Module 5 – Administration

This toolkit is designed for Expert Business Practitioner Exam Aspirants. There are five Modules. Study Each module per week to stick to schedule. Technical Parts of applications are depicted in Videos, you can learn more about them from experience League. You can visit Get prep page to understand the contents and anticipate the learning journey.

This is Expert Exam, Business Practitioner toolkit final Module (5). This module contains three sections.

1. Analytics Admin Guide
2. Frequently asked questions (Data Governance)
3. Classification Rule Builder workflow

Section 5.1 Analytics Admin Guide

This help is intended for administrators of Adobe Analytics. It includes help on user and product management in the Admin Console, setting up report suites, variables, classifications, and data collection.

Adobe Analytics currently has two areas for administrators:

- Adobe Admin Console: Use this area for provisioning Experience Cloud tools, and managing user permissions. It is located at adminconsole.adobe.com.
- Analytics Admin Tools: Use this area for report suite and variable management. It can be accessed by clicking Admin in the top header of Adobe Analytics.

This guide covers:

- All tasks that are done in Analytics Admin Tools. This area includes setting up report suites, variables, classifications, or data governance. See Admin Tools for a list of report suite and company settings available.
- All Analytics-specific tasks that are done in the Adobe Admin Console. This area includes product provisioning and user permission management. See Adobe Analytics in the Adobe Admin Console for a list of actions that can be done in the Adobe Admin Console.

This guide does not cover many of the generic capabilities that the Adobe Admin Console offers. Instead, see Admin Console in the Enterprise user guide.

Adobe admin console

Use the Adobe Admin Console to manage Analytics products and users. Adobe Admin Console is located at adminconsole.adobe.com.

This chapter explains concepts you need to understand about Analytics-specific product profiles and permissions in the Adobe Admin Console.

- Permissions
  - Product profiles for Adobe Analytics
  - Product profile permissions for Report Suite Tools

- Product profile permissions for Analytics Tools

Add an administrator in Adobe Analytics

View the following video demonstration to learn how to add an administrator in Adobe Analytics: Add an administrator in Adobe Analytics

Adobe Analytics first admin guide

Before any users can be assigned roles in Adobe Analytics, a user must be assigned as a first admin in Experience Cloud. The first admin can then provision users in the organization with other key roles.

A first admin is the starting point in enabling the rest of the organization to use each Experience Cloud solution, including Adobe Analytics.

Provisioning process for a first admin

After a contract is signed:

1. The provisioning team at Adobe prepares for the account to be created.
2. The first admin receives an email with login credentials before the contract's start date.

IMPORTANT: Ensuring the first admin's contact info is given to Adobe and accurate before the contract is signed is highly recommended.

Next steps

After a first admin is provisioned for your organization, the first admin can then provision users in the organization with other key roles.

For information about how to provision users in your organization with key roles for Adobe Analytics, see Admin roles in Adobe Analytics.

Administrator roles in Adobe Analytics

Adobe Analytics supports various types of administrators. Full Adobe Analytics admins have access to everything in Adobe Analytics, while other admins and users can perform more specialized tasks.

NOTE: Before any users can be assigned roles in Adobe Analytics, a user must be assigned as a first admin in Experience Cloud. The first admin can then provision users in the organization with other key roles, as described in this article. For more information about the first admin, see Adobe Analytics first admin guide.

Key roles in Experience Cloud and Adobe Analytics

Consider the following key roles when using Adobe Analytics:

- **Full Adobe Analytics admins:** These users have full access to everything in Adobe Analytics, including report suite settings and user permissions. Depending on how your organization is

structured, different people or teams can be responsible for different facets of Analytics administration. For example, one person is responsible for the designation of what variables to use in an implementation. Another person can be responsible for enabling users to correctly pull reports by ensuring everyone has the correct permissions. Identify at least one user who can be responsible for Analytics report suite settings and user permissions, and they can invite other Analytics admins from there.

