Process Director Documentation

System Administrator's Guide

Last Updated: 2025-06-24, 11:26

Contents

Documentation Formatting Note

Text and Code Formatting Conventions

To highlight terms and concepts that have special relevance, this documentation implements several formatting conventions to make key words and terms more noticeable.

- Control Label: This format will identify the text labels or properties for Process Director objects, or the names of dialog boxes.
  Example: The Name text box.
- UI Element: This format will identify user interface elements such as buttons, tabs, or other UI objects used to perform interface operations.
  Example: The Submit button.
- Formal Control Name: This format will identify named Process Director controls.
  Example: A Section End control.
- Process Director Object: This format will identify named instances of Process Director Folders, Forms, Process Timelines, Knowledge Views, etc.
  Example: The Travel Expense Approval Process Timeline.
- **Key Terms**: This format will identify key terms and concepts introduced into the text of the document, and which are important to learn.
  Example: A **Case** is group of processes, transactions, or responses that define a complex activity.
- `Code`: This format will identify code samples, system variables, formulas, or other fixed programmatic syntax.
  Example: Type the following formula: `AirFare + Lodging`.
- `Code Option`: A section of a code sample to denote placeholder values that must be replaced by the user manually at design time.
  Example: `{CURR_USER, format=FormatType}`
- `Code Comment`: A section of a code sample that is used for text comments, rather than runnable code.
  Example: `// This is a comment.`
- `Code Variable`: A programming object whose value is usually determined from a command written in code.
  Example: `var formControls = BaseCurrentForm.FormControls;`

In addition to the above, extended samples of program code are presented in a special format to set them off from the rest of the text, as demonstrated below:

```
// Called after database initialized
public override void SetSystemVars(BPLo-
gix.WorkflowDirector.SDK.bp bp)
{
    // Before we make SDK calls that access the database,
    // ensure DB has been opened
    if (bp.DBOpenComplete)
    {
        // Place custom code here
    }
}
```

Important text or warnings are presented in a special callout box for special attention:

> **This is an Important item.**

Notes of general interest are also presented in special callout boxes:

> **This is a note.**

Hopefully, the use of these formatting conventions will make it easier for you to determine the various types of objects to which the text refers.

Icons

Some universal icons are used in the documentation. They are listed below:

ICON	NAME	DESCRIPTION
#	Link	A hyperlink to the specific URL and named anchor of a topic, heading, or other item.
+	Dropdown Closed	An icon that, when clicked, will expand dropdown text in a topic.
−	Dropdown Open	An icon that, when clicked, will close the expanded dropdown text in a topic.

Finally, some topic headers within each online document may display a link symbol (#) when you mouse over the header. Clicking the link will navigate to that specific section of the document, which can then be bookmarked in your browser.

Other Conventions

URLs displayed in sample will, unless used for commands or URLs used on the local host machine, use the "HTTPS" prefix by default, as modern practice has evolved to use the encryption layer to access URLs, instead of the plain-text method (HTTP) of accessing URLs.

Process Director Documentation

System Administrator's Guide

Last Updated: 2025-06-24, 11:26

System Administration Reference Guide

Welcome to the System Administration Reference Guide for BP Logix Process Director software. BP Logix specialists update Online Help regularly.

Browsing Help

You can browse the help for each documentation section by using the mini Table of Contents on the right side of the page. To switch to a different section of the documentation, you can choose the desired section from the dropdown menus in the page header. Additionally, you can navigate backwards from any page to a higher-level help topic by using the bread crumb list that is displayed at the top of the page, just above the page content.

Searching Help

The search bar enables you to search for documentation topics from any or all of the Process Director documentation topics. To search across all topics, simply enter your desired search term in the search bar. To limit the topics returned by your search, click on the search bar's Filter icon to display the list of search filters, then click on the filter you'd like to apply to your search.

User Feedback

Every topic page in the documentation has a feedback button at the bottom of each page. To provide feedback, simply click the feedback button to display the Feedback dialog box, and enter your feedback in the dialog box. Your email address will be included with your feedback as a required field, so that a documentation specialist can contact you directly.

System Administration Overview

The administration section of Process Director is completely web-based, giving you full control of accessibility anywhere. You may access the administration section by navigating to `http://[your-server-name]/admin/admin.aspx`. You must be a System Administrator or on the local server to access this area of the installation.

There are two different types of admin permissions: System Administrator and Partition Administrator.

System Administrator

A user may only be a System Administrator if the checkbox for System Administrator is checked in the user’s profile. The user can only be granted that permission by a System Administrator. A System Administrator has the ability to configure Process Director and has access to the administration section of the server. The System Administrator has a subset of permissions that can be given to an individual user.

ADMINISTRATOR TYPE	DESCRIPTION
System Configuration Admin	A subset of the System Administrator user, with access only to the Configuration tab.
System User Admin	A subset of the System Administrator user, with access only to the User Administration tab.
System Installation Admin	A subset of the System Administrator user, with access only to the Installation Settings tab.
System Troubleshooting Admin	A subset of the System Administrator user, with access only to the Troubleshooting tab.

A user can be configured with one or more of these options. If user is configured as System Administrator, all of these options are selected.

NOTE: If values are entered in the Local IP Addresses under Properties, Installation Settings, the above user settings are ignored and full access is granted as if a System Administrator.

You can also access the IT Admin area on the server **locally** without logging in.

Partition Administrator

A user may be an administrator if the user is in an “administrators” group. An administrator doesn't have access to the IT Admin area of the server, but is an administrator of the partition, which grants full permission on every Content List object on that partition, regardless of permission settings.

Custom Variables

A number of default and administrative system settings are addressed through the use of Custom Variables in the Customization file. Please refer to the Customization file topic of the Developer's Reference Guide for a complete list of these Custom Variables and their settings.

Documentation Organization

This document is divided into four main sections, each of which contains topics specific to that section. You can navigate to each section using the Table of Contents displayed on the upper right section of this page, or by using one of the links below:

IT Admin Area: Documentation about the Administrative user interface of Process Director's IT Admin area.

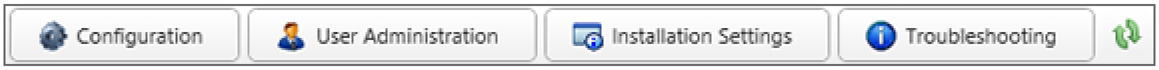
Meta Data Administration: Basic documentation about the use of Meta Data in a Process Director installation. Detailed use and implementation of Meta Data is covered in detail in the Meta Data topic of the Implementer's Reference Guide.

Common Admin Actions: Documentation about common administrative tasks and system configurations, in addition to configuration tasks that might be performed via the user interface of the IT Admin area.

Miscellaneous Administration Notes: Notes about various common issues that might occur and resolutions/workarounds that might be needed. This section primarily covers issues that arise from third-party or database component providers.

IT Admin Area

When navigating to the IT Admin area you'll see menu buttons that provide access to each section of the IT Admin area. Each section will contain pages you can use to administer Process Director.



Clicking any of the buttons will display the home page for the selected section, as well as a second series of buttons to enable you to access the different pages in that section. The highlighted buttons indicate the section and page you are currently viewing.

Each section of the IT Admin Area has a corresponding section in this chapter of the documentation. You can navigate to each section using the Table of Contents displayed on the upper right section of this page, or by using one of the links below:

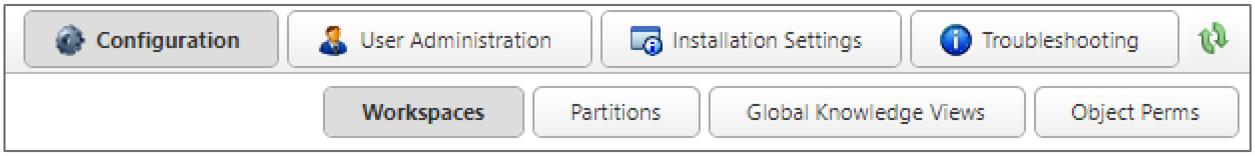
Configuration Section: This section of the documentation discusses the administration of Workspaces, Partitions, Global Knowledge Views, and Object Permissions.

User Administration Section: This section of the documentation discusses the administration of Users, Groups, Authentication Settings, Delegation, User Directory Synchronization, User Permissions, and User References.

Installation Settings Section: This section of the documentation discusses the administration of Properties, Global Vairables, Database Settings, and Licensing.

Troubleshooting Section: This section of the documentation discusses the administration of Sever Control actions, System Information, User Impersonation, Audit and System Logs, and running Email Tests on the system.

Configuration Section



This section of the IT Admin area enables you to configure the Workspaces, Partitions, and Global Knowledge Views in your installation. Additionally, this section contains an Object Perms page to create a report of object permissions on your system. Workspaces will be discussed below, while the linked topics will cover the remaining items in this section of the IT Admin area.

When importing XML files from another system, always import the Partition XML file first, then Global Knowledge Views, and the Workspaces last.

The Configuration section consists of four configuration pages. You can navigate to each page using the Table of Contents displayed at the upper left corner of the page, or use the links below.

Workspaces: Defines the appearance and content on a user’s homepage, or home pages, if the user is member of more than one workspace.

Partitions: Separate data stores or independent sections of a Process Director installation which don't interact with each other or share data.

Global Knowledge Views: Knowledge Views that are available to all users across all partitions.

Object Perms: A searchable permissions report that indicates which users have access to which Process Director Objects, and the permissions they've been granted.

Workspaces

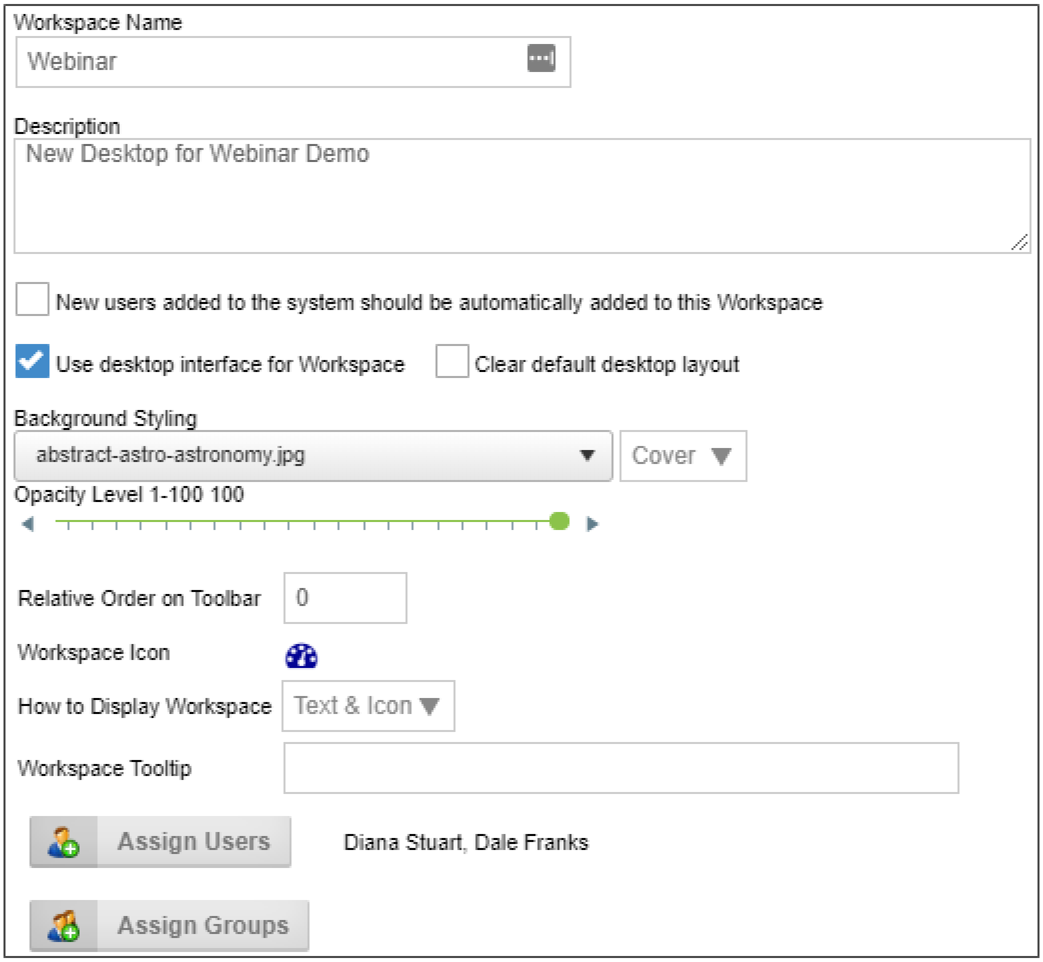
A workspace defines the appearance and content on a user’s homepage (similar to a portal). A workspace lets you configure multiple ways to display your Process Director Homepage. A default workspace consists of a Top Navigation and Homepage Windows which displays the content you want. You can Create, Edit and Delete a workspace in the list displayed. Once you have created a workspace you'll assign users and/or groups to that workspace. If a user is assigned to more than 1 workspace, additional tabs will be available on the homepage that displays the list of workspaces to which they are assigned.

> ⓘ **For Process Director v4.5 and higher, an additional user interface for the Workspace, the Desktop Interface, is also provided. Please see the Desktop Interface topic of the Implementer's Guide for more information about this feature, and its differences from the default Workspace. Some Workspace properties are only relevant top the Desktop interface.**

Creating Workspaces

To add a new workspace, create it by clicking on the Create Workspace Actions Link, which will open the configuration screen for the new workspace.

The workspace configuration screen is composed of two separate sections. The top section contains the workspace options.



