BIG-IP® Access Policy Manager® and F5 Access for Android

Version 3.0.4

Table of Contents

Legal Notices

Legal notices

Publication Date

This document was published on November 5, 2017.

Publication Number

MAN-0740-01

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks/*.

All other product and company names herein may be trademarks of their respective owners.

Patents

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

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Overview: F5 Access for Android

F5 Access and mobile devices

F5 Access for mobile devices provides full network access through BIG-IP® Access Policy Manager®. With network access, users can run applications such as RDP, SSH, Citrix, VMware View, and other enterprise applications on their mobile devices.

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

F5 Access features include:

- Support for F5 Access on Chrome OS
- N-factor authentication (at least two input fields, password and passcode) support
- User name and password, client certificate, and RSA SecurID support
- Support for RSA SecurID software tokens
- Multiple input field support
- Credential caching support
- Support for biometric authentication, PIN, pattern, or device password to make a connection, when using cached credentials
- Support for checking information from client devices
- Support for roaming between cellular and WiFi networks
- Landing URI support
- Logging support to report issues
- Support for certificate-only authentication
- Support client certificate for DTLS tunnels and SSL tunnels
- Per-app VPN support for Android 5.0 and later
- Always-On mode for Android 7.0 and later for devices managed by an MDM

About SAML support

F5 Access for mobile devices provides the following SAML support:

- Service provider-initiated access only, for example, APM acting as the service provider (SP)
- Web Logon mode only

When you use F5 Access as a client performing the 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 an 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 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®: SAML Configuration* guide.

About supported authentication types

F5 Access for Android and Chrome OS provides these authentication types:

Authentication type	Description
Regular Logon	Provides the following two options: • Username and password • Client certificate + username and password (prompt if password field is empty)
Certificate-only	Provides a certificate-only authentication without a username and password by adding a certificate in the configuration while leaving the username field empty.
Web Logon	Provides the following three options: • Username and password • Username/password + RSA SecurID + any other server-side checks • Username + RSA SecurID (not available for Chrome OS) ***Tip:*** *Client certificate is supported for the Web Logon authentication type in Android 5.0 and higher.*

About establishing VPN connections

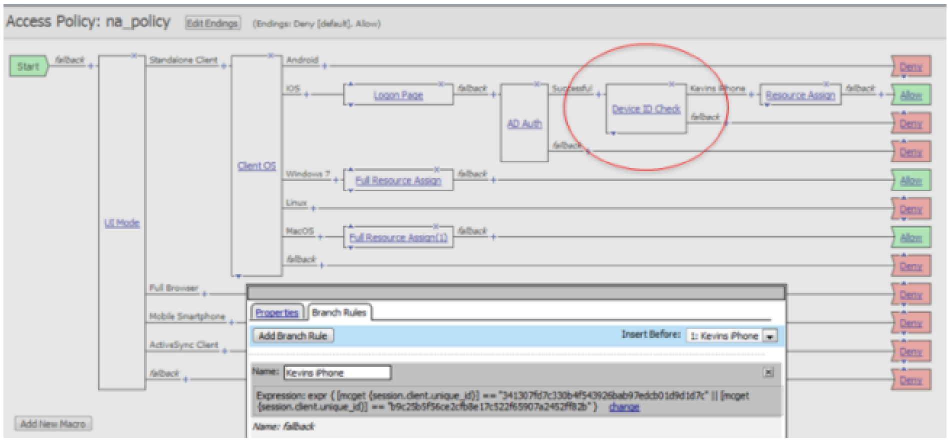
You can use F5 Access to establish a VPN tunnel connection.

About pre-logon checks supported for Android and Chrome OS devices

Access Policy Manager® can check unique identifying information from an Android client device. The supported session variables, which become populated with the Android client device information, are gathered automatically, and can easily be combined with an LDAP or AD query to implement white-listing in a custom action to improve access context. This information allows the Access Policy Manager to perform pre-logon sequence checks and operations based on information about the connecting device. Using such information, the Access Policy Manager can perform the following tasks:

- Deny access if the Android or Chrome OS version is less than the required level.
- Log UDID information.

