BIG-IP® Access Policy Manager® and F5 Access for Chrome OS v1.0.0

1.0.0

Table of Contents

Legal notices

Publication Date

This document was published on December, 2015.

Publication Number

MAN-0607-00

Copyright

Trademarks

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*

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

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: F5 Access for Chrome OS

What does F5 Access do for Chrome OS devices?

F5 Access for Chrome OS 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 Chrome OS devices.

For information about how to use F5 Access, refer to the *F5 Access for Chrome OS User Guide* on your device.

F5 Access 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
- Logging support to report issues
- Support for certificate-only authentication
- Support client certificate for DTLS tunnels and SSL tunnels

About SAML support

F5 Access app for Chrome OS 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 F5 Access as a client performing SP-initiated access, F5 Access 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 F5 Access back to the SP with assertion. APM then accepts the assertion and establishes a VPN connection. You can then access back-end resources through F5 Access.

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

F5 Access app for Chrome OS 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 field is blank)
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 blank.
Web Logon	Provides the following two options: • User name and password • User name/password + RSA + any other server-side checks

About establishing VPN connections

You can use F5 Access with a Chrome OS device to establish a VPN tunnel connection.

About network integration on Chrome OS 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, smart phones, or other mobile devices to browse the web.

Chapter 2

Configuring Access Policy Manager for F5 Access

Prerequisites for configuring F5 Access

Before configuring F5 Access for Chrome OS 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* guide.

Access Policy Manager configuration for F5 Access for Chrome OS devices

To configure F5 Access for mobile devices support on BIG-IP® Access Policy Manager®, use the 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®.

About access policy branches for F5 Access

You can configure separate access policy branches for F5 Access.

F5 Access does not support client-side checks; however, you can configure an access policy that provides network access for Chrome OS clients by using any of these methods:

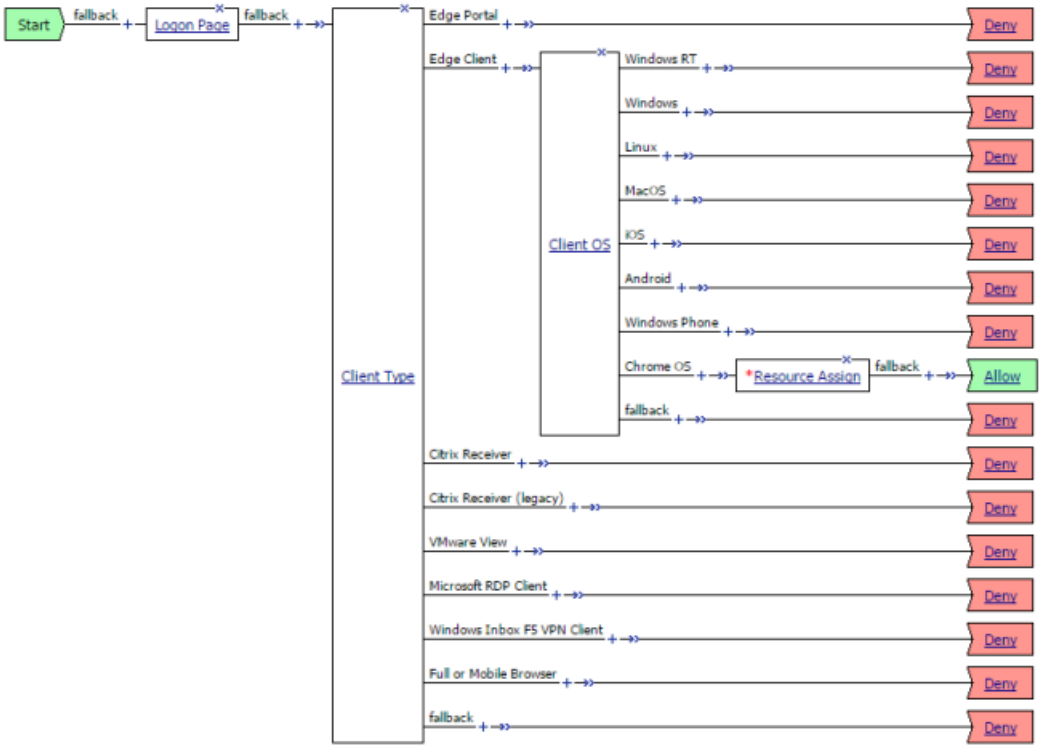
- Create an access policy using **Client-Side Capability**. This provides a branch for clients that do not support client-side checks. Assign authentication and a network access resource to this branch.
- Use an existing access policy with client-side checks. The Chrome OS client will fail to the fallback branch of the first client-side check. Assign authentication and a network access resource to this branch.

