Managing API Keys

On this page:

Related pages:

- Roles and Permissions
- Analytics Events API

The Analytics Events REST API provides three independent endpoints for the following responsibilities:

- Schema Management
- Publish Events
- Query Events

API Keys provide a secure authentication mechanism for a caller to prove identity when using these public REST APIs.

Because call sites can vary across your infrastructure, departments, and geographic regions, these credentials could be widely distributed and hard to control. Publishing or querying events from different call sites therefore requires fine-grained control over the keys and the operations allowed for a particular key. You may also need to revoke these keys on demand if they are found to be compromised.

For these reasons, managing access for the Analytics Events API uses API keys. Your organization can create multiple API keys, manage and distribute them based on your own internal policies. For instance, each department or geographic region may be assigned their own API key for distribution and control management. If an API key is compromised, it can be deleted and a new key created without other undesirable side effects.

API keys are only valid for calling the public Analytics Events REST API and can't be used to access the AppDynamics Controller or data in any other way. For details on using the API keys, see the Analytics Events API documentation.

> ⓘ If you have deployed EUM such that you are using an on-premises Events Service for transaction and log analytics data, and the SaaS Events Service for your EUM data, you can not query the browser or mobile request data using the Analytics API. This setup is sometimes called "hybrid mode".

API Key Permissions

API keys are used only for Analytics Events REST APIs. When you create an API key, you can specify read and write permissions for each API key.

Operations allowed for a user with the Manage API permission:

- Add: Creates an API key
- Disable: Disables the calls using that key temporarily, but does not remove the key
- Enable: Re-enables a disabled key
- Delete: Removes the key permanently

> ⓘ It may take up to 15 minutes for a key which has been deleted or disabled to be detected and all operations using that key to be rejected.

When you create an API key, you see permissions for the various event types (logs, transactions, browser and mobile) in our platform. By using these permissions you can restrict or grant access to specific event types for each specific API key.

Examples

You can generate an API key for your partners enabling them to only publish custom events. Just check "Publish all Custom Events" checkbox when you create their API key.

You can generate an API key for to enable various users to only query Apache log data. Just check the "apache" source type under "Log Permissions.

Once an API Key is created, you cannot change the permissions. You can grant permissions for API Keys as follows:

Custom Analytics Events:

- Manage Schema: Enables creation of schemas using the Analytics Events Schema Management APIs
- Query Custom Events: Enables you to query all Analytics event types (with the appropriate permissions)
- Publish Custom Events: Enables you to publish Analytics custom events using the Analytics Events Publish APIs

Transactions: Grant permission to query all transactions or on an application by application basis.

Logs: Grant permission to query all logs or specific source types.

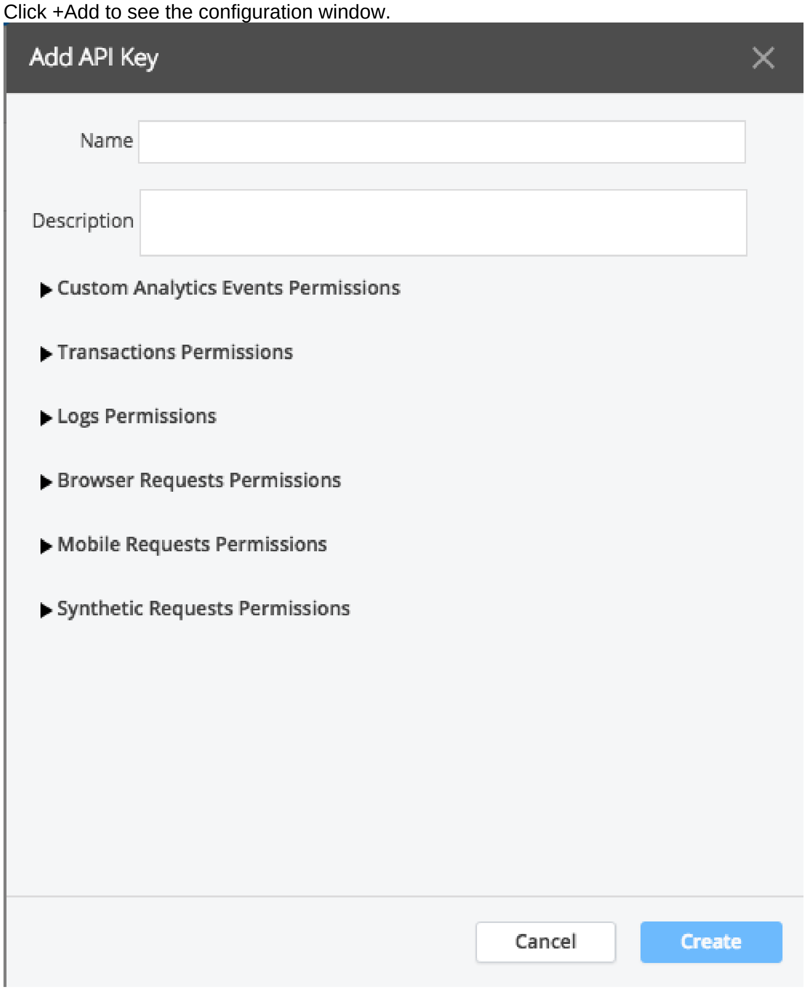
Browser Requests: Grant permission to query all browser requests or on an application by application basis.

