F5® BIG-IQ® Centralized Management: Local Traffic & Network Implementations

Version 5.4

Table of Contents

Managing Local Traffic Profiles

How do I manage LTM profiles in BIG-IQ?

You can create or modify custom LTM® profiles in BIG-IQ® Centralized Management and then attach them to a local traffic object (such as a virtual server, pool, or pool member) to deploy them to your managed devices.

When you create a profile, you specify a parent profile from which the custom profile inherits its properties. You then specify which of these properties you want to override. You can name any existing profile as a parent profile. When you modify a profile that has *child profiles* (that is, profiles that name your profile as a parent profile), all of the child profiles inherit any changes you made in the parent profile (except those you choose to override).

You can also copy a profile from one BIG-IP device to another: import the profile from the source device, associate the profile to the objects on the target device that you want to use that profile, and deploy your changes.

Important: *If you share profiles between devices, we recommend that you use unique profile names. Otherwise, BIG-IQ will attempt to define all profiles that share a name with the same parameters and values. When you deploy changes, you will have the opportunity to decline this behavior, but you can avoid having to do so by naming each profile uniquely.*

Create an LTM profile

You must discover a device and import that device's service configurations before you can add a profile to that device from BIG-IQ® Centralized Management.

Creating a new profile allows you to specify the parameters that define the characteristics you want your virtual servers to use. Each virtual server that references this profile uses the parameters you specify for this profile. Additionally, the parameters you define for this profile are given to the profiles that name this profile as their parent profile.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Profiles**.
   The screen displays the list of profiles defined on this device.
2. Click **Create**.
   The New Profiles screen opens.
3. In the **Name** field, type in a name for the LTM profile you are creating.
4. For **Partition**, type the name of the BIG-IP® device partition on which you want to create the profile.
5. For the **Type**, select the type of profile you want to create.
   The **Parent Profile** setting displays.
6. From **Parent Profile**, select the parent profile from which you want your profile to inherit settings.

   Note: *The parent profile you select determines the value of the profile parameters for this profile. You can override these values, but if you do not, changes made to parameters in the parent profile propagate to all child profiles.*

A number of additional settings display, specifying the parameters associated with the parent profile you selected. There are two controls for each field. The first one (a check box) controls whether you want to override the inherited value for that field. The second control (the type varies by field) sets the value you want for the parameter.

7. For any fields you want to override, select the **Override** check box and then specify the value you want for the fields you selected.

   Note: *You can select* ***Override All*** *if you want to override all of the parent profile parameter values.*

   Important: *If you override a parent profile parameter, regardless of whether or not you change the parameter's value, then future changes to the parent's parameter value will not be inherited by this profile.*

   Note: *For detailed information about the impact of using a particular profile parameter value, refer to the BIG-IP Local Traffic Management: Profiles Reference on* `support.F5.com`.

8. If you are adding a profile that requires a security parameter, specify the passphrase in the corresponding **Passphrase** field.

   Note: *For version 12.0.0 devices, you do not need to supply the pass phase for the profile. For devices earlier than version 12.0.0, if you plan to make changes to a Client SSL profile, you need to supply the pass phrase for that profile. If you do not change any of the parameters for the profile or associate the profile with a virtual server or another client SSL profile, then you can leave this field blank. So, if you add a pre-version 12.0.0 device that has a significant number of profile definitions, you do not need to add the pass phrase for every profile, just the ones that you plan to change or associate with an LTM object.*

9. Click **Save & Close**.
   The system creates the new profile you specified and adds it to the list of profiles.

You can now use the profile you created. You can select it when you configure a virtual server. You can also use it as a parent profile to base new BIG-IP LTM profiles on.

You must deploy your changes to the BIG-IP device before you can see these changes on the device.

Edit an LTM profile

By editing a profile, you can revise the parameters that define the characteristics you want your virtual servers to use. Each virtual server that references this profile uses the parameters you specify for this profile. Additionally, the parameters you define for this profile are given to the profiles that name this profile as their parent profile.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Profiles**.
   The screen displays the list of profiles defined on this device.
2. Click the name of the profile you want to edit.
   The screen displays the current settings for the selected profile.
3. Under Referenced by, note the virtual servers and profiles that refer to this profile.

   Changes you make to this profile impact all of the virtual servers listed here.

   Any changes you make to this profile are also inherited by all profiles listed here that name this profile as their parent profile.
4. Under the **Override All** check box, select the check box corresponding to any fields you want to override, and then specify the value you want for the fields you selected.

Note: *You can select* ***Override All*** *if you want to override all of the parent profile parameter values.*

Note: *For detailed information about the impact of using a particular profile parameter value, refer to the BIG-IP Local Traffic Management: Profiles Reference on* `support.F5.com`.

5. If you imported a profile that requires a security parameter, specify the passphrase in the corresponding **Passphrase** field.

Important: *For imported profiles that use passphrases:*

- If the profile was imported from a version 12.0.0 or later device, you do not need to re-enter the passphrase.
- If the profile was imported from a device earlier than version 12.0.0 and you plan to make changes to the profile (or if you associate the profile with a virtual server or a child profile), then you must supply the passphrase for the imported profile.
- If you do not change any of the parameters for the profile or associate the profile with a virtual server or a child profile, then you do not need to re-enter the passphrase.

6. When your edits are complete, click **Save & Close**.
   The system updates the profile with the settings you specified and adds it to the list of profiles.

You must deploy your changes to the BIG-IP® device before you can see these changes on the device.

Copy an LTM profile from one device to existing objects on another

To copy a profile from one device to another, the target device must have objects that use the profile. If these objects do not already exist on the target device, you can create them as part of the workflow. Refer to *Copy an LTM profile from one device to new objects on another* on `support.f5.com` for that workflow.

To copy a profile from one device to another, you import the profile from the source device, associate the profile to selected objects on the target device, and then deploy your changes to the target device.

Note: *In this release, support for copying profiles is limited to the following profile types:*

SSL

clientssl
serverssl
certificateauthority

HTTP

http

Persistence(default and fallback)

cookie
source_addr
ssl
universal

Protocol

tcp
fastL4

Acceleration

Web Acceleration
OneConnect

HTTP Compression

Note: *If you import a read-only profile from a BIG-IP 13.0 device, you cannot copy that profile to an BIG-IP 11.0 device. The following version 13.0 profiles are read-only:*

- tcp
- f5-tcp-lan
- f5-tcp-mobile
- f5-tcp-progressive
- f5-tcp-wan

1. Identify your source and target BIG-IP devices as well as the name of the profile you want to copy and the objects that you want to attach the profile to.
   a) Identify the source BIG-IP device (the device that has the profile you want to copy).
   b) Identify the name of the profile that you want to copy.
   c) Identify the target BIG-IP device (the device to which you want to copy the profile).
   d) Identify the objects on the target device that you want to attach the profile to.
2. If you have not already discovered and imported services for both the source and target device, do that now.

   For details on how to discover a device and import services, refer to *Device Discovery and Basic Device Management* on `support.f5.com`.

   When discovery and import is complete, both devices will be under management, the BIG-IQ device will have all of the profiles from the source device, as well as all of the objects from the target device that you want to use the profile with.
3. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC**.
4. Click the name of a local traffic object that you want to associate the profile with when you copy it to the target BIG-IP device.
   For example, if you plan to associate the profile with a virtual server, click **Virtual Servers**.
   The list of objects of the type you selected (virtual servers in this case) that reside on the devices managed by this BIG-IQ device is displayed.
5. Click the name of the object that you want to associate with the copied profile.
   The properties screen for the selected object opens.
6. For the profile type that you want to associate with this object, select the specific profile you want to use.
   For example, if you are associating an HTTP profile with a virtual server, you might select **/common/http** from the **HTTP Profile** parameter.
7. Repeat the previous step for the other profiles you want to associate with this object.
8. When you are finished assigning profiles to this object, click **Save & Close**.
   The system saves the profile associations for the object you selected.
9. Repeat the previous five steps for the other object types that you want to copy profiles for to the target device.
   For example, you might specify virtual servers first, and then define the pools, pool members, and nodes.
10. When you have specified all of the objects and profiles you want to copy, deploy these changes to the target device.

    For details on deploying changes to a managed device, refer to *Deploying Changes* on `support.f5.com`.

You must deploy your changes to the target BIG-IP® device before the profiles are copied.

Copy an LTM profile from one device to new objects on another

To copy a profile from one device to another, you import the profile from the source device, associate the profile to selected objects on the target device, and then deploy your changes to the target device.

Note: *In this release, support for copying profiles is limited to the following profile types:*

SSL
clientssl
serverssl
certificateauthority

HTTP
http

Persistence(default and fallback)
cookie
source_addr
ssl
universal

Protocol
tcp
fastL4

Acceleration
Web Acceleration
OneConnect
HTTP Compression

Note: *If you import a read-only profile from a BIG-IP 13.0 device, you cannot copy that profile to an BIG-IP 11.0 device. The following version 13.0 profiles are read-only:*

- tcp
- f5-tcp-lan
- f5-tcp-mobile
- f5-tcp-progressive
- f5-tcp-wan

1. Identify your source and target BIG-IP devices as well as the name of the profile you want to copy and the objects that you want to attach the profile to.
   a) Identify the source BIG-IP device (the device that has the profile you want to copy).
   b) Identify the name of the profile that you want to copy.
   c) Identify the target BIG-IP device (the device to which you want to copy the profile).
   d) Identify the objects on the target device that you want to attach the profile to.
2. If you have not already discovered and imported services for both the source and target device, do that now.

   For details on how to discover a device and import services, refer to *Device Discovery and Basic Device Management* on `support.f5.com`.

   When discovery and import is complete, both devices will be under management, and the BIG-IQ will have all of the profiles from the source device.

3. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC**.
4. Click the name of a local traffic object that you want to associate the profile with when you copy it to the target BIG-IP device.
   For example, if you plan to associate the profile with a virtual server, click **Virtual Servers**.
   The list of objects of the type you selected (virtual servers in this case) that reside on the devices managed by this BIG-IQ displays is displayed.
5. Click **Create**.
   The create new object screen for the selected object opens.
6. In the **Name** field, type in a name for the object you are creating.
7. From the **Device** list, select the device on which to create the new object.
8. For the profile type that you want to associate with this object, select the specific profile you want to use.
   For example, if you are associating an HTTP profile with a virtual server, you might select **/common/http** from the **HTTP Profile** parameter.
9. Specify the additional settings needed to suit the requirements for this object.

   The parameters required to create an LTM object vary with the object type. (For example, the only required parameters for a new virtual server are the **Name**, **Device**, **Destination Address**, and **Service Port**.) The remaining parameters are optional and perform the same function as they do when you configure a virtual server on a BIG-IP device.

   Note: *For details about the purpose or function of a particular setting, refer to the BIG-IP reference information on support.f5.com.*

   ---

10. Repeat the previous step for the other profiles you want to associate with this object.
11. When you are finished assigning profiles to this object, click **Save & Close**.
    The system saves the profile associations for the object you selected.
12. Repeat the previous eight steps for the other object types that you want to copy profiles for to the target device.
    For example, you might specify virtual servers first, and then define the pools, pool members, and nodes.
13. When you have specified all of the objects and profiles you want to copy, deploy these changes to the target device.

    For details on deploying changes to a managed device, refer to *Deploying Changes* on `support.f5.com`.

You must deploy your changes to the target BIG-IP® device before the profiles are copied.

Managing Virtual Servers

How do I change object settings on a managed device?

To change the object settings on a managed device, there are four tasks to perform.

This figure illustrates the workflow you perform to manage the objects on BIG-IP® devices. Changing the settings is the second step in this process.

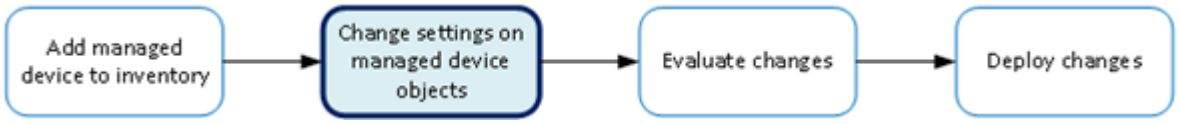

Figure 1: Change managed object workflow

What virtual server management tasks can I perform?

There are a number of ways you can use BIG-IQ® Centralized Management to manage the virtual servers on the managed BIG-IP® devices:

- Create a new virtual server.
- Modify an existing virtual server.
- Clone the settings of an existing virtual server to create a new one.
- Attach a sequence of iRules® to a virtual server.
- View statistics for a virtual server.
- Deploy the virtual server immediately to your managed device.

Note: *You (or someone else) can also deploy your changes later. For more information about managing changes, look on* `support.F5.com` *in F5 BIG-IQ Centralized Management: Device for the topic: Deploying Changes.*

- Add or remove permissions for a virtual server and assign them to roles that have been defined on this BIG-IQ system. For more information about managing permissions, look on `support.F5.com` in *F5 BIG-IQ Centralized Management: Licensing and Initial Setup* for the topic: *Users, User Groups, Roles, and Authentication*.

Create a new virtual server

In BIG-IQ® Centralized Management, you can use the Local Traffic interface to add a virtual server to a managed device.

Important: *When you are revising configurations on devices that belong to a high availability cluster, it is important to let the changes synchronize to the cluster members instead of trying to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

---

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Virtual Servers**.
   The screen displays the list of virtual servers defined on this device.

2. Click **Create**.
   The New Virtual Server screen opens.
3. In the **Name** field, type in a name for the virtual server you are creating.
4. From the **Device** list, select the device on which to create the virtual server.
5. For the **Destination Address**, type the IP address of the destination that you want this virtual server to send its traffic to.
6. In the **Service Port** field, type a service port number, or select a type from the list.

   When you select a type from the list, the value in the **Service Port** field changes to reflect the associated default, which you can change.
7. Specify the additional settings needed to suit the requirements for this virtual server.

   The remaining parameters on this screen are optional and perform the same function as they do when you configure a virtual server on a BIG-IP device.

   Note: *For details about the purpose or function of a particular setting, refer to the BIG-IP reference information on support.f5.com.*
8. Click **Save & Close**.
   The system creates the new virtual server with the settings you specified.

Clone a virtual server

You can use the BIG-IQ® Local Traffic interface to create a new virtual server based on the specifications for an existing one. Cloning can save you a lot of time if you need to create multiple virtual servers with similar settings.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Virtual Servers**.
   The screen displays the list of virtual servers defined on this device.
2. Select the check box for the virtual server that you want to clone.
3. Click the **Clone** button.
   The BIG-IQ creates a new virtual server using the settings of the one you selected and opens the Virtual Servers Clone screen so you can modify its parameters.
4. Modify the parameters for the new virtual server as needed.

   Important: *Two virtual servers cannot share the same* ***Destination Address****,* ***Protocol****, and* ***VLAN****.*
5. When you are satisfied with the settings for the new virtual server, click **Clone**.
   The system creates the new virtual server with the settings you specified.

