Configure IoT Application Monitoring

In addition to enabling and disabling **IoT Monitoring**, you can also configure the display names of network requests and exclude network requests matching given criteria from being monitored.

You can:

- Use the AppDynamics default naming rule, which you can leave as is or modify.
- Disable/modify the default naming configuration.
- Create custom include rules to override the default convention.
- Create custom exclude rules to exclude from monitoring network requests that meet certain criteria.

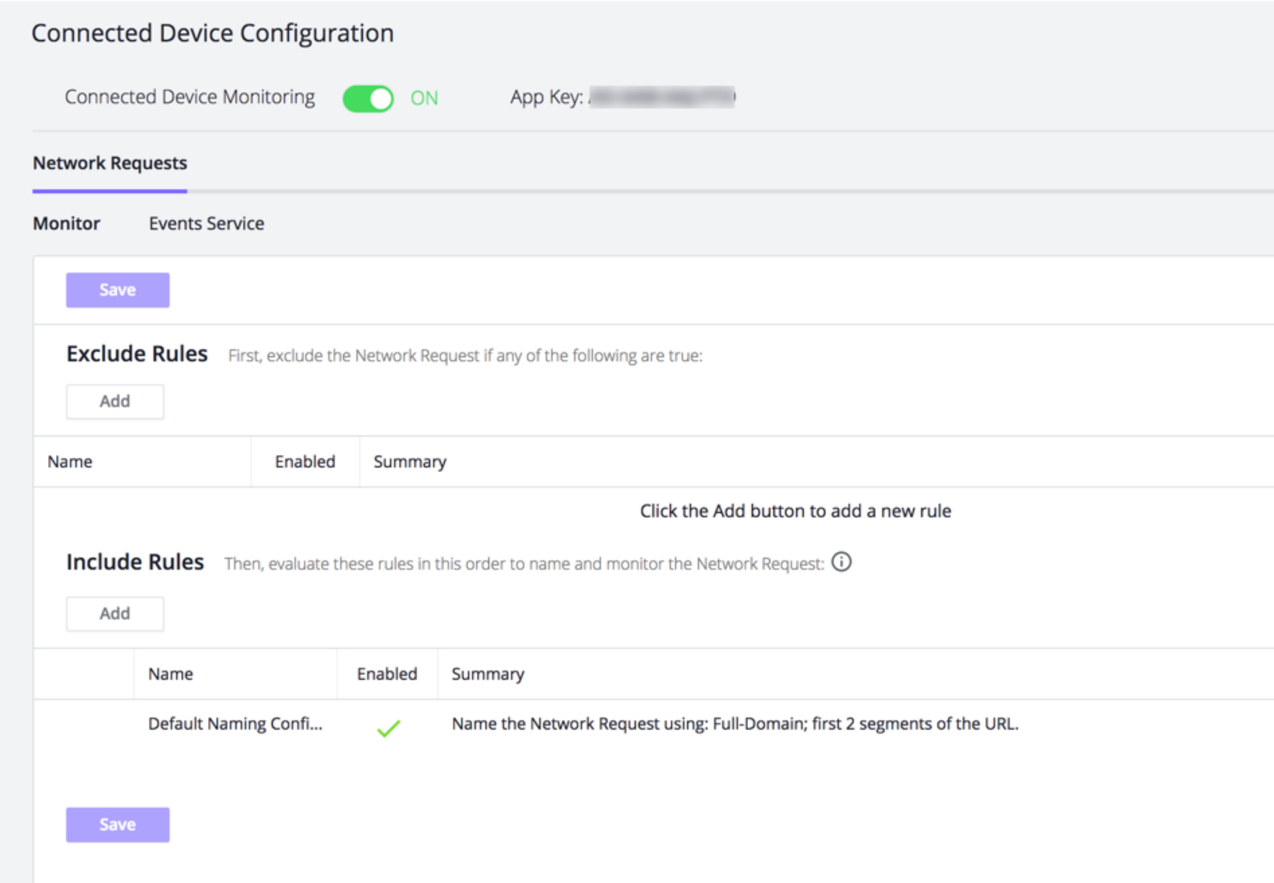
Access the IoT App Configuration

To access connected device configuration:

1. Open the IoT application in which you are interested.
2. From the left-hand navigation menu, click **Configuration**.

Enable/Disable IoT Monitoring

From the **Configuration** page, toggle the **Connected Device Monitoring** switch to **ON** to enable monitoring or **OFF** to disable monitoring.



Connected Device Configuration

Connected Device Monitoring ON App Key: [redacted]

Network Requests

Monitor Events Service

Exclude Rules First, exclude the Network Request if any of the following are true:

Name	Enabled	Summary

Click the Add button to add a new rule

Include Rules Then, evaluate these rules in this order to name and monitor the Network Request:

Name	Enabled	Summary
Default Naming Confi...	✓	Name the Network Request using: Full-Domain; first 2 segments of the URL.