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



Properties | Branch Rules

Add Branch Rule — Insert Before: 1: Kevins iPhone

Name: Kevins iPhone

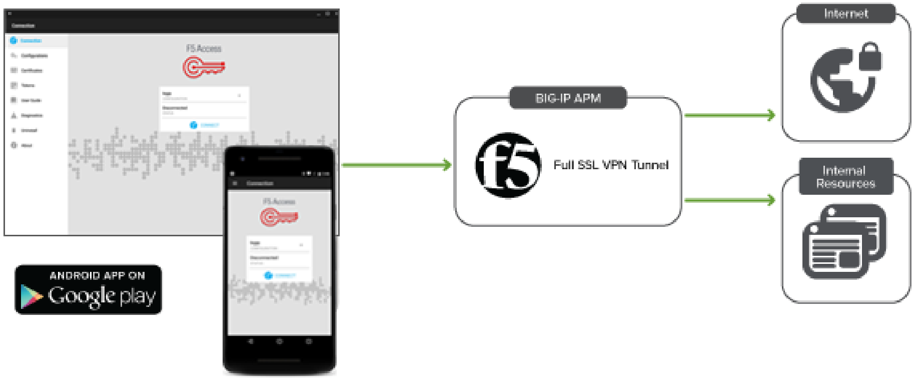
Expression: expr { [mcget {session.client.unique_id}] == "341307fd7c330b4f543926bab97edcb01d9d1d7c" || [mcget {session.client.unique_id}] == "b9c25b5f56ce2cfb8e17c522f65907a2452ff82b" } change

Name: fallback

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

About network integration on Android and 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, smartphones, or other mobile devices to browse the web.



Configuring Access Policy Manager for F5 Access

Prerequisites for configuring F5 Access

Before configuring F5 Access for Android and Chrome OS devices, you must complete the following requirements:

- Set up BIG-IP® Access Policy Manager®.
- Run the Network Access Setup Wizard.

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

To configure F5 Access for Android and Chrome OS device 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 F5 Access.

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 and Android 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 Android and 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 **Android** or **Chrome OS** branch.

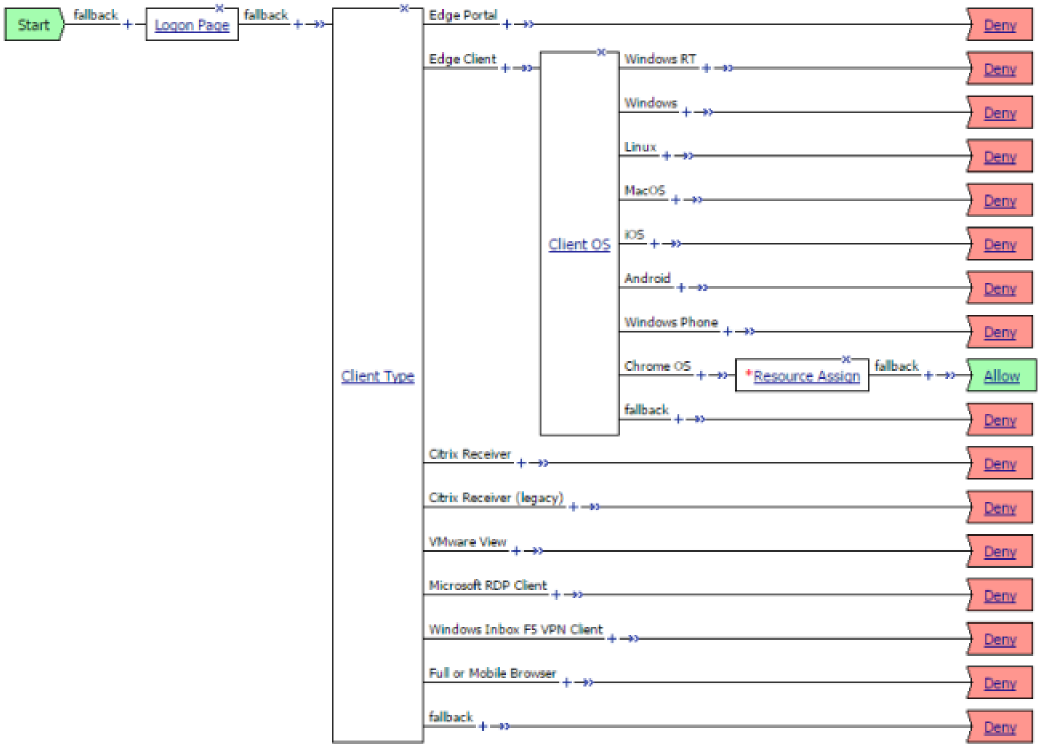
F5 Access for Android or Chrome OS is detected with the following access policy items:

