

BIG-IP Application Visibility: How to configure the BIG-IP system

Overview: About the BIG-IP configuration for BIG-IQ application visibility

The F5® BIG-IQ® Centralized Management Application Summary dashboard displays statistics for applications and users that are managed by the BIG-IP® system. This includes the most requested applications, and how often individual users access the applications. For example, as an administrator, you can see the application summary report for the SharePoint application managed by the BIG-IQ system. You can use the report to track usage statistics, such as the request count for SharePoint and the most frequent users by request count. You can also adjust the time slider to see statistics for a certain period.

To display these statistics, you must configure the BIG-IP system to classify the application traffic, create log messages, and send them to the BIG-IQ system. You can choose from two types of configurations:

Basic

A Basic configuration is your starting point to configure the BIG-IP system for application visibility. In some cases, you only need this option to generate the application logs and send them to the BIG-IQ system.

Advanced

In an Advanced configuration, after you configure a basic configuration and validate the reports, you might need to configure more BIG-IP resources such as classification presets and profiles. This situation typically occurs if there is not a predefined classification profile in the application that you want to display statistics and reports in.

Before you begin configuring application visibility, refer to *Access Reporting and Statistics*, in the *F5® BIG-IQ® Centralized Management: Monitoring and Reports* guide.

Note: Configure both BIG-IP® LTM® and BIG-IP® APM®. Portal Access is not supported.

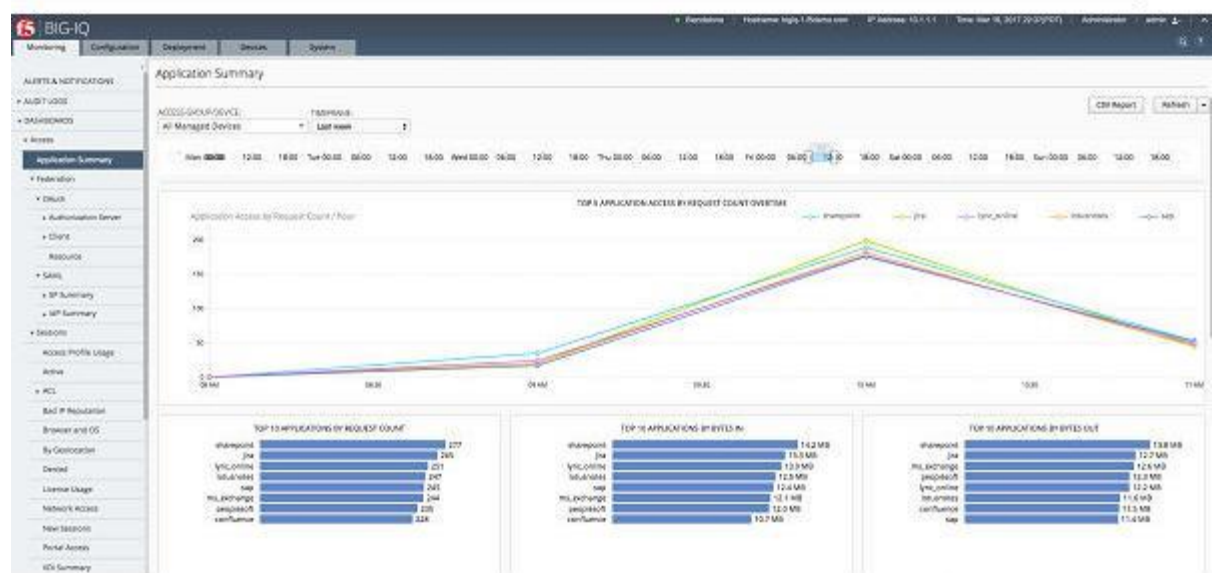


Figure 8: Sample Application Summary dashboard

Notice the length of time displayed by the line graph, dictated by the time slider above. Also notice the top ten applications, with SharePoint at number one. You can select an application and view the usage over time and the top users for that application.

View the Application Summary dashboard

The BIG-IQ[®] Centralized Management Application Summary dashboard displays information regarding the applications linked to the system.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS > Access > Application Summary**.

The Application Summary screen opens, showing detailed information and charts for specific applications.

What is a basic configuration?

