

Insights Censorship & Privacy Settings

Brief Overview

WalkMe has created a security mechanism that allows you to prevent the collection of your users' sensitive information.

The censorship and privacy settings in Insights allow you to disable the collection of properties that might contain Personal Identifiable Information (PII) and prevent the collection of end-users' sensitive information on certain elements.

The censorship mechanism is performed entirely on the client side, meaning the censored information never even reaches the WalkMe servers.

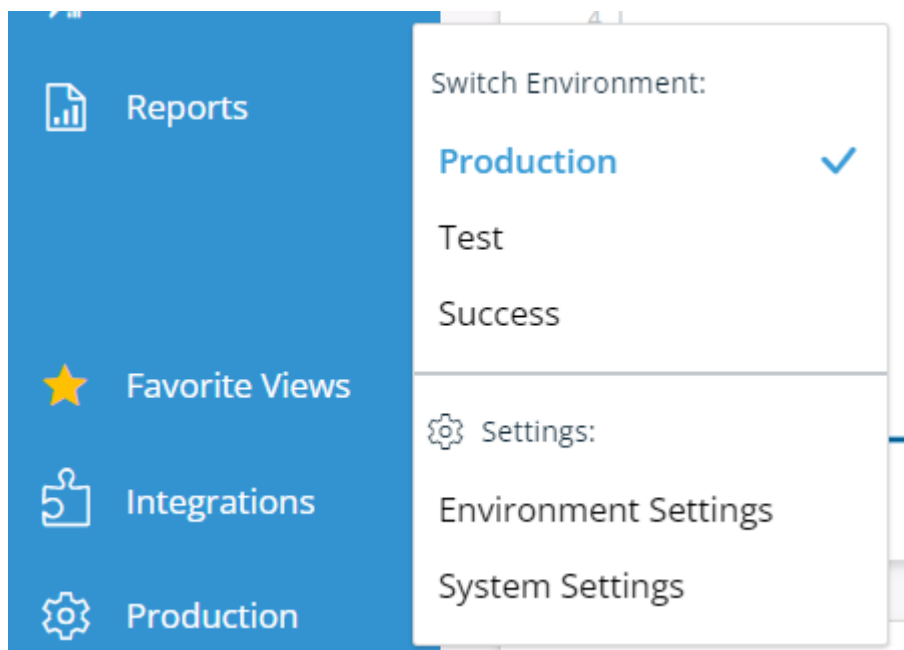
If you need an Insights refresher, please refer to the following article: [Insights: Getting Started Guide](#)

How It Works


Access censorship & privacy settings

To access your settings, please follow these steps:

1. Log into [Insights](#) at insights.walkme.com
2. Go to the system you want to access
3. Click on the environment name and click on **Environment Settings**



4. **Censorship & Privacy** will be the first tab:


SYSTEMS OVERVIEW
ACTIVITY BOARD
ADOPTION PROJECTS
ALL SYSTEMS REPORTS

Overview

Apps

Users

Behavior Based Segmentation

Sessions

Funnels

Tracked Events

Reports

Favorite Views

Integrations

Production

Production Environment Settings

Censorship & Privacy

Collection Enablement

Session Playback

Censorship and Privacy Settings

Censor elements by ID
All elements with the following IDs will be censored on the client side before collection

Censor elements by class
All elements with the following classes will be censored on the client side before collection

*Alternatively, add the class **.wm-hide** to any element, to censor it on the client side before collection

Censor event properties ⓘ
Selected event properties will be censored on the client side before collection

PII fields
Enable or disable the collection of values of data-fields that might contain Personal Identifiable Information (PII)

☒ **Page URL**
Session Playback events will still collect the URL domain and path, while the query and hash parts will be censored