- Add a **Client OS** Access Policy item, and assign authentication and resources to the **Chrome OS** branch.

Example of basic access policy that supports F5 Access

You can configure an access policy branch to direct Chrome OS device users to F5 Access, and direct non-F5 Access device users to a fallback branch.

This example displays a simple access policy.



Customizing an access policy to support F5 Access on Access Policy Manager

Create an access policy that supports F5 Access for Chrome OS.

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 after the `Logon Page` action.
4. On the **Endpoint Security (Server-Side)** tab, select **Client Type**, and click **Add Item**.
5. Click **Save**.
6. Click the plus **(+)** sign that appears on the Edge Client branch of the `Client Type` action.
7. On the **Endpoint Security (Server-Side)** tab, select **Client OS**, and click **Add Item**.
8. On the **Chrome OS** branch, assign a network access resource.
9. On the **Chrome OS** branch, click the ending, and on the **Select Ending** screen, select **Allow**.
10. Click **Save**.
11. Click **Apply Access Policy**.

This access policy now supports F5 Access for Chrome OS.

Chapter 3

Deploying F5 Access with Google Apps for Work

Installing F5 Access with Google Apps for Work

The Google Apps for Work administrator can choose whether F5 Access is installed automatically for the organization unit, or whether users must install the app themselves.

1. Sign in to the Google Apps for Work Admin console.
2. Click **Device Management**.
3. Click **Chrome Management**.
4. Click **User settings**.
5. Select an organization unit to which you want the settings to apply.
6. In the **Force-installed Apps and Extensions** area, click **Manage force-installed apps**.
7. Select **Chrome Web Store** in the left pane, and search by the application name `F5 Access`.
8. Click **Add** in the **F5 Access** row.
9. Click the **Save** button.
10. Click **Save** to save the user settings.

F5 Access for Chrome OS is now configured to be automatically installed on user machines in the selected organization unit. See *Set Chrome Policies for Users* on the Google support site for additional information.

Note: *This link is for a third-party site, and thus is subject to change at any time.*

Making F5 Access available to users in Google Apps for Work

The Google Apps for Work administrator can make the F5 Access app available for users to download and install on their own devices.

1. Sign in to the Google Apps for Work Admin console.
2. Click **Device Management**.
3. Click **Chrome Management**.
4. Click **User settings**.
5. Select an organization unit to which you want the settings to apply.
6. In the **Allowed Apps and Extensions** area, select the allow or block policy stance.
   - If you select **Allow all apps and extensions except the ones I block**, users can install F5 Access with no further configuration.
   - If you select **Block all apps and extensions except the ones I allow**, specify that F5 Access is an allowed app. Select **Chrome Web Store** in the left pane, type `F5 Access`, add the **F5 Access** app, and click **Save**.
7. Click **Save** to save the user settings.

Users can now download and install F5 Access for Chrome OS. See *Set Chrome Policies for Users* on the Google support site for additional information.

Note: *This link is for a third-party site, and thus is subject to change at any time.*

Recommending the F5 Access app to users in Google Apps for Work

The Google Apps for Work administrator can recommend the F5 Access app to users to download and install on their own devices.

1. Sign in to the Google Apps for Work Admin console.
2. Click **Device Management**.
3. Click **Chrome Management**.
4. Click **User settings**.
5. Select an organization unit to which you want the settings to apply.
6. In the **Recommended Apps and Extensions** area, click **Manage**.
7. Select **Chrome Web Store** in the left pane, and search by the application name `F5 Access`.
8. Click **Add** in the **F5 Access** row.
9. Click **Save** to save the user settings.

Users now see the F5 Access app as a recommended app for their domain. See *Set Chrome Policies for Users* on the Google support site for additional information.

Note: *This link is for a third-party site, and thus is subject to change at any time.*

Specifying VPN configurations for F5 Access with Google Apps for Work

The Google Apps for Work administrator can specify VPN configurations to include with the F5 Access app.

Note: *Users cannot delete or modify VPN configurations added to the app by administrators.*

1. Create a text file in your text editor.
2. Specify VPN configurations in the text file, with the required information.
3. Save the text file.

The text file that contains VPN configurations can be uploaded to add those configurations to the F5 Access app.

