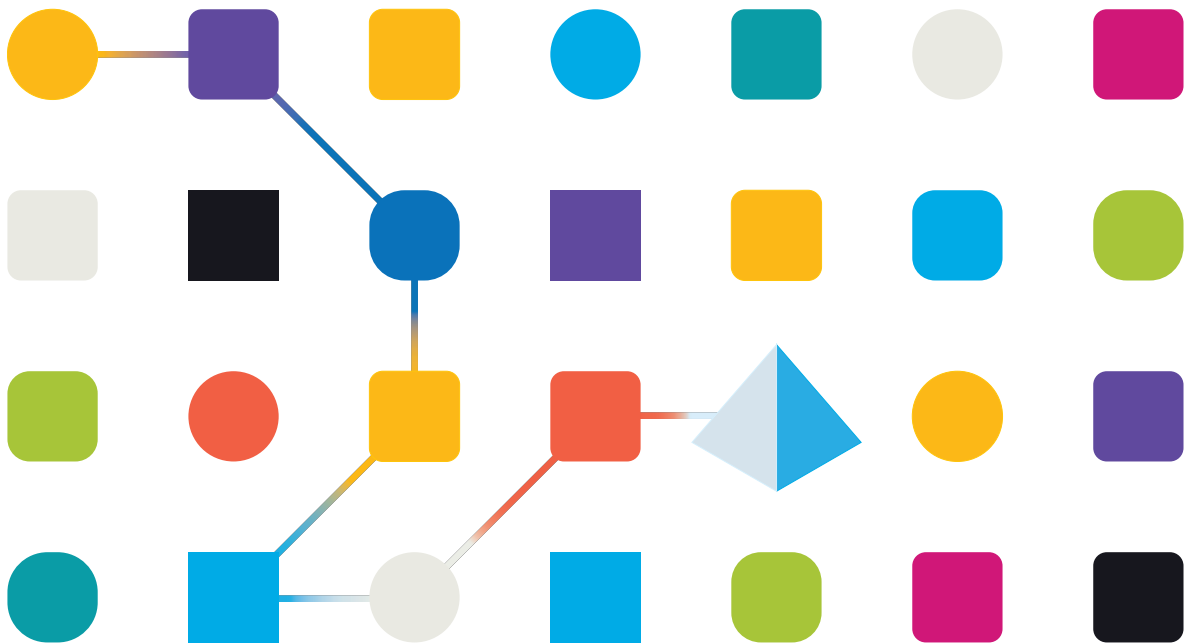




# Process Intelligence 2.0

## Installation Guide for Windows

Document Revision: 1.0



## Trademarks and Copyright

The information contained in this document is the proprietary and confidential information of Blue Prism Limited and should not be disclosed to a third-party without the written consent of an authorized Blue Prism representative. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying without the written permission of Blue Prism Limited.

© **Blue Prism Limited, 2001 – 2023**

“Blue Prism”, the “Blue Prism” logo and Prism device are either trademarks or registered trademarks of Blue Prism Limited and its affiliates. All Rights Reserved.

All trademarks are hereby acknowledged and are used to the benefit of their respective owners. Blue Prism is not responsible for the content of external websites referenced by this document.


Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.  
Registered in England: Reg. No. 4260035. Tel: +44 370 879 3000. Web: [www.blueprism.com](http://www.blueprism.com)

# Contents

<b>Installation</b> .....	<b>4</b>
Installation overview .....	4
<b>System requirements and prerequisites</b> .....	<b>6</b>
Process Intelligence .....	6
Recording Service .....	7
Recorder .....	8
<b>Recording Service</b> .....	<b>10</b>
Install the Recording Service .....	10
Uninstall the Recording Service .....	12
Upgrade the Recording Service .....	12
<b>Process Intelligence</b> .....	<b>13</b>
Install Process Intelligence .....	13
Uninstall Process Intelligence .....	17
Upgrade Process Intelligence .....	19
Update a Process Intelligence license .....	19
<b>Recorder</b> .....	<b>20</b>
Install the Process Intelligence Recorder .....	20
Uninstall the Recorder via the command line .....	26
Upgrade the Recorder .....	26
<b>Advanced configuration</b> .....	<b>28</b>
Use OAuth to access Process Intelligence .....	28
Configure HTTPS .....	30
Network connection settings .....	34
Check TCP/IP port availability .....	35
Change URL and port .....	35
Change SMTP mail server configuration .....	36
Update Active Directory security groups accessing Recording Service resources .....	37
Configure Active Directory (AD) security groups to connect the Recording Service with Recorder instances .....	38
Configure the Recording Service .....	39
Recorder logs .....	48
Background upload of zipped CSV files .....	50
Back up and restore the PostgreSQL databases .....	50
Move database tables with screenshots to a new hard disk .....	52
Configure Twilio SMS service to receive SMS notifications from Process Intelligence .....	52
<b>Troubleshooting</b> .....	<b>54</b>
Process Intelligence .....	54
Recording Service .....	55
Recorder .....	56
Recorder may break clipboard operations such as copy/paste .....	57

## Installation

This installation guide is intended for system administrators and engineers and includes instructions for installation and configuration of Blue Prism Process Intelligence on Windows.

 Please make yourself familiar with the [system prerequisites](#) before starting the installation.

### Installation overview

#### Step 1. Make sure your computers are all set up and ready

Before you begin installing the Process Intelligence system:


1. Check the [system requirements](#) to understand whether your computer supports the Process Intelligence components.
2. Apply the latest Windows and other programs updates to ensure your computers have the latest security updates.
3. Reboot to ensure that any pending installs or updates do not hinder the Process Intelligence components installation.
4. Free up space. Remove unnecessary files and applications from your %SystemDrive%, as well as discs that you intend to use, for example, to store the Process Intelligence databases.
5. If you intend to configure HTTPS, see [Using HTTPS](#).


#### Step 2. Install the Recording Service component

1. Run the Recording Service installer and follow the on-screen instructions in the installation wizard. If you receive a **User Account Control** notification, select **Yes**.
2. Specify the necessary [network settings](#).
3. Make sure the Recording Service component has been installed correctly by performing a [health check on the Recording Service](#).

See [Install Recording Service](#) for step-by-step guidance.

#### Step 3. Install the Process Intelligence component


 If you intend to use Process Intelligence in the Cloud, you can skip this step.

 The Recording Service and Process Intelligence components must be installed on separate computers.

1. Run the installer and follow the on-screen instructions in the installation wizard. If you receive a **User Account Control** notification, select **Yes**.
2. Specify the necessary [network settings](#).
3. Make sure the Process Intelligence component has been installed correctly by performing a health check on Process Intelligence.

See [Install Process Intelligence](#) for step-by-step guidance.


## Step 4. Establish the trust relationship between Recording Service and Process Intelligence


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


OAuth must be configured so the Recording Service and Process Intelligence components can interact with each other.

1. Register the Recording Service as a client on the Process Intelligence website and obtain the required credentials (**Client ID** and **Client Secret**).  
See [Register a new client on the Process Intelligence website](#) for guidance.
2. On the Recording Service website specify the connection details to Process Intelligence using the credentials you obtained at step 1.  
See [Configure connection settings in Recording Service](#) for guidance.

## Step 5. Install the Recorder component on users' computers

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


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

 If you plan to record user activities which are using Windows RemoteApp and Citrix Workspace App, install the Recorder on a terminal server.

1. Install the Recorder on the users' workstations using the method of your choice.  
See [Install Recorder](#) for guidance.
2. Enable the Recorder browser extensions on the workstations.  
See [Enable Recorder Chrome browser extension](#) for guidance.

Now you have all the Process Intelligence system components installed, and you can start working with them.

## System requirements and prerequisites

 Please note the following general prerequisites:

- The Recording Service and Process Intelligence components must be installed on separate computers.
- The user workstations installing the Recorder component and the server hosting the Recording Service component must all be members of the same Active Directory domain. For more information, see [Configure Active Directory \(AD\) security groups to connect the Recording Service with Recorder instances on page 38](#).
- Recording Service performance may vary depending on the hardware configuration. If you intend to use more than 20 Recorder instances, it is recommended to store PostgreSQL databases partially or fully on the SSD for better performance. For more information, see [Move database tables with screenshots to a new hard disk on page 52](#).

## Process Intelligence

<b>Operating system</b>	Microsoft® Windows Server® 2019 Version 1809 (OS Build 17763.2565) or later
<b>CPU</b>	4 cores or more
<b>RAM</b>	16 GB or more
<b>HDD</b>	512 GB or more  This depends on the actual amount of data loaded into the application. Production environments may require more disk space, depending on the actual volume of data loaded into the application.
<b>Browser (to access the Blue Prism Process Intelligence website)</b>	<ul style="list-style-type: none"> <li>• Google Chrome 109 or later</li> <li>• Microsoft Edge 109 and later</li> </ul>

<p><b>Additional software</b></p>	<p>Additional requirements for Windows</p> <ul style="list-style-type: none"> <li>• Microsoft Windows Subsystem Linux</li> </ul> <p>If this Windows feature is disabled, the Process Intelligence Setup will prompt you to enable it. After that, you will need to restart your computer to apply the changes.</p> <ul style="list-style-type: none"> <li>• Redis 5 for Linux</li> </ul> <p>Process Intelligence uses Redis for Linux therefore additional software is needed. Please download the following installation packages into the same folder:</p> <ul style="list-style-type: none"> <li>• <a href="#">Linux Ubuntu 20.04 LTS (Ubuntu_2004.2020.424.0_x64.appx)</a></li> <li>• <a href="#">gcc-10-base_10.3.0-1ubuntu1_20.04_amd64</a></li> <li>• <a href="#">libatomic1_10.3.0-1ubuntu1_20.04_amd64.deb</a></li> </ul> <ul style="list-style-type: none"> <li>• Microsoft .NET Framework 4.5*</li> <li>• PostgreSQL 12.*</li> <li>• NodeJS 16.15*</li> <li>• Python 3.8.10 (64-bit)*</li> <li>• Microsoft Visual c++ 2015-2019 Redistributables (x64)*</li> <li>• SMTP Server</li> </ul> <p>Process Intelligence needs access to a running SMTP server to be able to send verification emails, notifications, invitations, and alerts.</p>
<p><b>Other requirements</b></p>	<ul style="list-style-type: none"> <li>• Ensure the administrator user performing the installation has the appropriate permissions to set the PowerShell Execution Policy to RemoteSigned. For more information, see <a href="#">Install Process Intelligence on page 13</a>.</li> <li>• You must have a <a href="#">configured Twilio account</a> if you want to enable SMS notifications in Process Intelligence.</li> </ul>

\* included with the Process Intelligence 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

<p><b>Operating system</b></p>	<p>Microsoft® Windows Server® 2016, 2019, or 2022</p>
--------------------------------	---