Workspace Name
Webinar

Description
New Desktop for Webinar Demo

□ New users added to the system should be automatically added to this Workspace

☑ Use desktop interface for Workspace □ Clear default desktop layout

Background Styling
abstract-astro-astronomy.jpg ▼ Cover ▼
Opacity Level 1-100 100

Relative Order on Toolbar 0

Workspace Icon

How to Display Workspace Text & Icon ▼

Workspace Tooltip

Diana Stuart, Dale Franks

The bottom section of the workspace configuration screen contains a tabbed interface, containing tabs to configure the Top Navigation Buttons, the Home Page Windows, and the Advanced Options.

Workspace Options

To configure a new workspace, edit the following options:

Workspace Name

The Workspace Name property is the name that will display in Process Director's interfaced tabs at the top of the screen. As such, the name, while it should be appropriately descriptive, should also be brief, so that it can be displayed without the tab taking up too much screen space.

Description

Type in a brief description of the Workspace's purpose and the type of users who should be assigned to it.

New users added to the system should automatically be added to this workspace

Checking this option ensures that, whenever any new user us added to Process Director, the user will automatically be added as a member of this workspace.

Use desktop interface for Workspace

For users of Process Director v5.23 and higher, the Desktop interface for Workspaces is available. The Desktop interface enables users to customize the visual appearance of their Workspace. Please see the Desktop Workspace topic for a description of how end users view the workspace.

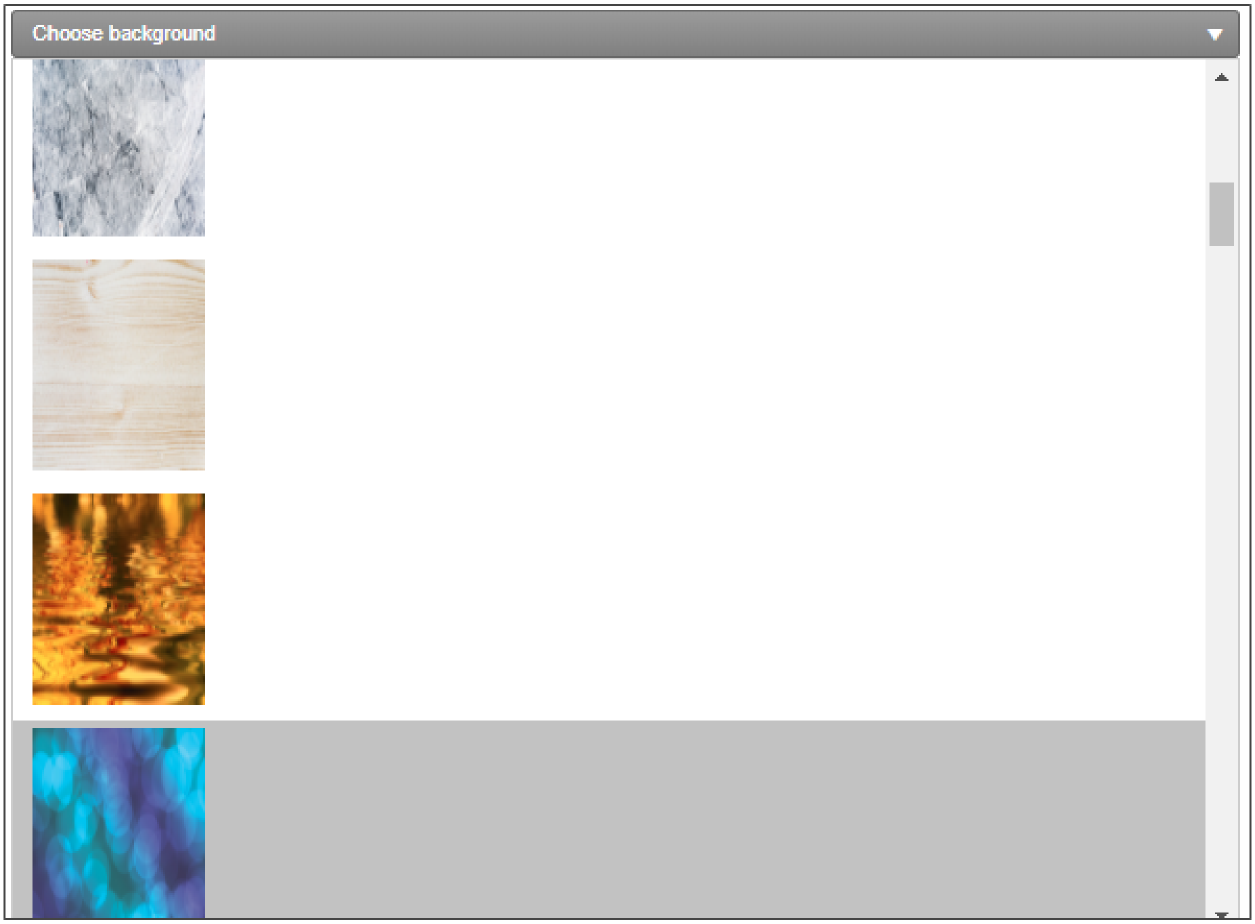
> ⓘ **For Process Director v6.1.200 and below, the Desktop interface is not compatible with the operation of Case Management applications, due to the way that opening Case instances works in the product.**

Clear default desktop layout

This will clear customized Workspaces for end users.

Background Styling

This option enables you to select an image from a dropdown control that contains a number of stock background images, and will use that image as a background image for the Workspace.



Next to the image dropdown, an additional Background Image Sizing dropdown enables you to specify how the background image will appear on the form. The following options are available:

- Cover: The image will expand to fill the entire page background.
- Center: The image will appear in its actual size, centered on the page vertically and horizontally.
- Tile: The image will appear in its actual size, aligned to the top left of the window, and will tile vertically and horizontally.
- Tile X: The image will appear in its actual size, aligned to the top left of the window, and will tile along the X-axis only.
- Tile X: The image will appear in its actual size, aligned to the top left of the window, and will tile along the Y-axis only.

Finally, an Opacity Level property enables you to set the opacity percentage by changing a slider value from 0 to 100.

Relative Order on Toolbar

You can change the order in which workspace tabs appear on the workspace bar by entering a number into this property.

Workspace Icon

This property identifies the icon that will appear on the workspace tab, in addition to the text, if desired. To change the icon, click on the default icon to open the Icon Chooser, which will display all of the standard Process Director icons, as well as any custom icons added to the installation. You can select a different icon by simply clicking on the icon you desire. The Icon Chooser will close and the icon you selected will automatically appear in the Workspace Icon property.

How to display workspace

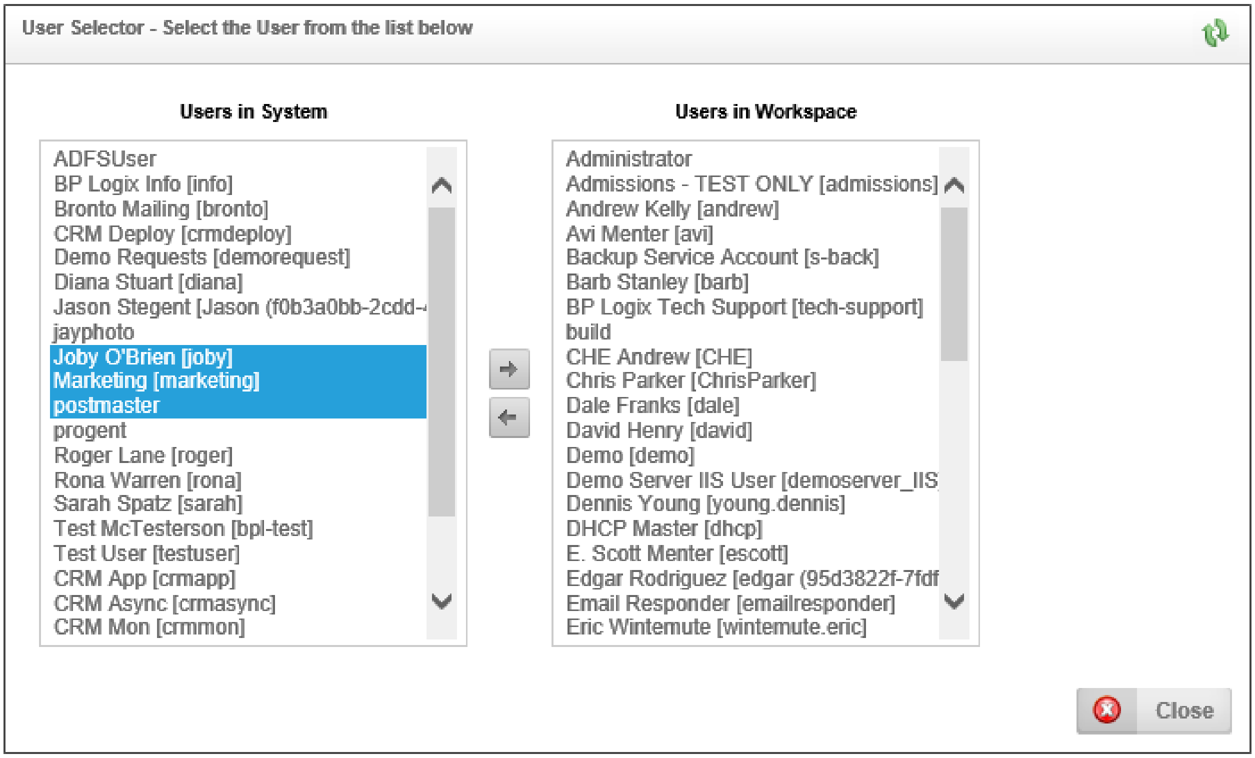
The workspace tab can be displayed with only the icon, only the workspace name, or both the icon and workspace name.

Workspace Tooltip

The Workspace Tooltip property defines the text you desire to have displayed in a popup tooltip when users place the mouse over the workspace tab.

Assigning Users

Clicking on the Assign Users button will open the User Selector dialog box, which enables you to select users to assign to the workspace.



User Selector - Select the User from the list below

Users in System

ADFSUser
BP Logix Info [info]
Bronto Mailing [bronto]
CRM Deploy [crmdeploy]
Demo Requests [demorequest]
Diana Stuart [diana]
Jason Stegent [Jason (f0b3a0bb-2cdd-
jayphoto
Joby O'Brien [joby]
Marketing [marketing]
postmaster
progent
Roger Lane [roger]
Rona Warren [rona]
Sarah Spatz [sarah]
Test McTesterson [bpl-test]
Test User [testuser]
CRM App [crmapp]
CRM Async [crmasync]
CRM Mon [crmmon]

Users in Workspace

Administrator
Admissions - TEST ONLY [admissions]
Andrew Kelly [andrew]
Avi Menter [avi]
Backup Service Account [s-back]
Barb Stanley [barb]
BP Logix Tech Support [tech-support]
build
CHE Andrew [CHE]
Chris Parker [ChrisParker]
Dale Franks [dale]
David Henry [david]
Demo [demo]
Demo Server IIS User [demoserver_IIS
Dennis Young [young.dennis]
DHCP Master [dhcp]
E. Scott Menter [escott]
Edgar Rodriguez [edgar (95d3822f-7fdf
Email Responder [emailresponder]
Eric Wintemute [wintemute.eric]

To assign a user, or users, to the workspace. Select the user(s) in the Users in System list box by clicking on them with your mouse. To select multiple contiguous users, you can press and hold the right mouse button while dragging the mouse over the list of users. To select multiple non-contiguous users from the list, press and hold the [CTRL] key on a Windows PC or the [COMMAND] key on a Macintosh PC while clicking on the individual users you wish to select. Once the users are highlighted, add them to the Users in Workspace list box by clicking the Add button.

→

To remove users from the Users in Workspace list box, select the users you wish to remove from the list box, and click the Remove button.

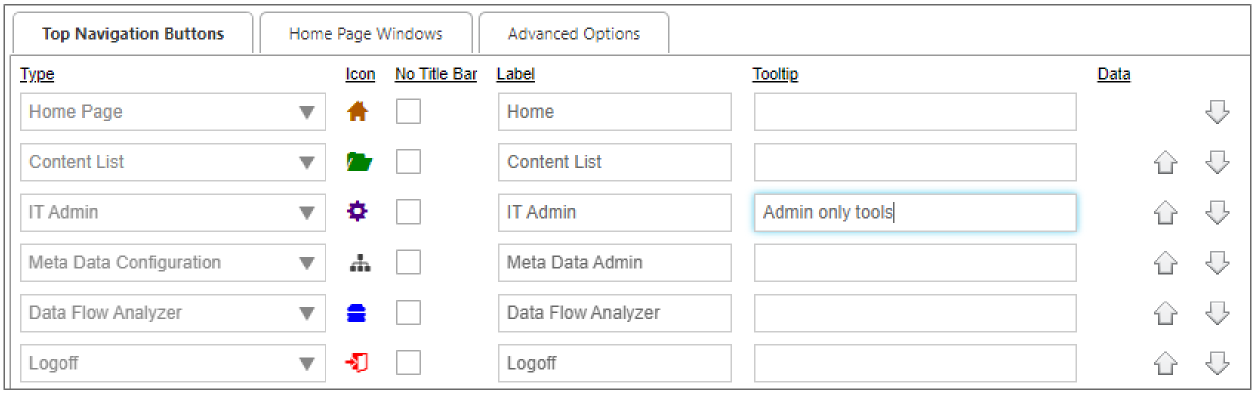
←

Assigning Groups

Clicking on the Assign Groups button will open the Group Selector dialog box, which enables you to select groups to assign to the workspace. This functionality works just like the Assign Users functionality.

Top Navigation Buttons #

Specify the navigation buttons to display at the top of the Homepage. Specify the type of button, the name of the button and optional icon, and if any, the additional configuration for the button. You can also specify the tooltip that displays when the user mouses over the button, as well as in what order the button appears in the navigation bar.



