BIG-IP® Access Policy Manager®: Edge Client® and Application Configuration

Version 11.4

Table of Contents

Legal Notices

Publication Date

This document was published on May 15, 2013.

Publication Number

MAN-0462-00

Copyright

Trademarks

Access Policy Manager, Advanced Client Authentication, Advanced Routing, APM, 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 Management Pack, F5 Networks, F5 World, Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iApps, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, Message Security Manager, MSM, OneConnect, OpenBloX, OpenBloX [DESIGN], Packet Velocity, Policy Enforcement Manager, PEM, Protocol Security Manager, PSM, Real Traffic Policy Builder, Rosetta Diameter Gateway, Scale^{N}, Signaling Delivery Controller, SDC, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TMOS, Traffic Management Operating System, Traffix Diameter Load Balancer, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, VIPRION, vCMP, 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 U.S. Patent 7,114,180; 8,301,837. This list is believed to be current as of May 15, 2013.

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.

Chapter 1

BIG-IP Edge Client for Windows

About installation choices for BIG-IP Edge Client on Windows

The BIG-IP® Access Policy Manager® includes automatic installation support for Windows clients. Access Policy Manager (APM®) downloads components to the end user's computer at initial login. These downloaded client components enable the various features of the Access Policy Manager functionality.

This download occurs automatically for those systems that support software installation. For clients that do not support automatic software installation, you can configure and distribute the BIG-IP Edge Client®, configured to meet the needs of the client systems you support.

The requirements for automatic installation differ depending on whether the Windows client initiates a session from a browser, or instead starts a network access tunnel.

- To automatically install a control from a browser session, the controls require certain conditions:
  - The user must have ActiveX enabled if the browser is Internet Explorer.
  - If the browser is not Internet Explorer, the user must allow software installation.
- If the client starts a network access tunnel, one of the following must be true:
  - The client has Administrator privileges on the client system.
  - The client control is already installed on the system.
  - The Component Installer Package for Windows has been installed on the system.

Access policy sessions other than network access tunnels do not require administrative access. All client-side checks and actions, except the Windows group policy action, can run without administrative rights.

Overview: Configuring APM for BIG-IP Edge Client for Windows

To use the BIG-IP® Edge Client® for Windows, you must configure settings for the BIG-IP Edge Client for Windows in a connectivity profile on Access Policy Manager® (APM). The connectivity profile for Windows includes Win/Mac Edge Client settings including:

- The list of servers to display on the BIG-IP Edge Client
- DNS settings for location-awareness for mobile clients, such as laptops that roam.

A Windows client package is attached to the connectivity profile. APM® can use it for automatic installation on Windows systems. You can customize the Windows client package. You can also download and distribute it.

Task Summary

Customizing a connectivity profile for BIG-IP Edge Clients for Windows
Customizing the Windows client package for BIG-IP Edge Client
Downloading the Windows client package for BIG-IP Edge Client

About location awareness

The BIG-IP® Edge Client™ provides a location awareness feature. Using location awareness, the client connects automatically only when it is not on a specified network. You can specify the networks that are considered in-network by adding DNS suffixes to the connectivity profile.

Customizing a connectivity profile for BIG-IP Edge Clients for Windows

You must create a connectivity profile before you start this task.

A connectivity profile automatically contains settings for BIG-IP® Edge Client® for Windows. You update the settings to specify how to handle password caching and component updates, to specify the servers to display on the clients, and to supply DNS names to support location awareness.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From the left pane of the popup screen, select **Win/Mac Edge Client**.
   Edge Client action and password caching settings display in the right pane.
4. Set Edge Client action settings:
   a) (Optional) Retain the default (selected) or clear the **Save Servers Upon Exit** check box.

      Specifies whether the BIG-IP Edge Client maintains a list of recently used Access Policy Manager servers. The BIG-IP Edge Client always lists the servers defined in the connectivity profile, and sorts the list of servers by most recent access, whether this option is selected or not. However, the BIG-IP Edge Client lists user-entered servers only if this option is selected.

   b) (Optional) Select the **Reuse Windows Logon Session** check box.

      When selected, the client tries to use the Windows login session for the APM session also. This is cleared by default.

   c) Select the **Reuse Windows Logon Credentials** check box.

      When selected, the client tries to use the credentials that were typed for Windows login to start the APM session.

      Note: *To use this option, you must also include the User Logon Credentials Access Service in the customized Windows client package for this connectivity profile.*

      ---

5. Set password caching settings for enhanced security:
   a) (Optional) Select the **Allow Password Caching** check box.

      This check box is cleared by default.

      The remaining settings on the screen become available.

   b) (Optional) From the **Save Password Method** list, select **disk** or **memory** .

      If you select **disk**, an encrypted password is saved on disk and cached when the system reboots or when the BIG-IP Edge Client is restarted.

      If you select **memory**, the BIG-IP Edge Client caches the user's password within the BIG-IP Edge Client application for automatic reconnection purposes.

      If you select **memory**, the **Password Cache Expiration (minutes)** field displays with a default value of 240.

   c) If the **Password Cache Expiration (minutes)** field displays, retain the default value or type the number of minutes to save the password in memory.