<b>Additional software</b>	<ul style="list-style-type: none"> <li>• Microsoft® Internet Information Services (IIS) 8.5*</li> <li>• ASP.NET Core Hosting Bundle 6.0.12* (version 7.0 is not supported)</li> <li>• PostgreSQL v. 12 or later*</li> </ul>
<b>Browser (to access the Recording Service website)</b>	Google Chrome 109 or later
<b>Hard disk requirements</b>	<p>The 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.</p> <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> Only the database table with screenshots may be moved to the new hard disk. For more information, see <a href="#">Move database tables with screenshots to a new hard disk on page 52</a>.</p> </div>
<b>Other requirements</b>	<ul style="list-style-type: none"> <li>• The Recording Service works with Process Intelligence 2.0.</li> <li>• Windows authentication is used to authorize the connection between the Recording Service and the Recorder instances installed on users' workstations. Configure the Active Directory security groups you plan to use to connect the Recording Service with the Recorder instances in advance. For more information, see <a href="#">Configure Active Directory (AD) security groups to connect the Recording Service with Recorder instances on page 38</a>.</li> </ul>


\* 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

<b>Operating system</b>	<p>Microsoft® Windows 10 (x64) and 11 (x64) Microsoft® Windows Server® 2016, 2019, and 2022</p> <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> The Recorder can be installed on Microsoft Windows Server 2016, however correct log recording is not guaranteed.</p> </div>
<b>Additional software</b>	<p>Microsoft .NET Framework 4.6.2* Microsoft .NET 6.0.12 and later*</p>



<b>Browser (to record user activities)</b>	<ul style="list-style-type: none"><li>• Browser Google Chrome 109 or later The following versions are not supported:<ul style="list-style-type: none"><li>• Google Chrome Portable</li><li>• Google Chrome Standalone for one user</li><li>• Google Chrome Standalone for multiple users</li></ul></li><li>• Microsoft Edge 109 or later</li><li>• Mozilla Firefox 109 or later (Limited support. See <a href="#">Known issues</a> for details). Mozilla Firefox ESR is not guaranteed to fully work.</li></ul>
<b>Other requirements</b>	<ul style="list-style-type: none"><li>• The Recorder works with Process Intelligence 2.0 and the Recording Service that comes with it.</li><li>• Windows authentication is used to authorize the connection between the Recording Service and the Recorder instances installed on users' workstations. Configure the Active Directory security groups you plan to use to connect the Recording Service with the Recorder instances in advance. For more information, see <a href="#">Configure Active Directory (AD) security groups to connect the Recording Service with Recorder instances on page 38</a>.</li></ul>

\* included with the Recorder installer.

## Recording Service

The Recording Service includes a database and a website. It is delivered as a separate distribution kit.

### Install the Recording Service

1. Run the Recording Service installer.
2. Select the language in which you want to run the installation wizard.
3. Read and, if you agree to terms, accept the license agreement.
4. Specify the folder where the Recording Service should be installed.

The default installation folder is: C:\inetpub\ABBY Recording Service.

5. Specify the 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 HTTPS is used). You will be asked for the SSL certificate and the private key when setting up HTTPS.
- 80 (if HTTP is used). The default website 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 the 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 [Check TCP/IP port availability](#). 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.




For interaction between the Recording Service and Process Intelligence components, it is recommended to use the same protocol, for example, HTTP and HTTP or HTTPS and HTTPS.

6. . On the Active Directory Security screen, specify the names of the security groups you configured before installing the Recording Service. For more information, see [Configure Active Directory security groups to connect the Recording Service with Recorder instances](#).

You can change the Active Directory security groups configuration after the installation. For more information, see [Update Active Directory security groups](#).


7. The Recording Service needs access to the PostgreSQL database. You can install PostgreSQL on the same computer as the Recording Service or a separate computer.

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

 If PostgreSQL is already installed on the current computer, instead of the **PostgreSQL Database Options** step, the **Database Connection** step will open. At this step, you need to specify the database connection settings.

- a. If you have selected **Install PostgreSQL on this machine**, you will be prompted to provide the following details:

- Provide PostgreSQL superuser credentials – These credentials will be used by the installation program to create a database user for the Recording Service.

 The PostgreSQL superuser name can contain only English letters and digits from 0 to 9 and cannot include any of the following characters: - \/: \*? "<> |

- Specify the TCP/IP port for the 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 [Check TCP/IP port availability](#).
- Specify the service account – By default, the PostgreSQL services operate with the **superuser** account. To change the default user, select **Specify service user credentials** option and set new credentials for running the PostgreSQL service.

- b. Specify the destination folders.


- Installation directory – PostgreSQL will be installed into specified folder. The default installation folder is: C:\Program Files\PostgreSQL\12.
- Data directory – Enter the path where the database needs to be installed. The default path is: C:\Program Files\PostgreSQL\12\data.

- c. Specify the PostgreSQL database name and user that will work with the Recording Service and database.

8. If you have selected **Connect to remote / another preinstalled version of PostgreSQL database**, specify the database connection settings.

9. Perform a health check of the installation.


Navigate to **Start** menu > **Recording Service**. The Recording Service website will open in your browser. If the Recording Service has been installed correctly, you will see the Recording Service website with the default template.

 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](#).

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

## Uninstall the 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 on-screen instructions.


 Your database and recorded logs are maintained while uninstalling.

## Upgrade the Recording Service

You can install a new version of the Recording Service and your databases and logs will be maintained.


To do this:

1. Back up the Recording Service database. For more information, see [Back up and restore the PostgreSQL databases on page 50](#).
2. Run the Recording Service installer to start the installation wizard.
3. Follow the instructions in the installation wizard.


 While upgrading Recording Service version 1.1 to 2.0, a warning displays that the upgrade is not supported because the currently installed version is corrupted. This is not applicable and will not stop you from upgrading to version 2.0 if you click **Next** in the wizard. The wizard will prompt you to uninstall the current version and install the new version.

If you cannot upgrade the Recording Service using the wizard, perform the following steps:

1. Uninstall your Recording Service.  
Your database is maintained while uninstalling.
2. Run the Recording Service installer to start the installation wizard.
3. Follow the instructions in the installation wizard.
4. To connect to the existing database, provide the following details at the Database Connection step.
  - User login and password – Specify the PostgreSQL superuser credentials.
  - Server name – Specify the name of the server where PostgreSQL is installed.
  - Port – Specify the TCP/IP port for the PostgreSQL database.
5. At the Create Database step specify:
  - Username – This will be used for interaction between the Recording Service and PostgreSQL database.

 You must specify a new username during every new installation.

- Database name – The installer will assign the database to the specified user.


 If you enter the name of a non-existent database, the installer will create a new database with the specified name.


## Process Intelligence

Process Intelligence includes a database and a website. You can obtain the component in one of the following ways:

- Installation package – You can purchase a license and download the distribution kit via the links you received from your Blue Prism sales representative.
- Online subscription – You can purchase a subscription to Blue Prism Process Intelligence deployed in the Cloud. If you using this option, you don't need to install Process Intelligence locally.


## Install Process Intelligence

 The Process Intelligence 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. If you have deleted something from the installation directory by accident, you will have to uninstall and then re-install Process Intelligence.

 You must be a system administrator of the machine on which Process Intelligence is being installed.

1. Open and run PowerShell as an administrator and use the following command to change the execution policy for PowerShell:

```
Set-ExecutionPolicy RemoteSigned
```

 If you receive 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.

2. Log in as a Windows administrator or run the Process Intelligence setup as an administrator.
3. Run the installer.
4. The installation wizard displays a sequence of screens with detailed instructions for each installation step. Use the **Back** and **Next** buttons to navigate through the screens. To quit the installation wizard at any stage, click **Close**.
5. Read and accept the license agreement.

## 6. Check and install the prerequisites.

The wizard checks for the third-party applications that are required to configure and operate Process Intelligence. Some of the applications will have to be downloaded and installed manually. If your computer meets the system requirements, you will be taken straight to selecting a destination folder, and the additional steps described below will not display.

- a. Enable Windows features – If the **Microsoft Windows Subsystem Linux** feature is disabled, the wizard will prompt you to enable it. After that, your computer will be restarted automatically. You must save your work before continuing with the installation. After restarting, the installation will be auto-resumed. If it doesn't resume automatically you must run the installer again.
- b. Install Redis – Download the following installation packages into the same folder:
  - [Linux Ubuntu 20.04 LTS](#)
  - [gcc-10-base\\_10.3.0-1ubuntu1\\_20.04\\_amd64.deb](#)
  - [libatomic1\\_10.3.0-1ubuntu1\\_20.04\\_amd64.deb](#)
- c. Specify a folder where you want to save the packages.
- d. Specify a folder where Ubuntu will be extracted to. The default folder is: C:\Program Files (x86)\Ubuntu.

## 7. Select a destination folder where Process Intelligence will be installed. The default folder is: C:\Program Files\Blue Prism Process Intelligence.

## 8. Select the PostgreSQL database which Process Intelligence needs to access. You can install PostgreSQL on the same computer as Process Intelligence or on a separate computer.

If you have already installed PostgreSQL on the current computer or another one, select **Connect to existing database**. Otherwise, select **Install local database** and follow the instructions.


The following PostgreSQL database tables will be created:

- **timeline** – The admin database which contains all information about users, their activity, and their projects.
- **timeline-log** – The log database which contains detailed records of ABBYY Timeline events such as security, errors, and notifications.
- **timeline-000** – The user database which contains information about user repositories.

## 9. If you selected **Install local database**, configure access to the local database as follows:

- a. Enter the PostgreSQL superuser username and password. These will be used by the installation program to create a database user for Process Intelligence.
- b. Specify the TCP/IP port. The default is TCP/IP port 5432.. Make sure that it is not being used by any other application. For more information, see [Check TCP/IP port availability](#).
- c. Specify the server name where PostgreSQL should be installed. By default, localhost is used.
- d. Enter the path where the database needs to be installed. The default path is: C:\Program Files\PostgreSQL\12.


10. If you selected **Connect to existing database**, this means PostgreSQL is already installed on the remote or local server.

 If the database already exists 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 Process Intelligence to connect to the detected database. Otherwise, select **Reinstall Timeline database tables and user**. In this case, the installer will delete the detected database and install a new one.

Configure the database connection settings as follows:

- a. Enter the username and password for the PostgreSQL user who will own the databases.
  - b. Specify the server name where PostgreSQL will be installed. The default is localhost.
  - c. Specify the TCP/IP port. The default is TCP/IP port 5432.
  - d. Enter a name for each database:
    - i. timeline is the only valid name for the admin database.
    - ii. timeline-log or timeline\_log are the only valid names for the log database.
    - iii. timeline-000 or timeline\_000 are the only valid names for the user database.
  - e. If your PostgreSQL is configured with SSL support, select **Use SSL for the database connection**. 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.
11. Create a first admin user account for Process Intelligence – 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 Process Intelligence 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.