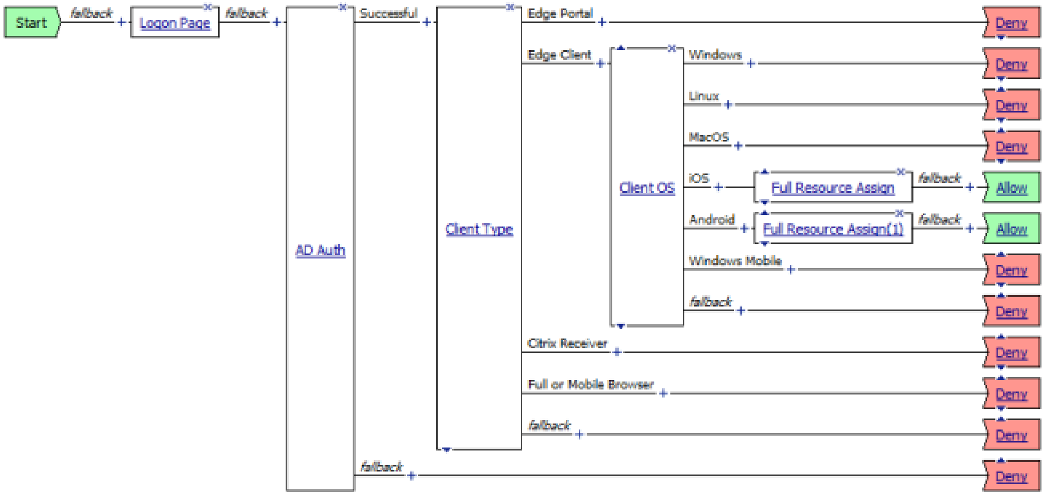
Access policy item	Value
Client Type	Edge Client
Client OS	Android (for Android devices)
Client OS	Chrome OS (for Chrome OS devices)

Example of basic access policy that supports F5 Access

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

These examples display 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 Android / 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 **Android / Chrome OS** branch, assign a network access resource.
9. On the **Android / 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 Android / Chrome OS.

About RSA SecurID two-factor authentication with F5 Access for Android and Chrome OS

RSA SecurID two-factor authentication is configured in an access policy. For more information, see *Big-IP Access Policy Manager: Authentication Methods* for your Access Policy Manager version.

Android devices with F5 Access can generate software tokens using an imported token. You can import tokens from a URL or by scanning a QR code.

Note: *For Chrome OS, only URL token import is supported.*

- To import from a URL, the user must enter the URL in Compact Token Format (CTF) with one of 2 supported prefixes: `http://127.0.0.1/securid/` or `f5access://securid/`.
- To import from a QR code, the user scans the QR code when the camera opens.

Note: *F5 Access asks for permission to take pictures and record video on your device. This permission is required to scan QR codes and import RSA token from the device. If you select Deny for this permission, you will not be able to use the Scan QR Code feature.*

The URL and QR code images can be generated with the RSA TokenConverter tool. See your RSA documentation for detailed information on installing and using TokenConverter.

The following examples include URL and QR code generation commands.

URL import with default prefix http://127.0.0.1/securid/

```
>java -jar TokenConverter.jar test.sdtid -android -p 123456 -o out.txt
```

URL import with custom prefix f5access://securid/

```
>java -jar TokenConverter.jar test.sdtid -prefix f5access://securid/ctf?ctfData=
-android -p 123456 -o out.txt
```

QR code import with default prefix http://127.0.0.1/securid/

```
> java -jar TokenConverter.jar test.sdtid -qr -android -p 123456 -o qr.jpeg
```

QR code import with custom prefix f5access://securid/

```
> java -jar TokenConverter.jar test.sdtid -qr -prefix
f5access://securid/ctf?ctfData= -android -p 123456 -o qr.jpeg
```

Using CT-KIP to dynamically generate software tokens with F5 Access for Android and Chrome OS

F5 Access can import tokens using the Cryptographic Token Key Initialization Protocol (CT-KIP). This eliminates the need to deliver a token in CTF format. F5 Access and the RSA authentication server (for example, RSA Authentication Manager) use a four-pass CT-KIP protocol to exchange information that dynamically establishes a shared seed on the mobile app and the server. In this way, the CT-KIP protocol protects against potential token seed interception.