- **Data Collection admins:** These users have full access to everything in Adobe Experience Platform Data Collection, including publishing permissions, creating containers, and user permissions. These users are not necessarily programmers, but having at least a beginner's knowledge of HTML, CSS, and JavaScript is beneficial. They are responsible for working with your organization's website owners to get tags implemented on your site. Identify at least one user who is responsible for your organization's implementation, and they can invite other data collection admins from there.
- **Product Profile admins:** These users can add or remove users to a product profile, adjust permissions items in their product profile, and assign or remove product profiles to user groups. Product Profile admins do not have full access to Adobe Analytics. However, they are ideal for team leads or managers who need to grant and manage access to Adobe Analytics for their team. For more information about product profiles, see Product profiles for Adobe Analytics.
- **Support delegates**: Also known as supported users, they have no additional privileges in the Analytics interface. Instead, they receive additional privileges when communicating with Adobe Customer Care. These users are almost always Analytics admins as well, as it helps Customer Care troubleshoot issues with them. Identify at least one Analytics admin who is responsible for facilitating interactions between end users and Adobe Customer Care.
- **Website owners:** These individuals or teams are responsible for the coding and development of your website. They do not require accounts, but they want to work with data collection admins to get the tag code and implement it on your website.
- **End users:** these users typically view reports and seek answers to business questions. Analytics admins grant these users permissions to work in the product.

Grant full product admin access for Analytics

System-level admins do not have direct access to products; however, they can give themselves access by adding themselves as a product-level admin.

To give Adobe Analytics access to yourself or to others:

1. Log in to the Admin Console with your Adobe ID credentials.
2. Click the **Products** tab at the top. All products purchased by your organization are on the left. Click **Adobe Analytics**, then click the **New Profile** button.
3. Name this profile 'Analytics full admin access', then click **Next** > **Save**.
4. Back on the Product Profiles page, click the newly created profile, then click the **Permissions** tab.
5. Click one of the permission line items. If **Auto-include** is available, enable it. If **Auto-include** is not available, click **Add all**. Both options move all permission items to the right column.
6. Click **Save**.
   Repeat the above step for all permission categories.
7. After all permission categories are granted to the profile, go back to the Products page by clicking **Product** at the top.
8. Under the Adobe Analytics tile, click **Assign Users**.
9. Enter the email address you would like to give full Analytics access to, and assign them the newly created full admin access profile. Click **Save**.

The user now has full access to Adobe Analytics.

Grant product admin access for Data Collection in Experience Platform

Product admin access for Data Collection in Experience Platform is nearly identical to granting product admin access for Analytics.

1. Log in to the Adobe Admin Console with your Adobe ID credentials.
2. Click the **Products** tab at the top. All products purchased by your organization are on the left. Click **Experience Platform Launch**, then click **New Profile**.
3. Name this profile 'Data Collection full admin access', then click **Done**.
4. Back on the **Product Profiles** page, click the newly created profile, then click the **Permissions** tab.
5. Click one of the permission line items. If **Auto-include** is available, enable it. If auto-include is not available, click **Add all**. Both options move all permission items to the right column.
6. Click **Save**. Repeat the above step for all permission categories.
7. Once all permission categories are granted to the profile, go back to the Overview page by clicking **Overview** at the top.
8. Under the Experience Platform Launch tile, click **Assign Users**.
9. Enter the email address you would like to give full Analytics access to, and assign them the newly created full admin access profile. Click **Save**.
10. The user now has full access to Experience Platform Data Collection.

Grant product admin access for Product Profiles

For information about assigning users as product profile admins, see the "Manage product profile admins" section in the article, Manage product profiles for enterprise users in the Enterprise user guide.

Next steps

Create a Report Suite: Have your Analytics admin log in to the tool and create a report suite for data collection

Create an Analytics tag property: Have your Data Collection admin log in to the tool and create a property to implement on your site

Before any users can be assigned roles in Adobe Analytics, a user must be assigned as a first admin in Experience Cloud. The first admin can then provision users in the organization with other key roles, as described in this article. A first admin is the starting point in enabling the rest of the organization to use each Experience Cloud solution.

After a contract is signed

1. The provisioning team at Adobe prepares for the account to be created.
2. The first admin receives an email with login credentials before the contract's start date.

IMPORTANT

Ensuring the first admin's contact info is given to Adobe and accurate before the contract is signed is highly recommended.