 This user must be a member of the **Admin AD Security group** you specified during the **Recording Service installation**.

12. Configure the SMTP server access to enable Process Intelligence to send out emails for several features such as alerts, user invitations, and email notifications. For example, during a user registration process, a verification email message is sent to the user. The user won't be able to use Process Intelligence until they complete the instructions contained in the message.
  - a. Mail server host – Specify the server name where the SMTP mail server is installed.
  - b. Mail server port – Provide the SMTP mail server port number.
  - c. Mail server username and password – Provide the SMTP mail server access credentials.
  - d. Email sender – Provide the email sender address that is used to fill the 'From' header field of emails.

- e. Mail server security – Specify the mail server security options. To decide which option you need 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](#).
  - i. Select **Non secure** if the SMTP server does not use TLS. This is a typical use case for 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** if you want the app to use TLS to connect to the SMTP server from the start. This 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, for example, self-signed SSL certificate.

13. Configure the base URL and ports as follows:

- a. Enter the **Base URL** that hosts Process Intelligence and through which users will be able to access the Process Intelligence website.

The base URL must be a fully qualified URL. The lowercase pattern is recommended. It should match the computer name on which you are installing Process Intelligence and must be accessible both from the computer on which the Recording Service component is installed and from the administrator browser. The base URL also is used for links inside email messages sent by Process Intelligence.

Examples:

The base URL of the HTTP endpoint, if a custom port is specified:

`http://myprocessintelligence.com:8080`

The base URL of the HTTPS endpoint, if a custom port is specified:

`https://myprocessintelligence.com:30443`

- b. Specify the TCP/IP port for the Process Intelligence website. By default, TCP/IP port 80 is used for the website. Make sure that it is not being used by any other website. For more information, see [Check TCP/IP port availability](#). You can also [set a different port number](#) later.


Select **Use HTTPS** if you want to secure the data being transferred. For setting up HTTPS you need to supply the SSL certificate and the private key. Currently, Process Intelligence does not accept .pfx files. If 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.



If you install the program in a production environment, it is strongly recommended to use HTTPS.



14. Set up the service – Specify the user credentials under which the Process Intelligence service will run. Provide the login in the format of domain\user. The following options are available:
  - If the computer is an Active Directory domain member, you can specify:
    1. Domain user account. Login example: MYDOMAIN\username
    2. Local machine account. Login example: MYCOMPUTERNAME\username
  - If the computer is part of a workgroup, specify the local machine account. Specify the valid password for the user account used to install Process Intelligence.

 You cannot change the specified user account after the installation has completed.

15. Configure SMS notifications – Configure the Twilio SMS service to receive SMS notifications from Process Intelligence containing verification codes, alert notifications, and error messages.

A Twilio account is required to configure and send SMS notifications. You will need to enter the following information to configure SMS notifications:

  - a. Account SID – A Twilio String Identifier (SID), a unique key that is used to identify your Twilio account.
  - b. Auth token – The authentication token generated for your Twilio account.
  - c. Phone number – The sender's phone number for the Twilio account.
16. Create firewall exceptions – The 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, inbound and outbound rules in Windows Firewall. For more details, see [Network connection settings](#).
17. Perform a health check – Check that Process Intelligence is working properly by doing the following:
  - a. Open a browser and enter `{URL}:{port}` in the address bar, where:
    - `{Url}` is the base URL you specified during the Process Intelligence installation or the public IP address or the full name of the computer on which Process Intelligence is installed.
    - `{port}` is the port assigned to the Process Intelligence website during the installation process. By default, TCP/IP port 80 is used.

Example: `http://myprocessintelligence:8080` or  
`https://myprocessintelligence:30443`
  - b. If the installation was carried out correctly, the Process Intelligence website will launch.
  - c. Log in using the Process Intelligence first admin account credentials.

## Uninstall Process Intelligence

1. Run the installer to start the installation wizard.
2. In the program dialog box, click **Uninstall Blue Prism Process Intelligence powered by ABBYY Timeline**.

3. In the next dialog box specify whether you want to uninstall the product completely or maintain the databases for future use (for example, if you choose to install a newer version).
  - If you want to remove the product completely, including the databases, select **Delete Blue Prism Process Intelligence database and data folder** and provide PostgreSQL superuser credentials.
  - If you want to uninstall the product but keep the databases, proceed to the next step.
4. Click **Uninstall** to start the uninstall process.  
Click **Cancel** if you want to cancel the uninstall.
5. Click **Finish** to close the installation wizard.
6. Restart your machine.

## Upgrade Process Intelligence

To upgrade your Process Intelligence instance to a new version:

1. Back up the Process Intelligence database. For more information, see [Back up and restore the PostgreSQL databases on page 50](#).
2. Run the installer to start the installation wizard.
3. In the program dialog box, select **Update** and follow the instructions in the installation wizard.

If you cannot upgrade Process Intelligence using the wizard, perform the following steps:

1. Uninstall Process Intelligence.
2. Run the installer and follow the on-screen instructions in the installation wizard.
3. Perform a [health check](#).


## Rebuild existing Task Mining projects

After the upgrade process is complete, you need to rebuild all your previous Task Mining projects so that they are available in Process Intelligence 2.0.

1. Open a browser and enter {URL};{port} in the address bar, where:
  - {Url} is either the Base URL you specified during the Process Intelligence installation, or the public IP address or the full name of the machine on which Process Intelligence is installed.
  - {port} is a custom port assigned to the Process Intelligence website during the installation process. 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.

Example: `http://myprocessintelligence:8080` or `https://processintelligence:30443`

2. Log in using the first admin account credentials you specified during the Process Intelligence installation process.
3. Click your user avatar in the navigation menu and select **Open Admin app**.
4. In the Admin app, navigate to the Project tab and click **Rerun all task mining cutting**.

 Do not refresh or close this browser page until the process has finished.

## Update a Process Intelligence license

 You must have system administrator privileges to update a Process Intelligence license.

To update your license:

1. On the computer on which Process Intelligence is installed, stop the `timelinepi` service using the Services snap-in or open Command Prompt as administrator and enter: `sc stop timelinepi`
2. Navigate to the Process Intelligence installation folder and open the license folder. The default is `C:\Program Files\Blue Prism Process Intelligence powered by ABBYY Timeline\license`.
3. Back up the existing `timelinepi.lic` file.
4. Replace the `timelinepi.lic` file with the new license file.
5. Start the `timelinepi` service using Services snap-in, or run Command Prompt as administrator and enter: `sc start timelinepi`

## Recorder


The Recorder installation includes a recorder, the Recorder Log Viewer, and the browser extensions for Google Chrome, Mozilla Firefox, and Microsoft Edge. It is delivered as a separate distribution kit.

## Install the Process Intelligence Recorder

### Prerequisites

The following requirements must be met before installing the Recorder:

- The user workstations installing the Recorder component and the server hosting the Recording Service component must all be members of the same Active Directory domain.
- All user accounts on whose computers you intend to install the Recorder must be added to the Recorder writers Active Directory security group [you created before the installation](#).
- The appropriate browser extensions must be installed to ensure that user activities are recorded in Google Chrome, Microsoft Edge, and Mozilla Firefox browsers. The Firefox extension has several limitations. Please refer to the [Known issues](#) for more details.
- If you plan to record user activities which are using Windows RemoteApp and Citrix Workspace App, install the Recorder on a terminal server.

 The Recorder can be installed on the terminal server the same way as on a workstation. It will log the actions of users connecting to this server via a Citrix client or RDP. The Recorder has been tested with the following terminal server configuration:

- A computer running under Microsoft Windows Server 2016 (Remote Desktop, RemoteApp, and Remote Desktop Web Access).
- Citrix Workspace App 7.

You might be prompted for a system reboot during the Recorder installation. Please save your work first, otherwise you may lose unsaved changes.

### Interactive installation

1. Run the Recorder installer.
2. Select the language in which you want to run the installation.  
The Recorder is available in two languages, English and Japanese. The Japanese interface is only available on operating systems where the Japanese locale is enabled.
3. Read, and if you agree with the terms, accept the license agreement.
4. Specify the folder where the Recorder will be installed. The default installation folder is: C:\Program Files\BPPI Recorder.
5. Specify a local or network folder where the program will store its data. To keep data in the %appdata%\BPPI\Recorder\ folder, select **Use AppData folder**.

Depending on the operating mode (set in the next installation step), different data is stored in the specified folder:

- When installed in **Standalone** mode, application logs and logs with recorded user activity are stored in the folder.
- When installed in **Server managed** mode, only application logs are stored in the folder.

6. If required, specify a tag. A tag is a descriptive text string for the workstation on which your Recorder instance is being installed. When installing in **Server managed** mode, the tag is passed to the Recording Service and helps the administrator identify a workstation on 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 the Recorder on several workstations, such as, the 'accounting department' tag. You can then easily find these workstations in the **Recorders** list on the Recording Service website when filtering by the 'accounting department' tag.


7. Select the Recorder operation mode:

- a. **Standalone** – When this mode is enabled:

- Recording control (start/stop) remains with the local computer.
- The logs with the recorded data are saved on the local computer.
- The setup installs the Recorder Log Viewer utility. The utility enables logs to be opened that were recorded by the Recorder when installed in Standalone mode. For detailed information on using the Recorder Log Viewer, see [Recorder logs](#).

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


- Recorded logs are stored on users' computers and are not sent to the Recording Service for processing, so there are no forms in these logs. If you plan to upload logs to Process Intelligence for testing purposes, you must open your logs in the Recorder Log Viewer utility. The forms will be detected automatically and the Forms folder will be created inside your logs. To upload the processed logs to Process Intelligence, see [Upload logs from a Recorder installed in standalone mode](#).

 Forms are supported in the Recorder Log Viewer which is installed with the BPPI Recorder 2.0 and later.


- Text data in text logs is not encrypted except for passwords, and data in screenshots is not blurred.

- b. **Server managed** – When this mode is enabled, the recording can be started and stopped from the Recording Service. User activity logs are automatically saved to the server. Specify the website on which the Recording Service is installed and accessible over network.

8. Select the browser extensions you want to install. Extensions allow the Recorder to capture user actions in the Google Chrome, Microsoft Edge, and Mozilla Firefox browsers.

 The Firefox extension has several limitations. Please refer to the [Known issues](#) for more details.

After the Recorder has been installed on the users' workstations, each user must enable the browser extensions. See instructions for [Google Chrome](#), [Microsoft Edge](#), and [Mozilla Firefox](#).

 If a user has just been added to the Recorder-writer Active Directory security group, you may need to restart the computer to allow the Recorder installed in the Server managed mode to connect to the Recording Service.

## Command line installation

You can install the Recorder components in silent mode using the command line. For silent installation, enter:

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

You can use the following command-line options described below.