Important: *CT-KIP exchanges require netrwork connectivity between the RSA Authentication Manager and the mobile device.*

The following URL formats are supported:

RSA default CT-KIP URL

```
http://127.0.0.1/securid/ctkip?scheme=<http or
https>&url=<service_address>&activationCode=<activation_code*>
```

With custom f5access:// prefix

```
f5access://securid/ctkip?scheme=<http or
https>&url=<service_address>&activationCode=<activation_code*>&name=<optional_token_name>
```

Note: *The activation code is required, but you do not need to provide the activation code in the URL. If the activation code is not included in the URL, the user is prompted to enter the activation code.*

Configuring Per-App VPN with APM and F5 Access

What is per-app VPN?

With Android 5.0, Google enhanced their VPN framework to support application level layer-3 tunneling. Users must first connect with F5 Access manually, then start the app on the device with traffic that is required to go through the VPN tunnel. Admin users can configure a list of allowed apps or disallowed apps; traffic from the "allowed apps" list are able to pass through the VPN tunnel while traffic from the "disallowed apps" list are unable to pass through. Use the allowed apps or disallowed apps URL scheme parameters if the device is not a managed device using a Mobile Device Manager (MDM) solution.

Users can have multiple configurations, but can choose only one at a time. Per-app VPN gives IT granular control over corporate network access, and ensures that data transmitted by managed apps travels only through a separate VPN tunnel and are isolated in the workspace. Meanwhile, other data, like an employee's personal web browsing activity, does not use the VPN. Per-app VPN also works with the mobile browser on a per-app basis on Android 5.0 and later versions. Users with Android for Work should use the same configuration as per-app VPN with Android F5 Access.

A per-app VPN configuration requires four configuration components.

- A device under MDM management.
- A managed app installed on the device, or the mobile browser.
- F5 Access for Android installed on the managed device. For Android for Work, F5 Access should be installed within the Android for Work container.
- A related F5 Access configuration (VPN). This is configured with an MDM command that associates the app with an F5 Access configuration.

Note: *Per-app VPN is currently not supported for Android apps on Chrome OS.*

Additional Access Policy Manager Configuration Information

F5 Access for Android and Chrome OS session variables

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

Session variable	Description
session.client.type	Indicates the client type. For example, `Standalone`.
session.client.platform	Indicates the platform type, such as `Android or Chrome OS`.
session.client.plugin	Indicates whether the client is a plugin. This is always set to `0`.
session.client.app_id	The app ID for the client. For F5 Access for Android and Chrome OS this is `com.f5.edge.client_ics`.
session.client.app_version	The Android and Chrome OS app version for the client. For F5 Access for Android 3.0.4 this is `3.0.4`.
session.user.agent	Indicates the browser, device type, and operating system version of the client, as well as the version of F5 Access.
session.client.model	Indicates the model name of the mobile device. For example, `Nexus 6P`
session.client.platform_version	Indicates the platform and version of the mobile device. For example, 7.0.0 ***Note:*** *For Android Runtime on Chrome (ARC) the platform version points to Android container version instead of Chrome OS version.*
session.client.unique_id	Indicates the unique ID of the device. For example, 8ccaf965e51e3077.
session.client.imei	Indicates the IMEI ID of the device. For example, 490154203237518. (Not applicable for Chrome OS)
session.client.jailbreak	Indicates the jailbreak status of the device. `0` indicates the device is not jailbroken, `1` indicates the device is jailbroken, and an empty response indicates that the status of the device is unknown.
session.client.biometric_fingerprint	Indicates whether the device supports biometric fingerprint authentication. `1` indicates that a fingerprint is configured, `0` indicates that a fingerprint is not configured, or the device does not support fingerprint authentication.
session.client.vpn_scope	Indicates the scope of the VPN tunnel. The result is `device` for a device-wide VPN connection, and `per-app` for a per-app VPN. (Not applicable for Chrome OS)
session.client.vpn_tunnel_type	Indicates the type of VPN tunnel. For F5 Access for Android and Chrome OS, this is `L3`.

