Access Policy Manager® Tech Note for BIG-IP® Edge Portal™ App

Version 1.0.3

Table of Contents

Legal Notices

Publication Date

This document was published on July 14, 2013.

Publication Number

MAN-0478-00

Copyright

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, Alive With F5, APM, Application Acceleration Manager, Application Security Manager, 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, Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, Scale^{N}, Signalling Delivery Controller, SDC, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TMOS, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, VIPRION, vCMP, VE F5 [DESIGN], Virtual Clustered Multiprocessing, WA, WAN Optimization Manager, WebAccelerator, WOM, 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 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/ .

Chapter 1

What is Edge Portal?

The BIG-IP® Edge Portal™ app streamlines access to portal access web sites and applications that reside behind a BIG-IP ® Access Policy Manager™. Using the BIG-IP® Edge Portal™ app, users can access internal web pages and web applications securely, as allowed by the BIG-IP ® Access Policy Manager™ Portal Access configuration.

For information on how to use the BIG-IP® Edge Portal™ App, refer to the online user guide in the app.

Edge Portal app features include:

- Username and password authentication
- Passcode lock enforced on the device
- Client certificate support
- Saving credentials and sessions
- Saving local bookmarks and favorites
- Accessing bookmarks with keywords
- Embedded web viewer
- Display of all file types supported by the device's operating system

Chapter 2

BIG-IP Edge Portal user-agent string

BIG-IP® Edge Portal sends version information in the user-agent string.

BIG-IP® Edge Portal™ sends Edge Portal version information, along with browser information, in the user-agent string. The following are examples of user-agent strings for Edge Portal. You can use this version information, which is stored in the session variable *session.user.agent*, to make policy decisions.

Device OS	Example user-agent string
Android	`Mozilla/5.0 (Linux; U; Android 2.2; en-us; SGH-T849 Build/FROYO) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1 EdgePortal/1.0.0`
iOS	`Mozilla/5.0 (iPad; U; CPU OS 3_2_2 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Mobile/7B500 EdgePortal/1.0.1`

Chapter 3

Task summary for Edge Portal configuration

To set up this configuration, perform the procedures in the task list.

Task List

Running the portal access setup wizard

Running the portal access setup wizard quickly sets up an access policy and a virtual server for you.

1. Follow the instructions in the wizard to create your access policy and virtual server.
2. Configure the following settings to ensure that your users can connect to the Edge Portal app:
   a) Uncheck the **Enable Antivirus Check in Access Policy** box.
   b) In the **Web Application start URI** box, type the starting URI for your web application
   c) In the **Virtual Server IP address** box, type the IP address for your virtual server.
3. Click **Finished**.

You have just completed configuring a portal access resource to support the Edge Portal app.

The next task is to assign ACLs to your access policy.

Assigning ACLs to your access policy

Before you assign ACLs to an access policy, you must:

- Define a web application resource
- Create an access profile

Add ACLs to limit access to resources.

1. Create or select an existing **Access Policy**.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure to launch the visual policy editor.
   The visual policy editor opens the access policy in a separate screen.
3. On an access policy branch, click the plus symbol (+) to add an item to the access policy.
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
4. Click the **Assignment** tab, select **ACL Assign**, and click **Add Item**.

5. Click the **Add/Delete Static ACLs** link.
6. Select ACLs to assign to your access policy, and click **Save** when finished.
7. Click **Apply Access Policy**.

Your next task is to disable the Home tab. If this is enabled, it's likely that the Edge Portal app will not render properly.

Disabling the Home tab

Disabling the Hometab will ensure that the Edge Portal app renders properly.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click on the name of your access policy that you created.
3. Select the Access Policy tab.
4. In the Web Applications section, click the entry that begins with the name you created.
5. Under the **Resource Items Properties** section, make sure the Home Tab option is unchecked. If not, uncheck the Enabled box.
6. Click **Update**.

Configuring password caching for Edge Portal in APM 11.3.x and earlier

You configure password caching on the server to simplify the user experience with the Edge Portal app, and to require screen lock security on the Edge Portal device.

Note: *Use this procedure with Access Policy Manager® 11.3.x and earlier.*

1. Navigate to **Access Policy** > **Secure Connectivity** > **Connectivity Profiles**.
2. Click the name of the connectivity profile associated with the Web Applications configuration.
3. Click the **Client Configuration** tab.
4. In the Session Settings section, next to General, select the check box **Enable User Password Caching**.
5. Select the password caching option you want to use.

Option	Description
Allow user to save encrypted password on disk	Allows the user to save the encrypted password on the device without a time limit.
Cache password within application for *x* minute(s)	Specifies that the user password is cached in the application on the user's device for the specified period of time.

6. In the Client Policy section, next to Session Policy, select the check box **Enforce session settings (do not allow users to change session settings)**.
7. Click **Update**.

Password caching is configured for the time period you set. Users are required to configure security to connect to the server. The minimum security requirement is a 4-digit PIN. Edge Portal supports password

locking, and does not support pattern locking. If a user attempts to unlock the device five times unsuccessfully, the cached credentials are deleted from the device.

Configuring password caching for Edge Portal in APM 11.4 and later

You configure password caching on the server to simplify the user experience with the Edge Portal app, and to require screen lock security on the Edge Portal device.