Option	Default Value	Description
/silent		<p>Runs the installation in silent mode.</p> <p>No setup dialog boxes are displayed, and the program is installed in default configuration.</p>
/passive		<p>Runs the installation with the progress bar only to be displayed. No other dialog boxes are displayed.</p>
installDir=<path>	C:\Program Files\ABBYY Recorder	The path to the folder where the Recorder will be installed.
DataPath=<path>	%appdata%\ABBYY\Recorder	<p>Folder where the program will store its data.</p> <p>Depending on the operating mode, different data are stored in the specified folder:</p> <ul style="list-style-type: none"> <li>• If you specify <b>ServerUrl</b> value to install ABBYY Recorder in <b>Server managed</b> mode, only application logs are stored in the folder.</li> <li>• If you install ABBYY Recorder in <b>Standalone</b> mode, application logs and logs with recorded user activity are stored in the folder.</li> </ul>
Tag=<tag>		Tag describing current workstation. No tag is added by default.

Option	Default Value	Description
ServerUrl=<server URL>		<p>Enables the <b>Server managed</b> mode. Specify the website URL on which the Recording Service is installed and accessible over network.</p> <p>If this option is not specified, the default installation is in <b>Standalone</b> mode.</p>
ChromeExt=<true false>	true	Installs the Recorder Chrome extension.
EdgeExt=<true false>	true	Installs the Recorder Edge extension.
FirefoxExt=<true false>	true	<p>Installs the Recorder Firefox extension.</p> <p>The setup can only install the Firefox extension under a current user account. For more information, see <a href="#">Recorder Firefox browser extension limitations on page 58</a>.</p> <p>Each user must remove the Firefox extension from Mozilla Firefox manually. For more information, see <a href="#">Install the Firefox browser extension</a>.</p>

Option	Default Value	Description
ControlButtonsVisible=<true false>	true	<p>Specifies the mode where most of the standard user interface (UI) is disabled.</p> <p>The Recorder introduces a custom UI option as an alternative to the classic UI, which hides the <b>Enable/Disable</b> buttons from the user interface when installed in Server managed mode.</p> <p>It is not recommended to install the Recorder with a custom UI in a production environment.</p> <p>For detailed instructions, see <a href="#">Install the Recorder with a custom UI to prevent users from controlling the Recorder below</a>.</p>

### Install the Recorder with a custom UI to prevent users from controlling the Recorder

The Recorder includes a powerful security feature that allows users to stop the Recorder from recording their desktop activity. However, in cases where the recording process must only be managed by the administrator through the Recording Service, the end user is prevented from turning the Recorder on or off. For such cases, a custom UI option is available in the Recorder as an alternative to the classic UI, which 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 and the parameter `controlButtonVisible = false`. The `controlButtonVisible` parameter specifies the mode in which most of the standard Recorder UI is turned off, and prevents the user from controlling when the 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 are installed. The Firefox extension is not 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/>.




## Perform health check

Verify that the Recorder has installed correctly by doing the following:

- Check that the Recorder icon appears in the system tray.
- Open your browser and make sure the Recorder extensions appear in the extensions list.

## Enable the Chrome browser extension


To enable the Chrome browser extension for the Recorder, carry out the steps listed below on all the workstations that have the Recorder installed.

 An internet connection is required on the workstations.

1. Open or restart Chrome.
2. Click the menu button, click **More tools**, and then click **Extensions**.  
The **Extensions** screen appears.
3. Find the **ABBYY Recorder** extension in the list and enable it by using the slider.  
The Chrome browser extension is now enabled.

## Enable the Edge browser extension

To enable the Recorder Edge extension, carry out the steps listed below on all the workstations which have the Recorder installed:


 An internet connection is required on the workstations.

1. Launch a browser in Microsoft Edge.
2. Click the menu button, and then click **Extensions**.  
The **Extensions** screen displays.
3. Locate the **ABBYY Recorder** extension in the list and enable it using the slider.  
The Recorder Edge extension is now enabled.


## Enable the Firefox browser extension

To enable the Recorder Firefox extension, carry out the steps listed below on the all the workstations who have the Recorder installed:

1. Open a browser in Mozilla Firefox.
2. Click the menu button and select **Add-ons and Themes**.
3. Click **Extensions**.  
The **Extensions** screen displays.
4. Locate the **ABBYY Recorder** extension in the list and click **Enable**.

 If the extension is not listed, it may not have been installed and you will need to install it manually, see instructions [below](#).

The Recorder extension is now enabled.

 In order for the Recorder extension to work properly, the Firefox browser and the Process Intelligence Recorder must be run under the same account.

## Install the Firefox extension manually

To install the Firefox extension manually:


1. Open a browser in Mozilla Firefox.
2. Click the menu button and select **Add-ons and Themes**.
3. Click **Extensions**.  
The **Extensions** screen displays.
4. Click the Settings gear icon next to the add-on search bar and select **Install Add-on From File**.
5. Select %ABBY Recorder folder%\FirefoxExtension\abbyy\_recorder-\*.xpi and click **Open**.
6. Your Firefox browser will prompt you to install the Recorder extension. Click **Add** to allow the installation.

The Firefox extension is now installed.

## Uninstall the Recorder via the command line

To uninstall the Recorder in silent mode using the command line, open the Command Prompt and run the following command:

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

 The Recorder setup cannot remove the Recorder Firefox extension from the Mozilla Firefox browser. If you have the Recorder Firefox extension installed on workstations, you must uninstall this extension from your Firefox browser manually, see [Uninstall the Recorder Firefox extension below](#).

## Uninstall the Recorder Firefox extension

Once you have successfully uninstalled the Recorder, you must remove the Recorder Firefox extension from Mozilla Firefox manually as follows:

1. Open a browser in Mozilla Firefox.
2. Click the menu button and select **Add-ons and Themes**.
3. Click **Extensions**.  
The Extensions screen displays.
4. Locate the **ABBY Recorder** extension in the list.
5. On the right-hand side, click the ellipsis (three dots) icon and select **Remove** from the drop-down menu.

## Upgrade the Recorder

To upgrade the Recorder, run the **Abbyy.Recorder.<version>.exe** file and follow the instructions in the installation wizard.

During the upgrade process, all previous settings are maintained. This means that if you specify a new tag, it will not change on the Recording service website. To change the tag:

1. Open the Recording Service website and navigate to 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**.

## Advanced configuration

### Use OAuth to access Process Intelligence

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 the Recording Service and Process Intelligence components, it is recommended to register the Recording Service as a client on the Process Intelligence website.

 Before you begin, ensure you have administrator permissions assigned.


#### Overview


1. Register the Recording Service as a client on the Process Intelligence website and obtain credentials.  
For more information, see [Register a new OAuth client on the Process Intelligence website below](#).
2. On the Recording Service website, specify the connection details to Process Intelligence using the credentials you obtained at step 1.  
For more information, see [Configure authentication settings in the Recording Service on the next page](#).

#### Register a new OAuth client on the Process Intelligence website

1. Log into the Process Intelligence website using the credentials specified during [installation](#).
2. Navigate to **Account Settings** > **OAuth** tab and click **Register client**.

3. On the registration page, complete the following fields:
  - a. **Name** – Enter a unique name that identifies the application that you require OAuth access for. For example, RecordingService.

 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 the Recording Service. For example, `https://recorder.myCompany.com`
  - 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`

 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.
  - d. **Client logo** – This is optional. You can 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.
  - e. **Confidential client** – Select **Confidential clients** as the Recording Service is able to securely authenticate with the authorization server.
  - f. **Scopes** – Select **Read projects** and **Write projects** scope values to request access to submit data from the Recording Service to Process Intelligence. 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**.

The **Client ID** and **Client Secret** details are auto-generated.
5. Copy the **Client ID** and **Client Secret** fields for use on the Recording Service.

### Configure authentication settings in the Recording Service

1. Log into the Recording Service website you installed during [Recording Service installation](#).
2. Navigate to **Settings > Timeline authentication** and complete the following fields:
  - a. **Process Intelligence URL** – Enter the URL of the Process Intelligence website.
  - b. **Client ID** and **Client Secret** – Enter the **Client ID** and **Client Secret** you obtained after registering the client [above](#).

3. Click **Save connection** and wait for the notification to appear.

If the connection is successful, it displays **Save**. Otherwise, the following error displays: 'The server is unreachable, please notify the administrators and try again later'.

If the connection fails:

- a. Check the connection settings you specified above.
- b. Ensure the Process Intelligence website is available.
- c. Ensure the firewall settings. For more information, see [Network connection settings on page 34](#).
- d. Make sure the ports specified during the Recording Service installation are not being used by other applications. For more information, see [Check TCP/IP port availability on page 35](#).

## Configure 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 Process Intelligence and Recording Service. You can choose one of the following options:


- Use an 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.

- 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 not recommended to use a self-signed SSL certificate.

 If you install the program in a production environment, it is strongly recommended to use HTTPS instead of HTTP.

## Set up HTTPS for Process Intelligence

Below is a general sequence of steps necessary for setting up HTTPS for the Process Intelligence component:

1. Obtain an SSL certificate.
2. Extract the certificate and keys from a .pfx file.


Currently, Process Intelligence 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. See [Extract .cert and .key files from the .pfx file](#).


### 3. Set up HTTPS.

You can enable SSL and configure HTTPS during one of the following stages:

- During the Process Intelligence installation process. See [Set up HTTPS during Process Intelligence installation](#).
- After the Process Intelligence installation has completed. See [Set up HTTPS without reinstalling Process Intelligence](#).

#### Extract .cert and .key files from the .pfx file

 Ensure OpenSSL is installed on the server that contains the SSL certificate.

 Name your private key and certificate files as server.key and server.cert respectively, as Process Intelligence 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 at the previous step.  
The .cert file and the decrypted and encrypted .key files are available in the path where you started OpenSSL.
7. Rename your .cert and .key files to server.cert and server.key if you haven't done so already as Process Intelligence only accepts files with these names.

#### Set up HTTPS during Process Intelligence installation


1. Run the Process Intelligence installer and follow the on-screen instructions in the Installation Wizard. For more information, see [Install Process Intelligence on page 13](#).

2. Enable SSL between the remote PostgreSQL instance and application at the Database Connection step.  
If your remote PostgreSQL is configured with SSL support:
  - a. Select **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, select **Use CA Root certificate file** and provide the full path to your root certificate.
3. Enable SSL between application and client at the Base URL and Ports Configuration step:
  - a. Specify the TCP/IP port for the Process Intelligence website. For example, 443.
  - b. Select **Use HTTPS**.
  - c. Provide paths to server.cert, server.key, and the password files.
4. Set up a network connection for Process Intelligence. For more information, see [Network connection settings on page 34](#).
  - a. In Windows Firewall, open the rules for inbound Process Intelligence connections.
  - b. Add a TCP/IP port specified during the installation process to the exception list. For example, 443.
5. Check whether HTTPS is working as expected by opening a browser on any computer and entering the **{ProcessIntelligenceUrl}:{port}** in the address bar, where:
  - **{ProcessIntelligenceUrl}** is the Base URL you specified during the Process Intelligence installation or the public IP address or the full name of the computer where Timeline is installed.
  - **{port}** is the custom port assigned to the Process Intelligence 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 are used.Example: `https://myprocessintelligence:30443`

### Switch from HTTP to HTTPS without reinstalling Process Intelligence

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

1. Go to the computer on which Process Intelligence is installed.

 To perform all steps below, you must be a system administrator of the computer.

