BIG-IP® Local Traffic Manager: Configuring a Custom Cipher String for SSL Negotiation

Version 13.0

Table of Contents

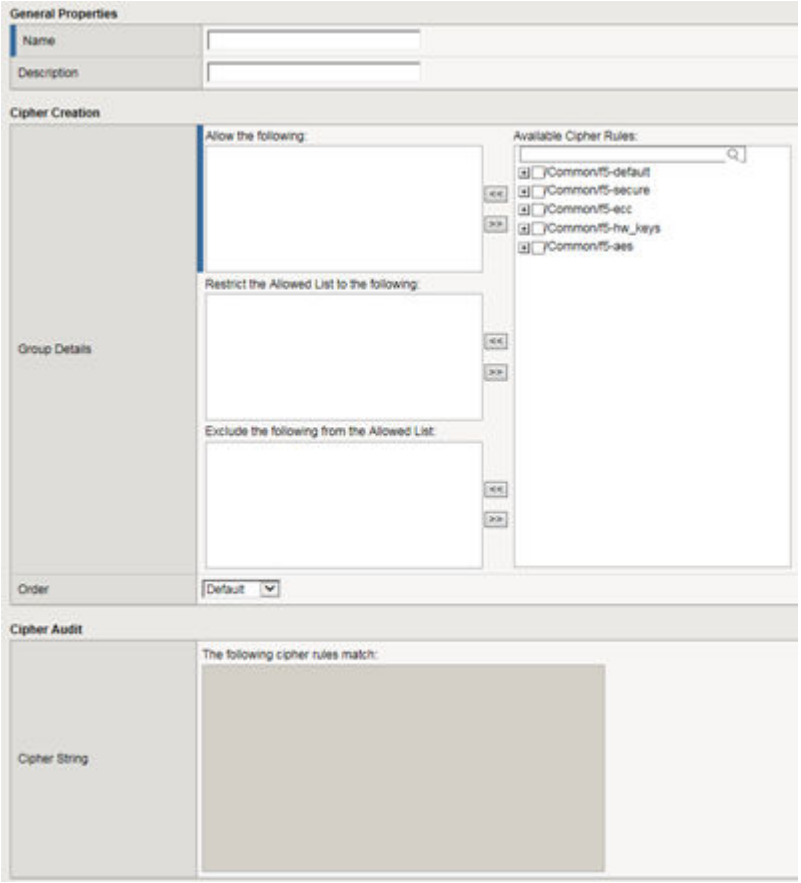
Configuring a custom cipher string for SSL negotiation

Overview: Configuring a custom cipher string for SSL negotiation

Before the BIG-IP® system can process SSL traffic, you need to define the cipher string that you want the system to use when negotiating security settings with client or server systems.

Typing a raw cipher string on the system is tedious and can easily contain typos. It can also be unsecure, since the cipher string could inadvertently cause the system to negotiate in a way that you didn't intend.

To avoid these problems, you can use cipher rules and cipher groups. With cipher rules and groups, you instruct the BIG-IP system which cipher suites to include and exclude, and the system will build the cipher string for you. This illustration shows the main screen for creating a cipher group.



Use of cipher groups and cipher rules is optional.

About BIG-IP cipher support

The BIG-IP® system supports a large set of cipher suites that you can choose from to build the cipher string used for security negotiation.

Supported cipher suites include various combinations of encryption algorithms and authentication mechanisms, including RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm), and ECDSA (Elliptic Curve Digital signature Algorithm).

The system includes a default cipher string represented by the keyword `DEFAULT`, which contains a subset of the cipher suites that the BIG-IP system supports.

What is a cipher rule?

A *cipher rule* is an object that contains cipher-related information such as an encryption algorithm and a key exchange method. The BIG-IP system will use one or more cipher rules within a cipher group, to build the cipher string that the system will use to negotiate SSL security parameters with a client or server system.

You can use pre-defined cipher rules that the BIG-IP system provides, or you can create your own. In either case, after you decide which cipher rules you want to use, you then specify the cipher rules within a *cipher group*, which is the object that builds the actual cipher string that the system will use during SSL negotiation. Then you just need to specify the cipher group within a Client SSL or Server SSL profile, and assign the profile to a virtual server.

An example of a cipher rule might be one that specifies only ciphers that use a particular bulk encryption algorithm and a key exchange method.