VPN policy file specification for F5 Access

This is the file specification for the file you create to upload VPN configurations to F5 Access with Google Apps for Work.

```
{
 "type":"object",
 "properties":{
  "Configurations":{
   "type":"array",
   "items":{
    "type":"object",
    "properties":{
     "name":{
      "type":"string"
     },
     "server":{
      "type":"string"
     },
     "weblogon":{
      "type":"boolean"
     },
     "certificate":{
      "type":"object",
      "properties":{
       "issuer":{
        "type":"object",
        "properties":{
         "CN":{
          "type":"string"
         }
        }
       }
      }
     }
    }
   }
  }
 }
}
```

VPN policy settings for F5 Access with Google Apps for Work

These settings can be configured in the VPN policy for F5 Access with Google Apps for Work.

Policy setting	Description
name	(Required) The name of VPN configuration.
server	(Required) The URL of the BIG-IP® server.
weblogon	(Optional) Specify this value as `true` to enable Web authentication mode. This is set to `false` by default.

Policy setting	Description
certificate/issuer/CN	(Optional) The Common Name of the certificate authority that issued client certificate. Use this to auto-select a client certificate from the device certificate store.

Example VPN policy for F5 Access with Google Apps for Work

These settings can be configured in the VPN policy for F5 Access with Google Apps for Work.

```
{
            "Configurations": {
               "Value": [
                  {
                        "name":     "DemoVPN1",
                        "server":   "https://myvpn.server.company.com",
                        "weblogon":  false
                        "certificate": {
                            "issuer": {"CN":"DemoIssuerCA"}
                        }
                  },
                  {
                    "name":     "DemoVPN2",
                    "server":   "https://myvpn2.server.company.com",
                    "weblogon":  true
                  },
                  {
                    "name":     "DemoVPN3",
                    "server":   "https://myvpn3.server.company.com",
                  }
               ]
            }
}
```

Uploading a VPN policy file in Google Apps for Work

Install a VPN configuration file through App Management in Google Chrome for Work.

1. Sign in to the Google Apps for Work Admin console.
2. Click **Device Management**.
3. Click **Chrome Management**.
4. Click **App Management**.
5. Search by the application name **F5 Access**.
6. Select the application and click **User settings**.
7. Select an organization unit to which you want the settings to apply.
8. Click **Upload configuration file**, and select the policy file to upload.
9. Click **Save** to save the user settings.

The VPN configuration file now applies to the F5 Access app. See *Manage Chrome Apps individually* on the Google support site for additional information.

Note: *This link is for a third-party site, and thus is subject to change at any time.*

Increasing security by disabling Chrome Developer Tools

We recommend that you disable Chrome Developer Tools in the F5 Access app to avoid potential security risks.

1. Sign in to the Google Apps for Work Admin console.
2. Click **Device Management**.
3. Click **Chrome Management**.
4. Click **User settings**.
5. Select an organization unit to which you want the settings to apply.
6. In the **Developer Tools** area, click **Never allow use of built-in developer tools**.
7. Click **Save** to save the user settings.

Chrome Developer Tools are now disabled in the F5 Access app.

Increasing security by locking the device screen when idle

We recommend that you enable the device screen lock policy for the F5 Access app to avoid potential security risks.

1. Sign in to the Google Apps for Work Admin console.
2. Click **Device Management**.
3. Click **Chrome Management**.
4. Click **User settings**.
5. Select an organization unit to which you want the settings to apply.
6. In the **Screen Lock** area, click **Always automatically lock screen on idle**.
7. Click **Save** to save the user settings.

The device screen lock policy is now enforced for F5 Access app users.

Providing certificate access to F5 Access users

F5 Access for Chrome OS can authenticate with client certificates to the BIG-IP® Access Policy Manager®. Such client certificates must be pre-installed on Chrome devices in order to be available to F5 Access. Google Apps for Work administrator has to allow access to the enterprise certificates and keys to F5 Access.

For more information, see *Manage certificates* on the Google support site.

Note: *This link is for a third-party site, and thus is subject to change at any time.*

---

1. Sign in to the Google Apps for Work Admin console.
2. Click **Device Management**.
3. Click **Chrome Management**.

4. Click **App Management**.
5. Search by the application name **F5 Access**.
6. Select the application and click **User settings**.
7. Select an organization unit to which you want the settings to apply.
8. In the **Allow access to client certificates and keys** area, click **Override** if you want to override the settings for the organization unit.
9. Set **Allow access to client certificates and keys** to **ON**.
10. Click **Save** to save the user settings.

