BIG-IP® Access Policy Manager® and BIG-IP® Edge Client™ for Windows Phone 8.1 v1.1

Contents

Legal Notices 5

Chapter 1: Overview: BIG-IP Edge Client for Mobile Devices 7
What does BIG-IP Edge Client do for Windows Phone? 8

Chapter 2: Overview: Access Policies for BIG-IP Edge Client 9
About access policy branches for BIG-IP Edge Client 10
Understanding basic access policy that supports BIG-IP Edge Client 10

Chapter 3: Overview: Configuring a VPN connection for BIG-IP Edge Client 11
About VPN support for BIG-IP Edge Client 12
Creating a new VPN profile 12
Configuring a VPN connection to auto-trigger 12
Establishing a VPN connection using a provisioned configuration 13
Terminating an existing VPN connection 13
About VPN deployment using Airwatch 13
Deploying a VPN profile using Airwatch 13

Legal Notices

Publication Date

This document was published on April 16, 2015.

Publication Number

MAN-0393-06

Copyright

Copyright © 2015, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, Application Acceleration Manager, Application Security Manager, APM, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, iCall, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, LineRate, LineRate Systems [DESIGN], Local Traffic Manager, LROS, LTM, Message Security Manager, MobileSafe, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, SDAC (except in Japan), SDC, Signalling Delivery Controller, Solutions for an application world, Software Designed Applications Services, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix (except Germany), Traffix [DESIGN] (except Germany), Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

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: *http://www.f5.com/about/guidelines-policies/patents*

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.

Chapter 1

Overview: BIG-IP Edge Client for Mobile Devices

Topics:

- *What does BIG-IP Edge Client do for Windows Phone?*

What does BIG-IP Edge Client do for Windows Phone?

BIG-IP® Edge Client® for Windows Phone provides full network access through BIG-IP® Access Policy Manager®. With network access, users can run applications such as RDP, SSH, and other enterprise applications on their mobile devices. The BIG-IP Edge Client application for Windows Phone provides the following features:

- Regular logon authentication support for user name and password
- Support for multifactor authentication using client certificates
- Support for client certificate-only authentication
- Support for Access Policy ending redirects
- Support for deployment redirects using GTM and APM

Note: For more information about supported features, refer to *Release Note: BIG-IP Edge Client for Windows Phone 8.1 v1.1*.

Chapter 2

Overview: Access Policies for BIG-IP Edge Client

Topics:

- *About access policy branches for BIG-IP Edge Client*

About access policy branches for BIG-IP Edge Client

You can configure separate access policy branches for BIG-IP® Edge Client®.

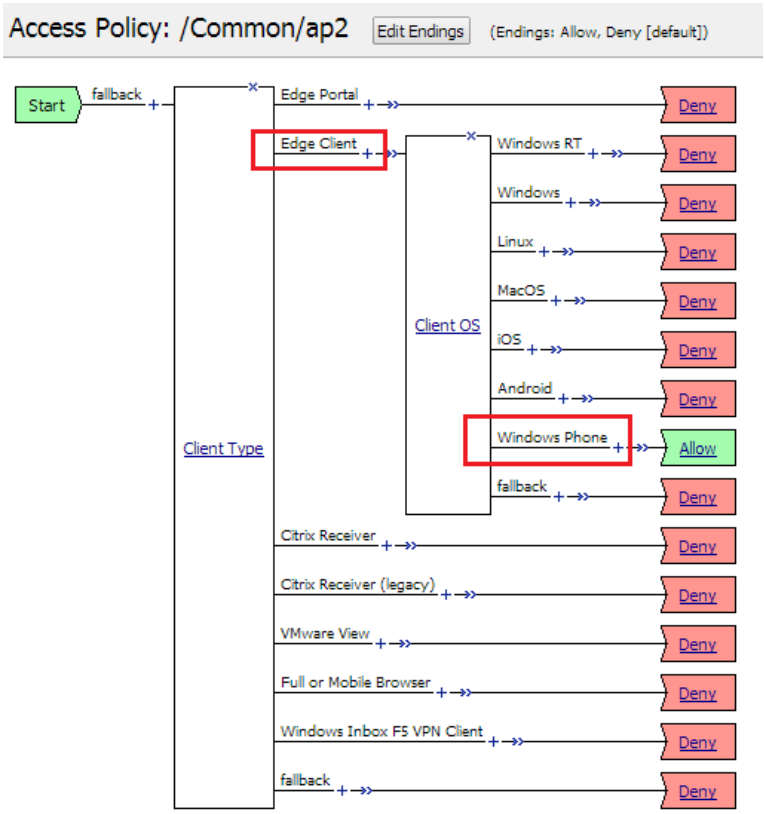
BIG-IP Edge Client does not support client-side checks; however, you can configure an access policy that provides network access for Windows Phone clients by using any of these methods:

- Create an access policy using **Client-Side Check Capability**. This provides a branch for clients that do not support client-side checks. Assign authentication and a network access resource to this branch.
- Use an existing access policy with client-side checks. The Windows Phone client will fail to the fallback branch of the first client-side check. Assign authentication and a network access resource to this branch.
- Create a specific branch for Windows Phone clients. Use the *session.client.platform* variable to identify the client. Add authentication and assign a network access resource for Windows Phone clients to this branch.

Understanding basic access policy that supports BIG-IP Edge Client

You can configure an access policy branch to direct mobile device users to BIG-IP® Edge Client®, and direct non-mobile device users to a fallback branch.

This example displays a simple access policy.