The basic BIG-IP[®] system configuration for BIG-IQ[®] application visibility is when a classification profile is already available to the administrator. This situation occurs when you want to track predefined access applications in BIG-IQ, such as SharePoint, OWA, PeopleSoft, or Lotus Notes. When you configure the virtual server for one or more of these applications, the BIG-IP system has already configured a classification profile. For most other applications, this basic configuration does not apply, and you must create the classification profile as well as other necessary resources.

In some cases, you might want to define your own signatures. If so, even in a basic configuration, you must upload the signatures in Traffic Intelligence.

For a basic configuration, configure the following resources in both the BIG-IQ and BIG-IP systems:

- Enable remote logging in the Access area of BIG-IQ. Refer to the "BIG-IQ Centralized Management: Access" manual to learn how to configure remote logging.
- Update classification signatures in BIG-IP Traffic Intelligence.
- Configure a virtual server in BIG-IP Local Traffic.
- Attach an existing classification profile to the virtual server.

Note: You must use BIG-IP version 13.0 as well as BIG-IQ version 5.2 or later.

Note: As part of the remote log configuration process, the system creates only the classification profile object name (classification _access). Because this classification profile is not attached to any virtual servers, you must add it to the virtual server used for applications that display reporting data. You should also enable the classification profile on the virtual server.

About traffic signatures for application visibility

Classification signatures define different types of traffic that the BIG-IP[®] system can recognize through Traffic Intelligence. The system recognizes a predefined set of signatures for common applications and application categories that are updated periodically. You can download signature updates from F5 Networks, and schedule the system to automatically update the signatures (pull the updated signatures automatically). You can also manually install the classification signatures and updates, for example, if the BIG-IP system does not have Internet access.

Signatures are updated once a month and have the following requirements:

- Set up the DNS server on the BIG-IP system in order for the automatic updates to work.
- The management network should be on the Internet.

Scheduling automatic signature updates

You can set up the BIG-IP® system to automatically update the classification signatures. This ensures that the system always has the latest classification signature files.

1. On the Main tab, click **Traffic Intelligence > Applications > Signature Update**. The Signatures screen opens.
2. Click **Check for Updates** to manually upload a signature file update if one is available. You see the current date and time in the **Latest Update Check** setting of the Signature Definitions area.
3. To upload a signature file update, in the Signature Definitions area, click **Import Signatures**. The Applications screen displays a **Signatures File** field where you can select the new signature file.
4. To discard and remove any installed upgrades and reset the classification engine and signatures to factory default, click **Reset to Defaults**.
5. In the **Signatures File** field, click **Choose File** to navigate to the previously uploaded signatures file.
6. Click **Upload**.
A message displays indicating whether your upload was successful.
7. For the **Automatic Updates Settings**, in the **Signature Update** screen, select **Enabled**.
8. From the **Update Schedule** setting, select **Daily**, **Weekly**, or **Monthly** to specify how often you want the system to check for updates.
9. Click **Update** to save your settings.

The signature updates take effect immediately.

Modify the virtual server for a basic configuration

Before you configure the virtual server in the BIG-IP® system, you must enable remote logging in the BIG-IQ® system.

For the BIG-IQ system to display statistics and reporting for an application such as SharePoint, OWA, or Lotus Notes, the application's virtual server must have a classification profile attached.

1. In the Main tab, click **Local Traffic > Virtual Servers > Virtual Server List**. A list of existing virtual servers displays.
2. Select the virtual server of the application that you wish to map to the BIG-IQ system. The virtual server editing (properties) screen opens.
3. From the **Configuration** list, select **Advanced**.
4. From the **Classification Profile** list, select `classification_access`.

This classification profile was created by the BIG-IP system when you enabled remote logging in the BIG-IQ system.

5. Click **Update**.

You have added a classification profile to the virtual server.

What is an advanced configuration?

If you want to display statistics and reports using the Access feature of BIG-IQ® in an application that does not have a predefined classification profile, you must create the classification profile and attach it to the virtual server. This is considered an advanced configuration and applies to most applications.

Because of this, you must configure the following resources in both BIG-IQ and BIG-IP® systems:

1. Enable remote logging in BIG-IQ Access. Refer to the *BIG-IQ Centralized Management: Access* manual to learn how to configure remote logging.
2. Create a classification policy in BIG-IP system Traffic Intelligence screens.

