.

You start a connection to access network resources.

1. Log in to the macOS device and launch the F5 Access application from the Finder or the Launch Pad.
2. Start a connection by selecting an exisiting connection from the list.

3. You can also start a connection from the **System Preference > Network** panel.


Network
Search
Location: Automatic
Ethernet
Connected
F5APMServer
Not Connected
AppleTest
Not Connected
demo
Not Connected
Status: Not Connected
Server Address: https://example.com
Account Name: testuser
Connect
VPN Application: F5Access
Show VPN status in menu bar
Revert
Apply

Configuring Access Policy Manager for F5 Access

What does F5 Access do for macOS devices?

F5 Access for macOS provides full network access through BIG-IP® Access Policy Manager®. With network access, users can run applications such as RDP, SSH, Citrix, VMware View, and other enterprise applications on their macOS devices.

F5 Access features include:

- User name and password, and client certificate support
- Support for DNS address space for split-tunneling configurations
- Landing URI support
- Logging support to report issues
- Support client certificate for DTLS tunnels and SSL tunnels
- Per-app VPN support

About supported authentication types

F5 Access for macOS provides these authentication types:

Authentication type	Description
VPN On-Demand	Provides the following three options: • Username and password • Client certificate • Client certificate + username and password
Regular Logon	Provides the following three options: • Username and password • Client certificate • Client certificate + username and password
Per-App VPN	• Username and password • Client certificate • Username/password + client certificate

About establishing VPN connections

The F5 Access application (app) for macOS devices provides users with two options to establish a VPN tunnel connection. A user can start a tunnel connection explicitly with the F5 Access application, or implicitly through the VPN On-Demand functionality.

For example, a connection can be configured to automatically trigger whenever a certain domain or host name pattern is matched.

About pre-logon checks supported for macOS devices

For macOS devices, Access Policy Manager® can use only the following preconfigured pre-logon checks:

- Client Type - result is F5 Access
- Client OS - result is MacOS

Other session variables can be checked using custom expressions. See the list of session variables for macOS for more information.

Setting up network access

You can force traffic through a tunnel on F5 Access.

Note: *Although you disable* ***Allow local subnet access*** *while enabling* ***Force all traffic through tunnel****, the client still permits local subnet traffic to travel outside of the tunnel. This is a limitation of macOSand not of F5 Access.*

---

1. On the Main tab, click **Access Policy** > **Network Access** > **Network Access List**.
   The Network Access List screen opens.
2. Click the name to select a network access resource on the Resource List.
   The Network Access editing screen opens.
3. To configure the network settings for the network access resource, click **Network Settings** on the menu bar.
4. To optionally force all traffic through the tunnel, next to **Traffic Options**, enable **Force all traffic through tunnel**.

   If you enable **Use split tunneling for traffic**, you must also specify either a DNS suffix or DNS Address Space pattern to use the VPN DNS servers. If the "DNS Suffix" and "DNS Address Space" fields are both left blank, then F5 Access does not use the VPN DNS servers and sends all DNS traffic to public DNS servers.
5. To allow local subnet traffic to bypass the tunnel, select the **Enable** check box for **Allow Local Subnet**. This traffic bypasses the tunnel.
6. Click **Update**.

Prerequisites for configuring F5 Access

Before configuring F5 Access for macOS devices, you must complete the following requirements:

- Set up BIG-IP® Access Policy Manager®.
- Create a network access resource.
- Run the Network Access Setup Wizard.
- Create a connectivity profile.

Additional information about network access and connectivity profiles can be found in the *BIG-IP® Access Policy Manager®: Network Access Configuration* guide.

Access Policy Manager configuration for F5 Access for macOS devices

To configure F5 Access for mobile devices support on BIG-IP® Access Policy Manager®, use the following configuration steps:

- Run the Network Access Setup Wizard.
- Optionally, set up `SSO` and `ACLs` for your network access. Refer to the *BIG-IP® Access Policy Manager® Configuration Guide* on the AskF5™ Knowledge Base for instructions.
- Customize an access policy to support F5 Access.