What is a cipher group?

A *cipher group* contains a list of cipher rules, and the instructions that the BIG-IP® system needs for building the cipher string it will use for security negotiation. The instructions tell the system which cipher rules to include in the string, and how to apply them (allow, disallow, and so on, and in what order).

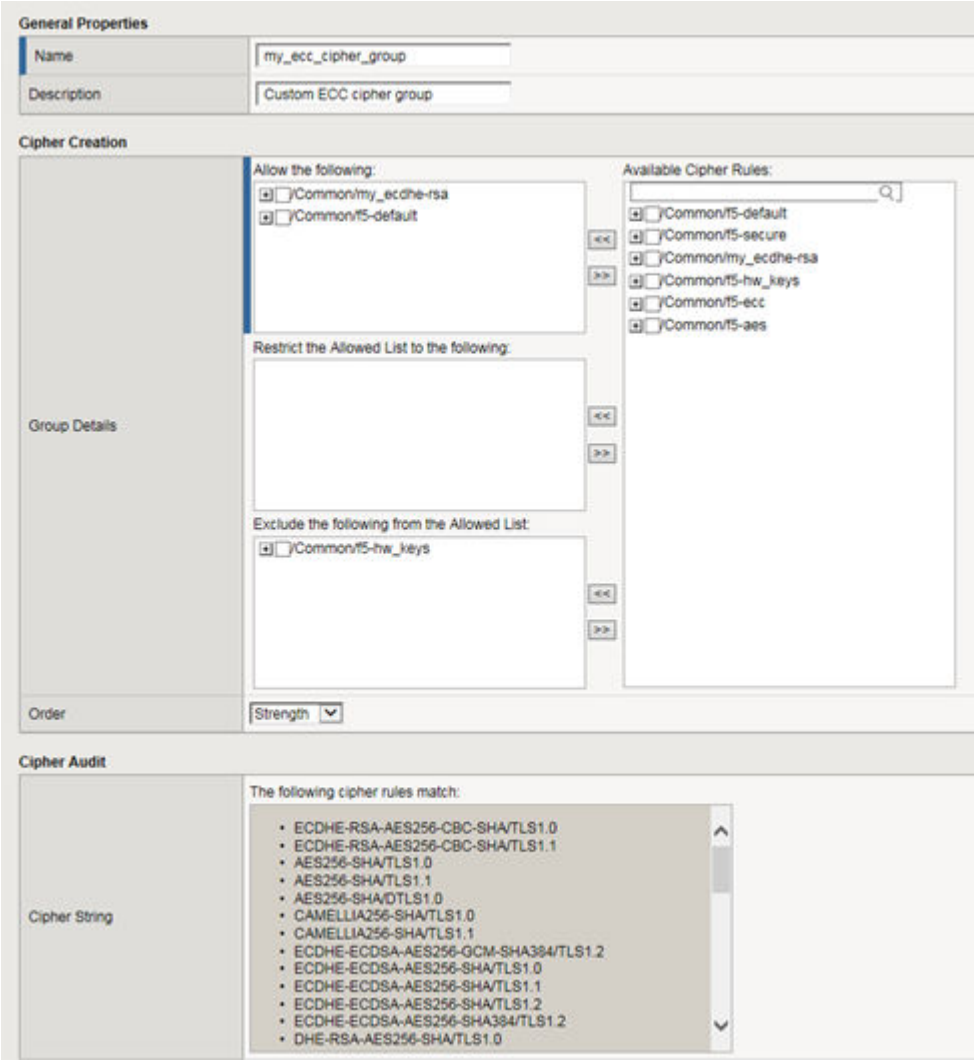
Pre-built cipher groups

The BIG-IP system offers a few pre-built cipher groups that you can choose from to use as is to build your final cipher string, However, it's common to create your own custom cipher group instead.

Custom cipher groups

This illustration shows an example of a custom cipher group. Using this cipher group, the BIG-IP system builds the final cipher string using a user-created custom cipher rule named `/Common/my_ecdhe_rsa` and the pre-built cipher rule `/Common/f5-default`.

Notice that the system will exclude from the string any cipher suites defined in the pre-built cipher rule `/Common/f5-hw_keys`.



Also notice that the cipher group displays a preview of the final cipher string after the instructions are applied.