6. From the **Component Update** list, select **yes** (default), **no**, or **prompt** .

   If you select **yes**, APM updates the BIG-IP Edge Client software automatically on the Windows client when newer versions are available. This option applies to updates for the BIG-IP Edge client, but not to other client components. When updating the other client components, prompts are controlled by your

browser security settings, the publisher of the update package, and the presence of the F5 Networks Component Installer Service.

7. From the left pane of the popup screen, select **Server List**.
   A table displays in the right pane.
8. Specify the servers that you want defined in the client downloads.

   The servers you add here appear as connection options in the BIG-IP Edge Client.

   a) Click **Add**.
      A table row becomes available for update.
   b) You must type a host name in the **Host Name** field.

      Typing an alias in the **Alias** field is optional.
   c) Click **Update**.
      The new row is added at the top of the table.
   d) Continue to add servers, and when you are done, click **OK**.

9. From the left pane of the popup screen, select **Location DNS List**.
   Location DNS list information is displayed in the right pane.
10. Specify DNS suffixes that are considered to be in the local network.

    DNS suffixes specified here conform to the rules specified for the local network. When the BIG-IP Edge Client is configured to use the option Auto-Connect , the client connects when the systems DNS suffix is not one defined on this list. When the client DNS suffix does appear on this list, the client automatically disconnects. If you do not specify any DNS suffixes, the option Auto-Connect does not appear in the downloaded client.

    a) Click **Add**.
       An update row becomes available.
    b) Type a name and click **Update**.
       The new row displays at the top of the table.
    c) Continue to add DNS names and when you are done, click **OK**.

11. 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 to a virtual server.

Customizing the Windows client package for BIG-IP Edge Client

You must create a connectivity profile before you start this task.

You customize a Windows client package for a connectivity profile to select the components to install, and to specify settings for BIG-IP® Edge Client® (if you include the component), and for Dialup Settings if you need them.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Select a connectivity profile.
3. Click the **Customize Package** button.
   The Customize Windows Client Package popup screen displays with Available Components displayed. Most components are selected by default.
4. Clear the check box for any component that you want to exclude from the package.

If you clear the **BIG-IP Edge Client** check box, **BIG-IP Edge Client** is no longer available for selection in the left pane.

If you clear the **Dialup Entry/Windows Logon Integration** check box, **Dialup Settings** is no longer available for selection in the left pane.

5. Select the **User Logon Credentials Access Service** check box to include the software service that allows the client to store encrypted Windows logon credentials and use those credentials to log in to Access Policy Manager®.
6. Select the **Machine Certificate Checker Service** check box to include a service that can check the machine certificate on a client endpoint even when the user does not have admin privilege.

   Without this service, a user running without admin privilege cannot pass the Machine Cert Auth endpoint security check.
7. If the BIG-IP Edge Client check box is selected, select **BIG-IP Edge Client** from the left pane.

   BIG-IP Edge Client settings display in the right pane.
   a) To add the virtual servers (from the Windows/Mac Edge Client section of the connectivity profile) to the Windows Trusted sites list the first time the client starts. retain selection of the the **Add virtual server to trusted sites list** check box. Otherwise, clear it.

      Virtual servers added to the Trusted sites list with this option remain on the trusted sites list indefinitely. This works with the User Logon Credentials Access Service setting (available on the Available Components screen) to provide seamless logon with the BIG-IP Edge Client™ if Access Policy Manager accepts the same credentials that users use to log on to Windows.
   b) To automatically start the BIG-IP Edge Client™ after the user logs on to Windows, retaing selection of the **Auto launch after Windows Logon** check box. Otherwise, clear it.
   c) To enable the BIG-IP Edge Client to try to connect to VPN right after the user logs on to Windows and to prohibit the user from disconnecting VPN, select the **Enable always connected mode** check box. This setting is cleared by default.

      The user is prevented from accessing the Internet and the local network until a VPN connection is established.
8. Click **Download**.

   The screen closes and the package, `BIGIPEdgeClient.exe`, downloads.

The customized package, `BIGIPEdgeClient.exe`, is downloaded to your client. It is available for you to distribute, if needed. The customized package is downloaded to clients automatically only when the Windows/Mac Edge Client settings in the related connectivity profile allow password caching and component updates.

Downloading the Windows client package for BIG-IP Edge Client

You can download a Windows client package and distribute it to clients whose configuration does not allow an automatic download.

Note: *If you have already customized a Windows client package for a connectivity profile, a customized package file,* `BIGIPEdgeClient.exe`*, was downloaded to your system. If you cannot find the package, use this procedure.*

---

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Select a connectivity profile.
3. Click the **Customize Package** button.

The Customize Windows Client Package popup screen displays with Available Components displayed. Most components are selected by default.

4. Click **Download**.

   The screen closes and the package, `BIGIPEdgeClient.exe`, downloads.

The customized package, `BIGIPEdgeClient.exe`, is downloaded to your client. It is available for you to distribute, if needed. The customized package is downloaded to clients automatically only when the Windows/Mac Edge Client settings in the related connectivity profile allow password caching and component updates.

Overview: Downloading the Component Installer

Installing and running a BIG-IP® APM® component on Windows-based systems require certain user rights. Pre-installing components provides a seamless upgrade for clients after you upgrade the BIG-IP® Access Policy Manager®.

