BIG-IP® Access Policy Manager® and BIG-IP® Edge Client™ for Android v2.0.8

Technical Note

Contents

Legal notices

Publication Date

This document was published on November, 2015.

Publication Number

MAN-0414-03

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*

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 Apache Ant software, distributed by the Apache Software Foundation under the Apache License, version 2.0.

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 opencsv 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.

This product may include Intel SDD software subject to the following license; check your hardware specification for details.

1. LICENSE. This Software is licensed for use only in conjunction with Intel solid state drive (SSD) products. Use of the Software in conjunction with non-Intel SSD products is not licensed hereunder. Subject to the terms of this Agreement, Intel grants to You a nonexclusive, nontransferable, worldwide, fully paid-up license under Intel's copyrights to:

- copy the Software onto a single computer or multiple computers for Your personal, noncommercial use; and
- make appropriate back-up copies of the Software, for use in accordance with Section 1a) above.

The Software may contain the software or other property of third party suppliers, some of which may be identified in, and licensed in accordance with, any enclosed "license.txt" file or other text or file.

Except as expressly stated in this Agreement, no license or right is granted to You directly or by implication, inducement, estoppel or otherwise. Intel will have the right to inspect or have an independent auditor inspect Your relevant records to verify Your compliance with the terms and conditions of this Agreement.

2. RESTRICTIONS. You will not:

a. copy, modify, rent, sell, distribute or transfer any part of the Software, and You agree to prevent unauthorized copying of the Software; and,
b. reverse engineer, decompile, or disassemble the Software; and,
c. sublicense or permit simultaneous use of the Software by more than one user; and,
d. otherwise assign, sublicense, lease, or in any other way transfer or disclose Software to any third party, except as set forth herein; and,
e. subject the Software, in whole or in part, to any license obligations of Open Source Software including without limitation combining or distributing the Software with Open Source Software in a manner that subjects the Software or any portion of the Software provided by Intel hereunder to any license obligations of such Open Source Software. "Open Source Software" means any software that requires as a condition of use, modification and/or distribution of such software that such software or other software incorporated into, derived from or distributed with such software:

a. be disclosed or distributed in source code form; or
b. be licensed by the user to third parties for the purpose of making and/or distributing derivative works; or
c. be redistributable at no charge.

Open Source Software includes, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models substantially similar to any of the following:

a. GNU’s General Public License (GPL) or Lesser/Library GPL (LGPL),
b. the Artistic License (e.g., PERL),
c. the Mozilla Public License,
d. the Netscape Public License,
e. the Sun Community Source License (SCSL),
f. vi) the Sun Industry Source License (SISL),
g. vii) the Apache Software license, and
h. viii) the Common Public License (CPL).

3. OWNERSHIP OF SOFTWARE AND COPYRIGHTS. Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You may not remove any copyright notices from the Software. Intel may make changes to the Software, or to materials referenced therein, at any time and without notice, but is not obligated to

support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right or license under Intel patents, copyrights, trademarks, or other intellectual property rights.

4. Entire Agreement. This Agreement contains the complete and exclusive statement of the agreement between You and Intel and supersedes all proposals, oral or written, and all other communications relating to the subject matter of this Agreement. Only a written instrument duly executed by authorized representatives of Intel and You may modify this Agreement.
5. LIMITED MEDIA WARRANTY. If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety (90) days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.
6. EXCLUSION OF OTHER WARRANTIES. EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel does not warrant or assume responsibility for any errors, the accuracy or completeness of any information, text, graphics, links or other materials contained within the Software.
7. LIMITATION OF LIABILITY. IN NO EVENT WILL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.
8. TERMINATION OF THIS AGREEMENT. Intel may terminate this Agreement at any time if You violate its terms. Upon termination, You will immediately destroy the Software or return all copies of the Software to Intel.
9. APPLICABLE LAWS. Claims arising under this Agreement will be governed by the laws of Delaware, excluding its principles of conflict of laws and the United Nations Convention on Contracts for the Sale of Goods. You may not export the Software in violation of applicable export laws and regulations. Intel is not obligated under any other agreements unless they are in writing and signed by an authorized representative of Intel.
10. GOVERNMENT RESTRICTED RIGHTS. The Software is provided with "RESTRICTED RIGHTS." Use, duplication, or disclosure by the Government is subject to restrictions as set forth in FAR52.227-14 and DFAR252.227-7013 et seq. or their successors. Use of the Software by the Government constitutes acknowledgment of Intel's proprietary rights therein. Contractor or Manufacturer is Intel Corporation, 2200 Mission College Blvd., Santa Clara, CA 95054.