Best practices for BIG-IP cipher strings

For security and performance reasons, consider the following recommendations:

- Always append cipher suites to the `DEFAULT` cipher string.
- Include a cipher string that specifies the ECC key type, because its shorter length speeds up encryption and decryption while still offering virtually the same level of security.
- Disable ADH ciphers but also include the keyword `HIGH`. To do this, just include both `!ADH` and `:HIGH` in your cipher string.
- For AES, DES, and RC4 encryption types, make sure you specify the DHE key exchange method. DHE uses *Forward Privacy*, which creates a key that it throws away after each session so that the same session key never gets used twice. When you use DHE, make sure that the SSL private key isn't being shared with a monitoring system or a security device like an intrusion detection or prevention system. And by the way, diagnostic tools like `ssldump` won't work when you're using Forward Secrecy.
- Disable EXPORT ciphers by including `!EXPORT` in the cipher string.
- If you can live with removing support for the SSLv3 protocol version, do it. This protocol version is unsecure. Simply include `:!SSLv3` in any cipher string you build.

View all cipher suites supported by BIG-IP system

Before you start this task, make sure your user account gives you permission to access the BIG-IP® advanced shell.

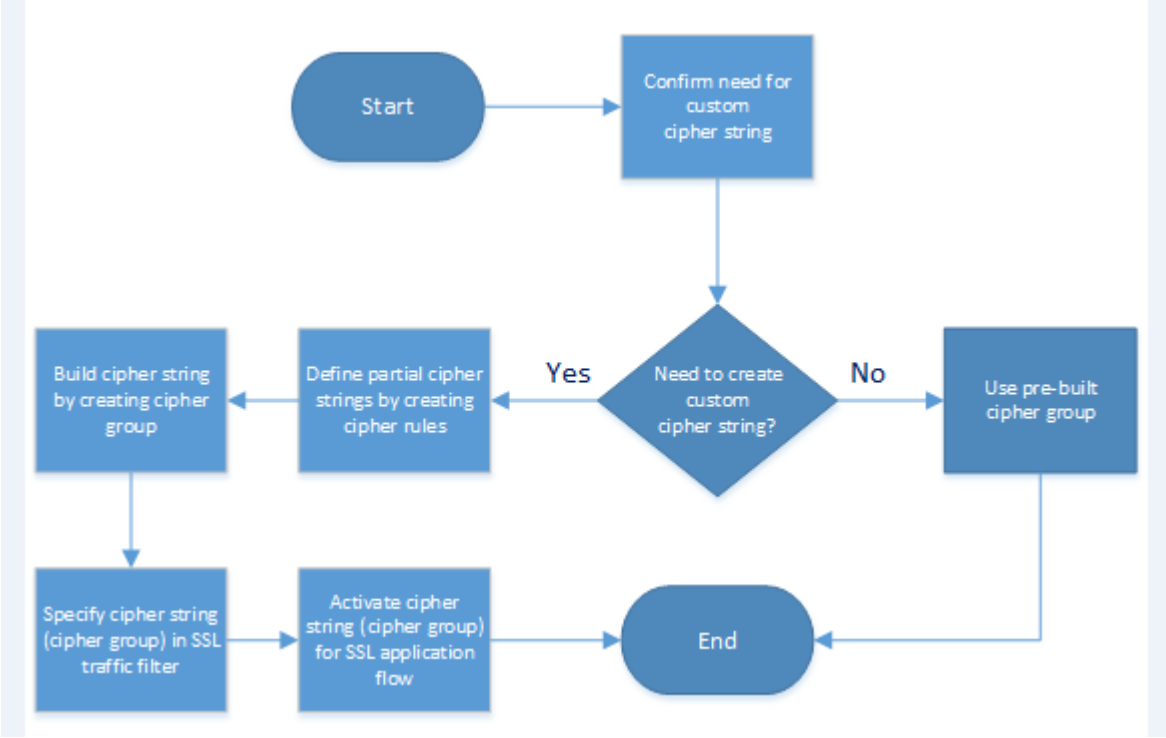
You can use the BIG-IP advanced shell to view all cipher suites that the BIG-IP system supports.

1. Using a console access application such as PuTTY, log in to the advanced shell on the BIG-IP system.
2. At the system prompt, type either `tmm --clientciphers all` or `tmm --serverciphers all`.
   The system lists all supported cipher suites for either client-side or server-side traffic.

