BIG-IP® Access Policy Manager®: Edge Client® and Application Configuration

Version 7.1.6

Table of Contents

Overview: APM Clients

About the Network Access client component

The browser-based Network Access client component provides full network access through BIG-IP® Access Policy Manager®. The client component provides users with access to IP-based applications, network resources, and intranet files available, as if they were physically working on the office network.

About BIG-IP Edge Client

BIG-IP® Edge Client® provides full network access through BIG-IP Access Policy Manager®. Edge Client for Windows, Edge Client for Mac, and F5 Access for macOS provide clients with access to IP-based applications, network resources, and intranet files available, as if they were physically working on the office network. Edge Client software comprises individual components that provide network access features and application access.

In addition, Edge Client provides these features:

- Automatic reconnection
- Location awareness
- Password caching
- Captive portal detection
- Notifications

Uploading Desktop Client packages to the BIG-IP

Download a new client package from the downloads site at *https://downloads.f5.com*.

Install a new Desktop Client package to the BIG-IP to make the latest client components and installers available.

1. On the Main screen, click **System** > **Software Management** > **APM Clients**.
2. Click **Import**.
3. Next to Software Image, click **Choose File** and select the .iso file you downloaded.
4. Click **Import**.
   The new Desktop Client ISO file is imported.

About BIG-IP Edge and F5 Access Apps

BIG-IP® Edge and F5 Access Apps are available from external download sites and provide network access for supported mobile clients. Tech notes for each of the Edge and F5 Access Apps list the supported features for the mobile client and provide configuration tips. For Edge Apps documentation, refer to the AskF5™ Knowledge Base located at `http://support.f5.com/`.

About VPN connections from the command line

Access Policy Manager® (APM®) CLIs are available for Linux and Windows clients. The CLIs support making a VPN connection with an access policy that includes a Logon Page and any authentication types that require user name and password only. Endpoint security inspections are not supported.

The Linux CLI for Linux is available for download from the BIG-IP® system. The Windows CLI is installed with the BIG-IP Edge Client® for Windows.

Additional resources and documentation for BIG-IP Access Policy Manager

You can access all of the following BIG-IP® system documentation from the AskF5™ Knowledge Base located at `http://support.f5.com/`.

Document	Description
BIG-IP APM® Client Compatibility Matrix	This matrix specifies client compatibility across access and endpoint security features as well as browsers, operating systems, third-party products, and so on.
BIG-IP® APM® and F5 Access Apps technical notes	Client software technical notes provide information on obtaining, installing, and using F5 Access Apps for mobile clients.
F5 Access and BIG-IP Edge Apps Client Compatibility Matrix	This matrix specifies client compatibility across F5 Access Apps, Edge Apps, and Access Policy Manager.
BIG-IP® Access Policy Manager®: Application Access	This guide contains information for an administrator to configure application tunnels for secure, application-level TCP/IP connections from the client to the network.
BIG-IP® Access Policy Manager®: Authentication and Single-Sign On	This guide contains information to help an administrator configure APM for single sign-on and for various types of authentication, such as AAA server, SAML, certificate inspection, local user database, and so on.
BIG-IP® Access Policy Manager®: Customization	This guide provides information about using the APM customization tool to provide users with a personalized experience for access policy screens, and errors. An administrator can apply your organization's brand images and colors, change messages and errors for local languages, and change the layout of user pages and screens.
BIG-IP® Access Policy Manager®: Edge Client and Application Configuration	This guide contains information for an administrator to configure the BIG-IP® system for browser-based access with the web client as well as for access using BIG-IP Edge Client® and BIG-IP Edge Apps. It also includes information about how to configure or obtain client packages and install them for BIG-IP Edge Client for Windows, Mac, and Linux, and Edge Client command-line interface for Linux.
BIG-IP® Access Policy Manager®: Implementations	This guide contains implementations for synchronizing access policies across BIG-IP systems, hosting content on a BIG-IP system, maintaining OPSWAT libraries, configuring dynamic ACLs, web access management, and configuring an access policy for routing.

Document	Description
BIG-IP® Access Policy Manager®: Network Access	This guide contains information for an administrator to configure APM Network Access to provide secure access to corporate applications and data using a standard web browser.
BIG-IP® Access Policy Manager®: Portal Access	This guide contains information about how to configure APM Portal Access. In Portal Access, APM communicates with back-end servers, rewrites links in application web pages, and directs additional requests from clients back to APM.
BIG-IP® Access Policy Manager®: Secure Web Gateway	This guide contains information to help an administrator configure Secure Web Gateway (SWG) explicit or transparent forward proxy and apply URL categorization and filtering to Internet traffic from your enterprise.
BIG-IP® Access Policy Manager®: Third-Party Integration	This guide contains information about integrating third-party products with Access Policy Manager (APM®). It includes implementations for integration with VMware Horizon View, Oracle Access Manager, Citrix Web Interface site, and so on.
BIG-IP® Access Policy Manager®: Visual Policy Editor	This guide contains information about how to use the visual policy editor to configure access policies.
Release notes	Release notes contain information about the current software release, including a list of associated documentation, a summary of new features, enhancements, fixes, known issues, and available workarounds.
Solutions and Tech Notes	Solutions are responses and resolutions to known issues. Tech Notes provide additional configuration instructions and how-to information.

BIG-IP Edge Client for Windows

About Component Installer

The Component Installer service enables you to install and upgrade client-side Access Policy Manager® (APM®) components on Windows-based clients for all kinds of user accounts, regardless of the rights under which the user is working. This component is especially useful for installing and upgrading client-side components when the user has insufficient rights to install or upgrade the components directly.

After you install the Component Installer, it automatically installs and upgrades client-side APM components. It can also update itself. The Component Installer requires that installation or upgrade packages be signed using the F5® Networks certificate or another trusted certificate. By default, F5 Networks signs all components using the F5 Networks certificate.

Downloading and installing the Component Installer

You can pre-install client components for your users who do not have administrative privileges on Windows-based systems.

1. On the Main screen, click the F5® logo to display the Welcome page.
2. Scroll to the Downloads area.
3. In the links for BIG-IP® Edge Client® Components, click **Component Installer Package for Windows**.
   The MSI installer downloads to your local folder.
4. On Windows-based clients, install the Component Installer with elevated privileges so that it can install, upgrade, and run APM® components that require elevated privileges.

   For information about configuring the MSI installer to run with elevated privileges, see the documentation for your operating system.

Overview: Configuring and installing Edge Client for Windows

Users of BIG-IP® Edge Client®for Windows can connect securely and automatically to your network while roaming using the automatic reconnect, password caching, and location awareness features of Edge Client. You can also enforce Always Connected mode, and configure the list of trusted sites to which to allow access. You can customize the client package and you must download it and make it available to users as hosted content on the BIG-IP system or through another delivery mechanism. Users must install the package, or Component Installer, if available on the client, can install it for them.

Task summary

About Machine Cert Auth and user privilege

A Machine Cert Auth check requires administrative privilege. The Windows client package associated with a connectivity profile can be configured to include a Machine Certificate Checker Service component. The service can check the machine certificate on a client endpoint even when the user does not have admin privilege. The option to include this component in the package is disabled by default.

About Edge Client location awareness

The BIG-IP® Edge Client® provides a location-awareness feature. Using location awareness, the client connects automatically only when it is not on a specified network. The administrator specifies the networks that are considered in-network, by adding DNS suffixes to the connectivity profile. With a location-aware client enabled, a user with a corporate laptop can go from a corporate office, with a secured wireless or wired network connection, to an offsite location with a public wireless network connection, and maintain a seamless connection to allowed corporate resources.

About Edge Client automatic reconnection

BIG-IP®Edge Client® provides an automatic reconnection feature. This feature attempts to automatically reconnect the client system to corporate network resources whenever the client connection drops or ends prematurely.

About Always Connected mode

BIG-IP®Edge Client® provides Always Connected mode. This feature allows you to specify that the client is always connected to the VPN, and allows you to configure the behavior when the client is not connected. You can specify whether the client is connected automatically after Windows logon, and configure exclusion addresses.

Configuring a connectivity profile for Edge Client for Windows

Update the connectivity profile in your Network Access configuration to configure security settings, servers, and location-awareness for BIG-IP® Edge Client® for Windows.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From the left pane of the popup screen, select **Win/Mac Edge Client**.
   Edge Client settings for Mac and Windows-based systems display in the right pane.
4. Set Edge Client action settings:
   a) Retain the default (selected) or clear the **Save Servers Upon Exit** check box.

      Specifies whether Edge Client maintains a list of recently used user-entered APM® servers. Edge Client always lists the servers that are defined in the connectivity profile, and sorts them by most recent access, whether this option is selected or not.
   b) To enable the client to try to use the Windows logon session for an APM session also, select the **Reuse Windows Logon Session** check box.

      This is cleared by default.
   c) To enable the client to try to use the credentials that they typed for Windows logon in an APM session also, select the **Reuse Windows Logon Credentials** check box.

      This is cleared by default.

      Note: *To support this option, you must also include the* ***User Logon Credentials Access Service*** *in the Windows client package for this connectivity profile and you must ensure that the access policy includes an uncustomized* ***Logon Page*** *action.*

      ---
5. To support automatic reconnection without the need to provide credentials again, allow password caching.

a) Select the **Allow Password Caching** check box.

This check box is cleared by default.

The remaining settings on the screen become available.

b) To require device authentication to unlock the saved password, select **Require Device Authentication.**

This option links the option to use a saved password to a device authentication method. Supported device authentication methods include PIN, passphrase, and biometric (fingerprint) authentication on iOS and Android. Android devices also support pattern unlocking.

c) From the **Save Password Method** list, select **disk** or **memory**.

If you select **disk**, Edge Client caches the user's password (in encrypted form) securely on the disk where it is persisted even after the system is restarted or Edge Client is restarted.

If you select **memory**, Edge Client caches the user's password within the BIG-IP Edge Client application for automatic reconnection purposes.

If you select **memory**, the **Password Cache Expiration (minutes)** field displays with a default value of 240.

d) If the **Password Cache Expiration (minutes)** field displays, retain the default value or type the number of minutes to save the password in memory.

6. To enable automatic download and update of client packages, from the **Component Update** list, select **yes** (default).

If you select **yes**, APM® updates Edge Client software automatically on the client system when newer versions are available. This option applies to updates for theses components only: BIG-IP Edge Client, component installer service, DNS relay proxy service, and user logon credentials access service.

7. Specify DNS suffixes that are considered to be in the local network.

Providing a list of DNS suffixes for the download package enables Edge Client to support the autoconnect option. With **Auto-Connect** selected, Edge Client uses the DNS suffixes to automatically connect when a client is not on the local network (not on the list) and automatically disconnect when the client is on the local network.

a) From the left pane of the popup screen, select **Location DNS List**.
Location DNS list information is displayed in the right pane.

b) Click **Add**.
An update row becomes available.

c) Type a name and click **Update**.

Type a DNS suffix that conforms to the rules specified for the local network.

The new row displays at the top of the table.

d) Continue to add DNS names and when you are done, click **OK**.

8. Click **OK**.
The popup screen closes, and the Connectivity Profile List displays.

Configuring Always Connected mode for the Windows Edge Client

Update the connectivity profile in your Network Access configuration to configure Always Connected mode.

1. On the Main tab, click **Access** > **Connectivity/VPN** > **Connectivity** > **Profiles**.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From the left pane of the popup screen, select **Win/Mac Edge Client**.
Edge Client settings for Mac and Windows-based systems display in the right pane.
4. Set Edge Client action settings:

a) Retain the default (selected) or clear the **Save Servers Upon Exit** check box.

Specifies whether Edge Client maintains a list of recently used user-entered APM® servers. Edge Client always lists the servers that are defined in the connectivity profile, and sorts them by most recent access, whether this option is selected or not.

b) To enable the client to try to use the Windows logon session for an APM session also, select the **Reuse Windows Logon Session** check box.

This is cleared by default.

c) To enable the client to try to use the credentials that they typed for Windows logon in an APM session also, select the **Reuse Windows Logon Credentials** check box.

This is cleared by default.