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 Android User Guide* on your device.

BIG-IP Edge Client features include:

- N-factor authentication (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
- Support client certificate for DTLS tunnels and SSL tunnels
- Per-app VPN support for Android 5.0

About SAML support

The BIG-IP® Edge Client ® app for mobile devices provides the following SAML support:

- Service provider-initiated access only, for example, APM acting as the service provider (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 back-end 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® for Android devices provides these authentication types:

Authentication type	Description
Regular Logon	Provides the following two options: • 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: • User name and password • User name/password + RSA + any other server-side checks

Authentication type	Description
	• 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® with an Android device to establish a VPN tunnel connection.

About pre-logon 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-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 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.

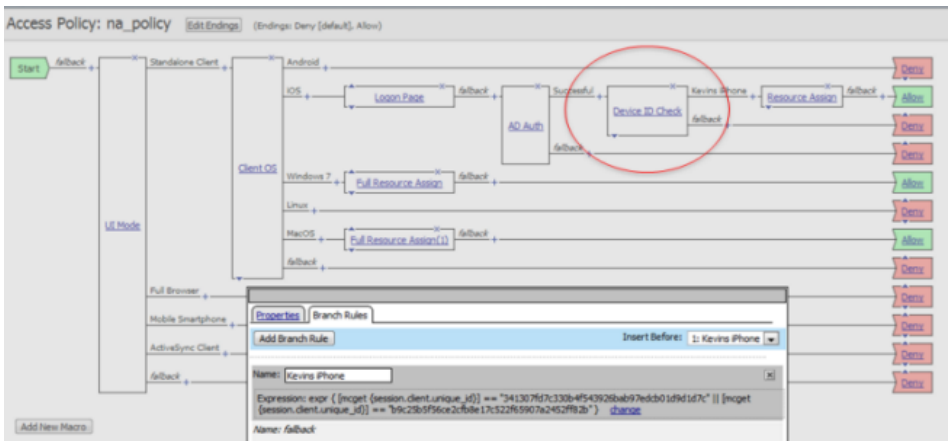
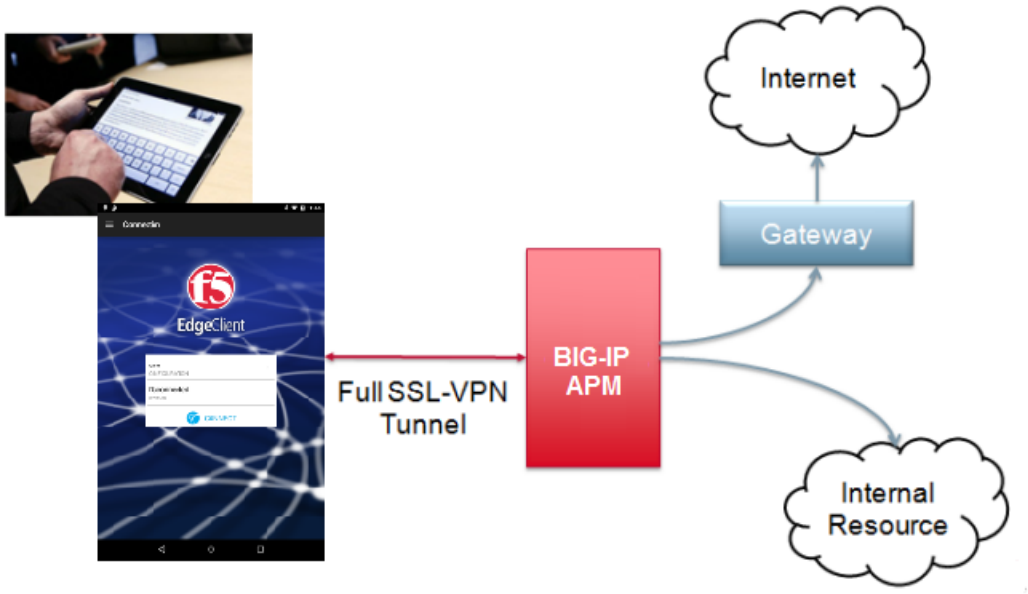


Figure 1: Example of a custom action for checking device's UDID

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.


