ABBYY

ABBYY® Timeline 6.0

Deployment Guide on Windows Systems

Table of Contents

Table of Contents

About This Document

This deployment guide is intended for system administrators and engineers. It includes instructions for installation and configuration of ABBYY Timeline 6.0 on Windows.

Introducing ABBYY Timeline

ABBYY Timeline is a Process Intelligence platform featuring advanced process discovery, analysis, monitoring, simulation, and task mining. It uses the latest artificial intelligence (AI) to enable enterprises to automatically build an interactive digital twin of business processes that reveals inefficiencies and process bottlenecks. With this insight, they can apply automation where it will have the greatest impact and predict future outcomes.

ABBYY Timeline employs an exciting new patent-pending approach to process intelligence called Timeline Analysis which allows users to load events from a variety of systems and in different formats which it then automatically organizes into its corresponding process instances and allows them to be analyzed with a variety of visualization, discovery and query techniques. ABBYY Timeline accepts event data from any number of systems of record and automatically reconstructs the underlying business process logic behind the data. A variety of pre-built analyses are ready to quantify your process performance, identify your process execution issues and perform root cause analysis. The ABBYY Timeline platform also supports operational monitoring through its continuous assessment of new event data to determine if any adverse conditions occur and can immediately notify you or other business operations personnel so you can act.

The ABBYY Timeline engine consumes data from a variety of sources to detect and present detailed views of your business processes. This is often the same exact data being used today for other simpler analyses. This new insight is delivered via a variety of new process and timeline visualization tools developed to not only make these new insights easier to understand but also to allow users to manipulate the information to gain a deeper understanding of those processes. Users armed with this insight have concrete facts on which to take actions to improve operational efficiency by promoting clearly superior best practices and eliminating costly inefficiencies that previously went undetected.

Using advanced algorithms, ABBYY Timeline extracts and reads the time stamps used to record specific events along your processes. The software then visually models these time stamps in such a way that you can instantly identify deviations from an ideal process flow – to find the root cause of a problem that may be costing your business money.

ABBYY Timeline is aimed for use by anyone involved in business process improvements of any type of scale or nature.

On-Premises or Hybrid Installation

Whether you use Timeline via ABBYY's SAAS instance or installed on-premises the recommended

configuration of Timeline requires 3 key components:

1. The Timeline core (either hosted by ABBYY or installed on-premises).

2. Recorder which captures individual users' desktop sessions.

3. Recording Service that manages the deployed Recorders.

Recorders and Recording Service must always be on-premises - local to the users being recorded. There is no difference in functionality whether Timeline is accessed via ABBYY's cloud instance or installed locally.

The purpose and functions of platform components are described in the table below.

Component	Description
ABBYY Recording Service	ABBYY Recording Service collects user interaction logs from multiple users over time and allows to submit obscured data into ABBYY Timeline. It is only on-premises and includes databases and website.
ABBYY Recorder	Captures individual users' desktop sessions. It is only on-premises and includes Recorder, Recorder Log Viewer, and browser extensions for Google Chrome, Mozilla Firefox and Microsoft Edge.
ABBYY Recorder Log Viewer	Allows users to view the logs recorded by ABBYY Recorder.
ABBYY Timeline	Timeline analyzes user-desktop interaction data to assist organizations in understanding how people work and how tasks are completed. Combined with process details mined from system event data, Task Mining enables organizations to enhance operational efficiency, improve customer experience, and accelerate impactful digital transformation. It accelerates digital transformation time to value by automating how you discover, analyze, monitor, and improve your processes. It is either hosted by ABBYY or installed on-premises. There is no difference in functionality whether Timeline is accessed via ABBYY's cloud instance or installed locally.

Standalone Recorder mode

There is an option to test Timeline's Task Mining features without installing the Recording Service. In this case, you need to install Recorder component in standalone mode. All recordings, in this case, will be stored on a local user's computer and then must be uploaded to the Timeline project manually. Before uploading, you should use the Recorder Log Viewer utility to inspect locally saved logs. This gives the option to detect forms and see recorded data without having to install Recording Service and set up the Active Directory groups that it utilizes.

Limitation of Standalone Recorder mode:

- Forms are not detected

- Only passwords are encrypted in text logs, other text data are not encrypted, and data in screenshots aren't blurred.

It is not recommended to use **Standalone Recorder Mode** for production deployments and recommend it is limited to trial activities.

Deployment Workflow Guideline

Ready to deploy? The instruction below walks you through deploying and initial setup of the ABBYY Timeline system, step-by-step.

Step 1. Make sure your computers are ready for ABBYY Timeline system

Before you begin installing ABBYY Timeline system:

1. Check the system requirements 19 .
   These requirements help you know whether your computers support ABBYY Timeline components.

2. Apply the latest Windows and other program updates.
   These updates ensure that your computer has the latest security updates.

3. Reboot.
   The reboot ensures that any pending installs or updates don't hinder the ABBYY Timeline components install.

4. Free up space.

Remove unneeded files and applications from your %SystemDrive%, as well as discs that you intend to use, for example, to store the Timeline or Recording Service databases.

5. If you intend to configure HTTPS, please visit the 'Using HTTPS 58' section.

Step 2. Install ABBYY Recording Service

If you are not going to use the Task Mining feature, skip this step.

1. Run the **ABBYY.RecordingService.6.0.*.exe** file and follow the on-screen instructions in the Installation Wizard.
   If you receive a **User Account Control** notice, choose **Yes**.

2. Specify the necessary network settings 65.

3. Make sure Recording Service has been installed correctly by performing a health check on Recording Service 39.

Please refer to the 'Installing Recording Service 36' section for guidelines.

Step 3. Install ABBYY Timeline

If you are going to use Timeline in the cloud, please, skip this step.

Important. Recording Service and Timeline components must be installed on separate computers.

1. Run the **ABBYY-Timeline-6.0.*-installer.exe** file and follow the on-screen instructions in the Installation Wizard.
   If you receive a **User Account Control** notice, choose **Yes**.

2. Specify the necessary network settings 64.

3. Make sure the Timeline has been installed correctly by performing a health check on Timeline 30.

Please refer to the 'Installing ABBYY Timeline 24' section for guidelines.

Step 4. Establish the trust relationship between ABBYY Recording Service and ABBYY Timeline

If you are not going to use the Task Mining feature, skip this step.

For interaction between Recording Service and Timeline, OAuth must be configured 56 .

1. Register Recording Service as a client on the Timeline website and obtain credentials (**Client ID** and **Client Secret**).
Please refer to the 'Registering a New Client on ABBYY Timeline website 56 ' section for guidelines.

Register OAuth client   ✕

* Name

Recording Service

* App URL

https://recordingservice.abbyy.com

* Redirect URI

https://recordingservice.abbyy.com/api/auth/callback

☑ Confidential client

Confidential clients are applications that are able to securely authenticate with the authorization server, for example being able to keep their registered client secret safe. Non-confidential (Public) clients are unable to use registered client secrets, such as native applications. They are expected to authenticate with client ID and PKCE flow

Client logo

⬆ Change logo

Scopes

☑ Read projects

☑ Write projects

☐ Read repositories

☐ Write repositories

Close   **Register**

2. In the Recording Service website specify the Timeline authentication details using the credentials you obtained in step 1.
Please refer to the 'Configuring connection setting in Recording Service ⌐58⌐' section for guidelines.
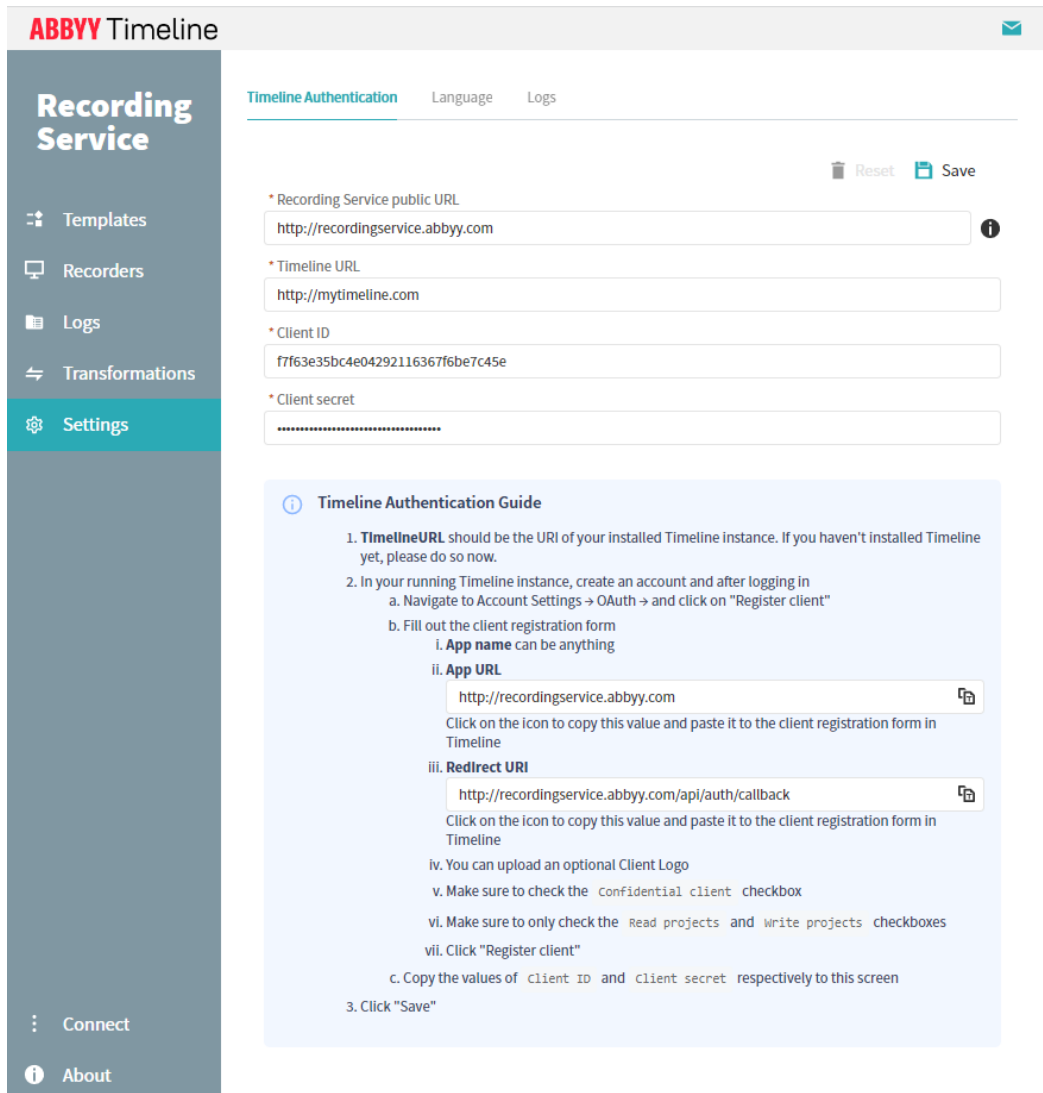
Step 5. Install ABBYY Recorder on users' computers

If you are not going to use the Task Mining feature, skip this step.

Important. The user workstations installing the Recorder, and the server hosting the Recording Service must all be members of the same Active Directory domain.

If you plan to record activities of users that work using Windows RemoteApp and Citrix Workspace App, install the Recorder on a terminal server.

ABBYY Recorder can be installed on the terminal server as if it was a workstation. It will log the actions of users connecting to this server via a Citrix client or RDP.

1. Install the Recorder on the users' workstations using the method of your choice.
   Please refer to the 'Installing Recorder 42 ' section for guidelines.

2. Turn on Recorder extensions on the workstations.
   Please refer to the 'How to Turn Recorder Chrome Extension on 49 ' section for guidelines.

Now you have all the ABBYY Timeline system components installed, and you can start working with it.

After you complete all the steps above, refer to the 'Access control in Recording Service & Timeline 12 ' section. Here you will find basic instructions about users' roles and permissions in Timeline and Recording Service.

See also:

- Configuring Recording Service 14

- Getting Started with Task Mining 16

- Getting Started with Process Analysis 18

Access control in Recording Service & Timeline

Accounts and users in Timeline

An account is a representation of the organization, company, or just a group of users. A user is a person having a unique identifier (login) in Timeline. In the current version, login is identical to user's email address. Each user belongs to one and only one account. Once any user signs up for Timeline, they are automatically linked to an account.

During the Timeline installation in the 'Admin User Account' step 27 , a user account is created. This user is automatically assigned the **Account owner** role. **Account owner** is a user who has full control over the account.

In order for company employees to get access to the Timeline website and data analysis features, employees just need to register on the Timeline website deployed for the organization. Another way is when the **Account** owner adds users to the account on the Timeline website in the account settings. We recommend that you add a user with the **Admin** role to your account to manage users in your account. Users with this **Admin** role have access to a Timeline account and control (add, remove, delete) other users related to the account.