☒ **Page title**

Page view collection
Enable or disable the collection of new page loads

☒ **Collect page view**

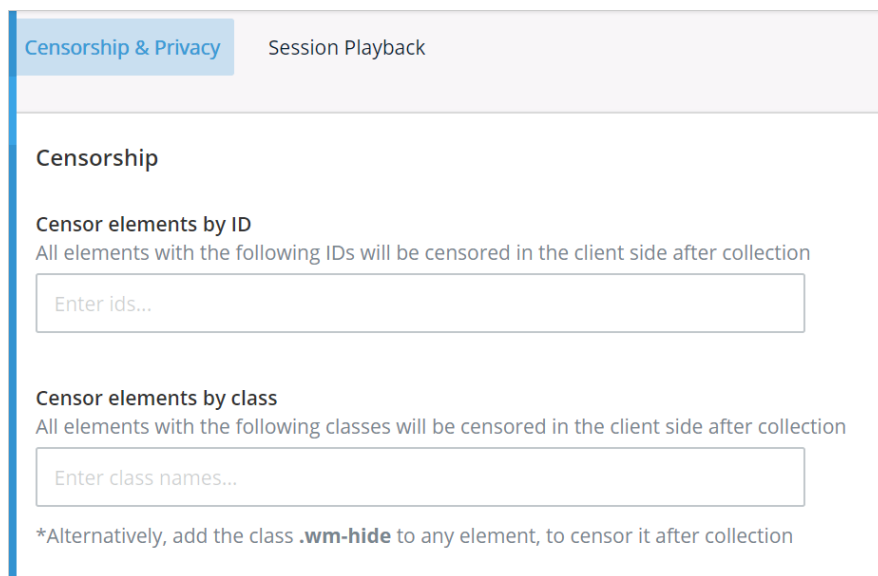
⚠ Notice: For settings to apply, enable the suitable recording mode (e.g. Session Playback) in the Editor and publish settings to Production.

Censor HTML Elements By ID or Class

Insights offers you the ability to not collect sensitive elements containing specific ID and class attributes.

To do so, enter the ID or class attribute names you would like to censor in the **Censor elements by ID** or **Censor elements by class** fields. You can add periods inside of the ID and class names if needed.

You may also choose to add the class “wm-hide” to any element on your website to censor that element.



Censorship & Privacy Session Playback

Censorship

Censor elements by ID
All elements with the following IDs will be censored in the client side after collection

Enter ids...

Censor elements by class
All elements with the following classes will be censored in the client side after collection

Enter class names...

*Alternatively, add the class **.wm-hide** to any element, to censor it after collection

Note

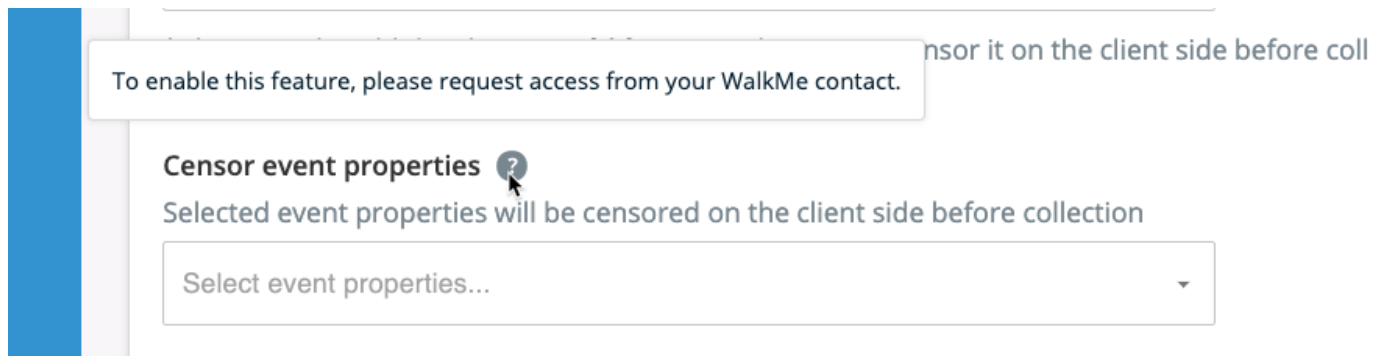
- This censorship is only relevant and available for accounts with [Digital Experience Analytics \(DXA\)](#) or [Session Playback](#) enabled
- There is no limit to the number of elements that you can censor

Censor event properties

If needed, event properties can also be censored. Please reach out to your Customer Success Manager or WalkMe contact to request access.