Additional Resources:

- Analytics tools permissions summary
    - Analytics permissions in Admin Console
    - Product profiles for Adobe Analytics
    - Product profile permissions for Report Suite Tools
    - Product profile permissions for Analytics Tools
- **Analytics admin tools**
    - Admin tools overview
    - Code Manager
    - Data Sources
    - Exclude by IP address
    - Logs
    - Reporting Activity Manager
    - Report Suite manager
        - Edit settings of a report suite
            - General
                - General Account settings
                - Internal URL Filters
                - Customize Calendar
                - Paid Search Detection
                    - Paid search detection overview
                    - Configure paid search detection
                - Customize Menus
                - Processing Rules
                    - Processing rules overview
                    - Processing Rules
                        - How processing rules work
                        - Create processing rules
                        - View active processing rules
                        - View processing rule history
                        - Restore processing rules
                        - Copy processing rules to another report suite
                        - Dimensions available to processing rules
                    - Processing rules examples
                        - Examples of processing rules
                        - Populate a campaign ID from a query string parameter
                        - Set the product view event from the product overview page
                        - Add a subcategory by concatenating the category and page name
                        - Determine a path by copying an eVar value to a prop
                        - Clean up values in a report
                        - Populate internal search terms using a query string parameter
                        - Copy a context data variable to an eVar

Section 5.2: Frequently asked questions (Data governance)

How does Adobe Analytics support access and delete requests for end users (Data Subjects) validated by customers (Data Controllers)?

When various Data Privacy rules (GDPR, CCPA) take effect, Adobe Analytics will support processing verified requests submitted by Data Controllers to the Experience Cloud Data Privacy API to enable a more automated process. Adobe's Data Privacy API is designed to help process individual rights requests (e.g., access and delete requests) for our customers' data stored across Adobe Experience Cloud solutions. It is flexible and scales according to the number of data access and delete requests your company receives from Data Subjects.

Also, the Privacy Service API allows the customer to check the status on how the data access and delete requests that are being fulfilled. For more details see Privacy Service API documentation.

Who is responsible for receiving, accepting, and fulfilling Data Privacy requests from end users?

The Data Controller has the sole responsibility for receiving and accepting requests. The Data Controller validates the Data Subject's identity and then fulfills the request. Part of this responsibility may involve contacting Adobe with Data Subjects' IDs that may be associated with data stored in Adobe Analytics. As the Data Processor, Adobe must provide reasonable assistance to the Controller to process verified requests within an acceptable amount of time.

How will Adobe Customers (Data Controllers) find out which Data Privacy requests map to which IDs in Adobe Analytics for Data Privacy processing?

The Data Controllers determine how to resolve identity for requests from the Data Subjects. Consider deploying Adobe's Data Privacy ID Retrieval Tag. Your development teams save time by using our Data Privacy ID retrieval tag to capture user IDs (cookie IDs). They can then use our Data Privacy API to send those user IDs to the relevant solutions in the Adobe Experience Cloud for Data Privacy request processing. The Data Privacy API can support a broad range of customer IDs across multiple Adobe solutions.

If a Data Subject submits a request along with an identifier (custom variable - prop or eVar), then Adobe Analytics scans then entire retained history of the data collected for the given identifier. For more details about how to configure custom IDs stored in Analytics props or eVars, please refer to the Analytics documentation on namespaces.

How can Adobe Analytics Data Governance assist with processing Data Privacy requests?

Data Governance is a new tool within Adobe Analytics that provides Data Controllers the ability to apply data controls and classifications across their Analytics data. This new tool empowers Adobe customers to customize the processing of their Data Privacy data access and data delete requests. In the Data Governance console, admins can define the desired settings that should be applied to various data columns that reside in Adobe Analytics. Once those labels are defined, Adobe will honor and process any downstream access or delete requests according to the customers' desired label settings. It is the responsibility of the Data Controller to review and council with their legal representatives regarding these label settings.

The Data Governance tool contains the following data labels:

- **Identity Data Labels**: Used to classify data that can identify an individual either directly or in combination with other data. (None, I1, I2)
- **Sensitive Data Labels**: Used to classify data as data that may be defined as sensitive under applicable law. (None, S1, S2) Note that currently the use of Sensitive Data in Adobe Analytics is generally prohibited except for precise geo-location data properly obtained under applicable law, which may be considered Sensitive Data in some jurisdictions.
- **Data Privacy Data Labels**: Used to define the fields that may contain personal identifiers for use in Data Privacy requests or that should be removed as part of a Data Privacy delete request. These labels may overlap the Identity and Sensitive Data labels, in some cases.

For more information on Data Governance labels, see Data Privacy Labels for Analytics Variables.

How can I validate that the Privacy Service requests are working properly to delete data from Adobe Analytics?

Typically, Analytics customers set up some test report suites to verify functionality before it is released to the general public. Pre-production websites or apps send data into these test/dev/QA report suites to evaluate how things will work when the code releases before real traffic is sent to the production report suites.

However, with a normal configuration, GPDR request processing cannot be tested first on these test report suites, before applying requests to production report suites. This is because a Data Privacy request is automatically applied to all report suites in the Experience Cloud organization, which is often all report suites for your company.

