ABBYY

ABBYY® Timeline 6.0

Recording Service User's Guide

Table of Contents

About This Document

This Recording Service User's Guide is intended for managers who manages the process of data preparing and then send them to Timeline. It is intended to provide advice on collecting and preparing data related to users' desktop activity as well as tips on configuring Recording Service features.

Workflow Guideline

The guidelines below will help you to get acquainted with the working process. For additional information about the steps, follow the links in the descriptions.

Important. Role required: Recording Service user.
If your account is not added to the **Admin AD Security group** specified during the Recording Service installation, you will not have access to the Recording Service website.

1. Make sure the Timeline connection settings are set:

    a. Go to **Settings** > **Timeline Authentication** and check if the fields are filled and the Save button is disabled.
        Note. Authentication settings are set by the system administrator after the Recording Service installation. Most likely, you do not have access to edit these settings.

2. Go to **Settings** > **Logs** and review the default settings for additional options related to personifying recorded logs and blurring sensitive information in text logs and screenshots.
    Important. These settings are available only to admins of the Recording Service.
    For details, see Settings > Logs 30.

3. Make sure all installed Recorders appear in the **Recorders** section, and their status is **online**.
    If a recorder instance does not appear in the list, contact your administrator to resolve this issue.

4. Go to **Templates** and review the parameters in the default template.
    Use **Templates** to specify what data needs to be logged and how it is to be processed. Here you can schedule recording sessions of user activity, enable advanced logging if you plan to export processes from Timeline for further import and refinement in Blue Prism applications, or allow Recording Service to log user activities in one log, in case a user works on multiple computers.
    For details, see Configuring and Applying Templates 9.

    a. **Setup Included and Excluded lists**
        It is a very powerful feature that allows defining fine-grain control over what applications should be monitored and logged and which ones should be excluded completely. To utilize this filtering mechanism to eliminate unwanted events from your logs, you can set up lists of included and excluded applications for logging.

Using **Included** and **Excluded** lists can significantly reduce the amount of unwanted data in the project and make analyzing tasks and processes easier. This becomes very important when dealing with large datasets that include important events which may be surrounded by third-party actions. As a result, the important ones are made harder to isolate and analyze by multiple case and path deviations complicated by unnecessary data.

Before recording logs, application lists can be configured using the template on the Recording Service website > **Template** tab.

b. Add transformations

It happens that sensitive data can be captured by Recorder as event names, for example, email addresses or IDs. This data can be viewed in the **Task Definition Editor** after uploading the logs to ABBYY Timeline. To hide such data from users, you can use transformations. This feature allows finding and replacing text in logs in order to redact sensitive information. By default, there are no transforms specified. To add transformations to the template, add them on the **Transformations** tab in advance.

Transformations complement the **Obfuscate user data** feature, which is enabled by default. For example, transformations allow you to replace an URL or some text in logs that should remain confidential, while obfuscation allows you only to mask text data or blur information in pictures.

5. Go to **Recorders**, select a recorder instance, and click **Start**.
   All user actions will be recorded in logs and sent to the Recording Service to process.
   If necessary, you can stop the recording at any time by clicking **Stop**.

6. Connect to your account in Timeline.
   Click **Connect** on the left bar and then click **Connect** in the opened **Connect to your Timeline account** dialog.
   As a result, the Timeline login form will open. Enter your Timeline credentials and click **Allow** in the access permission window.

This will enable Recording Service to upload logs into your account projects.
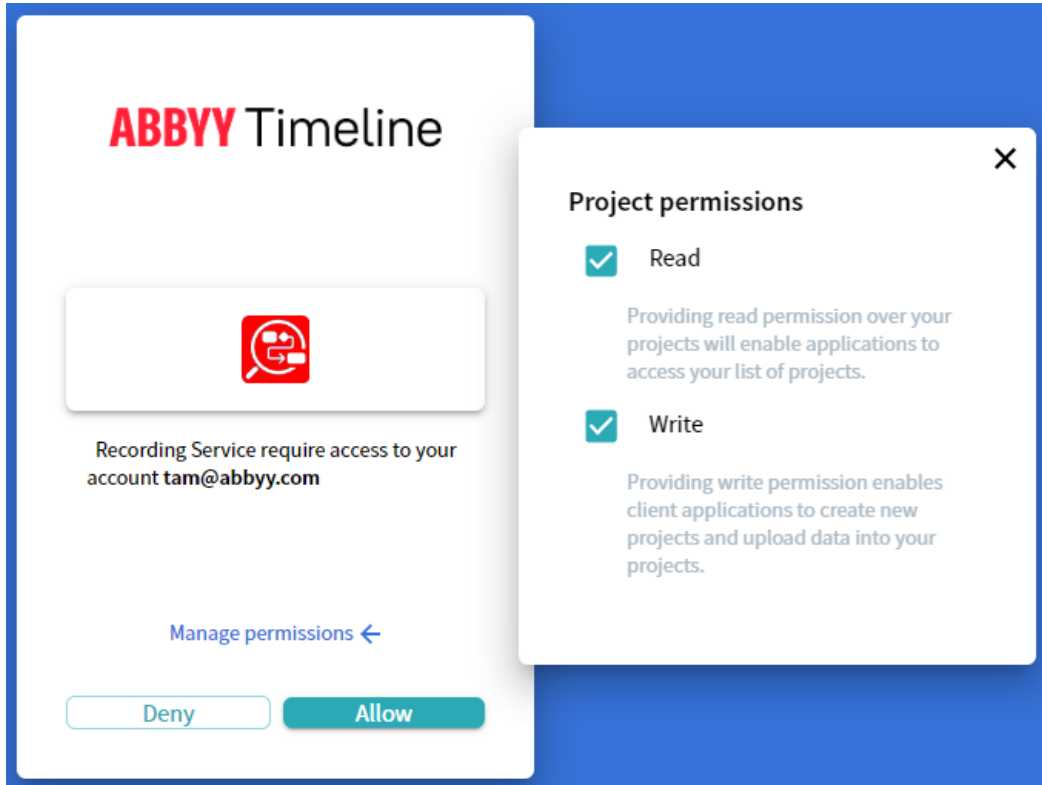
7. Upload logs to Timeline from Recording Service. To do this:

