

**BIG-IP[®] Access Policy Manager[®] and
BIG-IP[®] Edge Client[™] for Android v2.0.6
Technical Note**

Contents

Legal Notices.....	5
Acknowledgments.....	7
Chapter 1: Overview: BIG-IP Edge Client for Mobile Devices.....	11
What does BIG-IP Edge Client do for mobile devices?.....	12
About SAML support.....	12
About supported authentication types.....	12
About establishing VPN connections.....	13
About pre-logon checks supported for Android devices.....	13
About network integration on Android devices.....	13
Setting up a network access.....	14
Chapter 2: Configuring Access Policy Manager for BIG-IP Edge Client.....	15
Access Policy Manager configuration for BIG-IP Edge Client for mobile devices.....	16
Running the Network Access Setup Wizard.....	16
Customizing an access policy to support BIG-IP Edge Client on Access Policy Manager 10.x.....	16
Customizing an access policy to support BIG-IP Edge Client on Access Policy Manager 11.x.....	17
Chapter 3: Configuring a Connectivity Profile with Access Policy Manager	
Version 11.5 and later.....	19
About connectivity profiles.....	20
Creating a connectivity profile.....	20
Overview: Configuring APM for BIG-IP Edge Applications.....	20
Chapter 4: Overview: Access Policies for BIG-IP Edge Client.....	23
About access policy branches for BIG-IP Edge Client.....	24
Understanding basic access policy that supports BIG-IP Edge Client.....	24
Chapter 5: Additional Access Policy Manager Configuration Information.....	25
Android clients using session variables.....	26
Access Policy Manager configuration tips.....	26
About starting the client from a URL scheme.....	27
Examples of starting a client from a URL.....	28
About defining a server from a URL.....	29
Examples of defining a server from a URL.....	29

Legal Notices

Publication Date

This document was published on October 10, 2014.

Publication Number

MAN-0414-03

Copyright

Copyright © 2014, 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.

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.

This product includes Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software developed by Daniel Stenberg. Copyright ©1996 - 2012, Daniel Stenberg, (daniel@haxx.se). All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,
2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

This product includes gson software, distributed under the Apache License version 2.0. Copyright © 2008-2011 Google Inc.

This product includes ec2-tools software, copyright © 2008, Amazon Web Services, and licensed under the Amazon Software License. A copy of the License is located at <http://aws.amazon.com/asl/>.

This product includes Boost libraries, which are distributed under the Boost license (http://www.boost.org/LICENSE_1_0.txt).

This product includes jxrlib software, copyright ©2009 Microsoft Corp. All rights reserved. Distributed under the new BSD license.

This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>).

This product includes libmagic software, copyright © Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995. Software written by Ian F. Darwin and others; maintained 1994- Christos Zoulas.

This product contains OpenLDAP software, which is distributed under the OpenLDAP v2.8 license (BSD3-like).

This product includes node-uuid software, copyright © 2010-2012, Robert Kieffer, and distributed under the MIT license.

This product includes opensv software, which is distributed under the Apache 2.0 license.

This product includes owasp-jave-encoder software, copyright © 2014, Jeff Ichnowski, and distributed under the New BSD license.

Chapter

1

Overview: BIG-IP Edge Client for Mobile Devices

Topics:

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

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 Android User Guide* on your device.

BIG-IP Edge Client features include:

- N-factor auth (at least two input fields, password and passcode) support
- User name and password and client certificate authentication
- Multiple input field support.
- Credential caching support.
- Support for checking information from client devices.
- Support for roaming between 3G and WiFi networks.
- Landing URI support.
- Logging support to report issues.
- Support for certificate-only authentication.

About SAML support

The BIG-IP® Edge Client® application for mobile devices provide the following SAML support:

- SP-initiated access only (e.g. APM acting as the SP).
- Web Logon mode only.