Still, there are a few ways that you can test your Data Privacy processing prior to applying it to all your report suites:

- One option is to set up a separate Experience Cloud organization that contains only test report suites. Then use this Experience Cloud organization for your Data Privacy testing and your normal Experience Cloud organization for actual Data Privacy processing.
- Another option is to assign different namespaces to the IDs in your test report suites, versus those in your production report suites. For example, you can prefix each namespace with "qa-" in your test report suites. When you submit Data Privacy requests with only namespaces with the qa prefix, these requests will only run against your test report suites. Later, when you submit requests without the qa prefix, they will apply to your production report suites. **This is the recommended approach, unless you use the visitorId, AAID, ECID or customVisitorId namespaces. These namespaces are hardcoded and you cannot specify alternate names for them in your test report suites.**

Where do I get started on getting Data Privacy ready with Adobe Analytics?

For a step-by-step walkthrough to get ready for Data Privacy rules, see Adobe Analytics Data Privacy Workflow.

How should Data Controllers think about consent when it comes to user engagement?

GDPR and CCPA are good opportunities to re-consider your consent management strategy and practices. This includes determining when consent is needed and thinking about the value proposition for the user. Consider the value proposition for consumer privacy, which can help drive conversion and loyalty. The consent management space (e.g., tools, standards, best practices) is rapidly evolving, and is an area to watch. To minimize impact on user engagement, Controllers should work with vendors in this space as well as with their legal counsel, to ensure that they are following emerging laws and guidance on consent and cookies. Thinking about "experiential privacy" by using an on-brand, contextually relevant experience that sets out the value proposition of your data collection activities is a good strategy. You, as the Data Controller, are responsible for obtaining explicit consent from your Data Subjects before you collect data about them (possibly including Adobe Analytics data) and for implementing an opt-out mechanism on your web site. This lets your Data Subjects opt out of future Adobe Experience Cloud data collection.

How should Data Controllers think about data retention when it comes to Data Privacy?

Personal data generally should not be retained for longer than necessary to achieve the purpose for which it was collected. Adobe's General Terms apply a default 25-month data retention plan, unless a different data retention term is contractually agreed upon. Customers are required to set their data retention policy before Adobe can process a Data Privacy request. Each report suite's current data retention policy is displayed in the new Data Governance Admin UI. Customers should contact their Adobe representative if they need to adjust their data retention policy. Please refer to Adobe Analytics Data Retention FAQs.

Can a customer reduce or extend the default data retention period?

Customers can request that their data be deleted sooner than 25 months by calling Customer Care. Customers can also extend data retention beyond 25 months by purchasing an extension. Extensions are available in increments of 1 additional year, up to a maximum of 8 additional years (10 years total). These extensions will require updated contract terms and additional fees.

What privacy considerations should a Data Controller account for when personal data is exported from Adobe Analytics?

If a customer uses Adobe Analytics Data Feeds to export data from Analytics into their enterprise data warehouse or into other systems outside of Adobe, it is the responsibility of the Customer (the Data Controller) to ensure that delete requests are applied to the data. This also applies to on-premise implementations of Adobe Data Workbench, where an ongoing Adobe Analytics data feed is populating the Data Workbench data. Adobe may provide tools to assist in finding and deleting the records from certain types of data feeds, including those used for Data Workbench, but it is still the Customer's (Data Controller) responsibility to ensure that the data is deleted consistent with their own, internal data retention and deletion policies. Please also consider cases where employees have downloaded Adobe Analytics reports that contain personal data. These reports may need to be updated or deleted if a Data Privacy-related delete request is received involving an ID that is present in the report. Customers should work with their own company's legal counsel to determine retention periods, and privacy and security requirements that should be applied to these types of documents.

Some data we were not supposed to collect was accidentally sent into Adobe Analytics. Can we use the Data Privacy API to clean up this data?

The Data Privacy Service API has been provided to help you fulfill Data Privacy requests, which are time sensitive. Using this API for other purposes is not supported by Adobe and may impact Adobe's ability to provide timely turn-around of high priority, user-initiated Data Privacy requests for other Adobe customers. We ask that you do not use the Data Privacy API for other purposes such as clearing out data that was accidentally submitted across large groups of visitors. You should also be aware that any visitor who has a hit deleted (updated or anonymized) as a result of a Data Privacy deletion request will have their state information reset. The next time the visitor returns to your website, they will be a new visitor. All eVar attribution will start again, as will information such as visit numbers, referrers, first page visited, etc. This side effect is undesirable for situations where you want to clear out data fields, and highlights one reason why the Data Privacy API is inappropriate for this use. Please contact your Adobe Account Team to coordinate with our Engineering Architect consulting team to further review & provide level of effort to remove any PII or data issues.