You can also use the Component Installer feature to provide completely transparent installation and upgrading of components, regardless of the rights you are running under. Your security policy may prohibit granting users the power-user rights needed to install ActiveX components, or your browser security policy may prohibit downloading active elements. For these reasons, you might prefer to pre-install components on your users Windows systems.

You can use the Clients Download screen to download the Component Installer Package containing the Windows components needed for the various Access Policy Manager functions. You can use the Component Installer service to install and upgrade client-side Access Policy Manager components for all kinds of user accounts, regardless of the rights under which the user is working.

This component is especially useful for installing and upgrading client-side components when the user has insufficient rights to install or upgrade the components directly. For information about configuring the MSI installer to run with elevated privileges, see the documentation for your operating system. You must use an account that has administrative rights to initially install the Component Installer on the client computer as a part of Client Components Package (MSI). Once installed and running, the Component Installer automatically installs and upgrades client-side Access Policy Manager components. It can also update itself. The Component Installer requires that the installation or upgrade packages be signed using the F5 Networks certificate or another trusted certificate. By default, F5 Networks signs all components using the F5 Networks certificate.

Downloading the Component Installer package

You must use an account that has administrative rights to initially install the Component Installer on the client computer as a part of the Client Components Package (MSI). The Component Installer requires that the installation or upgrade packages be signed using a trusted certificate.

Your security policy may prohibit granting users the power-user rights needed to install ActiveX components, or your browser security policy may prohibit downloading active elements. As a workaround, you can pre-install client components on your Windows system.

1. On the Main screen, click the F5® logo to display the Welcome page.
2. In the Downloads section, click the **Component Installer Package for Windows** link.

The MSI installer downloads to your local folder.

User rights requirements for endpoint security checks

This table lists user rights required to use endpoint security components on Windows clients from a network access tunnel.

Access Policy Manager plugin	Guest rights	User rights	Power User rights	Administrator rights
Antivirus	No supported	Supported	Supported	Supported
Firewall	No supported	Supported	Supported	Supported
Windows File	No supported	Supported	Supported	Supported
Machine Cert	No supported	Supported	Supported	Supported
Windows information	No supported	Supported	Supported	Supported
Windows Process	No supported	Supported	Supported	Supported
Registry	No supported	Supported	Supported	Supported
UI mode	Supported	Supported	Supported	Supported
Client-Side Capability	Supported	Supported	Supported	Supported
Client OS	Supported	Supported	Supported	Supported
Landing URI	Supported	Supported	Supported	Supported
Logging action	Supported	Supported	Supported	Supported
Anti-Spyware	Supported	Supported	Supported	Supported
Hard Disk Encryption	Supported	Supported	Supported	Supported
Patch Management	Supported	Supported	Supported	Supported
Peer-to-peer	Supported	Supported	Supported	Supported
Windows Cache and Session Control	Supported	Supported	Supported	Supported

User rights requirements for access policy actions

This table lists user rights required on Windows clients to use actions other than endpoint security client checks from a network access tunnel.

Access Policy Manager component	User rights	Power User rights	Admin rights
Client Cert Inspection	Supported	Supported	Supported
On-Demand Cert Auth	Supported	Supported	Supported
Active Directory (auth or query)	Supported	Supported	Supported
HTTP Auth	Supported	Supported	Supported
LDAP (auth or query)	Supported	Supported	Supported

Access Policy Manager component	User rights	Power User rights	Admin rights
RADIUS (auth or accounting)	Supported	Supported	Supported
RSA SecurID	Supported	Supported	Supported

Overview: Downloading FullArmor GPAnywhere for VPN

This download enables the FullArmor GPAnywhere management tool for VPN integration with Windows clients. You can use this tool to create Group Policy templates, which you can then use to apply Group Policy to computers outside of an Active Directory domain. With VPN, you can distribute Group Policy Object templates through SSL VPN.

Downloading FullArmor GPAnywhere for VPN

Download an installer that enables FullArmor GPAnywhere integration with Windows clients. You can use FullArmor GPAnywhere to apply Group Policy to computers that are not part of an Active Directory domain, and distribute Group Policy templates through SSL VPN to manage and secure the computers.

1. On the Main screen, click the F5 logo to display the welcome page.
2. In the Downloads section, click the **FullArmor GPAnywhere for VPN** or the **FullArmor GPAnywhere for VPN (x64 edition)** link.

The MSI installer downloads to your local folder.

Overview: Installing and using the client troubleshooting utility

Access Policy Manager® provides a client troubleshooting utility for BIG-IP® Edge Client® on Windows. Clients can use the client troubleshooting utility on Windows systems to check the availability and version information for Windows client components, and run Network Access diagnostic tests.

Task Summary

Downloading the client troubleshooting utility
Viewing client components in the client troubleshooting utility
Generating a client troubleshooting report
Running a Network Access diagnostic test

Downloading the client troubleshooting utility

You must download this client troubleshooting utility if you want to run it on Windows.

1. On the main screen, click the F5 logo to display the Welcome page.
2. In the Downloads section, click the **Client Troubleshooting Utility for Windows** link.

The file `f5wininfo.exe` is saved to your local disk.