Attach iRules to virtual servers

You can use the BIG-IQ® Local Traffic interface to attach iRules® to a set of virtual servers. Adding an iRule sequence to a group of servers at once can save time and help you cut down on errors that result from performing repetitious tasks.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Virtual Servers**.
   The screen displays the list of virtual servers defined on this device.
2. Select the check boxes associated with the virtual servers to which you want to attach iRules.
3. Click **Attach iRules**.
   The Bulk Attach iRules screen opens.

4. To specify which iRules to attach to the selected virtual servers, select them in the **Available iRules** list, and move them to the **iRules to be Attached** list.
5. Specify the order in which you want the iRules to attach using the up and down arrows.
6. For **Location**, specify the list position to attach these iRules.
   - To add the rules to the beginning of the existing list, click **Attach to top of each virtual server's iRules list**.
   - To add the rules to the end of the existing list, click **Attach to bottom of each virtual server's iRules list**.
7. Use the **Duplicate Policy** setting to specify whether to keep the iRule list order for iRules that are already attached to the virtual servers.
   - To keep the existing list order, click **Keep virtual servers' existing rules list order**.
   - To change the existing list order to what you specified previously, click **Reorder virtual servers' existing rules to preserve selected rules order**.
8. Click **Save & Close**.

Change virtual server settings

Using the BIG-IQ® user interface to make revisions to your virtual server configurations simplifies managing your devices.

Important: *If you revise configurations on devices that belong to a high availability cluster, the synchronizes BIG-IQ cluster members automatically when you deploy the change. Do not try to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Virtual Servers**.
   The screen displays the list of virtual servers defined on this device.
2. Click the name of the virtual server that you want to change.

   If you select the check box for the virtual server instead of the name, there are a couple of unique operations that you can perform. You can either clone a virtual server to create a new one based on the selected server (see *Cloning a virtual server*), or you can attach iRules to several virtual servers at once (see *Attaching iRules to virtual servers*).

   The Properties screen for the virtual server opens.
3. Make changes to the properties you want to modify.

   Note: *For detailed information about the impact of using a particular profile parameter value, refer to the BIG-IP Local Traffic Management: Profiles Reference on* `support.F5.com`.
4. When you are satisfied with the changes you have made, click **Save & Close**.
   The revisions you saved are made, and the Properties screen for the selected object closes.

Changes that you make are made only to the pending version. The *pending version* serves as a repository for changes you stage before deploying them to the managed device. Object settings for the pending version are not the same as the object settings on the actual BIG-IP® device until they are deployed or discarded.

To apply the working configuration settings to the BIG-IP device, you now need to deploy the revisions.

Managing iRules

How do I change object settings on a managed device?

To change the object settings on a managed device, there are four tasks to perform.

This figure illustrates the workflow you perform to manage the objects on BIG-IP® devices. Changing the settings is the second step in this process.

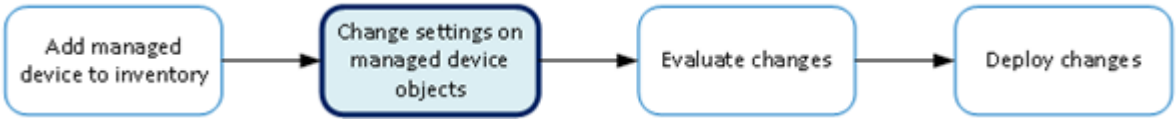

Figure 2: Change managed object workflow

Create a new iRule

You can use the BIG-IQ® Local Traffic interface to add a new iRule to a managed device.

Important: *When revising configurations on devices that belong to a high availability cluster, it is important to let the changes synchronize to the cluster members instead of trying to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

Important: *Rules are different from most other Local Traffic objects in that they associate with virtual servers instead of devices. So to deploy a new iRule to a device, you attach the iRule to a virtual server associated with the target device and then deploy that change.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **iRules**.
   The screen displays the list of iRules defined on this device.
2. Click **Create**.
   The New iRule screen opens.
3. For **Name**, type a name for the iRule you are creating.
4. For **Partition**, type the name of the BIG-IP device partition on which you want to create the iRule.
5. For the **Body**, compose the script sequence that defines the iRule.
   For guidance on creating an iRule, consult the AskF5™ (`support.f5.com`) Knowledge Base. You can search the AskF5 website for iRules documentation that provides an overview of iRules, lists the basic elements that make up an iRule, and shows some examples of how to use iRules.
6. Click **Save & Close**.
   The system creates the new iRule with the settings you specified.

To deploy this iRule to a device, attach the iRule to a virtual server associated with the target device and then deploy that change.

Attach iRules to virtual servers

You can use the BIG-IQ® Local Traffic interface to attach iRules® to a set of virtual servers. Adding an iRule sequence to a group of servers at once can save time and help you cut down on errors that result from performing repetitious tasks.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Virtual Servers**.
   The screen displays the list of virtual servers defined on this device.
2. Select the check boxes associated with the virtual servers to which you want to attach iRules.
3. Click **Attach iRules**.
   The Bulk Attach iRules screen opens.
4. To specify which iRules to attach to the selected virtual servers, select them in the **Available iRules** list, and move them to the **iRules to be Attached** list.
5. Specify the order in which you want the iRules to attach using the up and down arrows.
6. For **Location**, specify the list position to attach these iRules.
   - To add the rules to the beginning of the existing list, click **Attach to top of each virtual server's iRules list**.
   - To add the rules to the end of the existing list, click **Attach to bottom of each virtual server's iRules list**.
7. Use the **Duplicate Policy** setting to specify whether to keep the iRule list order for iRules that are already attached to the virtual servers.
   - To keep the existing list order, click **Keep virtual servers' existing rules list order**.
   - To change the existing list order to what you specified previously, click **Reorder virtual servers' existing rules to preserve selected rules order**.
8. Click **Save & Close**.

Managing Pool & Pool Members

How do I change object settings on a managed device?

To change the object settings on a managed device, there are four tasks to perform.

This figure illustrates the workflow you perform to manage the objects on BIG-IP® devices. Changing the settings is the second step in this process.

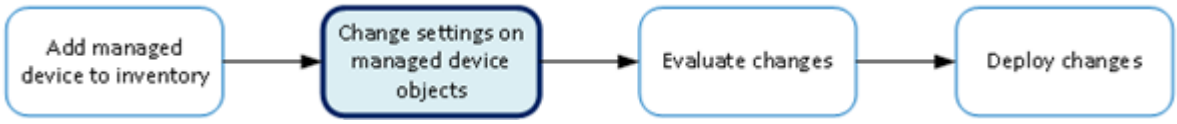

Figure 3: Change managed object workflow

What pool and pool member management tasks can I perform?

There are a number of ways you can use BIG-IQ® Centralized Management to manage the pools and pool members on your managed BIG-IP devices:

- Create a new pool or pool member.
- Modify an existing pool or pool member.
- View statistics for a pool.
- Deploy the pool and pool member immediately to your managed device; for pool members, you can enable, disable, or force offline immediately.

  Note: *You (or someone else) can also deploy your changes later. For more information about managing changes, look on* `support.F5.com` *in F5 BIG-IQ Centralized Management: Device for the topic: Deploying Changes.*

- Add or remove permissions for a pool or pool member and assign them to roles that have been defined on this BIG-IQ system. For more information about managing permissions, look on `support.F5.com` in *F5 BIG-IQ Centralized Management: Authentication, Roles, and User Management*.

Create a new pool

You can use the BIG-IQ® Local Traffic interface to add a pool to a managed device.

Important: *When revising configurations on devices that belong to a high availability cluster, it is important to let the changes synchronize to the cluster members instead of trying to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Pools**.
   The screen displays the list of pools defined on this device.
2. Click **Create**.
   The New Pool screen opens.

3. In the **Name** field, type in a name for the pool you are creating.
4. From the **Device** list, select the device on which to create the pool.
5. Specify the additional settings needed to suit the requirements for this pool.

   The remaining parameters on this screen are optional and perform the same function as they do when you configure a pool on a BIG-IP device.

   Note: *For details about the purpose or function of a particular setting, refer to the BIG-IP reference information on support.f5.com.*

6. To add a new pool member for this pool, click **New Member**.
   a) Specify the **Node Type**:
   b) If you want the new member to be an existing BIG-IP® node, select **Existing Node** and then select the **Node**.
   c) If you want the new member to be identified by an IP address, select **New Node** and then type the **Node Name** and **Node Address** for the node.
   d) For the **Port**, type the service port for the pool member.
   e) Specify the additional settings needed to suit the requirements for this pool member.

      The remaining parameters on this screen are optional and perform the same function as they do when you configure a pool member on a BIG-IP device.

      Note: *For details about the purpose or function of a particular setting, refer to the BIG-IP reference information on support.f5.com.*

   f) When you finish specifying the settings for this pool member, click **Save & Close**.

   The new pool member is added to the specifications for the pool you are creating.

   Note: *When you create a new pool member while creating a new pool, the new pool member is not actually created until you save the new pool. When you create a new pool member for an existing pool member, the new member is ready to use as soon as you save it.*

7. When you finish specifying the settings for this pool, click **Save & Close**.
   The system creates the new pool with the settings you specified.

Create a new pool member

You can use the BIG-IQ® Local Traffic interface to add a pool member to a pool.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Pool Members**.
   The screen displays the list of pool members defined on this device.
2. Click the name of the pool to which you are going to add a new member.
   The properties screen for that pool opens.
3. Near the bottom of the screen, click the **New Member** button.
   The New Pool screen opens.
4. Specify the **Node Type**:
   - If you want the new member to be an existing BIG-IP® node, select **Existing Node** and then select the **Node**.
   - If you want the new member to be identified by an IP address, select **New Node** and then type the **Node Name** and **Node Address** for the node.
5. For the **Port**, type the service port for the pool member.
6. Specify the additional settings needed to suit the requirements for this pool member.

The remaining parameters on this screen are optional and perform the same function as they do when you configure a pool member on a BIG-IP device.

Note: *For details about the purpose or function of a particular setting, refer to the BIG-IP reference information on support.f5.com.*

7. When you finish specifying the settings for this pool member, click **Save & Close**.
8. Click **Save & Close**.
   The system creates the new pool member with the settings you specified.

How do I delegate pool member management tasks?

BIG-IQ® Centralized Management makes it straightforward for you to delegate users permissions (enable, disable, or force offline) that allow them to manage pool members only for the specific pools you assign to them.

To provide enable, disable, and force offline permissions for a specific set of pool members, you need to perform three tasks. For example, consider a scenario in which you have 10 pools that service your Alaska clients and you want to delegate management authority for the pool members in those pools. Here are the tasks you would perform:

1. **Add a custom resource group and assign pools to it** - in this task, you specify the pools that you want your delegate to manage and name the resource group (for example, `Alaska Services Pools`).
2. **Add a custom role** - when you create a role you specify a role type and associate it with a resource group. The role type defines the permissions, and the resource group defines the objects to which those permissions apply.
   - You name the new role something intuitive (for example: `Alaska Services Pool Manager`).
   - You assign the built in role type named **Pool Member Operator**. This role has all the permissions (enable , disable, and force offline) needed, so you do not need a custom role.
   - Assign the role to the **Alaska Services Pools** resource group you just created.
3. **Add a custom user** - Finally, you create a user and assign them the **Alaska Services Pool Manager** role. Users who log in with this user name will have the permissions (defined by the role type) and access scope (defined by the resource group) to manage the pool members that belong to the 10 pools in the **Alaska Services Pools** resource group.

For step by step guidance on each of these tasks, refer to *How do I give users customized permissions to specific BIG-IP resources based on their job responsibilities?* on `support.f5.com`

Create a new node

You can use the BIG-IQ® Local Traffic interface to add a node to a managed device.

Nodes are the basis for creating a load balancing pool. For any server that you want to be part of a load balancing pool, you must first create a node, that is, designate that server as a node. After designating the server as node, you can add the node to a pool as a pool member. You can also associate a health monitor with the node, to report the status of that server.

Important: *When revising configurations on devices that belong to a high availability cluster, it is important to let the changes synchronize to the cluster members instead of trying to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Nodes**.
   The screen displays the list of nodes defined on this device.
2. Click **Create**.
   The New Node screen opens.
3. In the **Name** field, type a name for the node you are creating.
4. From the **Device** list, select the device on which to create the node.
5. For the **Address** field, type the IP address that identifies the new node.
6. Specify the additional settings needed to suit the requirements for this node.

   The remaining parameters on this screen are optional and perform the same function as they do when you configure a node on a BIG-IP device.

   Note: *For details about the purpose or function of a particular setting, refer to the BIG-IP reference information on support.f5.com.*
7. Click **Save & Close**.
   The system creates the new node with the settings you specified.

Change settings for a pool

Using the BIG-IQ® user interface to make revisions to your pool configurations simplifies managing your devices.

Important: *If you revise configurations on devices that belong to a high availability cluster, the system synchronizes BIG-IQ cluster members automatically when you deploy the change. Do not try to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Pools**.
   The screen displays the list of pools defined on this device.
2. Click the name of the pool that you want to change.

   If you select the check box for the pool instead of the name, you can either delete or deploy the pool, or you can view statistics for the pool.

   The Properties screen for the pool opens.
3. Make changes to the pool properties you want to modify.

   Note: *For detailed information on the impact of using a particular pool parameter value, refer to the BIG-IP Local Traffic Manager: Implementations on* `support.f5.com`*. For the most comprehensive detail, use the work flow that best matches the purpose of the pool you are configuring.*
4. You can expand the Advanced Properties area and make additional pool parameter changes.

   Note: *For detailed information on the impact of using a particular pool parameter value, refer to the BIG-IP Local Traffic Manager: Implementations on* `support.f5.com`*. For the most comprehensive detail, use the work flow that best matches the purpose of the pool you are configuring.*
5. To make revisions to the permissions associated with this pool, on the left, click **Permissions**.

   Note: *For detailed information about managing permissions, refer to How do I limit privileges for users based on their specific role in the company? or How do I give users customized permissions to*

specific BIG-IP resources based on their job responsibilities? in F5 BIG-IQ Centralized Management: Authentication, Roles, and User Management on `support.f5.com`.

6. When you are satisfied with the changes you have made to the pool, click **Save & Close**.
   The revisions you saved are made, and the Properties or Permissions screen for the pool closes.

Changes that you make to pools or pool members are made only to the pending version. The *pending version* serves as a repository for changes you stage before deploying them to the managed device. Object settings for the pending version are not the same as the object settings on the actual BIG-IP® device until they are deployed or discarded.

To apply the working configuration settings to the BIG-IP device, you now need to deploy the revisions.

Change settings for a pool member

Modifying your pool member configurations using the BIG-IQ® user interface, simplifies the device management process.

Important: *If you revise configurations on devices that belong to a high availability cluster, the system synchronizes BIG-IQ cluster members automatically when you deploy the change. Do not try to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Pool Members**.
   The screen displays the list of pool members defined on this device.
2. Click the name of the pool member that you want to change.

   If you select the check box for the pool member instead of the name, you can either enable, disable or force the pool member offline.