Note: *To support this option, you must also include the* ***User Logon Credentials Access Service*** *in the Windows client package for this connectivity profile and you must ensure that the access policy includes an uncustomized* ***Logon Page*** *action.*

---

5. To support automatic reconnection without the need to provide credentials again, allow password caching.

a) Select the **Allow Password Caching** check box.

This check box is cleared by default.

The remaining settings on the screen become available.

b) From the **Save Password Method** list, select **disk** or **memory**.

If you select **disk**, Edge Client caches the user's password (in encrypted form) securely on the disk where it is persisted even after the system is restarted or Edge Client is restarted.

If you select **memory**, Edge Client caches the user's password within the BIG-IP Edge Client application for automatic reconnection purposes.

If you select **memory**, the **Password Cache Expiration (minutes)** field displays with a default value of 240.

c) If the **Password Cache Expiration (minutes)** field displays, retain the default value or type the number of minutes to save the password in memory.

6. To enable automatic download and update of client packages, from the **Component Update** list, select **yes** (default).

If you select **yes**, APM® updates Edge Client software automatically on the client system when newer versions are available. This option applies to updates for theses components only: BIG-IP Edge Client, component installer service, DNS relay proxy service, and user logon credentials access service.

7. Specify DNS suffixes that are considered to be in the local network.

Providing a list of DNS suffixes for the download package enables Edge Client to support the autoconnect option. With **Auto-Connect** selected, Edge Client uses the DNS suffixes to automatically connect when a client is not on the local network (not on the list) and automatically disconnect when the client is on the local network.

a) From the left pane of the popup screen, select **Location DNS List**.
Location DNS list information is displayed in the right pane.

b) Click **Add**.
An update row becomes available.

c) Type a name and click **Update**.

Type a DNS suffix that conforms to the rules specified for the local network.

The new row displays at the top of the table.

d) Continue to add DNS names and when you are done, click **OK**.

8. Click **OK**.
The popup screen closes, and the Connectivity Profile List displays.

Customizing a downloadable client package for Windows

Customize a Windows client package to specify the client components to install, and to customize settings for BIG-IP® Edge Client® and Dialup Settings components if you include them.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select a connectivity profile.
3. Click the **Customize Package** button.
   The Customize Windows Client Package popup screen displays with Available Components displayed.
4. Make sure that only the components that you want to include in the package are selected.
5. To include the software service that allows the client to store encrypted Windows logon credentials and use those credentials to log on to APM®, select the **User Logon Credentials Access Service** check box.

   Note: *For clients to use the service, you must also select the* ***Reuse Windows Logon Credentials*** *check box in the connectivity profile.*

   ---

6. To include a service that can check the machine certificate on a client endpoint even when the user does not have admin privilege, select the **Machine Certificate Checker Service** check box.

   Without this service, a user running without admin privilege cannot pass the Machine Cert Auth endpoint security check.
7. If the **BIG-IP Edge Client** check box is selected, from the left pane select **BIG-IP Edge Client**.

   BIG-IP Edge Client settings display in the right pane.

   a) To add the virtual servers that are defined in the Windows/Mac Edge Client settings of the connectivity profile to the Windows Trusted sites list the first time the client starts, retain selection of the **Add virtual server to trusted sites list** check box. Otherwise, clear it.

      Virtual servers added to the Trusted sites list with this option remain on the trusted sites list indefinitely. This works with the **User Logon Credentials Access Service** setting (available on the Available Components screen) to provide seamless logon with Edge Client if APM accepts the same credentials that users use to log on to Windows.

   b) To automatically start the Edge Client after the user logs on to Windows, retain selection of the **Auto launch after Windows Logon** check box. Otherwise, clear it.

   c) To enable the Edge Client to try to connect to VPN right after the user logs on to Windows and to prohibit the user from disconnecting VPN, select the **Enable always connected mode** check box. This setting is cleared by default.

      The user is prevented from accessing the Internet and the local network until a VPN connection is established.
8. To customize Dialup Settings (if selected on the Available Components screen), from the left pane select **Dialup Settings**.
   Dialup Entry / Windows Logon Integration settings display in the right pane.
9. With **Dialup Settings** selected, you can specify how you want the user to authenticate to APM.

   Note: *Users must always type a user name and password to log on to Windows. Subsequently, clients authenticate to APM.*

   - If you want the access policy to run and display a screen where the user must click **Logon**, select the **Enforce Access Policy in Custom Dialer** check box and clear the **Prompt Username and Password** check box. (With these settings, username and password fields are prefilled and the access policy runs.)

- If you want the user to view a logon prompt and click **Connect**, clear the **Enforce Access Policy in Custom Dialer** check box and select the **Prompt Username and Password** check box. (With these settings, username and password fields are prefilled and the access policy does not run.)
- If you do not want the user to do anything to authenticate to APM, clear the **Enforce Access Policy in Custom Dialer** and **Prompt Username and Password** check boxes. (With these settings, the access policy does not run and the logon prompt is suppressed.)

10. Click **Download**.

    The screen closes and the package, `BIGIPEdgeClient.exe`, downloads.

The customized package, `BIGIPEdgeClient.exe`, is downloaded to your client. It is available for you to distribute.

Downloading the client package for Windows

You can download a Windows client package and distribute it to clients.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select a connectivity profile.
3. Click the **Customize Package** button.
   The Customize Windows Client Package popup screen displays with Available Components displayed.
4. Click **Download**.

   The screen closes and the package, `BIGIPEdgeClient.exe`, downloads.

The customized package, `BIGIPEdgeClient.exe`, is downloaded to your client. It is available for you to distribute. Users must install the package, or, if Component Installer is available on the client, it can install the package for the user.

About Network Access features for Windows-based clients

Access Policy Manager® (APM®) supports all Network Access features with BIG-IP® Edge Client® for Windows. For a complete list of Network Access features, refer to *BIG-IP® Access Policy Manager®: Network Access* on AskF5™ at `http://support.f5.com/`. For notes about endpoint security features, refer to *BIG-IP® APM® Client Compatibility Matrix* on AskF5™ at `http://support.f5.com/`.

About connection options on Edge Client for Windows

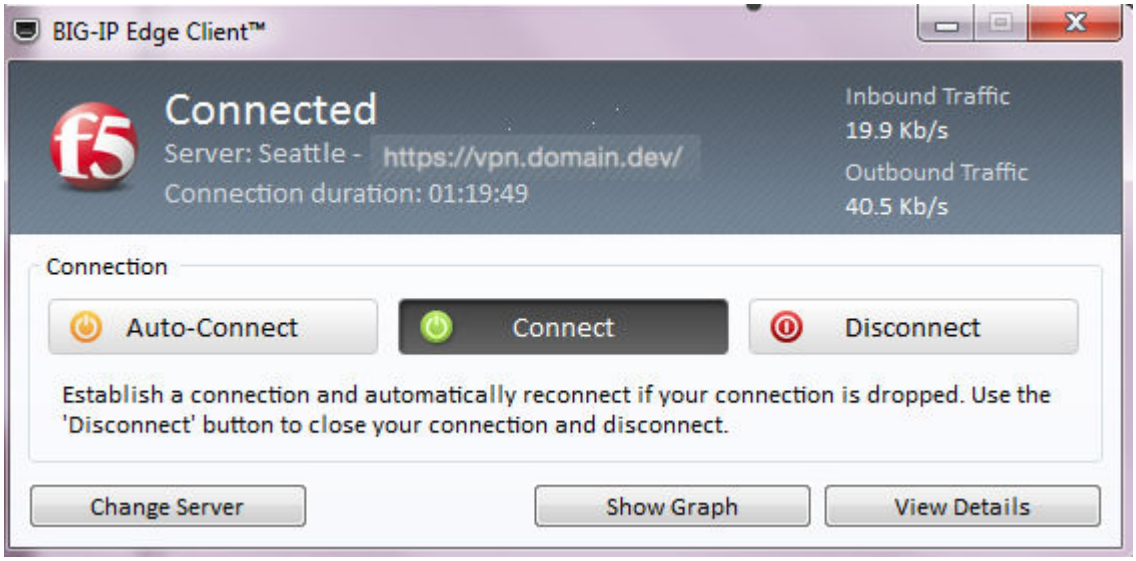


Figure 1: User interface on a Windows-based system

BIG-IP® Edge Client® for Windows user interface displays these connection options.

Auto-Connect
Starts a secure access connection as it is needed. This option uses the DNS suffix information defined in the connectivity profile to determine when the computer is on a defined local network. When the computer is not on a defined local network, the secure access connection starts. When the computer is on a local network, the client disconnects, but remains active in the system tray. This option does not display if DNS suffixes were not defined.

Connect
Starts and maintains a secure access connection at all times, regardless of the network location.

Disconnect
Stops an active secure access connection, and prevents the client from connecting again until a user clicks **Connect** or **Auto-Connect**.

About browser-based connections from Linux, Mac, and Windows clients

For Linux, Mac OS X, and Windows-based systems, the Network Access client component is available for automatic download from the BIG-IP® system.

Note: *The client component supports secure remote web-based access to the network. It is not the same as the customizable client package that is associated with the connectivity profile.*

The first time a remote user starts Network Access, APM® downloads a client component. This client component is designed to be self-installing and self-configuring. If the browser does not meet certain requirements, APM prompts the user to download the client component and install it manually.

Generating a troubleshooting report from Edge Client for Windows

A troubleshooting report provides numerous details about the client and its functioning, such as log files and their contents, components and versions, and so on.

1. Open the BIG-IP® Edge Client® user interface.

   On a client with a **Start** button, you can type **BIG-IP** in the search field and, in the results, click **BIG-IP Edge Client**.
2. Click the **View Details** button.
   The Details popup screen displays.
3. Click the **Diagnostics Report** button.
   A Save As popup screen opens.
4. Select a location, specify a file name, and click **Save**.
   A Collecting data popup screen remains open until the report completes.
5. Navigate to the location with the downloaded file, extract the files to a folder, and click the HTML file in the folder.
   The F5 Report displays in a browser screen.
6. Open the BIG-IP® Edge Client® user interface.

   On a client with a **Start** button, you can type **BIG-IP** in the search field and, in the results, click **BIG-IP Edge Client**.
7. Click the **View Details** button.
   The Details popup screen displays.
8. Click the **Diagnostics Report** button.
   A Save As popup screen opens.
9. Select a location, specify a file name, and click **Save**.
   A Collecting data popup screen remains open until the report completes.
10. Navigate to the location with the downloaded file, unzip it to a folder, and click the HTML file in the folder.
    The report displays.

Overview: Installing and using the client troubleshooting utility

Access Policy Manager® provides a client troubleshooting utility for Windows-based systems. Users can access the utility to check the availability and version information for Windows client components, and run Network Access diagnostic tests. The utility is integrated into BIG-IP® Edge Client® for Windows. To run Network Access diagnostics and troubleshooting reports on clients that have only the browser-based Network Access client component, you can download and install the client troubleshooting utility.

Task summary

Downloading the client troubleshooting utility

To run the client troubleshooting utility from the command line on a Windows-based system, you must first download the utility from the BIG-IP® system.

1. On the Main screen, click the F5® logo to display the Welcome page.
2. Scroll to the Downloads area.

3. In the links for BIG-IP® Edge Client® Components, click **Client Troubleshooting Utility for Windows**.

The file `f5wininfo.exe` is saved to your local disk.

Viewing client components in the client troubleshooting utility

You can use the client troubleshooting utility to view client components on Windows-based systems.

1. Double-click `f5wininfo.exe` to start the client troubleshooting utility.
   The F5® BIG-IP® Edge Components Troubleshooting screen opens.
2. Use the navigation panel on the left to explore the component categories.

Generating a client troubleshooting report

You can generate a client troubleshooting report on Windows-based systems and include several types of data, a Network Access diagnostic test and so on, in the report.

1. Double-click `f5wininfo.exe` to start the client troubleshooting utility.
   The F5 BIG-IP® Edge Components Troubleshooting screen opens.
2. Click **File** > **Generate Report**.
   The Report screen opens.
3. Under **Type**, select the types of reports that you want to run.
4. Under **Format**, select **html** or **text** for the type of report.
5. To generate a compressed report, select the **compressed** option.
6. To view the report without saving the report, click **View**.
   While the report runs, a Collecting Data popup screen opens and a System Information popup screen opens if the system information report type runs; the popup screens close. If you selected **html** format, the report opens in a browser screen.