2. Stop the timelinepi service using the Services snap-in or open Command Prompt as administrator and use:  
`sc stop timelinepi`
3. Open the Process Intelligence installation folder and copy the server.cert and server.key to the ssl subfolder.
4. Start the timelinepi service using Services snap-in or run Command Prompt as administrator and use:  
`sc start timelinepi`



- By default, the Process Intelligence website uses the 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 Process Intelligence](#). Update the appropriate Windows Firewall rules or to the settings of any other firewall that you are using.
- Open a browser on any computer and enter **{ProcessIntelligenceUrl}:{port}** in the address bar, where:
  - {ProcessIntelligenceUrl}** is the [Base URL you specified during Process Intelligence installation](#) or the public IP address or the full name of the computer on which Process Intelligence is installed.
  - {port}** is the HTTPS port assigned to the Process Intelligence website during installation process.

Example: `https://myprocessintelligence:30443`

## Set up HTTPS for the Recording Service

Below is a general sequence of steps necessary to set up HTTPS for the Recording Service during the installation process:

- Obtain an SSL certificate.  
The SSL certificate should be installed in Microsoft IIS on the server you plan to install the Recording Service.
- Run the Recording Service installer and follow the on-screen instructions in the installation wizard. For more information, see [Install the Recording Service](#).

At the **Destination Folder** step:

- Select **Use HTTPS**.
- Select the SSL certificate from the list.

You can find the thumbprint of your certificate in the Internet Information Services (IIS) Manager:

- In the **Connections** field, select the server name (host).
  - Open **Server Certificates**.
  - Open your certificate details and find the thumbprint.
- Set up a network connection for the Recording Service. For more information, see [Network connection settings on the next page](#).
    - In Windows Firewall, open the rules for inbound Recording Service connections.
    - Add the TCP/IP port specified during the installation process to the exception list. For example, 443.
  - Check whether HTTPS works as expected by opening a browser on any computer and entering **{url}:{port}** in the address bar, 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.

### 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. In the Connections panel, select the Recording Service site.
2. In the Action panel, click **Bindings....**
3. In the Site Bindings dialog, click **Add**.  
The Add Site Binding dialog displays.
4. Select **HTTPS** and provide an SSL certificate issued to the site URL.
5. Restart the Recording Service site.

### Network connection settings

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

 Please note the following:

- The Recording Service and Process Intelligence components must be installed on separate computers. These components use different versions of PostgreSQL. They cannot be installed on one computer.
- For interaction between the Recording Service and Process Intelligence components, you must use the same protocol, for example, HTTP and HTTP, or HTTPS and HTTPS. If you are going to use Process Intelligence in the Cloud, use HTTPS.

### Process Intelligence

The Process Intelligence 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 Process Intelligence listens on.

Component name	Protocol type	Port	Traffic direction	Use
Process Intelligence	TCP/IP	80 or the port used during installation (if using HTTP) 443 or the port used during installation (if using HTTPS)	Inbound	HTTP or HTTPS connections to the Process Intelligence website.
PostgreSQL	TCP/IP	5432	Inbound	Connections to PostgreSQL database server from the remote computer where Process Intelligence 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	<ul style="list-style-type: none"> <li>• Connections to PostgreSQL database server.</li> <li>• Connections to Process Intelligence.</li> </ul>
PostgreSQL	TCP/IP	5432	Inbound	Connections to PostgreSQL database server from the remote computer where the Recording Service is hosted.

### Check TCP/IP port availability

If the Recording Service 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 application is using specified port, use the **netstat** command line:

Open the command prompt (**Start > Run > cmd**) and use **netstat -ano | find /i "<port\_number>"**.


It will show you all processes that use the 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.
- **-n** – Displays active TCP connections and port numbers in numerical form.  
If you would like 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.

### Change URL and port

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

1. Go to the computer on which Process Intelligence is installed.

 To perform all steps below, you must be a system administrator of the computer.


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

```
sc stop timelinepi
```

To ensure the correct operation of Process Intelligence, you need to stop the **timelinepi** service prior to changing the Process Intelligence configuration file.

3. Open the **Command Line** and use **netstat -a** to get a list of ports and choose an available port.
4. Find the folder where Process Intelligence is installed 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.: `<envname="PROXY_PORT" value="8080"/>`  
If you use HTTPS port, change the value for the **PROXY\_SSL\_PORT** option.  
e.g.: `<envname="PROXY_SSL_PORT" value="30443"/>`
  - b. Find the line contains **BASE\_URL** and enter the public IP address of the computer on which the ABBYY Timeline is installed in the value.  
e.g.: `<envname="BASE_URL" value="https://mytimeline.com"/>`  
or  
`<envname="BASE_URL" value="http://mytimeline.com"/>`
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
```

 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.

## Change SMTP mail server configuration

SMTP mail server configuration is done during the [Process Intelligence installation](#). You can change your mail server settings later using the **TimelinePI.xml** configuration file.

1. Go to the computer on which Process Intelligence is installed.

 To perform all steps below, you must be a system administrator of the computer.

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


```
sc stop timelinepi
```

To ensure the correct operation of Process Intelligence, you need to stop the **timelinepi** service prior to changing the Process Intelligence configuration file.

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

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

- `<envname="MAIL_SERVER_HOST" value="" />`  
This line contains the host of the SMTP mail server, enter the address in the value.  
For example, `<envname="MAIL_SERVER_HOST" value="example.smtp.com" />`
- `<envname="MAIL_SERVER_PORT" value="" />`  
This line contains the port of the SMTP mail server, enter the port in the value.  
For example, `<envname="MAIL_SERVER_PORT" value="465" />`
- This line contains the user that will be used to authenticate with the SMTP mail server, enter the username in the value.  
`<envname="MAIL_SERVER_USERNAME" value="" />`  
For example, `<envname="MAIL_SERVER_USERNAME" value="example_user" />`
- `<envname="MAIL_SERVER_PASSWORD" value="" />`  
This line contains the password of the user that will be used to authenticate with the mail server, enter the password in the value.  
For example, `<envname="MAIL_SERVER_PASSWORD" value="example_password" />`
- `<envname="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**.
- `<envname="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**.
- `<envname="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**.

 It is recommended that Process Intelligence and the Exchange server use the same TLS settings.

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

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

6. Start **timelinepi** service using **Services** snap-in or run Command Prompt as administrator and enter:

```
sc start timelinepi
```

## Update Active Directory security groups accessing Recording Service resources

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

1. Go to the workstation on which the Recording Service is installed.


To perform all activities below, you must be a system administrator of the workstation.

2. Find the folder where the Recording Service is installed and open **Appdata.production.json** using any text editor.

By default, the component is installed into C:\inetpub\ABBY Recording Service

3. 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"  
}
```


 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.

## Configure Active Directory (AD) security groups to connect the Recording Service with Recorder instances

Active Directory (AD) security groups provide access control to Recording Service:

- The Recording Service collects data from Recorders that are running on workstations. The access of workstations to the Recording Service is controlled via AD security groups.
- User permissions on the Recording Service website are also managed via AD security groups.

 AD security groups must be created prior to installing Recording Service. All machines on which the Recorder and the Recording Service are to be installed must be members of the same AD domain.

If not already present, create the following security groups in AD and add user accounts to them:

- Recording Service admin group (for example, 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.
- Recording Service user group (for example, 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.
- Recorder user group (for example, 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 the Recording Service.

## Specify AD security groups when installing the Recording Service

When installing the Recording Service and [setting the AD security groups](#), specify the names of the configured groups in the related setup fields. The name must be in the format: Domain\Group Name.

- **RS admin** – The name of the Recording Service admin group, for example, Domain\RS-admins.
- **RS user** – The name of the Recording Service user group, for example, Domain\RS-users.
- **Recorder user** – The name of the Recorder user group, for example, Domain\Recorder-users.

### Can I specify existing AD groups?

For testing purposes or if you're not a member of an AD domain, you may specify:

- RS admin and RS user – local admin user account(s)
  - Domain user in the format `Domain\UserName`
  - Local group or user in the format `ComputerName\GroupName` or `ComputerName\UserName`  
To display the computer name, open the Command Prompt (**Start > Run > cmd**) and type `hostname`.  
You may create a local group, add domain users or groups to it, and specify this group in the **Admin AD Security group** field.
- Recorder user – Everyone  
Allows any Recorder instances installed in the domain to send logs to the Recording Service.  
The format depends on your Windows locale, for example, in English: Everyone.

### How to find out which AD groups I am a member of?

1. Open the Command Prompt (**Start > Run > cmd**).
2. Enter `whoami/groups`.  
All distribution groups and nested groups will display.

### Can I change the specified groups after the Recording Service has been installed?

You can change AD security groups configuration after the Recording Server and Recorder installation. For more information, see [Update Active Directory security groups accessing Recording Service resources on page 37](#).

## Configure the Recording Service

### Configure and apply templates

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

The **Templates** page displays basic information on templates, and allows you to review the default template setting or add a custom template. All options available in the default template can be set in your custom template as well.



If your account is not added to the **Admin AD Security group** specified during the Recording Service installation, you will not have access to the site.

To configure and apply templates:


1. Open the Recording Service website and click **Templates** in the navigation menu.
2. In the **Template name** column, click **Default**. Review and modify the available options if required.



The **Default** template cannot be renamed or deleted.

- **Start recording when assigned to Recorder** – If enabled, this starts recording user actions after you assigned a template to a Recorder. The automatic start recording option is disabled by default.

- **Record screenshots** – User activity and screenshots of the applications used are recorded in logs by default. Disable this option if you do not need to save screenshots.
- **Record extended application info** – Enables the logging of the additional information required to generate a Blue Prism Capture JSON file. Enable this option if you plan to export processes from Process Intelligence for import and further refinement in Blue Prism applications.
- **Obfuscate user data** – Allows protecting sensitive information and ensuring data security by encrypting records in text logs and blurring data in screenshots. Enabled by default.
- **Scheduled recording** – Enables the scheduling of recording sessions of user activity for the Recorder instance.
- **Merge data from multiple hosts** – Enables the logging a user's activities in one log if the user works on multiple machines, for example, PC and remote desktop.

 If different tags were added to each Recorder instance during installation, they will be listed separated by commas in the resulting log. During the logging process, the list of tags may not display immediately.