Top Navigation Buttons | Home Page Windows | Advanced Options

Type	Icon	No Title Bar	Label	Tooltip	Data	
Home Page ▼	🏠	☐	Home			⇩
Content List ▼	📂	☐	Content List			⇧ ⇩
IT Admin ▼	⚙	☐	IT Admin	Admin only tools		⇧ ⇩
Meta Data Configuration ▼	🖧	☐	Meta Data Admin			⇧ ⇩
Data Flow Analyzer ▼	☰	☐	Data Flow Analyzer			⇧ ⇩
Logoff ▼	⇥	☐	Logoff			⇧ ⇩

For Process Director v6.1.0 and higher, many of the available Workspace navigation button types are already built into the product UI. Items such as IT Admin, Logout, Content List, Meta Data Admin, etc., are now permanently displayed in the UI for users with the appropriate permissions. These items will no longer be displayed as Navigation buttons in the Workspace. This change will enable you to use the available space for custom items, rather than having to configure navigation buttons for items that are already displayed to the user by default.

Button Types

The available button types are described in the table below.

TYPE	DESCRIPTION
Button Not Used	This doesn't display any button.
Home Page	Links to the home page of the Workspace.
Meta Data Configuration	Links to the Meta Data configuration.
IT Admin	Links to the IT Admin area.

TYPE	DESCRIPTION
User Settings	Links to the currently logged in user profile settings.
Logoff	Logs off the current user.
Partition Knowledge View (...)	Links to a specified Knowledge View in a partition.
Partition Report (...)	Links to a specified report in a partition. ⓘ **This option won't appear for users who don't have the Advanced Reporting component.**
Partition Chart(...)	Links to a specified Chart in a partition.
Partition Dashboard(...)	Links to a specified Dashboard in a partition.
Partition Form (...)	Links to a specific Form Definition in a partition.
Specific URL (...)	Links to a specific URL (e.g. http://www.-google.com).
Execute JavaScript	Enables you to run a JavaScript command when the button is pressed. When selected, a JavaScript input box will appear, into which you can place any JavaScript command. For example, you can use the “window.open” JavaScript command to open a new browser window.
All Knowledge Views and Reports	Links to a Global Knowledge View that lists all Knowledge Views and Reports to which the current logged in user has permissions.
Content List	Links to a Content List to which the current logged in user has permissions.
Find Forms With Value	Links to a Knowledge View that will search any form field on any form.

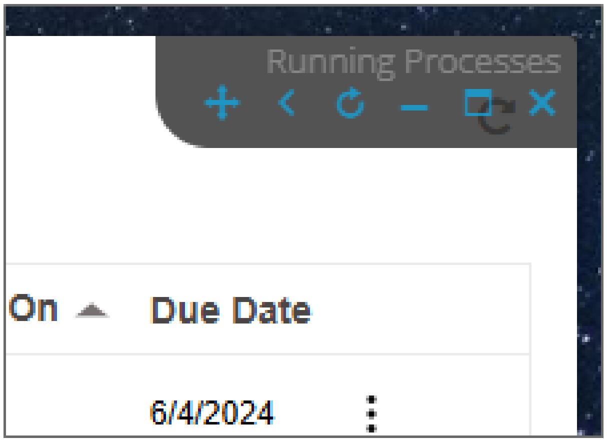
TYPE	DESCRIPTION
Forms I Can Submit	Links to a Knowledge View that returns forms the current user is allowed to submit.
Running Processes	Links to a Knowledge View that returns a list of running processes.
Task List	Links to a Knowledge View that returns a list of tasks that are assigned to you.

Icon

The Icon property identifies the icon that will appear on the navigation button. Clicking on the default iron will open the Icon Chooser dialog box, from which you can select the icon you desire to display as the button icon.

No Title Bar

This property is relevant only to the Desktop workspace type. When checked, the default title bars for each portlet will be removed. Mousing over the portlet will display a small title/function bar in the upper right corner of the portlet.



Label

The label property specifies the text that will appear on the navigation button.

Tooltip

The Tooltip property defines the text you desire to have displayed in a popup tooltip when users place the mouse over the navigation button.

Data

The Data property is used for navigation buttons that point to a Content List item. The property consists of a Picker control from which you can choose the Content List item to which you wish to navigate.

Order

You can change the order of the workspace navigation buttons using the arrow buttons to move a button up or down in the button list.

Process Director v6.1.0 UI Changes

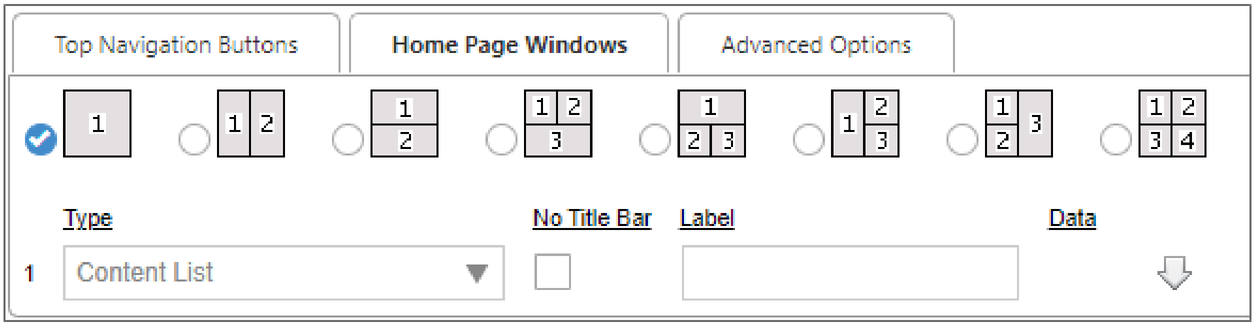
For Process Director v6.1.0 and higher, navigation buttons for items that are built directly into the new Navigator UI no longer appear in the Workspace Navigation Bar. In previous versions, access to the IT Admin area, Meta Data Admin, etc., were provided as Navigation Bar items, since they were not included in the main product UI. With the Navigator UI, these items can be accessed directly via the product UI, so there's no need to include them in your Workspace navigation scheme any more. Removing built-in UI items from the Workspace Navigation Bar frees up screen space to add additional custom items of your own. This change enables you build truly custom Workspace navigation schemes without worrying about needing to include standard UI items in the Workspace.

Upgrading to v6.1.0 will not change the Workspace configuration, and these built-in items, if included in the Workspace configuration will still appear in the Top Navigation Buttons tab of the Workspace configuration screen. They just won't display in the Workspace Navigation Bar for end users.

Home Page Windows #

Specify the Homepage Windows by selecting the window template and associate a type for each window. Each line will correspond with the window number. Each window can be defined to display different content.

When multiple portlets are displayed in a workspace, each portlet is divided by splitter bars. The user can manually drag and drop the splitter bars to new positions to resize the portlets. Additionally, the splitter bars will show on mobile devices with thicker bars to allows resizing the bars easier on touchscreens. The width of the splitter bar can be customized using the SplitterWidth custom variable.



	Type	No Title Bar	Label	Data
1	Content List	□		

The first selection you can make is the desired page layout. The row of radio buttons illustrate the number and arrangement of the portlets that will appear on the page. A portlet is a window on a page inside of which is displayed a Content List item, such as a report, Form, report, etc. You can select to display up to four portlets on the home page in a variety of arrangements, each of which is illustrated by a small sample page diagram.

Below the selection for the layout of the portlets, a list of Portlet configuration controls will appear, based on the layout you select.

Type

These are the available portlet types you can select from the Type property dropdown controls.

Window Types

These are the available Portlet types.

TYPE	DESCRIPTION
Meta Data Configuration	Links to the Meta Data configuration
IT Admin	Links to the IT Admin area.
User Settings	Links to the currently logged in user profile settings.
Data Flow Analyzer	Links to the Process Director Data Flow Analyzer.
Partition Knowledge View (...)	Links to a specific Knowledge View in a partition
Partition Report (...)	Links to a specific Report in a partition.
Partition Chart (...)	Links to a specific Chart in a partition.

TYPE	DESCRIPTION
Partition Dashboard (...)	Links to a specific Dashboard in a partition
Specific URL (...)	Links to a specific URL (e.g. http://www.google.com). You may type the actual URL, or use a custom variable to provide the URL by using the syntax "{customvar:VAR_NAME}", where VAR_NAME is the name of the custom variable you create. Refer to the Developer's Guide for information on how to create custom variables.
Partition Form (...)	Links to a specific Form in a partition.
Partition Form Instance (...)	Links to a specific Form Instance in a partition.
All Knowledge Views and Reports	Links to a Global Knowledge View that lists all Knowledge Views and Reports the current logged in user has permission to.
Content List	Links to a Content List the current logged in user has permission to.
Forms I Can Submit	Links to a Knowledge View that returns Forms the current user is allowed to submit
In-Process Forms	Links to a Knowledge View that returns a list of Forms that are being used in running processes
Running Processes	Links to a Knowledge View that returns a list of running processes
Task List	Links to a Knowledge View that returns a list of tasks that are assigned to you.

ⓘ **When the Workspace displays a Dashboard as a portlet, the Dashboard can be exported with the Workspace.**

No Title Bar

This property is relevant only to the Desktop workspace type. When checked, the default title bars for each portlet will be removed. Mousing over the portlet will display a small title/function bar in the upper right corner of the portlet.

Label

This property is relevant only to the Desktop workspace type. When configured, the default object name will be replaced with the Label you provide, if any, in this setting. If you leave the Label property blank, the default object name will be displayed as the portlet title.

Data

The Data property for each window type will appear as a Picker control, from which you can select a Content List item that is appropriate for the selected Type property.

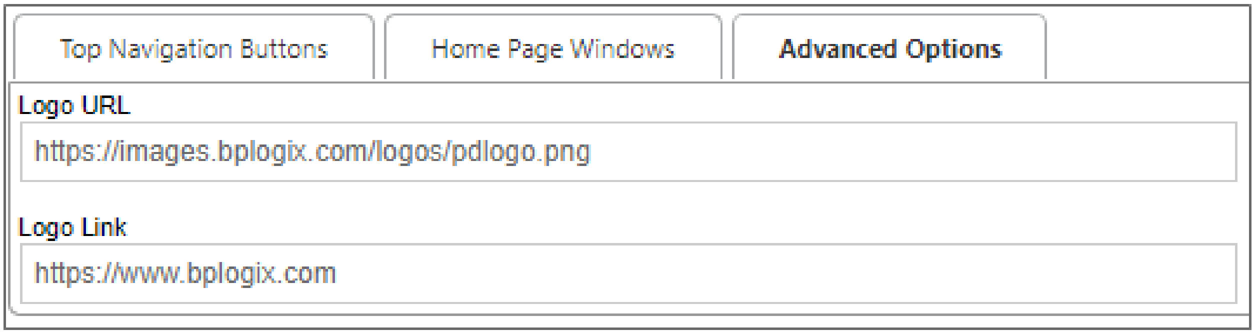
Order

You can change the order of the workspace navigation buttons using the arrow buttons to move a button up or down in the button list.

ⓘ **When using the Desktop interface for a Workspace, ALL navigation buttons and portlets can be customized by the end user as Workspace windows, and the configuration desired by the end user can be saved as their default layout. Please see the Desktop Workspace topic for more information about how end users see and can customize the Desktop Workspace.**

Advanced Options

Specify the advanced options. A specific logo and link can be selected for this profile.



Logo URL
https://images.bplogix.com/logos/pdlogo.png

Logo Link
https://www.bplogix.com

Logo URL

Enter a URL of an image to display in place of the default BP Logix logo. For best results, the logo image should be sized to approximately 120x30 pixels.

Logo Link

Enter the URL to which the user should be directed when clicking the logo image. The default link is to the BP Logix web site.

Direct URL Access to a Workspace

Hotlinks can be used to directly access a specific workspace on the system. To access a workspace directly via a URL, use the following syntax in the address bar of your browser:

```
http://server_name/home.aspx?profile=profile_name
```

Where `server_name` is the host where Process Director is installed and `profile_name` is the name of the workspace. A user must be a member of the workspace for the page to be displayed.

Continue

Continue to the documentation for the Partitions page.

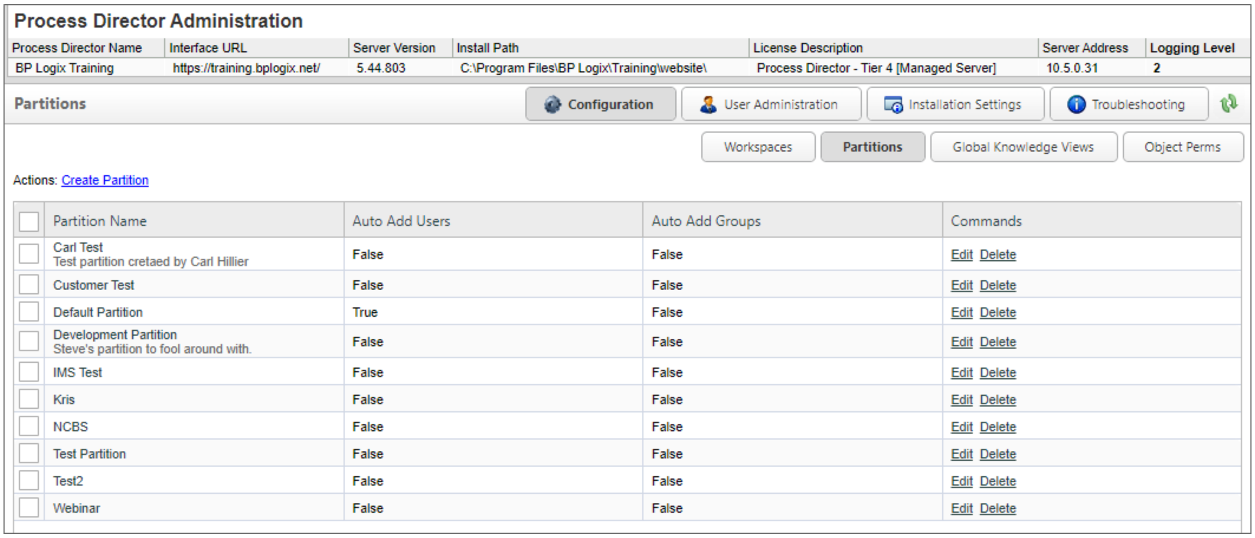
Partitions

Process Director enables you to create partitions in an installation, if needed. **Partitions** function as separate data stores or independent sections of a Process Director installation. Objects stored in one partition can't interact with objects stored in a different partition. Similarly, users assigned to one partition can't see or work with objects stored in a different partition. One common use of partitions is to segregate sensitive data from data that is more generally accessible. For instance, Process Director objects that support HR operations, which often use sensitive privacy data, can be placed in a partition that can only be accessed by HR personnel.