Session variable	Description
session.client.vpn_start_type	Indicates how the VPN connection was initiated. • `manual` - Indicates that the connection was initiated by the user. • `mdm` - Indicates that the connection was initiated by an MDM. • `system` - Indicates that the connection was initiated on system start-up, in Always-On Mode.
session.client.device_passcode_set	Indicates whether the user has a device unlock passcode, PIN, pattern, or biometric authentication configured. The results is `1` if a device lock is configured, and `0` if it is not.
session.client.always_connected_mode	Indicates whether Always-On Mode is configured for the device. The results is `1` if Always-On Mode is enabled, and `0` if it is not.
session.client.hostname	This is a human-readable mobile device name. The results depends on the device manufacturer and OS version, this might be a Bluetooth device name that can be changed by user, a Wi-Fi Direct device name that can be changed by user, or a Linux hostname (for example, `android-8ab2bead5c56a02a`).
session.client.js	Indicates whether the device used Web Logon mode to log on. The result is `1` if Web Logon Mode was used, and `0` if it was not.

Access Policy Manager configuration tips

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

Feature	Information
Proxy servers	Public and private-side proxy servers are not currently supported.
Client endpoint checks	Client end-point checks are not currently supported.
Require device authentication	For devices with Android 6.0 or later, F5 Access can require device authentication with one of the device locking methods, including biometric authentication, a PIN, a pattern, or a passphrase. To enable device authentication for F5 Access, in the **Connectivity Profile** under **Android Edge Client**, enable the options **Allow Password Caching** and **Require Device Authentication**. This setting has no effect on for devices with a pre-Android 6.0 OS. On such devices, even with this setting configured on the server, users must enter a password for each connection.
Password caching policy	• In the Connectivity profile, you can configure password caching by enabling the setting `Allow Password Caching`. When this setting is enabled, after a successful logon the submitted credentials are cached. • Specify a `Save Password Method`. • If you select **disk**, an encrypted password is cached on the device with no expiration time.

Feature	Information
	• If you select **memory**, an encrypted password is cached on the device for the time specified in the **Password Cache Expiration (minutes)** field. • Credentials are not cleared if the user disconnects or restarts the device. • If credentials are cached and the **Save Password Method** is **memory**, then 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 username of the configuration within the application changes. • The F5Access user switches between configurations. • To require the user to authenticate on the device before unlocking the cached credentials, select **Require Device Authentication.**
Client certificates	Client certificate authentication is supported in Web Logon mode with or without a password. In standard logon mode, certificates are supported, but a password is required. A password (including an empty password) can be saved in the configuration.

About starting the client from a URL scheme

You can start F5 Access connections for users from a URL. You can then provide these URLs to users, so they can start the VPN connection without having to manually start the application. If there is already an active connection, a prompt appears to warn the user that the existing connection must be stopped before the new connection can start. The connection uses a client certificate if it is specified in the existing configuration.

URL connections use the following parameters. This is an example, you must provide your own parameters and values.

```
f5access://{start|stop}?[parameter1=value1&parameter2=value2...]
```

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

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

```
f5access-lite://{start|stop}?[parameter1=value1&parameter2=value2...]
```

The syntax to start a connection from a URL follows.

`start`

Starts a connection. The `start` command requires either the `name` or `server` parameter to be present in the URL. If the `name` parameter is specified, then F5 Access looks for the name in the list of existing configuration entries. If the `server` parameter is specified, then the `name` parameter is set to the same value as the `server` parameter. A new configuration is created if a configuration with that name does not exist. If the specified configuration already exists, the other parameters specified in the URL are merged with the existing configuration. The result of this merged configuration is used only for the current, active connection, and does not persist. If a `name` is specified with other parameters, such as `server`, `username`, or `password`, those parameters override what is specified in the configuration.

`sid`
A parameter used to specify the session ID with which to start the connection. When the parameter `sid` is provided, the `username` and `password` parameters are ignored, and no additional authentication occurs.

`username`
A parameter used to specify the user name with which to start the connection. When the `username` is specified without a `password`, then an authentication prompt is displayed.

`password`
A parameter used to specify the password with which to start the connection. When the `password` parameter is specified, it is used as a one-time password and not saved in the configuration.

`postlaunch_url`
A parameter used to specify the URL that starts after the connection starts.

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

`hide_ui_when_connected`
An optional parameter to minimize the F5 Access user interface for users when a connection has been established successfully.

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

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

`securid_sn`
An optional parameter to present the software token serial number for RSA SecurID authentication.

`allowBypass`
An optional parameter to allow apps to bypass VPN connection.

Examples of starting a client from a URL

The following examples illustrate how to start F5 Access connections for users from a URL.