The following conditions must be met before using this option:

- The Recorder is installed on every machine a user works on, and all Recorder instances display under the **Recorders** tab. In the **Host** column you can see the machine name visible on the network within the Active Directory domain.
- Each of the Recorder instances must be set to use the same template.
- **Application list** – The options to use excluded or included 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. Such events can be harder to understand and analyze when there are a lot of case and path variants and deviations which are further complicated by unnecessary data.


The default template contains a predefined excluded list, which includes the most popular messengers. Some of the information in them may not be related to the tasks that a user performs. To exclude the logging in the desired messenger, enable the Excluded List option and mark an item.

For more information on setting up **Excluded** and **Included lists**, see [Exclude and include applications](#).

- **Transformations**  
Transformations allow you to find and replace text in logs in order to redact sensitive information, such as email addresses or IDs. This option complements the **Obfuscate user data** feature. For example, transformations allow you to replace an URL or some text in logs that should remain confidential, while obfuscation allows you only to mask text data or blurs information in screenshots.  
By default, there are no transformations specified. To add transformations to the template, you need to add them to the **Transformations** tab in advance. When adding a transformation, you must specify:



- **Regular expression** – This will be used to search for text in the recorded logs.
- **Replacement**– Enter a string to replace the found text.

 Transformations added to a template are applied during the log recording to which the template is assigned. Transformations cannot be undone. For more information on using transformations, see [Add and apply transformations](#).

3. Click **Recorders** in the navigation menu to assign the template to a Recorder instance.

The list of connected recorders displays.

- a. Mark the recorder instance on which you want to set up a template and start recording.

The **Host** column displays the machine names that are visible on the network in the Active Directory domain. The **Tag** column displays tags added during the installation of Recorder instances.

- b. Click **Set Template**.


The list of available templates displays.

- c. Click the template you want to use, and then click **Select**.

- d. The recording runs automatically when the **Start recording when assigned to Recorder** option is enabled in the template. If this doesn't happen, click **Start** to run the recording.

## Exclude and include applications

Application lists can be configured to control which websites and applications are included in the logs. This should be done before starting to record logs.

 The Recorder browser extension must be installed on the user's machine for this functionality to work as expected.

To do this:

1. On the Recording Service website, click **Templates** in the navigation menu.
2. Click the template for which you want to configure application lists.
3. In the Application list pane, add a new item to the excluded and/or included list.

By default, user activities are recorded for all websites and desktop applications that users interact with on their machines. Use the Excluded List or Included List options to specify a list of websites or applications that should be excluded from, or included in your logs. Both options can be used to define a website that should be included and a subset of that to be excluded. If the same item appears in both lists, user activities will not be recorded for the specified application or website.

- To prevent the recording of user activity for a particular website or desktop application, enable the **Excluded List** option.
- To track and record user activity for a particular website or desktop application, enable the **Included List** option.

4. Click **Add item**.

The Add item dialog displays.

5. Specify the websites and/or desktop applications that you want to exclude or include. You can enter a file path, a URL, or combine valid literal paths and \* (asterisk) wildcard characters.


Examples:

- Full path to the application: C:\Program Files\ABBYY Recorder\Abbyy.Recorder.App.exe
- Using \* (asterisk) characters in the file path: \*\Abbyy.Recorder.App.exe or C:\Program Files\ABBYY\*.exe
- Using \* (asterisk) characters in the URL: https://recordingservice.abbyy.com/\* (the URL above will prevent/allow user activities to be recorded for the specified web page) or https://\*.abbyy.com/\* (the URL will prevent/allow user activities to be recorded across all the URL's sub-domains.)

6. Click **Save**.


### Examples

The examples in the table assume that the Recorder browser extensions are installed on a user's machine. If the extensions are not installed, user activities are not recorded in Google Chrome, Microsoft Edge, and Mozilla Firefox browsers.

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

Excluded List	Included List	Description
-	https://*.blueprism.com/*	Records user activities in all applications, browsers, and sites that match the https://*.blueprism.com/* template.
https://*.abbyy.com/*	-	Records user activities in all applications and browsers. Recording is disabled in the sites that match the template https://*.blueprism.com/*.
*\firefox.exe	-	Records user activities in all applications and browsers except the Firefox browser.
-	*\Chrome.exe	Records user activities only in the Google Chrome browser. Recording is disabled for other browsers and applications.
-	*\Chrome.exe, https://*.blueprism.com/*	Records user activities only in the Google Chrome browser and sites that match the specified template. For example, the following site will be recorded: <a href="https://www.blueprism.com/products/blue-prism-process-intelligence/">https://www.blueprism.com/products/blue-prism-process-intelligence/</a> Recording is disabled for other browsers and applications.

Excluded List	Included List	Description
*\firefox.exe	https://*.blueprism.com/*	Records user activities in all applications and browsers except the Firefox browser. Recording in browsers will be carried out only for sites that match the <a href="https://*.blueprism.com/">https://*.blueprism.com/</a> template.
-	*\chrome.exe, \firefox.exe, \excel.exe	Records user activities in the Google Chrome and Firefox browsers and Microsoft Excel. Recording is disabled for the Microsoft Edge browser and other applications.
*\teams.exe	-	Records user activities in all browsers. Recording is disabled for Microsoft Teams.
https://procurement.blueprism.com*	https://*.blueprism.com/*	Records user activities in all applications and browsers Recording in browsers will be carried out only for sites that match the <a href="https://*.blueprism.com/">https://*.blueprism.com/</a> templates. Recording is disabled for <a href="https://procurement.blueprism.com/">https://procurement.blueprism.com/</a> site.
-	http*, *\firefox.exe, \chrome.exe, \edge.exe	Records user activities in Google Chrome, Microsoft Edge, and Mozilla Firefox browsers. Recording is disabled for all desktop applications.

 It is not recommended to record messenger information, as often messages have sensitive information. Recording in messengers can affect the performance of the user's machine as well. The following messengers should be added to the Excluded list:

- Adium
- Atlassian HipChat
- Blackberry Messenger
- Brosix
- Cisco Jabber
- Cisco Webex
- Discord
- Facebook Messenger
- Google Hangouts
- IBM Lotus Sametime
- Lync
- Microsoft Teams
- Signal

- Skype
- Skype for Business
- Slack
- Telegram
- Viber
- WeChat
- WhatsApp

### Predefined Excluded List

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

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

### Add and apply transformations

Transformations can be used in the Recording Service to:


- Remove sensitive data that has been captured by the Recorder.

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

- Combine the names of several similar events to a common name.

If you notice similar unique strings like opening PO-BankOfAmerica and opening PO-CitiBank, you can use transformations to convert these events to a common type, for example, opening new PO. This new event can then be marked as either a start event or end event in the Task Definition Editor.

**Transformations** complement the [Obfuscate user data](#) function.

 Transformations can greatly affect the result of the automatic task definition in Process Intelligence, and they cannot be undone.

### Prerequisites

Complete the following steps before applying transformations in production environments:

1. Record a representative sample of logs for creating and testing regular expressions.

To do this:

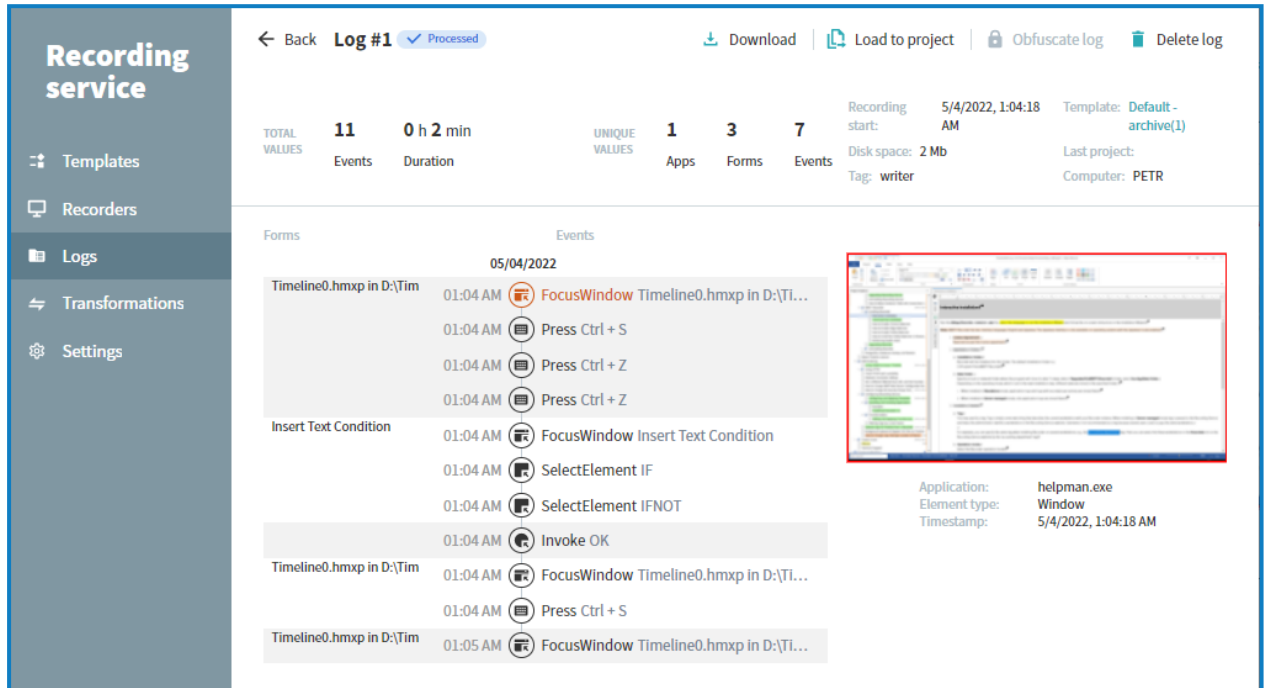
- a. Open the Recording Service website and click **Recorders** in the navigation menu.
- b. Select a Recorder instance.
- c. Make sure the correct template is assigned to this instance.
- d. Click **Start**.

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

To do this:

- a. Click **Logs** in the navigation menu.
- b. Select the log and click its **LogID**.

A window with information about the selected log displays.



This window shows all the events recorded in the current log. The selected event is highlighted and the associated screenshot is displayed, provided that you had enabled screenshot recording. The path to the application name or URL is displayed below the screenshot.

Inspect all event names and text in the URL, for example, titles, names, addresses, and other fragments of texts that should remain confidential.

3. Prepare regular expressions and replacement strings.

Examples:


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

- 4. Add transformations and apply them to one or two logs to make sure the changes are correct. For more information, see [Add transformations on the next page](#) and [Post-recording transformation on the next page](#).
- 5. Once you are satisfied with the changes, apply transformations to all recorded logs, or add them to the template to transform data on the fly.