a. Go to **Logs**
    All recorded events are collected into logs and available in the **Logs** tab.
    Note. The logs may take some time to process. We recommend that you wait a while before starting to work with the logs.

b. Select logs and click **Load to project** in the top right corner.

c. In the opened **Project list** windows enter the name for your new Task Mining project and click **Create** to upload logs.

d. All selected logs will be queued for upload.
    Information about the upload process is displayed in the message box. You can abort the upload by clicking **Cancel** in the message box.
    Note. It is impossible to cancel the upload of logs that have already been submitted to Timeline by the moment of cancellation. Such logs will be available for work on the Timeline website.

e. Click ✉ to see the log import status. After the program finishes the import, click the project name link to navigate to the **Task view** page with project overview information.
    Note. The **Task view** page opens on the Timeline website.

8. Task definition
    The collected data is uploaded into a Task Mining project on the Timeline website, where tasks should be defined manually or identified automatically based on recurring actions, e.g. filling in documents, creating tables or diagrams, or generating analytical reports.

9. Data analysis
    Using the collected data, ABBYY Timeline will automatically discover which tasks will benefit most from process automation. Task Mining will help you examine the complexity of the tasks, the order of actions employed by each user to complete the same task, the time spent on each task, routines performed by all users, etc.

For detailed instructions on task definition, forms review, log cutting, task schema, and all the details of working with a Task Mining project, see Timeline user's guide > 'Task Mining' section.

Configuring and Applying Templates

Configure the template to specify what data needs to be logged and how it is to be processed. To do this, open the Recording Service website and go to the **Template** tab. Here you can add, change, or remove a template. A **Default** template is created during the Recording Service installation process. You can add and customize new templates.

Go to the **Templates** tab on the Recording Service website to see basic information on templates, review the Default template setting or add a custom template. For detailed information on the **Default** template and available settings, see below. All options available in the Default template you can set in your custom template.

Before you begin

Role required: Recording Service user.
Note. If your account is not added to the **Admin AD Security group** specified during the Recording Service installation, you will not have access to the Recording Service website.

Basic steps

Open the Recording Service website and go to **Templates**. On the page that opens, you will see all created templates. The **Default** template is always there. It cannot be renamed or deleted. But you can change its settings and save the changes. To change the template settings, click on its name.

To create a new template, click **Add template** in the top right corner. The following settings are available in templates:

1. **Start recording when assigned to recorder**
   If you need to start to record user actions after you assigned a template to a recorder, turn this toggle switch on.
   By default, the automatic start record is disabled.

2. **Record extended application info**
   Enable this option if you plan to export processes from Timeline for further import and refinement in Blue Prism applications. This option allows you to log additional information required to generate a Blue Prism JSON file.

3. **Scheduled recording**

   Toggle on this option to schedule recording sessions of user activity for the recorder instance. When enabled, the configuration panel shows.

   a. Select days of the week when recording sessions should be captured.

   b. Specify the time interval when user activity is recorded using **From** and **To** fields.

   c. Click the clock icon to set the start and the end time.
      Important. **From** and **To** values cannot be the same.

   d. Click **Save template** in the top right corner to apply changes.