Viewing client components in the client troubleshooting utility

You can use the client troubleshooting utility to view client components on Windows.

1. Double-click `f5wininfo.exe` to start the client troubleshooting utility.
   The F5 BIG-IP® Edge Components Troubleshooting window opens.
2. Use the navigation panel on the left to explore the component categories.

Generating a client troubleshooting report

You can use the client troubleshooting utility to generate a client troubleshooting report on Windows.

1. Double-click `f5wininfo.exe` to start the client troubleshooting utility.
   The F5 BIG-IP® Edge Components Troubleshooting window opens.
2. Click **File** > **Generate Report**
   The Report window opens.
3. Under **Type**, select the type of report you want to generate.
4. Under **Format**, select **html** or **text** for the type of report.
5. If you want to generate a compressed report, select the **compressed** option.
6. If you want to view the report without saving the report, click **View**.

Running a Network Access diagnostic test

You can use the client troubleshooting utility to run a Network Access diagnostic test on Windows.

1. Double-click `f5wininfo.exe` to start the client troubleshooting utility.
   The F5 BIG-IP® Edge Components Troubleshooting window opens.
2. Click **Tools** > **Network Access Diagnostic**
   The Network Access Diagnostic window opens.

The client troubleshooting utility runs a Network Access diagnostic.

Chapter 2

BIG-IP Edge Client for Mac

About client installation on Macintosh systems

The BIG-IP® Access Policy Manager ®(APM) includes network access support for remote Mac OS X clients. You can use APM® for secure remote access in mixed-platform environments. You do not need to preinstall or preconfigure any client software if the client allows installation of the required browser components.

The first time a remote user starts network access, the BIG-IP APM downloads a client component. This client component is designed to be self-installing and self-configuring, but the user's browser must have Java enabled on Macintosh systems. If the browser does not support this requirement, the BIG-IP APM prompts the user to download the controller client component from the controller and install it manually.

Note: *The remote user must have superuser authority, or must be able to supply an administrative password in order to successfully install the network access client.*

The Macintosh systems must also include PPP support; (this is most often the case). When the user runs the network access client and makes a connection for the first time, the client detects the presence of PPPD (Point-to-Point Protocol Daemon), and determines whether the user has the necessary permissions to run it. If PPPD is not present, or if the user does not have permissions needed to run the daemon, the connection fails.
After installation, the Macintosh client must restart the browser before starting network access.

Overview: Configuring APM for BIG-IP Edge Client for Mac

To use the BIG-IP® Edge Client® for Mac, you must configure settings for the Mac Edge Client in a connectivity profile on Access Policy Manager®. The connectivity profile for a Mac includes Win/Mac Edge Client settings:

- The list of servers to display on the BIG-IP Edge Client.
- DNS settings for location-awareness for mobile clients, such as laptops that roam.

A Mac client package is attached to the connectivity profile. You can customize it. You can also download and distribute it.

Task summary

Customizing a connectivity profile for Mac Edge Clients
Customizing the Mac client package for BIG-IP Edge Client
Downloading the Mac client package for the BIG-IP Edge Client

Customizing a connectivity profile for Mac Edge Clients

You must create a connectivity profile before you start this task.

A connectivity profile automatically contains settings for BIG-IP® Edge Client® for Macintosh. You update the settings to specify how to handle password caching and component updates, to specify the servers to display on the clients, and to supply DNS names to support location awareness.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.

2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From the left pane, select **Win/Mac Edge Client**.
   Edge Client action and password caching settings display in the right pane.
4. Set Edge Client action settings:
   a) (Optional) Retain the default (selected) or clear the **Save Servers Upon Exit** check box.

      The setting specifies whether the BIG-IP Edge Client maintains a list of recently used Access Policy Manager servers. The BIG-IP Edge Client always lists the servers defined in the connectivity profile, and sorts the list of servers by most recent access, whether this option is selected or not. However, the BIG-IP Edge Client lists user-entered servers only if this option is selected.

5. Set password caching settings for enhanced security:
   a) (Optional) Select the **Allow Password Caching** check box.

      This check box is cleared by default.

      The remaining settings on the screen become available.
   b) (Optional) Select **disk** or **memory** from the **Save Password Method** list.

      If you select **disk**, an encrypted password is saved on disk and cached when the system reboots or when the BIG-IP Edge Client is restarted.

      If you select **memory**, the BIG-IP Edge Client caches the user's password within the BIG-IP Edge Client application for automatic reconnection purposes.

      If you select **memory**, the **Password Cache Expiration (minutes)** field displays with a default value of 240.
   c) If the **Password Cache Expiration (minutes)** field displays, retain the default value or type the number of minutes to save the password in memory.
   d) From the **Component Update** list, select **yes** (default) or **no**.

      If you select **yes**, APM updates the BIG-IP Edge Client software automatically on the Mac client when newer versions are available.

6. From the left pane, select **Server List**.
   A table displays in the right pane.
7. Specify the servers that you want defined in the client downloads.

   The servers you add here appear as connection options in the BIG-IP Edge Client.
   a) Click **Add**.
      A table row becomes available for update.
   b) You must type a host name in the **Host Name column**.

      Typing an alias in the **Alias** column is optional.
   c) Click **Update**.
      The new row is added at the top of the table.
   d) Continue to add servers and when you are done, click **OK**.