By default, a Process Director installation contains only one partition, known as the "Default" partition. Additional partitions, if necessary, can be added by system administrators.

Partitioning a system can provide secure grouping of users, documents, permissions and processes. Users can belong to multiple partitions, but this is only required when a system must be logically divided into multiple server partitions (e.g. application service providers). All users are automatically a member of the default partition (named “Default Partition”). Information can be shared across partitions for more flexibility with business processes.

The Partitions page of the IT Admin area's Configuration section displays a list of partitions on the system. You can create, edit and delete partitions from the list displayed. Once you have created your partition, click on the Edit link next to that partition. You can now administer the users and groups in that partition.



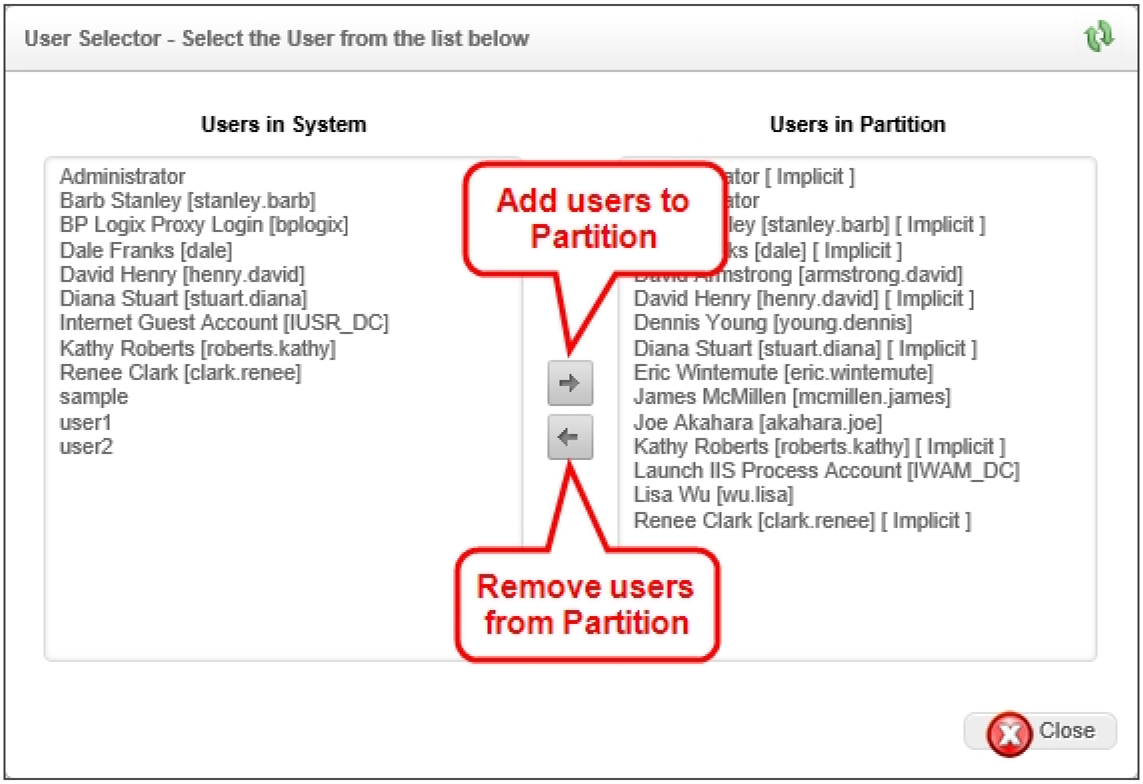
Process Director Administration

Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
BP Logix Training	https://training.bplogix.net/	5.44.803	C:\Program Files\BP Logix\Training\website\	Process Director - Tier 4 [Managed Server]	10.5.0.31	2

Actions: Create Partition

□	Partition Name	Auto Add Users	Auto Add Groups	Commands
□	Carl Test Test partition cretaed by Carl Hillier	False	False	Edit Delete
□	Customer Test	False	False	Edit Delete
□	Default Partition	True	False	Edit Delete
□	Development Partition Steve's partition to fool around with.	False	False	Edit Delete
□	IMS Test	False	False	Edit Delete
□	Kris	False	False	Edit Delete
□	NCBS	False	False	Edit Delete
□	Test Partition	False	False	Edit Delete
□	Test2	False	False	Edit Delete
□	Webinar	False	False	Edit Delete

When adding users and groups you'll notice that some users might have “[Implicit]” next to the user name. This implies that they were added to the partition through a group. If a group is added to a partition that the user is a member of, the user will be added. If the group was removed the user will be removed. “[Implicit]” won't show if the user was added directly.



Users in System

Administrator
Barb Stanley [stanley.barb]
BP Logix Proxy Login [bplogix]
Dale Franks [dale]
David Henry [henry.david]
Diana Stuart [stuart.diana]
Internet Guest Account [IUSR_DC]
Kathy Roberts [roberts.kathy]
Renee Clark [clark.renee]
sample
user1
user2

Users in Partition

ator [Implicit]
ator
ley [stanley.barb] [Implicit]
ks [dale] [Implicit]
mstrong [armstrong.david]
David Henry [henry.david] [Implicit]
Dennis Young [young.dennis]
Diana Stuart [stuart.diana] [Implicit]
Eric Wintemute [eric.wintemute]
James McMillen [mcmillen.james]
Joe Akahara [akahara.joe]
Kathy Roberts [roberts.kathy] [Implicit]
Launch IIS Process Account [IWAM_DC]
Lisa Wu [wu.lisa]
Renee Clark [clark.renee] [Implicit]

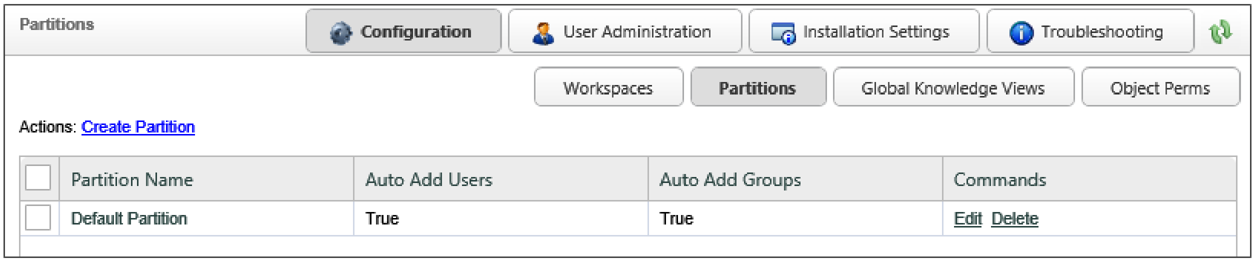
Add users to Partition

Remove users from Partition

> ⓘ **When importing XML/PDZ files from another system, always import the Partition files first, then Global Knowledge Views, and the Profiles last.**

Creating a Partition

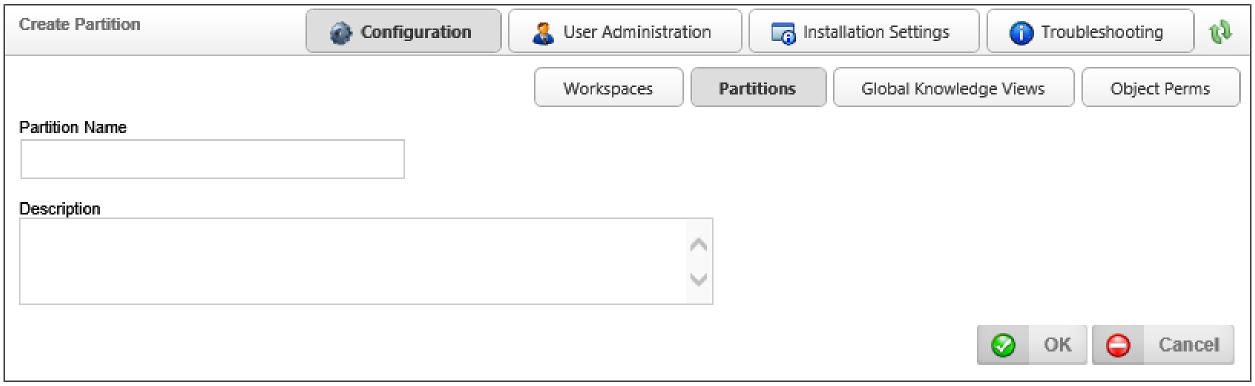
In the Configuration section of the IT Admin area, click the Partitions button to view the Partitions page. The Partitions page will display a list of the current partitions.



Actions: Create Partition

□	Partition Name	Auto Add Users	Auto Add Groups	Commands
□	Default Partition	True	True	Edit Delete

To create a new partition, click the Create Partition link in the Actions links displayed on the upper left portion of the screen. Clicking the Create Partition link will open the Create Partition screen.



Partition Name

Description

In the Partition Name property text box, enter the name for the partition, then enter a brief description in the Description property field. When you have entered a name and description, click the OK button to create the partition, and open the Edit Partition screen. In the Edit Partition screen, there are some additional properties that can be set.

New users added to the system should be automatically added to this partition

If this box is checked, then every time a new user is added to Process Director, the user will automatically be added to this partition.

New groups added to the system should be automatically added to this partition

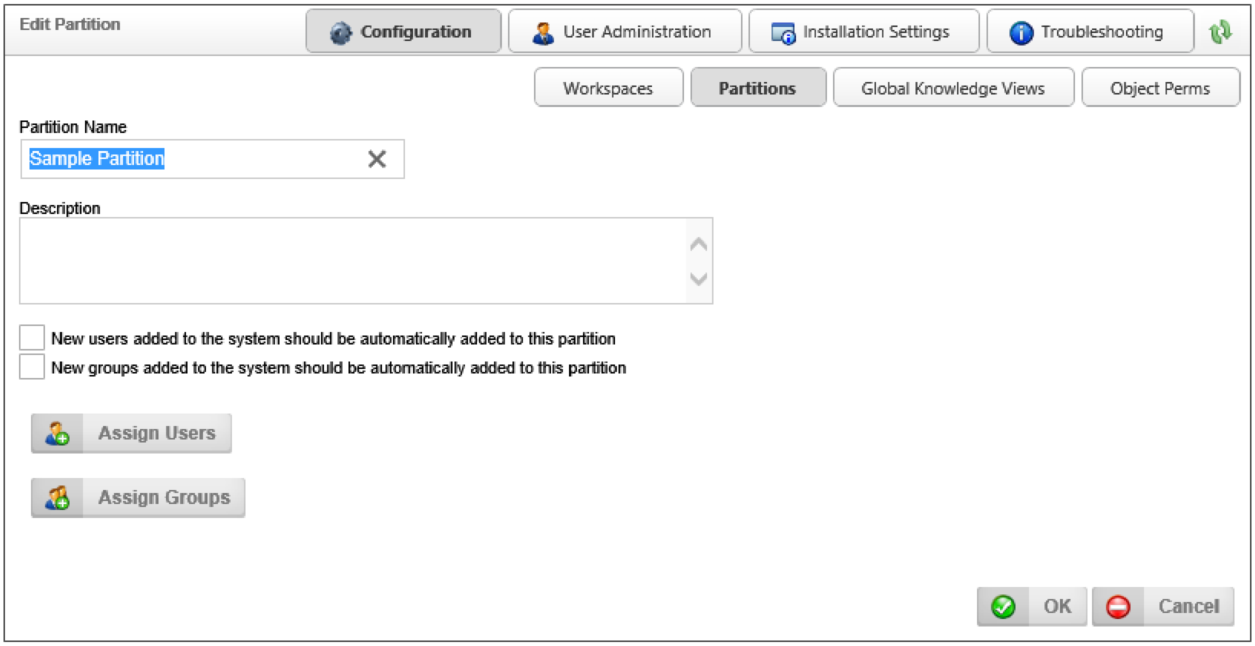
If this box is checked, then every time a new user group is added to Process Director, it will automatically be added to this partition.

Assign Users

Clicking on the Assign Users button will open the User Selector dialog box, which enables you to select users to assign to the partition.

Assign Groups

Clicking on the Assign Groups button will open the Group Selector dialog box, which enables you to select groups to assign to the workspace.