Running the Network Access Setup wizard

Configure Access Policy Manager® to provide users with full network access from their mobile devices using the Network Access Setup wizard for remote access.

1. On the Main tab, click **Wizards** > **Device Wizards**.
   The Device Wizards screen opens.
2. For Access Policy Manager Configuration, select **Network Access Setup Wizard for Remote Access**, and then click **Next**.
3. Click **Finished**.

You now have network access resource that supports F5 Access for mobile devices.

Overview: Access Policies for F5 Access

About access policy branches for F5 Access

You can configure separate access policy branches for F5 Access.

F5 Access does not support client-side checks; however, you can configure an access policy that provides network access for macOS clients by using any of these methods:

- Create an access policy using **Client-Side Capability**. This provides a branch for clients that do not support client-side checks. Assign authentication and a network access resource to this branch.
- Use an existing access policy with client-side checks. The macOS client will fail to the fallback branch of the first client-side check. Assign authentication and a network access resource to this branch.
- Add a **Client OS** Access Policy item, and assign authentication and resources to the **macOS** branch.

F5 Access for macOS is detected with the following access policy items:

Access policy item	Value
Client Type	F5 Access
Client OS	MacOS

Configuring an access policy for F5 Access for macOS

Configure an access policy to identify and allow access to macOS devices.

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

   Note: *An access profile name must be unique among all access profile and any per-request policy names.*

4. From the **Profile Type** list, select **SSL-VPN**.
   Additional settings display.
5. From the **Profile Scope** list, retain the default value or select another.
   - **Profile**: Gives a user access only to resources that are behind the same access profile. This is the default value.
   - **Virtual Server**: Gives a user access only to resources that are behind the same virtual server.
   - **Global**: Gives a user access to resources behind any access profile that has global scope.
6. In the Language Settings area, add and remove accepted languages, and set the default language.

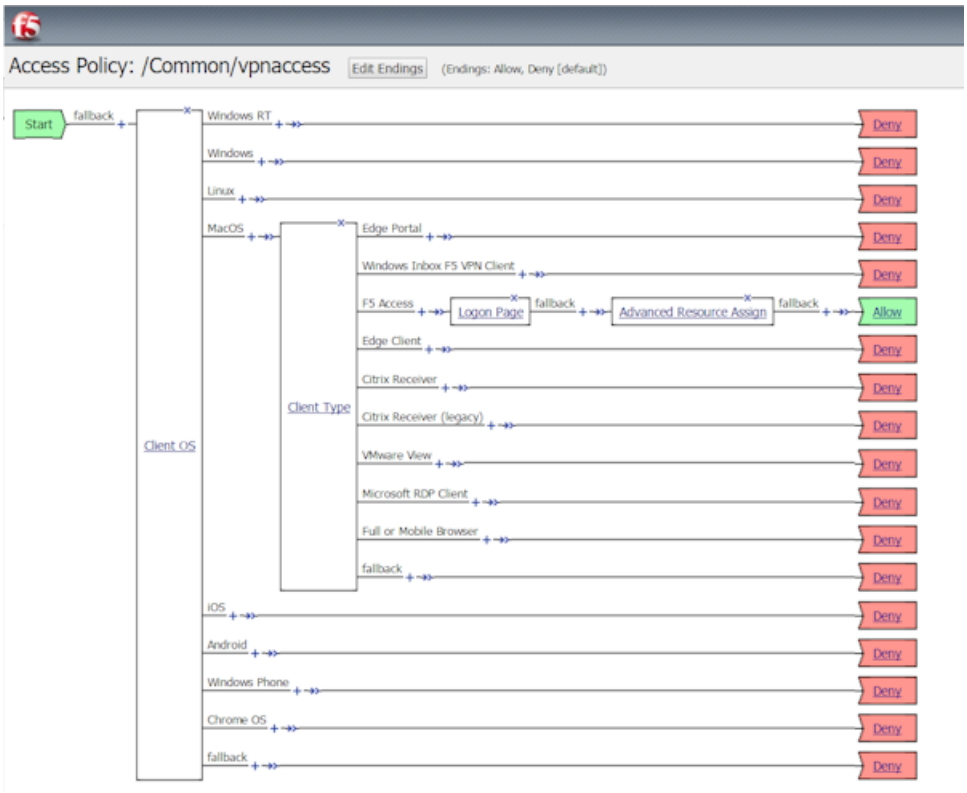
   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.