## Add transformations

To add a transformation:

1. Click **Transformations** in the navigation menu.
2. Click **Add Transformation**.
3. Specify the transformation parameters:
  - **Regular expression** – To search for a text string, enter a regular expression using Regex syntax.
  - **Replacement** – To replace instances of the text string in logs with another string, enter the replacement string.
  - **Case insensitive** – By default, the search is case sensitive. If this option is selected, the search will be case insensitive.

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

## Apply transformations

### On-the-fly transformation


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

1. Click **Templates** in the navigation menu.
2. Click a template name or create a new one.
3. Click **Transformations** and then **Add item**.
4. In the next window, select the required transformations and click **Add**.
5. Assign the transformation to a Recorder instance.
  - a. Click **Recorders** in the navigation menu to assign the template to a Recorder instance. The list of connected recorders displays.
  - b. Mark the recorder instance on which you want to set up a template and start recording.
  - c. Click **Set Template**. The list of available templates displays.
  - d. Click the template you want to use, and then click **Select**.
  - e. The recording runs automatically when the **Start recording when assigned to Recorder** option is enabled in the template. If this doesn't happen, click **Start** to run the recording.

### Post-recording transformation

You can apply transformations to recorded logs. To do this:

1. Click **Logs** in the navigation menu.
2. Select the required logs.
3. Click **Apply transformation**.
4. In the next window, select the transformation and click **Apply to selected logs**.

 If you cancel a running transformation, the transformed portion cannot be undone.


## Filter logs by user name

If you log user activity on a terminal server, all logs are recorded under the same machine name, regardless of whether different users work on the same machine. We recommend that you enable the display of the User name column on the Logs screen to allow filtering logs by user. You can also load logs of different users to different projects.

To display the User name column on the Logs screen:

1. Navigate to the Recording Service installation folder and open the appsettings.Production.json file using a text editor.

By default, it is installed under C:\inetpub\ABBY Recording Service.

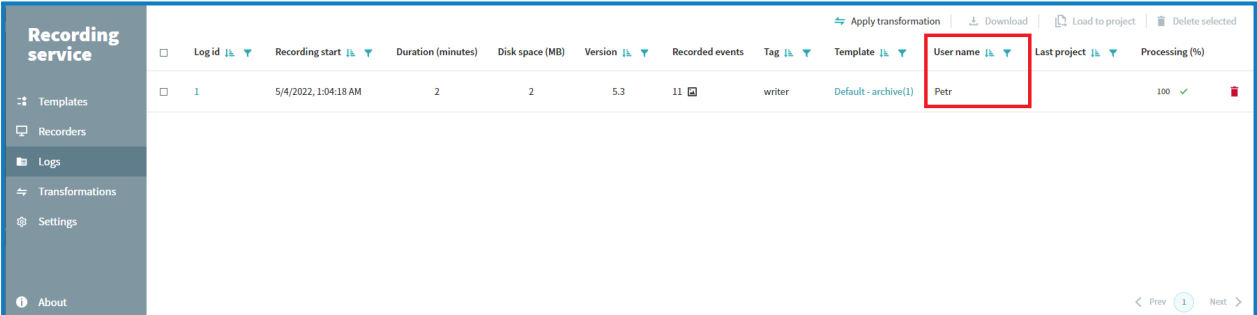
 You need administrator privileges to edit the appsettings.Production.json file.

2. Add the following line to the appsettings.Production.json file:

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

3. Save the file.
4. Restart the Recording Service website in the Internet Information Services (IIS) Manager.
5. Open the Recording Service website and click **Logs** in the navigation menu.

The User name column will display on the screen if there are recorded logs.




Log id	Recording start	Duration (minutes)	Disk space (MB)	Version	Recorded events	Tag	Template	User name	Last project	Processing (%)
1	5/4/2022, 1:04:18 AM	2	2	5.3	11	writer	Default - archive(1)	Petr		100

## Recorder logs

### View logs

1. If you have installed the Recorder in Standalone mode, run the Recorder and start recording. After the recording has stopped, the logs are available to view.
2. Click **Start > Run > ABBYY Recorder > Log Viewer** to open the Recorder Log Viewer.
3. Click **Open New** and select a local or network folder with logs.

 If you try to open invalid log folder, you will see the error message: *An error occurred: Folder <selected folder> contains no valid logs or no screenshots.* For more details, see the Input section above.

The selected log will be open in the Log Viewer. For more details, see the Log Viewer components below.



## Log Viewer components

The Recording Service Log Viewer workspace has three main components that are immediately visible:

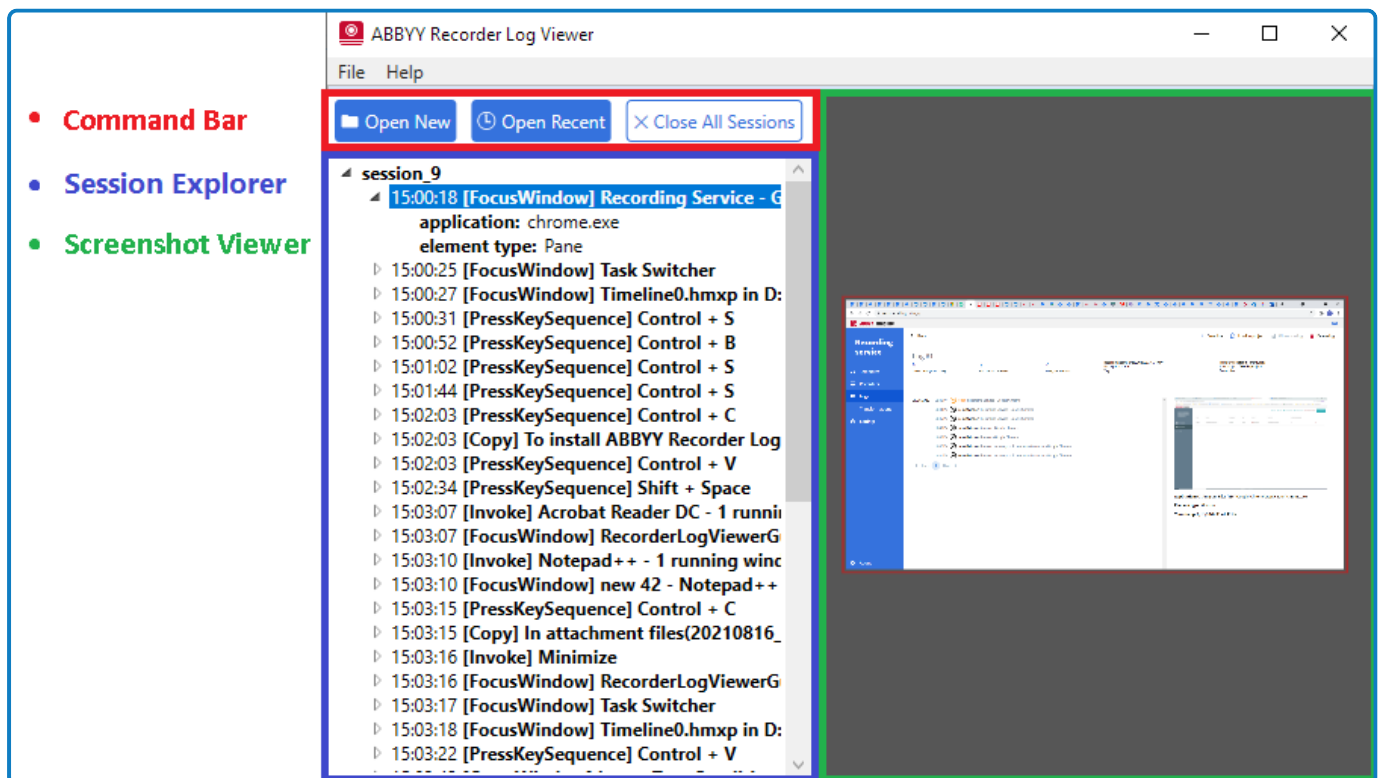
1. The **Command Bar** where you access all program functions.
  - a. To open a log, click **Open New**.  
When you open a log, its contents are displayed in **Session Explorer**. You can open multiple logs and navigate between them using **Session Explorer**.
  - b. To open one of the previously viewed logs, click **Open Recent**.  
The list shows five recent logs that you've opened. You can open a log by clicking on its entry. If the log you want isn't in the recent logs list, click **Open New** to see log locations you can browse to find the log.
  - c. To close all open logs, click **Close All Sessions**.
2. The **Session Explorer** for navigating a session of the opened logs.

This shows all recorded events in a session. For each event, you can see the following entries:

- Application – Contains the path to the application EXE file or website URL where the user performed the action.
- Element type – Optional element contains the type of item associated with the event. For example, the Window, Button.
- Value – Optional element. May contain encrypted copied or pasted text, URL if the event happened in the browser, coordinates of the mouse click in the followed format: x, y:

To close one of the open logs, select the session and click **Delete**.

3. The **Screenshot Viewer** the see the screenshots of the recorded events.



## Upload logs from a Recorder installed in standalone mode

If the Recorder is installed in standalone mode, logs are not processed and sent to the Recording Service. Thus, it is impossible to [use the Recording Service tools to upload logs](#) to Process Intelligence.


To upload logs to Process Intelligence:

1. Open the logs folder. By default, logs are saved to the %appdata%\ABBY\Recorder\Recorded folder.
2. Select the folder that contains the **Commands** and **Screenshots** subfolders and zip it. Do the same with all the folders in the logs folder.
3. Open the Process Intelligence website.
4. Create a new project or open an existing one with the **Recording Service** data source enabled (click **Project** > **Details** > **Data sources** and select **Recording Service**).

5. Select **Project** > **Upload data**.

The Upload page displays.

6. Click **Browse File** and select the ZIP file you created earlier.


 The total size of selected zip files must not exceed 10 GB.

7. Click **Upload**.
8. Once the upload is complete, navigate to **View** > **Home** and define **Tasks**.

## Background upload of zipped CSV files

The background upload feature in Process Intelligence involves monitoring a folder for files copied to it. 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 the STORAGE variable is in the TimelinePI.xml configuration file.

The ZIP file can be copied to the specified folder via an SFTP upload, or it can be an otherwise shared folder.

 It is recommended to use archiving software that supports the Deflate compression when zipping CSV files. For example, you can use 7Zip or PeaZip instead of the standard Windows archiver.

For information on configuring the background upload, see [Automated file upload via SFTP](#).

## Back up and restore the PostgreSQL databases

The Recording Service and Process Intelligence 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 Process Intelligence applications.

One of the following options can be used to back up your PostgreSQL database:

- [File system level backup on the next page](#)
- [SQL dump on the next page](#)

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

## File system level backup

This backup strategy requires to directly copy the files that PostgreSQL uses to store the data in the database. It is highly recommended to back up your Recording Service and Process Intelligence 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.

To do this:

1. Open Internet Information Services (IIS) Manager and stop the RecordingService website.
2. Shut down a PostgreSQL database server.
3. Copy the data directory.

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

If you are using SSD and HDD to store databases, copy all your PostgreSQL data directories.