4. **Merge data from multiple hosts**

   This option allows logging user activities in one log if a user works on multiple computers. For example, they works on their PC, and then switches to RDP and works there.
   Note. If different tags were added during the installation to each Recorder instance, all tags will be listed separated by commas for the resulting log. During the logging process, the list of tags may not appear immediately, but with some delay.
   Before using this option, make sure the following conditions are met:

   a. Recorder is installed on every computer a user works on and all recorder instances display on the **Recorders** tab. In the **Host** column, you can see a computer name visible on the network within the Active Directory domain

   b. Each of the Recorder instances must be set in the same template.

5. **Application list**

   The use **Included** and **Excluded** lists can significantly reduce the amount of unwanted data in the project and make analyzing tasks and processes easier. This becomes very important when dealing with large datasets that include important events which can be made harder to understand and analyze when there are a lot of case and path variants and deviations which are further complicated by unnecessary data.
   The default template contains a [predefined excluded list](#)⌐12⌐. It includes the most popular messengers. Correspondence in them may not be related to the tasks that a user performs. To disable logging in the desired messenger, turn the **EXCLUDED LIST** on and mark an item.

   For details on setting up **Excluded** and **Included lists**, see the '[Excluding and Including Applications](#)⌐11⌐' and '[Examples](#)⌐14⌐' sections.

6. **Transformations**

   Transformations allow finding and replacing text in logs in order to redact sensitive information, such as email addresses or IDs. This option complements the **Obfuscate user data** feature. For example, transformations allow you to replace an URL or some text in logs that should remain confidential, while obfuscation allows you only to mask text data or blur information in pictures.

   By default, there are no transforms specified. To add transformations to the template, add them on the **Transformations** tab in advance. During adding a transformation, you must specify:

   a. **Regular expression**

      It will be used to search for the text in the recorded logs.

   b. **Replacement**

      A string to replace the found text.

      Important. Transformations can greatly affect the results of an automatic task definition in ABBYY Timeline. It is impossible to undo transformations.

      For detailed instructions on using transformation see '[Transformations]22'.

Excluding and Including Applications

Before log recording, application lists can be configured using the template on the Recording Service website:

1. Open the Recording Service website and go to **Templates**.

2. Select a template by clicking its name.

3. In the **Application list** add a new item to the excluded and/or included list.
   By default, user activities are recorded across all websites and desktop applications that users interact with on their computers.
   Using **EXCLUDED LIST** and **INCLUDED LIST** allows you to specify a list of websites or applications that should be excluded and included in your logs respectively. Using both **INCLUDE** and **EXCLUDE** lists can define a site that should be included and a subset of that to be excluded. If the same item appears in both lists, user activities will not be recorded across the specified application or website. The item will be excluded from your logs.
   Important. To operate correctly, the Recorder browser extension must be installed on the user's computer.

    a. To prevent the recording of user activity for a particular website or desktop application, turn on the **EXCLUDED LIST** toggle switch.

    b. To track and record user activity for a particular website or desktop application, turn on the **INCLUDED LIST** toggle switch.

4. Click **Add item**.

5. Use the **Add item** form that will open to specify particular websites and/or desktop applications. You can either enter a file path or URL or combine valid literal paths and * (asterisk) wildcard characters.
Examples:

    a. Full path to the application:
```
C:\Program Files\ABBYY Recorder\Abbyy.Recorder.App.exe
```

    b. Using * (asterisk) characters in the file path:
```
*\Abbyy.Recorder.App.exe
C:\Program Files\ABBYY*.exe
```

    c. Using * (asterisk) characters in the URL:
```
https://recordingservice.abbyy.com/*
```
The sample URL above will prevent/allow user activities to be recorded for the specified web pages.

```
https://*.abbyy.com/*
```
The sample URL above will prevent/allow user activities to be recorded across all the URL's sub-domains.

6. Click **Save**.

Predefined Excluded List

The **Default** template contains a predefined **Excluded List** of ignored messengers and their websites. Enable the **EXCLUDED LIST** to prevent all user activities from being recorded on specified applications and websites. By default, **Excluded List** is disabled. The table below lists the applications and corresponding items in the **Excluded List**.

Important. The new **Default** template is available in Recording Service 5.2 or late installed for the first time. When Recording Service upgrades from earlier versions to 6.0, user settings are maintained. This prevents unexpected impacts on processing logs. You can add listed items to the **Excluded List** manually.

Applications	Item in the Excluded List
Blackberry Messenger	*\BBM Enterprise.exe
Brosix	https://web.brosix.com/* *\Brosix.exe
Cisco Webex	https://web.webex.com/ *\CiscoJabber.exe
Discord	https://discord.com/channels/* *\Discord.exe
Facebook Messenger	https://facebook.com/messages/* *\Messenger.exe
Google Hangouts	https://mail.google.com/chat/* https://hangouts.google.com/*
Lync	*\lync.exe
Sametime	*\stcommunity.exe
Signal	*\Signal.exe
Skype	https://web.skype.com/* *\Skype.exe
Slack	https://app.slack.com/* *\slack.exe
Teams	https://teams.microsoft.com/* *\Teams.exe
Telegram	https://web.telegram.org/* *\Telegram.exe

Applications	Item in the Excluded List
Viber	*\Viber.exe
WeChat	https://web.wechat.com/* *\WeChat.exe
WhatsApp	https://web.whatsapp.com/* *\WhatsApp.exe

Examples

The examples in the table below require the Recorder browser extensions to be installed. Otherwise, user activities will not be recorded in Google Chrome, Microsoft Edge, and Mozilla Firefox.