Task summary for configuring a custom cipher string

There are a few tasks you need to perform to use cipher rules and cipher groups to configure the cipher string that the BIG-IP® system will use for SSL negotiation.

This illustration shows the order that you need to perform these tasks in.



Confirm the need for a custom cipher string
Create partial cipher strings to include in a custom cipher string
Build a custom cipher string
Specify a custom cipher string within an SSL traffic filter
Activate a cipher string for an application flow

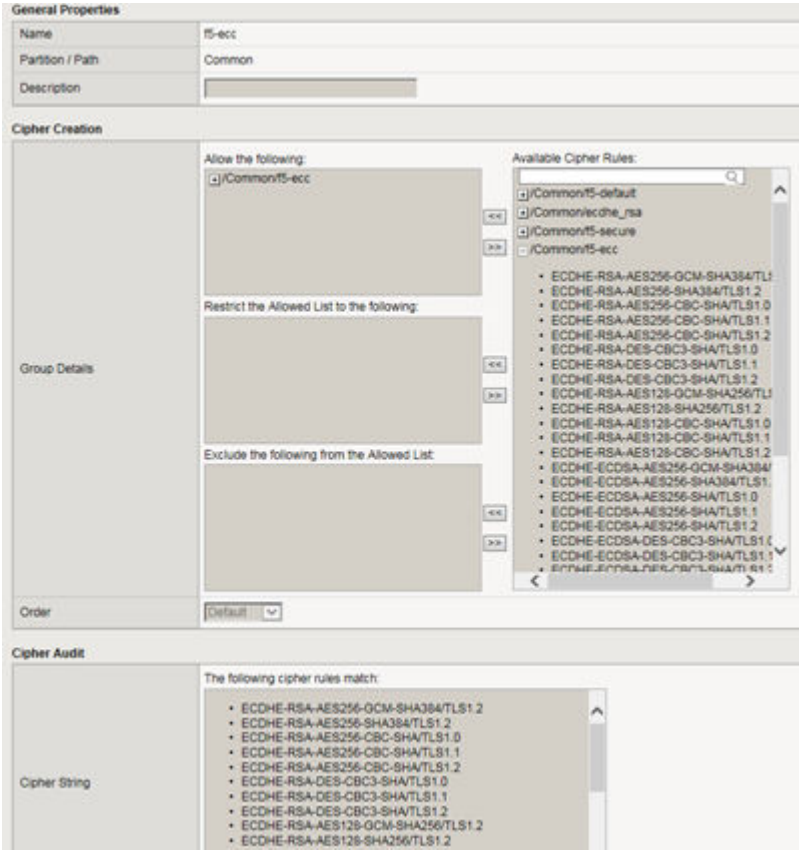
Confirm the need for a custom cipher string

Before you create and deploy a custom cipher string, you can review the pre-built cipher groups on the BIG-IP® system to see if any of them already contains the cipher suites you need.

1. On the Main tab, click **Local Traffic** > **Ciphers** > **Groups**.
   The screen displays a list of pre-built cipher groups.

2. In the Name column, click the name of a cipher group.
   For example, click `/Common/f5-ecc`.
   The system displays the contents of the cipher group.
3. In the **Available Cipher Rules** list, find the corresponding cipher rule and click the plus sign to view the cipher suites included in the rule.

   For example, this shows the pre-built cipher group `/Common/f5-ecc` and the cipher suites included in it.



   If the cipher suites in the corresponding cipher rule are not sufficient for your cipher string, you'll need to create your own custom cipher group.
4. Click **Cancel**.
5. As an option, you can repeat this task for any other pre-built cipher groups.

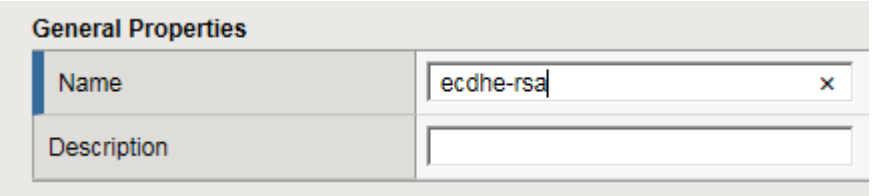
Create partial cipher strings to include in a custom cipher string

When you create your own cipher rules for a custom cipher group, the BIG-IP® system can build a cipher string that includes or excludes the cipher suites you need for negotiating SSL connections.