Adding new users via account settings

1. Open a browser and enter **{timelineURL}:{port}** in the address bar, where:
   {TimelineUrl} is the Base URL you specified during the Timeline installation or the public IP address or the full name of the computer on which Timeline is installed.
   {port} is a custom port assigned to the Timeline website during the installation process. If you are using the default port (80 or 443), you do not need to add them to the {**timelineURL**}. By default, TCP/IP port 80 or 443 is used.
   Example: http://mytimeline:8080 or https://mytimeline:30443

2. Login using the Timeline admin credentials you specified in the 'Admin User Account' step 27 during the Timeline installation process.

3. Click your user avatar at the bottom of the left bar, then select **Account**.

4. In the **Account** page click **Users** and then click **Add users**.

5. In the **Invite users to account** window enter user emails separated by commas.

6. Timeline will send an automatically generated invitation to join the account to all specified addresses. Once users followed the link from an email, they are immediately linked to the account.

7. (Optional) To assign a user account administrator rights, select it in the **Users** table and click **Promote to admin**.

Important. User permissions in Timeline are regulated by **Role**. A role is a set of permissions for a particular scope. Roles determine what people can see and do in Timeline. There are administrative roles that are designed for people responsible for managing accounts and data. Non-administrative roles let people work with data in Timeline and access analysis results. For more information about roles and permissions, see Timeline manual -> 'Accounts, User Roles & Permissions' section.

Users and permissions in Recording Service

Access control in Recording Service is carried out by Active Directory security groups. Groups govern both communication between Recording Service and Recorders that are running on workstations, and user access to the Recording Service website. Groups must be created prior to installing the Recording Service. During the installation of Recording Service, all created groups are specified. In order for the logs recorded by Recorder on the user's computer to be sent to Recording Service for processing, or for the user to have access to the Recording Service website, user accounts must be added to the Active Directory security groups specified during the Recording Service installation.

If you need to grant users access to Recording Service, depending on their role, add them to the appropriate Active Directory groups.

For more information about Active Directory groups, see: 'Configuring Active Directory Groups to Configure Access to Recording Service 33'.

Configuring Recording Service

After you installed Recording Service and set up a trust relationship with Timeline, Recording Service is actually ready to go.

To improve the quality of recorded logs, anonymize information, and ensure data security, you can change the following settings in Recording Service:

- **Change 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.

- **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.

- **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.

For details on all the features of Recording Service, see the Recording Service user's guide.

Getting Started with Task Mining

Task Mining will help you get an insight into your employees' interactions with the software used inside your company and see how much time they spend on specific processes or stages. This information will give you a better understanding of the efficiency at each stage and automate business routines wherever possible.

Basic stages

1. Record users' activity inside applications
    On each user's machine, Recorder is installed. This module works in the background and automatically collects information about business operations performed by the user (e.g. selecting table cells, copying and pasting data, editing fields, clicking links, etc.). Recorded user actions and their associated screenshots are sent to the central server.

    a. Go to **Templates** and click **Default** in the **Template name** column. Review and modify the options if needed.
        In the template, you can specify what data to be logged and how to process it. Please refer to the Recording Service user's guide for guidelines.

    b. Go to **Recorders**.
        You will see the list of connected recorders that were installed in **Server managed** mode. Installed in this mode, recorders are automatically added to the **Recorders** list.

    c. Select a recorder and click **Start**.
        This starts recording all user's desktop events to log.

2. 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.
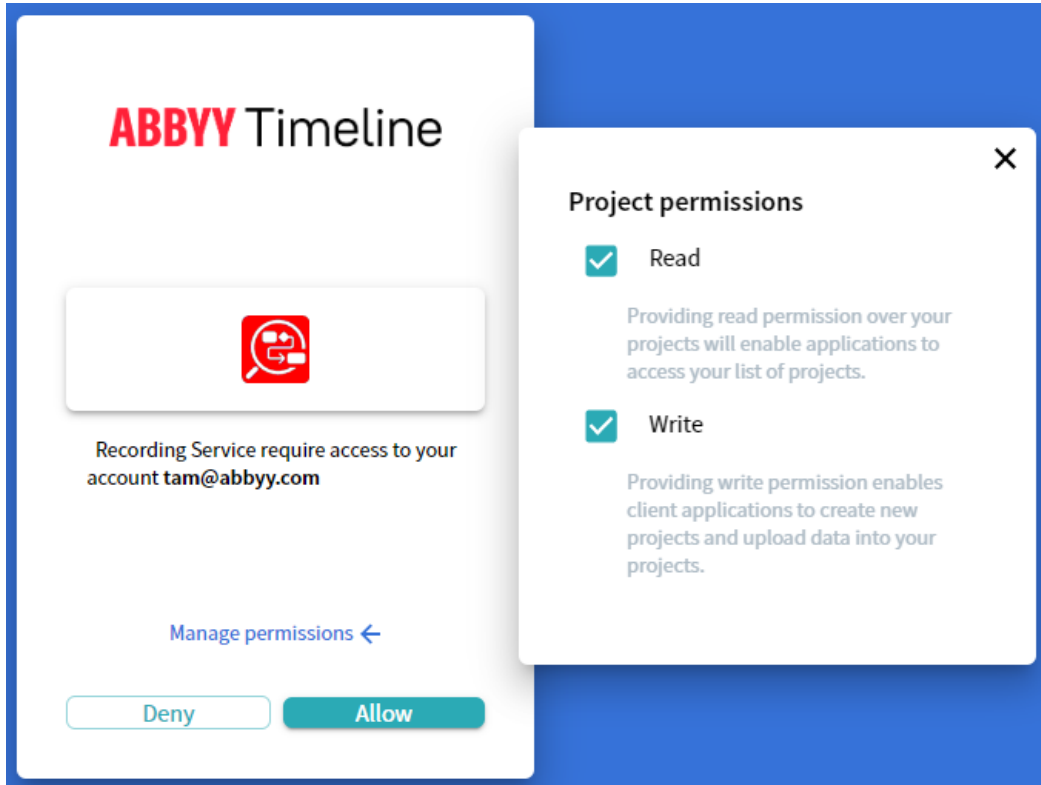
3. Upload logs to Timeline from Recording Service. To do this:

   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 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.

4. 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.

5. 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.

Getting Started with Process Analysis

Timeline Process analysis uses digital footprints and logs so that you can examine your company's performance metrics and business processes in real time and zoom into individual stages. For example, you can find out the average time it takes to have a document approved by your Accounts Payable, or see if a required step has been accidentally skipped when paying an invoice. Process analysis gives you a complete picture of the workings of your business and enables you to predict process outcomes and assess the potential benefits of automation.

Important. Recording Service is not required to use Process Analysis features. All analysis modules are located on the Timeline website. Here you will find such new features as **Simulation** and **Process view**. Only CSV files are accepted as input.

For detailed instructions on how to start analyzing your business processes, see Timeline user's guide > 'Process Analysis project' section.

System Requirements and Prerequisites

Important.

- Recording Service and Timeline must be installed on separate computers.

- The user workstations installing the Recorder, and the server hosting the Recording Service must all be members of the same Active Directory domain. Please refer to the "Configuring Active Directory Groups to Connect Recording Service with Recorders 33 " section for details.

- Recording Service performance may vary depending on the hardware configuration. If you intend to use more than 20 Recorder instances, store PostgreSQL databases partially or fully on the SSD for better performance. For details see "How to move database tables with screenshots to a new hard disk 41 ".

Timeline

Operating system	Microsoft® Windows Server® 2019 Version 1809 (OS Build 17763.2565) or later
CPU	4 cores or more
RAM	16 GB or more
HDD	512 GB or more Depends on the actual amount of data loaded into the application. Production environment may require more disk space, depending on the actual volume of data loaded into the application.
Browser (to access the ABBYY Timeline website)	• Google Chrome 109 or later • Microsoft Edge 109 or later
Additional software	• Microsoft Windows Subsystem Linux If this Windows feature is disabled, the ABBYY Timeline Setup will prompt you to enable it. After that, you will need to restart your computer to apply the changes.

| | • Redis 5 for Linux
ABBYY Timeline uses Redis for Linux therefore additional software is needed. Please, download the following installation packages into the same folder:

   o Linux Ubuntu 20.04
     (CanonicalGroupLimited.UbuntuonWindows_2004.2021.825.0.AppxBundle)

   o gcc-10-base_10.3.0-1ubuntu1_20.04_amd64

   o libatomic1_10.3.0-1ubuntu1_20.04_amd64.deb

• Microsoft .NET Framework 4.5*[20]

• PostgreSQL 12.*[20]

• NodeJS 16.15*[20]

• Python 3.8.10. (64-bit)*[20]

• Microsoft Visual c++ 2015-2019 Redistributables (x64)*[20]
• GraphViz 2.49.0*[20]
• SMTP Server
ABBYY Timeline needs access to a running SMTP server to be able to send verification emails, notifications, invitations, and alerts, etc. |
| Other requirements | • To install ABBYY Timeline on Windows successfully, make sure the user you are installing under is able to set the **PowerShell Execution Policy** to **RemoteSigned**. For details, see Installing Timeline [24].

• Obtain Twilio account
You need to have a configured Twilio account if you want to enable SMS notifications feature in Timeline. |

* included with the ABBYY Timeline installer.

Scaling guidelines

The exact calculation of necessary hardware requires multiple parameters such as data volume and use patterns. However, the general guidelines could be defined as following:

- If the number of concurrent users is less than 10 and the data update frequency is one per day or less, a single server should be sufficient.

- For more users or more frequent data updates, a separate server for DBMS is recommended.

- For the fault-tolerant environment, use two identical servers and any standard load balancer.

Recording Service

Operating system	Microsoft® Windows Server® 2016, 2019, 2022
Additional software	- Microsoft® Internet Information Services (IIS) 8.5[*] [22] - ASP.NET Core Hosting Bundle 6.0.12[*] [22] Recording Service requires 6.0.12 and later as part of a minor update, version 7.0.* is not supported. - PostgreSQL v. 12 or later[*] [22]
Browsers (to access the Recording Service website)	Google Chrome 109 or later
Hard disk requirements	Recording Service performance may vary depending on the hardware configuration. If you intend to use more than 20 Recorder instances, store PostgreSQL databases partially or fully on the SSD for better performance. **Important**. Only the database table with screenshots is allowed to be moved to the new hard disk. For details see "How to move database tables with screenshots to a new hard disk [41]".

Other requirements	1. The Recording Service works with Timeline 6.0
	2. Windows authentication is used to authorize the connection between the Recording Service and the Recorder instances installed on users' workstations. Configure Active Directory Groups you plan to use to connect Recording Service with Recorders in advance. Please refer to the '[Configuring Active Directory Groups to Connect Recording Service with Recorders](#) 33' section for guidelines.

* included with the Recording Service installer.

Hardware configuration example

If recording is done for 10 employees during 4 weeks (1 person generates approximately 5000 UI events per day):

- Operating system: Windows Server 2019

- CPU: 8 cores or more

- RAM: 16 GB or more

- Hard disk space: 256 GB HDD/SSD

- Logs with screenshots require at least 200 GB

Recorder

Operating system	Microsoft® Windows 10 (x64), 11 (x64)
	Microsoft® Windows Server® 2016, 2019, and 2022 **Important**. It is allowed to install Recorder on Microsoft Windows Server 2016, but correct log recording is not guaranteed.
Additional software	- Microsoft .NET Framework 4.6.2[*](#) 23 - Microsoft .NET 6.0.12 and later[*](#) 23

Browser (to record user activities)	- Browser Google Chrome 109 or later
	  Important. The following versions are not supported:
	  o Google Chrome Portable

	o Google Chrome Standalone for one user o Google Chrome Standalone for multiple users • Microsoft Edge 109 or later • Mozilla Firefox 109 or later (Limited support. See [Known Issue] 74 for details) **Important**. Mozilla Firefox ESR is not guaranteed to fully work.
Other requirements	1. Recorder works with Recording Service that comes with Timeline 6.0. 2. Windows authentication is used to authorize the connection between the Recording Service and the Recorder instances installed on users' workstations. Configure Active Directory Groups you plan to use to connect the Recording Service with Recorders in advance. Please refer to the '[Configuring Active Directory Groups to Connect Recording Service with Recorders] 33' section for guidelines.

* included with the Recorder installer.

Installation, Removal and Upgrade

This section provides instructions for installing the ABBYY Timeline components, upgrading, and removing them from your computers.

ABBYY Timeline

This section contains information about installing and removing ABBYY Timeline.

Important. The ABBYY Timeline installer does not have a repair mode. Please do not edit/delete anything in the installation folder unless you have received clear instructions on what to do. In case you deleted something from the installation directory by accident, you will have to uninstall, then re-install ABBYY Timeline.