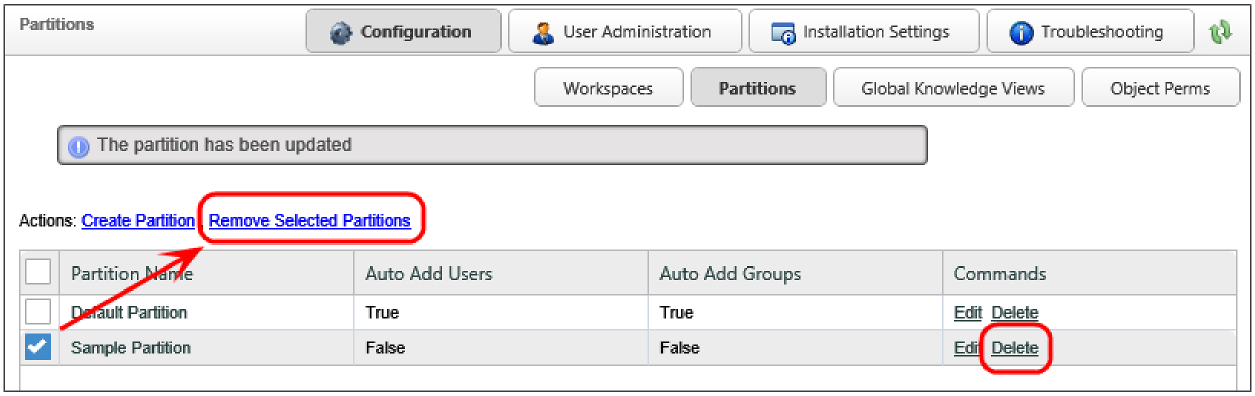
Partition Name
Sample Partition

Description

□ New users added to the system should be automatically added to this partition
□ New groups added to the system should be automatically added to this partition

Deleting a Partition

Once a partition has been created, you can delete the partition from the Partitions page. Each partition has a Delete link in the Commands column that you can click to select the partition. Additionally, you can remove multiple partitions at the same time by checking the check box next to the partition names, which will cause a Remove Selected Partitions link to appear in the actions links at the top of the page. Once you have checked the partitions you wish to remove, click the Remove Selected Partitions link.



The partition has been updated

Actions: Create Partition | Remove Selected Partitions

□	Partition Name	Auto Add Users	Auto Add Groups	Commands
□	Default Partition	True	True	Edit Delete
☑	Sample Partition	False	False	Edit Delete

Continue

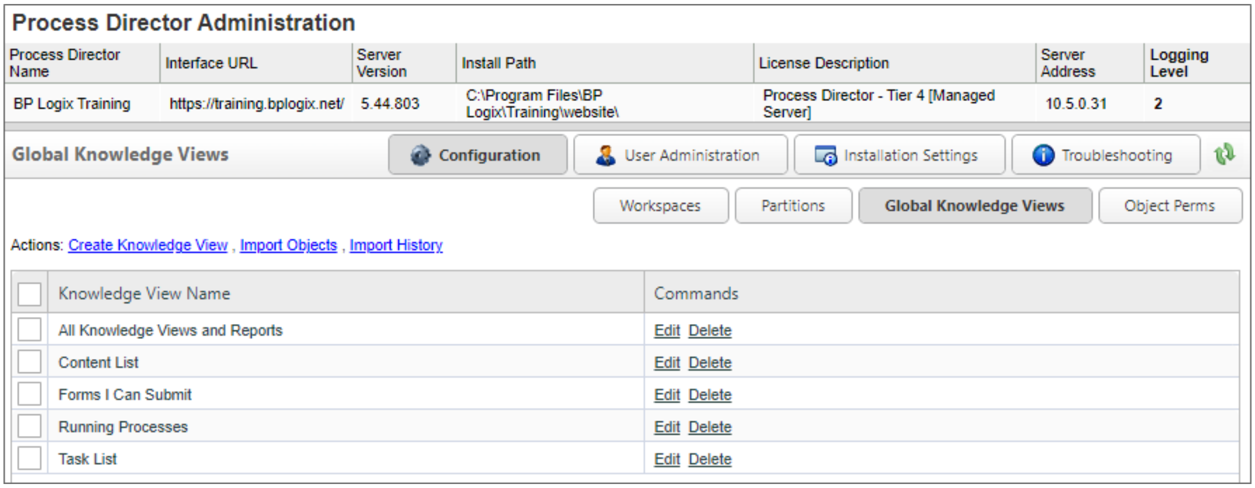
Continue to the documentation for the Global Knowledge Views page.

Global Knowledge Views

A **Global Knowledge View** is a Knowledge View that is available to all users across all partitions. By default, Global Knowledge Views are created as Content List Knowledge Views. All lists in Process Director, including the Content List are Global Knowledge Views. These Global Knowledge Views have functions and options similar to specific Knowledge Views in a partition. A Global Knowledge View has some restrictions on the data in columns and filters. Data that is specific to a partition can't be used (e.g. Form fields, categories), and won't be made available to users who create Global Knowledge Views

ⓘ When importing XML/PDZ files from another system, always import the Partition files first, then Global Knowledge Views, and the Profiles last.

Global Knowledge Views can be accessed by clicking the Global Knowledge Views button in the Configuration section of the IT Admin area.



Process Director Administration

Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
BP Logix Training	https://training.bplogix.net/	5.44.803	C:\Program Files\BP Logix\Training\website\	Process Director - Tier 4 [Managed Server]	10.5.0.31	2

Global Knowledge Views

Actions: Create Knowledge View , Import Objects , Import History

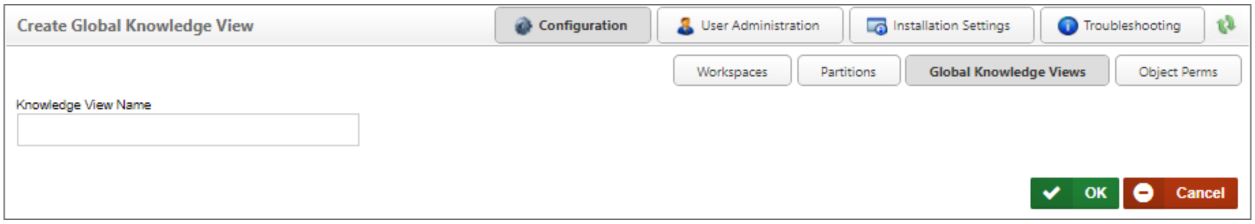
□	Knowledge View Name	Commands
□	All Knowledge Views and Reports	Edit Delete
□	Content List	Edit Delete
□	Forms I Can Submit	Edit Delete
□	Running Processes	Edit Delete
□	Task List	Edit Delete

One common use of Global Knowledge Views is to create customized task lists and custom content lists. They can also be used to provide metrics for system usage.

! BP Logix recommends that you don't edit any of the default Global Knowledge Views, as doing so will fundamentally alter the operation of Process Director for end users.

Creating Global Knowledge Views

To create a new item, click the Create Knowledge View action link. The Create Global Knowledge View dialog box will appear.

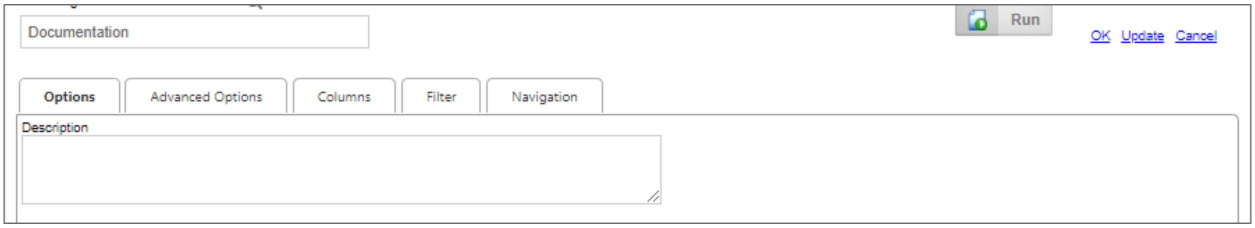

Create Global Knowledge View

Knowledge View Name

Provide the Knowledge View Name and click the OK button to close the dialog and open the new Global Knowledge View definition.

Configuring a Global Knowledge View

As mentioned previously, Global Knowledge Views are available across all partitions, to all users, and thus can't display partition-specific information. The properties available for a Global Knowledge View, therefore, is a subset of the properties that are available to you when creating a normal Knowledge View inside the Content List, i.e., a partition Knowledge View. The tabbed interface is slightly different as well, using horizontal, rather than vertical tabs, with the tabs named slightly differently.


Documentation

Description

In the Global Knowledge View, the Options tab contains the property settings you'd normally find on the Configure tab of a partition Knowledge View, while the Advanced Options tab contains the properties found on the Options tab of a partition Knowledge View. The properties are largely the same, though the Global Knowledge Views has fewer configurable properties. One notable exception to property locations is the Knowledge View Type property, which is found on the Advanced Options tab of the Global Knowledge View. Additionally, configuring the Global Knowledge View's navigation structure, if any, is performed on its own tab, named Navigation. The Columns and Filter tab of the Global Knowledge View is largely the same as those used in the configuration for a partition Knowledge View.

Since all of the available properties for a Global Knowledge View are also detailed in the Knowledge View Definitions topic of the Implementer's Guide, we won't replicate them here. Please refer to that topic for property configuration.

Process Director v6.0 and Higher

A new property on the Options tab of the Global Knowledge View definition, Use Process Director 6.0 style, displays the Knowledge View with the updated styles used in, as the property indicates, Process Director v6.0 and higher.

For Process Director v6.1.0 and higher, a default name has been applied to the Content List Global Knowledge View via a system variable: `{FOLDER_PATH, nulll="Content List"}`. This ensures that the appropriate folder path appears as the page title in the Content List, or, if no folder path exists, the title will be “Content List”. This value can be overwritten in the Global Knowledge View by administrators.

Other Considerations

The Process Director Content List, Task List, Forms I Can Submit, and other universal items are, by default, generated from Global Knowledge Views. Changes to any of the existing Global Knowledge Views on your system will have unexpected results. Once again, BP Logix recommends that you don't edit any of the default Global Knowledge Views, as doing so will fundamentally alter the operation of Process Director for end users.

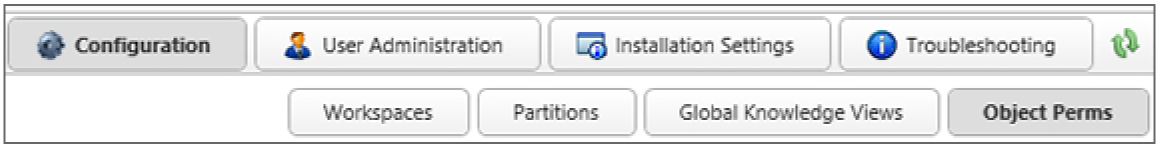
The best practice is to create new Global Knowledge Views, if necessary, to display in Workspaces, Dashboards, or other interface elements. In most cases, however, the creation of new Global Knowledge Views is unnecessary. Remember, creating a Global Knowledge View is only needed if you wish to expose the Knowledge Views to all users in the organization.

Continue

Continue to the documentation for the Object Perms page.

Object Permissions

Administrators of Subscription, Cloud, or on-Premise installations with the Compliance Option will notice an additional Object Perms button in the IT Admin interface. Process Director provides a searchable report of all object permissions on the Object Perms page.



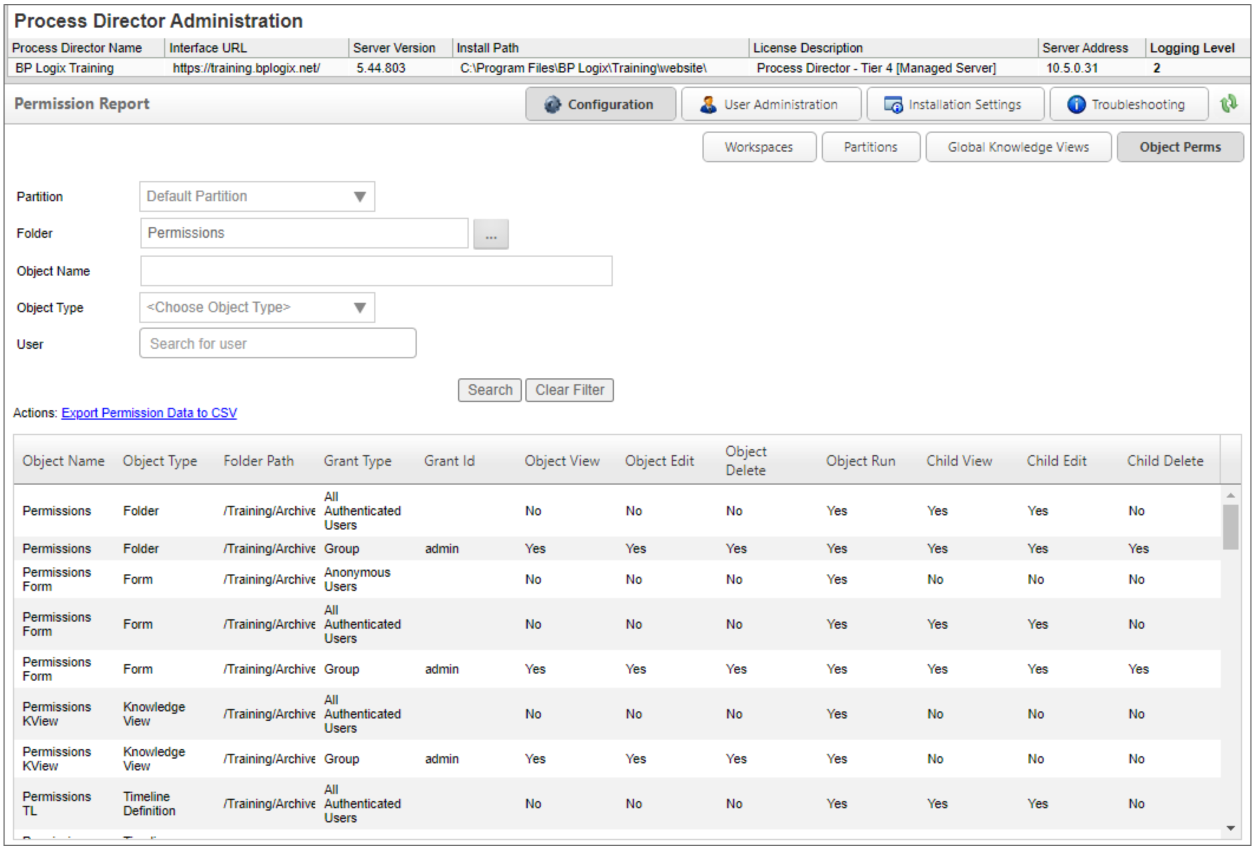
The Object Perms page enables you to find specific objects and view a report of permissions that are applicable to that object.