Certificates are now allowed for F5 Access app users.

Chapter 4

Additional Access Policy Manager Configuration Information

F5 Access for Chrome OS Session variables

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

F5 Access Session Variables

F5 Access for Chrome OS supports the following session variables and values.

Table 1:

Session variable	Description	Example value
session.client.app_version	Returns the version of the F5 Access app.	`1.0.0.0`
session.client.cpu	Returns the client CPU type.	`ARM`, `ARM64`, `x86` or `x64`
session.client.model	Returns the type of client device.	`Chromebook`, `Chromebox`, `Chromebit`, or `Chromebase`
session.client.platform	Returns the operating system name.	`ChromeOS`
session.client.platform_version	Returns the version of the operating system.	`45.0.2454.4`
session.client.type	Returns the client type.	For this client, this value is always `Standalone`
session.client.activex	Returns results of the ActiveX check.	For this client, this value is always `0`
session.client.jailbreak	Returns results of a jailbreak check.	For this client, this value is always `0`
session.client.version	Returns the client protocol version.	For this client, this value is always `2.0`

Session variable	Description	Example value
session.client.js	Returns results of the JavaScript check.	For this client, this value is always `0`
session.client.plugin	Returns results of the client plugin capability check.	For this client, this value is always `0`
session.client.vpn_scope	Returns the VPN connection scope.	For this client, the value is always `device`
session.client.vpn_scope	Returns the VPN tunnel type.	For this client, the value is always `L3`
session.client.vpn_start_type	Returns the VPN connection start method.	For this client, the value is always `manual`

Access Policy Manager configuration tips

The following table provides tips for setting up F5 Access for Chrome OS devices.

Feature	Information
Client endpoint checks	Client endpoint 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.
	• On the Chrome OS 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 defining a server from a URL

You can add BIG-IP® server definitions to F5 Access from a URL. You can provide these URLs to users, so they can create and/or start VPN connections without having to manually start the application.

Use the following URL and parameters to create a server:

```
http://cdn.f5.com/product/apm/edgeclient/chromeos/api/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.

Important: *When `username` is specified, web logon mode is automatically disabled.*

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.

Important: *When `password` is specified, web logon mode is automatically disabled.*

cert_issuer_cn

Certificate common name. Matches the common name of the issuer of a valid certificate pre-installed on the device.

Important: *When `cert_issuer_cn` is specified, Web Logon is automatically disabled.*

logon_mode

Specifies whether the logon mode is the standard logon (`native`) or web logon (`web`). The default logon mode is `native`.

Examples of defining a server from a URL

The following examples illustrate how to define servers for F5 Access connections from a URL.

Create a server at `access.siterequest.com` in Web Logon mode:

```
http://cdn.f5.com/product/apm/edgeclient/chromeos/api/create?server=
access.siterequest.com&logon_mode=web
```

Create a server named ChromeAccess at: `access.siterequest.com`

In this scenario, *`logon_mode`* is not specified, so native logon mode is assumed.

```
http://cdn.f5.com/product/apm/edgeclient/chromeos/api/create?name=
ChromeAccess&server=access.siterequest.com
```

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

```
http://cdn.f5.com/product/apm/edgeclient/chromeos/api/create?name=
ChromeAccess&server=access.siterequest.com&username=
hromeAccess&password=ChromeOSdemo&cert_issuer_cn=DemoIssuerCA
```

Create the same server with a user name and certificate:

```
http://cdn.f5.com/product/apm/edgeclient/chromeos/api/create?name=
ChromeAccess&server=access.siterequest.com&username=
ChromeAccess&cert_issuer_cn=DemoIssuerCA
```

Create the same server with a certificate:

```
http://cdn.f5.com/product/apm/edgeclient/chromeos/api/create?name=
ChromeAccess&server=access.siterequest.com&cert_issuer_cn= DemoIssuerCA
```

Enforcing logon mode for F5 Access clients

You can force F5 Access clients to log on through the native logon dialog box, or to log on with a web page, by enforcing the logon mode.

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 **Chrome OS Edge Client**.
   F5 Access settings for Chrome OS systems display in the right pane.
4. To force the app to use a selected logon mode and prevent users from changing it:
   a) Select the **Enforce Logon Mode** check box.
   b) From the **Logon Method** list, select **web** or **native**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

Index