If you are going to use ABBYY Timeline in the cloud, please skip this chapter.

Installing Timeline

Before you begin

1. Log in as a Windows administrator or start Timeline Setup with **Run as Administrator**. To perform all activities below, you must be a system administrator of the computer on which Timeline is being installed.

2. Ensure the **Execution Policy for PowerShell** is set to **RemoteSigned**. To verify the current settings for the execution policy:

   a. Start Windows PowerShell with **Run as Administrator**

   b. Use **Set-ExecutionPolicy RemoteSigned** to set the policy to **RemoteSigned**.
   If the command was executed without errors, go to the Timeline installation procedure by starting the Timeline installer with Run as Administrator.
   If you get an access is denied error, you do not have the permissions to change the execution policy. Please contact your system administrator to have your permissions changed.

Interactive installation

Run the **ABBYY-Timeline-<version>-installer.exe** file, select the language to run the Installation Wizard and follow the on-screen instructions.

The Installation Wizard will display a sequence of pages with detailed instructions for each installation step. Use the **Back** and **Next** buttons to navigate the pages. To quit the Installation Wizard at any stage, click **Close**.

1. **License Agreement**
   Read and accept the license agreement.

2. Check and install prerequisites
   Timeline Setup checks third-party applications that are required to configure and operate ABBYY Timeline. Some of the applications you must download and install manually. If your computer meets the system requirements, the steps described in this paragraph will not display.

   a. **Enable Windows Features**
      If the **Microsoft Windows Subsystem Linux** feature is disabled, the Timeline Setup will prompt you to enable it. After that, your computer will be restarted automatically. Please save your work before continuing the installation. After restarting, the Timeline installation will be auto-resumed. If it doesn't run automatically, please run the **ABBYY-Timeline-<version>-installer.exe** file again.

   b. **Redis installation**

      i. Download the following installation packages into the same folder:
         - [Linux Ubuntu 20.04](#)
         (CanonicalGroupLimited.UbuntuonWindows_2004.2021.825.0.AppxBundle)
         - [gcc-10-base_10.3.0-1ubuntu1_20.04_amd64](#)
         - [libatomic1_10.3.0-1ubuntu1_20.04_amd64.deb](#)

      ii. **Source Folder**
         Specify a folder where you renamed the packages specified above.

      iii. **Ubuntu Installation Folder**
         Specify a folder where Ubuntu will be extracted to. The default folder is:
         C:\Program Files (x86)\Ubuntu

3. **Installation Folder**

Select a destination folder where Timeline will be installed.

The default folder is: C:\Program Files\ABBYY Timeline

4. **Select Database**

Timeline needs access to PostgreSQL. You can install PostgreSQL on a computer along with Timeline or a separate one.

If you already installed PostgreSQL on another computer, select **Connect to existing database**. This option is useful if you install the program in a production environment where the host machine is accessible from outside the corporate network. If you prefer to keep Timeline and the database on the same machine, select **Install local database**. This option is useful if you install the program for testing purposes.

Go to the next step to specify database connection settings.

5. **Database Connection**

Specify connection parameters to Timeline databases located on a local or remote PostgreSQL.

a. **Install local database**

If you selected this option, you need to configure access to a local PostgreSQL instance. To set up access to an existing PostgreSQL instance, go to step 5b below 27 . Using the options specified in this clause, Timeline Setup creates the following databases during the installation process:

timeline - the Admin database. It contains all information about users, their activity, and projects.

timeline-log - the Log database. It contains detailed records of Timeline events such as security, errors, and notifications.

timeline-000 - the User database. It contains information about user repositories.

i. **PostgreSQL user** and **PostgreSQL password**

Provide PostgreSQL superuser credentials. These will be used by the installation program to create a database user for Timeline.

ii. **PostgreSQL port**

Specify TCP/IP port for PostgreSQL. By default, TCP/IP port **5432** is used. Make sure that it is not being used by any other application. For more information, see the Check TCP/IP port availability 63 section.

iii. **Data directory**

Enter the path where the database needs to be installed.

The default path is: C:\Program Files\PostgreSQL\12

b. **Connect to existing database**

If you selected **Connect to existing database** in step 4, this means PostgreSQL is already installed on a remote or local server. To create and configure access to the Timeline databases, specify connection parameters for the Admin, Log, and User databases.

Note. If the Timeline databases already exist on the specified PostgreSQL server and the PostgreSQL version is supported, the **Review Database Configuration** step will open. Select **Connect to the existing Timeline database** if you want ABBYY Timeline to connect to the detected database. Otherwise, select **Reinstall Timeline database tables and user**. In this case, the installer will delete the detected databases and install new ones.

i. **PostgreSQL user** and **PostgreSQL password**

Provide the credentials of the PostgreSQL user who will own the Timeline databases. For example, **TimelineUser**.

ii. **PostgreSQL host**

Specify the server name where PostgreSQL is installed. By default, **localhost** is used.

iii. **PostgreSQL port**

Specify TCP/IP port for PostgreSQL. By default, TCP/IP port 5432 is used.

iv. **Database name**

A name must be given for each database:

timeline is the only valid name for the Admin database.

timeline-log or **timeline_log** is the only valid name for the Log database.

timeline-000 or **timeline_000** is the only valid name for the User database.

v. Select **Use SSL for the database connection**, if your PostgreSQL is configured with SSL support.

If your PostgreSQL is configured with SSL support and a CA Root certificate file is used, provide the full path to the CA Root certificate file.

6. **Admin User Account**

Create a first admin user account for ABBYY Timeline. Enter a valid email address using an existing domain name that is configured to receive emails, for example, **user@domain.com**, and a password. This will be the first user and the one that will have access to the ABBYY Timeline website, where other users can be administered.

The password you specified must contain only English letters and digits from 0 to 9. It must be at least eight characters long, contain at least one uppercase letter, one

lowercase letter, and one number.

Important. It is this user who will have a super admin role and have access to the Admin app. Once the installation is complete, you can log into the Admin app via the Timeline website.

7. **Mail Server Configuration**

   Configure the SMTP server access to allow Timeline to send out emails in several features such as Alerting, User invitation, Email verification, etc. For example, during a user registration process, a verification email message is sent to the user. The user won't be able to use Timeline until he completes the instructions contained in the message. Provide general information to configure SMTP mail server and specify its security options. To decide which options you have to select, please refer to the documentation of your mail server. The server's basic settings are set during installation. You can change the SMTP Mail Server configuration after installation.

   a. **Mail server host**

      Enter server name where the SMTP mail server is installed.

   b. **Mail server port**

      Enter the SMTP mail server port number.

   c. **Mail server username** and **Mail server password**

      Enter the SMTP mail server access credentials. Keep these fields empty if your mail server requires no authentication.

   d. **Email sender**

      Enter the e-mail sender address used to fill the 'From' header field of e-mails.

   e. **Mail server security**

      Specify mail server security options. To decide which option you have to select, refer to the documentation of your mail server. Mail server basic settings are set during installation. You can change the SMTP Mail Server configuration after installation. For more information, see 'Change SMTP Mail Server Configuration' 67.

      i. Select **Non secure** in case your SMTP server does not use TLS. This is a typical use case for mock, local mail services, for example, mailcatcher.

      ii. Select **Require TLS after connection** if the initial connection should happen over an unencrypted connection and then the STARTTLS command should be used to upgrade to a secure connection. For example, Microsoft Exchange.

    iii. Select **Secure from the start of the connection** then the app will use TLS to connect to the SMTP server from the start. It is the most secure option, however not all mail servers support this option.

    iv. Select **Allow self-signed certificate** if your mail server uses an unauthorized, e.g., self-signed, SSL certificate.

8. **Timeline Base URL and Ports Configuration**

    a. Enter the **Base URL** that hosts Timeline and via which users will be able to access the Timeline website.
Base URL must be a fully qualified URL. The lowercase pattern is recommended. Do not use extra spaces and forward slash '/' at the end of the base URL. It should match the computer name on which you are installing Timeline and must be accessible both from the computer on which Recording Service is installed and from the administrator browser. It also is used for links inside email messages sent by the Timeline.

The Base URL must have the following syntax: `http[s]://hostname:port`
If you are using the default port (80 or 443), you do not need to add them to the base URL

Examples:
The base URL of the HTTP endpoint, if a custom port is specified:
`http://mytimeline.com:8080`
The base URL of the HTTPS endpoint, if a custom port is specified:
`https://mytimeline.com:30443`

    b. Specify TCP/IP port for the Timeline website.
By default, TCP/IP port 80 is used for the Timeline website. Make sure that it is not being used by any other website. For more information, see the 'Check TCP/IP port availability [63]' section. You can also set a different port number later [66].

Select **Use HTTPS** if you want to secure data transferred, and then go to the next step to set the SSL connection settings.
Note. Currently, Timeline does not accept .pfx files. In case you have a .pfx file, you should convert it to .key and .cert files. The key and certificate files must be named **server.key** and **server.cert** since Timeline accepts only files with these names.

Important. If you install the program in a production environment, it is strongly recommended to use HTTPS and highly discouraged HTTP.

9. **Service Setup**

   Current user account is used to run the **timelinepi** service. If the computer is a member of an Active Directory domain, the current domain user account will be set to run the service. If the computer is part of a workgroup, the local computer account will be set. For the service to work properly, specify the valid password for the user account used to install Timeline.

   Important. It is prohibited to change the specified user account after the installation is completed.

10. SMS Sender

    Configure Twilio SMS service to receive SMS notifications from Timeline containing verification codes, alert notifications, and error messages.
    Important. Twilio account is required to configure and send SMS notifications.

    a. **Account SID**

       This line contains a Twilio String Identifier (SID), a unique key that is used to identify your Twilio account

    b. **Auth token**

       Enter your Auth token, generated for your Twilio account.

    c. **Phone number**

       Enter the phone number from your Twilio account. It will be the sender's number.

11. Create firewall exceptions after installation is complete

    Installer does not create any software or hardware firewall exceptions. You must set up exception settings to allow interactions between components to take place inside a network. For example, you create inbound and outbound rules in Windows Firewall. For detailed information, see '[Network connection settings](#) 64'.

Performing health check

Check that Timeline is working properly by doing the following:

1. Open a browser and enter **{timelineURL}:{port}** in the address bar, where:
   {TimelineUrl} is the Base URL you specified during the Timeline installation or the public IP address or the full name of the computer on which Timeline is installed.
   {port} is a custom port assigned to Timeline website during the installation process. If you are using the default port (80 or 443), you do not need to add them to the {**timelineURL**}. By default, TCP/IP port 80 or 443 is used.

Example: http://mytimeline:8080 or https://mytimeline:30443

2. If the installation was carried out correctly, the Timeline website will open.

3. Login using the Timeline admin credentials you specified in [the 'Admin User Account' step] 27 during the Timeline installation process.

Upgrading Timeline

If you own ABBYY Timeline 5.3 or later, you can upgrade to ABBYY Timeline 6.0. This means that you can install a new version of ABBYY Timeline and your databases will be maintained.

Before you begin

We recommend you backup the Timeline database. To do this, use PostgreSQL utilities. It includes utilities that allow you to make backups. These are **pg_dump**/**pg_dumpall** and **pg_basebackup**. For detailed information, refer to https://www.postgresql.org/docs/12/backup.html or [PostgreSQL Databases Backup and Restore] 52 section.

Basic steps

1. Run the **ABBYY-Timeline-6.0.*-installer.exe** file to start the Installation Wizard.

2. In the program dialog box, select **Update** and follow the instructions of the Installation Wizard.
   Important. Upgrading within the same version is not supported.

3. After the installation process is complete, you need to rebuild all old Task Mining projects so that they are available to work in Timeline 6.0.
   For detailed instructions on rebuilding of the existing Task Mining project, see below.

If you can't upgrade ABBYY Timeline using the Setup, perform the following steps:

1. Uninstall your ABBYY Timeline

   ▪ If you uninstall ABBYY Timeline 4.8, your databases are maintained while uninstalling, but the previous settings are removed.

   ▪ If you uninstall ABBYY Timeline 4.11 or later, you will be asked whether you want to uninstall the product completely or maintain the databases.

2. Run the **ABBYY-Timeline-6.0.*-installer.exe** file and follow the on-screen instructions in the Installation Wizard.

3. Perform a health check 30.

How to Rebuild on the existing Task Mining project

1. Open a browser and enter **{timelineURL}:{port}** in the address bar, where:
   {TimelineUrl} is the Base URL you specified during the Timeline installation or the public IP address or the full name of the computer on which Timeline is installed.
   {port} is a custom port assigned to Timeline website during the installation process. If you are using the default port (80 or 443), you do not need to add them to the {**timelineURL**}. By default, TCP/IP port 80 or 443 is used.
   Example: http://mytimeline:8080 or https://mytimeline:30443

2. Login using the Timeline admin credentials you specified in the 'Admin User Account' step 27 during the Timeline installation process.