8. From the left pane, select **Location DNS List**.
   A table is displayed in the right pane.
9. Specify DNS suffixes that are considered to be in the local network.

   DNS suffixes specified here conform to the rules specified for the local network. When the BIG-IP Edge Client is configured to use the option Auto-Connect , the client connects when the systems DNS suffix is not one defined on this list. When the client DNS suffix does appear on this list, the client automatically disconnects. If you do not specify any DNS suffixes, the option Auto-Connect does not appear in the downloaded client.
   a) Click **Add**.

An update row becomes available.

b) Type a name and click **Update**.
The new row displays at the top of the table.

c) Continue to add DNS names and, when you are done, click **OK**.

10. 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.

Customizing the Mac client package for BIG-IP Edge Client

You must create a connectivity profile before you start this task.

You customize a Mac client package for a connectivity profile to specify BIG-IP® Edge Client® settings for the Mac.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Select a connectivity profile.
3. Click the arrow on the **Customize Package** button and select **Mac**.
   The Customize Mac Client Package screen displays.
4. Retain the selection or clear the **Auto launch BIG-IP Edge Client after User Log In** check box.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The customized package, `BIGIPMacEdgeClient.zip`, is downloaded to your client. It is available for you to distribute, if needed. The customized package is downloaded to clients automatically only when the Windows/Mac Edge Client settings in related connectivity profile allow password caching and component updates.

If you plan to distribute Mac client packages to your users and you customize Mac client packages with different settings for different connectivity profiles, you need to rename or otherwise organize the packages. Otherwise, your download location contains packages named `BIGIPMacEdgeClient.zip`, `BIGIPMacEdgeClient.zip(1)`, and so on.

Downloading the Mac client package for the BIG-IP Edge Client

You can download a Mac Client package and distribute it to clients whose configuration does not allow an automatic download.

Note: *If you already customized a Mac Client package for a connectivity profile, a customized package file, `BIGIPMacEdgeClient.exe`, was downloaded to your system. If you cannot find the package, use this procedure.*

---

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Select a connectivity profile.
3. Click the arrow on the **Customize Package** button and select **Mac**.

The Customize Mac Client Package screen displays.

4. Click **Download**.

   The screen closes and the package, `BIGIPMacEdgeClient.zip`, downloads.

The customized package, `BIGIPMacEdgeClient.zip`, is downloaded to your client. It is available for you to distribute, if needed. The customized package is downloaded to clients automatically only when the Windows/Mac Edge Client settings in the related connectivity profile allow password caching and component updates.

Overview: Installing and using BIG-IP Edge Client for Mac

The first time a remote user starts network access, the BIG-IP® Access Policy Manager ® (APM) downloads a client component. This client component is designed to be self-installing and self-configuring, but the user's browser must have Java enabled on Macintosh systems. If the browser does not support this requirement, the BIG-IP® APM® prompts the user to download the controller client component from the controller and install it manually.

Note: *The remote user must have superuser authority, or must be able to supply an administrative password in order to successfully install the network access client.*

The Mac system must also include PPP support (this is most often the case). When the user runs the network access client and makes a connection for the first time, the client detects the presence of PPPD (Point-to-Point Protocol Daemon), and determines whether the user has the necessary permissions to run it. If PPPD is not present, or if the user does not have permissions needed to run the daemon, the connection fails.

After installation, the Macintosh client must restart the browser before starting network access.

Task summary

Configuring applications to start on a Mac OS client
Editing the log level in the configuration file for Mac OS

About establishing client connections from a Mac system

You can initiate connections through network access from Macintosh OS X, by connecting to the virtual server address using a supported browser, or by starting the BIG-IP® Edge Client®.

Configuring applications to start on a Mac OS client

The launch application feature specifies a client application that starts when the client begins a network access session. You can use this feature when you have remote clients who routinely use network access to connect to an application server, such as a mail server.

1. On the Main tab, click **Access Policy** > **Network Access** > **Network Access List**.
   The Network Access List screen opens.
2. In the Name column, click the name of the network access resource you want to edit.
3. To configure applications to start for clients that establish a network access connection with this resource, click **Launch Applications** on the menu bar.

4. Click **Add** to add an application list.
5. In the **Application Path** field, type `open` .
6. In the **Parameters** field, type a parameter.
   For example, type `-a/Applications/ie.app http://www.f5.com`.
7. From the **Operating System** list, select **Mac**.
8. Click **Finished** to add the configuration.

Now when remote users with assigned resources make a network access connection, the application you configured starts automatically.

Editing the log level in the configuration file for Mac OS

You can edit log settings in the configuration file on Mac OS systems.

1. In the `~/Library/F5Networks.` directory, open the `f5networks.conf` file.
2. Edit the settings to change the log level.
   For debugging purposes, set the values to 5.

Supported network access features for Mac and Linux clients

BIG-IP® Access Policy Manager® supports all of the primary network access features on Macintosh and Linux clients, except for Drive Mappings and some client checks.