   The Properties screen for the pool member opens.
3. Make changes to the pool member properties you want to modify.

   Note: *For detailed information about managing permissions for this pool member, refer to How do I limit privileges for users based on their specific role in the company? or How do I give users customized permissions to specific BIG-IP resources based on their job responsibilities? in F5 BIG-IQ Centralized Management: Authentication, Roles, and User Management on* `support.f5.com`.
4. When you are satisfied with the changes you have made to the pool member, click **Save & Close**.
   The revisions you saved are made, and the Properties or Permissions screen for the pool member closes.

Changes that you make to pool members are made only to the pending version. The *pending version* serves as a repository for changes you stage before deploying them to the managed device. Object settings for the pending version are not the same as the object settings on the actual BIG-IP® device until they are deployed or discarded.

To apply the working configuration settings to the BIG-IP device, you need to deploy the revisions.

Make bulk changes to a set of pool members

Your must have been granted read/write access to the pool this set of pool members belongs to before you can make changes to those pool members.

Using the BIG-IQ® user interface to enable, disable, or force offline a group of pool members simplifies managing your devices.

Important: *If you revise configurations on devices that belong to a high availability cluster, the system synchronizes BIG-IQ cluster members automatically when you deploy the change. Do not try to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Pool Members**.
   The screen displays the list of pool members defined on this device.
2. Select the checkbox for the pool members that you want to change.
3. Click the button for the bulk action you want to take (**Enable**, **Disable**, or **Force Offline**).
4. When you change the state for a pool member, a prompt displays. You have three response options to this prompt..
   - If you want the change to occur immediately, click **Change Now**.
   - If you want the change to occur later, click **Change Later**. You can then evaluate and deploy the state change at a more convenient time.
   - If you decide not to make the change at all, click **Cancel**.

- When you click **Change Now**, it triggers an immediate deployment to the devices that house the impacted pool members.
- When you click **Change Later**, changes that you make to pool members are made only to the pending version. The *pending version* serves as a repository for changes you stage before deploying them to the managed device. Object settings for the pending version are not the same as the object settings on the actual BIG-IP® device until they are deployed or discarded.

Create a new SNAT pool

You can use the BIG-IQ® Local Traffic interface to add a SNAT pool to a managed device.

Important: *When revising configurations on devices that belong to a high availability cluster, it is important to let the changes synchronize to the cluster members instead of trying to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **SNAT Pools**.
   The SNAT Pools screen displays a list of SNAT translation members defined on this device.
2. Click **Create**.
   The New SNAT Pool screen opens.
3. In the **Name** field, type a name for the SNAT pool you are creating.
4. From the **Device** list, select the device on which to create the SNAT pool.
5. In the **Member List**, type the IP address of the first SNAT translation member you want to include in the SNAT pool.

   Use the + button to add more members, or you can use the **x** button to delete a member.
6. In the **Partition** field, type the name of the partition in which you want to create this SNAT pool.

   An *administrative partition* is a logical container that you create that contains a defined set of BIG-IP® system objects. If you enter a partition name that does not exist, you get an error when you try to deploy this SNAT pool.
7. Click **Save & Close**.
   The system creates the new SNAT pool with the settings you specified.

Managing Local Traffic Monitors

How do I change object settings on a managed device?

To change the object settings on a managed device, there are four tasks to perform.

This figure illustrates the workflow you perform to manage the objects on BIG-IP® devices. Changing the settings is the second step in this process.

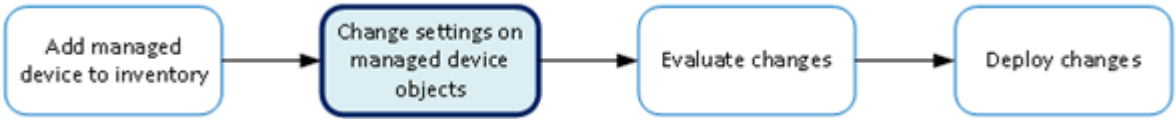

Figure 4: Change managed object workflow

What LTM monitor management tasks can I perform?

With HTTP and HTTPS monitors you can track the availability of these services on the nodes, pools, or pool members to which you attach them. To add or edit monitors, you need to log in as an Administrator or ADC Editor.

Note: *You can not make revisions to the root (or parent) monitors that ship with the product; you can only revise the child monitors that you (or another user) have created.*

Create an LTM monitor

You add a new HTTP or HTTPS LTM® monitor so that you can track the availability of these services on the nodes, pools, or pool members to which you attach that monitor.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Monitors**.
   The screen displays the list of monitors defined on this device.
2. Click **Create**.
   The New Monitor screen opens.
3. In the **Name** field, type in a name for the monitor you are creating.
4. For **Partition**, type the name of the BIG-IP® device partition on which you want to create the monitor.
5. In the **Description** field, type in a brief description for the monitor you are creating.
6. For **Type**, select the type of monitor you want to create.
   The **Monitor Template** setting displays.
7. From **Monitor Template**, select the parent monitor from which you want your monitor to inherit settings.
   A number of additional fields display. The fields that display depend on which monitor template you choose, **HTTP** or **HTTPS**.
8. For **Interval**, either use the default, or specify, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown.

9. From **Up Interval**, specify which interval the system uses to perform the health check when a resource is up.

Option	Description
Disabled	Specifies that the system uses the interval specified in **Interval** to check the health of the resource.
Enabled	Enables specification of a different interval to use when checking the health of a resource that is up.

10. For **Time Until Up**, specify the number of seconds to wait after a resource first responds correctly to the monitor before setting the resource to `up`.

    During the interval, all responses from the resource must be correct. When the interval expires, the resource is marked `up`. The default is 0, meaning that the resource is marked `up` immediately when the first correct response is received.

11. For **Timeout**, specify the number of seconds the target has in which to respond to the monitor request.

    The default is 16 seconds. If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Note that **Timeout** and **Time Until Up** combine to control when a resource is set to `up`.

12. For **Manual Resume**, specify whether the system automatically changes the status of a resource to `Enabled` at the next successful monitor check.

    If you set this option to **Yes**, you must manually re-enable the resource before the system can use it for load balancing connections. The default is **No**.

13. For **Send String**, specify the text string that the monitor sends to the target object.

    You must include `\r\n` at the end of a non-empty **Send String**. The default setting is `GET /\r\n`, which retrieves a default HTML file for a web site. To retrieve a specific page from a web site, specify a fully-qualified path name, for example:

```
GET /www/siterequest/index.html\r\n
```

14. For **Receive String**, specify a regular expression to represent the text string that the monitor looks for in the returned resource.

    The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names.

    Note: *If you do not specify both a **Send String** and a **Receive String**, the monitor performs a simple service check and connect only.*

    ---

15. For **Receive Disable String**, specify a regular expression to represent the text string that the monitor looks for in the returned resource.

    This setting works like **Receive String**, except that the system marks the node or pool member disabled when its response matches **Receive Disable String**.

    Note: *To use this setting, you must specify both **Receive String** and **Receive Disable String**.*

    ---

16. If you selected **HTTPS**, for **Cipher List**, specify the list of ciphers for this monitor.

    The default list is `DEFAULT:+SHA:+3DES:+kEDH`.

17. If the monitored target requires authentication, for the **User Name**, specify the user name.

18. If the monitored target requires authentication, for the **Password**, specify the password.

19. If you selected **HTTPS**, for **Compatibility**, specify the SSL option setting.

    If you select **Enabled**, the SSL option (in OpenSSL) is set to **ALL**.

20. If you selected **HTTPS**, for **Client Certificate**, select the client certificate that the monitor sends to the target SSL server.

    The default is **None**.

21. If you selected **HTTPS**, for **Client Key**, select the key for the client certificate that the monitor sends to the target SSL server.

    The default is **None**.

22. For **Reverse**, specify whether the system marks the target resource down when the test is successful.

    This setting is useful, for example, if the content on your web site home page is dynamic and changes frequently. You might want to set up a reverse ECV service check that looks for the string Error. A match for this string means that the web server was down. To use this option, you must specify values for **Send String** and `Receive String`.

23. For **Transparent**, specify whether the system operates in transparent mode.

    A monitor in transparent mode directs traffic through the associated pool members or nodes (usually a router or firewall) to the aliased destination (that is, it probes the Alias Address-Alias Service Port combination specified in the monitor). If the monitor cannot successfully reach the aliased destination, the pool member or node through which the monitor traffic was sent is marked `down`.

24. For **Alias Address**, specify an alias IP address for the monitor to check, on behalf of the pools or pool members with which the monitor is associated.

    The default setting is ***All Addresses**. If the health check for the alias address is successful, the system marks all associated objects up. If the health check for the alias address is not successful, then the system marks all associated objects down.

25. For **Alias Service Port**, specify an alias port or service for the monitor to check, on behalf of the pools or pool members with which the monitor is associated.

    The default setting is ***All Ports**. If the health check for the alias port or service is successful, the system marks all associated objects up. If the health check for the alias port or service is not successful, then the system marks all associated objects down.

26. For **IP DSCP**, specify the differentiated services code point (DSCP).

    DSCP is a 6-bit value in the Differentiated Services (DS) field of the IP header. It can be used to specify the quality of service wanted for the packet. The valid range for this value is 0 to 63 (hex 0x0 to 0x3f). The default is 0 (zero).

27. For **Adaptive**, specify whether adaptive response time monitoring is enabled for this monitor.

Option	Description
Enabled	The monitor determines the state of a service based on how divergent from the mean latency a monitor probe for that service is allowed to be. When enabled, you can set values for the **Allowed Divergence**, **Adaptive Limit**, and **Sampling Timespan** monitor settings.
Disabled	The monitor determines the state of a service based on the **Interval**, **Up Interval**, **Time Until Up**, and **Timeout** monitor settings.

    If you select **Enabled** for this control, three additional controls are displayed.

28. If you enabled **Adaptive**, for **Allowed Divergence**, specify the type of divergence used for adaptive response time monitoring.

Option	Description
Absolute	The number of milliseconds the latency of a monitor probe can exceed the mean latency of a monitor probe for the service being probed. Tip: In typical cases, if the monitor detects three probes in a row that miss the latency value you set, the pool member or node is marked `down`.
Relative	The percentage of deviation the latency of a monitor probe can exceed the mean latency of a monitor probe for the service being probed.

29. If you enabled **Adaptive**, for **Allowed Divergence**, specify the absolute number of milliseconds that may not be exceeded by a monitor probe, regardless of **Allowed Divergence** for a probe to be considered successful.

This value applies regardless of the value of the **Allowed Divergence** setting.

30. If you enabled **Adaptive**, for **Sampling Timespan**, specify the length, in seconds, of the probe history window that the system uses to calculate the mean latency and standard deviation of a monitor probe.

Edit an LTM monitor

You revise HTTP or HTTPS LTM® monitors when you want to change the details of how the monitor determines when a service is operational.

Note: *You cannot edit monitors root monitors.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Monitors**.
   The screen displays the list of monitors defined on this device.
2. Select the monitor you want to edit.
   The Monitors Properties screen opens to display the current settings for the selected monitor.
3. In the **Description** field, if this is not an imported profile you can add or revise a brief description for the monitor you are editing.
4. From **Interval**, specify, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown.

   The default is 5 seconds.
5. For **Up Interval**, specify which interval the system uses to perform the health check when a resource is up.

Option	Description
Disabled	Specifies that the system uses the interval specified in **Interval** to check the health of the resource.
Enabled	Enables specification of a different interval to use when checking the health of a resource that is up.

6. For **Time Until Up**, specify the number of seconds to wait after a resource first responds correctly to the monitor before setting the resource to up.

   During the interval, all responses from the resource must be correct. When the interval expires, the resource is marked up. The default setting is 0, meaning that the resource is marked up immediately when the first correct response is received.
7. From **Timeout**, specify the number of seconds the target has in which to respond to the monitor request.

   The default is 16 seconds. If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Note that **Timeout** and **Time Until Up** combine to control when a resource is set to up.
8. For **Manual Resume**, specify whether the system automatically changes the status of a resource to `Enabled` at the next successful monitor check.

   If you set this option to **Yes**, you must manually re-enable the resource before the system can use it for load balancing connections. The default setting is **No**.
9. For **Send String**, specify the text string that the monitor sends to the target object.

   You must include `\r\n` at the end of a non-empty **Send String**. The default setting is `GET /\r\n`, which retrieves a default HTML file for a web site. To retrieve a specific page from a web site, specify a fully qualified path name, for example:

```
GET /www/siterequest/index.html\r\n
```

10. For **Receive String**, specify a regular expression to represent the text string that the monitor looks for in the returned resource.

    The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names.

    Note: *If you do not specify both a* ***Send String*** *and a* ***Receive String****, the monitor performs a simple service check and connect only.*

11. For **Receive Disable String**, specify a regular expression to represent the text string that the monitor looks for in the returned resource.

    This setting works like **Receive String**, except that the system marks the node or pool member disabled when its response matches **Receive Disable String**.

    Note: *To use this setting, you must specify both* ***Receive String*** *and* ***Receive Disable String****.*

12. If you selected **HTTPS**, for **Cipher List**, specify the list of ciphers for this monitor.

    The default list is `DEFAULT:+SHA:+3DES:+kEDH`.

13. If the monitored target requires authentication, for the **User Name**, specify the user name.
14. If the monitored target requires authentication, for the **Password**, specify the password.

    Important: *For imported monitors that use passwords:*

    - If the monitor was imported from a version 12.0.0 or later device, you do not need to re-enter the password.
    - If the monitor was imported from a device earlier than version 12.0.0 and you plan to make changes to the monitor (or if you associate the monitor with an LTM object or child monitor), then you must supply the password for the imported monitor.
    - If you do not change any of the parameters for the monitor or associate the monitor with an LTM object or child monitor, then you do not need to re-enter the password.

15. If you selected **HTTPS**, for **Compatibility** specify the SSL option setting.

    If you select **Enabled**, the SSL option (in OpenSSL) is set to **ALL**.

16. If you selected **HTTPS**, for **Client Certificate**, select the client certificate that the monitor sends to the target SSL server.

    The default setting is **None**.

17. If you selected **HTTPS**, for **Client Key**, select the key for the client certificate that the monitor sends to the target SSL server.

    The default setting is **None**.

18. For **Reverse**, specify whether the system marks the target resource down when the test is successful.

    This setting is useful, for example, if the content on your web site home page is dynamic and changes frequently. You might want to set up a reverse ECV service check that looks for the string Error. A match for this string means that the web server was down. To use this option, you must specify values for **Send String** and **Receive String**.

19. For **Transparent**, specify whether the system operates in transparent mode.

    A monitor in transparent mode directs traffic through the associated pool members or nodes (usually a router or firewall) to the aliased destination (that is, it probes the Alias Address-Alias Service Port combination specified in the monitor). If the monitor cannot successfully reach the aliased destination, the pool member or node through which the monitor traffic was sent is marked down.

20. For **Alias Address**, specify an alias IP address for the monitor to check, on behalf of the pools or pool members with which the monitor is associated.