3. Create a new application from the Traffic Intelligence application list by customizing a category.
4. Update the existing classification preset or create a new preset.
5. Create a classification profile in the BIG-IP system's Local Traffic settings if you created a new classification preset. Otherwise, update the existing classification profile to include the existing preset.
6. Configure a virtual server in the BIG-IP system's Local Traffic settings.

Note: Advanced configuration is introduced in BIG-IP version 13.1 and 13.0 Hotfix build 13.0.0 HF3.

Note: As part of the remote log configuration, only the classification profile object name (classification_access) is created. Because this classification profile is not attached to any virtual servers, you must add to the virtual server used for applications that display reports. You should also enable the classification profile on the virtual server.

Creating a custom local traffic policy

You can create a custom local traffic policy to manage traffic assigned to a virtual server.

1. On the Main tab, click **Local Traffic > Policies**.

For more information about local traffic policies, refer to *BIG-IP® Local Traffic Manager™: Implementations*.

The Policy List screen opens.

2. Click **Create**.

The New Policy List screen opens.

3. In the **Policy Name** field, type a unique name for the policy, such as companyA.

4. In the **Description** field, type some descriptive text that identifies the policy definition.

5. From the **Strategy** list, select the action that the policy initiates when there are multiple rules that match.

Rule	Description
------	-------------

All	Uses the first or best strategy to resolve the conflict of rule match.
------------	--

Best	Applies the actions of the rule specified in the list of defined strategies for the associated policy.
-------------	--

First	Applies the actions of only the first rule. This implies that the rule with the lowest ordinal, highest priority, or first in the list is applied.
--------------	--

6. From the **Type** list, select **CE Profile** to attach the policy to a CE profile.

7. Click **Create Policy**.

This creates a policy that manages traffic assigned to a virtual server.

You have created a new local traffic policy for application visibility.

Creating a category

On the BIG-IP® system, you can create customized categories for classifying traffic if the predefined categories are not sufficient for your needs. For example, if you plan to create new application types unique to your organization, you can create a category to group them together. Alternatively, you can add an existing category to your application list.

1. On the Main tab, click **Traffic Intelligence > Applications > Application List**. The Applications screen displays a list of the supported classification categories.
2. On the Main tab, click **Traffic Intelligence > Categories > Category List**. The Category list screen opens.
3. Click **Create**.

The New URL Category screen opens.

4. In the **Name** field, type a name for the classification category.
5. In the **Description** field, type optional informative text.
6. In the **Category ID** field, type an identifier for this category, a unique number.
7. In the **Application List** setting, select applications from the list and use the Move buttons to move applications from one list to the other.
8. Click **Finished**.

You have created custom applications to handle the traffic.

Create a classification application

The BIG-IP® system classifies many categories of traffic and specific applications within those categories. You can create a new classification application, and determine which categories and applications of traffic the system can classify.

1. On the Main tab, click **Traffic Intelligence > Applications > Application List**. The Applications screen displays a list of the supported classification categories.
2. To view the applications in each category, click the + icon next to the category.
3. To view or edit the properties of the application or category, click the name to open its properties screen.

***Tip:** Here you can view the application or category ID number.*

4. Click **Create**.
5. In the **Name** field, type a name for the classification application.
6. In the **Description** field, type a descriptive text identifying the classification application.
7. In the **Application ID** field, type the identifier for a category, a new, unique number.
8. From the **Category** list, select an existing category or a category that you created.
9. Click **Finished**.

About presets and profiles

In BIG-IP® application visibility, as part of the advanced configuration, there are two ways to configure the BIG-IP® classification preset and classification profile.

- You can use the existing classification preset, and make sure it is associated with the current classification profile.
- You can create a new classification preset, but you must also associate it with a new classification profile.

Updating classification presets

On the BIG-IP® system, you can update classification preset settings for a classification policy that you have previously created. Alternatively, you can create a new preset for application visibility.

1. On the Main tab, click **Traffic Intelligence > Presets**.
The Presets screen displays a list of the supported classification categories.
2. From the preset list, select the preset **CE**.
3. From the **Policies** setting, move policies from the **Available** list to the **Enabled** list.
4. Click **Update**.