Our legal team has determined that values we have been collecting in a variable for years no longer comply with our updated privacy policy. Can we use the Data Privacy API to clear out all values from this variable?

The Data Privacy Service API has been provided to help you fulfill Data Privacy requests, which are time sensitive. Using this API for other purposes is not supported by Adobe and may impact Adobe's ability to provide timely turn-around of high priority, user-initiated Data Privacy requests for other Adobe customers. We ask that you do not use the Data Privacy API for other purposes such as clearing out data that was accidentally submitted across large groups of visitors. You should also be aware that any visitor who has a hit deleted (updated or anonymized) as a result of a Data Privacy deletion request will have their state information reset. The next time the visitor returns to your website, they will be a new visitor. All eVar attribution will start again, as will information such as visit numbers, referrers, first page visited, etc. This side effect is undesirable for situations where you want to clear out data fields and highlights one reason why the Data Privacy API is inappropriate for this use. Please contact your Adobe Account Team to coordinate with our Engineering Architect consulting team to further review and provide level of effort to remove any PII or data issues.

Additional Data Privacy Resources:

- GDPR Common Terms
- Experience Cloud Data Privacy Care Package
- Experiential Privacy Blog Post

SECTION 5.3 Classification Rule Builder workflow

Rather than maintaining and uploading classifications each time your tracking codes change, you can create automatic, rule-based classifications and apply them across multiple report suites. Rules are processed at frequent intervals, depending on your volume of classification related traffic.

Important Notice before you get started

Keep this in mind before you start using classification rules:

- Sub-classifications are not supported with Classification Rule Builder (CRB).
- Our current classification system can only export up to 10 million rows at a time.

Step	Where Performed	Description
Step 1 (Prerequisite): Set up your classification schema.	Admin > Report Suites > Edit Settings > <Traffic Classifications or Conversion Classifications>	Choose a variable and define the classifications to use for that variable. Variables must have at least one classification column created before they are available for use in rules. Once classifications are enabled, you can use the importer and the rule builder to classify specific values.
Step 2: Create a rule set.	Admin > Classification Rule Builder > Add Rule Set	A rule set is a group of classification rules for a specific variable.
Step 3: Configure report suites and variables.	Classification Rule Builder > <your rule set>	Apply the rule set to report suites and variables.
Step 4: Add classification rules to the set.	Classification Rule Builder > <your rule set>	Match a condition to a classification, and then specifying the action to take for the rule. Be familiar with the information in How Rules Are Processed.
Step 5: Test a Classification Rule Set	Testing Page	You will want to test rules for validation by editing them in Draft mode. In Draft mode, rules cannot run. This step is important when using regular expressions.

Step	Where Performed	Description
Step 6: Activate valid rules.	Rules Page	Once rules are valid, activate the rule set. You can overwrite existing keys, if necessary. See How Rules Are Processed.
Step 7 (Optional): Delete unwanted rules.	Rules Page	Delete unwanted rules from a set. Note: Deleting rules does not delete classified data uploaded. See Delete classification data if you need to delete classified data.

- When CRB requests an export, it pulls both classified AND unclassified values, with unclassified values coming through at the end of the export. This means that, over time, you could fill up 10 million classified values - without ever getting to the unclassified values.
- Because the architecture is set up in a way that CRB could be pulling from "n" number of servers, this can lead to inconsistencies as to which servers get picked up and in what order. For that reason, it is very difficult to get to unclassified values.

This is the **workaround** for those who have more than 10 million classified values for a dimension: You will need to export unclassified values via FTP, in 10-million batches, and manually classify them.

Getting Started with Classification Rules

Admin > Classification Rule Builder

Here are the high-level steps you take to implement classification rules:

NOTE: Groups with permissions to use the classification import tool can use classification rules. See How Rules Are Processed for important processing information.

Additional Resources

Blog: For additional information about this feature, see the Digital Marketing Blog: Rule-based Classifications.

Video: View the Classifications Overview video.

Additional Important Resources:

- Classification sets
  - Classification sets overview
  - Manage classification sets
    - Classification set manager
    - Create a classification set
    - Classification set settings