In the top portion of the Object Perms page, there are five filter fields you can use to create relatively specific searches to return a list of only those permissions that interest you. You can filter the object permissions by:

- Partition
- Folder
- Object Name
- Object Type
- User

Entering a value in any or all of the filter fields, then clicking the Search button will display only object permissions that match the entered values. You can clear all of your search filters and start from scratch with a new search by clicking the Clear Filter button.

Each object displayed in the search results identifies the object, folder path, grant type, and a column for each of the permissions.



Process Director Administration

Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
BP Logix Training	https://training.bplogix.net/	5.44.803	C:\Program Files\BP Logix\Training\website\	Process Director - Tier 4 [Managed Server]	10.5.0.31	2

Permission Report

Partition: Default Partition

Folder: Permissions

Object Name:

Object Type: <Choose Object Type>

User: Search for user

Actions: Export Permission Data to CSV

Object Name	Object Type	Folder Path	Grant Type	Grant Id	Object View	Object Edit	Object Delete	Object Run	Child View	Child Edit	Child Delete
Permissions	Folder	/Training/Archive	All Authenticated Users		No	No	No	Yes	Yes	Yes	No
Permissions	Folder	/Training/Archive	Group	admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Permissions Form	Form	/Training/Archive	Anonymous Users		No	No	No	Yes	No	No	No
Permissions Form	Form	/Training/Archive	All Authenticated Users		No	No	No	Yes	Yes	Yes	No
Permissions Form	Form	/Training/Archive	Group	admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Permissions KView	Knowledge View	/Training/Archive	All Authenticated Users		No	No	No	Yes	No	No	No
Permissions KView	Knowledge View	/Training/Archive	Group	admin	Yes	Yes	Yes	Yes	No	No	No
Permissions TL	Timeline Definition	/Training/Archive	All Authenticated Users		No	No	No	Yes	Yes	Yes	No

The resulting list of object permissions can be exported to a comma-separated text file that is viewable in Excel by clicking the link labeled, Export Permission Data to CSV.

User Administration

You can manage users and groups remotely through the web-based IT Admin area. You can access this section by navigating to the User Administration section of the IT Admin area.

Process Director organizes users in the database as follows:

+ partitions

    + users

    + groups

        + users

Users or groups can be members of partitions. Users can also belong to multiple groups, allowing for role based administration.

The following User IDs will be created on a new Process Director installation. These users have no passwords and have been given full permission to all objects.

- Administrator
- user1
- user2

The following group is created on a new Process Director installation. The user named Administrator is a member of this group.

- admin

Users may fall into one of two primary classes:

- Authenticated users have a named Process Director user account. This account may either be Built-In or Windows account. All of these users are positively authenticated in the system prior to granting access. Authenticated users may have full access as regular licensed users, or may have intermittent access to the system through an additional licensed component that assigns temporary day passes to the user that expire in, as their name suggests, one day.
- Unauthenticated users don't have a user account, and their access to the system is governed by a license component that issues a pass to the user that enables them to access the system—either anonymously, or by identifying them via an email address—for a single access instance.

Cloud users that are licensed for *any* day passes should pre-load/configure all named users who may consume day passes, prior to their use. All that's required is the UserID, authentication mechanism(such as SAML or built-in login, and the license type. This list of temporary users can be entered annually, or loaded using the Excel import feature in the User Administration page. If you use a self-provisioning for new users, then the self-provisioned user will consume day passes unless their user record is updated manually by the administrator. Setting the DefaultNewUsersToDayPass custom variable will force all new users to be added as day pass users.

User Administration Pages

The User Administration section enables access to the administrative pages that manage users, groups, and other user-related system settings. You can navigate to each section using the Table of Contents displayed on the upper right section of this page, or by using one of the links below:

Users: This page is where system users are created and managed.

Groups: This page is where user Groups are created an managed.

Authentication Settings: Where the different authentication methods are configured.

Delegation: Where delegation of tasks between users are created and managed.

User Directory Synchronization: Where you can create directory synchronization profiles to create and synchronize users sourced from your Active Directory or other LDAP systems.

User Perms: Where you can view user permissions.

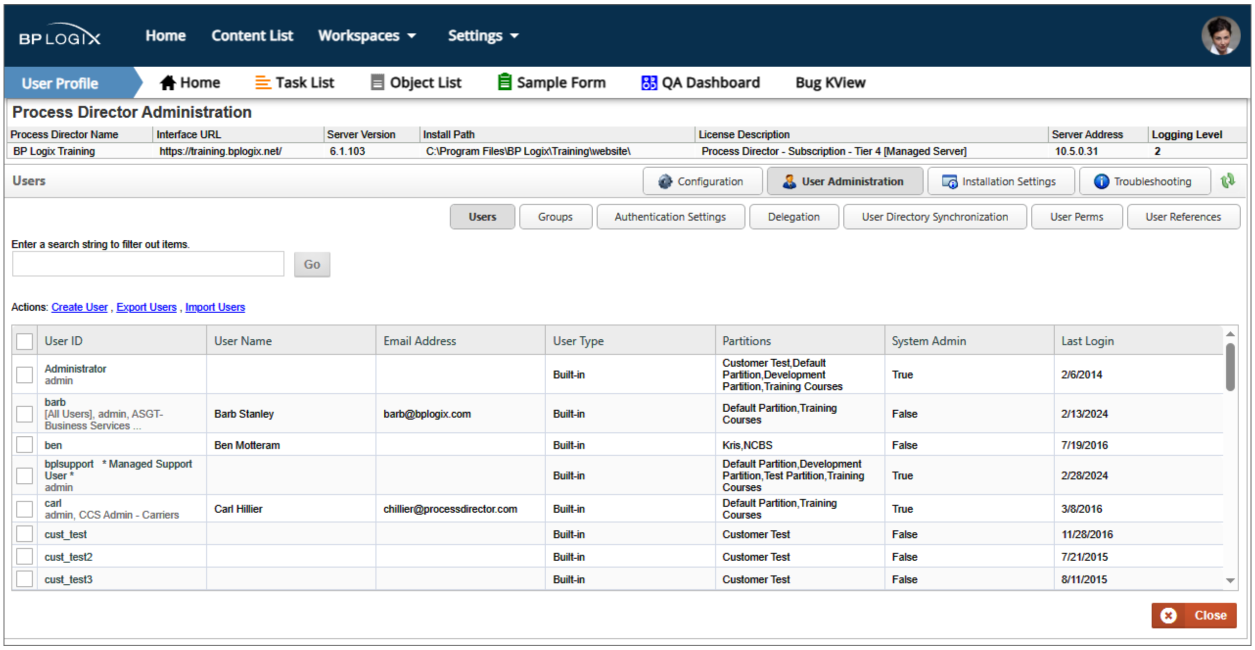
User References: Where you can view and search a list of Content List objects that reference specific users on your system.

Users Page

Process Director users are created and managed from the Users page of the User Administration section.

Searching Users

The Users page displays a list of users on the system.



Process Director Administration

Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
BP Logix Training	https://training.bplogix.net/	6.1.103	C:\Program Files\BP Logix\Training\website\	Process Director - Subscription - Tier 4 [Managed Server]	10.5.0.31	2

Users

Enter a search string to filter out items.

Actions: Create User , Export Users , Import Users

☐	User ID	User Name	Email Address	User Type	Partitions	System Admin	Last Login
☐	Administrator admin			Built-in	Customer Test,Default Partition,Development Partition,Training Courses	True	2/6/2014
☐	barb [All Users], admin, ASGT-Business Services ...	Barb Stanley	barb@bplogix.com	Built-in	Default Partition,Training Courses	False	2/13/2024
☐	ben	Ben Motteram		Built-in	Kris,NCBS	False	7/19/2016
☐	bplsupport * Managed Support User * admin			Built-in	Default Partition,Development Partition,Test Partition,Training Courses	True	2/28/2024
☐	carl admin, CCS Admin - Carriers	Carl Hillier	chillier@processdirector.com	Built-in	Default Partition,Training Courses	True	3/8/2016
☐	cust_test			Built-in	Customer Test	False	11/28/2016
☐	cust_test2			Built-in	Customer Test	False	7/21/2015
☐	cust_test3			Built-in	Customer Test	False	8/11/2015

Systems with a large number of users, i.e., more than 100, will see a search box at the upper left corner of the page to search for specific users via User ID. For Process Director v5.44.800 and higher, the search box will, when a value is entered, search all user attributes that are displayed in the User List, such as Group names, to return the matching users, as an improvement to this search feature.

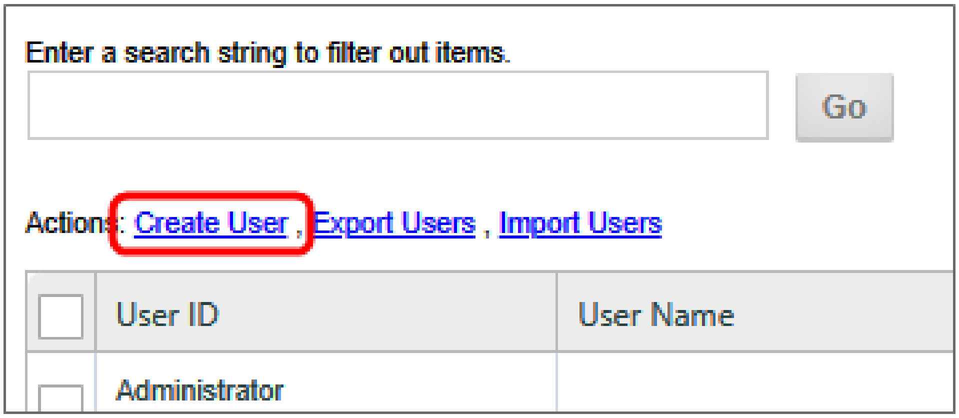
For Process Director v6.1.300 and higher, an additional check box, labeled Extended Search (slower) will perform a more comprehensive, though slower, search for users that match the specified attribute entered in the search box.

Adding a New User

This section describes how to add users to Process Director using built-in user accounts. This isn't required for users that are created by Windows SSO, synchronization with your LDAP server, or an external authentication system (SAML).

For built-in users, a User ID and password must be added to the Process Director database before a login can occur. When a user is configured in the Process Director database, additional information such as the user’s email address and alias can be configured.

On the Users page of the IT Admin area's User Administration section, click on the Create User link. This will prompt you to enter a User ID for the new user. Please Note: This will create a built-in user, not a Windows user.



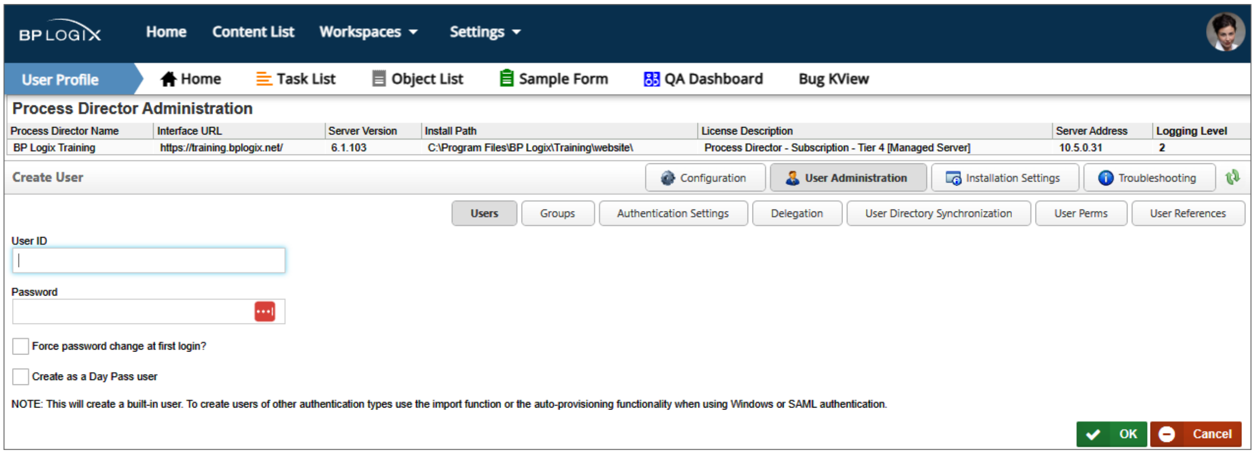
Enter a search string to filter out items.

Actions: Create User , Export Users , Import Users

□	User ID	User Name
□	Administrator	

Create User Screen

This screen enables you to specify the new user to add to the Users list.



Process Director Administration

Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
BP Logix Training	https://training.bplogix.net/	6.1.103	C:\Program Files\BP Logix\Training\website\	Process Director - Subscription - Tier 4 [Managed Server]	10.5.0.31	2

Create User

User ID

Password

□ Force password change at first login?