Running a Network Access diagnostic test

You can use the client troubleshooting utility to run a Network Access diagnostic test on Windows-based systems.

Note: *If BIG-IP® Edge Client® for Windows is installed, you can run a Network Diagnostics test from the user interface.*

---

1. Double-click `f5wininfo.exe` to start the client troubleshooting utility.
   The F5® BIG-IP® Edge Components Troubleshooting screen opens.
2. Click **Tools** > **Network Access Diagnostic**.
   The Network Access Diagnostic popup screen opens.

Overview: Reusing Windows logon credentials for Edge Client

If you want users of BIG-IP® Edge Client® for Windows to start a Network Access session with the credentials that they typed to log on to a Windows-based system, you must configure the connectivity profile, the client download package, and the access policy to support this.

Important: *A client must be joined to a domain to reuse Windows logon credentials. This will not work if the client is standalone, and not joined to a domain.*

Task summary

Configuring a connectivity profile to reuse Windows logon credentials

For users to reuse Windows credentials to start a Network Access session, you must select the **Reuse Windows Logon Credentials** check box in the connectivity profile.

Important: *A client must be joined to a domain to reuse Windows logon credentials. This will not work if the client is standalone, and not joined to a domain.*

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From the left pane of the popup screen, select **Win/Mac Edge Client**.
   Edge Client settings for Mac and Windows-based systems display in the right pane.
4. Select the **Reuse Windows Logon Credentials** check box.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

Customizing the Edge Client package for Windows logon credentials reuse

For users to reuse their Windows credentials to start a Network Access session, the Edge Client® package must contain the user logon credentials access service.

Important: *A client must be joined to a domain to reuse Windows logon credentials. This will not work if the client is standalone, and not joined to a domain.*

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select the connectivity profile for which you want to customize the client package.
3. Click the **Customize Package** button.
   The Customize Windows Client Package popup screen displays with Available Components displayed.
4. Select the **User Logon Credentials Access Service** check box.

   This software service allows the client to store encrypted Windows logon credentials and use those credentials to log on to Access Policy Manager®.
5. Click **Download**.

   The screen closes and the package, `BIGIPEdgeClient.exe`, downloads.

You must make the downloaded package available to your users, as hosted content or through some other delivery mechanism. Users must install the package or, Component Installer, if present on user systems, can install it for them.

Configuring an access policy for Windows logon credentials reuse

For users to reuse Windows credentials to start a Network Access session, you must ensure that the access policy includes a Logon Page action that has not been customized.

Important: *A client must be joined to a domain to reuse Windows logon credentials. This will not work if the client is standalone, and not joined to a domain.*

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. In the Per-Session Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Make any adjustments needed to the access policy to ensure that it includes a Logon Page action that has not been customized. (Other logon page actions do not support the reuse Windows logon credentials option.)

   Note: *The Logon Page action must contain only the default fields and the JavaScript cannot be removed or otherwise changed as can be done through Access Policy Manager® Customization. If necessary, you can delete a Logon Page action and add it to the policy again to ensure that it is not customized.*

   ---

4. Click **Finished**.
   The popup screen closes.
5. Click the **Apply Access Policy** link to apply and activate the changes to the policy.

BIG-IP Edge Client and F5 Access for macOS

Requirements for client installation and use on Mac

The table lists requirements for installing and using client components on a macOS system. These requirements apply to the Network Access client component that is downloaded from the browser and to BIG-IP® Edge Client® for Mac and F5 Access for macOS.

Requirement	Specification
Browser	For App Tunnels to work, the browser must have Java enabled. For installation, Java is optional. The client uses Java to streamline the installation process only. Without Java, users can manually download and install the client packages. ***Note:*** *Java App Tunnels are supported on Edge Client only.*
Installation privilege	The remote user must have superuser authority, or, must be able to supply an administrative password to successfully install the Network Access client.

About browser-based connections from Linux, Mac, and Windows clients

For Linux, Mac OS X, and Windows-based systems, the Network Access client component is available for automatic download from the BIG-IP® system.

Note: *The client component supports secure remote web-based access to the network. It is not the same as the customizable client package that is associated with the connectivity profile.*

The first time a remote user starts Network Access, APM® downloads a client component. This client component is designed to be self-installing and self-configuring. If the browser does not meet certain requirements, APM prompts the user to download the client component and install it manually.

Overview: Configuring and installing Edge Client for Mac

Users of BIG-IP® Edge Client® for Mac can connect securely and automatically to your network while roaming using the automatic reconnect, password caching, and location awareness features of Edge Client. You can customize the client package; you must download it and make it available to users as hosted content on the BIG-IP system, or through another delivery mechanism.

Task summary

About Edge Client location awareness

The BIG-IP® Edge Client® provides a location-awareness feature. Using location awareness, the client connects automatically only when it is not on a specified network. The administrator specifies the

networks that are considered in-network, by adding DNS suffixes to the connectivity profile. With a location-aware client enabled, a user with a corporate laptop can go from a corporate office, with a secured wireless or wired network connection, to an offsite location with a public wireless network connection, and maintain a seamless connection to allowed corporate resources.

About Edge Client automatic reconnection

BIG-IP® Edge Client® provides an automatic reconnection feature. This feature attempts to automatically reconnect the client system to corporate network resources whenever the client connection drops or ends prematurely.

Configuring a connectivity profile for Edge Client for Mac

Update the connectivity profile in your Network Access configuration to configure security settings, servers, and location-awareness for BIG-IP® Edge Client® for Mac.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From the left pane of the popup screen, select **Win/Mac Edge Client**.
   Edge Client settings for Mac and Windows-based systems display in the right pane.
4. Retain the default (selected) or clear the **Save Servers Upon Exit** check box.

   Specifies whether Edge Client maintains a list of recently used user-entered APM® servers. Edge Client always lists the servers that are defined in the connectivity profile, and sorts them by most recent access, whether this option is selected or not.
5. To support automatic reconnection without the need to provide credentials again, allow password caching.
   a) Select the **Allow Password Caching** check box.

      This check box is cleared by default.

      The remaining settings on the screen become available.
   b) To require device authentication to unlock the saved password, select **Require Device Authentication.**

      This option links the option to use a saved password to a device authentication method. Supported device authentication methods include PIN, passphrase, and biometric (fingerprint) authentication on iOS and Android. Android devices also support pattern unlocking.
   c) From the **Save Password Method** list, select **disk** or **memory**.

      If you select **disk**, Edge Client caches the user's password (in encrypted form) securely on the disk where it is persisted even after the system is restarted or Edge Client is restarted.

      If you select **memory**, Edge Client caches the user's password within the BIG-IP Edge Client application for automatic reconnection purposes.

      If you select **memory**, the **Password Cache Expiration (minutes)** field displays with a default value of 240.
   d) If the **Password Cache Expiration (minutes)** field displays, retain the default value or type the number of minutes to save the password in memory.
6. To enable automatic download and update of client packages, from the **Component Update** list, select **yes** (default).

   If you select **yes**, APM® updates Edge Client software automatically on the client system when newer versions are available.
7. Specify the list of APM servers to provide when the client connects.

   The servers you add here display as connection options in the BIG-IP Edge Client.

Note: *Users can select from these servers or they can type a hostname.*

a) From the left pane of the popup screen, select **Server List**.
A table displays in the right pane.
b) Click **Add**.
A table row becomes available for update.
c) You must type a host name in the **Host Name** field.
Typing an alias in the **Alias** field is optional.
d) Click **Update**.
The new row is added at the top of the table.
e) Continue to add servers, and when you are done, click **OK**.

8. Specify DNS suffixes that are considered to be in the local network.
Providing a list of DNS suffixes for the download package enables Edge Client to support the autoconnect option. With **Auto-Connect** selected, Edge Client uses the DNS suffixes to automatically connect when a client is not on the local network (not on the list) and automatically disconnect when the client is on the local network.
a) From the left pane of the popup screen, select **Location DNS List**.
Location DNS list information is displayed in the right pane.
b) Click **Add**.
An update row becomes available.
c) Type a name and click **Update**.
Type a DNS suffix that conforms to the rules specified for the local network.
The new row displays at the top of the table.
d) Continue to add DNS names and when you are done, click **OK**.
9. Click **OK**.
The popup screen closes, and the Connectivity Profile List displays.

Customizing a downloadable client package for Mac

Customize a Mac client package for a connectivity profile to specify whether to launch BIG-IP® Edge Client® after a user logs in to the Mac.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
A list of connectivity profiles displays.
2. Select a connectivity profile.
3. Click the arrow on the **Customize Package** button and select **Mac**.
The Customize Mac Client Package screen displays.
4. Retain the selection or clear the **Auto launch BIG-IP Edge Client after User Log In** check box.
5. Click Download.
The customized package, `BIGIPMacEdgeClient.zip`, is downloaded to your client. It is available for you to distribute.

If you plan to distribute Mac client packages to your users and you customize multiple Mac client packages (for different connectivity profiles), you need to rename or otherwise organize the packages. Otherwise, your download location contains packages named `BIGIPMacEdgeClient.zip`, `BIGIPMacEdgeClient.zip(1)`, and so on.

Downloading the ZIP file for Edge Client for Mac

You can download a Mac Client package and distribute it to clients.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.

A list of connectivity profiles displays.

2. Select a connectivity profile.
3. Click the arrow on the **Customize Package** button and select **Mac**.
   The Customize Mac Client Package screen displays.
4. Click **Download**.

   The screen closes and the package, `BIGIPMacEdgeClient.zip`, downloads.

The ZIP file includes a Mac installer package (PKG) file and configuration settings.

Distribute the entire ZIP file to your users.

Specifying applications to start on a Mac

The launch application feature specifies a client application that starts when the client begins a Network Access session. You can use this feature when you have remote clients who routinely use Network Access to connect to an application server, such as a mail server.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Network Access (VPN)** > **Network Access Lists**.
   The Network Access Lists screen opens.
2. In the Name column, click the name of the network access resource you want to edit.
3. To configure applications to start for clients that establish a Network Access connection with this resource, click **Launch Applications** on the menu bar.
4. Click **Add** to add an application list.
5. In the **Application Path** field, type `open` .
6. In the **Parameters** field, type a parameter.
   For example, type `-a/Applications/ie.app http://www.f5.com`.
7. From the **Operating System** list, select **Mac**.
8. Click **Finished** to add the configuration.

Now when remote users with assigned resources make a Network Access connection, the application you configured starts automatically.

Editing the log level for Edge Client on Mac

You can edit log settings in the configuration file on Mac systems.

1. In the `~/Library/F5Networks.` directory, open the `f5networks.conf` file.
2. Edit the settings to change the log level.

   For debugging purposes, set the values to 48.