7. Click **Finished**.
8. Click the name of the access profile for which you want to edit the access policy.
   The properties screen opens for the profile you want to edit.
9. Click the **Access Policy** tab.
10. In the General Properties area, click the **Edit Access Policy for Profile** ***profile_name*** link.
    The visual policy editor opens the access policy in a separate screen.
11. Click **Add Item**.
    The screen is not active while the visual policy editor creates the action. The screen closes and a Properties screen displays.
12. Click the Endpoint Security (Server-Side) tab, and select Client OS.
13. Click **Add Item**.
    The screen is not active while the visual policy editor creates the action. The screen closes and a Properties screen displays.
14. Click **Save**.
15. On the MacOS branch, click **Add Item**.
16. Click the Endpoint Security (Server-Side) tab, and select Client Type.
17. Click **Save**.
18. On the F5 Access branch, add the authentication and resource actions you require. For example, add a Logon Page, Client Certificate, and Resource Assign actions.
19. When you have finished configuring the access policy, click **Apply Access Policy**.

Example of basic access policy that supports F5 Access

You can configure an access policy branch to direct macOS device users to F5 Access, and direct non-F5 Access device users to a fallback branch.

This example displays a simple access policy.


Access Policy: /Common/vpnaccess
Edit Endings
(Endings: Allow, Deny [default])
Start
fallback
Client OS
Windows RT
Windows
Linux
MacOS
Client Type
Edge Portal
Windows Inbox F5 VPN Client
F5 Access
Logon Page
fallback
Advanced Resource Assign
fallback
Allow
Edge Client
Citrix Receiver
Citrix Receiver (legacy)
VMware View
Microsoft RDP Client
Full or Mobile Browser
fallback
iOS
Android
Windows Phone
Chrome OS
fallback
Deny

Configuring Per-App VPN with APM and F5 Access

What is per-app VPN?

Apple's VPN framework supports application-level layer-3 tunneling for TCP and UDP connections. Apps can be configured to automatically connect to a VPN when they are started. Safari can be configured for per-app VPN with a configuration profile and without an MDM, and on a per-URL basis.

A per-app VPN configuration requires three configuration components.

- A device under MDM management or a configuration profile installed manually. For more information, see *macOS Sierra: Use configuration profiles*.
- F5 Access for macOS installed on the device.
- A per-app VPN profile, and a related F5 Access configuration (VPN). This is configured with an MDM command that associates the app with an F5 Access configuration, or manually on the macOS device.

About access policies for per-app VPN

Creating an access profile

You create an access profile to provide the secured connection between the per-app VPN and the virtual server.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.
4. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
5. Click **Finished**.

The access profile appears in the Access Profiles List.

About setting up Access Policy Manager for per-app VPN

- If there is routing required behind the BIG-IP® device, the SNAT Automap should be enabled.

Configuring a virtual server for per-app VPN

You must have Access Policy Manager® licensed and provisioned.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the Client SSL profile you previously created, and using the Move button, move the name to the **Selected** list.
4. From the **Source Address Translation** list, select **Auto Map**.
   The BIG-IP® system uses all of the self IP addresses as the translation addresses for the pool.
5. In the Access Policy area, from the **Access Profile** list, select the access profile.
6. From the **Connectivity Profile** list, select the connectivity profile.
7. Click **Update** to save the changes.

The virtual server is configured for per-app VPN.

About managing devices

With an MDM, you manage devices by enrolling them. Refer to your MDM documentation to enroll devices.

Important: *A user must enroll the device with the MDM in order for you to manage the device. However, you can deploy VPN configurations to the devices that aren't under management. F5 Access must be installed on the device to deploy configurations or manage the device. F5 Access can be installed either by the user, or deployed with the MDM solution.*

Creating a configuration profile for the managed device

A configuration profile enables the per-app VPN feature on a managed device, and specifies which apps use the VPN.