List of available event properties:

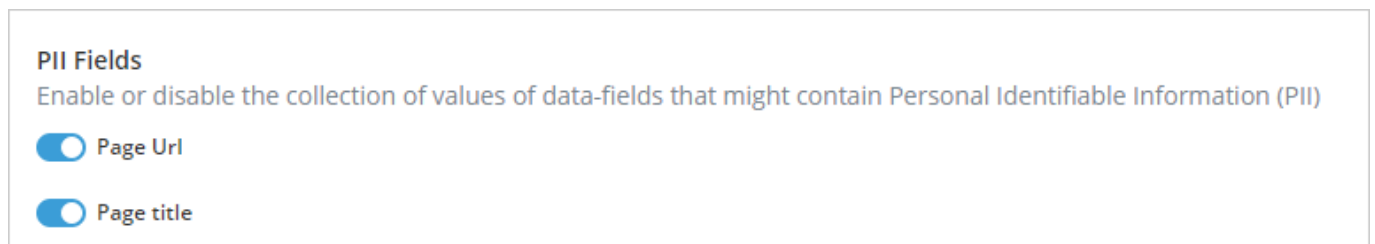
- Browser Name
- Browser Version
- Is Mobile Device
- OS Name
- OS Version
- Screen Height
- Screen Width
- Timezone
- URL Pathname (keeping all other URL parts like # ? and Domain)



PII fields

There are two fields that WalkMe collects that may contain Personally Identifiable Information (PII):

1. **Page URL:** The URL where the event occurred
2. **Page title:** The title of the page where the event occurred



Turning off collection for either of these fields means that collection of the field will be disabled in all events sent to Insights. This may affect some reports that rely on this information.

Note

- Disabling the collection of both page URL and page title will automatically disable page view collection
- Disabling page URL and page title collection will not affect existing Tracked Events based on

page views, however, disabling Page URL collection will affect Tracked Events that have an event scope, meaning a URL property is included in the Tracked Event's definition

Page view collection

Page views are collected for users by default in Insights. To opt-out of the collection of Page views can do so in the Environment Settings.

1. Go to the Page View Collection
2. Turn off the **Collect page view** toggle
3. Click **Save Settings**

Page View Collection

Enable or disable the collection of new page loads

 **Collect page view**

Note

The collection of page views is automatically disabled for customers who have turned off the collection of **Page URLs** and **Page Titles** in the Censorship & Privacy PII Settings.

Publish settings

After setting up your environment settings, make sure to the do the following for changes to take affect:

1. Click **Save Settings**
2. Perform a settings publish in the Editor



Tip

Please refer to the following article for more information: [How to Publish Global Settings](#)

Technical Information

Understanding element censorship

On accounts with DXA enabled, WalkMe collects the following fields by default:

- Name attribute
- Title attribute
- Element text
- Element value
- Element label

If you are concerned that any of these fields may contain sensitive user information, please censor the element(s) you are concerned about.

Note

- If an element is censored, the above fields will not be sent, but events will still be collected
 - For example, a click on a censored button that contains the user's email will still be sent as a click with the element classes and ID, but the email text will not be included in the collected event
- If Session Playback is enabled the censored element will be blocked

Understanding password field censorship

Insights will **never** collect keystroke data inside password fields, meaning inputs with type="password". This is by design and there is no way to change this behavior.

No retroactive censorship

It is important to be aware that after applying any of the settings in this section, your chosen censorship settings will only apply to **subsequently** recorded sessions.

If you discover that you have recorded sensitive information prior to activating your desired settings, please contact [WalkMe Support](#) to help you resolve this issue.