The default setting is ***All Addresses**. If the health check for the alias address is successful, the system marks all associated objects up. If the health check for the alias address is not successful, then the system marks all associated objects down.

21. For **Alias Service Port**, specify an alias port or service for the monitor to check, on behalf of the pools or pool members with which the monitor is associated.

    The default setting is ***All Ports**. If the health check for the alias port or service is successful, the system marks all associated objects up. If the health check for the alias port or service is not successful, then the system marks all associated objects down.

22. For **IP DSCP**, specify the differentiated services code point (DSCP).

    DSCP is a 6-bit value in the Differentiated Services (DS) field of the IP header. It can be used to specify the quality of service desired for the packet. The valid range for this value is 0 to 63 (hex 0x0 to 0x3f). The default is 0 (zero).

23. For **Adaptive**, specify whether adaptive response time monitoring is enabled for this monitor.

Option	Description
Enabled	The monitor determines the state of a service based on how divergent from the mean latency a monitor probe for that service is allowed to be. When enabled, you can set values for the **Allowed Divergence**, **Adaptive Limit**, and **Sampling Timespan** monitor settings.
Disabled	The monitor determines the state of a service based on the **Interval**, **Up Interval**, **Time Until Up**, and **Timeout** monitor settings.

    If you select **Enabled** for this control, three additional controls are displayed.

24. If you enabled **Adaptive**, for **Allowed Divergence**, specify the type of divergence used for adaptive response time monitoring.

Option	Description
Absolute	The number of milliseconds the latency of a monitor probe can exceed the mean latency of a monitor probe for the service being probed. Tip: In typical cases, if the monitor detects three probes in a row that miss the latency value you set, the pool member or node is marked down.
Relative	The percentage of deviation the latency of a monitor probe can exceed the mean latency of a monitor probe for the service being probed.

25. If you enabled **Adaptive**, for **Allowed Divergence**, specify the absolute number of milliseconds that may not be exceeded by a monitor probe, regardless of **Allowed Divergence**.

    For a probe to be considered successful, this value applies regardless of the value of the **Allowed Divergence** setting.

26. If you enabled **Adaptive**, for **Sampling Timespan**, length, in seconds, of the probe history window that the system uses to calculate the mean latency and standard deviation of a monitor probe.

27. Click **Save & Close**.

Copy an LTM monitor from one device to existing objects on another

To copy a monitor from one device to another there must be objects on the target device that use the monitor. If these objects do not exist on the target device you can create them as part of the workflow. Refer to *Copy an LTM monitor from one device to new objects on another* on `support.f5.com` for that workflow.

To copy a monitor from one device to another, you import the monitor from the source device, associate the monitor to selected objects on the target device, and then deploy your changes to the target device.

1. Identify your source and target BIG-IP devices as well as the name of the monitor you want to copy and the objects that you want to attach the monitor to.
   a) Identify the source BIG-IP device (the device that has the monitor you want to copy).
   b) Identify the name of the monitor that you want to copy.
   c) Identify the target BIG-IP device (the device to which you want to copy the monitor).
   d) Identify the objects on the target device that you want to attach the monitor to.
2. If you have not already discovered and imported services for both the source and target device, do that now.

   For details on how to discover a device and import services, refer to *Device Discovery and Basic Device Management* on `support.f5.com`.

   When discovery and import is complete, both devices will be under management, the BIG-IQ will have all of the monitors from the source device, and the BIG-IQ will have all of the objects from the target device that you want to use the monitor with.
3. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC**.
4. Click the name of a local traffic object that you want to associate the monitor with when you copy it to the target BIG-IP device.
   For example, if you plan to associate the monitor with a pool, click **Pools**.
   The list of objects of the type you selected (pools in this case) that reside on the devices managed by this BIG-IQ displays is displayed.
5. Click the name of the object that you want to associate with the copied monitor.
   The properties screen for the selected object opens.
6. The steps for identifying which monitor you want to copy depends on the type of object you are going to associate it with.

Option	Description
To copy a monitor to a pool	• For Health Monitors, select the specific monitor you want to copy to the selected device. • To specify an additional monitor to copy to this device, click + (+) and then repeat the previous step. • To remove a monitor you have specified to copy to this device, click × (X).
To copy a monitor to a pool member	• For Health Monitors, select **Member Specific**. • From Select Monitors, select the specific monitors you want to copy to the selected device. • To specify an additional monitor to copy to this device, click + (+) and then repeat the previous step. • To remove a monitor you have specified to copy to this device, click × (X).
To copy a monitor to a node	• For Health Monitors, select **Node Specific**. • From Select Monitors, select the specific monitors you want to copy to the selected device. • To specify an additional monitor to copy to this device, click + (+) and then repeat the previous step. • To remove a monitor you have specified to copy to this device, click × (X).

7. When you are finished assigning monitors to this object, click **Save & Close**.
   The system saves the monitor associations for the object you selected.
8. Repeat the previous three steps for the other object types that you want to use to copy monitors to the target device.
   For example, you might specify pools first and then define monitors for pool members and nodes.

9. When you have specified all of the objects and monitors you want to copy, deploy these changes to the target device.

   For details on deploying changes to a managed device, refer to *Deploying Changes* on `support.f5.com`.

You must deploy your changes to the target BIG-IP® device before the monitors are copied.

Copy an LTM monitor from one device to new objects on another

To copy a monitor from one device to another, you import the monitor from the source device, associate the monitor to selected objects on the target device, and then deploy your changes to the target device.

1. Identify your source and target BIG-IP devices as well as the name of the monitor you want to copy and the objects that you want to attach the monitor to.
   a) Identify the source BIG-IP device (the device that has the monitor you want to copy).
   b) Identify the name of the monitor that you want to copy.
   c) Identify the target BIG-IP device (the device to which you want to copy the monitor).
   d) Identify the objects on the target device that you want to attach the monitor to.
2. If you have not already discovered and imported services for both the source and target device, do that now.

   For details on how to discover a device and import services, refer to *Device Discovery and Basic Device Management* on `support.f5.com`.

   When discovery and import is complete, both devices will be under management, and the BIG-IQ will have all of the monitors from the source device.
3. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC**.
4. Click the name of a local traffic object type that you want to associate the monitor with when you copy it to the target BIG-IP device.

   Note: *To add a monitor to a new pool member, these two steps are a little different. You don't add a new pool member from the Pool Members screen; instead, you add new pool members by editing an existing pool or adding a new pool and then creating a new member from the pools screen.*

   For example, if you plan to associate the monitor with a pool, click **Pools**.
   The list of objects of the type you selected (pools in this case) that reside on the devices managed by this BIG-IQ displays is displayed.
5. Click **Create**.
   The create new object screen for the selected object opens.
6. In the **Name** field, type in a name for the object you are creating.
7. From the **Device** list, select the device on which to create the new object.
8. If you are adding a new node, type the IP address for the node in the **Address** field.
9. The steps for identifying which monitor you want to copy depends on the type of object you are going to associate it with.

Option	Description
To copy a monitor to a pool	• For Health Monitors, select the specific monitor you want to copy to the selected device. • To specify an additional monitor to copy to this device, click + (+) and then repeat the previous step. • To remove a monitor you have specified to copy to this device, click × (X).

Option	Description
To copy a monitor to a pool member	• *__Note:__ Remember, to access the New Pool Member properties screen, you need to add a new member by either editing an existing pool or creating a new pool and then click __New Member__.* • For Health Monitors, select **Member Specific**. • From Select Monitors, select the specific monitors you want to copy to the selected device. • To specify an additional monitor to copy to this device, click (+) and then repeat the previous step. • To remove a monitor you have specified to copy to this device, click (X).
To copy a monitor to a node	• For Health Monitors, select **Node Specific**. • From Select Monitors, select the specific monitors you want to copy to the selected device. • To specify an additional monitor to copy to this device, click (+) and then repeat the previous step. • To remove a monitor you have specified to copy to this device, click (X).

10. Specify any additional settings needed to suit the requirements for this object.

    Note: *For details about the purpose or function of a particular setting, refer to the BIG-IP reference information on support.f5.com.*

11. When you are finished assigning monitors to this object, click **Save & Close**.
    The system saves the monitor associations for the object you selected.
12. Repeat the previous six steps for the other object types that you want to use to copy monitors to the target device.
    For example, you might specify pools first and then define monitors for pool members and nodes.
13. When you have specified all of the objects and monitors you want to copy, deploy these changes to the target device.

    For details on deploying changes to a managed device, refer to *Deploying Changes* on `support.f5.com`.

You must deploy your changes to the target BIG-IP device before the monitors are copied.

Managing Network Objects

How do I change object settings on a managed device?

To change the object settings on a managed device, there are four tasks to perform.

This figure illustrates the workflow you perform to manage the objects on BIG-IP® devices. Changing the settings is the second step in this process.

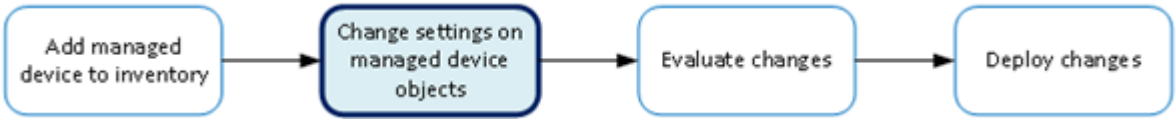

Figure 5: Change managed object workflow

Change a network object

You can make revisions to the configuration of Local Traffic objects to simplify managing your devices.

1. At the top of the screen, click **Configuration**, and then, on the left, click **NETWORK**.
2. Under **NETWORK**, click the object type that you want to modify, such as **Interfaces** or **VLANs**.
   The screen displays a list of objects of that type that are defined on this BIG-IQ®.
3. Click the name of the object you want to change.
   The Properties screen for the selected object opens.
4. Make changes to the properties that you want to modify.
5. When you are satisfied with the changes you have made, click **Save & Close**.
   The revisions you saved are made, and the Properties screen for the selected object closes.

Changes are made only to the pending version. The *pending version* serves as a repository for changes you stage before deploying them to the managed device. Object settings for the pending version are not the same as the object settings on the actual BIG-IP® device until they are deployed or discarded.

To apply the pending version settings to the BIG-IP device, you next need to deploy the revisions.

Manage a network interface

You can use the BIG-IQ® Local Traffic component to enable or disable network interfaces on a managed device.

Important: *When you revise configurations on devices that belong to a high availability cluster, it is important to let the changes synchronize to the cluster members instead of trying to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

---

1. At the top of the screen, click **Configuration**, and then, on the left, click **NETWORK** > **Interfaces**.
   The screen displays the list of interfaces defined on this device.
2. Select the check box for the interface you want to change, and then click **Enable** or **Disable**.

Create a new route

You can use the BIG-IQ® Local Traffic component to add a route to a managed device.

Important: *When revising configurations on devices that belong to a high availability cluster, it is important to let the changes synchronize to the cluster members instead of trying to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **NETWORK** > **Routes**.
   The screen displays the list of routes defined on this device.
2. Click **Create**.
   The New Route screen opens.
3. In the **Name** field, type in a name for the route you are creating.
4. In the **Description** field, type in a brief description for the route you are creating.
5. From the **Device** list, select the device on which to create the route.
6. For **Partition**, type the name of the BIG-IP device partition on which you want to create the route.
7. In the **Destination/Mask** field, type a self IP address and net mask for this route.

   These addresses display in the Destination and Netmask columns of the routing table.

   For example:

```
10.145.193.0/24
```

8. Specify the **Resource** setting.
   - To use a gateway, select **Use Gateway**, and then from **Gateway Address**, choose either **IP Address** or **IPv6 Link-Local Address**. This is the method through which you want the BIG-IQ system to forward packets to the route destination.
   - To use a pool, select **Use Pool**, and then select the pool through which you want the BIG-IQ system to forward packets to the route destination.
   - To use a VLAN or tunnel, select **Use VLAN/Tunnel**, and then select the VLAN or tunnel through which you want the BIG-IQ system to forward packets to the route destination.
   - To reject packets forwarded to the route destination, select **Reject**.
9. In the **MTU** field, type an optional frame size value for Path Maximum Transmission Unit (MTU). By default, BIG-IP® devices use the standard Ethernet frame size of 1518 bytes (1522 bytes if VLAN tagging is used) with the corresponding MTU of 1500 bytes. For BIG-IP devices that support Jumbo Frames, you can specify another MTU value.
10. Click **Save & Close**.
    The system creates the new route with the settings you specified.

Create a new route domain

You can use the BIG-IQ® Local Traffic component to add a route domain to a managed device. Using route domains, you can assign the same IP address to more than one device on a network, as long as each instance of the IP address resides in a separate route domain.

1. At the top of the screen, click **Configuration**, and then, on the left, click **NETWORK** > **Route Domains** .
   The screen displays the list of route domains defined on this device.
2. Click **Create**.

The New Route Domain screen opens.

3. In the **Name** field, type in a unique name for the route you are creating.
4. In the **ID** field, type an integer to represent the route domain.

   The integer must be unique on the BIG-IP® device and be between 1 and 65534. The default value (0) indicates that all VLANs on a system pertain to this route domain. When you create new route domains, you can assign VLANs to those route domains which moves the VLANs out of the default route domain.

   Important: *When you assign a VLAN to a route domain, keep in mind that any self IP addresses that use that VLAN must use the same route domain. For example, if self IP* `10.0.0.0%20` *(route domain with ID 20) is assigned to VLAN-1, you cannot assign VLAN-1 to any route domain except a route domain with ID 20.*
5. In the **Description** field, type in a brief description for the route domain you are creating.
6. From the **Device** list, select the device on which to create the route domain.
7. For **Partition**, type the name of the BIG-IP device partition on which you want to create the route domain.
8. Select **Strict Isolation** if you want to enforce cross-routing restrictions.

   When **Enabled** is selected, routes cannot cross route domain boundaries (so they are strictly isolated to the current route domain). The default is enabled. When this setting is disabled, routes can cross route domains. For example, you could add a route to the routing table with a `10.0.0.0%20` (route domain 20) destination and a gateway of `172.27.84.29%32` (route domain 32).
9. To specify a VLAN or tunnel for the BIG-IP device to use in the route domain, select it in the **Available** list, and use the arrow to add it to the **Selected** list.

   Note: *A VLAN and tunnel can only be referenced by one route domain at a time, so if the VLAN or tunnel you select is currently referenced by another route domain, it will be removed from that route domain when you attach it to this route domain.*

   Note: *Before removing a VLAN from a route domain, recall that every self IP address must use the same route domain as its VLAN, so make sure the VLAN is not already in use by a self IP address. For example, if a self IP address uses a VLAN named* `VLAN-2` *and also uses the default route domain 0, do not remove* `VLAN-2` *from route domain 0.*
10. Click **Save & Close**.
    The system creates the new route domain with the settings you specified.

Create a new VLAN

You can use the BIG-IQ® Local Traffic component to add a VLAN to a managed device. Using VLANs, you can assign the same IP address to more than one device on a network, as long as each instance of the IP address resides in a separate VLAN.