Name IoT Network Requests

The following sections show you how to modify the default naming configuration for network requests and create include naming rules for network requests.

Access Network Requests Rules

From the **Configuration** page, click the **Monitor** tab if it's not selected already.

Default Network Request Naming Configuration

By default, AppDynamics names network requests using:

- the hostname
- the first two segments of the URL

For example, if an application makes this HTTP request: `http://myapp.com/friends/profiles/12345`

The default name that is displayed in the Controller UI for that request is: `myapp.com/friends/profiles`

If this is adequate for your needs, you can leave the default as is. The naming rules you configure here apply to all the IoT applications that are in the same IoT App Group.

Modify the Default Naming Configuration Rule

You may want to configure a different default rule for naming your network requests to help you visualize the parts of your application more clearly. The task is similar to configuring naming rules for business transactions on the server side. Try to group logically related requests together while keeping unrelated requests in separate groups.

- If the default hostname and first two segments of the URL for all your requests are identical, you might want to name the requests based on the last segments or a selection of non-contiguous segments of the URL to distinguish among requests in the network requests list.
- You can also name the requests based on query parameters. For example, if the request passes an order number, you could specify that the value of the `order-number` query parameter is used in the network request name.
- You can also base the name on a regular expression run on the URL. AppDynamics uses the Java libraries for regular expressions. For more information see:
  - Tutorial: http://download.oracle.com/javase/tutorial/essential/regex/index.html
  - Javadoc: http://download.oracle.com/javase/1.5.0/docs/api/java/util/regex/Pattern.html

Modifying the default network request naming rule

The default configuration covers how all your requests are named if you do not customize them further.

1. From the **Network Request** tab, scroll down to the **Include Rules** section.
2. Double-click **Default Naming Configuration**.
3. In the **Include Rule** dialog, select the elements you want to use for your default network request naming.
4. Click **OK.**
5. Click **Save.**

Create IoT Network Request Include Rules

By default, the same request naming rule is applied to every URL that your application requests. If you want to apply different naming rules to different URLs, create include rules.

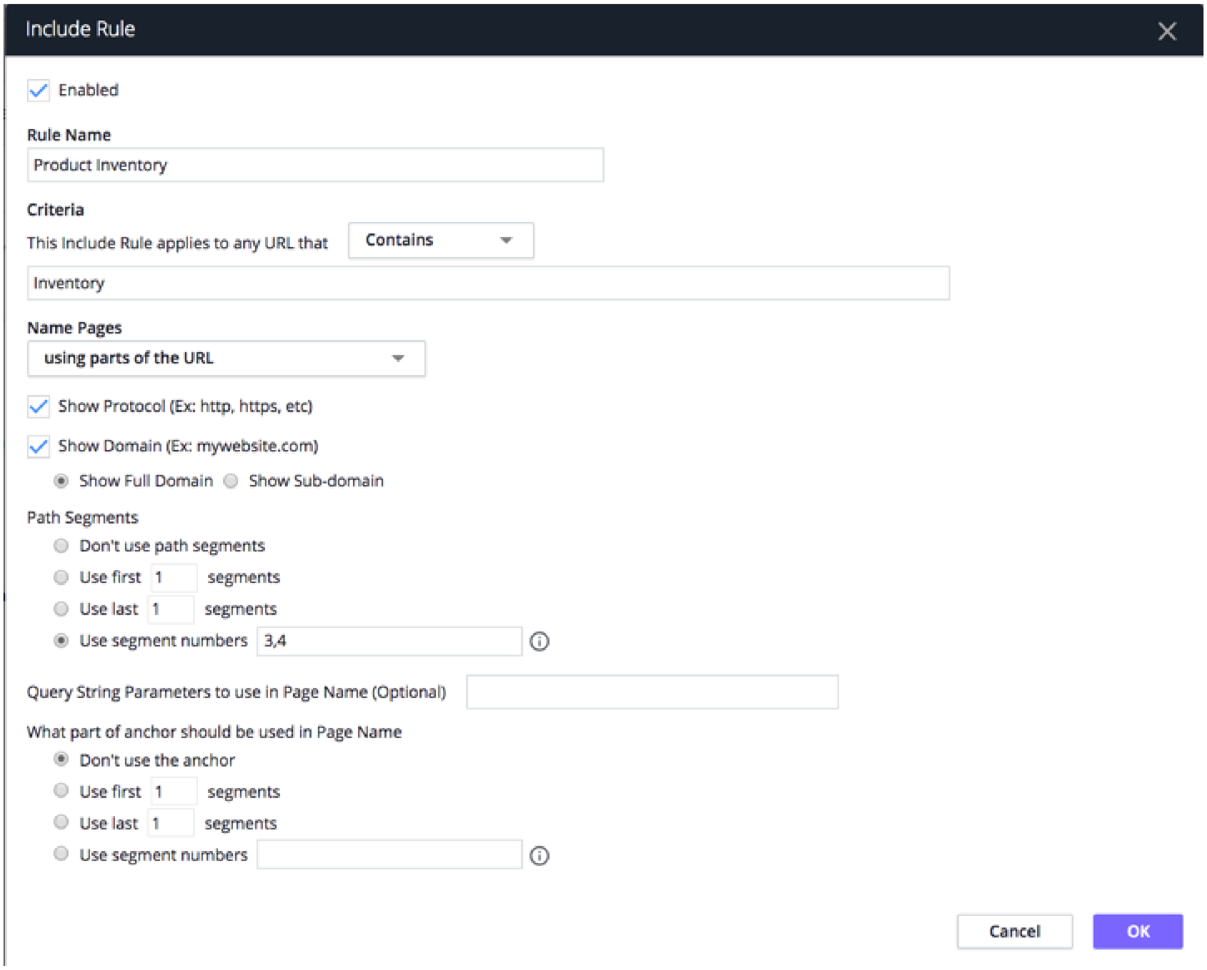
For example, if some requests call your own in-house server and others call out to a third-party API, you may want to see all the third-party API calls as one network request and use the default naming rules for the calls to your own server. You would create a custom naming rule that matches the third party calls and uses only the host in the default rule name or perhaps also include certain query parameters.