Important. If the same item appears in both lists, user activities will not be recorded across the specified application or website. The item will be excluded from your logs.

EXCLUDED LIST	INCLUDED LIST	Description
-	https://*.abbyy.com/*	Records user activities in all applications, browsers, and sites that match the https://*.abbyy.com/* template.
https://*.abbyy.com/*	-	Records user activities in all applications and browsers with the exception that recording is disabled for sites that match the https: //*.abbyy.com/* template.
*\firefox.exe	-	Records user activities in all applications and browsers except the Firefox browser.
-	*\Chrome.exe	Records user activities only in the Google Chrome browser. Recording is disabled for other browsers and applications.
-	*\Chrome.exe, https://*.abbyy.com/*	Records user activities only in the Google Chrome browser and sites that match the specified template. For example, the following sites will be recorded: https://help.abbyy.com/, https://www.abbyy.com/solutions/business-process/

EXCLUDED LIST	INCLUDED LIST	Description
		Recording is disabled for other browsers and applications.
*\firefox.exe	https://*.abbyy.com/*	Records user activities in all applications and browsers except the Firefox browser. Recording in browsers will be carried out only for sites that match the https://*.abbyy.com/* template.
-	*\chrome.exe, *\firefox.exe, *\excel.exe	Records user activities in the Google Chrome and Firefox browsers, as well as Microsoft Excel. Recording is disabled for the Microsoft Edge browser and other applications.
*\teams.exe	-	Records user activities in all browsers. Recording is disabled for Microsoft Teams.
https://procurement.abbyy.ru/*	https://*.abbyy.ru/*, https://abbyy.ru/*	Records user activities in all applications and browsers. Recording in browsers will be carried out only for sites that match the https://*.abbyy.ru/*, https://abbyy.ru/* templates. Recording is disabled for the https://procurement.abbyy.ru/* website.
-	http*, *\firefox.exe, *\chrome.exe, *\edge.exe	Records user activities in Google Chrome, Microsoft Edge, and Mozilla Firefox browsers. Recording is disabled for all desktop applications.

Important. We recommend not recording messenger information, as it often contains messages with sensitive information. Doing so can negatively affect machine performance as well.

We recommend adding the following messengers to the **Excluded** list:

- Adium

- Atlassian HipChat

- Blackberry Messenger

- Brosix

- Cisco Jabber

- Cisco Webex

- Discord

- Facebook Messenger

- Google Hangouts

- IBM Lotus Sametime

- Lync

- Microsoft Teams

- Signal

- Skype

- Skype for Business

- Slack

- Telegram

- Viber

- WeChat

- WhatsApp

How to Apply Templates and Start Recording

For all the settings specified in the template applied when recording user actions, you should assign the desired template to the selected recorder instance:

1. Go to **Recorders**.
   You will see the list of connected recorders.
   The **Host** column displays computer names that are visible on the network in the Active Directory domain. The **Tag** column displays tags added during the installation of recorder instances.

2. Check the recorder instance, you want to configure with a template and start recording and click **Set Template**.
   In the opened list chose the template, and then click **Select**.

3. The recording runs automatically if the **Start recording when assigned to recorder** is enabled in the template. Otherwise, click **Start** to run the recording.

Recorders

On the **Recorders** page, you will find all installed recorder instances that were able to connect to Recording Service. A Recorder instance is a workstation where Recorder has been installed. Information about instances and the logs that were recorded on each workstation is displayed in the **Recorders** table. Only Recorders installed in **Server managed mode** get into the table of recorders.

Before you begin

Important. Role required: Recording Service user.
If your account is not added to the **Admin AD Security group** specified during the Recording Service installation, you will not have access to the Recording Service website.

Basic Options

Open the Recording Service website and go to **Recorders**. On the page that opens, you will see all installed recorder instances that were able to connect to Recording Service. The **Host** column displays computer names that are visible on the network in the Active Directory domain. The **Tag** column displays tags added during the installation of recorder instances.

The following operations are available for the selected recorder instance:

- Set template.
  Check the recorder instance you want to assign the logging template to and click **Set Template**.
  In the opened list chose the template, and then click **Select**.
  Note. The recording runs automatically if the **Start recording when assigned to recorder** is enabled in the template.

- Start or stop log recording on the selected workstation.
  Check the recorder instance, and then click **Start** or **Stop** to run log recording or stop it.
  Note. The log recording runs automatically when a template is set, if the **Start recording when assigned to recorder** is enabled in the template.

