BIG-IP® Access Policy Manager® and BIG-IP® Edge Client™ for iOS v1.0.3

Technical Note

IT agility. Your way.

Contents

Legal Notices

Publication Date

This document was published on February 1, 2012.

Publication Number

MAN-0393-01

Copyright

Trademarks

Patents

This product may be protected by U.S. Patent 7,114,180. This list is believed to be current as of February 1, 2012.

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.

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, *This software* refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. *Similar operating systems* includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

Chapter 1

Overview: BIG-IP Edge Client for Mobile Devices

Topics:

What does BIG-IP Edge Client do for mobile devices?

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

For information about how to use BIG-IP Edge Client, refer to the *BIG-IP® Edge Client™ for iOS User Guide* on your device.

BIG-IP Edge Client features include:

- N-factor auth (at least two input fields, password and passcode) support
- Username and password, client certificate , RSA SecurID support
- Multiple input field support
- Credential caching support
- Support for DNS address space for split tunneling configurations
- Support for checking information from client devices
- Support for automatically launching applications on client devices
- Support for roaming between 3G and WiFi networks
- Landing URI support
- Logging support to report issues
- Support for private-side internal proxy servers

About supported authentication types

The BIG-IP® Edge Client™ app for mobile devices provides the following authentication methods.

Authentication method	Description
VPN On-Demand	Provides the following two options: • Client certificate • Client certificate + Username and Password (no runtime prompt)
Regular Logon	Provides the following two options: • Username and Password • Client certificate + Username and Password (prompt if password is empty)
Web Logon	Provides the following two options: • Username and Password • Username/password + RSA + any other server-side checks  ***Tip:*** *Client certificate is not currently supported for the Web Logon authentication method.*

About establishing VPN connections

The BIG-IP® Edge Client™ app for mobile devices provides users with two options to establish a VPN tunnel connection. A user can start a tunnel connection explicitly with the BIG-IP Edge Client app, or implicitly through the `VPN On-Demand` functionality.

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

VPN On-Demand considerations:

- `VPN On-Demand` is allowed only if the client certificate authentication method is used (legacy logon mode). Username and Password can be used along with the client certificate, but are optional.
- When `VPN On-Demand` initiates a connection, user intervention is not allowed. For example, if a password is needed for authentication, but is not supplied in the configuration, the connection fails. Note that RSA authentication is not supported.
- `VPN On-Demand` supports only two authentication types. After you have imported the configuration profile, using the app you can perform configurations to add additional credential authentication.

About pre-logon checks supported for iOS devices

Access Policy Manager can check unique identifying information from an iOS client device. The supported session variables, which gets populated with the iOS client device information, are gathered automatically and can easily be combined with an LDAP or AD query to implement white-listing in a custom action to improve access context. This information allows Access Policy Manager to perform pre-logon sequence checks and actions based on information about the connecting device. Using such information, Access Policy Manager can perform the following tasks:

- Deny access if the iOS version is less than the required level
- Log UUID and MAC address information

The following example displays an access policy with a custom action of Device ID Check to check the device's UUID.