About connection options on Edge Client for Mac

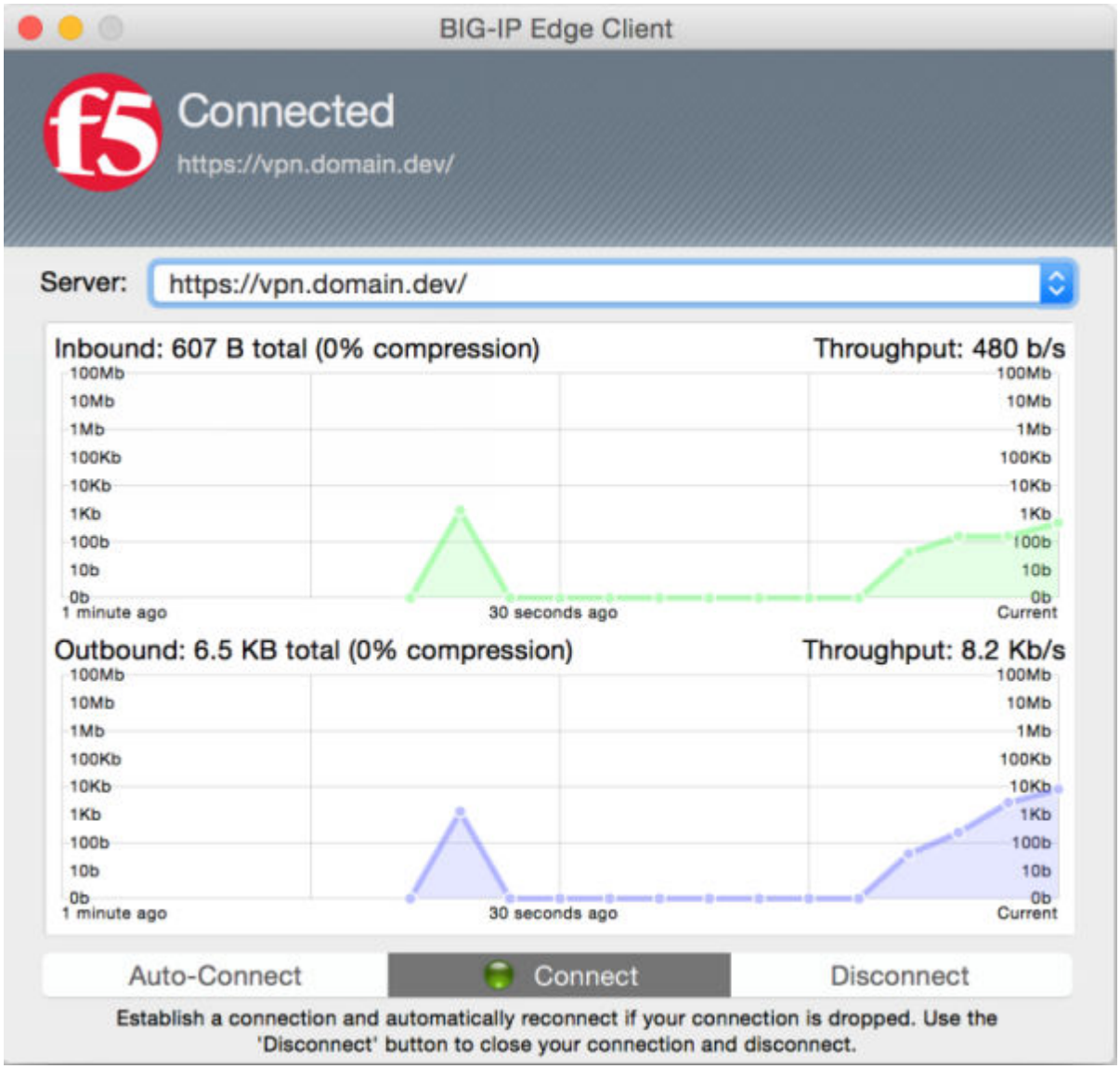


Figure 2: User interface on a Mac

BIG-IP® Edge Client® for Mac user interface displays these connection options.

Auto-Connect
Starts a secure access connection as it is needed. This option uses the DNS suffix information defined in the connectivity profile to determine when the computer is on a defined local network. When the computer is not on a defined local network, the secure access connection starts. When the computer is on a local network, the client disconnects, but remains active in the system tray. This option does not display if DNS suffixes were not defined.

Connect
Starts and maintains a secure access connection at all times, regardless of the network location.

Disconnect
Stops an active secure access connection, and prevents the client from connecting again until a user clicks **Connect** or **Auto-Connect**.

About Network Access features for Mac clients

Access Policy Manager® (APM®) supports all of the primary Network Access features for Mac clients, except for Drive Mappings and some endpoint security features.

For endpoint security support, refer to *BIG-IP® APM® Client Compatibility Matrix* on AskF5™ at `http://support.f5.com/`.

For information about Network Access features, refer to *BIG-IP® Access Policy Manager: Network Access* on AskF5™ at `http://support.f5.com/`.

VPN component installation and log locations on a Mac

On Macintosh operating systems, the client installs the VPN components and writes VPN logs to the locations listed in the table.

VPN component	Location
Network Access plugin	`/Library/Internet Plugins/`
Endpoint Security (client checks)	`~/Library/Internet Plugins/`

VPN logs are written to the following directory: `~/Library/Logs/F5Networks`.

Clients for Linux

About Linux clients

Access Policy Manager® (APM®) supports two Linux clients, a CLI and Network Access client components for browser-based access. On the CLI for Linux, APM supports logon with user name and password only and does not support any endpoint security features.

On the client component for Linux, APM supports all of the primary Network Access features, except for Drive Mappings and some endpoint security features. For endpoint security support for the web client for Linux, refer to *BIG-IP® APM® Client Compatibility Matrix* on AskF5™ at `http://support.f5.com/`. For information about Network Access features, refer to *BIG-IP® Access Policy Manager: Network Access* on AskF5™ at `http://support.f5.com/`.

About browser-based connections from Linux, Mac, and Windows clients

For Linux, Mac OS X, and Windows-based systems, the Network Access client component is available for automatic download from the BIG-IP® system.

Note: *The client component supports secure remote web-based access to the network. It is not the same as the customizable client package that is associated with the connectivity profile.*

The first time a remote user starts Network Access, APM® downloads a client component. This client component is designed to be self-installing and self-configuring. If the browser does not meet certain requirements, APM prompts the user to download the client component and install it manually.

Requirements for client installation and use on Linux

The table lists requirements for installing Network Access client components on a Linux system and using them for web-based access.

Requirement	Specification
Browser	Use Firefox for installing the client component. The browser must support the installation of plugins.
Firewall settings	If you have a firewall enabled on your Linux system, you must enable access on IP address 127.0.0.1, port `44444`.
PPP	The system must support PPP. (This is usually the case.) The user must have permission to run the PPP daemon.
Installation privilege	The remote user must have superuser authority, or, must be able to supply an administrative password to successfully install the Network Access client.

About Network Access features for Linux clients

Access Policy Manager® (APM®) supports two Linux clients, a CLI and Network Access client components that support web-based access. On the CLI for Linux, APM supports logon with user name and password only and does not support any endpoint security features.

With the web-based client components for Linux, APM supports all of the primary Network Access features, except for Drive Mappings and some endpoint security features. For endpoint security support for the web client for Linux, refer to *BIG-IP® APM® Client Compatibility Matrix* on AskF5™ at `http://support.f5.com/`. For information about Network Access features, refer to *BIG-IP® Access Policy Manager: Network Access* on AskF5 at `http://support.f5.com/`.

Specifying applications to start on a Linux client

You can specify applications to start when the client begins a Network Access session. You might do this when you have remote clients that routinely use Network Access to connect to an application server, such as a mail server.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Network Access (VPN)** > **Network Access Lists**.
   The Network Access Lists screen opens.
2. In the Name column, click the name of the network access resource you want to edit.
3. To configure applications to start for clients that establish a Network Access connection with this resource, click **Launch Applications** on the menu bar.
4. Click **Add** to add an application list.
   A screen opens showing the Add Application To Launch area.
5. In the **Application Path** field type an application to launch.
   For example, type `/usr/bin/mozilla` to start Mozilla.
6. In the **Parameters** field, type a parameter.
   For example, type `http://www.f5.com`.
7. From the **Operating System** list, select **Unix**.
8. Click **Finished** to add the configuration.

Now, when remote users with assigned resources make a Network Access connection, the application you configured starts automatically.

Overview: Installing and using the CLI for Linux

The BIG-IP® Access Policy Manager® includes a CLI for Linux. With the CLI, users can initiate VPN connections through APM® from the command line. You can download and deploy this client to your organization's Linux desktops.

Task summary

Downloading the Linux command line client

You can download the BIG-IP® Edge ®command line client for Linux installer, as a gzipped `.tar` file, and distribute it to clients for installation.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Client Downloads**.
   A list of available client downloads displays.
2. Click **BIG-IP Edge Command Line Client for Linux**.
   The file `linux_sslvpn.tgz` is downloaded to your local directory.

The Linux command line client is ready to be installed.

Installing the CLI for Linux

Install the command line interface for Linux so that users can start and stop Network Access sessions from the command line.

1. Extract the file `linux_sslvpn.tgz` to your local directory.
2. Extract the file `linux_sslvpn.tar` to your local directory.
3. Run the install script `Install.sh` under the root account.

The following text appears when installation is complete:

```
--> f5fpc is installed in /usr/local/bin
--> Please check f5fpc --help command to get started
--> Uninstaller located in /usr/local/lib/F5Networks/uninstall_F5.sh
```

Importing a certificate to the local trust store

You can import an untrusted certificate to the local trust store and change it into a trusted certificate.

1. Using operating system commands, place the certificate in any folder in the operating system.
   For example, `/etc/certs`.
2. Change the directory.
   For example, `cd /etc/certs`.
3. Type the command `c_rehash ./`.

The certificate is installed.

Note: *Alternatively, instead of installing the certificate, you can specify the `--cacert` option to import a certificate to the local store.*

Linux client commands

The following commands are supported by the Linux command line client. All commands that are invoked on the Linux command line client begin with the command `f5fpc`.

To start a VPN connection, type either of the following commands:

- `f5fpc -- start [`*`arguments`*`]`
- `f5fpc - s [`*`arguments`*`]`

Note: *This requires the `--host` or `-t` argument at the minimum.*

Use the following table to assign arguments to the Linux commands.

Arguments	Description
`--nonblock` `-b`	Returns the command line interface immediately after the command.
`--host [https://]`*`hostname`*`[:port]` `-t [https://]`*`hostname`*`[:port]`	The host name to which the client starts the VPN connection. This is required.

Arguments	Description
`--user` *username* `-u` *username*	The optional user name for the connection.
`--password` *password* `p` *password*	The optional password for the connection.
`--userhex` *hex-encoded-username* `-U` *hex-encoded-username*	The optional hex-encoded user name for the connection.
`--passwordhex` *hex-encoded-password* `-P` *hex-encoded-password*	The optional hex-encoded password for the connection.
`--cert` *certificate* `-r` *certificate*	Specifies an optional client certificate.
`--key` *certificate_key* `-k` *certificate_key*	Specifies the key for an optional client certificate.
`--keypass` *SSL_certificate_password* `-y` *SSL_certificate_password*	Specifies the password for an optional SSL certificate.
`--cacert` *trusted_CA_certificate* `-a` *trusted_CA_certificate*	Specifies a certificate from a trusted certificate authority (CA). If `--cacert` or `--cacertdir` is specified, then the server certificate validates for trust against the specified certificate or directory. If `--cacert` or `--cacertdir` is not specified, then the default location `/etc/ssl/certs` is checked to verify trust. The `--nocheck` option can be specified if a server certificate check is not desired, though this is not recommended.
`--cacertdir` *trusted_CA_certificate_directory* `-d` *trusted_CA_certificate_directory*	Specifies a certificate directory that contains a certificate from a trusted CA. If `--cacert` or `--cacertdir` is specified, then the server certificate validates for trust against the specified certificate or directory. If `--cacert` or `--cacertdir` is not specified, then the default location `/etc/ssl/certs` is checked to verify trust. The `--nocheck` option can be specified if a server certificate check is not desired, though this is not recommended.
`--nocheck` `-x`	Specifies that the trusted CA certiicate is not verified for trust at all. If `--cacert` or `--cacertdir` is specified, then the server certificate validates for trust against the specified certificate or directory. If `--cacert` or `--cacertdir` is not specified, then the default location `/etc/ssl/certs` is checked to verify trust. The `--nocheck` option can be specified if a server certificate check is not desired, though this is not recommended.

To stop the VPN connection, type either of the following commands:

- `f5fpc -- stop`
- `f5fpc --o`

To display the connection status, type either of the following commands:

- `f5fpc -- info`

- `f5fpc --i`

To display the command line client help, type either of the following commands:

- `f5fpc -- help`
- `f5fpc --h`

Info command status and error codes

The following status codes and error codes might be displayed when you run the `--info` command.