Create a configuration profile for the device.

Configuration profiles are described at the *Apple Configuration Profile Reference*.

Configure Access Policy Manager ®to provide the necessary support for per-app VPN features.

Per-App VPN configuration profile settings

Settings for the per-app VPN profile in an MDM.

Per-App VPN settings

The per-app VPN payload supports all of the keys described in the *Apple Configuration Profile Reference*. These keys, specific to the per-app VPN payload, are described in that reference as well.

Table 1: Per-App VPN specific keys

Key	Type	Description
VPNUUID	String	A globally-unique identifier for this VPN configuration. This identifier is used to configure apps so that they use the per-app VPN service for all of their network communication.
OnDemandMatchAppEnabled	Boolean	If **true**, the per-app VPN connection starts automatically when apps linked to this per-app VPN service initiate network communication. If **false**, the per-app VPN connection must be started manually by the user before apps linked to this per-app VPN service can initiate network communication. If this key is not present, the value of the OnDemandEnabled key is used to determine the status of per-app VPN On Demand.
SafariDomains	Array	This optional key is a special case of App-to-Per App VPN Mapping. It sets up the app mapping for Safari with a specific identifier and a designated requirement. The array contains strings, each of which is a domain that triggers a VPN connection in Safari. Do not specify a full URI; rule matching works only with the domain name. The rule matching behavior is as follows: • Before being matched against a host, all leading and trailing dots are stripped from the domain string. For example, if the domain string is "`.com`" the domain string used to match is "`com`". • Each label in the domain string must match an entire label in the host string. For example, a domain of "`example.com`" matches "`www.example.com`", but not "`old.badexample.com`". • Domain strings with only one label must match the entire host string. For example, a domain of "`com`" matches "`com`", not "`www.example.com`".

Example per-app VPN configuration profile

Includes a sample configuration profile for the per-app VPN configuration profile.

Per-App VPN configuration example profile

The following example uses sample data only. For your own configuration, items like the `PayloadDisplayName`, `Payload UUID`, and password and certificate information must be customized to your network and installation.

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE plist PUBLIC "-//Apple//DTD
PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>PayloadContent</key>
    <array>
      <dict>
        <key>IPv4</key>
        <dict>
          <key>OverridePrimary</key>
          <integer>0</integer>
        </dict>
        <key>PayloadDescription</key>
        <string>Configures VPN settings, including authentication.</string>
        <key>PayloadDisplayName</key>
        <string>VPN (Per-App VPN Test)</string>
        <key>PayloadIdentifier</key>
        <string>com.f5.mdm.perapp.vpn.vpn</string>
        <key>PayloadOrganization</key>
        <string/>
        <key>PayloadType</key>
        <string>com.apple.vpn.managed.applayer</string>
        <key>PayloadUUID</key>
        <string>5A015006-C440-4C5C-B197-737CF4DCFA96</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
        <key>Proxies</key>
        <dict/>
        <key>UserDefinedName</key>
        <string>Per-App VPN Test</string>
        <key>VPN</key>
        <dict>
          <key>AuthName</key>
          <string>test</string>
          <key>AuthPassword</key>
          <string>test</string>
          <key>AuthenticationMethod</key>
          <string>Certificate</string>
          <key>PayloadCertificateUUID</key>
          <string>C9BF4927-E819-4521-88DE-2AEB6E1DC3D8</string>
          <key>RemoteAddress</key>
          <string>https://example.f5.com</string>
          <key>OnDemandMatchAppEnabled</key>
          <true/>
          <key>ProviderType</key>
          <string>packet-tunnel</string>
          <key>ProviderBundleIdentifier</key>
          <string>com.f5.access.macos.PacketTunnel</string>
        </dict>
        <key>VPNSubType</key>
        <string>com.f5.access.macos</string>
        <key>VPNType</key>
        <string>VPN</string>
        <key>VendorConfig</key>
        <dict/>
        <key>SafariDomains</key>
        <array>
          <string>example.com</string>
          <string>main.example.com</string>
        </array>
        <key>VPNUUID</key>
        <string>CAB8510C-3F8A-4C51-6FBD-21A21D485C3C</string>
```