Connecting to an existing configuration called `MYVPN`:

```
f5access://start?name=MYVPN
```

Connecting to an existing configuration called `MYVPN` and including the server URL `myvpn.siterequest.com`:

```
f5access://start?name=MYVPN&server=myvpn.siterequest.com
```

Connecting to a specific server called `myvpn.siterequest.com`:

```
f5access://start?server=myvpn.siterequest.com
```

Connecting to a specific server called `myvpn.siterequest.com` with web logon enabled:

```
f5access://start?server=myvpn.siterequest.com&logon_mode=web
```

Connecting to an existing configuration called `MYVPN` and including the username `smith` and the password `passw0rd`:

```
f5access://start?name=MYVPN&username=smith&password=passw0rd
```

Starting a connection to a configuration called `MYVPN` and specifying the post-launch URL `jump://?host=10.10.1.10&username=smith`:

```
f5access://start?name=MYVPN&postlaunch_url=jump%3A%2F%2F%3Fhost%3D10.10.1.10
%26username%3Dsmith
```

Starting a connection called `apm_rsa` with a SecurID software token `000117906115`.

```
f5access://start?name=apm_rsa&securid_sn=000117906115
```

Stopping a connection:

```
f5access://stop
```

Minimizing the F5 Access UI:

```
f5access://start?name=MYVPN&username=smith&password=passw0rd
&hide_ui_when_connected=yes
```

Starting a connection in Lite mode:

```
f5access-lite://start?name=apm&server=edgeportal.siterequest.com
&username=test&x-cancel=http%3A%2F%2Fgoogle.com
&x-error=http%3A%2F%2Fyahoo.com&x-success=http%3A%2F%2Ff5.com
```

Stopping a connection in Lite mode:

```
f5access-lite://stop?x-cancel=edgeportal.siterequest.com
&x-error=http%3A%2F%2Fyahoo.com&x-success=http%3A%2F%2Ff5.com
```

Allowing a list of applications to access the VPN:

```
f5access://start?name=myvpn&allowed_apps=com.android.chrome,org.mozilla.firefox
```

Preventing a list of applications access the VPN:

```
f5access://start?name=mvypn&disallowed_apps=com.android.chrome,org.mozilla.firefox
```

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:

```
f5access://create?server=server_address[&parameter1=value1&parameter2=value2...]
```

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

The syntax to define a server from a URL follows.

`server`
The server address is either a DNS name or an IP address.

`name`
An optional description of the server.

`username`
An optional parameter used to specify the user name with which to start the connection. When the `username` is specified without a `password`, then an authentication prompt is displayed. If no `username` is specified during server creation, the user is prompted for it at session initiation, if required.

`password`
An optional parameter used to specify the password with which to start the server connection. When the `password` parameter is specified, it is used as a one-time password and not saved in the configuration.

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

`cert_keychain_alias`
Identifies a certificate from the device credentials storage.

`certcn`

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

Important: *Only one of `certcn`, `cert_url`, or `cert_keychain_alias` can be specified.*

`logon_mode`

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

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

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

securid_sn

An optional parameter to present the software token serial number for RSA SecurID authentication.

allowBypass

An optional parameter to allow apps to bypass VPN connection.

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 `edgeportal.siterequest.com`:

```
f5access://create?server=edgeportal.siterequest.com
```

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

```
f5access://create?name=EdgePortal&server=edgeportal.siterequest.com
```

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

```
f5access://create?name=EdgePortal&server=edgeportal.siterequest.com
&username=edgeportal&password=androiddemo&certcn=clientcert-cert.siterequest.com
```

Create the same server with a user name and certificate:

```
f5access://create?name=EdgePortal&server=edgeportal.siterequest.com
&username=edgeportal&certcn=clientcert-cert.siterequest.com
```

Identify a certificate from the device credentials storage:

```
f5access://create?server=edgeportal.siterequest.com&name=EdgePortal
&cert_keychain_alias=<certificate alias>
```

Creating a connection called `apm_rsa` to server `https://rsa.siterequest.com` with a SecurID software token `000117906115`.

```
f5access://create?name=apm_rsa&server=https%3A%2F%2rsa.siterequest.com
&logon_mode=web&securid_sn=000117906115
```

Creating a list of applications allowed to access the VPN:

```
f5access://create?server=edgeportal.siterequest.com&name=EdgePortal
&allowed_apps=com.android.chrome,org.mozilla.firefox
```

Creating a list of applications forbidden to access the VPN:

```
f5access://create?server=edgeportal.siterequest.com
&name=EdgePortal&disallowed_apps=com.android.chrome,org.mozilla.firefox
```

Index