Error code/command status	Hex value	Shell value	Description
CLI_ERROR_SUCCESS	0x0	0	The command line operation was successful.
CLI_ERROR_USERS_DISCONNECT	0x150	80	The user was disconnected
CLI_ERROR_LOGON_FAILURE	0x151	81	Login failed due to incorrect authenticaion information or login errors.
CLI_ERROR_ATTENTION_REQUIRED	0x154	84	The user's attention is required.
CLI_ERROR_GENERIC_FAILURE	0x155	85	An error occurred in the system API.
CLI_ERROR_UNKNOWN_PARAMETER	0x156	86	An incorrect or unknown parameter was passed to the command line.
CLI_ERROR_WRONG_VALUE	0x157	87	This is an undefined error.
CLI_ERROR_UNKNOWN_SESSION_ID	0x158	88	An unknown session ID was encountered. The user should reconnect to the server.
CLI_ERROR_NO_PROFILE	0x15B	91	No such profile exists.
CLI_ERROR_MSGQ_OPEN_FAILURE	0x15D	93	The system failed to open the message queue.
CLI_ERROR_OPERATION_IN_PROGRESS	0x15F	95	An operation is in progress, please retry.
kss_Initialized	1	1	The session is initialized.
kss_LogonInProgress	2	2	The user login is in progress.
kss_Idle	3	3	The session is idle.
kss_Established	5	5	The session is established.
kss_AttentionReq	6	6	The session requires the user's attention.
kss_LogonDenied	7	7	Login was denied.
kss_LoggedOut	8	8	The user is logged out of the server.

Editing the log level for Edge Client on Linux

You can edit log settings in the configuration file on Linux systems.

1. In the `/usr/local/lib/F5Networks` directory, open the `f5networks.conf` file.
2. Edit the settings to change the log level.
   By default, the values are 0 (zero). For debugging purposes, set the values to 5.

VPN component installation and log locations on Linux

On Linux operating systems, the client installs the VPN components and writes VPN logs to the locations listed in the table.

Category	Location
VPN component	`/usr/local/lib/F5Networks`
VPN logs	`~/.F5Networks`

F5 Access Apps

Overview: Configuring APM for F5 Access Apps

F5® Access for Android, F5 Access for iOS, and F5 Access for Chrome OS enable secure network access for supported mobile clients. Previously, the Android and iOS products were called BIG-IP® Edge Client® for Android and BIG-IP Edge Client for iOS. For the clients to connect, you need a Network Access configuration on BIG-IP Access Policy Manager®. The Network Access Wizard creates a Network Access configuration with authentication, an access policy, and a virtual server with connectivity and access profiles.

You might need to update the connectivity profile or the network access resource to complete the configuration on APM®. Optionally, you can also configure SSO and ACLs, and add items to the access policy to enable SSO and enforce ACLs.

Task summary

Running the Network Access Setup wizard

Your DNS server must be configured to resolve internal addresses with DNS.

Configure Access Policy Manager® to provide users with full network access when they use BIG-IP® Edge Client® for iOS or BIG-IP Edge Client for Android.

Important: *You must specify either the DNS Default Domain Suffix or the DNS Address Space in the Network Access configuration. Otherwise, the system cannot resolve internal DNS addresses.*

---

1. On the Main tab, click **Wizards** > **Device Wizards**.
   The Device Wizards screen opens.
2. Select **Network Access Setup Wizard for Remote Access**, and then click **Next**.

   Tip: *Follow the instructions in the wizard to create your access policy and virtual server.*

   ---
3. To ensure that Edge Apps can connect from supported mobile devices, for **Client Side Checks**, clear the **Enable Antivirus Check in Access Policy** check box.

   Tip: *Follow the instructions in the wizard to create your access policy and virtual server.*

   ---
4. To specify the **DNS Address Space** setting, on the Network Access screen perform these substeps:
   a) From **Traffic Options**, select **Force Use split tunneling for traffic**.
      Additional settings display.
   b) In the **DNS Address Space** setting, for each address space, type the address in the form `site.siterequest.com` or `*.siterequest.com` , and click **Add**.
5. On the DNS Hosts screen, you can type a value in the **DNS Default Domain Suffix** field.
6. After you complete the wizard screens and create the configuration, on the Setup Summary screen click **Finished**.

You now have a network access configuration that supports BIG-IP Edge Client for mobile devices. All configuration object names are prefixed with the policy name that you entered in the wizard.

Configuring a connectivity profile for F5 Access for iOS

A connectivity profile automatically contains default settings for F5 Access for iOS. You should configure the connectivity profile settings to fit your situation.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From Mobile Client Settings in the left pane, select **iOS Edge Client**.
   Settings for the iOS Edge Client display in the right pane.
4. To enable users to save their passwords for reconnection purposes within a specified time period, select the **Allow Password Caching** check box.
   The additional fields in the area become available.
5. To enable device authentication on the client, select **Require Device Authentication**.
6. For **Save Password Method**, specify how to perform password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.
7. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
8. In the **On Demand Disconnect Timeout (minutes)** field, retain the default `2`, or type a different number of minutes before VPN on demand times out.
9. To force the app to use a selected logon mode and prevent users from changing it:
   a) Select the **Enforce Logon Mode** check box.
   b) From the **Logon Method** list, select **web** or **native**.

   Note: *This feature is supported with F5 Access for iOS and F5 Access for Android.*

   ---

10. Click **OK**.
    The popup screen closes, and the Connectivity Profile List displays.

You have now configured the security settings for BIG-IP Edge Client for iOS.

To provide functionality with a connectivity profile, you must add the connectivity profile and an access profile to a virtual server.

Configuring a connectivity profile for F5 Access for Android

A connectivity profile automatically contains settings for F5 Access for Android. You should configure the settings to fit your situation.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From Mobile Client Settings in the left pane, select **Android Edge Client**.
   Settings for the Android Edge Client display in the right pane.
4. To enable users to save their passwords for reconnection purposes within a specified time period, select the **Allow Password Caching** check box.
   The additional fields in the area become available.

5. For **Save Password Method**, specify how to perform password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.
6. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
7. To enhance security on the client, retain the selection of the **Enforce Device Lock** check box (or clear the check box).

   This check box is selected by default. Edge Portal® and Edge Client support password locking, but do not support pattern locking. If you clear this check box, the remaining settings in the area become unavailable.
8. For **Device Lock Method**, retain the default **numeric**, or select a different method from the list.
9. For **Minimum Passcode Length**, retain the default `4`, or type a different passcode length.
10. For **Maximum Inactivity Time (minutes)**, retain the default `5`, or type a different number of minutes.
11. To force the app to use a selected logon mode and prevent users from changing it:
    a) Select the **Enforce Logon Mode** check box.
    b) From the **Logon Method** list, select **web** or **native**.

    Note: *This feature is supported with F5 Access for iOS and F5 Access for Android.*
12. Click **OK**.
    The popup screen closes, and the Connectivity Profile List displays.

You have now configured the security settings for BIG-IP Edge Client for Android.

Overview: Configuring APM for Edge Portal Mobile Apps

BIG-IP® Edge Portal® for Android and BIG-IP Edge Portal for iOS streamline access to portal access web sites and applications that reside behind BIG-IP Access Policy Manager® (APM®). To support the clients, you need a Portal Access configuration on APM. The Portal Access Wizard creates a configuration with authentication, an access policy, and a virtual server with connectivity and access profiles.

You might need to update the connectivity profile or the access policy to complete the configuration on APM.

Task summary

Running the Portal Access wizard

Run the Portal Access Setup Wizard to quickly set up an access policy and a virtual server for your users.

1. On the Main tab, click **Wizards** > **Device Wizards**.
   The Device Wizards screen opens.
2. Select **Portal Access Setup Wizard** and click **Next**.
3. On the Basic Properties screen in the **Policy Name** field, type a name for the access policy.

   Note: *The name you type here prepends the name of the objects (for example, the virtual server) that the wizard creates for this configuration.*

4. To ensure that Edge Apps can connect from supported mobile devices, for **Client Side Checks**, clear the **Enable Antivirus Check in Access Policy** check box.

   Tip: *Follow the instructions in the wizard to create your access policy and virtual server.*

5. Click **Finished**.

You have created the configuration objects that are required for a Portal Access configuration to support BIG-IP® Edge Portal® mobile apps.

Configuring an access policy to support Edge Portal app

Configure an access policy to process access correctly for various client types, including the Edge Portal® app.

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. In the Per-Session Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click **Add New Macro**.
4. In the **Select macro template:** select Client Classification and Prelogon checks from the drop-down list.

   The macro inserts an antivirus check for those clients that can support it, and provides the appropriate terminal for each type of client.
5. Click **Save**.
6. Click the plus [+] sign that appears before the Logon Page action.
7. In the Macrocalls area, click the **Client Classification and Prelogon checks** button.
8. Click **Add item**.
   The Client Classification and Prelogon checks action appears in the access policy sequence.
9. Click the underlined word **Deny** in the ending field.
10. In the Select Ending area, click **Allow**.
11. Click **Save**.

Assigning ACLs to your access policy

Assign ACLs to limit access to resources.

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. In the Per-Session Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **Resource Assign** agent in the access policy branch.
   The Properties screen opens.
4. Click the **Add/Delete Resources** link.
   A popup screen with a tab for each resource type displays.
5. Select the tab, select the ACLs to add to the access policy, and click **Update** when finished.
6. Click **Apply Access Policy**.

Disabling the Home Tab

Disabling the Home Tab ensures that the BIG-IP® Edge Portal® app renders properly.

Note: *The Home Tab property exists for each portal access resource item.*

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Portal Access** > **Portal Access Lists**.
   The Portal Access List screen opens.
2. Click the name of a resource item for the portal access resource that you created.
   The properties screen for that resource item opens.
3. In the Resource Items Properties area, select **Advanced** and for **Home Tab**, make sure the **Enabled** check box is cleared.
4. Click **Update**.

Repeat this task for each portal access resource item.

Configuring a connectivity profile for Edge Portal for Android

A connectivity profile automatically contains settings for BIG-IP® Edge Portal® for Android clients. You should configure the settings to fit your situation.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From Mobile Client Settings in the left pane, select **Android Edge Portal**.
   Settings for the Android Edge Portal display in the right pane.
4. To enable users to save their passwords for reconnection purposes within a specified time period, select the **Allow Password Caching** check box.
   The additional fields in the area become available.
5. For **Save Password Method**, specify how to perform password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.
6. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
7. To enhance security on the client, retain the selection of the **Enforce Device Lock** check box (or clear the check box).

   This check box is selected by default. Edge Portal® and Edge Client support password locking, but do not support pattern locking. If you clear this check box, the remaining settings in the area become unavailable.
8. For **Device Lock Method**, retain the default **numeric**, or select a different method from the list.
9. For **Minimum Passcode Length**, retain the default `4`, or type a different passcode length.
10. For **Maximum Inactivity Time (minutes)**, retain the default `5`, or type a different number of minutes.
11. To force the app to use a selected logon mode and prevent users from changing it:
    a) Select the **Enforce Logon Mode** check box.
    b) From the **Logon Method** list, select **web** or **native**.

    Note: *This feature is supported with F5 Access for iOS and F5 Access for Android.*
12. Click **OK**.
    The popup screen closes, and the Connectivity Profile List displays.

You have now configured the security settings for BIG-IP Edge Portal for Android clients.

Configuring connectivity profiles for Edge Portal for iOS

A connectivity profile automatically contains settings for BIG-IP® Edge Portal® for iOS. You should configure the settings to fit your situation.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From Mobile Client Settings in the left pane, select **iOS Edge Portal**.
   Settings for the iOS Edge Portal display in the right pane.
4. To enable users to save their passwords for reconnection purposes within a specified time period, select the **Allow Password Caching** check box.
   The additional fields in the area become available.
5. For **Save Password Method**, specify how to perform password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.
6. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
7. Specify security by keeping **Enforce PIN Lock** set to **Yes**.
   Edge Portal supports PIN locking, but does not support pattern locking.
8. For **Maximum Grace Period (minutes)**, retain the default `2`, or type a different number of minutes.
9. To force the app to use a selected logon mode and prevent users from changing it:
   a) Select the **Enforce Logon Mode** check box.
   b) From the **Logon Method** list, select **web** or **native**.

   Note: *This feature is supported with F5 Access for iOS and F5 Access for Android.*

   ---

10. Click **OK**.
    The popup screen closes, and the Connectivity Profile List displays.

You have now configured the security settings for BIG-IP Edge Portal for iOS.

Configuring Access Policy Manager for MDM applications

Overview: Configuring APM for device posture checks with endpoint management systems

When you check the device posture of a mobile device from your endpoint management system, before allowing access to the corporate network, you can configure BIG-IP Access Policy Manager to verify the mobile device posture. The verification comes from the endpoint management system before allowing access from the access policy. An endpoint management system also controls the corporate data on mobile devices. Edge Client establishes a VPN connection with APM®, and an endpoint management system (Airwatch, MaaS360, or Intune) manages and sends device details to APM.