3. Click your user avatar at the bottom of the left bar, then select **Open Admin app**.
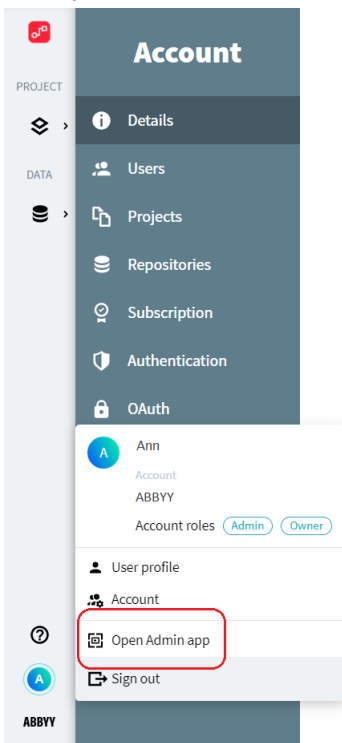
4. In the **Admin** app, go to the **Project** tab and click **Rerun all task mining cutting**.
   Important. Please do not refresh or close this browser page until the process is finished.

Uninstalling Timeline

1. Run the **ABBYY-Timeline-6.0.*-installer.exe** file to start the Installation Wizard.

2. In the program dialog box, click **Uninstall ABBYY Timeline**.

3. In the next dialog box specify whether you want to uninstall the product completely or maintain the databases for future use (e.g., if you choose to install a newer version).

   ▪ If you want to remove the Timeline product completely, including the databases, select **Delete ABBYY Timeline database and data folder** and provide PostgreSQL superuser credentials.

   ▪ If you want to uninstall the Timeline product while keeping the databases, proceed to the next step.

4. Click **Uninstall** to start the removal process.
   While product removal is still in progress, you have the option of canceling it by clicking **Cancel**.

5. Once the product is removed from your system, click **Finish** to close the Installation Wizard.

Configuring Active Directory Groups to Configure Access to Recording Service

Active Directory security groups provide access control to Recording Service:

- Recording Service collects data from Recorders that are running on workstations. The access of workstations to Recording Service is controlled via domain groups.

- User permissions on the Recording Service website are managed via domain groups as well.

Groups must be created prior to installing Recording Service.

Below you will find detailed information about Active Directory security groups:

- All computers on which Recorder and Recording Service is to be installed must be members of the same Active Directory domain.

- Create the following groups in Active Directory and add user accounts to them, which will be used to work with Recording Service and Recorder.
  Note. You can use an existing security group or create the following security groups in Active Directory.

  o Recording Service admin group (e.g. **Domain\RS-admins**)
    Assign this group full control over the Recording Service web application. Then add user accounts to the group to grant them admin access to the Recording Service website.

  o Recording Service user group (e.g. **Domain\RS-users**)
    Assign this group limited control over the Recording Service web application. Then add user accounts to the group to grant them user access to the Recording Service website. Users added to this group will not be able to change authentication settings and some security settings that are related to users and sensitive information.

  o Recorder user group (e.g. **Domain\Recorder-users**)
    Assign this group write access over Recording Service. Then add user accounts to the group to grant their Recorder instances write access to the Recording Service website. This will allow Recorder instances to send logs to Recording Service.

Specifying Active Directory Groups when installing Recording Service

When installing Recording Service, in the **Active Directory Security** 37 step, specify the names of the configured groups in the related setup fields. The name must be in the format:
Domain\Group Name

1. **RS admin**
   Enter here the name of the Recording Service admin group, for example, **Domain\RS-admins**

2. **RS user**
   Enter here the name of the Recording Service user group, for example, **Domain\RS-users**

3. **Recorder user**
   Enter here the name of the Recorder user group, for example, **Domain\Recorder-users**

Can I specify existing AD groups?

For testing purposes or in case do not have Active Directory, you may specify for:

- **RS admin** and **RS user** - local admins' user account(s)

  o Domain user
  Format: **Domain\UserName**

  o Local group or user
  Format: **ComputerName\GroupName** or **ComputerName\UserName**
  To display the computer name, open the **Command Prompt** (**Start** > **Run** > **cmd**) and type **hostname**.
  Note. You may create a local group, add domain users or groups to it, and specify this group to the **Admin AD Security group** field.

- **Recorder user** - Everyone
  Allows any Recorder instances installed in the domain to send logs to Recording Service.
  Format depends on your Windows locale, for example, in English: **Everyone**

How to find out which Active Directory groups in different languages you are a member of

1. Open the **Command Prompt** (**Start** > **Run** > **cmd**)

2. Use **whoami /groups**
   This command will list distribution groups and nesting.

Can I change the specified groups after Recording Service is installed?

You can change Active Directory Security Groups configuration after the Recording Server and Recorder installation. For more information, see the "How to Change AD Security Groups that Have Access to Recording Service Resources⌐70⌐" section.

ABBYY Recording Service

This section contains information about installing and removing Recording Service.

Installing Recording Service

Interactive installation

Run the **ABBYY.RecordingService.\<version\>.exe** file, select the language to run the Installation Wizard and follow the on-screen instructions in the Installation Wizard:

1. **License Agreement**
   Read and accept the license agreement.

2. **Destination Folder and Port Configuration**
   Specify installation folder and TCP/IP port to be used the Recording Service website:

   a. **Folder path**
      Specify a folder where Recording Service should be installed. The default installation folder is:
      C:\inetpub\ABBYY Recording Service

   b. **Web site port**
      Specify TCP/IP port to be used by the Recording Service website or keep the default value.
      By default, the following TCP/IP ports are used:

      - 443 (if use HTTPS)
        For setting up HTTPS you will be asking for the SSL certificate and the private key.

      - 80 (if use HTTP)
        The Default Web Site is running on port 80. If you plan to use port 80 for the Recording Service website, you may need to modify this port from 80 to a different one in the Internet Information Services (IIS) Manager.

        Make sure that specified port is not being used by any other application. In the event of port conflict, an alert will be displayed. Change the port number to continue. For more information, see the '[Check TCP/IP port availability](#) 63' section. You can also set a different port number for the Recording Service website later. To do this, change the port number in the Internet Information Services (IIS) Manager.

        Note: If you install the program in a production environment, it is strongly recommended to use HTTPS and highly discouraged HTTP.

3. **Active Directory Security Groups**

Specify the names of the Active Directory Security groups you configured before installing Recording Service. By specifying the AD groups to which you add users, you determine the user's role and access rights in Recording Service.

Please refer to the 'Configuring Active Directory Groups to Connect Recording Service with Recorders 33' section for guidelines.

You can change AD Security Groups configuration later. For more information, see the 'How to Change AD Security Groups that Have Access to the Recording Service Resources 70' section.

4. **PostgreSQL Database Options**

Recording Service needs access to the PostgreSQL database. You can install PostgreSQL on a computer along with Recording Service or a separate computer.

If you already installed PostgreSQL on another computer, select the **Connect to remote / another preinstalled version of PostgreSQL database**. Otherwise, select **Install PostgreSQL on this machine**.

Note. If PostgreSQL 12 is already installed on the current computer, instead of the **PostgreSQL Database Options** step, the **Database Connection** step will open. In this step, you need to specify the settings for connecting to the database.

a. **Install PostgreSQL 12 on this machine**

Allows you to install PostgreSQL and database on the local machine.
Go to the next step to specify PostgreSQL accounts and port to install PostgreSQL locally.

i. **Super user account**

1. Enter the PostgreSQL superuser credentials and the PostgreSQL port number. These credentials will be used by the installation program to create a database user for Recording Service.
Important. The PostgreSQL superuser name may contain only English letters and digits from 0 to 9 and may not include any of the following characters: - \ / : *? " < > |

2. Specify TCP/IP port for PostgreSQL. By default, TCP/IP port **5432** is used. Make sure that it is not being used by any other application. For more information, see the 'Check TCP/IP port availability 63' section.

ii. **Service account**

Specify the account used to start the PostgreSQL service. By default, the

PostgreSQL service runs under the **Network Service** account. To change the default account, select **Specify service account credentials** and enter other existing credentials for running the PostgreSQL service. Please make sure that the correct values are entered. Incorrect user credentials (e.g. a typo in a username) will cause a service start error.

Important. The account you specified must be granted the **Log on as a service** privilege.

i. **Port**

Specify CP/IP port for PostgreSQL. By default, TCP/IP port **5432** is used. Make sure that it is not being used by any other application. For more information, see the [Check TCP/IP port availability](#) 63 section.

ii. Go to the next step to specify PostgreSQL destination folders:

1. **Installation Directory**

PostgreSQL will be installed into the specified folder. The default installation folder is:

C:\Program Files\PostgreSQL\12

Important. The Installation directory must be empty.

2. **Data Directory**

Enter the path where the database needs to be installed.

The default path is: C:\Program Files\PostgreSQL\12\data

3. Go to the next step of the Installation Wizard to specify PostgreSQL database name and user that will work with Recording Service and database.

b. **Connect to remote / another preinstalled version of PostgreSQL database**

Allows you to specify connection settings to the existing database.

Go to the next step to specify database connection configuration.

During the installation of Recording Service, a shortcut to the Recording Service website is added to the Start menu.

Important. If you are using a software or hardware firewall, make sure that the configured ports are open in your firewall. For default network connection settings see '[Network connection settings](#) 64' section.

Recording Service performance may vary depending on the hardware configuration. If you intend to use more than 20 Recorder instances, store PostgreSQL databases partially or fully on the SSD for better performance. For details see "[How to move database tables with screenshots to a new hard disk](#) 41".

Performing health check

To perform a health check on Recording Service:

1. Go to **Start** menu > **ABBYY Recording Service**
   Recording Service website will open in your browser.

2. If Recording Service has been installed correctly, you will see the Recording Service Site with the default template.

Upgrading Recording Service

If you own Recording Service that comes along with ABBYY Timeline 5.3 or later, you can upgrade to Recording Service comes along with ABBYY Timeline 6.0. This means that you can install a new version of Recording Service, and your databases and logs will be maintained.

Before you begin

It is recommended that you backup your Recording Service database before you perform the upgrade. To do this, use PostgreSQL. It includes utilities that allow you to make backups. These are **pg_dump/pg_dumpall** and **pg_basebackup**. For detailed information, refer to https://www.postgresql.org/docs/12/backup.html or see 'PostgreSQL Databases Backup and Restore ⌐52⌐'.

Basic steps

1. Run the **ABBYY.RecordingService.<version>.exe** file to start the Installation Wizard.

2. Follow the instructions of the Installation Wizard.
   Important. During the upgrade process in the Active Directory security step specify the group for the Recording Service users. This group should contain users of the Recording Service. For more information see Active Directory groups and users roles, see Configuring Active Directory Groups to Configure Access to Recording Service ⌐33⌐.

The upgrade is performed by removing the old version while maintaining all the settings, databases, and logs from the previous version. In this case the installation of the new version is performed in silent mode. Go through all the steps of the Installation Wizard, and click **Uninstall** in the last step to to complete the upgrade process.

If you can't upgrade Recording Service using the setup, perform the following steps:

1. Uninstall your Recording Service.
   Your database is maintained while uninstalling.

2. Run the **ABBYY.RecordingService.<version>.exe** file to start the Installation Wizard.

3. Follow the instructions of the Installation Wizard.

4. To connect to the existing database, you must provide existing values in the **Database Connection** step.

   a. **User login** and **User password**
      Specify PostgreSQL superuser credentials.

   b. **Server name**
      Specify the server name where PostgreSQL is installed.

   c. **Port**
      Specify TCP/IP port for PostgreSQL.

5. In the **Create Database** step specify:

   a. **User to create**
      It is a username that will be used for interaction between Recording Service and the PostgreSQL database.
      Important. During every new installation, you must specify a new username.

   b. **Database name**
      Specify a database name. Installer will assign the database to the specified user.
      Note. If you enter the name of a non-existent database, the installer will create a new database with the specified name.

Uninstalling Recording Service

1. Open **Control Panel** -> **Programs** -> **Programs and Features** and select **ABBYY Recording Service**.

2. Click **Uninstall**.

3. In the Installation Wizard select **Uninstall** and follow the instructions of the Wizard.
   Note. Your database and recorded logs are maintained while uninstalling.

How to Move Database Table with Screenshots to a New Hard Disk

Recording Service performance may vary depending on the hardware configuration. If you intend to use more than 20 Recorder instances, store PostgreSQL databases partially or fully on the SSD for better performance.

Important. Only the database table with screenshots is allowed to be moved to a new hard disk.