- Add tag.
  A tag is a simple, non-unique text string that describes a workstation or group of workstations. Click **Set Tag**, enter text in the opened window and then click **Save** to save it as a tag.

Username is not recommended as a tag because several users could occupy the same workstation. For example, you can specify the same tag for several workstations, e.g., the 'accounting department' tag. Then you can easily find these workstations in the Recorders list by the 'accounting department' tag.

- Remove the selected instance from the list.
Important. Only an offline recorder instance is allowed to be deleted. In this case, the recorder instance only disappears from the list. As soon as the Recorder goes online again, it automatically appears in the list. It is not allowed to delete the recorder with statuses **online** and **recording**, only **offline**.
To delete an offline recorder select the recorder instance and click **Delete selected**.

- Delete logs.
Using this feature, you can delete all logs recorded on the selected hosts. This will delete the logs of all users who worked on this host computer.

Enabling and Disabling Recorder Instances

To log the actions of a particular user, a Recorder instance must be enabled on that user's computer. A user may disable event recording by clicking **Disable** in the Recorder menu in the system tray. This will stop recording and block recording control on this instance via the Recording Service UI. The Recorder will still appear in the list of Recorders on the Recording Service with a status shown as **online** but even if you click **Start** and **Refresh List** it will not be set to **recording**.

To start or resume recording using the Recording Service interface, the user must first enable recording by clicking the **Enable** button in the Recorder menu in the system tray.

If recording is to be controlled only by the administrator via the Recording Service website, all Recorder instances must be installed in silent mode using the parameter **controlButtonVisible = false**. For details, see "Preventing End-Users from Controlling Recorder."

Logs

On the **Logs** page, you will find detailed information about recorded user sessions from connected Recorder workstations. Only Recorders installed in the **Server managed** mode can send captured logs to Recording Service.

Before you begin

Important. Role required: Recording Service user.
If your account is not added to the **Admin AD Security group** specified during the Recording Service installation, you will not have access to the Recording Service website.

To be able to upload logs to the Timeline project, make sure that connection with Timeline is set. For details, see [Workflow Guideline](#) 5 .

Basic Options

Open the Recording Service website and go to the **Logs** tab. On the page that opens, you will see recorded user sessions from the connected Recorder instances. The information about each log includes: the log ID, the duration of the recorded session and its start time, the log size in MB, the Recorder version, the number of recorded events, the tag and the template used for the Recorder instance, and the computer username. If the log is uploaded to Timeline project(s), the name of the last project is displayed in the **Last project** column.

The following operations are available for the selected log(s):

- **Apply transformation**
  You can apply created [transformations](#) 22 for all recorded logs. To do this:

  o Select logs and click **Apply transformation** in the top right corner.

  o In the opened **Apply transformation** window, select transformations.

  o Click **Apply to all logs**.

- **Download**
  Allow saving selected logs to your computer as ZIP files. The archive includes folders having the names of downloaded log IDs. Each log folder consists of *Commands*, *Forms*, and *Screenshots* subfolders with applied export settings.
  For more information about export settings, see [Administrative settings > Logs](#) 30 .

- **Load to project**

  Using this feature, you can upload logs to the project in the connected Timeline account. To do this:

  o Select logs and click **Load to project** in the top right corner.

  o In the opened **Project list** windows enter the name for your new Task Mining project and click **Create** to upload logs.

  o All selected logs will be queued for upload.
  Information about the upload process is displayed in the message box. You can abort the upload by clicking **Cancel** in the message box
  Note. It is impossible to cancel the upload of logs that have already been submitted to Timeline by the moment of cancellation. Such logs will be available for work on the Timeline website.

  o Click ✉ to see the log import status. After the program finishes the import, click the project name link to navigate to the **Task view** page with project overview information.
  Note. The **Task view** page opens on the Timeline website.

- **Delete selected**

  Allow deleting selected logs from Recorder Service.
  Important. This action cannot be undone. Consider downloading logs to your computer before deletion.

To open detailed information about the log, click on its ID. You can see captured screenshots by clicking the event on the left. **Download**, **Load to project**, and **Delete log** options are available for the opened log.

Filtering Logs by a User Name

All logs are located in the **Logs** tab of the Recording Service website. You can find general information for each log there. The only thing that does not display by default is the name of the user accounts under which logs were recorded.

If you log user activity on a terminal server, all logs are recorded with the same computer name. The same happens if several users work on the same computer. It is recommended to enable the display of the **Username** column to identify the logs for each user. This name is useful for filtering logs by user. Further, you can load logs of different users to different Timeline projects.

To display usernames, perform the following actions:

1. Go to the Recording Service installation folder and open **appsettings.Production.json** using any text editor.
   By default, it is installed into *C:\inetpub\ABBYY Recording Service*.
   Important. Requires administrator privileges to edit **appsettings.Production.json**.