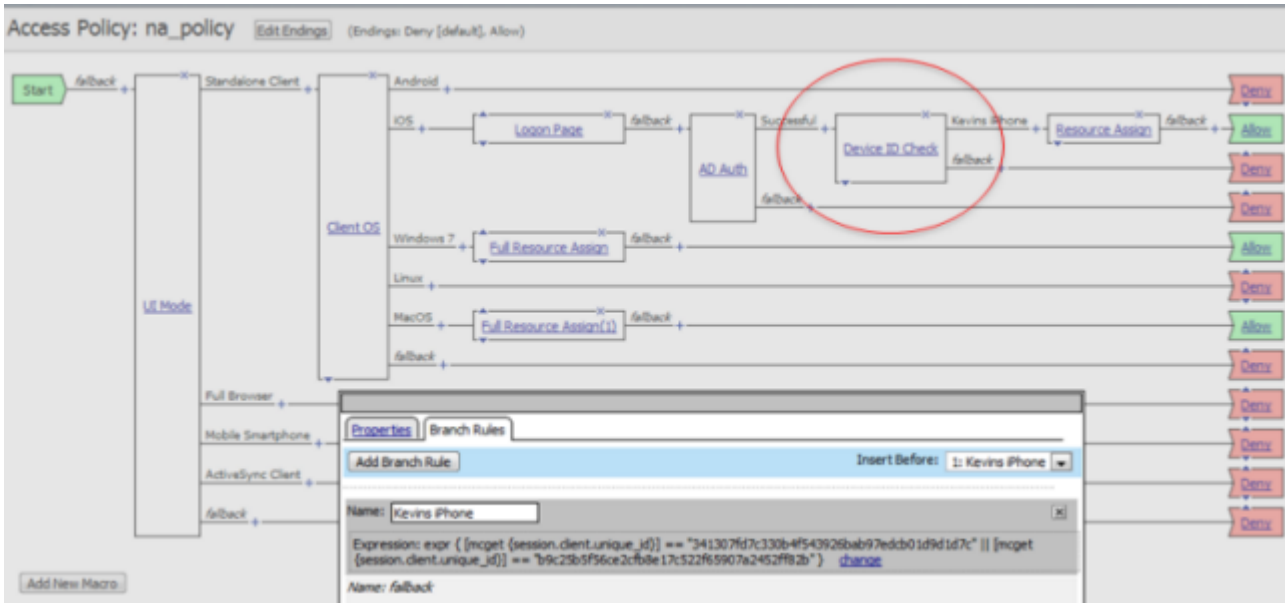


Figure 1: Example of a custom action for checking device's UUID

About automatically launching applications from mobile devices

Web applications can automatically launch from mobile devices when a client authenticates to the *BIG-IP® Edge Client™*. To make this work, the VPN client must support this action.

Task List

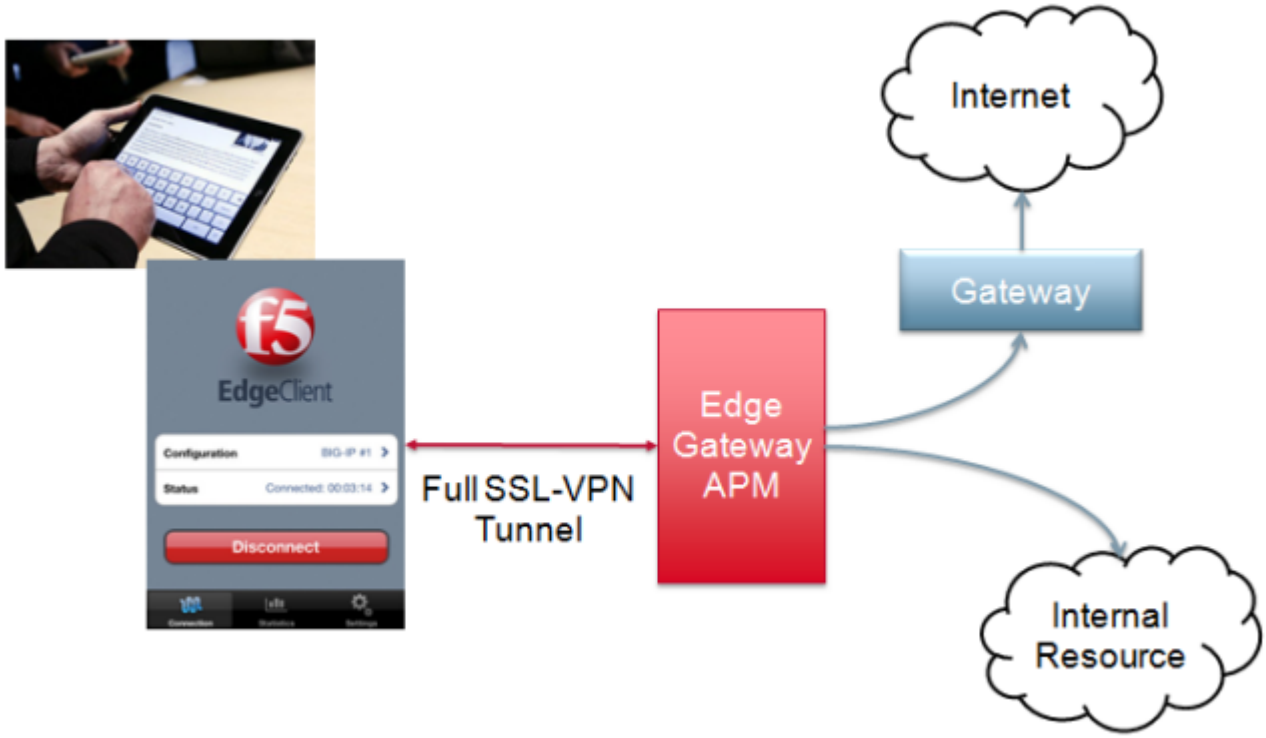
Auto-launching applications from the BIG-IP Edge Client

You can configure applications to automatically start on the BIG-IP Edge Client once a connection is initiated.