□ Create as a Day Pass user

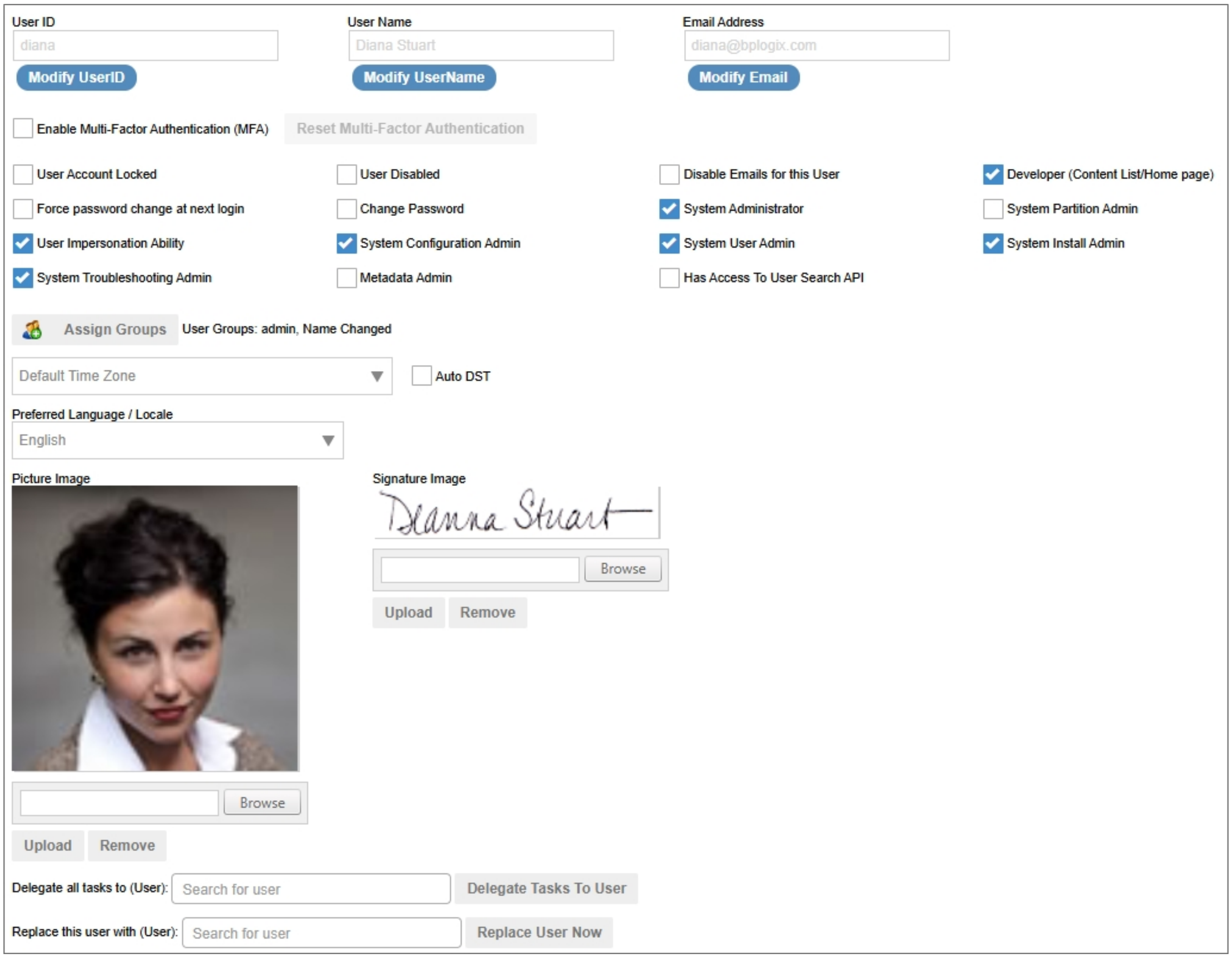
NOTE: This will create a built-in user. To create users of other authentication types use the import function or the auto-provisioning functionality when using Windows or SAML authentication.

Enter the user’s User ID and Password. You can force the user to change his password upon login. Click OK when done. After you create the user, you can click on the “Edit” link next to the user’s name and configure it further.

The User ID will also serve as the user’s login user name for Process Director. BP Logix highly recommends that administrators ensure that User ID’s are unique to each user. This may not be possible, however, when using SAML authentication for existing users where duplicate user names exist. In this case the SAML authentication must send a unique GUID or identifier for the users. There is a variable in the custom vars file called fAuthSAMLAllowDuplicateUserIDs that must be set to “true” to allow this behavior.

❗ In many cases, Process Director will return a comma-separated list of users. Since the users are identified by UserName, we strongly recommend that your users names do *not* include commas as part of the user name.

User Properties



User ID: diana

User Name: Diana Stuart

Email Address: diana@bplogix.com

□ Enable Multi-Factor Authentication (MFA)

□ User Account Locked	□ User Disabled	□ Disable Emails for this User	☑ Developer (Content List/Home page)
□ Force password change at next login	□ Change Password	☑ System Administrator	□ System Partition Admin
☑ User Impersonation Ability	☑ System Configuration Admin	☑ System User Admin	☑ System Install Admin
☑ System Troubleshooting Admin	□ Metadata Admin	□ Has Access To User Search API	

User Groups: admin, Name Changed

Default Time Zone ▼ □ Auto DST

Preferred Language / Locale: English ▼

Picture Image

Signature Image: Dianna Stuart

Delegate all tasks to (User): Search for user

Replace this user with (User): Search for user

For Process Director v6.1.200 and higher, the User ID, User Name, and Email Address properties can only be edited by clicking the Modify... button adjacent to each property to activate it. This feature was implemented to prevent password managers, like LastPass, from inadvertently altering the values in their property fields.

To set the user’s account properties, click on the Edit hotlink in the user's row of the user list. The Edit User configuration will display, with the User ID and User Name fields already configured. You may configure the remaining user properties.

Email Address

Enter an email address that will be associated with the user in the Email Address field. You can change the password by checking the Change Password box; an input field will appear prompting for a new password. Click OK to save the configuration.

Multi-Factor Authentication (MFA) Properties

Process Director v6.1.300 and higher enables the use of Multi-Factor Authentication (MFA) for Built-in user accounts. There are two MFA properties.

The Enable Multi-Factor Authentication (MFA) property will, when checked, activate the use of MFA for the specified user account.

The Reset Multi-Factor Authentication button will reset the existing MFA token sequence and require the user to create a new MFA token in their authenticator app.

Please see the Using Multi-Factor Authentication (MFA) topic for more details on how MFA is implemented in Process Director.

Miscellaneous Account Settings

Additional check boxes enable you to configure the following settings:

SETTING	DESCRIPTION
User Account Locked	Prevents the user from logging in, but does not disable the user account. This setting may be automatically applied if the user fails to enter their login credentials properly after a specified number of tries. This setting applies primarily to Built-In users.
User Disabled	Disables the user account, preventing the user from participating in any tasks, and deleting the user's participation from any existing tasks.
Disable Emails for this User	Prevents Process Director emails from being sent to the user.
Developer (Home Page/Content List)	For Process Director v6.1 and higher, this property gives users access to the new Content List menu and Home Page. While the Content List menu is visible by default to system administrators, non-administrative users must have

SETTING	DESCRIPTION
	this property checked in order to see it. This property enables you to give developers/implementers access to the full UI, without providing any access to the IT Admin section of the installation.
Force password change at next login	Force the user to change their password on the next login attempt.
Change Password	When checked, a text box will appear that enables you to enter a new password for the user.
Mobile App User	This setting appears only for installations that are licensed for the Mobile Application Component, with the appropriate mobile app custom variables configured properly. Checking this property indicates that the user will be granted access to the Mobile Application.
Mobile Admin User	This setting appears only for installations that are licensed for the Mobile Application Component, with the appropriate mobile app custom variables configured properly. Checking this property indicates that the user will be granted access to the Mobile Server as an administrator.

❗ If Mobile App User or Mobile Admin User are checked, the users will automatically be imported into the Mobile Application server as users with the appropriate levels of access. Only Mobile Admin Users can access the administrative UI of the mobile server, and only Mobile App Users will be granted access to the Mobile Application on their mobile device. A user who is both an app and admin user will need to have both properties checked.

Administrative Settings

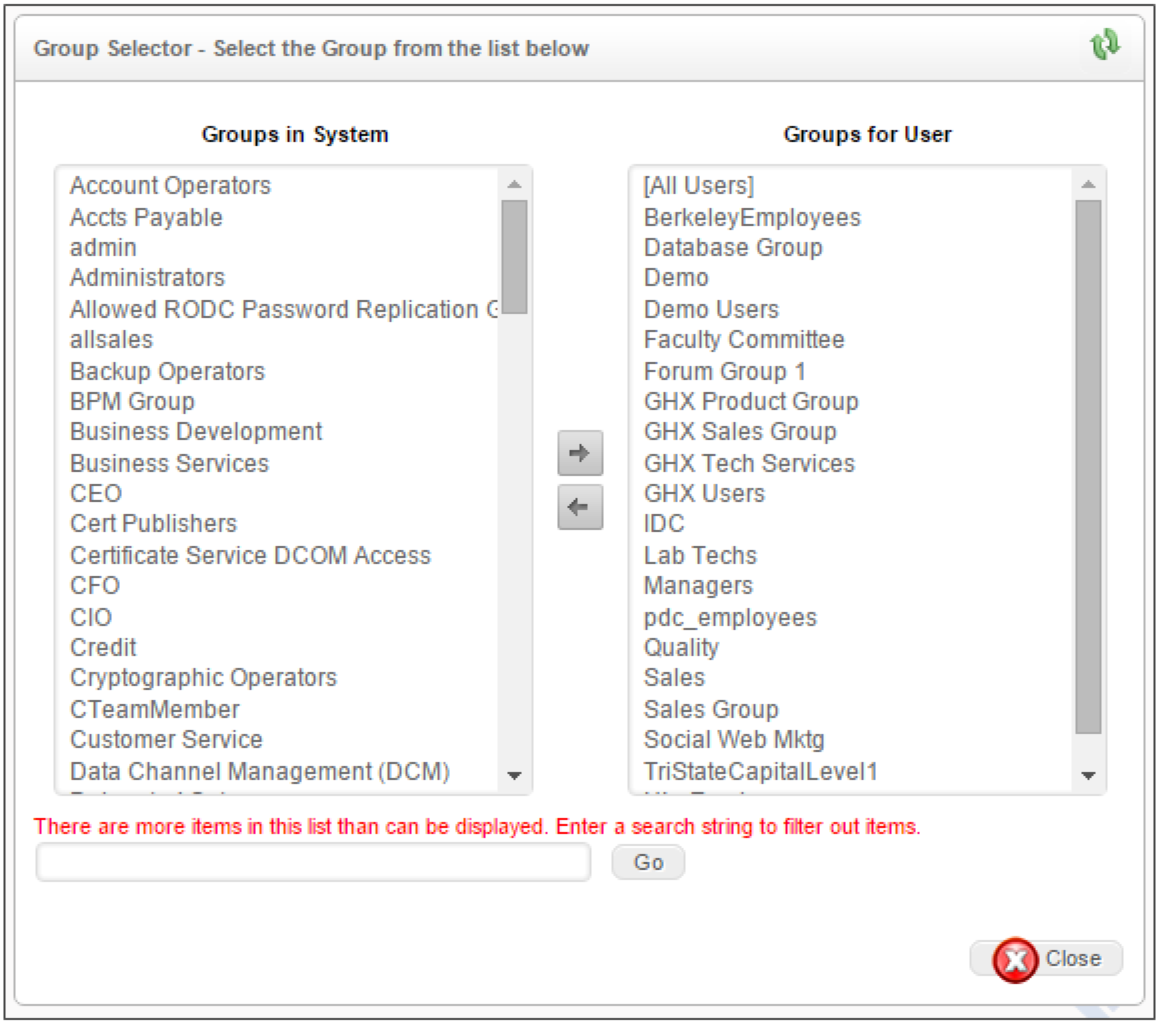
These settings enable you to grant the user different types of administrative privileges. You can grant users the following privileges by checking the corresponding checkboxes:

ADMIN TYPE	DESCRIPTION
System Administrator	The top-level Administrative user, with complete control of the Process Director Installation
System Partition Admin	This user type isn't technically a system administrator, and has no access to the IT Admin area of the installation. Users who are designated as system partition administrators, however, have full access to the Content List for the partitions to which they are a member, and have permission to create, edit, and delete all objects, irrespective of the Content List permissions that have been set in that Partition.
User Impersonation Ability	The ability for this user to impersonate other users.
System Configuration Admin	A subset of the System Administrator user with access only to the Configuration tab.
System User Admin	A subset of the System Administrator user, with access only to the User Administration tab.
System Install Admin	A subset of the System Administrator user, with access only to the Installation Settings tab.
System Troubleshooting Admin	A subset of the System Administrator user, with access only to the Troubleshooting tab.
Metadata Admin	Enables a user to access the Meta Data Administration section.

ADMIN TYPE	DESCRIPTION
Has Access To User Search API	For Process Director v6.1.400 and higher, this property grants the user access to the full user search API.

Assign Groups

You can assign the user to Process Director user groups by clicking the Assign Groups button. When you click the button, the Group Selector will open.



Account Operators
Accts Payable
admin
Administrators
Allowed RODC Password Replication G
allsales
Backup Operators
BPM Group
Business Development
Business Services
CEO
Cert Publishers
Certificate Service DCOM Access
CFO
CIO
Credit
Cryptographic Operators
CTeamMember
Customer Service
Data Channel Management (DCM)

[All Users]
BerkeleyEmployees
Database Group
Demo
Demo Users
Faculty Committee
Forum Group 1
GHX Product Group
GHX Sales Group
GHX Tech Services
GHX Users
IDC
Lab Techs
Managers
pdc_employees
Quality
Sales
Sales Group
Social Web Mktg
TriStateCapitalLevel1

There are more items in this list than can be displayed. Enter a search string to filter out items.

From the list box on the left, select the user group(s) to which you'd like to assign the user, then click the → button, which will move the group names over to the list box on the left.

To remove the user from a group, select the group from the list box on the left, then click the ← button to remove the group.