When you use Edge Client as a client performing SP-initiated access, Edge Client first connects to BIG-IP® Access Policy Manager® (APM®). Because there is no assertion, APM redirects the client to the IdP. The IdP then authenticates the user and redirects Edge Client back to the SP with assertion. APM then accepts the assertion and establishes a VPN connection. You can then access backend resources through Edge Client.

You can configure a BIG-IP system by configuring APM as an SP. The access policy that is associated with the configuration assigns a SAML AAA resource followed by a Network Access Resource. For more information about SAML configurations, refer to the *BIG-IP® Access Policy Manager®: Authentication and Single Sign-On* guide.

About supported authentication types

The BIG-IP® Edge Client® application for mobile devices provides these authentication types:

Authentication type	Description
Regular Logon	Provides the following two options: <ul style="list-style-type: none"> • User name and password • Client certificate + user name and password (prompt if password is empty)
Certificate-only	Provides a certificate-only authentication without a user name and password by adding a certificate in the configuration while leaving the user name field empty.
Web Logon	Provides the following three options: <ul style="list-style-type: none"> • User name and password • User name/password + RSA + any other server-side checks • Client certificate authentication (with or without password) in Android 4.3 and earlier (not currently supported in Android 4.4)

About establishing VPN connections

You can use BIG-IP® Edge Client® for mobile devices to establish a VPN tunnel connection.

About pre-logout checks supported for Android devices

Access Policy Manager® can check unique identifying information from an Android client device. The supported session variables, which become populated with the Android 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-logout 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 Android version is less than the required level.
- Log UDID information.

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

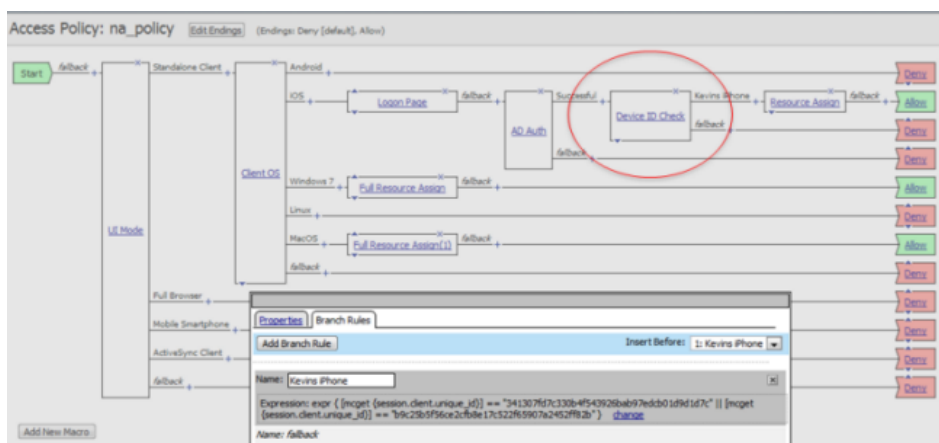
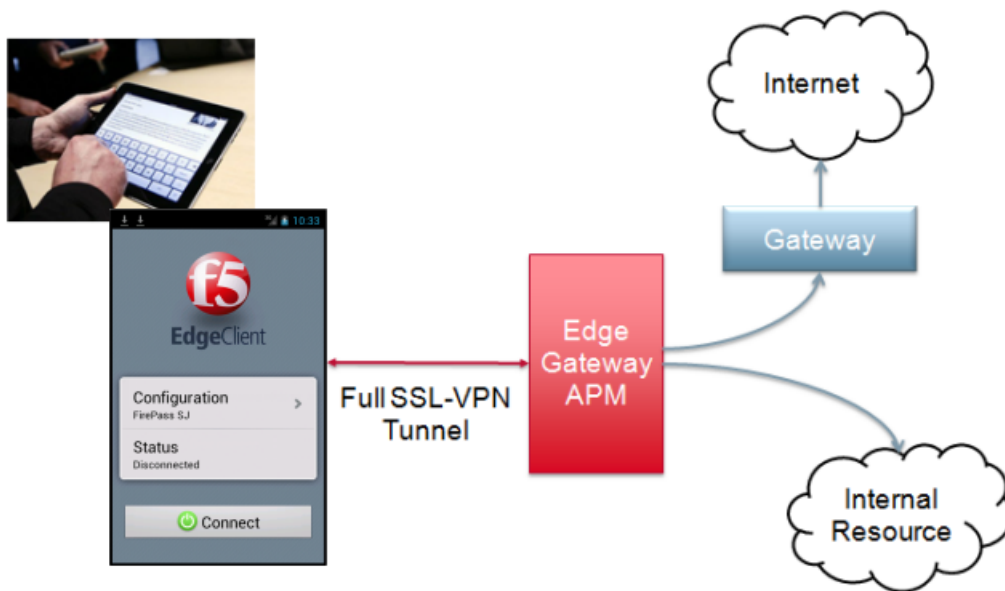