2. In the file add the following line:

```
"DiscloseOperators":"true",
```

3. Save the file.

4. Restart the Recording Service website in the Internet Information Services (IIS) Manager.

5. Open the Recording Service website and go to the **Logs** tab.
   The **Username** column will be displayed there only if there are recorded logs. This column displays the name of the user accounts under which logs were recorded.
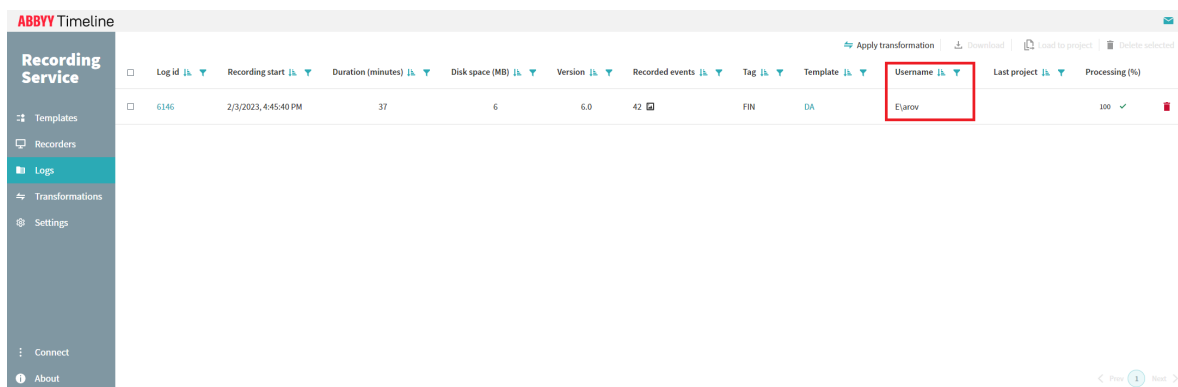
Storing Records in Logs

All records received throughout the day from a specific machine are recorded in a single log, even if the recording process was interrupted. A separate log is created for each day.

Transformations

Before you begin

Important. Role required: Recording Service user.
If your account is not added to the **Admin AD Security group** specified during the Recording Service installation, you will not have access to the Recording Service website.

Overview

Transformations allow you to edit and anonymize information in the recorded data in order to protect sensitive information.

For example, during the logging process, potentially sensitive information may appear in URLs or event names. This data can be viewed in the **Task Definition Editor** after uploading the logs to ABBYY Timeline. To hide this text from users, you can use transformations.

Use transformations to do the following:

1. Remove sensitive data that has been captured by Recorder as event names.
   For example, if it is recorded in the log that a user has opened a document called **PO-BankOfAmerica.pdf** or **BillGatesSalary.xls**, it is best to replace these with redacted strings like opening **PO-XXX.pdf** and opening **XXXsalary.xls** respectively. To do so, you will need to configure transformations as regular expressions and apply them to selected logs.

2. Cast the names of several similar events to a common name.
   If you notice similar unique strings like **opening PO-BankOfAmerica** and **opening PO-CitiBank**, you can use transformations to convert these events to a common type, e.g. **opening new PO**. This new event can then be marked as either a start event or an end event in **Task Definition Editor**.

Important. Be careful when using transformations.

- Transformations can greatly affect the results of an automatic task definition in ABBYY Timeline.

- Transformations cannot be undone.

For more information about creating and applying transformations, see [Before applying transformations in production environment](#) 23.

Before applying transformations in production environment

Transformations can greatly affect the results of an automatic task definition in ABBYY Timeline and it cannot be undone. Therefore it is very important to test transformations out by applying them to one or two logs.

How to test the transformations:

1. Record a representative sample of logs for creating and testing regular expressions. For recording, use the Recorder instance that is installed on a user computer whose workflow you plan to analyze using Timeline tools for further optimization. For test purposes, it is enough to run the recording for an hour.
   To do this:

   a. Go to the **Recorders** tab.

   b. Select a Recorder instance.

   c. Make sure the correct template is assigned to this instance.

   d. Click **Start**.