4. Start the PostgreSQL database server.
5. Start the RecordingService website.

## Restoring files

To restore your database, you can use whatever method you prefer for doing a 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 above, but 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 backups.

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. It must only 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 file system level backup method is that the `pg_dump` 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 more details, see the [PostgreSQL documentation](#).

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 is the database used by the Recording Service.
- su is the user with sufficient rights.

## Restoring the dump


Dumps are restored using the `pg_restore` utility. This restores a PostgreSQL database from an archive file created by `pg_dump`. For more details, see the [PostgreSQL documentation](#).

Example of command line to restore a dump:

```
pg_restore -d RFStorage \\fileshare\backups\august_backup
```

## Move database tables 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.


 Only database tables containing screenshots can be moved to a new hard disk.

You can do this once the Recording Service installation or upgrade is complete as follows:

1. Create a folder on HDD, for example, `D:\PostgresData`.
2. Provide full access to this folder to the account used to run the PostgreSQL service.  
The default account is `NT AUTHORITY\NetworkService`
3. Perform the following actions on your PostgreSQL instance as superuser:
  - 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';`

 Skip this step if you are registering a new tablespace for Recording Service 1.1 screenshots.

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

To do this, run the command `;ALTER TABLE "Blob" SET TABLESPACE new_tablespace;`

Example: `ALTER TABLE "Blob" SET TABLESPACE slow_large_disk;`


 Even if you moved the Recording Service 1.1 screenshots table, you need to repeat this step for the Recording Service 2.0 *Blob* table. Do not move the data files for any other tables.

## Configure Twilio SMS service to receive SMS notifications from Process Intelligence

The Twilio SMS Service is configured during the [Process Intelligence installation](#). This feature allows Process Intelligence to send SMS notifications containing verification codes, alert notifications, and error messages.

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

1. On the computer where Process Intelligence is installed, stop the timelinepi service using the Services snap-in or open Command Prompt as administrator and enter: `sc stop timelinepi`  
To ensure the correct operation of Process Intelligence, you must stop the timelinepi service before changing the Process Intelligence configuration file.

 You must be a system administrator of the computer.

2. Navigate to the folder where Process Intelligence is installed and open the TimelinePI.xml configuration file using any text editor. By default, Process Intelligence is installed at C:\Program Files\Blue Prism Process Intelligence powered by ABBYY Timeline.
3. 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  
  
For example: `<env name="TWILIO_ACCOUNT_SID" value="AC3f84d59206412725a03114dfb5163e33"/>`
  - b. `<env name="TWILIO_AUTH_TOKEN" value=""/>`  
This line contains an access token that Process Intelligence needs to connect to your Twilio account.  
  
For example: `<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.  
  
For example: `<env name="TWILIO_PHONE_NUMBER" value="+121313141516"/>`
4. Save the TimelinePI.xml configuration file.
5. Start the timelinepi service using Services snap-in or run Command Prompt as administrator and enter: `sc start timelinepi`

# Troubleshooting

## Process Intelligence

### The contents of the Form editor and One task wizard windows load slowly

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

This issue will be fixed in the next release.

### High CPU utilization may be observed after installation

You may experience a CPU load increase after installing Process Intelligence. This occurs when Redis is not installed correctly, and Process Intelligence is not able to connect to Redis. Continuous connection attempts cause the high CPU utilization.

To prevent this issue, you must be an administrator on the target machine and have enough permissions to install Ubuntu on Windows Subsystem for Linux. The Ubuntu installation must also be run as an administrator.

To solve this issue:

1. Stop the timelinepi service from services.msc or open Command Prompt as an administrator and run the command `sc stop timelinepi`.
2. Open PowerShell as an administrator and run the command `wslconfig /1` to retrieve the list of all the WSL installations in your Windows system.
3. Find Ubuntu (or Ubuntu-20.04) in the list and unregister the distribution by running the appropriate command, depending on the name in the list:

```
wslconfig /u Ubuntu
```

```
wslconfig /u Ubuntu-20.04
```

4. Open Windows Explorer, navigate to the Ubuntu installation folder which you have selected for Ubuntu during the [Process Intelligence installation](#). The default folder is C:\Program Files (x86)\Ubuntu.
5. Run the ubuntu.exe (or ubuntu2004.exe) file as an administrator and follow the instructions on the screen to complete the installation.
6. When the installation has completed, run ubuntu.exe (or ubuntu2004.exe) to open Ubuntu and login as a sudo user by executing the command `sudo su`.
7. Open Ubuntu Terminal and navigate to the source folder where you originally downloaded the distribution and which you have specified when installing Process Intelligence.
8. Run the commands below to install and start Redis:
  - `dpkg -i redis-tools_6.2.4-1r11~focal1_amd64.deb`
  - `dpkg -i redis-server_6.2.4-1r11~focal1_amd64.deb`
  - `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
```

9. Start the Process Intelligence service, either from services.msc or open Command Prompt as an administrator and run the command `sc start timelinepi`.

## Recording Service

### Common issues

- The Recording Service performance is lower if using HDD only, or SSD and HDD for storing the PostgreSQL database.
- It is not recommended to store logs on the Recording Service server for more than a week. After you submit logs to Process Intelligence, you can back up the logs to another server if necessary and remove them from the Recording Service server.
- 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 display.

### The Recording Service website does not open from its shortcut in the Start menu, the shortcut opens the default website

If the Recording Service website does not open when using its shortcut in the Start menu, the shortcut opens the default website instead, and the Recording Service website is running on port 80, do the following:

1. Open Internet Information Services (IIS) Manager.
2. Find the default website in the list and stop it.
3. Start the RecordingService website.

### The Recording Service installed successfully, but an error occurred while starting the Recording Service website

If the error NET :: ERR\_CERT\_AUTHORITY\_INVALID is displayed when you try to start the Recording Service website, make sure that you specified the correct SSL certificate when installing the Recording Service. Use Internet Information Services (IIS) Manager to do the following:

1. Open Internet Information Services (IIS) Manager and select the Recording Service 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 displays.
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 Recording Service 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* displays when attempting to start the Recording Service website, make sure the connection to the PostgreSQL database 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 prevent an event recording by clicking **Disable** in their Recorder menu in the system tray. This will stop the recording 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 their 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 logs may take some time to display in the **Recordings** tab.

## Logs are partially uploaded, or the upload fails

There are some restrictions when uploading logs:

- Logs cannot be uploaded if the total number of unique events in all logs exceeds 10000. If this limit is exceeded, an attempt to upload logs fails and the error *The selected logs have more unique events than the allowed limit.* displays. 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. Navigate to the **Logs** tab.
  2. Click the logs id and check the **UNIQUE EVENTS** field.
- Logs are not fully uploaded if the size of the uploaded screenshots in the logs exceeds 25 GB. If this limit is exceeded, the following message displays: *The size of the screenshots exceeded the maximum limit for the selected logs. Some screenshots will not be uploaded.* This means that text logs were uploaded completely to the Process Intelligence project, but image logs were only partially uploaded. Screenshots larger than 25 GB were not uploaded. To solve this issue, reduce the number of logs being uploaded and try again.

## Error may occur when attempting to delete logs

When attempting to delete logs from the Recording Service, the error message *Failed to delete the following logs*, followed by the list of selected logs, may occasionally display. Try to refresh your browser cache by pressing Ctrl + F5. Alternatively, open the Recording Service in a different browser.

## 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 it. In this case, the number of logging Recorders is equal to the number of users on the terminal server.

To solve this issue, you are recommended to reduce the `ScreenshotCapturingRateFps` value in the Recorder settings file:



1. Go to the folder where the Recorder is installed and open the settings.json file using any text editor. By default, the Recorder is installed in C:\Program Files\ABBYY Recorder.


 You need administrator privileges to edit the settings.json file.

2. In the settings.json file find the following line: `"ScreenshotCapturingRateFps": 12.0`
3. Change the value for this parameter to 8.0.
4. Save the settings.json file.
5. Restart the Recorder for the changes to take effect.

You can do this using the Start menu:

- Start > ABBYY Recorder > Stop ABBYY Recorder.
- Start > ABBYY Recorder > Start ABBYY Recorder.

Or restart the ABBYY.Recorder.AutoLauncher service using Services snap-in (Start > Settings > Control Panel > Administrative Tools > Services).

 You need administrator privileges to restart the Recorder.

## Recorder may break clipboard operations such as copy/paste

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

To do this:

1. Go to the folder where the Recorder is installed and open the settings.json file using any text editor. By default, the Recorder is installed in C:\Program Files\ABBYY Recorder.


 You need administrator privileges to edit the settings.json file.

2. In the settings.json file find the following line: `"DisableClipboardTracking": false`
3. Change the value for this parameter to true.
4. Save the settings.json file.
5. Restart the Recorder for the changes to take effect.

You can do this using the Start menu:

- Start > ABBYY Recorder > Stop ABBYY Recorder.
- Start > ABBYY Recorder > Start ABBYY Recorder.

Or restart the ABBYY.Recorder.AutoLauncher service using Services snap-in (Start > Settings > Control Panel > Administrative Tools > Services).

 You need administrator privileges to restart the Recorder

## Users are using Internet Explorer 11. Will their activity still be recorded?

It is not recommended to record users' activity in an 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 the Recording Service

If the Recorder failed to connect to the Recording Service using the URL specified during the Recorder installation, it will 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](#).

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 the 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 the **settings.json** file. You can find it on the user's computer in the Recorder installation folder, by default, C:\Program Files\ABBYY Recorder.

 Administrator privileges are required to edit the **settings.json** file.

- b. Find the **ServerManagedMode** section and check the value specified in the **Url** parameter. If required, change the value and restart the **ABBYY.Recorder.AutoLauncher** service using **Services** snap-in (**Start > Settings > ControlPanel > AdministrativeTools > Services**).

 Administrator privileges are required to restart this service.

## Recorder Firefox browser extension limitations

### Firefox extension install

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

If you install this extension, the Firefox browser will launch after the Recorder setup is complete. The Firefox browser is launched under the same account that in which Recorder has just been installed and it prompts the user to enable the installation. However, the Firefox extension will be unavailable to 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's browser.
- Use the Firefox Group Policy to install the Firefox extension so it is 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 information at <https://github.com/mozilla/policy-templates/blob/master/README.md#extensionsettings>

 When upgrading the Recorder, the Firefox extension needs to be updated manually.

### Firefox extension uninstall

The Recorder setup cannot remove the Firefox extension.

Each user must remove the Recorder Firefox extension from Firefox manually. See [Uninstall the Recorder Firefox extension](#) for details.

## After a successful Recorder installation, users did not detect the Recorder extension in a browser, although it was selected for installation

1. Make sure that the user has the Recorder extension installed in a [supported browser](#), and that it is enabled. See [Install the Recorder](#) 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 Blue Prism Support to solve this issue.