Feature	Notes
Secure remote access to an internal network	Includes support for IP-based applications.
Split tunneling	Only network traffic that you specify goes through the network access connection.
IP address filtering with connection-based ACL	Allows you to restrict groups of users to specific addresses, ranges of addresses, and ports.
DNS Servers	
DNS Suffixes	
Allow local subnets	Includes forcing all traffic through the tunnel.
Application launching	You must configure the starting of remote client applications based on the operating system on the remote computers. You can configure all other features independent of the remote client operating systems.

VPN component installation and log locations on Mac OS

On Macintosh operating systems, you install the VPN components and write VPN logs to the locations listed in the table.

VPN component	Location
Network Access plugin	`/Library/Internet Plugins/`

VPN component	Location
Endpoint Security (client checks)	`~/Library/Internet Plugins/`

VPN logs are written to the following directory: `~/Library/F5Networks`.

Chapter 3

BIG-IP Edge Client for Linux

Overview: Installing and using BIG-IP Edge Client for Linux

The BIG-IP® Access Policy Manager® (APM) includes network access support for remote Linux clients. You can use APM® for secure remote access in mixed-platform environments. You do not need to preinstall or preconfigure any client software if the client allows installation of the required browser components.

The first time a remote user starts network access, the BIG-IP APM downloads a client component. This client component is designed to be self-installing and self-configuring, but the user must use Firefox to be able to install a plugin on Linux systems. If the browser does not support this requirement, the BIG-IP APM prompts the user to download the controller client component from the controller and install it manually.

Note: *The remote user must have superuser authority, or must be able to supply an administrative password in order to successfully install the network access client.*

Linux systems must also include PPP support (this is most often the case). When the user runs the network access client and makes a connection for the first time, the client detects the presence of PPPD (Point-to-Point Protocol Daemon), and determines whether the user has the necessary permissions to run it. If PPPD is not present, or if the user does not have permissions needed to run the daemon, the connection fails.

Note: *If you have a firewall enabled on your Linux system, you must enable access on IP address* `127.0.0.1` *port 44444.*

Task summary

Configuring application starting on a Linux client
Editing the log level in the configuration file for Linux

About establishing client connections from Linux

You can initiate connections through network access from Linux systems, by connecting to the virtual server address using a browser, or by starting the BIG-IP® Edge Client®.

Configuring application starting on a Linux client

The launch application feature specifies a client application that starts when the client begins a network access session. You can use this feature when you have remote clients who routinely use network access to connect to an application server, such as a mail server.

1. On the Main tab, click **Access Policy** > **Network Access** > **Network Access List**.
   The Network Access List screen opens.
2. In the Name column, click the name of the network access resource you want to edit.
3. To configure applications to start for clients that establish a network access connection with this resource, click **Launch Applications** on the menu bar.
4. Click **Add** to add an application list.
   A screen opens showing the Add Application To Launch area.
5. In the **Application Path** field type an application to launch.
   For example, type `/usr/bin/mozilla` to start Mozilla.
6. In the **Parameters** field, type a parameter.
   For example, type `http://www.f5.com`.

7. From the **Operating System** list, select **Unix**.
8. Click **Finished** to add the configuration.

Now, when remote users with assigned resources make a network access connection, the application you configured starts automatically.

Editing the log level in the configuration file for Linux

You can edit log settings in the configuration file on Linux systems.

1. In the `/usr/local/lib/F5Networks` directory, open the `f5networks.conf` file.
2. Edit the settings to change the log level.
   By default, the values are 0 (zero). For debugging purposes, set the values to 5.

Supported network access features for Mac and Linux clients

BIG-IP® Access Policy Manager® supports all of the primary network access features on Macintosh and Linux clients, except for Drive Mappings and some client checks.

Feature	Notes
Secure remote access to an internal network	Includes support for IP-based applications.
Split tunneling	Only network traffic that you specify goes through the network access connection.
IP address filtering with connection-based ACL	Allows you to restrict groups of users to specific addresses, ranges of addresses, and ports.
DNS Servers	
DNS Suffixes	
Allow local subnets	Includes forcing all traffic through the tunnel.
Application launching	You must configure the starting of remote client applications based on the operating system on the remote computers. You can configure all other features independent of the remote client operating systems.

VPN component installation and log locations on Linux

On Linux operating systems, you install the VPN components and write VPN logs to the locations listed in the table.

Category	Location
VPN component	`/usr/local/lib/F5Networks`
VPN logs	`~/.F5Networks`

Chapter 4

BIG-IP Edge Command Line Client for Linux

About BIG-IP Edge Client for Linux command line

The BIG-IP® Access Policy Manager® includes a BIG-IP Edge Client® command line for Linux. You can download and deploy this client to your organization's Linux desktops.

Task summary

Downloading the Linux command line client
Installing the Linux command line client
Importing a certificate to the local trust store

Downloading the Linux command line client

You can download the BIG-IP® Edge command line client for Linux installer, as a gzipped `.TAR` file, and distribute it to clients for installation.

1. On the Main tab, click **Access Policy** > **Secure Connectivity** > **Client Downloads**.
   A list of available client downloads displays.
2. Click **BIG-IP Edge Command Line Client for Linux**.
   The file `linux_sslvpn.tgz` is downloaded to your local directory.

The Linux command line client is ready to be installed.

Installing the Linux command line client

You must download the file `linux_sslvpn.tgz` before you can install the command line client.