2. Examine the data that may appear in logs and select texts that should remain confidential. To do this:

   a. Go to the **Logs** tab.

   b. Select log and click its **LogID**.

c. As a result, a window with information about the selected log will open.
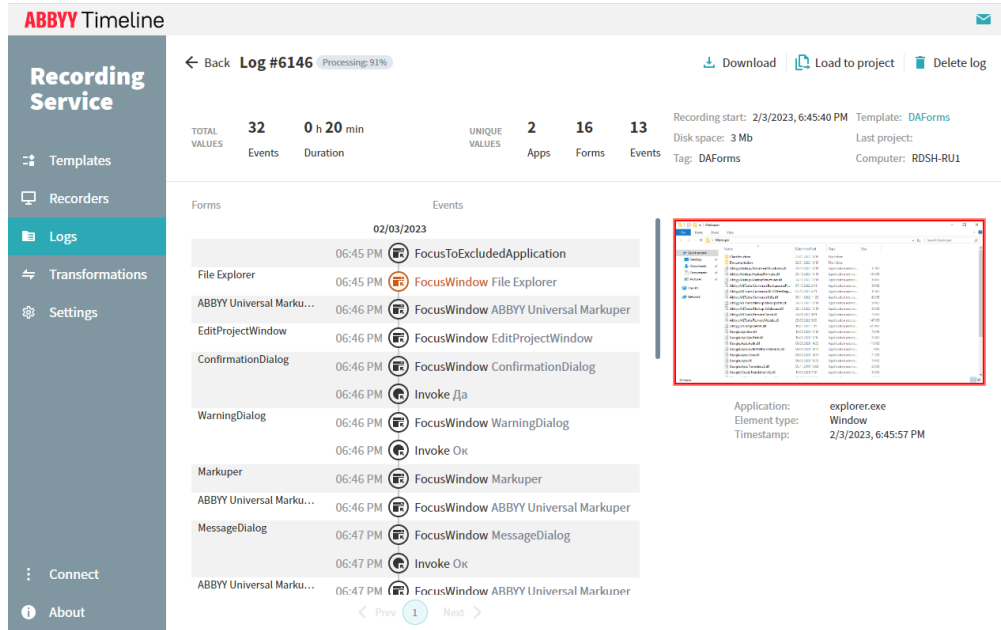
This window displays all events recorded in the current log. The selected event is highlighted in color, and a screenshot is displayed for it, in case you have enabled screenshot recording. The path to the application name or URL is displayed below the screenshot.

Inspect all event names and URL text. Sometimes titles, names, addresses, and other fragments of texts that should remain confidential may appear. In the following step, you can prepare regular expressions that will be used to find and replace all such occurrences in the detected text and URL's.

3. Prepare regular expressions and replacement strings.
   Examples:

What to look for	Regular expression to replace	Replacement string
John	(J|j)ohn	FIRST_NAME
john.smith@abbyy.com ivan.ivanov@abbyy.ru	\w+.\w+@abbyy\.(com|ru)	first.last@abbyy.com
Customer: John Doe	Customer:[\s+\w+]+	Customer: Customer's Name

4. Add transformations and test them out by applying them to one or two logs.
   For details, see 'How to add a new transformation 25 ' and 'Post-recording transformation 23 ' below.

5. If you are satisfied with the changes, apply the transformations to all recorded logs or add them to the template to transform data on the fly.

How to add a new transformation

1. Go to the **Transformations** tab.

2. Click **Add Transformation**.

3. In the opened windows, specify the following transformation parameters:

    a. **Regular expression**
        To search for a text string, enter a regular expression using Regex syntax.

    b. **Replacement**
        To replace instances of the text string in logs with another string, enter the replacement string.

    c. **Case insensitive**
        By default, the search is case-sensitive. If this option is selected, the search will not be case-sensitive.

Important. If you edit or delete a transformation, the changes will propagate to all the templates that include this transformation.

How to apply transformations

You can apply transformations to all recorded logs or add them to a template to transform data on the fly during log recording.

On-the-fly transformation

To apply transformations to logs while recording data, add transformations to a template and assign it to a recorder instance.

1. Go to the **Templates** tab.

2. Click a template name or create a new one.

3. Click **Transformations** and then **Add item**.

4. In the window that will open, select transformations and click **Add**.

5. Assign transformations to a recorder instance.
   To do this:

   a. Go to **Recorders**.

   b. Check the recorder instance you want to configure with a template with a new transformation

   a. Click **Set Template**.
      In the list that will open, click the template, and then click **Select**.

   b. The recording runs automatically when the **Start recording when assigned to recorder** is enabled in the template. Otherwise, click **Start** to run the recording.

Post-recording transformation

You can apply transformations to logs that have already been recorded. To do this, complete the following steps:

1. Go to the **Logs** tab.

2. Select logs.

3. Click **Apply transformation**.

4. In the opened form, select transformation and click **Apply to selected logs**.

Important. If you cancel a running transformation, the transformed portion will not be undone.

Settings

The **Settings** tab contains Timeline Authentication setting, interface language preferences, and additional options related to personifying recorded logs and blurring sensitive information. **Timeline Authentication** and **Logs** can only be managed by the admin of the Recording Service.

Timeline Authentication

For interaction between Recording Service and Timeline, OAuth must be configured.

OAuth is an authorization protocol that allows granting one service (application) the right to access user resources on another service. The protocol eliminates the need to pass the application a username and password and allows a third-party application to gain limited access to an application or service, on behalf of a resource owner.