1. At the top of the screen, click **Configuration**, and then, on the left, click **NETWORK** > **VLANs** .
   The screen displays the list of VLANs defined on this device.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type a unique name for the VLAN you are creating.
4. In the **Description** field, type a brief description for the VLAN you are creating.
5. In the **Tag** field, type a tag number for the VLAN.

The tag number can be between 1 and 4094, but must be unique on the target device. If you do not specify a value, the system automatically assigns a tag number.

6. From the **Device** list, select the device on which to create the VLAN.
7. For **Partition**, type the name of the BIG-IP device partition on which you want to create the VLAN.
8. In the **MTU** field, specify the maximum transmission unit (MTU) for traffic on this VLAN.
   The default is 1500.
9. To specify which interfaces this VLAN uses for traffic management, select one from the **Interface** list, and then select the **Tagging** for it.
   You can add more than one interface by clicking the Add + button.
10. Click **Save & Close**.
    The system creates the new VLAN with the settings you specified.

Create a new self IP address

You can use the BIG-IQ® Local Traffic component to add a self IP address to a managed device.

Important: *When revising configurations on devices that belong to a high availability cluster, it is important to let the changes synchronize to the cluster members instead of trying to make the same changes to multiple devices. If you try to replicate changes you made on one device in the cluster, the next config sync attempt could fail.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **NETWORK** > **Self IPs** .
   The screen displays the list of self IP addresses defined on this device.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type in a name for the self IP address you are creating.
4. From the **Device** list, select the device on which to create the self IP address.
5. For **Partition**, type the name of the BIG-IP device partition on which you want to create the self IP.
6. In the **IP Address** field, type either an IPv4 or an IPv6 address. For an IPv4 address, you should specify a /32 IP address per RFC 3021.
7. In the **Netmask** field, type the netmask for this self IP address. You must type the full netmask.
   Specifying the prefix length in bits is not supported. For example, you could type `255.255.255.255` or `ffff:ffff:ffff:ffff:0000:0000:0000:0000 or ffff:ffff:ffff:ffff::` (with two colons at the end).
8. For **VLAN/Tunnel**, select the VLAN or tunnel to associate with this self IP address.

   Important: *When you assign a VLAN to this self IP address, keep in mind that the self IP address and VLAN must use the same route domain. For example, if you assign self IP `10.0.0.0%20` (route domain with ID 20) to VLAN-1, you will not be able to assign VLAN-1 to any route domain except a route domain with ID 20.*

9. Specify the **Port Lockdown**.
   - Select **Allow Default** to activate only the default protocols and services. You can determine the supported protocols and services by logging in to the target BIG-IP device and running `tmsh list net self-allow defaults` on the command line.
   - Select **Allow All** to activate all TCP and UDP services on this self IP address.
   - Select **Allow None** to specify that this self IP address accepts no traffic. If you are using this self IP address as the local endpoint for WAN optimization, select this option to avoid potential port conflicts.

- Select **Allow Custom** or **Allow Custom (Include Default)** to expand the **Custom List** setting, where you can specify the ports, protocols, and services to activate on this self IP address.

10. For the **Traffic Group**, select a specific traffic group for the self IP address.
11. Click **Save & Close**.
    The system creates the new self IP address with the settings you specified.

Create a new DNS resolver

You can use the BIG-IQ® Local Traffic component to add a DNS resolver to a managed device. Using DNS resolvers, you can assign the same IP address to more than one device on a network, as long as each instance of the IP address resides in a separate DNS resolver.

1. At the top of the screen, click **Configuration**, and then, on the left, click **NETWORK** > **DNS Resolvers** .
   The screen displays the list of DNS resolvers defined on this device.
2. Click **Create**.
   The New DNS Resolver screen opens.
3. In the **Name** field, type in a unique name for the DNS resolver you are creating.
4. For **Partition**, type the name of the BIG-IP device partition on which you want to create the DNS resolver.
5. Select the **Route Domain Name** that this resolver uses for outbound traffic.

   The default is the default route domain.
6. To specify the Resolver properties, expand the Resolver area.
7. For the **Cache Size**, type the size of the internal DNS resolver cache.

   The default is 5767168 bytes. After the cache reaches this size, when new or refreshed content arrives, the system removes expired and older content and caches the new or updated content.
8. Select **Answer Default Zones** if you want the system to answer DNS queries for the default zones `localhost`, `reverse`, `127.0.0.1`, `::1`, and `AS112`.

   The default is disabled, meaning that the system passes along the DNS queries for the default zones.
9. Select **Randomize Query Character Case** if you want the internal DNS resolver to randomize character case in domain name queries issued to the root DNS servers.

   The default is enabled.
10. To specify the Traffic properties, expand the area and select the format or formats for which you want the system to answer and issue queries.
11. To specify a forward zone used to resolve matching DNS queries, expand the Forward Zones area and click **Add**.

    A popup screen opens.
    a) In the **Name** field, type in a unique name for the forward zone you are creating.
    b) In the **Address** field, type in an IP address for the forward zone you are creating.
    c) In the **Service Port** field, type in the port number for the forward zone you are creating.
    d) Click the **Add** button next to the Service Port.
       The address and port combination is added to the **Nameservers** box.
    e) To add additional nameservers, repeat the last two sub-steps.
12. When you are satisfied with the new forward zone, click the **Add** button.
13. If you have specified forward zones, select the check boxes for the zones you want to use.
14. When you are satisfied with the new DNS resolver, click **Save & Close**.
    The system creates the new DNS resolver with the settings you specified.

When the BIG-IP® system receives a query that cannot be resolved from the cache, the system forwards the query to a nameserver associated with the matching forward zone. When the nameserver returns a

response, the BIG-IP system caches the response, and returns the response to the resolver making the query.

To pin this resolver to specific devices, click **Configuration** > **LOCAL TRAFFIC** > **Pinning Policies**.

Note: *For details about how pinning works, refer to Managing Object Pinning on* `support.f5.com`.

Managing FEC Tunnel Profiles

How do I manage FEC tunnel profiles in BIG-IQ?

You can create or modify custom FEC tunnel profiles in BIG-IQ® Centralized Management and then attach the resulting tunnel to a virtual server to deploy them to your managed devices.

When you create a profile, you specify a parent profile from which the custom profile inherits its properties. You then specify which of these properties you want to override. You can name any existing profile as a parent profile. When you modify a profile that has *child profiles* (that is, profiles that name your profile as a parent profile), all of the child profiles inherit any changes you made in the parent profile (except those you choose to override).

Create an FEC tunnel profile

You must discover a device and import that device's service configurations before you can add a profile to that device from BIG-IQ® Centralized Management.

Creating a new profile allows you to specify the parameters that define the characteristics you want your virtual servers to use. Each virtual server that references this profile uses the parameters you specify for this profile. Additionally, the parameters you define for this profile are given to the profiles that name this profile as their parent profile.

1. At the top of the screen, click **Configuration**, and then, on the left, click **NETWORK** > **Tunnel Profiles**.
   The screen displays the list of FEC tunnel profiles defined on this device.
2. Click **Create**.
   The New FEC tunnel profile screen opens.
3. In the **Name** field, type in a name for the FEC tunnel profile you are creating.
4. For **Partition**, type the name of the BIG-IP® device partition on which you want to create the profile.
5. From **Parent Profile**, select the parent profile from which you want your profile to inherit settings.

   Note: *The parent profile you select determines the value of the profile parameters for this profile. You can override these values, but if you do not, changes made to parameters in the parent profile propagate to all child profiles.*

   Values for the selected parent profile display. There are two controls for each field. The first one (a check box) controls whether you want to override the inherited value for that field. The second control (the type varies by field) sets the value you want for the parameter.
6. For any fields you want to override, select the **Override** check box and then specify the value you want for the fields you selected.

   Note: *You can select* ***Override All*** *if you want to override all of the parent profile parameter values.*

   Important: *If you override a parent profile parameter, regardless of whether or not you change the parameter's value, then future changes to the parent's parameter value will not be inherited by this profile.*

Note: *For detailed information about the impact of using a particular profile parameter value, refer to the BIG-IP Local Traffic Management: Profiles Reference on* `support.F5.com`.

7. Click **Save & Close**.
   The system creates the new profile you specified and adds it to the list of profiles.

You can now use the profile you created. You can select it when you configure a virtual server. You can also use it as a parent profile to base new BIG-IP FEC tunnel profiles on.

To pin this profile to specific devices, click **Configuration** > **LOCAL TRAFFIC** > **Pinning Policies**.

Note: *For detail about how pinning works, refer to Managing Object Pinning on* `support.f5.com`.

Edit an FEC tunnel profile

By editing a profile, you can revise the parameters that define the characteristics you want your virtual servers to use. Each virtual server that references this profile uses the parameters you specify for this profile. Additionally, the parameters you define for this profile are given to the profiles that name this profile as their parent profile.

1. At the top of the screen, click **Configuration**, and then, on the left, click **NETWORK** > **Tunnel Profiles**.
   The screen displays the list of FEC tunnel profiles defined on this device.
2. Click the name of the profile you want to edit.
   The screen displays the current settings for the selected profile.
3. Under Referenced by, note the virtual servers and profiles that refer to this profile.

   Changes you make to this profile affect all of the virtual servers listed here.

   Changes you make to this profile are also inherited by all profiles that name this profile as their parent profile.
4. Under the **Override All** check box, select the check box corresponding to any fields you want to override, and then specify the value you want for the fields you selected.

   Note: *You can select* ***Override All*** *if you want to override all of the parent profile parameter values.*

   Note: *If you are editing a root profile, the override check boxes are disabled. Because a root profile does not have a parent profile, it does not inherit any settings, so there are no values to override.*

   Note: *For detailed information about the impact of using a particular profile parameter value, refer to the BIG-IP Local Traffic Management: Profiles Reference on* `support.F5.com`.
5. When your edits are complete, click **Save & Close**.
   The system updates the profile with the settings you specified and adds it to the list of profiles.

To pin this profile to specific devices, click **Configuration** > **LOCAL TRAFFIC** > **Pinning Policies**.

Note: *For detail about how pinning works, refer to Managing Object Pinning on* `support.f5.com`.

Managing Application Templates

How do I manage application templates in BIG-IQ?

You can create an application template in BIG-IQ® Centralized Management and then use that template to deploy applications to your managed devices.

An application template is a collection of objects and default parameter settings that you define. After you define the objects and default values for an application template, you use that template to create an application. When you create the application you decide which objects to include and which settings to revise. Finally, you can deploy the collection of objects in that template to any devices you manage.

You can think of the objects in an application template as a baseline for creating a new application. For example, if you create a template with a virtual server, two pools, and 5 nodes, then when you create a new application using that template each of those objects (with the default values you specified in the template) are included. When you define the application, you can omit or include these objects. Parameters you define as not visible are included using the default values specified in the application template. This allows you to maintain a consistent environment. Parameters that you define as editable are visible and can be revised.

Consider the following example. You want to standardize your HTTPS application to use a virtual server, a client SSL profile, a pool and a node. There are default values that you always want to use for some of these objects and there are values that will change from one application to the next. You create an application template that includes each of these objects. You define the parameters that have fixed default values as not editable, and the parameters that can change for each application as editable. Then when someone uses your template to create an application, all they need to do is provide the editable values (virtual server address, number of nodes and their addresses, and so forth) and then deploy the application. When you deploy the application, it will create just the right objects and settings. The workflow is illustrated in the following diagram:

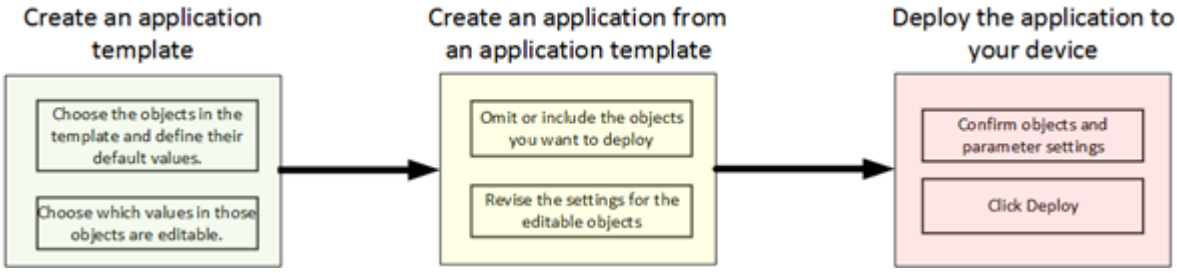

Figure 6: Application template workflow

Create an application template by manually specifying LTM objects

You can create an application template to specify a set of objects that define an application. That application can then be deployed to your BIG-IP devices.

1. At the top of the screen, click **Application** and then, on the left, click **Service Catalog**.
   The screen displays the list of service catalog templates defined on this device.
2. Click **Create**.
   The Create Template screen opens.
3. In the **Name** field, type a name for the application template you are creating.

4. In the **Description** field, type a brief description for the application template you are creating to help identify it when you want to use it later.

   After you define the name and (optional) description, you can define the default objects for this template immediately, or you can save the template and define the default objects later. In this workflow, we will continue on, defining the values now. You can either create these objects manually, or you can import objects that already exist on this BIG-IQ system.
5. On the left, under **Properties**, expand **Local Traffic** and then select the object type you want to define.
   For example, to add a default virtual server, you would expand **Local Traffic**, and then click **Virtual Servers**.
6. Click **Create**.
   The screen you use to define the selected object type (for example New Virtual Server) displays.
7. In the **Prompt** box, type the text string that you want to display for this object when someone uses this template to create a new application.
8. If you want applications created with this template to be able to include more than one copy of the object you adding, select **Enabled** for Allow Multiple Instances.
9. Specify all of the default parameters that you want to define for this object.

   Before you can add an object to the template, you must specify at least the required parameters for that object type. For example, to add a virtual server, you must provide a name, a destination address, and a service port; all other settings are optional.
10. For each parameter that you specify, determine whether you want the person who deploys an application using this template to be able to edit the default settings you are defining. For parameters that you want to allow to be changed, select **Editable**. Other parameters will be present (with the settings that you specify here), but they will not be visible in the user interface.
    Only the parameters you select will appear in the user interface when someone deploys an application using this template.
11. As you specify parameter values for this template object, you can click **Preview** in the upper right corner to see what the user interface will look like when someone uses this template to deploy an application.

    Note: *For detailed information on which parameter settings to specify for particular use cases, refer to the BIG-IP Local Traffic Manager: Implementations on* `support.F5.com`.

    ---
12. When you finish specifying parameters for this object, click **Save & Close**.
    BIG-IQ adds the object you defined to the list of objects in this template. When you finish adding an object to a template, you can use it to create an application.
13. If you want to add additional objects to this template, repeat the last eight steps for each of the objects that you want to add to this template.

    Once you specify the name and description BIG-IQ creates the template. So when you specify additional objects, you are actually editing the newly created template.

You can use the template to create a new application that deploys to your BIG-IP devices.