Task summary

Creating an endpoint management system connector with Airwatch

You must create a Server SSL profile on a BIG-IP® system and have access to an Airwatch system.

An endpoint management system on BIG-IP Access Policy Manager®(APM) is an object that stores information about the device management server, such as IP addresses and API credentials. You can configure more than one endpoint management system on the same BIG-IP system. APM® polls devices connected to configured endpoint management systems.

1. Log in to the Airwatch console using the administrator user name and password.
2. On the left panel, click **Accounts**.
   The View Role screen displays.
3. For the **Categories** setting, click **API** > **REST**.
4. Enable API access for the administrator.
5. On the left panel on the main screen, click **Groups & Settings**.
   The Settings popup screen opens.
6. Under the System tab, click **API** > **REST API**
   The System/Advanced/API/REST popup screen opens.
7. On the System/Advanced/API/REST screen, select the **General** tab.
8. Select the **Override** setting.
9. Select **Enable API Access**.
10. Copy the API key displayed next to **API key**.
11. Click **Save**.
12. On the BIG-IP system, on the Main tab, click **Access Policy** > **Authentication** > **Endpoint Management Systems**.
    The Endpoint Management Systems screen opens.
13. Click **Create**.
14. In the **Name** field, type a name for the endpoint management system.
15. In the **Type** list, select **Airwatch** for the endpoint management system.
16. In the **FQDN** field, type a fully qualified domain name.
17. In the **Port** field, type `443`.

18. From the **Server SSL Profile** list, select a previously created Server SSL profile in BIG-IP Local Traffic Manager™.
19. In **Update Interval (minutes)** field, type a number in minutes that represents how often APM updates the device database.
20. In the **Username** field, type the Airwatch administrator user name.
21. In the **Password** field, type the Airwatch administrator password.
22. In the **API Token** field, type or paste the API key copied from the Airwatch screen.
23. Click **Finished**.

You have created an endpoint management system. APM tests the connection to the device management server, and prints a test status in the **Status** field. If the status displays `OK`, APM starts the device database synchronization for the created endpoint management system.

Note: *The Airwatch interface might change.*

Creating an endpoint management system connector with MaaS360

You must create a Server SSL profile on a BIG-IP® system and have access to an MaaS360 system.

An endpoint management system on BIG-IP® Access Policy Manager®(APM) is an object that stores information about the device management server, such as IP addresses and API credentials. You can configure more than one endpoint management system on the same BIG-IP system. APM® polls devices connected to configured endpoint management systems.

1. Contact MaaS360 to obtain information needed to access the API.

   The information required includes the following data:

   - Application ID
   - Platform version
   - Version number
   - Access key
   - Service URL
2. Log in to the MaaS360 console using the administrator user name and password.
3. At the bottom of the screen, copy the Account ID.
4. On the BIG-IP system, on the Main tab, click **Access** > **Authentication** > **Endpoint Management Systems**.
   The Endpoint Management Systems screen opens.
5. Click **Create**.
   The New endpoint management system screen opens.
6. In the **Name** field, type a name for the endpoint management system.
7. In the **Type** list, select **MaaS360** for the endpoint management system.
   The Network location and API Credentials sections display.
8. In the **FQDN** field, type the service URL provided by MaaS360.
9. In the **Port** field, type `443`.
10. From the **Server SSL Profile** list, select a previously created Server SSL profile in BIG-IP Local Traffic Manager™.
11. In **Update Interval (minutes)** field, type a number in minutes that represent how often APM updates the device database.
12. In the **Username** field, type the MaaS360 administrator user name.
13. In the **Password** field, type the MaaS360 administrator password.
14. In the **Billing Id** field, type or paste the billing ID copied from the MaaS360 screen.

15. In the **Application Id** field, type the application ID provided by MaaS360.
16. In the **Access Key** field, type the access key provided by MaaS360.
17. In the **Platform** field, type the platform version of the MaaS360 console.
18. In the **App Version** field, type the current version number of the application that is linked to the account.
19. Click **Finished**.

You have created an endpoint management system. APM tests the connection to the device management server, and prints a test status in the **Status** field. If the status displays `OK`, APM starts the device database synchronization for the created endpoint management system.

Note: *The MaaS360 interface might change.*

Creating an Azure web application for Microsoft Intune on APM

Before you can configure a web application, contact Microsoft to purchase a Microsoft Intune subscription.

BIG-IP APM integrates Microsoft Intune by configuring a Microsoft Azure Client web application on the Microsoft Azure portal. This topic describes how to create a web application to obtain a client ID and a client secret.

1. On Microsoft Azure, on the main tab, click **Azure Active Directory**.
   The Azure Active Directory screen opens.
2. Click **App registrations**.
   The App registrations screen opens.
3. Click **New application registration**.
   A new Create screen opens.
4. In the **Name** field, type a name for the new web application.
5. From the **Application** type dropdown menu, select **Web app / API**.
6. In the **Sign-on URL** field, type a URL.

   This can be any URL, such as `https://localhost`.
7. Click **Create**.
   A list of applications displays in the Register app screen.
8. Copy the Application ID to your records.

   You use this ID as a client id when configuring EMS object on BIG-IP.
9. Click **Settings**.
   The **Settings** screen opens.
10. Click **Keys**.

    Use this option to create a secret key.

    The **Keys** screen opens.
11. In the Description field, enter any description for this secret key.
12. From the **Expires** dropdown menu, select **Never expires**.
13. Click **Save**.

    You should copy the key to the administrator records. You use this key as a client secret when configuring EMS object on a BIG-IP system.

    A new key displays in the Keys screen.
14. In the Registered app screen, under Settings, click **Required Permissions**.
    The Required permissions screen opens.
15. Click **Add**.

16. For the **Select a API** option, select **Microsoft Intune API**.
17. Click **Select**.
18. From the **APPLICATION PERMISSIONS** list, select **Get device state and compliance information from Microsoft Intune**.
19. Click **Select** and **Done**.
    A list of added permissions displays.
20. Click **Grant permissions**.
21. Navigate back to the Azure Active Directory screen.
22. Click **Enterprise Applications** > **All Applications**
    The new web application displays in the list.
23. Click **new-app** > **Permissions**.
    The Permissions screen opens the Microsoft Intune API with the permission, "Get device state and compliance information from Microsoft Intune."

You now have a tenant ID, client ID, and client secret.

From your BIG-IP system, create an Endpoint Management System for Microsoft Intune.

Creating an endpoint management system connector with Microsoft Intune

You must create a Server SSL profile on a BIG-IP® system and have access to a Microsoft Intune system.

An endpoint management system on BIG-IP® Access Policy Manager®(APM) is an object that stores information about the device management server, such as IP addresses and API credentials. You can configure more than one endpoint management system on the same BIG-IP system. APM® polls devices connected to configured endpoint management systems.

1. On the BIG-IP system, on the Main tab, click **Access** > **Authentication** > **Endpoint Management Systems**.
   The Endpoint Management Systems screen opens.
2. Click **Create**.
   The New endpoint management system screen opens.
3. In the **Name** field, type a name for the endpoint management system.
4. In the **Type** list, select **Microsoft Intune** for the endpoint management system.
   The Network location and API Credentials sections display.
5. From the **Server SSL Profile** list, select a previously created Server SSL profile in BIG-IP Local Traffic Manager™.
6. From the **DNS Resolver** list, select a previously created DNS Resolver in BIG-IP Local Traffic Manager™.

   Create a DNS Resolver the same way you create a Server SSL profile.
7. In **Update Interval (minutes)** field, type a number in minutes that represent how often APM updates the device database.
8. In the **Tenant Id** field, type the tenant ID that comes with a Microsoft Intune subscription.
9. In the **Client Id** field, type the client ID that becomes available after creating a web application.
10. In the **Client Secret** field, type the client secret that becomes available after creating a web application.
11. Click **Finished**.

You have created an endpoint management system. APM tests the connection to the device management server, and prints a test status in the **Status** field. If the status displays `OK`, APM starts the device database synchronization for the created endpoint management system.

Editing an endpoint management system profile

You can create an endpoint management system on BIG-IP APM with either Airwatch or MaaS360.

An endpoint system management system connector object on BIG-IP® Access Policy Manager®(APM®) is an object that stores information about the device management server, such as IP addresses and API credentials. You can configure more than one endpoint management system profile on the same BIG-IP system. APM polls devices connected to configured endpoint management systems.

1. On the BIG-IP system, on the Main tab, click **Access** > **Authentication** > **Endpoint Management Systems**.
   The Endpoint Management Systems screen with a list of endpoint management systems opens.
2. In the Name column, click the name of the endpoint management system you want to edit.
   The properties screen for that endpoint management system opens.
3. Edit one or more fields.

   The status of the endpoint management system updates during each sync interval. If you edit the **Username**, **FQDN**, or **Port** fields, the **Status** field displays the same status as the actual configuration status. If you edit other property fields, the **Status** field might be different than the actual configuration status. The correct status appears when the next sync interval begins
4. Click **Update**.

You have updated an endpoint management system.

Creating an access profile

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

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

   Note: *A access profile name must be unique among all access profile and any per-request policy names.*
4. From the **Profile Type** list, select one these options:
   - **LTM-APM**: Select for a web access management configuration.
   - **SSL-VPN**: Select to configure network access, portal access, or application access. (Most access policy items are available for this type.)
   - **ALL**: Select to support LTM-APM and SSL-VPN access types.
   - **SSO**: Select to configure matching virtual servers for Single Sign-On (SSO).

     Note: *No access policy is associated with this type of access profile*
   - **RDG-RAP**: Select to validate connections to hosts behind APM when APM acts as a gateway for RDP clients.
   - **SWG - Explicit**: Select to configure access using Secure Web Gateway explicit forward proxy.
   - **SWG - Transparent**: Select to configure access using Secure Web Gateway transparent forward proxy.
   - **System Authentication**: Select to configure administrator access to the BIG-IP® system (when using APM as a pluggable authentication module).

- **Identity Service**: Used internally to provide identity service for a supported integration. Only APM creates this type of profile.

  Note: *You can edit Identity Service profile properties.*

Note: *Depending on licensing, you might not see all of these profile types.*

Additional settings display.

5. 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.

6. Click **Finished**.

The access profile displays in the Access Profiles List. Default-log-setting is assigned to the access profile.

Configuring an access policy to include endpoint management integration

You can configure an access policy to perform compliance checks for connected devices. The Managed Endpoint Status action determines whether APM® recognizes a device with a device ID. The Managed Endpoint Notification action sends a push notification message to a device. You can create access policy checks using session variables and device posture information to allow or deny access.

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. In the Access Policy column, click the **Edit** link for the endpoint management type access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. Add a Managed Endpoint Status action:
   a) From the Endpoint Security (Server-Side) list, select **Managed Endpoint Status** and click **Add Item**.
      A popup Properties screen opens.
   b) In the **Name** field, type a name for the access policy action.
   c) For the **Endpoint Management System**, select the endpoint management system that you previously created.
   d) Click **Save**.

   The visual policy editor screen displays.
5. In both the compliant branch and not compliant branch of the Managed Device Status action, click the **(+)** icon anywhere in the access policy to add a new action item.
6. To add a Managed Endpoint Notification action, perform the following steps:
   a) From the Endpoint Security (Server-Side) list, select **Managed Endpoint Notification**.
      A popup Properties screen opens.
   b) In the **Name** field, type a name for the access policy action.

c) From the endpoint management system list, select the endpoint management system that you previously created.

Note: *The Intune endpoint management system does not support Endpoint Notification agent.*

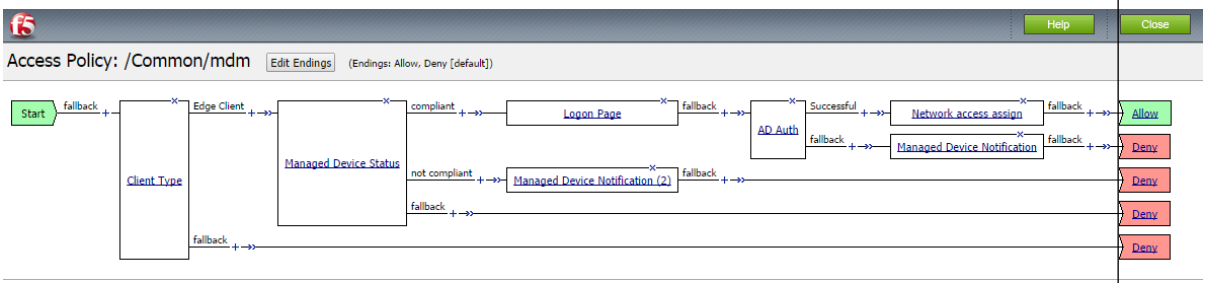
---

d) In the **Message** field, type a message that displays on a device.
e) Click **Save**.