Chapter 3

Overview: Configuring a VPN connection for BIG-IP Edge Client

Topics:

- *About VPN support for BIG-IP Edge Client*
- *About VPN deployment using Airwatch*

About VPN support for BIG-IP Edge Client

You can configure a VPN client plugin for BIG-IP® Edge Client® that integrates with the Windows Phone 8.1 platform. The VPN client collects user credentials and runs inside the Microsoft VPN framework. Windows Phone Edge Client 8.1 version 1.1 also supports client certificate authentication.

Note: The client certificate authentication option must be in request mode.

Creating a new VPN profile

You must first download the F5 BIG-IP Edge Client application from the Microsoft Windows Phone Store before you can create a new VPN profile.

You can create a new VPN connection on the BIG-IP® Edge Client® for Windows Phone.

1. On the main screen of the Windows Phone, tap **Settings** > **VPN**.
   The VPN screen displays.
2. Tap +.
   The Add Profile screen displays.
3. In the **Server name or IP address** field, type the name of the VPN server.
4. In the **Type** field, select **F5 BIG-IP Edge Client**.
5. In the **User name** field, type a user name for the VPN connection.
6. In the **Password** field, type a password for the VPN connection.
7. For the **Connect automatically** option, set the option to **Off**.
8. In the **Profile name** field, type name of the VPN server.
9. Click **Save**.
   The VPN screen displays.
10. Tap the VPN profile that you created.

    The VPN profile displays `not connected, manual` before you tap the profile.

    The VPN profile displays `connected, manual` after you tap the profile.

You have now created a new VPN connection.

Configuring a VPN connection to auto-trigger

You can configure a VPN connection to auto-trigger on the BIG-IP® Edge Client® for Windows Phone.

1. On the main screen of the Windows Phone, tap **Settings** > **VPN**.
   The VPN screen displays.
2. Tap +.
   The Add Profile screen displays.
3. In the **Server name or IP address** field, type the name of the VPN server.
4. In the **Type** field, select **F5 BIG-IP Edge Client**.
5. In the **User name** field, type a user name for the VPN connection.
6. In the **Password** field, type a password for the VPN connection.
7. For the **Connect automatically** option, set the option to **On**.

   By default, this option is turned to setting **On**.
8. Tap **IP ranges**.
   The IP ranges screen displays.
9. Tap +.
   The Add IP range or addresses screen displays.
10. In the **IP range or addresses** field, type an IP subnet in Cisco notation.

11. Tap **Save**.
    The Add Profile screen displays.
12. In the **Profile name** field, type the name of the VPN server.
13. Tap **Save**.

    You cannot tap **Save** if you set **Connect Automatically** to **On** and do not specify an IP range.

    The VPN screen displays.
14. Tap the VPN profile that you created.

    The VPN profile displays `Is ready, automatic` before you tap the profile.

    The VPN profile displays `connected, automatic` after you tap the profile.

You have now configured a VPN connection to auto-trigger based on IP addresses.

Establishing a VPN connection using a provisioned configuration

If you have a previously provisioned VPN configuration, you can connect to the existing VPN connection on the BIG-IP® Edge Client® for Windows Phone.

1. On the main screen of the Windows Phone, tap **Settings** > **VPN**.
   The VPN screen displays.
2. Tap a VPN profile.

   The VPN profile displays `not connected, manual` before you tap the profile.

   The VPN profile displays `connected, manual` after you tap the profile.

You are now connected to an existing VPN connection.

Terminating an existing VPN connection

You can terminate an existing VPN connection on the BIG-IP® Edge Client® for Windows Phone.

1. On the main screen of the Windows Phone, tap **Settings** > **VPN**.
   The VPN screen displays.
2. Tap a VPN profile.

   The VPN profile displays `connected, manual` before you tap the profile.

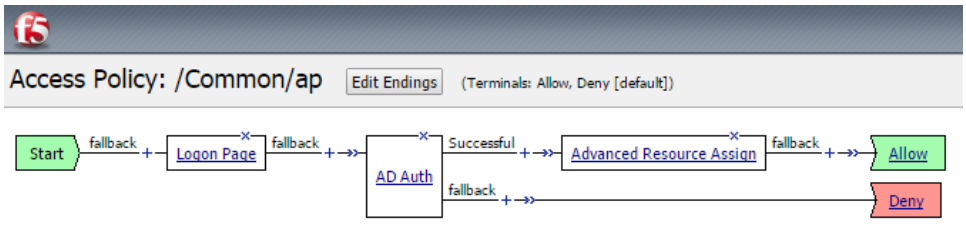
   The VPN profile displays `not connected, manual` after you tap the profile.

You have now terminated an existing VPN connection.

About VPN deployment using Airwatch

You can deploy an F5 VPN profile for Windows Phone 8.1 Edge Client v1.1 using the Airwatch MDM provider. This options provides more options than the standard VPN deployment, such as monitoring the client certificate usage and setting the landing URL.

This example displays a username and password authentication access policy.



Deploying a VPN profile using Airwatch

You can deploy a VPN connection on the BIG-IP® Edge Client® for Windows Phone using Airwatch 8.0.

1. On the Airwatch console, create a custom configuration.

   For more information on creating an Airwatch profile, refer to Airwatch documentation. For more information about custom configuration options, refer to *Release Note: Configuration Notes: Inbox F5 VPN Client for Microsoft Windows 8.1*.
2. Create an access policy in BIG-IP® Access Policy Manager®
3. Install Edge Client and Airwatch applications from the Windows Store.
4. Enroll the device with Edge Client.
   Edge Client deploys the F5 VPN profile.
5. Click the configuration name to connect to the VPN.

You have now deployed an F5 VPN connection profile.