1. On the Main tab, click **Local Traffic** > **Ciphers** > **Rules**.
   The screen displays a list of pre-built cipher rules.
2. Click **Create**.
3. In the **Name** field, type a name for the cipher rule.

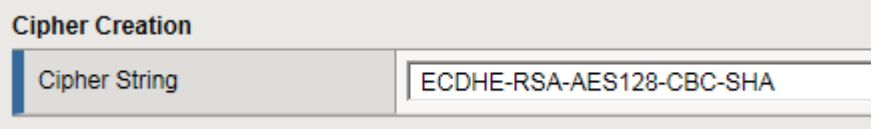
   Note: *Never include the prefix* `f5-` *in a cipher rule name. This prefix is reserved for pre-built cipher rules only.*

   For example:



4. In the **Cipher String** field, type a cipher string that represents one or more cipher suites.

   For example:



5. Click **Finished**.

The cipher rule now appears within any custom cipher group, in the list of available cipher rules.

Build a custom cipher string

Before starting this task, make sure you've confirmed the need to create a custom cipher string instead of using a pre-built cipher group.

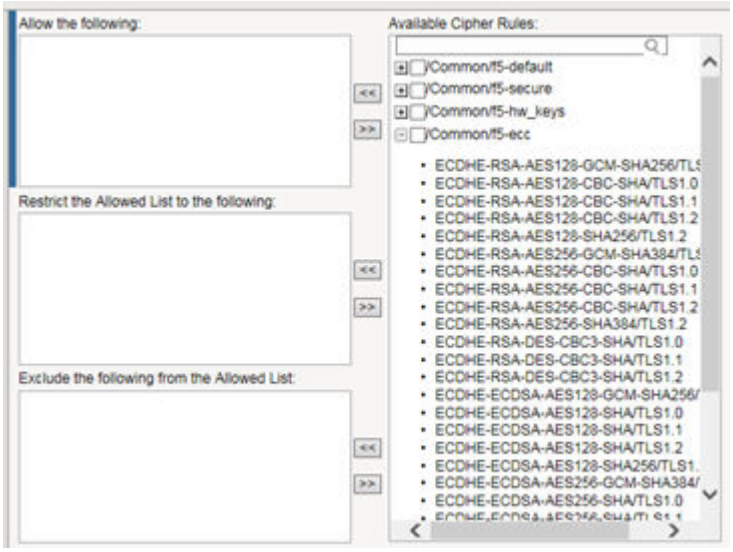
You build a final, custom cipher string by creating a cipher group. A *cipher group* contains the cipher rules and instructions that the BIG-IP® system needs for building the cipher string it will use for security negotiation with a client or server system.

1. On the Main tab, click **Local Traffic** > **Ciphers** > **Groups**.
   The screen displays a list of pre-built cipher groups.
2. Click **Create**.
3. In the **Name** field, type a name for the cipher group.

   Note: *Never include the prefix* `f5-` *in a cipher rule name. This prefix is reserved for pre-built cipher groups only.*

4. If you created any custom rules, then in the Cipher Creation area of the screen in the **Available Cipher Rules** list, verify that the custom rules appear in the list.
5. For each cipher rule in the **Available Cipher Rules** list, click the plus sign to view the cipher suites included in the rule.

   For example, this shows the cipher suites included in the pre-built cipher rule named `/Common/f5-ecc`.



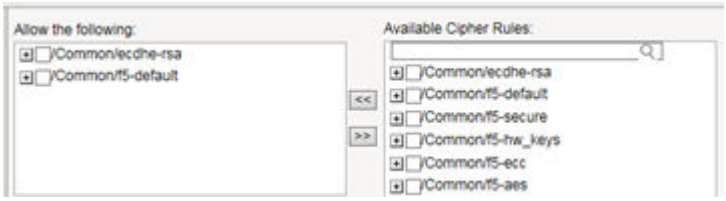
6. In the **Available Cipher Rules** list, select the boxes for the cipher rules you want to allow for negotiating security for SSL connections.