To do it, when the Recording Service installation or upgrade is complete, perform the following steps:

1. Create a folder on HDD, e.g., *D:\PostgresData*

2. Provide full access to this folder to account is used to run PostgreSQL service.
   The default account is: *NT AUTHORITY\NetworkService*

3. Perform as superuser the following actions on your PostgreSQL instance:

   a. Register a new tablespace to define an alternative location on the file system where the data files containing database tables and indexes will reside.
   To do this, run the command:
   CREATE TABLESPACE tablespace_name LOCATION 'directory';
   Example:
   CREATE TABLESPACE slow_large_disk LOCATION 'D:\PostgresData';

   Note. Skip this step if you register a new tablespace for the Recording Service 5.3 screenshots.

   b. Change the screenshot table's tablespace to the specified tablespace and move the data file(s) associated with the table to the new tablespace.

   ALTER TABLE "Blob" SET TABLESPACE new_tablespace;
   Example:
   ALTER TABLE "Blob" SET TABLESPACE slow_large_disk;
   Note. Even if you moved the Recording Service 5.3 Screenshot table, you need to repeat this step for the Recording Service 6.0 *Blob* table.
   Do not move the other tables' data files.

ABBYY Recorder

This section contains information about installing and removing Recorder.

Installing Recorder

Before you begin

Before you begin installing Recorder, pay attention to the following:

1. If you plan to record activities of users that work using Windows RemoteApp and Citrix Workspace App, install Recorder on a terminal server.
   ABBYY Recorder can be installed on the terminal server as if it was a workstation. It will log the actions of users connecting to this server via a Citrix client or RDP.
   Note. Recorder was tested with the following terminal server configurations:
   - a computer running under Microsoft Windows Server 2016 (Remote Desktop, RemoteApp and Remote Desktop Web Access).
   - Citrix Workspace App 7.

2. The user workstations installing the Recorder component, and the server hosting Recording Service must all be members of the same Active Directory domain.

3. Add the accounts of users on whose computers you intend to install Recorder to the Recorder writers Active Directory security group you configured before the installation 33.

4. If the appropriate browser extensions are not installed, user activities will not be recorded in Google Chrome, Microsoft Edge, and Mozilla Firefox.

5. The Firefox extension for Recorder has several limitations. For detailed information, please refer to the "Known issues" > "Recorder Firefox extension limitation 74" section.

6. A system reboot might be needed during the Recorder installation. Please save your work first, otherwise you may lose unsaved changes.

To install ABBYY Recorder, use one of the following methods:

- Interactive installation 43

- Command line installation 45

Interactive installation

Run the **Abbyy.Recorder.<version>.exe** file, select the language to run the Installation Wizard and follow the on-screen instructions in the Installation Wizard.

Note. ABBYY Recorder has two interface languages: English and Japanese. The Japanese interface is only available on operating systems with the Japanese locale enabled.

1. **License Agreement**
   Read and accept the license agreement.

2. **Application Folders**

   a. **Installation folder**
      Recorder will be installed into this folder. The default installation folder is:
      C:\Program Files\ABBYY Recorder

   b. **Data folder**
      Specify a local or network folder where the program will store its data. To keep data in **%appdata%\ABBYY\Recorder** folder, select **Use AppData folder**.
      Depending on the operating mode, which is set in the next installation step, different data are stored in the specified folder:

      i. When installed in **Standalone** mode, application logs and logs with recorded user activity are stored there.

      ii. When installed in **Server managed** mode, only application logs are stored there.

3. **Installation Details**

   a. **Tag**
      You may specify a tag. Tag is simply some text string that describes the current workstation with your Recorder instance. When installed in **Server managed** mode, tag is passed to Recording Service and helps the administrator identify a workstation in the Recording Service website. Username is not recommended as a tag because several users could occupy the same workstation.

      For example, you can specify the same tag when installing Recorder on several workstations, e.g., the 'accounting department' tag. Then you can easily find these workstations in the **Recorders** list on the Recording Service website by the 'accounting department' tag.

b. **Operation mode**

Select the Recorder operation mode:

i. **Standalone**

Standalone mode is useful for trial purposes. It has the following limitations:

- Forms are not detected.
Recorded logs are stored on users' computers and are not sent to Recording Service for processing, so there are no forms in these logs. If you plan to upload logs to Timeline for trial purposes, first open your logs in the Recorder Log Viewer utility. As a result, the forms will be detected automatically and the Forms folder inside your logs will be created. Next, to upload the processed logs to Timeline, follow the instructions in the Timeline guide, see 'Projects, Tools, and Data Analysis > Task Mining > Data Upload > Logs upload without Recording Service'.
Note. Forms are supported in Recorder Log Viewer 6.0 and later. The utility is installed with ABBYY Recorder set to the **Standalone** mode.

- Only passwords are encrypted in text logs, other text data are not encrypted, and data in screenshots aren't blurred.

When this mode is on:

- Recording control (start/stop) remains with the local computer.

- The logs with the recorded data are saved on the local computer.

- Setup installs the Recorder Log Viewer utility. The utility allows opening the logs recorded by the Recorder installed in **Standalone** mode.
For detailed information on usage of Recorder Log Viewer, see Recorder Log Viewer Guide.

i. **Server managed**

When this mode is on, the recording control (start/stop) can be performed from Recording Service. User activity logs are automatically saved to the server.
Specify the URL on which Recording Service is installed and accessible over Network.

4. **Installation Option**

Select browser extensions you want to install. Extensions allow Recorder to capture user actions in the Google Chrome, Microsoft Edge and Mozilla Firefox browsers.
Note. The Recorder Firefox extension has several features. Please refer to the 'Known issues' > 'Recorder Firefox extension limitation' 74 section for detailed information.

After Recorder is installed on users' computers, each user must enable extensions in browser. Below you will find instructions on how to enable the extension in <u>Google Chrome</u> 49 , <u>Microsoft Edge</u> 50 , and <u>Mozilla Firefox</u> 50 .

Note. If a user has just been added to the **Recorder user** 22 Active Directory group, you may need to restart the computer. This allows Recorder installed in the **Server managed** mode to connect to Recording Service.

Command line installation & Preventing End-Users from Controlling Recorder

Run the **Abbyy.Recorder.<version>.exe** file using the command line parameters described below.

Silent installation

To install Recorder in silent mode, use the following command line:
```
Abbyy.Recorder.<version>.exe /silent
```

For the command-line installation, use the following command-line options:

Option	Default Value	Description
/silent		Runs the installation in silent mode. In the case of silent installation, no setup dialog boxes are displayed, and the program is installed in default configuration.
/passive		Runs the installation with the progress bar only to be displayed. No other dialog boxes will be displayed.
installDir=<path>	C:\Program Files\ABBYY Recorder	The path to the folder where Recorder will be installed.
DataPath=<path>	%appdata%\ABBYY\Recorder	Folder where the program will store its data. Depending on the operating mode,

Option	Default Value	Description
		different data are stored in the specified folder: • If you specify **ServerUrl** ⌐47⌐ value to install Recorder in **Server managed** mode, only application logs are stored there. • If you install Recorder in **Standalone** mode, application logs and logs with recorded user activity are stored there.
Tag=<tag>		Tag is simply some text string that describes a workstation or a group of workstations. No tag is added by default. When installed in **Server managed** mode, tag is passed to Recording Service and helps the administrator identify a workstation in the Recording Service website. Username is not recommended as a tag because several users could occupy the same workstation. For example, you can specify the same tag when installing Recorder on several workstations, e.g., the 'accounting department' tag. Then you can easily find these workstations in the **Recorders** list on the Recording Service website by the 'accounting department' tag. **Note**. During the upgrade process, the Recorder installer maintains all your previous settings. This means that if you specify a new tag, it will not change on the recording service website. To change it:

Option	Default Value	Description
		1. Open the Recording Service website and go to the **Recorders** tab. 2. Select a recorder and click **Set tag**. 3. In the window that opens, enter a new tag and click **Save**.
ServerUrl=<server URL>		Turns the **Server managed** on. Specify the URL where Recording Service is installed and accessible over Network. If this option is not specified, the default installation is in **Standalone** mode.
ChromeExt=<true|false>	true	Installs Recorder Chrome extension.
EdgeExt=<true|false>	true	Installs Recorder Edge extension.
FirefoxExt=<true|false>	true	Installs Recorder Firefox extension. **Important**. • The Recorder setup can install the Recorder Firefox extension only under a current user account. How to solve this issue see 'Known Issues' > Recorder Firefox extension limitation 74 section. • The Recorder setup cannot remove the Recorder Firefox extension. Each user must remove the Recorder Firefox extension from Mozilla Firefox manually. For more information, see the 'How to Uninstall Recorder Firefox Extension 52' section.
ControlButtonsVisible =<true|false>	true	Specifies the mode where most of the standard UI is turned off.

Option	Default Value	Description
		Recorder offers a custom UI option as an alternative to the classic UI. It removes the **Enable**/**Disable** buttons from the Recorder UI when it is installed in **Server managed** mode. **Important**. It is highly discouraged to install Recorder with custom UI in production environment. For detailed instructions on installing Recorder with custom UI, see below.

Installing Recorder with custom UI to prevent End-Users from Controlling Recorder

Recorder offers a powerful security feature that allows users to disable when Recorder is recording their desktop activity. There are however some cases when the recording process needs to be managed only by the administrator through Recording Service thereby preventing the end user from turning Recorder on or off. For such cases, Recorder offers a custom UI option as an alternative to the classic UI. It removes the **Enable**/**Disable** buttons from the Recorder UI when it is installed in **Server Managed** mode. To use this option, all Recorders need to be installed in silent mode using the command line installation using the parameter **controlButtonVisible = false**. The **controlButtonVisible** parameter specifies the mode where most of the standard Recorder UI is turned off, preventing the user from controlling when Recorder is on or off.

Example: `Abbyy.Recorder.<version>.exe /silent installDir="C:\Recorder" DataPath="C:\Data" Tag="RecorderWorkstation1" ServerUrl="https://myrecordingservice.com/" FirefoxExt=false ControlButtonsVisible=false`

This command installs Recorder to the **C:\Recorder** folder in **Server managed** mode with the following settings:

- The **Enable/Disable** buttons are removed from the Recorder UI. Only the administrator has privileges to control the recording process through the Recording Service website.

- The Recorder Chrome and Edge extensions will be installed. The Firefox extension will not be installed.

- Program logs will be stored in the **C:\Data** folder.

- Logs of user activity will be sent to Recording Service hosted at **https://myrecordingservice.com/**.

How to Enable Chrome Extension

To turn on the ABBYY Recorder Chrome extension, carry out the steps listed below on the workstations.

Important. An internet connection is required on workstations.

1. Open or restart **Chrome**.

2. Click the menu button, click **More tools**, and then click **Extensions**.
   The **Extensions** page appears.
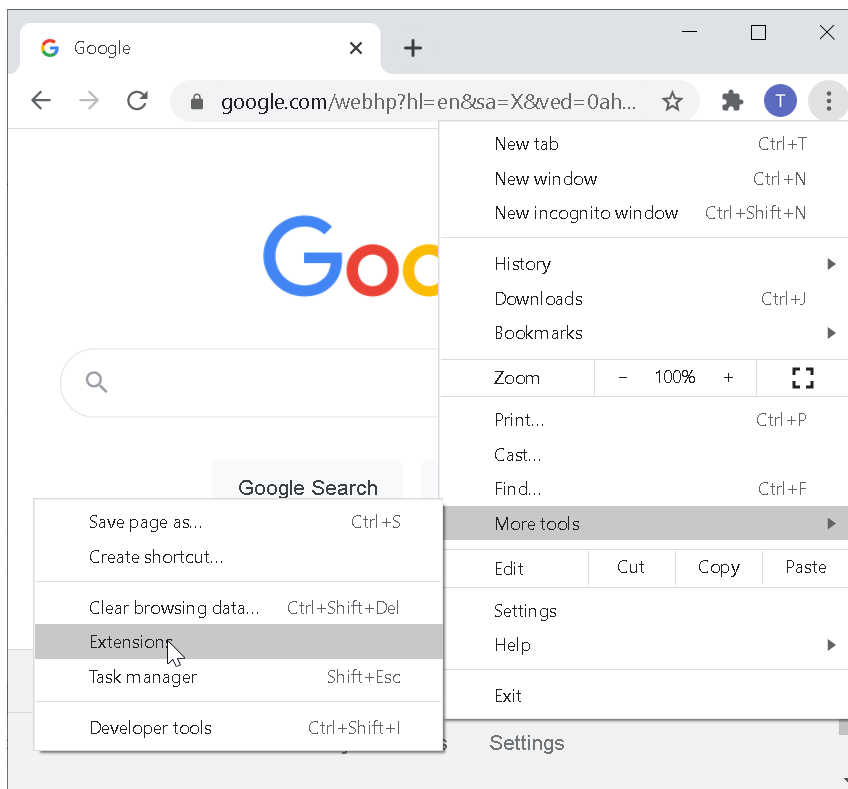
3. Find the **ABBYY Recorder** extension in the list and select the **Enable** check box.
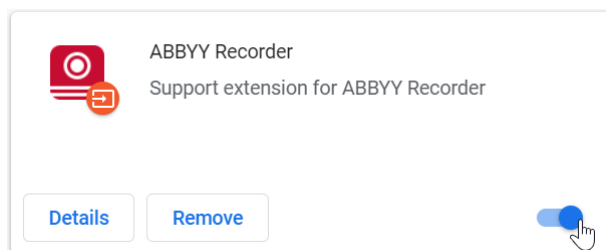
4. The Recorder extension is now enabled.