Create an application template by importing existing LTM objects

Before you can import objects to an application template, you must have either created or imported the LTM objects from one of your managed BIG-IP devices.

You can create an application template to specify a set of objects that define an application. That application can then be deployed to your BIG-IP devices.

Specifying the objects by importing existing objects saves time and insures that you get precisely the settings you are looking for.

1. At the top of the screen, click **Application** and then, on the left, click **Service Catalog**.
   The screen displays the list of service catalog templates defined on this device.
2. Click **Create**.
   The Create Template screen opens.
3. In the **Name** field, type a name for the application template you are creating.
4. In the **Description** field, type a brief description for the application template you are creating to help identify it when you want to use it later.

   After you define the name and (optional) description, you can define the default objects for this template immediately, or you can save the template and define the default objects later. In this workflow, we will continue on, defining the values now. You can either create these objects manually, or you can import objects that already exist on this BIG-IQ system.
5. On the left, under **Properties**, expand **Local Traffic** and then select the first object type you want to define.
   For example, to import a default virtual server, you would expand **Local Traffic**, and then click **Virtual Servers**.
6. Click **Import**.
   The Import Resources screen displays. The top half of the screen displays resources selected for import. The bottom half provides controls for selecting objects to import to this template.
7. From the Select Object Type box, select the type of object you want to import.
   Objects of the type you selected that are currently defined on this BIG-IQ display just below the select box.
8. Select the check box for each object that you want to import.
   The lower right part of the screen displays preview information for the selected object. If you select multiple objects, the most recently selected item is previewed.
9. When you have selected all of the objects that you want for a particular type, click **Add Selected**.
   The selected objects are added to the list of objects to be imported.
10. Repeat the last three steps for each of the default object types that you want to import to this template.
11. When you have assembled all of the objects you want to import to this template, click **Import**.

    Note: *When you import an object created outside of the service template user interface into a service template, only the object name is set to be editable (and visible when someone uses this template to create a new application). For example, if a virtual server named* `SeattleServer` *is created on one of the BIG-IP devices a BIG-IQ manages, that virtual server is imported to the BIG-IQ when you discover and import that device. You can then import* `SeattleServer` *into a service template, but only the name (*`SeattleServer`*) appears when that template is used to create an application. You can edit the visibility setting on the Edit Template screen for the imported object.*

    BIG-IQ adds the imported objects to the application template. Objects that are set to be editable will display when someone uses this template to create a new application.
12. If you want to edit any of the parameters for the objects you imported, click the name of the object to access the edit screen for that object.
    When you save the changes for an object, the revisions you made become part of the template and you can use it to create a new application that deploys to your BIG-IP devices.

Edit an application template

An application template specifies a set of objects and parameter settings that can be used to create an application that can be deployed to your BIG-IP devices. Editing an application template is similar to creating one; you can either add individual objects manually, or import them.

1. At the top of the screen, click **Application** and then, on the left, click **Service Catalog**.

The screen displays the list of service catalog templates defined on this device.

2. Click the name of the application template that you want to edit.
   The properties tab displays the name and description for the selected template.
3. On the left, under **Properties**, expand **Local Traffic** and then select the object type you want to edit. For example, to edit the list of virtual servers, you would expand **Local Traffic**, and then click **Virtual Servers**.
   The list of objects of the selected type defined for this application template displays. You can now either edit the settings for this template either manually or by importing existing objects.
4. Make the revisions you want to make for this template. You can edit the settings for this template either manually or by importing existing objects.
   - For details on making manual revisions, refer to *Create an application template by manually specifying LTM objects*
   - For details on importing template objects, refer to *Create an application template by importing existing LTM objects*
5. When your edits are complete, click **Save & Close**.
   The system updates the template with the settings you specified.

You must create an application with this template and deploy the application to the BIG-IP® device before the objects are created on the device.

Managing Applications

How do I manage applications in BIG-IQ?

You can create an application from an application template and then deploy that application to your managed devices.

An application template is a collection of objects that you define. When you create an application from the template, you can omit or include these objects. Parameters defined as not visible in the template are included using the default template values. Parameters defined as editable are visible and can be revised. Once you specify the objects and settings you need, you deploy the application to create those objects on devices you manage.

Create an application from a template

Before you can create an application from a template, you must have created a template.

Creating a new application from a template allows you to start from the set of objects defined in the template, modify or add objects, and then deploy the application to your BIG-IP devices. As you create the application, you define which of the template objects you want to include and revise the settings that need to be customized for each device.

1. At the top of the screen, click **Application** and then, on the left, click **Service Catalog**.
   The screen displays the list of service catalog templates defined on this device.
2. Select the template you want to use to create an application from, and then click **Create Application**.
   The Create Application screen opens.
3. In the **Name** field, type a name for the application you are creating.
4. In the **Prefix** box, type the prefix that you want the system to use to make certain that all of the objects created when you deploy an application are uniquely named. If you want to append this prefix to the names of the objects that this application creates, keep **Apply Prefix To Names** selected.

   Appending the prefix to the objects in this application makes these objects easier to find using search filters.

5. To help identify this application when you want to use it later, in the **Description** field, type a brief description for the application you are creating.
6. For Device, select the name of the device you want to deploy this application to.
7. Determine the objects that you want to deploy in this application.
   a) To omit any of the objects defined in this template, click the  (**X**) icon that corresponds to that object.
   b) To create additional copies of any of the objects defined in this template, click the  (+) icon that corresponds to that object.
   c) For each object you decide to include in the application, revise the settings that you need to change.

   Note: *When you specify values for fields that reference other configuration objects, you can select objects that already exist in BIG-IQ configuration. But you can also specify objects that are created when this application is deployed. These objects that don't yet exist in BIG-IQ configuration, but are created when this application is deployed are prefixed with a pound sign (#). For example a template could define a pool* ***MyPool1*** *and a node* ***45.54.45.54****. To specify the application-created object, you select the value prefixed with a pound sign (#) when you select the value for that node. (That option would appear as* ***#45.54.45.54*** *in the example cited here.*
8. When you have configured the objects that you want to include in this application, click **Create**.
   The application is created and is now ready to be deployed.

Edit and Review an application

Before you can review or revise an application, you must have created one.

An application specifies a set of objects that can be deployed to your BIG-IP devices. Reviewing and revising an application (either before or after you deploy it to your devices) allows you to make sure that the application has precisely the right objects and parameter settings.

1. At the top of the screen, click **Application** then, on the left, click **Applications**.
   The screen displays the list of applications defined on this device.
2. Click the name of the application that you want to edit.
   The Application Overview tab displays the name and description for the selected application.
3. On the left, select **Local Traffic**.
   The list of objects defined for this application displays. You can now review and revise the settings for each object.
4. Review and revise each object in the application until they are all correct.
5. When your edits are complete, click **Save & Close**.
   The system updates the application with the settings you specified.

You must deploy this application to the BIG-IP device before these objects and settings are created on the device.

Deploy an application

You deploy an application when you want to create a set of objects on a BIG-IP device.

1. At the top of the screen, click **Application** then, on the left, click **Applications**.
   The screen displays the list of applications defined on this device.
2. Click the name of the application that you want to deploy.
   The Application Overview tab displays the name and description for the selected application.
3. At the top of the screen, click **Deploy**.
   The objects defined in this application deploy to the BIG-IP device to which they are targeted.

Managing Logs

How do I manage my device logs on the BIG-IQ?

You can create, edit or delete log filters, log publishers, and log destinations for the logs produced on your managed BIG-IP devices. Just make whatever changes you want and then deploy them to the device.

What is a device-specific log destination type?

There are several log destination types you can create and manage with the BIG-IQ. Most log destination types are completely shared objects. That is they use one set of parameters regardless of which device they are deployed to. However, there are also 3 types of log destinations that can have device-specific settings. For these destination types, the configuration can be altered depending on which device the destination is deployed to. These device-specific log types are:

- IPFIX
- Remote High-Speed Log
- Management Port

IPFIX and Remote High-Speed Log destinations use pools that are per-device objects. As a result, they are always device-specific. Each BIG-IP that the destination is deployed to needs a log destination unique to that BIG-IP so that you can specify a pool on that BIG-IP the logs are forwarded to.

Management Port log destinations can either be completely shared objects or they can be device-specific. A shared log destination uses the same IP address and port for every BIG-IP device it is deployed to. A device-specific log destination uses a separate instance of the log destination (each with a unique IP address and port) for each BIG-IP it is deployed to.

Create a new log destination

Before you can create a new log destination, you must have configured a remote log server to send the logs to.

Use this screen to create a new log destination for a managed device.

Create a log destination to specify that log messages are sent to a remote log server.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Logs** > **Log Destinations**.
   The Log Destinations screen displays a list of the log destinations that are defined on this device.
2. To create a new log destination, click **Create**.
   The New Log destination screen opens so you can define the settings you want for this destination.
3. In the **Name** field, type in a name for the log destination you are creating.
4. For **Type**, select the kind of destination you are creating.
   Depending on the selection you make, additional controls are displayed.
5. Specify the additional settings needed to suit the requirements for this log destination. The fields required to create a new log destination depend on the type you choose. BIG-IQ denotes required fields using an amber box. You can also determine whether you have completed all of the required fields by noting whether the **Save & Close** button is enabled.

Note: *Except for the Devices and Device Specific settings, the parameters on this screen perform the same function as they do when you configure a log destination on a BIG-IP device. For details about the purpose or function of a particular setting, refer to the BIG-IP reference information on* `support.f5.com`*. From the BIG-IP Knowledge Center, select the BIG-IP LTM module and the software version you have installed; then select the appropriate guide. For example, information about the log destination parameters for BIG-IP version 13.0 is provided in the External Monitoring of BIG-IP Systems: Implementations, Version 13.0 guide.*

6. When you create a Log Destination and select a type of **IPFIX** or **Remote High-Speed Log**, you need to specify which devices to associate this destination with. When you create a Log Destination and select a type of **Management Port** you can specify device specific settings or, if no device specific settings are defined, the base configuration settings are used for any device associated with this log destination.

   Note: *For additional detail on device-specific log destination types, refer to What is a device specific log destination? in the F5 BIG-IQ Centralized Management: Local Traffic & Network Implementations guide on* `support.f5.com`*.*

   - If you have a lot of devices that you need to associate with this log destination and want to automate the process:
     1. Use the steps below to specify one device and then click **Save**.
     2. Associate this log destination with the log publishers that are pinned to your managed devices.
     3. Come back and edit this log destination. A **Find Relevant Devices** button displays. You can use this button to let BIG-IQ assemble a list of devices. BIG-IQ finds the BIG-IP devices that this destination can be deployed to. You can use the list to create a device-specific instance of this destination for each BIG-IP.
     4. Click **Save** to add the listed devices to the Device Specific list.
   - To specify the devices for this log destination manually:
     1. Select the device you want this destination to use
     2. If you are creating an **IPFIX** or **Remote High-Speed Log** destination log, select the pool that you want each device to use.
     3. Use the + button to add additional devices to the list.
     4. Use the × button to remove a device from the list.
     5. Click **Save** to add the listed devices to the Device Specific list.

   Devices you select for this log destination are added to the Device Specific list.

   Note: *Click on a device name in the Device Specific list to edit settings for that device. Bear in mind though that changes you make to one device do not change the settings for other devices, or for the base configuration for the log destination.*

7. Click **Save & Close**.
   The system creates the new log destination with the settings you specified.

Create a new log publisher

Before you can create a new log publisher, configure a log destination with a pool of remote log servers so you can assign it to your publisher as you create it.

Log publishers specify log destinations that BIG-IP devices can send their log messages to.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Logs** > **Log Publishers**.

The Log Publishers screen displays a list of the log publishers that are defined on this device.

2. To create a new log publisher, click **Create**.
   The New Log Publisher screen opens so you can define the settings you want for this publisher.
3. In the **Name** field, type in a name for the log publisher you are creating.
4. Select the Log Destinations for this publisher.
   a) Select a destination type from the Available list.
      The list of destinations displays only the type you selected.
   b) Select one or more destinations from the Available list.
   c) Move the selected destinations to the Selected list.

      If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.
5. Specify the additional settings needed to suit the requirements for this log publisher.

   The parameters on this screen are optional and perform the same function as they do when you configure a log publisher on a BIG-IP device.

   Note: *For details about the purpose or function of a particular setting, refer to the BIG-IP reference information on support.f5.com. From the BIG-IP Knowledge Center, select the BIG-IP LTM module and the software version you have installed; then select the appropriate guide. For example, information about the log publisher parameters for BIG-IP version 13.0 is provided in the External Monitoring of BIG-IP Systems: Implementations guide.*
6. Click **Save & Close**.
   The system creates the new log publisher with the settings you specified.

Create a new log filter

Before you create a new log filter, you must have configured at least one log publisher on this BIG-IQ.

Use this screen to create a new log filter for a managed device.

Create a custom log filters so you can specify the system log messages that you want to publish to a particular log.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Logs** > **Log Filters**.
   The Log Filters screen displays a list of the log filters that are defined on this device.
2. To create a new log filter, click **Create**.
   The New Log Filter screen opens so you can define the settings you want for this filter.
3. In the **Name** field, type in a name for the log filter you are creating.
4. Specify the additional settings needed to suit the requirements for this log filter.

   The remaining parameters on this screen are optional and perform the same function as they do when you configure a log filter on a BIG-IP device.

   Note: *For details about the purpose or function of a particular setting, refer to the BIG-IP reference information on support.f5.com. From the BIG-IP Knowledge Center, select the BIG-IP LTM module and the software version you have installed; then select the appropriate guide. For example, information about the log filter parameters for BIG-IP version 13.0 is provided in the External Monitoring of BIG-IP Systems: Implementations guide.*
5. Click **Save & Close**.
   The system creates the new log filter with the settings you specified.

Configure the BIG-IQ to manage an IPsec tunnel

How do I start managing an IPsec tunnel?

You can use BIG-IQ® Centralized Management to manage an IPsec tunnel. To set up IPsec tunnel management, you need to:

- Configure a data collection device.
- Configure the BIG-IQ system to manage the IPsec tunnel.
  - Create a forwarding virtual server for IPsec.
  - Create an IKE peer.
  - Create a custom IPsec policy.
  - Create a bidirectional IPsec traffic selector.
  - Configure the IKE daemon.
  - Verify IPsec connectivity.

After you complete these initial configuration tasks, you can manage the settings that control your IPsec tunnel traffic. You can also use the BIG-IQ statistics to troubleshoot the tunnel health.