Updating a classification profile

If you update the existing classification preset, update the existing classification profile and attach the existing preset. In the profile, you can change which virtual servers and which categories of traffic are included in the classification statistics.

1. On the Main tab, click **Local Traffic > Profiles > Classification**. The Classification screen opens.
2. Click **Create**.
The New Classification Profile screen displays.
3. In the **Name** field, type a name for the classification profile.
4. In the **Description** field, click the check box and type a description for the profile.
5. From the **Parent Profile** dropdown list, select an existing profile from which this profile is derived. This profile inherits settings from the parent profile.
6. Click the checkbox next to **Custom**.
7. From the **Preset** dropdown list, select the preset **CE**.
8. From the **Log Publisher dropdown** list, select **access-gpa-log-publisher**.
9. Click **Finished**.

The BIG-IP system classifies traffic for the virtual servers and categories specified in the Classification profile.

Creating classification presets

On the BIG-IP[®] system, you can create classification preset settings for a classification policy that you have previously created.

1. On the Main tab, click **Traffic Intelligence > Presets**.
The Presets screen displays a list of the supported classification categories.
2. Click **Create**.
The New Presets screen opens.
3. In the **Name** field, type a name for the application.
4. In the **Description** field, type optional descriptive text for the classification presets.
5. For the **Policy** setting, move the classification policies from **Available** list to the **Selected** list, to create a new preset.
6. In the **Allow Reclassification** list, **Enabled** is the default selection.
7. In the **Flow Bundling** list, **Enabled** is the default selection.
8. In the **Cache Results** list, **Enabled** is the default selection.
9. Click **Finished**.

Creating a classification profile

If you create a new classification preset, you must create a new classification profile and attach the preset. In the profile, you can change which virtual servers and which categories of traffic are included in the classification statistics.

1. On the Main tab, click **Local Traffic > Profiles > Classification**. The Classification screen opens.
2. Click **Create**.
The New Classification Profile screen displays.
3. In the **Name** field, type a name for the classification profile.
4. In the **Description** field, click the check box and type a description for the profile.
5. From the **Parent Profile** dropdown list, select an existing profile from which this profile is derived. This profile inherits settings from the parent profile.
6. Click the checkbox next to **Custom**.
7. From the **Preset** dropdown list, select the new preset that you created previously.
8. From the **Log Publisher dropdown** list, select **access-gpa-log-publisher**.
9. Click **Finished**.

The BIG-IP system classifies traffic for the virtual servers and categories specified in the Classification profile.

Modify the virtual server for an advanced configuration

Before you configure the virtual server in the BIG-IP® system, enable remote logging in BIG-IQ® and create a classification profile.

For the Access feature of BIG-IQ to display statistics and reporting for an application such as SharePoint, OWA, or Lotus Notes, the application's virtual server must have a classification profile attached.

1. In the Main tab, click **Local Traffic > Virtual Servers > Virtual Server**
List. A list of existing virtual servers displays.
2. Select the virtual server of the application that you want to map to the BIG-IQ system. The virtual server editing screen opens.
3. From the **Configuration** setting, select **Advanced**.
4. From the **Classification Profile** list, select the classification profile associated with the advanced configuration use case.
5. Click **Update**.

You have added a classification profile to the virtual server.

How much memory does application visibility need?

In the BIG-IP® system configuration for BIG-IQ® application tracking reporting, you do not need to allocate separate memory resources to enable the application visibility functionality. The runtime memory consumption depends on the amount of traffic processed, such as concurrent TCP flows.

Application visibility troubleshooting commands

Type these commands in the BIG-IP® UNIX shell to start and stop debugging and logging.

Command	Description
tmctl gpa_classification_stats	Displays classification results in a table that lists all applications that were classified, the number of flows, the bytes in, and the bytes out.
tmsh modify sys db tmm.cec.log.level value Debug	Generates debug logs. The log messages are stored in /var/log/tmm.
tmsh modify sys db tmm.gpa.log.level value Debug	
tmsh modify sys db tmm.cec.log.level reset-to-default	Stops debug log messages.
tmsh modify sys db tmm.gpa.log.level reset-to-default	