Mobile Requests: Grant permission to query all mobile requests or on an application by application basis.

Synthetic Requests Permissions: Grant permission to query all synthetic requests or on an application by application basis.

Create API Keys

1. From the **Analytics > Configuration** window, select the API Keys tab.
   Here you can see a list of existing Keys and have access to actions for managing the Keys.
2. Click +Add to see the configuration window.



Add API Key

Name

Description

▶ Custom Analytics Events Permissions

▶ Transactions Permissions

▶ Logs Permissions

▶ Browser Requests Permissions

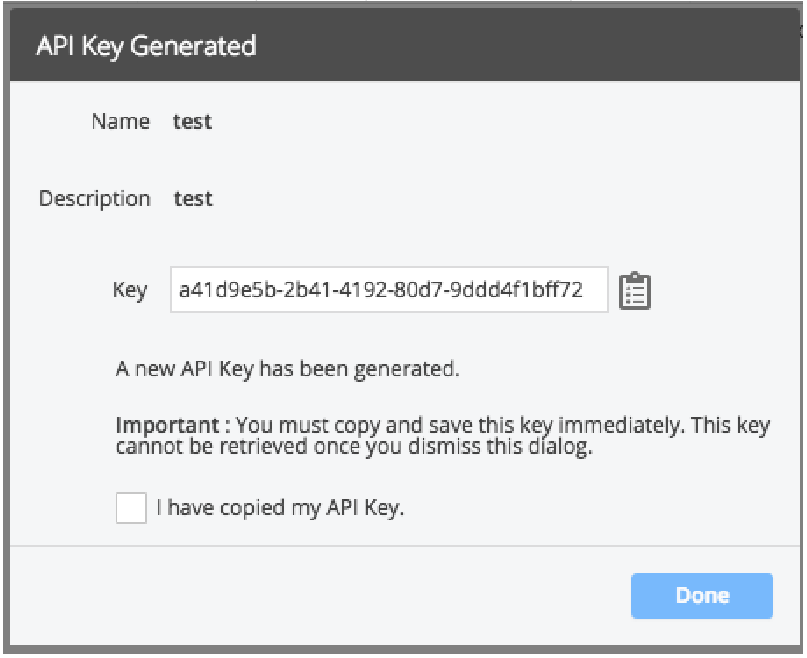
▶ Mobile Requests Permissions

▶ Synthetic Requests Permissions

3. Add a name and description and expand each permission section to select the permissions for this key.

Do NOT click Create until you have selected all the necessary permissions for your use case, including any necessary analytics data permissions, because you can not change the permissions once the key is created. Once the key is created, you can only edit the description and whether the key is enabled or disabled.

4. Click **Create**.
   You see a window containing the new key similar to the following:



API Key Generated

Name test

Description test

Key a41d9e5b-2b41-4192-80d7-9ddd4f1bff72

A new API Key has been generated.

Important : You must copy and save this key immediately. This key cannot be retrieved once you dismiss this dialog.

□ I have copied my API Key.

5. Copy and save the key. Check the check box indicating you have copied the key and click done. You cannot retrieve the key once you dismiss this dialog.