How to Enable Edge Extension

To turn on the ABBYY Recorder Edge extension, carry out the steps listed below on the workstations.

Important. An internet connection is required on workstations.

1. Open Microsoft Edge.

2. Click the menu button, and then click **Extensions**.
   The **Extensions** page appears.

3. Locate the **ABBYY Recorder** extension in the list and move the slider to On.

4. The Recorder extension is now enabled.

How to Enable Firefox Extension

To turn on the ABBYY Recorder Firefox extension, carry out the steps listed below on the workstations.

1. Open Mozilla Firefox.

2. Click the menu button and select **Add-ons and Themes**.

3. Click **Extensions**.
   The **Extensions** screen appears.

4. Locate the **ABBYY Recorder** extension in the list and click **Enable**.
   If the extension is not listed, it may not have been installed. How to install the extension manually, see the 'How to install the Firefox extension in browser manually 50 ' section.

5. The Recorder extension is now enabled.
   Important. In order for the Recorder extension to works properly, the Firefox browser and ABBYY Recorder must be run under the same account.

How to Install the Firefox Extension in Browser Manually

1. Open Mozilla Firefox.

2. Click the menu button and select **Add-ons and Themes**.

3. Click **Extensions**.

    The **Extensions** screen appears.

4. Press **Settings** (gear icon) next to the add-on search bar and select **Install Add-on From File**.

5. Select **%ABBYY Recorder folder%\FirefoxExtension\abbyy_recorder-*.xpi** and click **Open**.

6. Your Firefox browser will ask you to install the ABBYY Recorder extension right now.

7. Click **Add** to allow the installation.

Performing health check

Check that Recorder has been installed properly by doing the following:

*   Recorder icon appeared in the system tray.

*   Open your browser and make sure the **ABBYY Recorder** extension appeared in the extensions list.

Upgrading Recorder

If you own ABBYY Recorder that comes along with ABBYY Timeline 5.3 or later, you can upgrade to ABBYY Recorder comes along with ABBYY Timeline 6.0.

To upgrade ABBYY Recorder run the **Abbyy.Recorder.<version>.exe** file and follow the instructions of the Installation Wizard.

During the upgrade process, the installer maintains all your previous settings.

Note. During the upgrade process, the Recorder installer maintains all your previous settings. This means that if you specify a new tag, it will not change on the recording service website. To change it:

1. Open the Recording Service website and go to the **Recorders** tab.

2. Select a recorder and click **Set** tag.

3. In the window that opens, enter a new tag and click **Save**.

Uninstalling Recorder

This section contains information about removing Recorder.

Uninstalling ABBYY Recorder via the Command Line

To uninstall ABBYY Recorder in silent mode via the command line, run:

```
Abbyy.Recorder.<version>.exe /uninstall /silent
```

Important. The ABBYY Recorder setup cannot remove the ABBYY Recorder Firefox extension from the Mozilla Firefox browser. If you have the ABBYY Recorder Firefox extension installed on workstations, users must uninstall this extension from their Firefox browser manually. For detailed information see '[How to Uninstall ABBYY Recorder Firefox Extension](52)' section.

How to Uninstall ABBYY Recorder Firefox Extension

After the ABBYY Recorder uninstallation is complete, each user must remove the ABBYY Recorder Firefox extension from Mozilla Firefox manually:

1. Open Mozilla Firefox.

2. Click the menu button and select **Add-ons and Themes**.

3. Click **Extensions**.
   The **Extensions** screen appears.

4. Locate the **ABBYY Recorder** extension in the list.

5. On the right side, click the ellipsis (3-dot) icon and select **Remove** from the drop-down menu.

PostgreSQL Databases Backup and Restore

The Recording Service and Timeline databases contain valuable data. These PostgreSQL databases should be backed up regularly. It is highly important to backup databases before upgrading the Recording Service and Timeline applications.

We suggest you take one of the approaches to backing up your PostgreSQL database:

- File system level backup

- SQL dump

The following is an example of backing up and restoring Recording Service databases

File System Level Backup

This backup strategy is to directly copy the files that PostgreSQL uses to store the data in the database. We highly recommend backup your Recording Service and Timeline databases using this method before the upgrade. You can use whatever method you prefer for doing file system backups, but first you have to stop the Recording Service website in IIS and shut down a database server in order to get a usable backup.

Basic Steps

1. Open Internet Information Services (IIS) Manager and stop the **RecordingService** website.

2. Shut down a PostgreSQL database server

3. Copy **Data** Directory
   The default path is: C:\Program Files\PostgreSQL\12\data
   Note. If you are using SSD and HDD to store databases, copy all your PostgreSQL data directories

4. Start PostgreSQL database server.

5. Start **RecordingService** website.

Restoring Files

To restore your database, you can use whatever method you prefer for doing file system restore, but first you have to stop the Recording Service website in IIS and shut down a database server in order to get a usable backup. For example, repeat the backup steps, but in steps 3 and 3.a delete the current folders and replace them with the folders from the backup.

SQL dump

The idea behind this dump method is to generate a file with SQL commands that, when fed back to the server, will recreate the database in the same state as it was at the time of the dump. PostgreSQL provides the utility program **pg_dump** for this purpose. It extracts a PostgreSQL database into a script file or other archive file.

The approach is recommended for daily and weekly backing up.

You don't need to shut down a database server to get a usable backup. You can perform a backup procedure from any remote host that has access to the database. But the pg_dump utility does not operate with special permissions. In particular, it must have read access to all tables that you want to back up, so in order to back up the entire database, you almost always have to run it as a database superuser. If you do not have sufficient privileges to back up the entire database, you can still back up portions of the database to which you do have access.

An important advantage of pg_dump over the previous backup method is that pg_dump's output can generally be re-loaded into newer versions of PostgreSQL, whereas file-level backups and continuous archiving are both extremely server-version-specific.

For detailed information, see https://www.postgresql.org/docs/12/app-pgdump.html.

Example of command line to run on the same computer where the Recording Service database is installed:
*"C:\Program Files\PostgreSQL\12\bin\pg_dump.exe" -F d -Z 1 -U su -j 2 -f *
\fileshare\backups\august_backup RFStorage
where:

- *RFStorage* - the name of the database used by the Recording Service.

- *su* - user with sufficient rights.

Restoring the Dump

Dumps are restored using the **pg_restore** utility. It restores a PostgreSQL database from an archive file created by pg_dump.

For detailed information, see https://www.postgresql.org/docs/12/app-pgrestore.html

Example of command line to restore a dump is:
pg_restore -d RFStorage \\fileshare\backups\august_backup

About Timeline Licenses

When installing ABBYY Timeline, the license copies to the computer on which Timeline is being installed. Your license determines the Timeline subscription plan. You need to purchase a license update in order to add support for new features, extend the license period, the maximum number of users you can add to your Timeline account, or change other license parameters.

To get more information about subscription plans or purchase a license, contact your local ABBYY sales representative or submit a request to the ABBYY technical support service on this page.

Updating a License

1. Go to the computer on which Timeline is installed.
   Note. To perform all activities below, you must be a system administrator of the computer.

2. Stop the **timelinepi** service using Services snap-in or open Command Prompt as administrator and use:
   ```
   sc stop timelinepi
   ```

3. Go to the Timeline installation folder and open the **license** folder
   The default is C:\Program Files\ABBYY Timeline\license

4. Back up existing **timelinepi.lic** file.

5. Replace the **timelinepi.lic** file with the new one.

6. Start the **timelinepi** service using Services snap-in or run Command Prompt as administrator and use:
   ```
   sc start timelinepi
   ```

Administering

This section provides instructions for configuring the ABBYY Timeline components.

Using OAuth to Access Timeline

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.

For interaction between Recording Service and Timeline components, it is recommended to register Recording Service as a client on the Timeline website.

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 56' 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 58' section below.

Registering a New OAuth Client on the Timeline website

Role required: Timeline account admin

1. Open the Timeline website and login using credentials specified during the Timeline installation 27.

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, make 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: 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 the **Settings > Timeline Authentication** and fill the fields in:

   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 step 4 'Registering a New Client on the Timeline website' 57 section.

3. Click **Save**.
   Please wait for 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 56 '.

   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 63 ".

Using HTTPS

You can use HTTPS to secure data transferred between the application components and the client's browser.

To configure HTTPS, you need SSL certificates for Timeline and Recording Service. You can choose one of the following options:

1. Use SSL certificate issued by the Certification Authority (CA).
   This is the recommended approach for the application installation that is intended for a production environment. The connection to the server will be secure and users will not get any warnings from the browser.

2. Use a self-signed SSL certificate.
   If you do not have a signed certificate or if you only require a certificate for testing purposes, use a self-signed SSL certificate. However, in this case users will get warnings from the web browser about the use of a self-signed certificate as the server will not be considered secure.

If you install the program in a production environment, it is strongly recommended to use HTTPS with a CA certificate and a highly discouraged HTTP or self-signed SSL certificate.

How to Set up HTTPS for Timeline

Below is a general sequence of steps necessary for setting up HTTPS for Timeline.

Basic steps

1. Obtain an SSL certificate.

2. Extract the certificate and keys from a .pfx file.
   Currently, Timeline does not accept .pfx files. You must extract the **.cert** and **.key** files from the .pfx file, so that the certificate and the key files are available separately.
   For more information see "How to extract .cert and .key files from the .pfx 59 ".

3. Set up HTTPS.
   You can enable SSL and configure HTTPS on one of the following stages:

   - During the Timeline installation process
     For more information see "How to set up HTTPS during the Timeline installation 60 ".

   - After the Timeline installation is completed.
     For more information see "How to set up HTTPS without reinstalling Timeline 61 ".

How to extract .cert and .key files from .pfx

Prerequisites. Ensure OpenSSL is installed in the server that contains the SSL certificate.

Important. Name your private key and certificate files as **server.key** and **server.cert** respectively. The key and certificate files must be named **server.key** and **server.cert** since Timeline accepts only files with these names.

1. Start OpenSSL from the **OpenSSL\bin** folder.

2. Open the command prompt and go to the folder that contains your .pfx file.

3. Run the following command to extract the private key:
   ```
   openssl pkcs12 -in [yourfile.pfx] -nocerts -out [keyfile-encrypted.key]
   ```

   You will be prompted to type the import password. Type the password that you used to protect your keypair when you created the .pfx file. You will be prompted again to provide a new password to protect the .key file that you are creating. Store the password to your key file in a secure place to avoid misuse.

4. Run the following command to extract the certificate:
   ```
   openssl pkcs12 -in [yourfile.pfx] -clcerts -nokeys -out [certificate.cert]
   ```

5. Run the following command to decrypt the private key:
   ```
   openssl rsa -in [keyfile-encrypted.key] -out [keyfile-decrypted.key]
   ```

6. Type the password that you created to protect the private key file in the previous step.

7. The .cert file and the decrypted and encrypted .key files are available in the path, where you started OpenSSL.

8. Rename your **.cert** and **.key** files to **server.cert** and **server.key** as Timeline only accepts files with these names.

How to set up HTTPS during Timeline installation

1. Run the **ABBYY-Timeline-6.0.*-installer.exe** file and follow the on-screen instructions in the Installation Wizard. For more information see 'Installing Timeline 24'.

2. Enable SSL between the remote PostgreSQL instance and application in the **Database Connection** 27 step.
   If your remote PostgreSQL is configured with SSL support:

   a. Choose **Use SSL for the database connection**.

   b. Provide a path to your database SSL certificate.
      If your PostgreSQL is configured with SSL support and a CA root certificate file is used, choose **Use CA Root certificate file** and provide the full path to your root certificates for each remote database.

3. Enable SSL between application and client in the **Timeline Base URL and Ports Configuration** step:

    a. Specify TCP/IP port for the Timeline website. For example, 443.

    b. Choose **Use HTTPS**.

    c. Provide paths to **server.cert**, **server.key**, and the password (if presented) files.

4. Setup a network connection for Timeline. For more information see '[Network Connection Settings](#) 64'.

    a. In Windows Firewall, open the rules for inbound Timeline connections.

    b. Add a TCP/IP port specified during the installation process to the exception list. For example, 443 port.

5. Check whether HTTPS is functioning properly
    Open a browser on any computer and enter **{TimelineUrl}:{port}** in the address bar, where:

    - **{TimelineUrl}** is the [Base URL you specified during the Timeline installation](#) 29 or the public IP address or the full name of the computer where Timeline is installed.