1. From the main tab, click **Access Policy**.
2. Navigate to **Network Access**, and select the name of your network access from the list.
3. Select the **Launch Applications** tab.
4. In the **Application Path** field, type in your application path in the form of a URL scheme, for example, `skype://14082734800?call`.
5. From the **Operating System** selection box, select your operating system type.
6. Click **Finished.**
   On the device itself, a pre-launch warning is issued before the local application executes.

About secure web gateway integration on iOS devices

Access Policy Manager provides web application-level security to prevent malware attacks. As as administrator, you can enforce all web access through a secured gateway as well as bypass secure gateways for internal resources. This is especially useful where you have users using corporate iPads, or other mobile devices to browse the web, for example.



Task List

Setting up a secure web gateway

You can force traffic through a tunnel on the BIG-IP Edge Client. Please note that even though you disable **Allow local subnet access** while enabling **Force all traffic through tunnel**, the client will still permit local subnet traffic to travel outside of the tunnel. This is a limitation of iOS and not with the BIG-IP Edge Client.

1. On the **Main** tab, click **Access Policy** > **Network Access** .
   The Network Access List screen opens.
2. Click the name to select a network access resource on the Resource List.
   The Network Access editing screen opens.

   Note: *This screen also opens immediately after you create a new network access resource.*

3. To configure the network settings for the network access resource, click **Network Settings** on the menu bar.
4. Enable **Force all traffic through tunnel**.
   If you enable **Use split tunneling for traffic**, the client will not use the proxy settings.
5. Enable **Allow Local Subnet**.
6. Enable **Client proxy settings**.
7. Under **Client Options**, enable the **Client for Microsoft Networks** check box.
8. Click **Update**.

Chapter 2

Configuring Access Policy Manager for BIG-IP Edge Client

Topics:

Access Policy Manager configuration for BIG-IP Edge Client for mobile devices

To configure BIG-IP® Edge Client™ for mobile devices support on BIG-IP ® Access Policy Manager™, use the following configuration steps.

- Run the Network Access Setup Wizard.
- You can also set up `SSO` and `ACLs` for your network access (optional). Refer to the *BIG-IP Access Policy Manager Configuration Guide* on the AskF5 Knowledge Base for instructions.
- Customize an access policy to support BIG-IP Edge Client.

Running the Network Access Setup Wizard

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

1. On the Main tab, click **Wizards** > **Device Wizards.**
   The Device Wizards screen opens.
2. For Access Policy Manager Configuration, select **Network Access Setup Wizard for Remote Access**, and then click **Next**.
3. In the Basic Properties area of the wizard, clear the **Enable Antivirus Check in Access Policy** check box for Client Side Checks to ensure that your users can connect to BIG-IP Edge Client.
4. Click **Finished**.

You now have network access that supports BIG-IP Edge Client for mobile devices.

Customizing an access policy to support BIG-IP Edge Client on Access Policy Manager 10

Create an access policy that supports BIG-IP Edge Client for iOS.

Note: *This policy applies to Access Policy Manager version 10.x systems.*

1. On the Main tab, click **Access Policy** > **Access Profiles** .
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the profile you want to configure to launch the visual policy editor.
   The visual policy editor opens the access profile in a separate window or tab.
3. Click the plus [+] sign that appears before the `Logon Page` action.
4. Under **Server Side Checks**, select **UI Mode**, and click **Add Item**.
5. Click **Save**.
   The UI Mode action is added to the access policy, and several new branches appear.
6. On the Standalone Client branch of the UI Mode action, click the plus **[+]** sign.
7. Under **General Purpose**, select **Empty**, and click **Add Item**.
8. Click the Branch Rules tab.
9. Click **Add Branch Rule**.

10. Rename the new branch rule **Branch Rule *n*** to **iOS Edge Client**.
11. Next to **Expression: Empty**, click the **change** link.
12. Click the **Advanced** tab.
13. Type the following rule in the box: `expr { [mcget {session.client.platform}] == "iOS" }`
14. Click **Finished**, and then click **Save**.
15. Add the network access resource to the branch.
16. Click **Save**.
    This access policy now supports BIG-IP Edge Client for iOS.

Customizing an access policy to support BIG-IP Edge Client on Access Policy Manager 11

Create an access policy that supports BIG-IP Edge Client for iOS.