The visual policy editor screen displays.

You have an access policy that presents endpoint management integration with VPN access.

Access policy with endpoint management integration



Creating a virtual server

You create a virtual server for VPN traffic on the network.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. From the **Configuration** list, select **Advanced**.
5. In the **Destination Address** field, type the IP address for the virtual server.
   When you type the IP address for a single host, it is not necessary to append a prefix to the address.
6. In the **Service Port** field, type the port number.
7. From the **SSL Profile (Client)** list, select `clientssl`.
8. From the **Source Address Translation** list, select **Auto Map**.
9. Click **Finished**.
10. From the Access Profile list, select the access profile that you previously created.
11. From the Connectivity Profile list, select the connectivity profile that you previously created.

You have created a virtual server.

Hosting Files with Portal Access on Access Policy Manager

About using hosted files with a Portal Access resource

You can use hosted content that you have uploaded to the BIG-IP® Access Policy Manager® to provide the resource and resource items for a Portal Access resource.

When you use hosted content for a Portal Access resource, the link on the webtop for the portal access resource opens a file hosted on the system, instead of a URI. You configure the main Portal Access resource as this linked file. You then configure this file, and all related and required files, as resource items of this file.

In this example, a simple web page consisting of an HTML file, a CSS file, a JavaScript file, and an image are uploaded to a directory in the hosted content repository. The files are then specified as a Portal Access resource and resource items.

File	Location	Description
index.html	`/index.html`	The main web page that displays when the link is clicked. This is the Portal Access Resource.
styles.css	`/styles.css`	The CSS file for the page index.html.
test_image.jpg	`/test_image.jpg`	An image that is referenced on the page index.html.
script.js	`/js/script.js`	A JavaScript file that is referenced from the page index.html.

In this example, hosted content is uploaded as a single **ZIP** file, `test.zip`, then extracted to the location `/test` on the server.

Task summary

To add hosted content to a Portal Access link on Access Policy Manager® (APM®), complete these tasks.

Task list

Uploading files to Access Policy Manager for Portal Access

You upload files to Access Policy Manager® to provide content for a Portal Access webtop link.

Tip: *Before you upload multiple files to Access Policy Manager, you can combine the files in a ZIP archive format. Then, you can upload and extract the files in one step. In this example, four files are uploaded as a single ZIP archive, called* `test.zip`*.*

1. On the Main tab, click **Access** > **Webtops** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. Click the **Upload** button.
   The Create New File popup screen opens.

3. Under **Select File**, click the **Browse** button. Browse and select **test.zip**.
   The **Select File** and **File Name** fields are populated with the file name.
4. In the **File Destination Folder** field, specify the folder path `/test` in which to place the file.
5. From the **File Action** list, select **Upload and Extract**.
6. Click the **OK** button.
   The files appears in the hosted content list, in the folder specified. Any files in subfolders in the archive file also appear in subfolders in the hosted content list.

You must associate any access profiles that will access hosted content with the hosted content repository.

Associating hosted content with access profiles

A user can access hosted content that is associated with that user's access profile. Each access profile that requires hosted content access must be associated with the entire hosted content repository.

1. On the Main tab, click **Access** > **Webtops** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. On the **Upload** button, click the right-side arrow to select **Manage Access** from the list.
   The Access Settings popup screen opens.
3. Select the access profiles to associate with hosted content, then click **OK**.

   A user must belong to an associated access profile to access hosted content.

View the hosted content list, and verify that the access policy association was successful.

Creating a portal access configuration with hosted content

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Portal Access** > **Portal Access Lists**.
   The Portal Access List screen opens.
2. Click the **Create** button.
   The New Resource screen opens.
3. Type the name and an optional description.
4. From the **ACL Order** list, specify the placement for the resource.

Option	Description
Last	Select this option to place the new portal access resource last in the ACL list.
After	Select this option to select, from the list of configured ACLs, the ACL that this portal access resource should follow in sequence.
Specify	Select this option to specify an order number, for example, `0` or `631`for the ACL.

5. From **Configuration**, select **Basic** or **Advanced**.

   The **Advanced** option provides additional settings so you can configure a proxy host and port.
6. For the **Match Case for Paths** setting, select **Yes** to specify that portal access matches alphabetic case when matching paths in the portal access resource.
7. From the **Patching Type** list, select the patching type for the web application.

   For both full and minimal patching types, you can select or clear patching methods specific to your selection.
8. If you selected **Minimal Patching** and the **Host Patching** option, type a host search string, or multiple host search strings separated with spaces, and the host replace string, which must be the Access Policy Manager® virtual server IP address or fully qualified domain name.
9. Select the **Publish on Webtop** check box.
10. From the **Link Type** list, select **Hosted Content**.

11. From the **Hosted File** list, select `public/share/test/index.html`.

    This is the filename for this example scenario only. Please select the correct file for your own configuration.

12. In the Customization Settings for English area, in the **Caption** field, type a caption.

    The caption appears on the full webtop, and is required. This field is required even if you do not select the **Publish on webtop** option.

13. Optionally, in the **Detailed Description** field type a description for the web application.
14. In the **Image** field, specify an icon for the web application link. Click the **View/Hide** link to show the current icon.
15. If your application is behind a proxy server, to specify a proxy host and port, you must select **Advanced** for the configuration to display additional fields, and type the proxy host and proxy port.
16. Click the **Create** button.
    The Portal Access resource is saved, and the Portal Access Resource screen now shows a **Resource Items** area.

This completes the portal access resource configuration.

Specify all hosted content files used by this example (all files in the `/test` folder) as resource items.

Creating a portal access resource item for hosted content

You create a portal access resource item in order for hosted content to add a file that is part of a portal access hosted content resource. For example, you might add image files, CSS files, or scripts that are required by the web page or application. You typically use resource items to refine the behavior for web application directories; for example, you might specify `No Compression` and a `Cache All` caching policy for the images for a portal access resource.

Note: *You must add (separately) each hosted file used by the portal access resource, and the resource file itself, as resource items.*

---

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Portal Access** > **Portal Access Lists**.
   The Portal Access List screen opens.
2. Click the name of a portal access resource.
   The Portal Access Properties screen for that resource opens.
3. In the Resource Items area, click the **Add** button.
   A New Resource Item screen for that resource opens.
4. Select that the resource item type is **Hosted Content**.
5. From the **Hosted File** list, select the file to specify as a resource item.

   For purposes of this example, specify `public/share/test/index.html`, `public/share/test/test_image.jpg`, `public/share/test/style.css`, and `public/share/test/js/script.js`.

6. Configure the properties for the resource item.
   - To add headers, select **Advanced** next to New Resource Item.
   - To configure **Session Update**, **Session Timeout**, and **Home Tab**, select **Advanced** next to Resource Item Properties.
7. Click **Finished**.
   This creates the portal access resource item.

Implementation result

You have now added a portal access resource and portal access resource items that are based on uploaded hosted content.

Hosting a BIG-IP Edge Client Download with Access Policy Manager

About hosting a BIG-IP Edge Client file on Access Policy Manager

You can host files on BIG-IP® Access Policy Manager® (APM®) so clients can download them.

When you host a file on Access Policy Manager, you can provide the link to the file in a number of ways. In this example, the BIG-IP Edge Client® for Mac link is provided as a link on the user's webtop. The user connects through the web client, then clicks a link on the webtop to download the client file. To provide the BIG-IP Edge Client for Mac, first you must create a connectivity profile. Then, you can download the Mac client file as a ZIP file.

Task summary

To add the BIG-IP® Edge Client® for Mac file to the hosted content repository on Access Policy Manager®, so clients can download it, complete these tasks.

Task list

Configuring a connectivity profile for Edge Client for Mac

Update the connectivity profile in your Network Access configuration to configure security settings, servers, and location-awareness for BIG-IP® Edge Client® for Mac.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From the left pane of the popup screen, select **Win/Mac Edge Client**.
   Edge Client settings for Mac and Windows-based systems display in the right pane.
4. Retain the default (selected) or clear the **Save Servers Upon Exit** check box.

   Specifies whether Edge Client maintains a list of recently used user-entered APM® servers. Edge Client always lists the servers that are defined in the connectivity profile, and sorts them by most recent access, whether this option is selected or not.
5. To support automatic reconnection without the need to provide credentials again, allow password caching.
   a) Select the **Allow Password Caching** check box.

      This check box is cleared by default.

      The remaining settings on the screen become available.
   b) To require device authentication to unlock the saved password, select **Require Device Authentication.**

      This option links the option to use a saved password to a device authentication method. Supported device authentication methods include PIN, passphrase, and biometric (fingerprint) authentication on iOS and Android. Android devices also support pattern unlocking.

c) From the **Save Password Method** list, select **disk** or **memory**.

If you select **disk**, Edge Client caches the user's password (in encrypted form) securely on the disk where it is persisted even after the system is restarted or Edge Client is restarted.

If you select **memory**, Edge Client caches the user's password within the BIG-IP Edge Client application for automatic reconnection purposes.

If you select **memory**, the **Password Cache Expiration (minutes)** field displays with a default value of 240.

d) If the **Password Cache Expiration (minutes)** field displays, retain the default value or type the number of minutes to save the password in memory.

6. To enable automatic download and update of client packages, from the **Component Update** list, select **yes** (default).

   If you select **yes**, APM® updates Edge Client software automatically on the client system when newer versions are available.

7. Specify the list of APM servers to provide when the client connects.

   The servers you add here display as connection options in the BIG-IP Edge Client.

   Note: *Users can select from these servers or they can type a hostname.*

   ---

   a) From the left pane of the popup screen, select **Server List**.
   A table displays in the right pane.
   b) Click **Add**.
   A table row becomes available for update.
   c) You must type a host name in the **Host Name** field.

   Typing an alias in the **Alias** field is optional.

   d) Click **Update**.
   The new row is added at the top of the table.
   e) Continue to add servers, and when you are done, click **OK**.

8. Specify DNS suffixes that are considered to be in the local network.

   Providing a list of DNS suffixes for the download package enables Edge Client to support the autoconnect option. With **Auto-Connect** selected, Edge Client uses the DNS suffixes to automatically connect when a client is not on the local network (not on the list) and automatically disconnect when the client is on the local network.

   a) From the left pane of the popup screen, select **Location DNS List**.
   Location DNS list information is displayed in the right pane.
   b) Click **Add**.
   An update row becomes available.
   c) Type a name and click **Update**.

   Type a DNS suffix that conforms to the rules specified for the local network.

   The new row displays at the top of the table.

   d) Continue to add DNS names and when you are done, click **OK**.

9. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

Downloading the ZIP file for Edge Client for Mac

You can download a Mac Client package and distribute it to clients.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Select a connectivity profile.
3. Click the arrow on the **Customize Package** button and select **Mac**.

The Customize Mac Client Package screen displays.

4. Click **Download**.

   The screen closes and the package, `BIGIPMacEdgeClient.zip`, downloads.

The ZIP file includes a Mac installer package (PKG) file and configuration settings.

Distribute the entire ZIP file to your users.

Uploading BIG-IP Edge Client to hosted content on Access Policy Manager

Upload the client file to the Access Policy Manager® hosted content repository so you can provide it to clients through a download link.

1. On the Main tab, click **Access** > **Webtops** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. Click the **Upload** button.
   The Create New File popup screen opens.
3. For the **Select File** setting, click the **Browse** button. Browse and select the `BIGIPMacEdgeClient.zip` file that you previously downloaded.
   The **Select File** and **File Name** fields are populated with the file name.
4. From the **File Action** list, select **Upload Only**.
5. In the **File Destination Folder** field, specify the folder path in which to place the file. For purposes of this example, the folder `/client` is specified.
6. Click **OK**.
   The file appears in the hosted content list.