    - **{port}** is the custom port assigned to the Timeline website during the installation process. If you are using the default port (80 or 443), you do not need to add them to the {**timelineURL**}. By default, TCP/IP port 80 or 443 is used.

    Example: https://mytimeline:30443

How to switch from HTTP to HTTPS without reinstalling Timeline

If you did not configure HTTPS when installing Timeline, you can do it later without reinstalling Timeline. To do this:

1. Go to the computer on which Timeline is installed.
    Note: To perform all activities below, you must be a system administrator of the computer.

2. Stop the **timelinepi** service using **Services** snap-in or open **Command Prompt** as administrator and use:
    sc stop timelinepi

3. Open the Timeline installation folder and copy the **server.cert** and **server.key** to **ssl** subfolder.

4. By default, the Timeline website uses 443 TCP/IP port when using HTTPS.
   You can reassign port numbers. For more information see "Set a Different Website Base URL and Port Number for Timeline 66 "
   Then you need to make changes to the appropriate Windows Firewall rules or to the settings of any other firewall that you are using.

5. Make sure the HTTPS protocol is specified in the `BASE_URL` variable in the **TimelinePI.xml** configuration file. Update `base_url` with a port number in case of the custom port.
   Example: `BASE_URL=https://mytimeline.com:30443`

6. Start the **timelinepi** service using **Services** snap-in or run **Command Prompt** as administrator and use:
   `sc start timelinepi`

7. Perform a health check 30 .

How to Set up HTTPS for Recording Service

Below is a general sequence of steps necessary for setting up HTTPS for Recording Service during the installation process.

Important. Recording Service does not accept self-signed SSL certificates.

1. Obtain an SSL certificate.
   The SSL certificate should be installed in Microsoft IIS on the server you plan to install Recording Service.

2. Run the **ABBYY.RecordingService.<version>.exe** file and follow the on-screen instructions in the Installation Wizard. For more information see 'Installing Recording Service 36 '.
   During the **Destination Folder** step:

   a. Choose **Use HTTPS**.

   b. Select the SSL certificate from the list.
      You can find the thumbprint of your certificate in the **Internet Information Services (IIS) Manager**:

      i. In **Connections**, select the server name (host).

      ii. Open **Server Certificates**.

        iii. Open your certificate details and find **Thumbprint**.

3. Setup a network connection for Recording Service. For more information see '<u>Network Connection Settings</u> 65 '.

    a. In Windows Firewall, open the rules for inbound Recording Service connections.

    b. Add a TCP/IP port specified during the installation process to the exception list. For example, 443 port.

4. Check whether HTTPS is functioning properly
To make sure that HTTPS is functioning properly, open a browser on any computer and enter the following into the navigation bar:
https://{url}:{port}
where:
{url} is the name of the Recording Service website.
{port} is the port assigned to the Recording Service website during the installation process. For example, 443.

How to switch from HTTP to HTTPS without reinstalling Recording Service

If you did not configure HTTPS when installing **Recording Service**, you can do it later using IIS Manager:

1. Select **RecordingService** site in the **Connections** panel.

2. Click **Bindings...** in the **Action** panel.

3. In the **Site Bindings** windows click **Add**.
The **Add Site Binding** windows will open.

4. Select HTTPS type and provide an SSL certificate issued to the site URL.

5. Restart the site.

Check TCP/IP port availability

If the Recording Service or Timeline website does not open after the installation is complete, the problem may occur due to the busy TCP/IP port specified during installation.

To find open ports on a computer and to check what is using specified port, use **netstat** command line:

1. Open the **Command Prompt** (**Start** > **Run** > **cmd**) and use **netstat -ano | find /i "<port_number>"**.

It will show you all processes that use specified port. Notice the PID (process id) in the right column.

- **-a**
  Displays all active connections and the TCP and UDP ports on which the computer is listening on.

- **-n**
  Displays active TCP connections and port numbers in numerical form.
  If you want to free the port, go to **Task Manager**, sort by PID and close those processes.

- **-o**
  Displays active TCP connections and includes the process ID (PID) for each connection.

Network Connection Settings

The table below lists the ports that are used by default to access Timeline components or for interaction between components. If you are using a software or hardware firewall, make sure that the exception settings for Timeline and Recording Service have been set up accordingly on the computer where they installed.

If you reassign port numbers, you will need to make changes to the appropriate Windows Firewall rules or to the settings of any other firewall that you are using.

Timeline

Timeline setup does not create any software or hardware firewall exceptions. You must set up exception settings to allow interactions between components to take place inside a network. For example, you create inbound and outbound rules in Windows Firewall. The table below contains information about the ports that Timeline listens on.

Component name	Protocol type	Port	Traffic direction	Use
Timeline	TCP/IP	80 or the port used during the installation (if use HTTP)	Inbound	HTTP or HTTPS connections to the Timeline website.

Component name	Protocol type	Port	Traffic direction	Use
		443 or the port used during the installation (if use HTTPS)		
PostgreSQL	TCP/IP	5432	Inbound	Connections to the PostgreSQL database server from the remote computer where the Timeline is hosted.

Recording Service

Component name	Protocol type	Port	Traffic direction	Use
Recording Service	TCP/IP	80 (if use HTTP) 443 (if use HTTPS)	Inbound	HTTP or HTTPS connections to the Recording Service website.
Recording Service	TCP/IP	80 (if use HTTP) 443 (if use HTTPS)	Outbound	• Connections to the PostgreSQL database server. • Connections to Timeline.
PostgreSQL	TCP/IP	5432	Inbound	Connections to the PostgreSQL database server from the remote computer where Recording Service is hosted.

Set a Different Website Base URL and Port Number for Timeline

The port number used by the Timeline website is specified during the Timeline installation. By default, TCP/IP port 80 or 443 is used for the Timeline website. You can change the port number later using **TimelinePI.xml** configuration file:

1. Go to the computer where Timeline is installed.
   Note: To perform all activities below, you must be a system administrator of the computer on which Timeline is installed.

2. Stop the **timelinepi** service using **Services** snap-in or open **Command Prompt** as administrator and use:
   `sc stop timelinepi`
   To ensure the correct operation of Timeline, you need to stop **timelinepi** service prior to changing the Timeline configuration file.

3. Open **Command Line** and use **netstat -a** to get a list of ports and choose an available port.

4. Go to the Timeline installation folder and open **TimelinePI.xml** file using text editor.
   By default, the program is installed into C:\Program Files\ABBYY Timeline

5. In the **TimelinePI.xml** configuration file:

   a. Find the line contains **PROXY_PORT** and change the value.
      e.g.: `<env name="PROXY_PORT" value="8080"/>`
      If you use a HTTPS port, change the value for the **PROXY_SSL_POR**T option.
      e.g.: `<env name="PROXY_SSL_PORT" value="30443"/>`

   b. Find the line contains **BASE_URL** and add or change the port in the value.
      e.g.:
      `<env name="BASE_URL" value="https://mytimeline.com:8080"/>`
      or
      `<env name="BASE_URL" value="http://mytimeline.com:30443"/>`
      If you are using the default port (80 or 443), you do not need to add them to the URL. By default, TCP/IP port 80 or 443 is used.

6. Save the **TimelinePI.xml** file.

7. Start the **timelinepi** service using **Services** snap-in or run **Command Prompt** as administrator and use:
   `sc start timelinepi`

Important. If you reassign port numbers, you will need to make changes to the appropriate Windows Firewall rules or to the settings of any other firewall that you are using. Also, you will need to make changes to **BASE_URL**

How to Change AD Security Groups that Have Access to Recording Service Resources

Active Directory security groups are configured when installing the Recording Service. You can change groups that have full control and/or write access to Recording Service later using the **Appdata.production.json** configuration file.

To change the configuration of Active Directory security groups, perform the following actions:

1. Select the computer where Recording Service is installed.
   Important Note: To perform any of the steps below, you must be a system administrator of the computer.

2. Select the folder where Recording Service is installed and open **Appdata.production.json** using any text editor.
   By default, the component is installed into C:\inetpub\ABBYY Recording Service.

1. In the **Appdata.production.json** file, find the **ADGroupAccess** section and change the values for the **UiAdmin**, **UiUser** and **Recorder** parameters:
   ```
   "ADGroupAccess": {
   "UiAdmin": "MyDomain\\RS-admins",
   "UiUser": "MyDomain\\RS-users",
   "Recorder": "Everyone"
   }
   ```
   Important Note: Backslashes used in values must be escaped with a backslash.

3. Save the **Appdata.production.json** file.

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

How to Change SMTP Mail Server Configuration for Timeline

SMTP mail server is configured during the [ABBYY Timeline installation](#) ⌐28¬. You can change your mail server settings later using **TimelinePI.xml** configuration file.

To change mail server configuration, perform the following actions:

1. Go to the computer where Timeline is installed.
   Note. To perform all activities below, you must be a system administrator of the computer.

2. Stop the **timelinepi** service using **Services** snap-in or open **Command Prompt** as administrator and use:
   ```
   sc stop timelinepi
   ```
   To ensure the correct operation of Timeline, you need to stop **timelinepi** service prior to changing the Timeline configuration file.

3. Go to the folder where Timeline is installed and open **TimelinePI.xml** using any text editor.
   By default, Timeline is installed into C:\Program Files\ABBYY Timeline

4. In the **TimelinePI.xml** configuration file, find the following lines and change their values:

   a. `<env name="MAIL_SERVER_HOST" value=""/>`
      This line contains the host of the SMTP mail server, enter the address in the value.
      e.g.: `<env name="MAIL_SERVER_HOST" value="example.smtp.com"/>`

   b. `<env name="MAIL_SERVER_PORT" value=""/>`
      This line contains the port of the SMTP mail server, enter the port in the value.
      e.g.: `<env name="MAIL_SERVER_PORT" value="465"/>`

   c. This line contains the user that will be used to authenticate with the SMTP mail server, enter the username in the value. Keep this value empty if your mail server requires no authentication.
      `<env name="MAIL_SERVER_USERNAME" value=""/>`
      e.g.: `<env name="MAIL_SERVER_USERNAME" value="example_user"/>`

   d. `<env name="MAIL_SERVER_PASSWORD" value=""/>`
      This line contains the password of the user that will be used to authenticate with the mail server, enter the username in the value. Keep this value empty if your mail server requires no authentication.
      e.g.: `<env name="MAIL_SERVER_PASSWORD" value="example_password"/>`

   e. `<env name="MAIL_SERVER_SECURE" value="FALSE"/>`
      This line contains the option whether to use TLS from the start of the connection. If you want TLS from the start it should be **TRUE** otherwise it should be **FALSE**.
      Note. It is recommended Timeline and the Exchange server use the same TLS settings

f. `<env name="MAIL_SERVER_REQUIRE_TLS" value="FALSE"/>`
This line contains the option specifies whether the connection should be established on an unencrypted channel, then upgrade to a secure connection with a STARTTLS command. If so, specify **TRUE** otherwise **FALSE**.

g. `<env name="MAIL_SERVER_REJECT_UNAUTHORIZED" value="TRUE"/>`
This line contains the option to reject unauthorized certificates, for example, self-signed certificates. In that case, it should be **TRUE**. If you want to use a self-signed certificate specify **FALSE**.

h. `<env name="EMAIL_SENDER" value="noreply@example.com"/>`
This line contains the email sender address used to fill the 'From' header field of e-mails.

5. Save the **TimelinePI.xml** file.

6. Start the **timelinepi** service using **Services** snap-in or run **Command Prompt** as administrator and use:
   ```
   sc start timelinepi
   ```

How to Configure Twilio SMS Service to Receive SMS Notifications from Timeline

Twilio SMS Service is configured during the <u>ABBYY Timeline installation</u> 30. This feature allows Timeline to send SMS notifications containing verification codes, alert notifications, and error messages.

You can change the specified configuration later using **TimelinePI.xml** file. To change Twilio SMS service configuration, perform the following actions:

1. Go to the computer where Timeline is installed.
   Note. To perform all activities below, you must be a system administrator of the computer.

2. Stop the **timelinepi** service using **Services** snap-in or open **Command Prompt** as administrator and use:
   ```
   sc stop timelinepi
   ```
   To ensure the correct operation of Timeline, you need to stop **timelinepi** service prior to changing the Timeline configuration file.