Create a forwarding virtual server for IPsec

For IPsec, you create a forwarding (IP) type of virtual server to intercept IP traffic and direct it over the tunnel. With a forwarding (IP) virtual server, destination address translation and port translation are disabled.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Virtual Servers**.
   The screen displays the list of virtual servers defined on this device.
2. Click **Create**.
   The New Virtual Server screen opens.
3. For **Name**, type a name for the virtual server you are creating.
4. From **Device**, select the device on which to create the virtual server.
5. For **Partition**, type the name of the BIG-IP® device partition on which you want to create the virtual server.
6. For **Description**, type a brief description for the virtual server you are creating.
7. For **Destination Address**, type a wildcard network address in CIDR format, such as `0.0.0.0/0` for IPv4 or `::/0` for IPv6, to accept any traffic.
8. From **Service Port**, select ***All Ports**.
9. From **Protocol**, select ***All Protocols**.
10. For **VLANs and Tunnel Traffic**, retain the default selection, **All VLANs and Tunnels**.
11. Leave all other fields at their default settings.
12. Click **Save & Close**.
    The system creates the new virtual server with the settings you specified.

Create an IKE peer

The IKE peer object identifies to the system you are configuring the other device that it communicates with during Phase 1 negotiations. The IKE peer object also specifies the specific algorithms and credentials to use for Phase 1 negotiation.

Important: *You must configure the devices at both ends of the IPsec tunnel.*

1. At the top of the screen, click **Configuration**, then, on the left, click **NETWORK** > **IPsec** and then click **IKE Peers**.
2. Click **Create**.
   The New IKE Peer screen opens.
3. For **Name**, type a unique name for the IKE peer.
4. For **Description**, type a brief description of the IKE peer.
5. From **Device**, select the hostname of the device for which you are creating the new peer.
6. For the remainder of the fields on this screen, configure the values as you would if you were configuring an IKE peer on a BIG-IP® device.

   Note: *For details on configuring an IKE peer, refer to the BIG-IP TMOS: Tunneling and IPsec documentation on* `support.f5.com`
7. Click **Save & Close**.
   The system creates the new IKE peer with the settings you specified.

Create a custom IPsec policy

You can create a custom IPsec policy so that you can use a policy other than the default IPsec policy (`default-ipsec-policy` or `default-ipsec-policy-isession`). A typical reason for creating a custom IPsec policy is to configure IPsec to operate in Tunnel rather than Transport mode. Another reason is to add payload compression before encryption.

1. At the top of the screen, click **Configuration**, then, on the left, click **NETWORK** > **IPsec** and then click **IPsec Policies**.
2. Click **Create**.
   The New IPsec Policy screen opens.
3. For **Name**, type a unique name for the policy.
4. For **Description**, type a brief description of the policy.
5. For the remainder of the fields on this screen, configure the values as you would if you were configuring an IKE peer on a BIG-IP® device.

   Note: *For details on configuring a IPsec security policy, refer to the BIG-IP TMOS: Tunneling and IPsec documentation on* `support.f5.com`.
6. Click **Save & Close**.
   The system creates the new security policy with the settings you specified.

Create a bidirectional IPsec traffic selector

A traffic selector filters traffic based on the IP addresses and port numbers that you specify, as well as the custom IPsec policy you assign.

Important: *You must configure the devices at both ends of the IPsec tunnel.*

1. At the top of the screen, click **Configuration**, then, on the left, click **NETWORK** > **IPsec** and then click **Traffic Selectors**.
2. Click **Create**.
   The New Traffic Selector screen opens.
3. For **Name**, type a unique name for the traffic selector.
4. For **Description**, type a brief description of the traffic selector.
5. From **Device**, select the hostname of the device for which you are creating the new traffic selector.
6. For the remainder of the fields on this screen, configure the values as you would if you were configuring a traffic selector on a BIG-IP® device.

   Note: *For details on configuring a traffic selector, refer to the BIG-IP TMOS: Tunneling and IPsec documentation on* `support.f5.com`.
7. Click **Save & Close**.
   The system creates the new traffic selector with the settings you specified.

Configure the IKE daemon

To complete the configuration sequence for managing an IPsec tunnel on BIG-IQ®, you need to configure the IKE daemon.

1. At the top of the screen, click **Configuration**, then, on the left, click **NETWORK** > **IPsec** and then click **IKE Daemon**.
2. In the Name column, select the **ikedaemon** link that corresponds to the host name of the BIG-IP® device from which you imported the IPsec tunnel configuration.
   The IKE daemon properties screen for that BIG-IP device opens.
3. For **External Log Publisher**, select **default-ipsec-log-publisher**.
4. Click the **Save & Close** button at the bottom of the screen.

Verify IPsec connectivity

After you have configured an IPsec tunnel and before you configure additional functionality, you can verify that the tunnel is passing traffic.

Note: *Only data traffic matching the traffic selector triggers the establishment of the tunnel.*

1. At the top of the screen, click **Monitoring**, then, on the left, click **EVENTS** > **IPsec** > **Events** .
   The IPsec Event Logs screen opens and displays all of the logs collected from your IPsec tunnel.
2. Examine the screen, looking for event logs that relate to successful IPsec tunnel creation, to confirm IPsec connectivity.

Configure IPsec event viewing on the BIG-IQ

How do I configure viewing IPsec event logs?

You can use BIG-IQ® Centralized Management to view IPsec events. To set up IPsec event log viewing, you need to:

- Configure the BIG-IP® devices that comprise the IPsec tunnel to send events to the data collection device.
  - Create a remote log server pool.
  - Create a remote high-speed log destination for IPsec.
  - Create a remote Syslog destination for IPsec.
  - Configure a log publisher to send IPsec events to the BIG-IQ.
- Configure the BIG-IQ system to view IPsec events by enabling IPsec event collection.

After you complete these initial configuration tasks, you can view IPsec events on the BIG-IQ.

Create a pool of remote log servers

Creating a remote log server pool is part of the sequence you perform to route IPsec events from the BIG-IP® device to your data collection device so that you can view these events from the BIG-IQ®.

Important: *You must perform these steps for both of the BIG-IP devices that comprise the IPsec tunnel.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Pools**.
   The screen displays the list of pools defined on this device.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type in a name for the pool you are creating.

   Names must begin with a letter, and can contain only letters, numbers, and the underscore (_) character.

   Important: *The pool name is limited to 63 characters.*
4. From the **Device** list, select one of the devices that comprise the IPsec tunnel.
5. To add a new pool member for this pool, click **New Member**.
   a) Specify the **Node Type** select **New Node**:
   b) Type a helpful name for the **Node Name**.
   c) For the **Node Address** type the self IP address of the data collection device that you want events from this device to go to.
   d) For the **Port**, type `9997`.
   e) Click **Save & Close**.

   The new pool member is added to the specifications for the pool you are creating.

Note: *When you create a new pool member while creating a new pool, the new pool member is not actually created until you save the new pool. When you create a new pool member for an existing pool member, the new member is ready to use as soon as you save it.*

6. When you finish specifying the settings for this pool, click **Save & Close**.
   The system creates the new pool with the settings you specified.
7. Repeat the last 5 steps to add a pool and pool member for the other device that makes up the IPsec tunnel.

The remote log server pool you created is added to the pools list.

Create a remote high-speed log destination for IPsec

Before creating a remote high-speed log destination for IPsec, you must create a log publishing pool.

Creating a remote high-speed log destination is part of the sequence you perform to route IPsec events from the BIG-IP® device to your data collection device so that you can view these events from the BIG-IQ®.

Important: *You must perform these steps for both of the BIG-IP devices that comprise the IPsec tunnel.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Logs** > **Log Destinations**.
   The Log Destinations screen displays a list of the log destinations that are defined on this device.
2. Click **Create**.
   The New Log Destination screen opens.
3. In the **Name** field, type a name to identify the IPsec remote high speed log destination.
4. From the **Type** list, select **Remote High-Speed Log**.
5. Specify which devices to associate this destination with.
   a) Select the device you want this destination to use.
   b) Select the remote log server pool that you defined previously.
   c) Click **Save** to add the listed devices to the Device Specific list.

   Devices you select for this log destination are added to the Device Specific list.

   Note: *Click on a device name in the Device Specific list to edit settings for that device. Bear in mind though that changes you make to one device do not change the settings for other devices, or for the base configuration for the log destination.*
6. Click **Save & Close**.
   The system creates the new log destination with the settings you specified.

Create a remote Syslog destination for IPsec

Before creating a remote Syslog log destination for IPsec, you must create a log publishing pool and a high-speed log destination for IPsec.

Creating a remote Syslog log destination is part of the sequence you perform to route IPsec events from the BIG-IP® device to your data collection device so that you can view these events from the BIG-IQ® system.

Important: *You must perform these steps for both of the BIG-IP devices that comprise the IPsec tunnel.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Logs** > **Log Destinations**.
   The Log Destinations screen displays a list of the log destinations that are defined on this device.
2. Click **Create**.
   The New Log Destination screen opens.
3. In the **Name** field, type `IPsec-Syslog` to identify the IPsec Syslog destination.
4. From the **Type** list, select **Remote Syslog**.
5. From the **Syslog Format** list, select a format for the logs.
6. From the **Forward To** list, select the name of the IPsec remote high speed log.
7. Click **Save & Close**.
   The system creates the new log destination with the settings you specified.

Configure a log publisher to send IPsec events to the BIG-IQ

To send the IPsec event logs to the data collection device, you must configure a publisher to send them to the IPsec Syslog destination.

Important: *You must perform these steps for both of the BIG-IP devices that comprise the IPsec tunnel.*

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Logs** > **Log Publishers**.
   The Log Publishers screen displays a list of the log publishers that are defined on this device.
2. Click the log publisher named **default-ipsec-log-publisher**.
   The Log Publisher properties screen opens.
3. For the **Log Destinations** setting, select **IPsec-Syslog** from the **Available** list, and move it to the **Selected** list.
4. Click **Save & Close**.

To use the IPsec tunnel configuration to collect IPsec events, you must activate IPsec event collection for your data collection device (DCD) cluster.

Enable IPsec event collection

To view IPsec tunnel events on BIG-IQ®, you need to activate IPsec event collection for your data collection device (DCD) cluster.

1. At the top of the screen, click **System**, and then, on the left, click **BIG-IQ DATA COLLECTION** > **BIG-IQ Data Collection Devices**.
   The BIG-IQ Data Collection Devices screen opens to list the data collection devices in the cluster.
2. In the Services column, click **Add Services**.
   The Services screen for this DCD opens.
3. For IPsec, click **Activate**.

   The Listener Address displays the internal self IP address configured for the DCD. The self IP address is currently the recommended address for collecting event log data.

   The system begins collecting IPsec events.
4. Click the **Save & Close** button at the bottom of the screen.

You can now view IPsec event logs using the BIG-IQ user interface.

Troubleshooting an IPsecTunnel

Troubleshoot an unhealthy IPsec tunnel using performance statistics

Before you can troubleshoot the tunnel using statistics:

- You must have configured BIG-IQ® to display statistics for your IPsec tunnel.
- You need to know the IP address or host name of the BIG-IP® devices that form the IPsec tunnel.

When you learn that an IPsec tunnel is unhealthy (for example, your helpdesk might have opened a ticket), you can use the IPsec performance statistics to troubleshoot the tunnel.

Note: *If one end of the tunnel uses a device other than a BIG-IP device, you can troubleshoot only that end of the tunnel.*

---

1. At the top of the screen, click **Devices**.
2. Find one of the BIG-IP devices that form the IPsec tunnel.
   - If you have the IP address of the device, from the **Filter** selector, select **Address** and type the IP address of the BIG-IP device.
   - If you have the host name of the device, from the **Filter** selector, select **Device Name** and type the host name of the BIG-IP device.

   The filter you created displays at the top of the screen and only the BIG-IP device you identified is listed.
3. Click the device name for the BIG-IP device.
   The properties screen for the device opens.
4. On the left, click **Health**.
   A health summary screen displays current usage levels for the device.
5. In the upper right corner, click **View Health Statistics**.
   The Device Health statistics summary page opens, displaying data only for the selected BIG-IP device.
6. Scan the graphs for details about the device's performance that reveal the source of the issue. If you find the issue, skip to step 11.
7. In the upper left corner, click the back arrow.
   The health summary screen for the device opens again.
8. In the upper right corner, click **View Traffic Statistics**.
   The Device Traffic statistics summary page opens, displaying data only for the selected BIG-IP device.
9. Scan the graphs for details about the device's performance that reveal the source of the issue. If you find the issue, skip to step 11.
10. If you don't find the source of the problem after examining the traffic and device health statistics, delete the filter you created in step 2, and then repeat the last 8 steps for the other BIG-IP device in the IPsec tunnel. If only one end of the tunnel is made up of a BIG-IP device, proceed to the task *Troubleshoot an unhealthy IPsec tunnel using event logs*, to see if you can isolate the issue by inspecting the IPsec event logs. If you find the issue, skip to step 11.
11. Fix the issues you discovered with the configuration objects, and then deploy those changes to the relevant BIG-IP devices to resolve the problem.

If you were not able to isolate the cause of the issue, perform the task: *Troubleshoot an unhealthy IPsec tunnel using event logs*.

Troubleshoot an unhealthy IPsec tunnel using event logs

Before you can troubleshoot a tunnel by examining the IPsec event logs, you must have configured IPsec event logging. (See *Configure IPsec event viewing on the BIG-IQ* for details.)

When you learn that an IPsec tunnel is unhealthy (for example, your helpdesk might have opened a ticket), you can troubleshoot the tunnel by examining the IPsec event logs.

1. At the top of the screen, click **Monitoring**, then, on the left, click **EVENTS** > **IPsec** > **Events** . The IPsec Event Logs screen opens and displays all of the logs collected from your IPsec tunnel.
2. Use the **DEVICE**, **TIMEFRAME**, and **LOG LEVEL** filters to display the logs that you think will reveal the source of the issue.
3. Analyze the log of events to find the issue that is causing the IPsec tunnel to perform improperly.
4. Fix the issues you discover, and then deploy those changes to the relevant BIG-IP® devices.

Managing Object Pinning

What is object pinning?

You *pin* an object, such as a logging profile, to a pinning policy to have it included in a deployment. The pinning policy is associated with a BIG-IP® device and has the same name as the BIG-IP device. You do not create pinning policies. Pinning policies always exist to contain objects that get pinned to a policy.

You pin an object to a pinning policy for a BIG-IP device to mark the object as being used by the BIG-IP device configuration, and to have it deployed with that configuration and not deleted from the device. When an object is pinned for deployment to a BIG-IP device that is part of a cluster, the object is deployed to the other member of the cluster as well.

You use the Pinning Policies screen to pin policy objects so that they are deployed to a BIG-IP device, or to view the objects that are already pinned to be deployed to a BIG-IP device. The objects that can be selected for pinning differ depending on which service is being used. For example, only the Network Security service allows you to pin firewall policy objects, and only the Local Traffic service allows you to pin SMTP server objects. You can pin objects to, or unpin objects from, multiple BIG-IP device pinning policies at once.

Note: *Both the system and users can pin an object. But users can unpin only objects that are labeled as user pinned. For easy identification, objects pinned by a user are listed with the User identifier in the Pin Source Tags column on the Pinning Policy Properties screen. Any user can unpin a user pinned object.*

Pin objects to a BIG-IP device pinning policy

You pin objects, such as logging profiles, to BIG-IP®device pinning policies to ensure that the objects are deployed to BIG-IP devices. The process for pinning to a single BIG-IP device pinning policy differs from the process for pinning to several BIG-IP device pinning policies.