Internet
Gateway
BIG-IP
APM
Full SSL-VPN
Tunnel
Internal
Resource
EdgeClient

Chapter 2

Configuring Access Policy Manager for BIG-IP Edge Client

Topics:

Prerequisites for configuring Edge Client

Before configuring BIG-IP® Edge Client® for mobile devices, you must complete the following requirements:

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

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

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.
- Optionally, set up SSO and ACLs for your network access. Refer to the *BIG-IP® Access Policy Manager® Configuration Guide* on the AskF5™ Knowledge Base for instructions.
- Customize an access policy to support 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 setting is specified, internal DNS addresses cannot be resolved. The DNS server must also be configured to resolve internal addresses with DNS.

About access policy branches for BIG-IP Edge Client

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

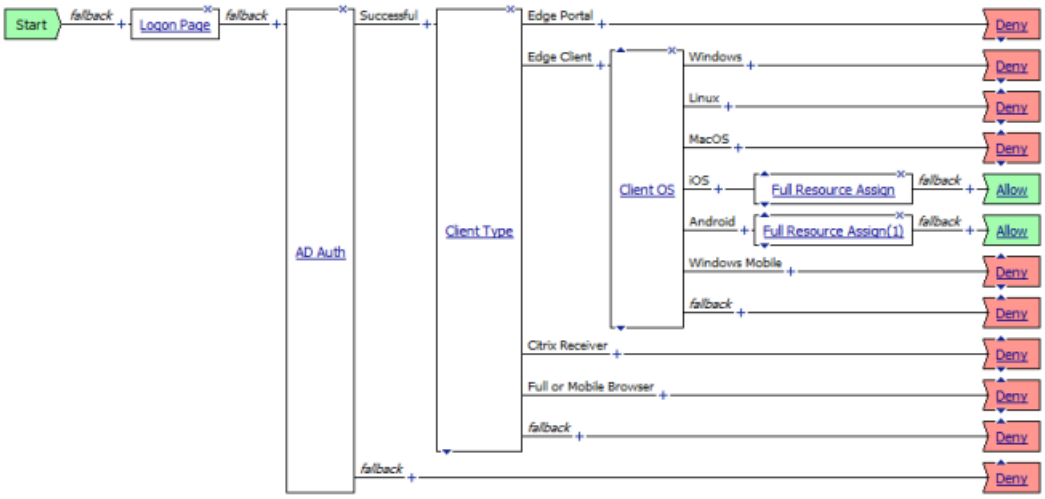
BIG-IP Edge Client does not support client-side checks; however, you can configure an access policy that provides network access for Android clients by using any of these methods:

- 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.



Customizing an access policy to support BIG-IP Edge Client on Access Policy Manager version 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 version 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 Per-App VPN with APM and Edge Client

Topics:

What is per-app VPN?

With Android 5.0, Google enhanced their VPN framework to support application level layer-3 tunneling. Users must first connect with Edge Client manually, then start the app on the device with traffic that is required to go through the VPN tunnel. Admin users can configure a list of allowed apps or disallowed apps; traffic from the "allowed apps" list are able to pass through the VPN tunnel while traffic from the "disallowed apps" list are unable to pass through. Use the allowed apps or disallowed apps URL scheme parameters if the device is not a managed device using a Mobile Device Manager (MDM) solution.

Users can have multiple configurations, but can choose only one at a time. Per-app VPN gives IT granular control over corporate network access, and ensures that data transmitted by managed apps travels only through a separate VPN tunnel and are isolated in the workspace. Meanwhile, other data, like an employee's personal web browsing activity, does not use the VPN. Per-app VPN also works with the mobile browser on a per-app basis on Android 5.0 and later versions. Users with Android for Work should use the same configuration as per-app VPN with Android Edge Client.

A per-app VPN configuration requires four configuration components.

- A device under MDM management.
- A managed app installed on the device, or the mobile browser.
- The Android Edge Client® installed on the managed device. For Android for Work, the Edge Client should be installed within the Android for Work container.
- A related Edge Client configuration (VPN). This is configured with an MDM command that associates the app with an Edge Client configuration.

About access policies for per-app VPN

For per-app VPN, an access policy requires a specific configuration.

Creating an access profile

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

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

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

The access profile appears in the Access Profiles List.

Configure the access policy to include an authentication check.