Note: *Use this procedure with Access Policy Manager® 11.4.0 and later.*

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Highlight the connectivity profile associated with the Web Applications configuration and click **Edit Profile**.
   The Edit Connectivity Profile screen pops up.
3. From Mobile Client Settings in the left pane, select **iOS Edge Portal**.
   Settings for the iOS Edge Portal display in the right pane.
4. Select the **Allow Password Caching** check box.
5. From **Save Password Method**, select the password caching option you want to use: **disk** or **memory**.
   Selecting **disk** allows the user to save the encrypted password on the device without a time limit. Selecting **memory** specifies that the user password is cached in the application on the user's device for a configurable period of time.
6. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
7. Keep **Enforce Pin Lock** set to **Yes** to support screen lock security.
   Edge Portal supports pin locking, and does not support pattern locking.
8. Type the **Maximum Grace Period (minutes)**
   Defaults to 2.

Password caching is configured for the time period you set. Users are required to configure security to connect to the server. The minimum security requirement is a 4-digit PIN. If a user attempts to unlock the device five times unsuccessfully, the cached credentials are deleted from the device.

Customizing an access policy to support Edge Portal app

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 **Add New Macro**.
4. In the **Select macro template:** select Client Classification and Prelogon checks from the drop-box.
5. Click **Save**.
6. Click the plus [+] sign that appears before the Logon Page action.

7. In the Macrocalls section, click the **Client Classification and Prelogon checks** button.
8. Click **Add item**.
   The Client Classification and Prelogon checks action appears in the access policy sequence.
9. Click the underlined word **Deny** in the ending box.
10. In the Select Ending: section, click **Allow**.
11. Click **Save**.
    You have just customized your access policy to support the Edge Portal app.

Chapter 4

About access policies for Edge Portal app

In your configuration, you might be required to configure separate access policy branches for Edge Portal app.

Edge Portal app does not support client-side checks. There are a number of ways you can configure an access policy to allow a connection to a web applications resource for iOS clients. Access Policy Manager allows flexibility when configuring access policies, so there are many possible ways to configure for Edge Portal clients. The following methods can work:

- Start the access policy with the Client-Side Check Capability check. This provides a branch for clients that do not support client-side checks, including mobile devices. Assign authentication and a web applications resource to this branch.
- Use an existing access policy with client-side checks. The mobile device will fail to the fallback branch of the first client-side check. Assign authentication and a web applications resource to this branch.
- Create a specific branch for mobile clients. You can use an empty action and session variables to identify the mobile client. On the branch you identify for mobile clients, add authentication and assign a web applications resource for mobile devices.

Access policy example

To differentiate the Edge Portal™ application for mobile devices from other client types and operating systems, you can use the **Client Classification and Prelogon Checks** macro.

The following information applies to this macro, and the access policy items configured within it:

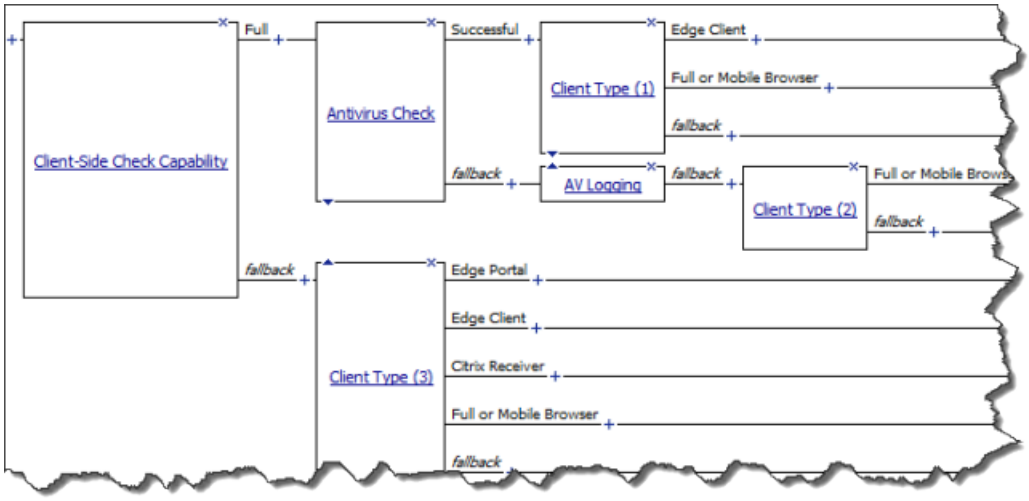
1. Client-side check capability. This checks that the client is capable of running client-side checks, and if the client is capable, an antivirus check is run. If the client is not capable of running client-side checks, it falls back to a client type check.
2. The client type check is an empty agent that is configured with branch rules for several client types, which you can view and edit on the **Branch Rules** page. The simple branch rule for Edge Portal is **Expression: Client is Portal Client**. The **Advanced** tab shows the full expression:

```
expr { [mcget {session.client.type}] == "portalclient" }
```

3. To obtain more information about client OS version or device type, you can inspect the *user-agent* session variable. For example, Edge Portal application uses the following user-agent strings, depending on OS version and device type:

Mobile Device Type	OS version	user-agent session variable
iPhone with iOS 5	5.0	*Mozilla/5.0 (iPhone; CPU iPhone OS 5_0 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Mobile/9A334 EdgePortal/1.0.3*
iPad	6.1.3	*Mozilla/5.0 (iPad; CPU OS 6_1_3 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Mobile/10B329 EdgePortal/1.0.3*
iPod Touch	5.0	*Mozilla/5.0 (iPod; U; CPU iPhone OS 5_0 like Mac OS X; en-us) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A334 Safari/7534.48.3 Safari/6533.18.5 EdgePortal/1.0.3*

Figure 1: Advanced access policy to support Edge Portal



Index