   Important: *We strongly recommend that you select the cipher rule* `/Common/f5-default`*, and for added security, select other cipher rules, too.*

   Here's an example of a list of available cipher rules that you might see within a cipher group. Notice that we've selected both a pre-built cipher rule and a custom cipher rule:

7. Move the selected cipher rules to the **Allow the following** box.

   Here we see that we're instructing the BIG-IP system to allow, during security negotiation, the cipher suites contained in the selected cipher rules:



8. Again from the **Available Cipher Rules** list, select the boxes for the cipher rules you want to restrict the allowed cipher rules to when negotiating security for SSL connections.
9. Using the Move button, move the selected cipher rules to the **Restrict the Allowed list to the following** box.
10. If you want to exclude any cipher rules from the allowed list, then from the **Available Cipher Rules** list, select the boxes for the rules you want to exclude.
11. Using the Move button, move the selected cipher rules to the **Exclude the following from the Allowed list** box.
12. From the **Order** list, select the order that you want the BIG-IP system to use when negotiating SSL connections.

    The choices are: **Default**, **Speed**, **Strength**, **FIPS**, and **Hardware**.

13. In the Cipher Audit area of the screen, view the cipher string that the BIG-IP system will construct based on the selections you made in the previous steps.
14. Click **Finished**.

After you complete this task, the BIG-IP system has a custom cipher group that the BIG-IP system will use to build the final cipher string.

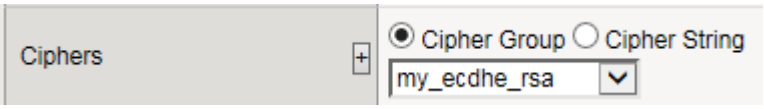
Specify a custom cipher string within an SSL traffic filter

Before starting this task, make sure that the relevant traffic filter for managing SSL traffic (either a Client SSL or Server SSL profile) exists on the BIG-IP® system.

Specifying a custom cipher group within a particular Client SSL or Server SSL profile tells the BIG-IP system which cipher string to use when negotiating security settings.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client** or **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The Client SSL or Server SSL profile list screen opens.
2. Click the name of a profile.
3. From the **Configuration** list, select **Advanced**.
4. On the right side of the screen, select the **Custom** check box.
5. For the **Ciphers** setting, click **Cipher Group** and from the list, select a custom cipher group.

   This shows a custom cipher group selected for the `Ciphers` setting:



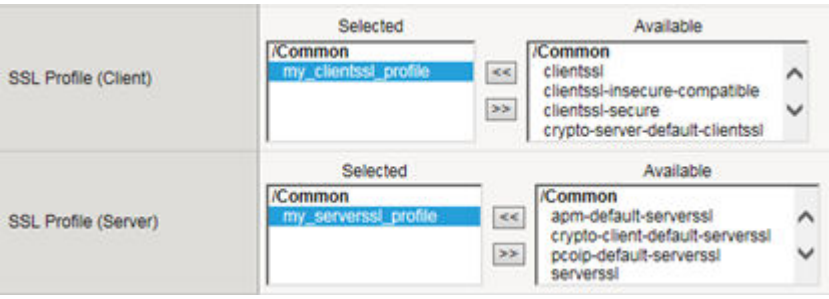
6. Click **Update**.

Activate a cipher string for an application flow

Before starting this task, make sure that the virtual server for the relevant SSL application flow exists on the BIG-IP® system.

You activate a cipher string for a specific application flow by assigning a Client SSL or Server SSL profile (or both) to a virtual server. This causes the BIG-IP system to use the cipher group specified in the profile to build the cipher string for negotiating security settings for SSL connections.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of a virtual server.
3. From the **Configuration** list, select **Advanced**.
4. For the **SSL Profile (Client)** and the **SSL Profile (Server)** settings, from the **Available** list, select the name of the SSL profile you previously created, and move the name to the **Selected** list:



Using the **SSL Profile (Server)** setting is optional.

5. Click **Update** to save the changes.

The BIG-IP system now uses the cipher group specified in an SSL profile to build a cipher string to use when negotiating security for the relevant application flow.

Legal Notices

Legal notices

Publication Date

This document was published on March 12, 2018.

Publication Number

MAN-0655-00

Copyright

Trademarks

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

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

Patents

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

Link Controller Availability

This product is not currently available in the U.S.

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.

Index