3. Go to the folder where Timeline is installed and open **TimelinePI.xml** using any text editor.
   By default, Timeline is installed into C:\Program Files\ABBYY Timeline

4. In the **TimelinePI.xml** configuration file, find the following lines and change their values:

   a. `<env name="TWILIO_ACCOUNT_SID" value=""/>`
      This line contains a Twilio String Identifier (SID), a unique key that is used to identify your Twilio account
      e.g.: `<env name="TWILIO_ACCOUNT_SID" value="AC3f84d59206412725a03114dfb5163e33"/>`

   b. `<env name="TWILIO_AUTH_TOKEN" value=""/>`
      This line contains an access token that Timeline needs to connect to your **Twilio** account.
      e.g.: `<env name="TWILIO_AUTH_TOKEN" value="ae356b78c7ch1293h123n2afe6a9"/>`

   c. `<env name="TWILIO_PHONE_NUMBER" value=""/>`
      This line contains the phone number from which SMS notifications are sent.
      e.g.: `<env name="TWILIO_PHONE_NUMBER" value="+121313141516"/>`

5. Save the **TimelinePI.xml** file.

6. Start the **timelinepi** service using **Services** snap-in or run **Command Prompt** as administrator and use:
   ```
   sc start timelinepi
   ```

How to Change AD Security Groups that Have Access to the Recording Service Resources

Active Directory security groups are configured when [installing the Recording Service](#) 37. You can change groups that have full control and/or write access to Recording Service later using the **Appdata.production.json** configuration file.

To change the configuration of Active Directory security groups, perform the following actions:

1. Select the computer on which Recording Service is installed.
   Important Note: To perform any of the steps below, you must be a system administrator of the computer.

2. Select the folder where Recording Service is installed and open **Appdata.production.json** using any text editor.
   By default, the component is installed into C:\inetpub\ABBYY Recording Service.

3. In the **Appdata.production.json** file, find the **ADGroupAccess** section and change the values for the **UiAdmin** and **Recorder** parameters:

```
"ADGroupAccess": {
"UiAdmin": "Domain\\UserName",
"Recorder": "ADGroupName"
}
```

Important Note: Backslashes used in values must be escaped with a backslash.

4. Save the **Appdata.production.json** file.

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

Background Upload of Zipped CSV Files to Timeline

The Timeline background-upload feature involves a folder that is monitored for files copied there. Whenever a new zip file is detected in that folder, the application grabs it and interprets it as an uploaded archive. The folder is defined as STORAGE\sftp, where STORAGE variable in the **TimelinePI.xml** configuration file.

The upload file can be copied to the specified folder by any means. It can be the target of an SFTP upload, or it can be an otherwise shared folder.

Important. Use **Deflate** compression method when zipping CSV files. Otherwise, ZIP files upload will fail. Please use archiving software that supports this method of compression. For example, you can use 7Zip or PeaZip instead of the standard Windows archiver.

For details on configuring background upload, see the 'Timeline User's Guide' > Automated File Upload Via SFTP.

Known Issues

Use this section to see if an issue affecting you is already known.

Recorder

Recorder process causes high CPU utilization recording on Windows Server 2016

Your terminal server may experience a CPU load increase after several users work on in. In this case, the number of logging Recorders is equal to the number of users on the terminal server.

To solve this issue it is recommended to reduce the **ScreenshotCapturingRateFps** value in the Recorder settings file:

1. Go to the folder where the Recorder is installed and open **settings.json** using any text editor.
   By default, it is installed into C:\Program Files\ABBYY Recorder.
   Important. Requires administrator privileges to edit **settings.json**.

2. In the **settings.json** file find the following line:
   ```
   "ScreenshotCapturingRateFps": 12.0,
   ```
   Change the value for this parameter to **8.0**

3. Save the **settings.json** file.

4. Restart Recorder for changes to take effect
   Do it in one of the following ways:

   a. Using **Start** menu:

      i. **Start** > **ABBYY Recorder** > **Stop ABBYY Recorder**.

      ii. **Start** > **ABBYY Recorder** > **Start ABBYY Recorder**.

   b. Restart **ABBYY.Recorder.AutoLauncher** service using **Services** snap-in (**Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**).

   Important. Requires administrator privileges to restart service or stop/start **Recorder** via **Start** menu.

Recorder may break such clipboard operations as copy/paste

If you notice that copy/paste operations are disabled when Recorder is recording logs, it is recommended to disable the logging of the **copy** event in the logs.

To do this:

5. Go to the folder where the Recorder is installed and open **settings.json** using any text editor.
   By default, it is installed into C:\Program Files\ABBYY Recorder.
   Important. Requires administrator privileges to edit **settings.json**.

6. In the **settings.json** file find the following line:
   ```
   "DisableClipboardTracking": false,
   ```
   Change the value for this parameter to **true**

7. Save the **settings.json** file.

8. Restart Recorder for changes to take effect
   Do it in one of the following ways:

   a. Using **Start** menu:

      i. **Start** > **ABBYY Recorder** > **Stop ABBYY Recorder**.

      ii. **Start** > **ABBYY Recorder** > **Start ABBYY Recorder**.

   b. Restart **ABBYY.Recorder.AutoLauncher** service using **Services** snap-in (**Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**).

   Important. Requires administrator privileges to restart service or stop/start **Recorder** via **Start** menu.

User is using Internet Explorer 11. Is his activity recorded?

It is not recommended to record users' activity in the Internet Explorer browser. Event recording in Internet Explorer is not fully supported, therefore events and/or screenshots may be lost during recording.

In order to record users' activity in a web browser, use supported browsers with the Recorder browser extensions installed.

Recorder instance installed in Server Managed mode does not display in Recording Service

If Recorder failed to connect to Recording Service using the URL specified during the Recorder installation, it does not display in the Recording Service web application.

To solve this issue:

1. Make sure a user account has been added to the Active Directory group [you created before the Recording Service installation](#) 22 .
   Add a user account to the Active Directory group if you have not done it before.

2. Check the Recorder instance status on the user's computer.
   If status is '**Failed to register recorder at: <SomeRecordingServiceUrl>. No such host is known**', make sure the Recording Service URL is correct. To check and/or change URL:

   a. Open **settings.json**
      You can find it on the user's computer in the Recorder installation folder.
      By default, it is installed into C:\Program Files\ABBYY Recorder.
      Important. Requires administrator privileges to edit **settings.json**.

   b. Find the **ServerManagedMode** section and check the value specified in **Url** parameter.
      If needs, change the value and restart the **ABBYY.Recorder.AutoLauncher** service using **Services** snap-in (**Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**).
      Important. Requires administrator privileges to restart service.

Recorder Firefox extension limitation

Firefox extension install

The Recorder setup can install the Firefox extension feature only under a current user account.

If you install this feature, the Firefox browser will launch after the Recorder setup is complete. The Firefox browser is launched under the same account as Recorder has just installed. It asks a user to add the Firefox extension right now. User should allow the installation of the extension. However, the Firefox extension will be unavailable for other users.

Issue. Users did not detect any new extensions in the Firefox browser as a result of your administrative setup.

Workaround. Use one of the following methods to solve the issue:

- Add the Firefox extension manually in a user browser.

- Use the Firefox Group Policy to install the Firefox extension, for the Firefox extension feature to be available to all users.
  When installing via Group Policy, specify the path to the Firefox extension:
  `%ABBYY Recorder folder%\FirefoxExtension\abbyy_recorder*.xpi`

  Contact the vendor for more info at https://github.com/mozilla/policy-templates/blob/master/README.md#extensionsettings
  Important. In case of the Recorder upgrade, the Firefox extension needs to be updated manually.

Firefox extension uninstall

The Recorder setup cannot remove the Recorder Firefox extension.

Each user must remove the Recorder Firefox extension from Firefox manually. See How to Uninstall Recorder Firefox Extension 52 for details.

After a successful Recorder installation, users did not detect the Recorder extension in a browser, though this feature has been selected to install

1. Make sure that the user has the Recorder extension installed in a supported browser 22, and it is enabled. See Installing Recorder 52 for details.

2. If a user removed the Recorder extension from a supported browser manually, then the Recorder installer will fail to install the Recorder extension later. Contact ABBYY to solve the issue.

Recording Service

Common Issues

1. Recording Service performance is lower if using HDD only or SSD and HDD for storing the PostgreSQL database.

2. We do not recommend storing logs on the Recording Service server for more than a week. After you submit logs to Timeline, you can backup logs to another server (if necessary) and remove them from the Recording Service server.

3. After the Recording Service upgrade is complete, the list of logs on the Recording Service website will be empty. It may take some time to display all existing logs. Please wait a couple of minutes, and the logs will gradually come into view.

Unable to open Recording Service website using its shortcut in the Start menu. The shortcut opens the Default Web Site.

If the Recording Service website is running on port 80, to solve this issue:

1. Open Internet Information Services (IIS) Manager

2. Find the Default Web Site and stop it.

3. Start the **RecordingService** website.

Recording Service installed successfully, but an error occurred while starting the Recording Service website:
NET :: ERR_CERT_AUTHORITY_INVALID.

If the error NET :: ERR_CERT_AUTHORITY_INVALID is displayed when you try to start the Recording Service website, make sure you specified the correct SSL certificate when installing Recording Service. Use Internet Information Services (IIS) Manager to do this:

1. Open Internet Information Services (IIS) Manager and select the **RecordingService** website.

2. Right-click on a website, and then click **Edit Bindings...**

3. In the **Site Bindings** window, click **Edit…**
   The **Edit Site Binding** window will open.

4. In the **SSL certificate** drop-down list, check the selected SSL certificate. Select another one if necessary, and then click **OK**.

5. Restart the **RecordingService** website for the changes to take effect.

6. Verify the changes by opening the website in a web browser.

An error occurred while starting the Recording Service website: HTTP Error 500.30 - ASP.NET Core app failed to start

If the error 'app failed to start' is displayed when you try to start the Recording Service website, make sure the connection to PostgreSQL is established. Then reload the **RecordingService** site in IIS Manager.

I'm trying to start a recording, but the recorder does not change the status to "record".

A user may forbid action recording by clicking **Disable** in his/her Recorder menu in the system tray. This will stop a record and block recording control on this instance via the Recording Service UI. The recorder continues to display on the Recording Service website in the recorders list. Its status is **online**, but the status does not change to **recording** after you click **Start** and then **Refresh List**.

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

Recording on the selected Recorder has started, but logs are not reflected in the UI.

After you click the **Start** button, make sure the recording has launched. To do this click the **Refresh list** button and check the recorder status changed to the **recording**.

Recorded events are saved to logs and sent to the server for processing. When processing is complete, the logs are displayed on the **Logs** tab. New log may take some time to display in the **Recordings** tab.

Logs are partially uploaded, or upload fails.

There are some a limitation to upload logs: unable to upload logs, if the total number of unique events in logs exceeds 10000. If the limit exceeds, an attempt to upload logs fails with an error: **The selected logs have more unique events than the allowed limit.**

To solve this issue, reduce the number of logs being uploaded and try again. To check the number of unique events in one log:

1. Go to **Logs**

2. Click logs ID and check the **UNIQUE EVENTS** field.

Timeline

The contents of the FormEditor and 'One task wizard' windows load slowly

If the Task Mining project contains a lot of forms or events in the forms, it can affect logs processing. Loading elements in Form editor and the Discover task feature can take some time.

This issue will be fixed in the next release.

Timeline process causes high CPU utilization after installation

You can experience a CPU load increase after Timeline installation.

The root cause of this issue is that Redis is not installed properly, and Timeline is not able to connect to Redis. Continuous connection attempts are causing high CPU utilization.

Important. To prevent this issue, you have to be an Administrator on the target machine and have enough permissions to install Ubuntu on Windows Subsystem for Linux. For proper Ubuntu installation please run the installation file as Administrator.

To solve this issue:

1. Stop the **timelinepi** service from **services.msc** or open the command prompt as Administrator and execute the following command:
   ```
   sc stop timelinepi
   ```

2. Open PowerShell as Administrator and list all the WSL installations in your Windows system executing the following command:
```
wslconfig /l
```
Find **Ubuntu** (or **Ubuntu-20.04**) in the list and unregister the distribution executing one of the commands below, depending on the name in the list:
```
wslconfig /u Ubuntu

wslconfig /u Ubuntu-20.04
```

3. Open Windows Explorer, then navigate to the **Ubuntu Installation Folder** 25 which you have selected for Ubuntu during the Timeline installation. The default folder is *C: \Program Files (x86)\Ubuntu*

4. Run the run **ubuntu.exe** (or **ubuntu2004.exe**) file as administrator and follow the instructions on the screen to install.

5. Once the installation is done, run **ubuntu.exe** (or **ubuntu2004.exe**) to open Ubuntu and login as sudo user by executing the command:
```
sudo su
```

6. In Ubuntu Terminal navigate to the **Source Folder** where you originally downloaded the distribution and which you have specified when installing Timeline.

7. Execute the commands below to install and start Redis:

   a. `dpkg -i redis-tools_6.2.4-1rl1~focal1_amd64.deb`

   b. `dpkg -i redis-server_6.2.4-1rl1~focal1_amd64.deb`

   c. `service redis-server start`
   You can test that your Redis server is running by connecting to the Redis CLI:
   ```
   redis-cli
   127.0.0.1:6379> ping
   ```

8. Start the Timeline service either from **services.msc** or executing the following command in the command prompt:
```
sc start timelinepi
```

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](#).