About setting up Access Policy Manager for per-app VPN

You configure specific settings in the Access Policy Manager® to provide per-app VPN tunnels. Configure these items on the Access Policy Manager.

- The virtual server should be configured with a basic configuration for the network access resource.
- If there is routing required behind the BIG-IP® device, the SNAT Automap should be enabled.

- You must specify the Client SSL profile on the virtual server. You must also include the same CA bundle on the server that is used to generate the authentication check for the client devices.

Configuring a virtual server for per-app VPN

You must have Access Policy Manager® licensed and provisioned.

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

The virtual server is configured for per-app VPN.

Chapter 4

Additional Access Policy Manager Configuration Information

Topics:

Android 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 Android.
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.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'`
session.client.jailbreak	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.
session.client.serial_number	Indicates the serial number of the mobile device. Sample string: `%session.agent_info.serial_number%= 'HT097P800388'`
session.client.imei	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 devices.

Feature	Information
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 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 events occurs:
	  • 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.

Feature	Information
	• 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.
Client certificates	Client certificate authentication is supported in Web Logon 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.

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. 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. This is an example, you must provide your own parameters and values.

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

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

You can start an alternate light client with no client branding, using the following parameters.

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

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 parameter. 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.

cert_url

The URL for downloading a client certificate in .P12 format.

cert_keychain_alias

Identifies a certificate from the device credentials storage.

logon_mode

An optional parameter that specifies whether the logon mode is the standard logon (`native`) or web logon (`web`). The default logon mode is `native`.

hide_ui_when_connected

An optional parameter to minimize the BIG-IP Edge Client user interface 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 `yes` or `no`. The default value is `no`. The mode fips_mode=yes cannot be used with logon_mode=web.

allowed_apps and disallowed_apps

Allows or prevents a list of applications access to the VPN. Only one option can be be used at a given time.

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
```

Identifying a certificate from the device credentials storage:

```
f5edgeclient://create?server=edgeportal.siterequest.com
&name=EdgePortal&cert_keychain_alias=ddd123
```

Stopping a connection:

```
f5edgeclient://stop
```

Minimizing the Edge Client UI:

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

Starting a connection in Lite mode UI:

```
f5edgeclient-lite://start?
name=apm&server=edgeportal.siterequest.com &username=test&x-
cancel=http%3A%2F%2Fgoogle.com &x-error=http%3A%2F%2Fyahoo.com&x-
success=http%3A%2F%2Ff5.com
```

Allowing a list of applications access the VPN:

```
f5edgeclient://start?
allowed_apps=com.android.chrome,org.mozilla.firefox
```

Preventing a list of applications access the VPN:

```
f5edgeclient://start?
disallowed_apps=com.android.chrome,org.mozilla.firefox
```

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.

You can start an alternate light client with no client branding, using the following parameters.

```
f5edgeclient-lite://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.

cert_url

The URL for downloading a client certificate in .P12 format.

cert_keychain_alias

Identifies a certificate from the device credentials storage.

logon_mode

An optional parameter that specifies whether the logon mode is the standard logon (`native`) or web logon (`web`). The default logon mode is `native`.

fips_mode

An optional parameter to enable a connection compatible with FIPS 140-2 operation mode. The value can be either `yes` or `no`. The default value is `no`. The mode `fips_mode=yes` cannot be used with `logon_mode=web`.

allowed_apps and disallowed_apps

Allows or prevents a list of applications access to the VPN. Only one option can be used at any time.

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 the name and server parameters 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
```

Identify a certificate from the device credentials storage:

```
f5edgeclient://create?server=edgeportal.siterequest.com&name=
EdgePortal&cert_keychain_alias=<certificate alias>
```

Stopping a connection in Lite mode:

```
f5edgeclient-lite://stop?x-cancel=edgeportal.siterequest.com &x-
error=http%3A%2F%2Fyahoo.com&x-success=http%3A%2F%2Ff5.com
```

Stopping a connection in Lite mode:

```
f5edgeclient-lite://stop?x-cancel=edgeportal.siterequest.com &x-
error=http%3A%2F%2Fyahoo.com&x-success=http%3A%2F%2Ff5.com
```

Creating a list of applications allowed to access the VPN:

```
f5edgeclient://create?
allowed_apps=com.android.chrome,org.mozilla.firefox
```

Creating a list of applications forbidden to access the VPN:

```
f5edgeclient://create?
disallowed_apps=com.android.chrome,org.mozilla.firefox
```