Figure 1: Example of a custom action for checking device's UDID

About network integration on Android devices

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



Setting up a network access

You can force traffic through a tunnel on the BIG-IP® Edge Client®.



Note: Although 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 Android 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 a name in the list to select a network access resource.
The network access properties screen opens.
3. To configure the network settings for the network access resource, click **Network Settings** on the menu bar.
4. For **Traffic Options**, enable **Force all traffic through tunnel**.

If you enable **Use split tunneling for traffic**, the client will use the proxy server if the destination matches the DNS address space or DNS suffixes. If you specify the destination using an IP address, the client will not use the proxy server, even if you include the proxy server in the split tunnel IP LAN address space.

If you enable **Force all traffic through tunnel**, the client will use the proxy server whether you specify the destination using an IP address or a host name.

5. For **Allow Local Subnet**, select the **Enable** check box.
6. For **Client Options**, enable **Client for Microsoft Networks**.
7. 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*](#)

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 these following configuration steps:

- Run the Network Access Setup Wizard.
- You can 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.

 **Important:** To resolve internal addresses with DNS, either the **Network Access DNS Address Space** or **DNS Default Domain Suffix** must be specified in the Network Access configuration. If neither field is configured, internal DNS addresses cannot be resolved. The DNS server must also be configured to resolve internal addresses with DNS.