Note: *This policy applies to Access Policy Manager version 11.x systems.*

1. On the Main tab, click **Access Policy** > **Access Profiles** .
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the profile you want to configure to launch the visual policy editor.
   The visual policy editor opens the access profile in a separate window or tab.
3. Click the plus [+] sign that appears before the `Logon Page` action.
4. Under **Server Side Checks**, select **Client Type**, and click **Add Item**.
5. Click **Save**.
   The Client Type action is added to the access policy, and several new branches appear.
6. On the Edge Client branch of the Clienty Type action, click the plus **[+]** sign.
7. Under **Server Side Checks**, select **Client OS**, and click **Add Item**.
8. Configure the **iOS** Branch Rule with the configuration objects and resources you want to assign to iOS Edge Client.
9. Click **Finished**, and then click **Save**.
10. Add the network access resource to the branch.
11. Click **Save**.
    This access policy now supports BIG-IP Edge Client for iOS.

Chapter 3

Overview: Access Policies for BIG-IP Edge Client

Topics:

About access policy branches for BIG-IP Edge Client

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

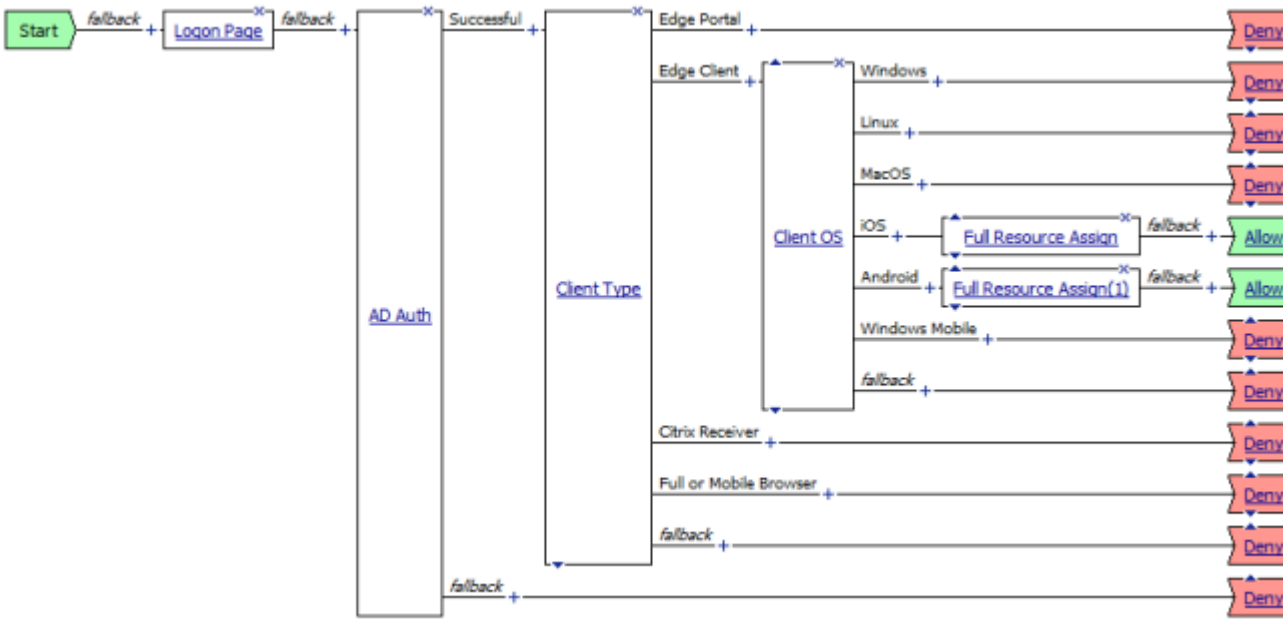
BIG-IP Edge Client does not support client-side checks; however, you can configure an access policy that provides network access for iOS clients with any of the following methods.

- 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 iOS 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 iOS clients. Use an empty action and empty session variables to identify the client. Add authentication and assign a network access resource for iOS clients to this branch.

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.

The following example displays a simple access policy.



Chapter 4

Additional Access Policy Manager Configuration Information

Topics:

Identifying iOS clients using session variables

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

Session variable	Description
session.client.type	Indicates the client type, such as `Standalone`.
session.client.platform	Indicates the platform type, such as iOS.
session.client.agent	Indicates the browser, device type, and operating system version of the client, as well as the version of BIG-IP Edge Client.
session.client.mac_address	Indicates the MAC address of the Wi-Fi adapter. Sample string: `%session.client.mac_address%= '90:21:55:07:4A:32'`
session.client.model	Indicates the model number of the mobile device. Sample string: `%session.client.model%= 'Nexus One'`
session.client.platform_version	Indicates the platform and version of the mobile device. Sample string:`%session.client.platform_version%= '2.3.3'`
session.client.unique_id	Indicates the unique ID of the mobile device. Sample string: `%session.client.unique_id%= '8ccaf965e51e3077'`

Additional Access Policy Manager configuration information

The following table provides tips for setting up the BIG-IP Edge Client for mobile devices.