You can use various Linux client commands with the BIG-IP® Edge command line client for Linux.

1. Extract the file `linux_sslvpn.tgz` to your local directory.
2. Extract the file `linux_sslvpn.tar` to your local directory.
3. Run the install script `Install.sh` under the root account.

The following text appears when installation is complete:

```
--> f5fpc is installed in /usr/local/bin
--> Please check f5fpc --help command to get started
--> Uninstaller located in /usr/local/lib/F5Networks/uninstall_F5.sh
```

Importing a certificate to the local trust store

You can import an untrusted certificate to the local trust store and change it into a trusted certificate.

1. Using operating system commands, place the certificate in any folder in the operating system.
   For example, `/etc/certs`.
2. Change the directory.
   For example, `cd /etc/certs`.
3. Type the command `c_rehash ./`.

The certificate is installed.

Note: *Alternatively, instead of installing the certificate, you can specify the* `--cacert` *option to import a certificate to the local store.*

Linux client commands

The following commands are supported by the Linux command line client. All commands that are invoked on the Linux command line client begin with the command `f5fpc`.

To start a VPN connection, type either of the following commands:

- `f5fpc -- start [`*`arguments`*`]`
- `f5fpc - s [`*`arguments`*`]`

Note: *This requires the* `--host` *or* `-t` *argument at the minimum.*

Use the following table to assign arguments to the Linux commands.

Arguments	Description
`--nonblock` `-b`	Returns the command line interface immediately after the command.
`--host [https://]`*`hostname`*`[:port]` `-t [https://]`*`hostname`*`[:port]`	The host name to which the client starts the VPN connection. This is required.
`--user` *`username`* `-u` *`username`*	The optional user name for the connection.
`--password` *`password`* `p` *`password`*	The optional password for the connection.
`--userhex` *`hex-encoded-username`* `-U` *`hex-encoded-username`*	The optional hex-encoded user name for the connection.
`--passwordhex` *`hex-encoded-password`* `-P` *`hex-encoded-password`*	The optional hex-encoded password for the connection.
`--cert` *`certificate`* `-r` *`certificate`*	Specifies an optional client certificate.
`--key` *`certificate_key`* `-k` *`certificate_key`*	Specifies the key for an optional client certificate.
`--keypass` *`SSL_certificate_password`* `-y` *`SSL_certificate_password`*	Specifies the password for an optional SSL certificate.
`--cacert` *`trusted_CA_certificate`* `-a` *`trusted_CA_certificate`*	Specifies a certificate from a trusted certificate authority (CA). If `--cacert` or `--cacertdir` is specified, then the server certificate validates for trust against the specified certificate or directory. If `--cacert` or `--cacertdir` is not specified, then the default location `/etc/ssl/certs` is checked to verify trust. The `--nocheck` option can be specified if a server certificate check is not desired, though this is not recommended.

Arguments	Description
`--cacertdir` *`trusted_CA_certificate_directory`* `-d` *`trusted_CA_certificate_directory`*	Specifies a certificate directory that contains a certificate from a trusted CA. If `--cacert` or `--cacertdir` is specified, then the server certificate validates for trust against the specified certificate or directory. If `--cacert` or `--cacertdir` is not specified, then the default location `/etc/ssl/certs` is checked to verify trust. The `--nocheck` option can be specified if a server certificate check is not desired, though this is not recommended.
`--nocheck` `-x`	Specifies that the trusted CA certiicate is not verified for trust at all. If `--cacert` or `--cacertdir` is specified, then the server certificate validates for trust against the specified certificate or directory. If `--cacert` or `--cacertdir` is not specified, then the default location `/etc/ssl/certs` is checked to verify trust. The `--nocheck` option can be specified if a server certificate check is not desired, though this is not recommended.

To stop the VPN connection, type either of the following commands:

- `f5fpc -- stop`
- `f5fpc --o`

To display the connection status, type either of the following commands:

- `f5fpc -- info`
- `f5fpc --i`

To display the command line client help, type either of the following commands:

- `f5fpc -- help`
- `f5fpc --h`

Info command status and error codes

The following status codes and error codes might be displayed when you run the `--info` command.

Error code/command status	Hex value	Shell value	Description
CLI_ERROR_SUCCESS	0x0	0	The command line operation was successful.
CLI_ERROR_USERS_DISCONNECT	0x150	80	The user was disconnected
CLI_ERROR_LOGON_FAILURE	0x151	81	Login failed due to incorrect authenticaion information or login errors.
CLI_ERROR_ATTENTION_REQUIRED	0x154	84	The user's attention is required.
CLI_ERROR_GENERIC_FAILURE	0x155	85	An error occurred in the system API.
CLI_ERROR_UNKNOWN_PARAMETER	0x156	86	An incorrect or unknown parameter was passed to the command line.
CLI_ERROR_WRONG_VALUE	0x157	87	This is an undefined error.