You must associate any access profiles that will access hosted content with the hosted content repository.

Associating hosted content with access profiles

A user can access hosted content that is associated with that user's access profile. Each access profile that requires hosted content access must be associated with the entire hosted content repository.

1. On the Main tab, click **Access** > **Webtops** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. On the **Upload** button, click the right-side arrow to select **Manage Access** from the list.
   The Access Settings popup screen opens.
3. Select the access profiles to associate with hosted content, then click **OK**.

   A user must belong to an associated access profile to access hosted content.

View the hosted content list, and verify that the access policy association was successful.

Creating a webtop link for the client installer

You can create and customize links that you can assign to full webtops. In this context, *links* are defined applications and web sites that appear on a webtop, and can be clicked to open a web page or application. You can customize these links with descriptions and icons.

1. On the Main tab, click **Access** > **Webtops** > **Webtop Links**.
2. Click **Create**.
   The New Webtop Link screen opens.
3. In the **Name** field, type a name for the webtop.
4. From the **Link Type** list, select **Hosted Content**.
5. From the **Hosted File** link, select `public/share/client/BIGIPMacEdgeClient.zip`.

6. In the **Caption** field, type a descriptive caption.

   The **Caption** field is pre-populated with the text from the **Name** field. Type the link text that you want to appear on the web link.
7. If you want to add a detailed description, type it in the **Detailed Description** field.
8. To specify an icon image for the item on the webtop, click in the **Image** field and choose an image, or click the **Browse** button.

   Click the **View/Hide** link to show or hide the currently selected image.
9. Click **Finished**.

The webtop link is now configured, and appears in the list, and on a full webtop assigned with the same action. You can edit the webtop link further, or assign it to an access policy.

Before you can use this webtop link, it must be assigned to an access policy with a full webtop, using either an advanced resource assign action or a webtop,links and sections assign action.

Adding a webtop, links, and sections to an access policy

You must have an access profile set up before you can add a webtop, links, and sections to an access policy.

You can add an action to an access policy to add a webtop, webtop links, and webtop sections to an access policy branch. Webtop links and webtop sections are displayed on a full webtop.

Important: *Do not assign a webtop for a portal access connection configured for minimal patching mode; this configuration does not work.*

---

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. 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.
3. On the menu bar, click **Access Policy**.
4. 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.
5. On a policy branch, click the **(+)** icon to add an item to the policy.
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
6. On the Assignment tab, select the **Webtop, Links and Sections Assign** agent and click **Add Item**.
   The Webtop, Links and Sections Assignment screen opens.
7. In the **Name** field, type a name for the policy item.

   This name is displayed in the action field for the policy.
8. For each type of resource that you want assign:
   a) Click the **Add/Delete** link next to the resource type (**Webtop Links**, **Webtop Sections**, or **Webtop**).

      Available resources are listed.
   b) Select from the list of available resources.

      Select only one webtop.
   c) Click **Save**.
9. Click the **Save** button to save changes to the access policy item.

You can now configure further actions on the successful and fallback rule branches of this access policy item.

Click the **Apply Access Policy** link to apply and activate your changes to this access policy.

Note: *To ensure that logging is configured to meet your requirements, verify the log settings for the access profile.*

Implementation result

As a result of these implementation tasks, you have added the client file to a webtop link.

Adding Hosted Content to Access Policy Manager

About uploading custom files to Access Policy Manager

You can upload custom files to BIG-IP® Access Policy Manager®(APM®) to provide resources directly to users.

For example, you can upload BIG-IP Edge Client® installers, antivirus or firewall update packages, or Citrix receiver files for your users to download. You can upload custom images, web pages, Java archives, JavaScript files, CSS files, archive files, and many other types of files as well.

Optionally, you can compress and upload multiple files as a single ZIP archive file. When you upload an archive file, you can choose to either upload the compressed file, or upload and extract the compressed file.

Upload Only
Select this option to upload an archived file that must remain in archive format. For example, you can upload a ZIP file for a user to download, containing a package of documents, or an application and related files. Some applications also use archived files; for example, you will upload a JAR file without extracting it.

Upload and Extract
Select this option to upload an archived file and extract it to the specified location. The folder hierarchy of the extracted file is preserved when you use this action. Select this option when you are uploading a collection of files that must be separated on the server for use by the end user; for example, to upload a web application that includes top-level HTML files, and subdirectories containing scripts, images, CSS, and other files.

Understanding hosted content

Hosted content is any type of file you would like to serve from Access Policy Manager® (APM®) to access policy users. Hosted content can include executable files, scripts, text, HTML, CSS files, and image files. You can serve hosted content from a webtop link, or from a portal access link.

About accessing hosted content

To access hosted content, a user must belong to an access profile that is associated with the hosted content. After content is uploaded to Access Policy Manager® (APM®), the entire hosted content library must be associated with one or more access profiles. These access profiles alone can view the content.

In addition, each file uploaded to the hosted content repository is assigned a permission level that determines the users who can access that content.

Permissions for hosted content

A permission level is assigned to each file in the hosted content repository, as described here.

Permission level	Description
policy	The file is available only to users who have successfully completed an access policy, with an **Allow** ending result, and an access profile

Permission level	Description
	associated with the hosted content repository. You can assign this to display an HTML file that only a verified user can see.
public	The file is available to anyone with an access profile associated with the hosted content repository. You can assign this to allow access to an installation package that a user needs to start an access session.
session	The file is available only to users with an active access policy session and an access profile associated with the hosted content repository. You can assign this to allow a user with an active session access to a required logon component.

Task summary

To add hosted content to Access Policy Manager® (APM®), complete these tasks.

Task list

Uploading files to Access Policy Manager

Before you upload multiple files to Access Policy Manager®, you can compress and combine the files into a ZIP archive file. Then, you can upload and extract the files in one step.

You can upload files to Access Policy Manager to provide content for public viewing, to provide pages and content to Portal Access connections, or to provide customized webtop links.

1. On the Main tab, click **Access** > **Webtops** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. Click the **Upload** button.
   The Create New File popup screen opens.
3. For the **Select File** setting, click the **Browse** button and select the file to upload.
   - To upload each file separately, select the first file, then repeat this step for all remaining files.
   - To upload all files at once from a compressed file, select the compressed file.

   The **Select File** and **File Name** fields are populated with the file name.
4. If you are uploading a compressed file that you want to extract, from the **File Action** list, select **Upload and Extract**.
5. Click **OK**.
   The file appears in the hosted content list.

You must associate any access profiles that will access hosted content with the hosted content repository.

Associating hosted content with access profiles

A user can access hosted content that is associated with that user's access profile. Each access profile that requires hosted content access must be associated with the entire hosted content repository.

1. On the Main tab, click **Access** > **Webtops** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.

2. On the **Upload** button, click the right-side arrow to select **Manage Access** from the list.
   The Access Settings popup screen opens.
3. Select the access profiles to associate with hosted content, then click **OK**.

   A user must belong to an associated access profile to access hosted content.

View the hosted content list, and verify that the access policy association was successful.

Implementation result

As a result of these implementation tasks, you have edited files and deleted hosted files on Access Policy Manager® as necessary.

Editing Hosted Content with Access Policy Manager

About editing hosted files on Access Policy Manager

You can upload custom files to BIG-IP® Access Policy Manager® to provide resources directly to users.

You might need to edit files after you upload them to Access Policy Manager, such as to rename a file or change the file MIME type. You can make these changes using the hosted content settings.

Task summary

To edit hosted content on Access Policy Manager®, complete these tasks.

Task list

Renaming or moving hosted content files

You can rename or move a hosted content file on Access Policy Manager®.

1. On the Main tab, click **Access** > **Webtops** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. At bottom left of the screen, click the right-side arrow on the **Edit** button to select **Rename/Move File** from the list.
   The **Rename/Move File Properties** popup screen opens.
3. In the **New File Name** field, type a new name for the file.
4. In the **New File Destination Folder**, specify a new destination folder for the file.
5. Click **OK**.
   The file changes are saved, and the screen returns to the hosted content list.

Editing hosted content file properties

You can edit the permissions and MIME type for hosted content files on Access Policy Manager®.

1. On the Main tab, click **Access** > **Webtops** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. At bottom left of the screen, click the right-side arrow on the **Edit** button to select **Edit File Properties** from the list.
   The **Edit File Properties** popup screen opens.
3. If the MIME type for the file is incorrect or must be changed, from the **Mime Type** list, select the MIME type for the file.
4. From the **Secure Level** menu, select the access level for the file.

Option	Description
policy	The file is available only to users who have successfully completed an access policy, with an **Allow** ending result. You might use this to display an HTML file that only a verified user can see.

Option	Description
public	The file is available to anyone. You might use this to allow access to an installation package that a user needs to start an access session.
session	The file is available only to users with an active access policy session. You might use this to allow a user with an active session access to a required logon component.

5. Click **OK**.
   The file changes are saved, and the screen returns to the hosted content list.

The settings for the file are displayed in the Hosted Content list.

Replacing a hosted file

You can upload a new version of a file to hosted content, to replace the current file on Access Policy Manager®.

1. On the Main tab, click **Access** > **Webtops** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. At bottom left of the screen, click the right-side arrow on the **Edit** button to select **Upload New Version** from the list.
   The **Upload New File Version** popup screen opens.
3. For the **Select File** setting, click the **Browse** button and select the file to upload.
   The **Select File** and **File Name** fields are populated with the file name.
4. If the MIME type for the file is incorrect or must be changed, from the **Mime Type** list, select the MIME type for the file.
5. From the **Secure Level** menu, select the access level for the file.

Option	Description
policy	The file is available only to users who have successfully completed an access policy, with an **Allow** ending result. You might use this to display an HTML file that only a verified user can see.
public	The file is available to anyone. You might use this to allow access to an installation package that a user needs to start an access session.
session	The file is available only to users with an active access policy session. You might use this to allow a user with an active session access to a required logon component.

6. Click **OK**.
   The file changes are saved, and the screen returns to the hosted content list.

View the hosted content list to verify your changes to the file.

Deleting a hosted file

You can delete one or more files from the hosted content on Access Policy Manager®.

1. On the Main tab, click **Access** > **Webtops** > **Hosted Content** > **Manage Files**.
   The Manage Files screen opens.
2. Select one or more files to delete. To select all files, select the check box at the top of the list, next to the Name column.
3. Click **Delete**, and in the **Delete File** popup screen that opens, click **Yes**.

The files are removed from the list.

Implementation result

As a result of these implementation tasks, you have edited files and deleted hosted files on Access Policy Manager® as necessary.

Managing Disk Space for Hosted Content

Overview: Managing disk space for hosted content files

By default, the BIG-IP® system allocates 512 MB of disk space to the sandbox for storing hosted content files. If disk space becomes exhausted when you try to upload a hosted content file, an error displays. You can increase the amount of disk space allocated to the sandbox to the maximum of 1024 MB, in addition to deleting any hosted content that you no longer need.

Task summary

Allocating the maximum amount of disk space for hosted content

You can specify the amount of disk space allocated for hosted content using a database variable.

Note: *The maximum supported disk space is 1024 MB.*

1. Log on to the BIG-IP® system command line and type `tmsh`.
2. Type this command sequence `sys db`.
3. To view the amount of space currently allocated for hosted content, type this command sequence `list total.sandbox.size value`.
4. To specify the amount of disk space allocated for hosted content:
   a) Type this command sequence `modify total.sandbox.size value`.
   This prompt displays. `Values: [enter integer value min:64 max:1024]`
   b) Type a value and press Enter.

Estimating hosted content file disk space usage

To estimate how much disk space hosted content files consume, you can display the sizes of the files in the sandbox from the command line.

1. Log on to the BIG-IP® system command line and type `tmsh`.
2. Type this command sequence `apm resource sandbox list files | grep size`.
   File sizes display.

```
            size 397325
            size 752662
```

Legal Notices

Legal notices

Publication Date

This document was published on February 14, 2019.

Publication Number

MAN-0462-07

Copyright

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*.

Link Controller Availability

This product is not currently available in the U.S.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a

residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Index

F

G

H

I

L

M

N

P

R

S

T

U

V

W