```
      </dict>
      <dict>
        <key>Password</key>
        <string>123456</string>
        <key>PayloadCertificateFileName</key>
        <string>identity.p12</string>
        <key>PayloadContent</key>
        <data>
            MIIL2QIBAzCCC58GCSqGSIb3DQEHAaCCC5AEgguMMIILiDCCBj8G
            CSqGSIb3DQEHBqCCBjAwggYsAgEAMIIGJQYJKoZIhvcNAQcBMBwG
            CiqGSIb3DQEMAQYwDgQIqckvWPHWFRUCAggAgIIF+N4kXpz9g4BB
            ... (etc...)
            </data>
        <key>PayloadDescription</key>
        <string>Provides device authentication (certificate or
identity).</string>
        <key>PayloadDisplayName</key>
        <string>identity.p12</string>
        <key>PayloadIdentifier</key>
        <string>com.f5.mdm.perapp.vpn.credential</string>
        <key>PayloadOrganization</key>
        <string/>
        <key>PayloadType</key>
        <string>com.apple.security.pkcs12</string>
        <key>PayloadUUID</key>
        <string>C9BF4927-E819-4521-88DE-2AEB6E1DC3D8</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
      </dict>
    </array>
    <key>PayloadDescription</key>
    <string>PerApp VPN Payload Test</string>
    <key>PayloadDisplayName</key>
    <string>MDM - Per-App VPN</string>
    <key>PayloadIdentifier</key>
    <string>com.f5.mdm.perapp.vpn</string>
    <key>PayloadOrganization</key>
    <string/>
    <key>PayloadRemovalDisallowed</key>
    <false/>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>06A850CC-BC81-43FB-AA16-42BE472D2421</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
  </dict>
</plist>
```

Additional Access Policy Manager Configuration Information

F5 Access for macOS session variables

The following table contains a list of session variables and their attributes.

Session variable	Description
session.client.type	Indicates the client type, for example `Standalone`.
session.client.activex	Indicates whether ActiveX is supported. The result is always `0` for macOS.
session.client.platform	Indicates the platform type, such as `MacOS`.
session.client.app_id	The app ID for the client. For F5 Access for macOS this is `f5_access`.
session.client.app_version	The app version for the client. For F5 Access for macOS 1.0.0 this is `1.0`.
session.client.model	Indicates the model number of the mobile device. For example, `MacBookPro10,1`
session.client.platform_version	Indicates the platform and version of the mobile device. For example, Version 10.12.6 (Build 16G29)
session.client.unique_id	Indicates the serial number of the device. For example, CA2DF1N6DLF3.
session.client.jailbreak	Indicates the jailbreak status of the device. `0` indicates the device is not jailbroken, `1` indicates the device is jailbroken, and an empty response indicates that the status of the device is unknown.
session.client.cpu	Indicates the client CPU type. For example, `ARM`.
session.client.biometric_fingerprint	Indicates whether the device supports biometric fingerprint authentication. This is always set to `0` on macOS.
session.client.vpn_scope	Indicates the scope of the VPN tunnel. The result is `device` for a device-wide VPN connection, and `per-app` for a per-app VPN.
session.client.vpn_tunnel_type	Indicates the type of VPN tunnel. For F5 Access for macOS, this is `L3`.
session.client.vpn_start_type	Indicates how the VPN connection was initiated. • `manual` - Indicates that the connection was initiated by the user. • `on-demand` - Indicates that the connection was initiated by Per-App VPN or an MDM.
session.client.version	Indicates the client protocol version. For macOS, the value is always `2.0`.
session.client.always_connected_mode	Indicates whether Always-On Mode is configured for the device. The result is always `0` for macOS.
session.client.hostname	This is the device host name (for example, `macos-system`).

Session variable	Description
session.client.js	Indicates whether the device used Web Logon mode. This is always set to `0` on macOS.

Index