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.x

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

 **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 screen 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 **Android 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}] == "Android"  && [mcget
{session.client.type}] == "Standalone" }
```

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 Android.

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

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



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 screen 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 Client Type action, click the plus (+) sign.

7. Under **Server Side Checks**, select **Client OS**, and click **Add Item**.

8. Configure the **Android** Branch Rule with the configuration objects and resources you want to assign to Android 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 Android.

Chapter

3

Configuring a Connectivity Profile with Access Policy Manager Version 11.5 and later

Topics:

- [About connectivity profiles](#)
- [Overview: Configuring APM for BIG-IP Edge Applications](#)

About connectivity profiles

In BIG-IP® Access Policy Manager®, a connectivity profile is the profile that you select in a virtual server definition to define connectivity and client settings for a network access session.

The connectivity profile contains:

- Compression settings for network access connections and application tunnels
- Citrix client settings
- Virtual servers and DNS-location awareness settings for BIG-IP Edge Client® for Windows and Mac
- Password caching settings for BIG-IP Edge Client for Windows, Mac, and mobile clients
- Security settings, in addition to password caching, for mobile clients

A connectivity profile is also associated with client download packages that you can customize.

Creating a connectivity profile

You create a connectivity profile to configure client connections for a network access tunnel, application access tunnel, and clients.

1. On the Main tab, click **Access Policy > Secure Connectivity**.
A list of connectivity profiles displays.
2. Click **Add**.
The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.
APM® provides a default profile, **connectivity**.
5. From the Compression Settings folder, click **Network Access** and make changes to the network access compression settings.
The settings specify available compression codecs for server-to-client connections.
The default settings are displayed in the right pane.
6. From the Compression Settings folder, click **App Tunnel** and make changes to the application tunnel compression settings.
The settings specify available compression codecs for server-to-client connections. By default, compression is enabled, but no codecs are selected in the Available Codecs area.
The default settings are displayed in the right pane.
7. Click **OK**.
The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the list.

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

Overview: Configuring APM for BIG-IP Edge Applications

A connectivity profile contains default settings for these mobile clients:

- BIG-IP® Edge Client® for Android
- BIG-IP Edge Portal® for Android
- BIG-IP Edge Client for iOS
- BIG-IP Edge Portal for iOS
- BIG-IP Edge Client for Windows Phone

The settings are security-related. They specify how to handle password caching (disabled by default in all cases), and device or PIN locking (enabled where supported). Customize the available settings to meet your requirements.

Chapter

4

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®.

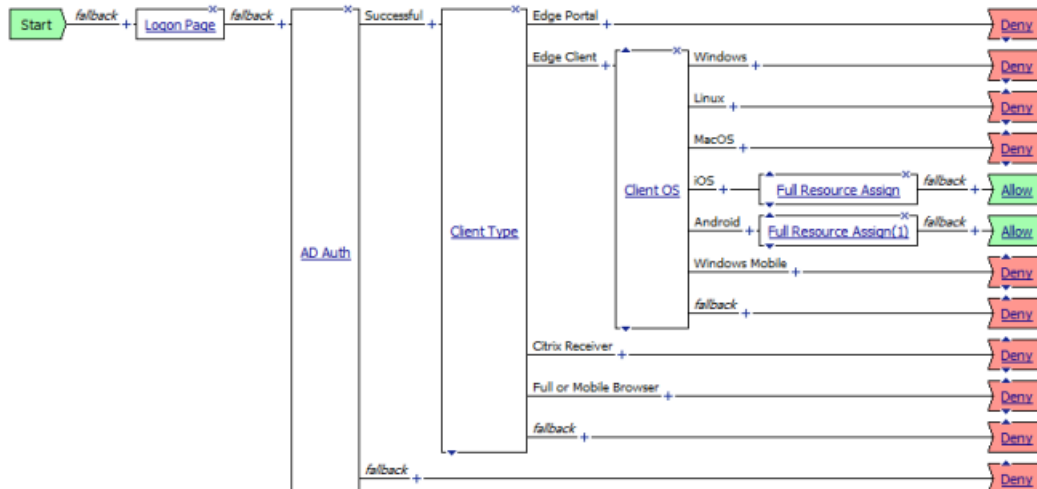
BIG-IP Edge Client does not support client-side checks; however, you can configure an access policy that provides network access for Android clients by using any of these methods:

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

5

Additional Access Policy Manager Configuration Information

Topics:

- [Android clients using session variables](#)
- [Access Policy Manager configuration tips](#)
- [About starting the client from a URL scheme](#)
- [About defining a server from a URL](#)

Android clients using session variables

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

Session variable	Description
<i>session.client.type</i>	Indicates the client type, such as Standalone.
<i>session.client.platform</i>	Indicates the platform type, such as Android.
<i>session.client.agent</i>	Indicates the browser, device type, and operating system version of the client, as well as the version of BIG-IP Edge Client.
<i>session.client.model</i>	Indicates the model number of the mobile device. Sample string: %session.client.model%= 'Nexus One'
<i>session.client.platform_version</i>	Indicates the platform and version of the mobile device. Sample string:%session.client.platform_version%= '2.3.3'
<i>session.client.unique_id</i>	Indicates the unique ID of the mobile device. Sample string: %session.client.unique_id%= '8ccaf965e51e3077'
<i>session.client.jailbreak</i>	Indicates the jailbreak status of the device. Sample string: %session.client.jailbreak%= '0', where 0 indicates the device is not jailbroken, 1 indicates the device is jailbroken, and an empty response indicates that the status of the device is unknown.
<i>session.agent_info.serial_number</i>	Indicates the serial number of the mobile device. Sample string: %session.agent_info.serial_number%= 'HT097P800388'
<i>session.agent_info.imei</i>	Indicates the international mobile equipment identity (IMEI) number of the mobile device. Sample string: %session.agent_info.imei%= '354957034052954'

Access Policy Manager configuration tips

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

Feature	Information
Client endpoint checks	Client end-point checks are not currently supported.
Password caching policy	<ul style="list-style-type: none"> 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 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: <ul style="list-style-type: none"> The specified credential cache duration expires. The server address of the configuration within the application changes. The user name of the configuration within the application 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. On the mobile device, even if a user clicks Disconnect, then terminates the application or restarts the device, cached credentials are not cleared until the specified cache time.

Feature	Information
Client certificates	Client certificate authentication is supported in Web Logoon mode with or without a password. In standard logon mode, certificates are supported, but a password is required. A password (including an empty password) can be saved in the configuration.
On-Demand Cert Auth	If used, the On-Demand Cert Auth action must be placed after other authentication actions in the access policy.

About 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 application (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.

logon_mode	An optional parameter that specifies whether the logon mode is the standard logon (<i>native</i>) or web logon (<i>web</i>). The default logon mode is <i>native</i> .
hide_ui_when_connected	An optional parameter to minimize the BIG-IP Edge Client UI for users when a connection has been established successfully.
fips_mode	An optional parameter to enable a connection compatible with FIPS 140-2 operation mode. The value can be either <i>yes</i> or <i>no</i> . The default value is <i>no</i> . The mode <i>fips_mode=yes</i> cannot be used with <i>logon_mode=web</i> .

Examples of starting a client from a URL

The following examples illustrate how to start BIG-IP® Edge Client® and Edge Client Lite 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 a specific server called myvpn.siterequest.com with web logon enabled:

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

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
```