Error code/command status	Hex value	Shell value	Description
CLI_ERROR_UNKNOWN_SESSION_ID	0x158	88	An unknown session ID was encountered. The user should reconnect to the server.
CLI_ERROR_NO_PROFILE	0x15B	91	No such profile exists.
CLI_ERROR_MSGQ_OPEN_FAILURE	0x15D	93	The system failed to open the message queue.
CLI_ERROR_OPERATION_IN_PROGRESS	0x15F	95	An operation is in progress, please retry.
kss_Initialized	1	1	The session is initialized.
kss_LogonInProgress	2	2	The user login is in progress.
kss_Idle	3	3	The session is idle.
kss_Established	5	5	The session is established.
kss_AttentionReq	6	6	The session requires the user's attention.
kss_LogonDenied	7	7	Login was denied.
kss_LoggedOut	8	8	The user is logged out of the server.

Chapter 5

BIG-IP Edge Applications

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

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.

Task Summary

Configuring security settings for iOS Edge Clients
Configuring security settings for Android Edge Clients
Configuring security settings for iOS Edge Portal clients
Configuring security settings for Android Edge Portal clients

Configuring security settings for iOS Edge Clients

You must create a connectivity profile before you start this task.

A connectivity profile automatically contains default settings for BIG-IP® Edge Client® for iOS clients. You update the settings to change the way password caching and on demand disconnect are handled.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From Mobile Client Settings in the left pane, select **iOS Edge Client**.
   Settings for the iOS Edge Client display in the right pane.
4. If you want users to be able to save their passwords, select the **Allow Password Caching** check box.
5. For **Save Password Method**, specify how to use password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.
6. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
7. For **Maximum Inactivity Time (minutes)**, retain the default **5**, or type a different number of minutes.
8. In the **On Demand Disconnect Timeout (minutes)** field, retain the default 2, or type a different number of minutes before VPN on demand times out .
9. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

You have now customized the password caching and on demand disconnect settings for BIG-IP Edge Client for iOS clients.

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

Configuring security settings for Android Edge Clients

You must create a connectivity profile before you start this task.

A connectivity profile automatically contains settings for BIG-IP® Edge Client® for Android clients. You update the settings to change the way password caching and device locking are handled.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From Mobile Client Settings in the left pane, select **Android Edge Client**.
   Settings for the Android Edge Client display in the right pane.
4. If you want users to be able to save their passwords, select the **Allow Password Caching** check box.
5. For **Save Password Method**, specify how to use password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.
6. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
7. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.
8. To enhance security on the client, retain the selection of the **Enforce Device Lock** check box (or clear the check box).

   This check box is selected by default. Edge Portal supports password locking, but does not support pattern locking. If you clear this check box, the remaining settings become unavailable.
9. For **Device Lock Method**, retain the default **numeric**, or select a different method from the list.
10. For **Minimum Passcode Length**, retain the default **4**, or type a different passcode length.
11. For **Maximum Inactivity Time (minutes)**, retain the default **5**, or type a different number of minutes.
12. Click **OK**.
    The popup screen closes, and the Connectivity Profile List displays.

You have now customized the password caching and device lock settings for BIG-IP Edge Client for Android clients.

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

Configuring security settings for iOS Edge Portal clients

You must create a connectivity profile before you start this task.

A connectivity profile automatically contains settings for BIG-IP® Edge Portal® for iOS clients. You update the settings to change the way password caching and device locking are handled.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.

A list of connectivity profiles displays.

2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From Mobile Client Settings in the left pane, select **Android Edge Portal**.
   Settings for the Android Edge Portal display in the right pane.
4. If you want users to be able to save their passwords, select the **Allow Password Caching** check box.
5. For **Save Password Method**, specify how to use password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.
6. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
7. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.
8. Specify security by keeping **Enforce PIN Lock** set to **Yes**.
   Edge Portal supports PIN locking, but does not support pattern locking.
9. For **Maximum Grace Period (minutes)**, retain the default 2, or type a different number of minutes.
10. Select **Yes** or **No** from the **Allow External Access** list.
11. For **Maximum Inactivity Time (minutes)**, retain the default **5**, or type a different number of minutes.
12. Click **OK**.
    The popup screen closes, and the Connectivity Profile List displays.

You have now customized the password caching and pin lock settings for BIG-IP Edge Portal for iOS clients.

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

Configuring security settings for Android Edge Portal clients

You must create a connectivity profile before you start this task.

A connectivity profile automatically contains settings for BIG-IP® Edge Portal® for Android clients. You update the settings to change the way password caching and device locking are handled.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From Mobile Client Settings in the left pane, select **Android Edge Portal**.
   Settings for the Android Edge Portal display in the right pane.
4. If you want users to be able to save their passwords, select the **Allow Password Caching** check box.
5. For **Save Password Method**, specify how to use password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.

6. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
7. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.
8. To enhance security on the client, retain the selection of the **Enforce Device Lock** check box (or clear the check box).

   This check box is selected by default. Edge Portal supports password locking, but does not support pattern locking. If you clear this check box, the remaining settings become unavailable.
9. For **Device Lock Method**, retain the default **numeric**, or select a different method from the list.
10. For **Minimum Passcode Length**, retain the default **4**, or type a different passcode length.
11. For **Maximum Inactivity Time (minutes)**, retain the default **5**, or type a different number of minutes.
12. Click **OK**.
    The popup screen closes, and the Connectivity Profile List displays.

You have now customized the password caching and device lock settings for BIG-IP Edge Portal for Android clients.

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

Index

U

V