Feature	Information
VPN On-Demand	A connection cannot be established if the server has an invalid certificate. To work around this issue, manually import the invalid certificate onto the device.
Proxy servers	Public and private-side proxy servers are not currently supported.
Client endpoint checks	Client end-point checks are not currently supported.

Password caching policy	• Under **Client Policy**, if **Enforce session settings** is not enabled, clients can save their encrypted password to disk, regardless of what settings are configured under **Session Settings**.
	• Under the `Password Caching Options`, if you set **Cache password within application for** for a specific amount of time, after a successful logon, the submitted credentials are cached until one of the following occurs:
	  • the specified credential cache duration expires
	  • the server address of the configuration within the app changes
	  • the username of the configuration within the app changes
	  • the BIG-IP Edge Client user switches between configurations and makes a new connection
	  • the configuration is deleted and a new one is created

Feature	Information
	• On the mobile device, even if a user clicks **Disconnect**, terminates the application, or restarts the device, cached credentials are not cleared until the specified cache time.
Client certificates	Client certificate authentication is supported, either with a certificate alone or with a certificate secured with a username and password. Client certificate authentication is not supported for the Web Logon authentication method.
`On-Demand Cert Auth`	If used, the `On-Demand Cert Auth` action must be placed after other authentication actions in the access policy.

Starting the client from a URL scheme

You can start BIG-IP® Edge Client™ connections for users from a URL. You can then provide these URLs to users, so they can start the VPN connection without having to manually start the app. If there is already an active connection, a prompt appears to warn the user that the existing connection must be stopped before the new connection can start. The connection uses a client certificate if it is specified in the existing configuration.

URL connections use the following parameters.

```
f5edgeclient://{start|stop}?[parameter1=value1&parameter2=value2...]
```

Note: *Special characters in parameters must be URL-encoded.*

The syntax to start a connection from a URL follows.

start Starts a connection. The `start` command requires either the `name` or `server` parameter to be present in the URL. If the `name` parameter is specified, then the Edge Client looks for the name in the list of existing configuration entries. If the `server` parameter is specified, then the `name` parameter is set to the same value as the `server`. A new configuration is created if a configuration with that name does not exist. If the specified configuration already exists, the other parameters specified in the URL are merged with the existing configuration. The result of this merged configuration is used only for the current, active connection, and does not persist. If a `name` is specified with other parameters, such as `server`, `username`, or `password`, those parameters override what is specified in the configuration.

sid A parameter used to specify the session ID with which to start the connection. When the parameter `sid` is provided, the `username` and `password` parameters are ignored, and no additional authentication occurs.

username A parameter used to specify the user name with which to start the connection. When the `username` is specified without a `password`, then an authentication prompt is displayed.

password A parameter used to specify the password with which to start the connection. When the `password` parameter is specified, it is used as a one-time password and not saved in the configuration.

postlaunch_url A parameter used to specify the URL that starts after the connection starts.

Examples of starting a client from a URL

The following examples illustrate how to start BIG-IP® Edge Client™ connections for users from a URL.

Connecting to an existing configuration called `MYVPN`

```
f5edgeclient://start?name=MYVPN
```

Connecting to an existing configuration called `MYVPN` and including the server URL `myvpn.siterequest.com`

```
f5edgeclient://start?name=MYVPN&server=
myvpn.siterequest.com
```

Connecting to a specific server called `myvpn.siterequest.com`

```
f5edgeclient://start?server=myvpn.siterequest.com
```

Connecting to an existing configuration called `MYVPN` and including the username `smith` and the password `passw0rd`

```
f5edgeclient://start?name=MYVPN&username=smith&password=
passw0rd
```

Starting a connection to a configuration called `MYVPN` and specifying the post-launch URL `jump://?host=10.10.1.10&username=smith`

```
f5edgeclient://start?name=MYVPN&postlaunch_url=
jump%3A%2F%2F%3Fhost%3D10.10.1.10%26username%3Dsmith
```

Stopping a connection

```
f5edgeclient://stop
```

Index