Creating an Include Rule

1. From the **Network Request** tab, scroll down to the **Include Rules** section.
2. Click **Add**.
3. In the **Include Rule** dialog, enter a name for the custom rule that you are creating.
4. Check the **Enabled** check box to enable the rule.
5. Select the check boxes and radio buttons and enter the match criteria for AppDynamics to use to name network requests.
6. Click **OK.**

Sample Include Rule

The following rule creates a custom match rule for requests in which the URL contains "inventory". This rule uses the protocol, the subdomain and the third and fourth segments of the URL in the network request name.



☑ Enabled

Rule Name

Product Inventory

Criteria

This Include Rule applies to any URL that Contains

Inventory

Name Pages

using parts of the URL

☑ Show Protocol (Ex: http, https, etc)

☑ Show Domain (Ex: mywebsite.com)

● Show Full Domain ○ Show Sub-domain

Path Segments

○ Don't use path segments
○ Use first 1 segments
○ Use last 1 segments
● Use segment numbers 3,4

Query String Parameters to use in Page Name (Optional)

What part of anchor should be used in Page Name

● Don't use the anchor
○ Use first 1 segments
○ Use last 1 segments
○ Use segment numbers

You can temporarily cancel the application of a custom naming rule by clearing the **Enabled** check box in the custom rule configuration. In this case, the default naming rule is applied to requests that would have been named by the disabled custom rule. To remove the rule permanently, select the custom rule in the **Custom Naming Rules** list and click the **Delete** icon.

Exclude IoT Network Requests

If there are certain types of requests that you do not want to monitor, create custom exclude rules for them based on the URL and/or the application name. Excluded network requests are not reported or counted toward the network request limit of 500 requests per controller application.

Creating an exclude rule

1. From the **Network Request** tab, scroll down to the **Exclude Rules** section.
2. Click **Add**.
3. In the **Exclude Rule** dialog, enter a name for the exclude rule that you are creating.
4. Check the **Enabled** check box to enable the rule.
5. Select the check boxes and radio buttons and enter the match criteria for AppDynamics to use to name network requests.
6. Click **OK.**

You can temporarily cancel the application of an exclude rule by clearing the **Enabled** check box in the exclude rule configuration. To remove the rule permanently, select the exclude rule in the **Exclude Rules** list and click the **Delete** icon.

Change Priority of Rules

Rules are evaluated in the order that they appear in the include or exclude list. You can change the priority of the rules by dragging and dropping rules towards the top (higher priority) or towards the bottom of the list (lower priority). Custom rules are always evaluated before the default naming rule, beginning with the custom rule that has the highest priority.

Your IoT app may make various kinds of network requests, and not all of them may be equally important to monitor in detail. For example, any requests to Google Analytics that your app may make are useful but probably aren't as important to analyze as the requests it makes to your backend.

To manage the impact on your overall Events Service usage, you can create rules which specify which of these network requests should be sent on to the Event Service, either by excluding a request entirely, including a particular request or a sample of that request types by percentage, or by simply allowing the request to be sent on.

In general, the behavior follows this pattern:

- If no rules are specified, data on all network requests are sent on.
- If exclude rules are specified, and a network request satisfies a rule, that data is *not* sent on.
- If include rules are specified, any network request that satisfies a rule is sent on, based on sampling defined by the percentage indicated in the rule.
- If both include and exclude rules are specified, a network request that satisfies an include rule but does *not* satisfy an exclude rule is sent on.