Minimizing the Edge Client UI:

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

About defining a server from a URL

You can add BIG-IP® server definitions to Edge Client® from a URL. You can provide these URLs to users, so they can start and save VPN connections without having to manually start the application.

Use the following URL and parameters to create a server:

```
f5edgeclient://create?
server=server_address [&parameter1=value1&parameter2=value2...]
```



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

The syntax to define a server from a URL follows.

server	The server address is either a DNS name or an IP address.
name	An optional description of the server.
username	An optional 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. If no username is specified during server creation, the user is prompted for it at session initiation, if required.
password	An optional parameter used to specify the password with which to start the server connection. When the password parameter is specified, it is used as a one-time password and not saved in the configuration.
certcn	Certificate common name. Matches the Common Name of a valid certificate installed through the Edge Client.
logon_mode	An optional parameter that specifies whether the logon mode is the standard logon (<i>native</i>) or web logon (<i>web</i>). The default logon mode is <i>native</i> .
fips_mode	An optional parameter to enable a connection compatible with FIPS 140-2 operation mode. The value can be either <i>yes</i> or <i>no</i> . The default value is <i>no</i> . The mode <i>fips_mode=yes</i> cannot be used with <i>logon_mode=web</i> .

Examples of defining a server from a URL

The following examples illustrate how to define servers for BIG-IP® Edge Client® connections from a URL.

Create a server at edgeportal.siterequest.com:

```
f5edgeclient://create?server=edgeportal.siterequest.com
```

Create a server named EdgePortal with the server URL edgeportal.siterequest.com:

In this scenario, both name and server are specified, and username and certcn are absent, so web logon is assumed.

```
f5edgeclient://create?name=EdgePortal&server=
edgeportal.siterequest.com
```

Create the same server with a user name, password, and certificate:

```
f5edgeclient://create?name=EdgePortal&server=
edgeportal.siterequest.com&username=edgeportal&password=
androiddemo&certcn=clientcert-cert.siterequest.com
```

Create the same server with a user name and certificate:

```
f5edgeclient://create?name=EdgePortal&server=
edgeportal.siterequest.com&username=
edgeportal&certcn=clientcert-cert.siterequest.com
```

Create the same server with a certificate:

```
f5edgeclient://create?name=EdgePortal&server=
edgeportal.siterequest.com&certcn= clientcert-
cert.siterequest.com
```