Basic steps

1. Register Recording Service as a client on the Timeline website and obtain credentials (**Client ID** and **Client Secret**).
   For more information, see the 'Registering a New Client on Timeline website 27 ' section below.

2. In the Recording Service website specify the authentication details to Timeline using the credentials you obtained in step 1.
   For more information, see the 'Configuring connection setting in Recording Service 27 ' section below.

Registering a New OAuth Client on the Timeline website

Role required: Timeline account admin

1. Open the Timeline website and log in using the credentials specified during the Timeline installation.

2. Click your user avatar at the bottom of the left bar and then select **Account** > **OAuth** and click **Register client**.

3. In the **Register OAuth client** form, fill in the following fields:

a. **Name**

Enter a unique name that identifies the application that you require OAuth access for. For example, RecordingService.

Note. The specified name is then presented to a user in the consent screen on the Recording Service website, making it clear to your users.

b. **App URL**

Enter the URL that hosts Recording Service. For example, https://recorder.myCompany.com

Note. To get the correct **App URL** and **Redirect URI** for the Recording Service, open the Recording Service website in your browser and go to the **Settings** tab. There you will find the "Timeline Authentication Guide". Find the value you need, copy, and paste it into the appropriate field on the Register OAuth Client form on the Timeline website.

c. **Redirect URI**

Enter the callback URL that the authorization server redirects to. Enter the full URL of the clients requesting access to the resource, appended by **/api/auth/callback**. For example, https://recorder.myCompany.com/api/auth/callback

d. **Confidential client**

Select **Confidential clients** as Recording Service is able to securely authenticate with the authorization server, for example being able to keep their registered client secret safe.

e. **Client logo**

This is optional. You may upload an image to use as the application logo. The logo appears on the approval page when you receive a request to grant a client application access to a restricted resource on the instance.

f. **Scopes**

Select **Read projects** and **Write projects** scope values to request access to submit data from Recording Service to Timeline. An application can request one or more scopes, this information is then presented to a user in the consent screen, and the access token issued to the application will be limited to the scopes granted.

4. Click **Register** and you will be able to see **Client ID** the auto-generated unique ID of the application. Copy **Client ID** and **Client Secret** fields for use on Recording Service.

Configuring authentication setting in Recording Service

Permission required: Recording Service admin.
Your account must be added to the Active Directory group specified during the Recording Service installation, which contains the email addresses of the Recording Service administrators.

1. Open Recording Service website.

2. Go to **Settings > Timeline Authentication** and fill in the fields:

    a. **Timeline URL**
        Enter the URI of the Timeline website.

    b. **Client ID** and **Client Secret**
        Enter the **Client ID** and **Client Secret** you obtain after registering the client in the 'Registering a New Client on the Timeline website' step 28 section.

3. Click **Save**.
    Please wait for a notification. If the connection is successful, it displays **Save**. Otherwise, an error appears: 'The server is unreachable, please notify the administrators and try again later'.
    If connection fails:

    a. Check the connection settings you specified above.

    b. Make sure the Timeline website is available.

    c. Check the firewall settings. For more information, see the 'Network Connection Settings 27'.

    d. Make sure the ports specified during the Recording Service installation are not being used by other applications. For more information, see the "Check TCP/IP port availability".

Language

Permission required: Recording Service user.
Your account must be added to the Active Directory group specified during the Recording Service installation, which contains the email addresses of the Recording Service users.

Using the tools on the **Language** tab you can manage your UI language preferences.

Logs

You may want to set up additional options before starting to work with logs. Decide whether to personify recorded logs to see who recorded them. If your processes involve sensitive information, obfuscate it in logs and blur it on screenshots.

Before you begin

Permission required: Recording Service admin.
Your account must be added to the Active Directory group specified during the Recording Service installation, which contains the email addresses of the Recording Service administrators.

Options

Logs settings are divided into two sections.

- **General**
  Settings having effect within Recording Service.

  o **Show username on the Logs tab**
    If turned on, adds a Username column to the table in the Logs tab. This column contains the names of users who recorded the logs. By default, this option is turned off.

- **Export**
  Settings having effect only when logs are exported from the Recording Service. Export means both uploading them directly to the Timeline and downloading logs from the Recording Service.

  o **Obfuscate user data**
    This option allows protecting sensitive information and ensures data security. By default, this option is turned on. This means when exporting logs, sensitive information is encrypted in text logs and blurred on screenshots as well. If the option is turned off, you can easily read all the texts and see data in the screenshots. To do this just go to the **Logs** tab and click **LogID**.

  o **Include username**
    If turned on, the exported logs contain the name of the user who recorded them. By default, this option is turned off.

- o Include computer name

  If turned on, the exported logs contain the name or ID of the computer on which they were recorded. By default, this option is turned off.

Technical Support

Should you have any questions regarding the use of ABBYY Timeline, please submit a request to the ABBYY technical support service on this [page](#).