1. Open the Pinning Policies screen. How you access the screen depends on the service you are using.
   - To pin Local Traffic service objects, click **Configuration** > **LOCAL TRAFFIC** > **Pinning Policies**.
   - To pin Network Security service objects, click **Configuration** > **SECURITY** > **Network Security** > **Pinning Policies**.
   - To pin Shared Security service objects, click **Configuration** > **SECURITY** > **Shared Security** > **Pinning Policies**.
   - To pin Access service objects, click **Configuration** > **ACCESS** > **Access Groups** > **Pinning Policies**. An Access group must exist to see this menu item.
2. Decide whether to pin to a single BIG-IP device pinning policy, or multiple BIG-IP device pinning policies.
   - Go to Step 3 to pin objects to a single BIG-IP device pinning policy.
   - Go to Step 4 to pin objects to multiple BIG-IP device pinning policies.
3. To pin objects to a pinning policy for a single BIG-IP device:
   a) Click the name of the BIG-IP device pinning policy to which you will pin objects. (It has the same name as the associated BIG-IP device.)
   The properties screen opens.
   b) At the top of the area near the bottom of the screen, select the type of object to be pinned.

The screen lists objects of the type you selected.

c) Select the check box to the left of the objects to be pinned, and click **Add Selected**.

4. To pin objects to multiple BIG-IP device pinning policies:
   a) Select the check boxes for the BIG-IP device pinning policies to which to pin objects, and click **Pin to Multiple Policies**.
   The properties screen opens and displays the selected BIG-IP device pinning policies.
   b) In the area near the bottom of the screen, select the type of object to be pinned.
   The screen lists objects of the type you selected.
   c) Select the check box for objects to be pinned and click **Add Selected**.
5. Save your work.

A dialog box displays the success of the pinning operation. The object, or objects, are pinned to the pinning policy for the BIG-IP device, or devices, and will be deployed with them.

Unpin objects from a BIG-IP device pinning policy

You unpin objects, such as logging profiles, from a BIG-IP® device pinning policy when they no longer need to be deployed with the BIG-IP device. The process for unpinning from a single BIG-IP device pinning policy differs from the process for unpinning from several BIG-IP device pining policies.

Note: *Both the system and users can pin an object. But users can unpin only objects that are labeled as user pinned. For easy identification, objects pinned by a user are listed with the User identifier in the Pin Source Tags column on the Pinning Policy Properties screen. Any user can unpin a user pinned object.*

1. Open the Pinning Policies screen. How you access the screen depends on the service you are using.
   - To unpin Local Traffic service objects, click **Configuration** > **LOCAL TRAFFIC** > **Pinning Policies**.
   - To unpin Network Security service objects, click **Configuration** > **SECURITY** > **Network Security** > **Pinning Policies**.
   - To unpin Shared Security service objects, click **Configuration** > **SECURITY** > **Shared Security** > **Pinning Policies**.
   - To pin Access service objects, click **Configuration** > **ACCESS** > **Access Groups** > **Pinning Policies**. An Access group must exist to see this menu item.
2. Decide whether to unpin from a single BIG-IP device pinning policy, or from multiple BIG-IP device pinning policies.
   - Go to Step 3 to unpin objects from a single BIG-IP device pinning policy.
   - Go to Step 4 to unpin objects from multiple BIG-IP device pinning policies.
3. To unpin objects from a single BIG-IP device pinning policy:
   a) Click the name of the BIG-IP device pinning policy from which to unpin objects.
   The properties screen opens.
   b) In the Selected Resources area, expand the resource type of the object you want to unpin.
   The screen lists objects of the type you selected.
   c) Select the check box for the objects to be unpinned and click **Remove**.

   Both the system and users can pin an object. But users can unpin only objects that are labeled as user pinned. For easy identification, objects pinned by a user are listed with the User identifier in the Pin Source Tags column on the Pinning Policy Properties screen. Any user can unpin a user pinned object.
4. To unpin objects from multiple BIG-IP device pinning policies:

a) Select the check boxes for the BIG-IP device pinning policies from which to unpin objects, and click **Unpin from Multiple Policies**.
The properties screen opens and displays the selected BIG-IP device pinning policies.

b) In the lower area of the screen, select the type of object to be unpinned.
The screen lists objects of the type you selected.

c) Select the check box for the objects to unpin and click **Add Selected**.

The Selected Resources area lists the objects to be unpinned. Both the system and users can pin an object. But users can unpin only objects that are labeled as user pinned. For easy identification, objects pinned by a user are listed with the User identifier in the Pin Source Tags column on the Pinning Policy Properties screen. Any user can unpin a user pinned object.

5. Save your work.

A dialog box displays the success of the unpinning operation. The object or objects are unpinned from the BIG-IP device pinning policy and will no longer be deployed to it.

Managing Address Lists

About address lists

Address lists, also called network address lists, are collections of IPv4 or IPv6 addresses, address ranges, nested address lists, geolocations, and subnets. These can be used by other parts of the BIG-IQ® Centralized Management system, such as firewall rules or firewall policies.

You can manage address lists from the following locations:

- **Configuration** > **NETWORK** > **Address Lists**
- **Configuration** > **SECURITY** > **Network Security** > **Address Lists**

Be aware of the following considerations about address lists.

- Address lists are containers and must contain at least one entry. You cannot create an empty address list; you cannot remove an entry in an address list if it is the only one.
- Before nesting an address list inside an address list, check to be sure this option is supported on each BIG-IP® device where you intend to deploy the address list.
- To pin an address list to a deployment, you must do so from the Local Traffic pinning policy user interface: **Configuration** > **LOCAL TRAFFIC** > **Pinning Policies**.
- You can add geolocation awareness to address lists, which enables you to specify source or destination IP addresses by geographic location rather than by their IP addresses. The geolocation is validated when the address list is saved. If you use a geolocation specification that is valid on the BIG-IQCentralized Management system, but not supported on a particular BIG-IP device because the device has a different geolocation database, it causes a deployment failure for that device. Importing a BIG-IP device with an invalid geolocation specification causes a discovery failure for that device.

Create address lists

You create address lists so that you can use them with other parts of the BIG-IQ® Centralized Management system, such as firewall rules. Address lists are a collection of addresses. You can access address lists from either the network or the network security configuration menu.

- To use the network configuration, click **Configuration** > **NETWORK** > **Address Lists**.
- To use the security configuration, click **Configuration** > **SECURITY** > **Network Security** > **Address Lists**.

1. Open the Address Lists screen.

   You can access the address list from either the network or network security configuration menu and it will behave in the same way.
2. Click **Create**.
   The New Address List screen opens.
3. On the left, click **Properties**.
4. Supply the properties for the address list.
   - In the **Name** setting, type a unique name for the address list.
   - In the **Description** setting, type an optional description for the address list.
   - In the **Partition** setting, type a partition if needed. The `Common` partition is the default.
5. On the left, click **Addresses**.
6. Supply the addresses for the address list.

The screen displays a template address for you to complete. An address list must contain at least one address.

7. In the **Type** column, select the address type, and then provide the address information in the **Addresses** column. You can also add a description for each address in the **Description** column.

   - To add a single address, select **Address** and type an IPV4 or IPV6 address.
   - To add an address list, select **Address List** and select the name of the address list.
   - To add a range of addresses, select **Address Range** and type the beginning and ending IPV4 or IPV6 addresses.
   - To add a location to the address list, select **Country/Region** and select the country and optionally, the region of the country. You can also select `Unknown` as the country or region option. Address locations can be used when defining rules based on where a system is located (the geolocation of the system), rather than on the IP address of the system.
   - To add a domain name, select **Domain Name** and type the domain name.

8. In the **Add/Remove** column, click + to add the address to the list.

   You can click **X** to delete an address from the list.

9. Continue to add or delete addresses to the address list until the address list is complete.
10. Save your work.

Edit address lists

You edit address lists to change the properties of the address list or to add, modify, or remove addresses from the address list, or both. You can access address lists from either the network or the network security configuration menu.

- To use the network configuration, click **Configuration** > **NETWORK** > **Address Lists**.
- To use the security configuration, click **Configuration** > **SECURITY** > **Network Security** > **Address Lists**.

1. Open the Address Lists screen.

   You can access an address list from either area and it will behave in the same way.

2. Click the name of the address list to edit it.
3. To modify the address list **Description**, click **Properties** and in the **Description** setting, type or revise an optional description for the address list.
4. On the left, click **Addresses**.
5. Add, modify, or delete addresses for the address list.

   - To modify that address, click the pencil icon to the left of the address.
   - To delete an address, click **X** in the **Add/Remove** column.
   - To add an address, click + in the **Add/Remove** column.

   An address list must contain at least one address.

6. If you are adding or modifying an address, supply or modify the settings.

   In the **Type** column, select the address type, and then provide the address information in the **Addresses** column. You can also add a description for each address in the **Description** column.

   - To add a single address, select **Address** and type an IPV4 or IPV6 address.
   - To add an address list, select **Address List** and select the name of the address list.
   - To add a range of addresses, select **Address Range** and type the beginning and ending IPV4 or IPV6 addresses.

- To add a location to the address list, select **Country/Region** and select the country and optionally, the region of the country. You can also select `Unknown` as the country or region option. Address locations can be used when defining rules based on where a system is located (the geolocation of the system), rather than on the IP address of the system.
- To add a domain name, select **Domain Name** and type the domain name.

7. In the **Add/Remove** column, click **+** to add the address to the list.

   You can click **X** to delete an address from the list.
8. Continue to add, modify, or delete addresses in the address list until the address list is complete.
9. Save your work.

Clone address lists

You can clone an address list to create a copy of it, which you can then edit to address any special considerations. You can access address lists from either the network or the network security configuration menu.

- To use the network configuration, click **Configuration** > **NETWORK** > **Address Lists**.
- To use the security configuration, click **Configuration** > **SECURITY** > **Network Security** > **Address Lists**.

1. Open the Address Lists screen.

   You can access an address list from either area and it will behave in the same way.
2. Select the check box next to the address list to clone.
3. Click **Clone**.
   The system makes a copy of that address list with the same name, but with `-CLONE` appended to the name and a blank **Description** field.
4. Change the address list properties and contained addresses as needed, such as providing a meaningful name or changing an address within the list.
5. Save your work.

The new address list is now defined and you can assigned it to an object.

Deploy address lists

If you want to do a quicker deployment by only deploying the address list portion of a configuration, you can do a partial deployment of the address list, instead of deploying the entire configuration. You can access address lists from either the network or the network security configuration menu.

- To use the network configuration, click **Configuration** > **NETWORK** > **Address Lists**.
- To use the security configuration, click **Configuration** > **SECURITY** > **Network Security** > **Address Lists**.

1. Open the Address Lists screen.

   You can access an address list from either area and it will behave in the same way.
2. Select the check box next to the address list to deploy.
3. Click **Deploy**.

The system displays the selected address list, with options for partial deployment selected. You can now continue the partial deployment process.

Delete address lists

You delete address lists you no longer use to avoid confusion in the user interface. You can access address lists from either the network or the network security configuration menu.

- To use the network configuration, click **Configuration** > **NETWORK** > **Address Lists**.
- To use the security configuration, click **Configuration** > **SECURITY** > **Network Security** > **Address Lists**.

1. Open the Address Lists screen.

   You can access an address list from either area and it will behave in the same way.
2. Click the check box next to the address list to delete.
3. Click **Delete**.
4. In the confirmation dialog box that opens, click **Delete** to confirm the removal.

   If the address list is pinned to a BIG-IP device pinning policy, the deletion will fail.

Managing Eviction Policies

Eviction policy overview

An eviction policy provides the BIG-IP® device with guidelines for how aggressively it discards flows from the flow table. You can customize the eviction policy to prevent flow table attacks, where a large number of slow flows are used to negatively impact system resources. You can also set the way that the system responds to such flow problems in an eviction policy, and attach such eviction policies globally, to route domains, and to virtual servers, to protect the system, applications, and network segments with a high level of customization.

Note: *For more information on how BIG-IP devices use eviction policies, refer to the BIG-IP system reference information on* `support.f5.com`*. From the BIG-IP Knowledge Center, select the BIG-IP AFM module and the software version you have installed; then select the appropriate guide. For example, information about the eviction policy parameters for BIG-IP version 13.0 is provided in the BIG-IP Network Firewall: Policies and Implementations, Version 13.0 guide in the Preventing Attacks with Eviction Policies and Connection Limits chapter.*

Create a new eviction policy

You can create a new eviction policy that provides guidelines to determine how aggressively your BIG-IP® devices discard flows from the flow table.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **Eviction Policies**.
   The Eviction Policies screen displays a list of the eviction policies that are defined on this device.
2. Click **Create**.
   The New Eviction Policy screen opens, so that you can specify settings for a new policy.
3. In the **Name** field, type in a name for the eviction policy you are creating.
4. Specify the additional settings needed for this eviction policy.

   Name is the only required parameter when you specify a new eviction policy. The remaining parameters on this screen are optional and perform the same function as they do when you configure an eviction policy on a BIG-IP® device.

   Note: *For details about the purpose or function of a particular setting, refer to the BIG-IP system reference information on* `support.f5.com`*. From the BIG-IP Knowledge Center, select the BIG-IP AFM module and the software version you have installed; then select the appropriate guide. For example, information about the eviction policy parameters for BIG-IP version 13.0 is provided in the BIG-IP Network Firewall: Policies and Implementations, Version 13.0 guide in the Preventing Attacks with Eviction Policies and Connection Limits chapter.*

   ---

5. Click **Save & Close**.

Manage eviction policies and general settings

You can use the BIG-IQ® to manage the settings for an existing policy and apply eviction policies to any managed device. Eviction policies establish guidelines for how aggressively a BIG-IP® device discards flows from the flow table.

1. At the top of the screen, click **Configuration**, and then, on the left, click **LOCAL TRAFFIC** > **General Settings**.
   The General Settings screen displays a list of the devices that are managed by this device.
2. Under Device, select the name of the device for which you want to manage eviction policies or general settings.
   The properties screen opens, so that you can specify the policy or general settings you want.
3. For the **Eviction Policy** setting, select the policy you want to use for this device.
4. If this device is running version BIG-IP 13.0.0 or later, you can revise the settings for SYN check threshold and SYN Cookie protection.

   Note: *For details about the purpose or function of a particular setting, refer to the BIG-IP system reference information on* `support.f5.com`*. From the BIG-IP Knowledge Center, select the BIG-IP AFM module and the software version you have installed; then select the appropriate guide. For example, information about the SYN check and SYN threshold parameters for BIG-IP version 13.0 is provided in the BIG-IP Systems: Protecting against SYN Flood Attacks, Version 13.0 guide.*

   ---

5. Click **Save & Close**.

Legal Notices

Legal notices

Publication Date

This document was published on December 29, 2017.

Publication Number

MAN-0577-08

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*.

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

L

M

N

O

P

R

S

T

V