> **When adding users to a group, the fStartUsersAddedToGroup custom variable determines whether the new user will be assigned to any running tasks that are assigned to that group.**

Time Zone

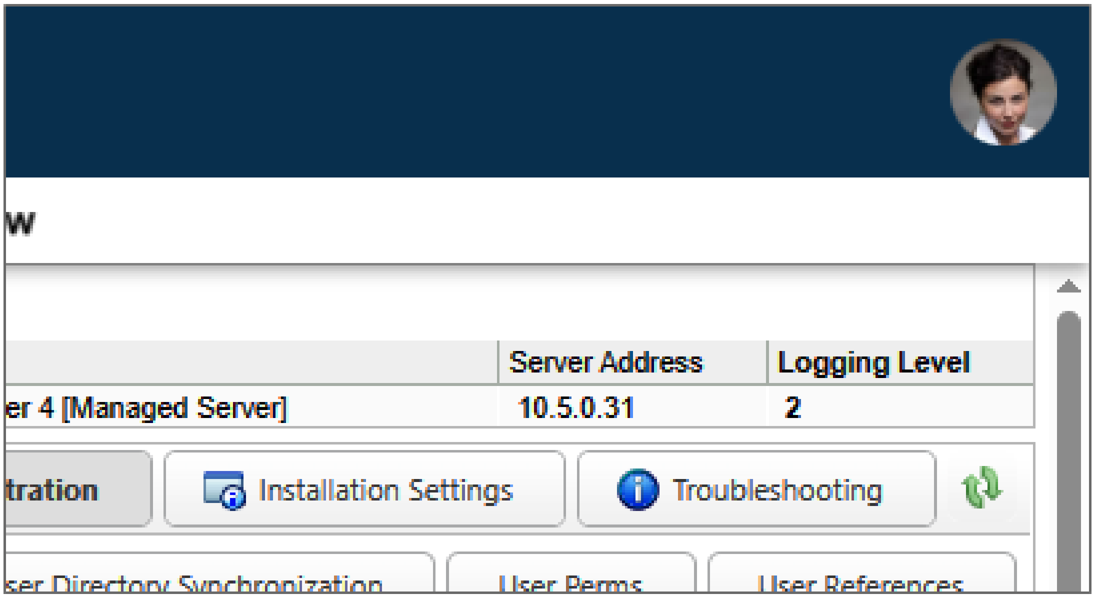
This dropdown control enables you to select the user's Time Zone. You can also allow Process Director to set the time zone to Daylight savings time automatically, by checking the Auto DST check box.

Preferred Language / Locale

You can set the appropriate language for the user, or select the default system language, by choosing it from this dropdown. The use of languages other than English will require that Process Director be localized for each additional language.

Picture Image

A picture of each user can be uploaded to Process Director. The image will appear in the user profile page for each user. It will also be displayed in the upper right corner of the page in Process Director v6.1, as the avatar for the User Profile menu.



	Server Address	Logging Level
er 4 [Managed Server]	10.5.0.31	2

You may upload the image by clicking on the Browse button to find and select the image. Once the image is selected, clicking the Upload button will upload the signature image to Process Director. Acceptable image formats include GIF, JPG, and PNG images.

Signature Image

Process Director can imprint an electronic signature in all routing slips for a user. If you have an image of the user's signature, you may upload the image by clicking on the Browse button to find and select the image. Once the image is selected, clicking the Upload button will upload the signature image to Process Director. Acceptable image formats include GIF, JPG, and PNG images.

Delegate all tasks to (User)

This user picker enables you to delegate another user to perform this user's tasks. For more information on user delegation, please see the User Delegation topic.

Replace this user with (User)

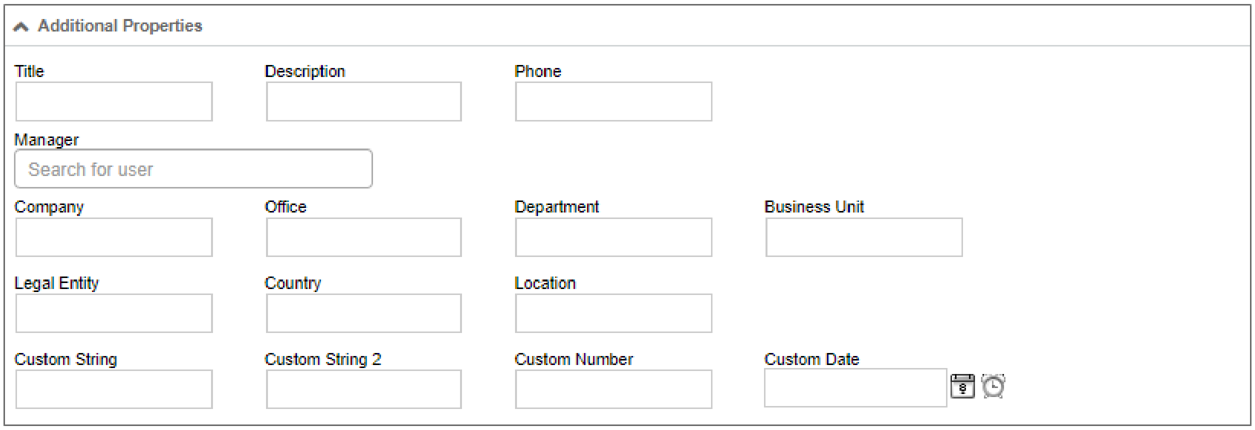
This user picker enables you to replace the current user with a selected user. This isn't a delegation. Instead, the current user will be completely replaced by the selected user in all assigned tasks, e.g., any task where the replaced user is specifically identified as the task assignee.

This replacement function will *not* replace the original user in any historical data, however, so an original user who was the original Timeline Initiator will still be listed as such. Similarly, if the original user is assigned a task via a user picker on a Form field, or from a Business Rule, the Replace user function will NOT replace the original user in those objects, either. For these reasons, we recommend that you immediately disable the account for the original user. When you do so, this will likely result in future tasks with assignments made via Form or Business Rule going into an error state when the original user is assigned if the Form or Business Rule isn't also edited when the original user is replaced.

The Replace User function isn't a panacea for user replacement. All it can do is try to make replacing a user easier than it would otherwise be.

Additional Properties Section

For User of Process Director v3.78 and higher, additional properties can be set for users. The Additional Properties section contains a number of text boxes to set these properties.



Available Properties

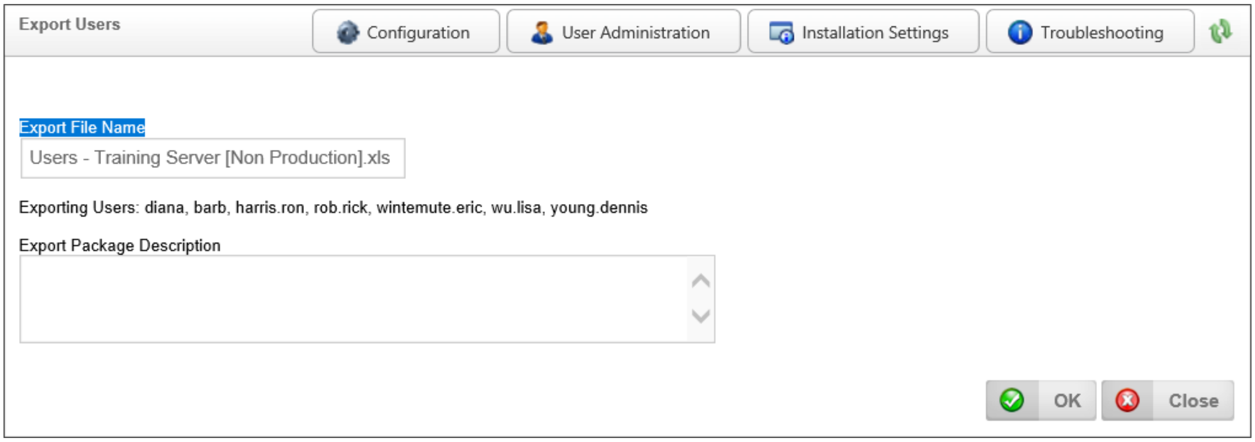
PROPERTY	DESCRIPTION
Title	A text box for the user's Title.
Description	A text box for a Description.
Phone	A text box for the user's phone number.
Manager	A UserPicker to choose the user's Manager.
Company	A text box for the user's Company.
Office	A text box for the user's Office name.
Department	A text box for the user's Department.
Business Unit	A text box for the user's Business Unit.
Legal Entity	A text box for the user's Business Entity.
Country	A text box for the user's Country.
Location	A text box for the user's Location.
Custom String	A text box for a custom string value.
Custom String 2	A text box for a custom string value.
Custom Number	A text box for a custom numeric value.
Custom Date	A DatePicker for a custom date value.

Exporting/Importing Users

Users can be exported or imported between systems using Excel files (.XLS, .XLSX or .CSV).

Exporting Users #

To export users, select one or more users from the User List, then click on the Export Users action link. An export box will appear that enables you to specify the name of the Excel file to which the list of selected users will be exported. A default name will be provided, but you can edit the default, at your discretion.



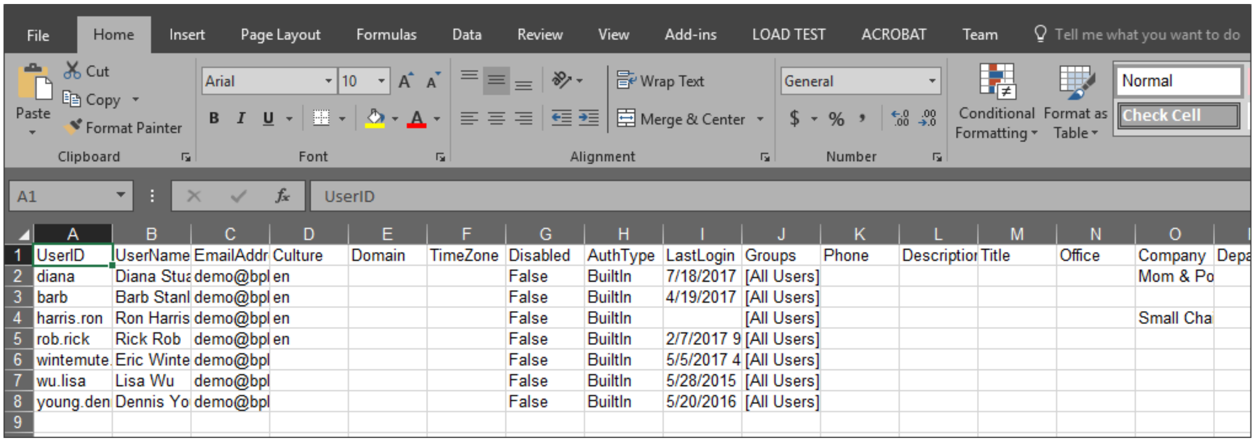
Export File Name

Users - Training Server [Non Production].xls

Exporting Users: diana, barb, harris.ron, rob.rick, wintemute.eric, wu.lisa, young.dennis

Export Package Description

Once you have done so, click the OK Button to complete the export and create the Excel file.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	UserID	UserName	EmailAddr	Culture	Domain	TimeZone	Disabled	AuthType	LastLogin	Groups	Phone	Descriptior	Title	Office	Company	Depa
2	diana	Diana Stua	demo@bpl	en			False	BuiltIn	7/18/2017	[All Users]					Mom & Po	
3	barb	Barb Stanl	demo@bpl	en			False	BuiltIn	4/19/2017	[All Users]						
4	harris.ron	Ron Harris	demo@bpl	en			False	BuiltIn		[All Users]					Small Cha	
5	rob.rick	Rick Rob	demo@bpl	en			False	BuiltIn	2/7/2017 9	[All Users]						
6	wintemute.	Eric Winte	demo@bpl				False	BuiltIn	5/5/2017 4	[All Users]						
7	wu.lisa	Lisa Wu	demo@bpl				False	BuiltIn	5/28/2015	[All Users]						
8	young.den	Dennis Yo	demo@bpl				False	BuiltIn	5/20/2016	[All Users]						
9																

The available columns in the exported Excel file are described below.

COLUMN	DESCRIPTION	DEFAULT VALUE
UserID	This is required on an import.	

COLUMN	DESCRIPTION	DEFAULT VALUE
UserName	The optional User Display Name.	
EmailAddress	The users email address.	
Culture	This is the optional culture for the user as defined by Windows (e.g. en).	
Domain	The optional Windows AD domain for the user.	
TimeZone	This is the optional time zone identifier for the user as defined by Windows (e.g. Pacific Standard Time).	
Disabled	This indicates if the user is disabled. If this is set to “true” or “1” on an import it WILL disable the user.	False
AuthType	The authentication type for the user. The authentication type can't be changed on an import. The available types are: Unknown, Built-In, Windows, LDAP, External, SAML, and Header.	Unknown
LastLogin	This is only available on the user export, it isn't used on the import.	
Groups	A comma separated list of groups this user belongs to.	
Phone	The optional phone number of the user.	
Password	This is only an option on the user import, the password is never exported.	
Description	An optional description for the user.	
Title	The optional title for the user.	
Office	The optional office for the user.	
Company	The optional company name for the user.	
BusinessUnit	The optional business unit for the user.	
LegalEntity	The optional legal entity for the user.	
Department	The optional department for the user.	

COLUMN	DESCRIPTION	DEFAULT VALUE
Country	An optional country for the user.	
Location	This is an optional location string.	
CustomString	This can be any string that should be associated with this user.	
CustomString2	This can be any string that should be associated with this user.	
CustomNumber	This can be any numeric value.	
CustomDate	This can be any date value.	
Manager	This is the USERID or UID of the manager record.	
PasswordChange	This indicates if the user should be required to change their password on the next login.	False
DayPass	This indicates if the user is a “Day Pass” user.	False
DeleteUser	This is an optional column that will, when set to "DELETE" on a user's row, delete the user from the system. **BP Logix strongly recommends that you disable, rather than delete users, to retain the user's activity history, but this is an available spreadsheet option, if needed.**	

Importing Users #

Once the Excel file has been exported, you can import the users to another system by transferring the Excel file between the systems.You may wish to edit certain attributes of the Excel file before importing it. When exporting/importing Built-in users between systems, the PasswordChange column, will, when set to 1", force the user to change the password on their next login.

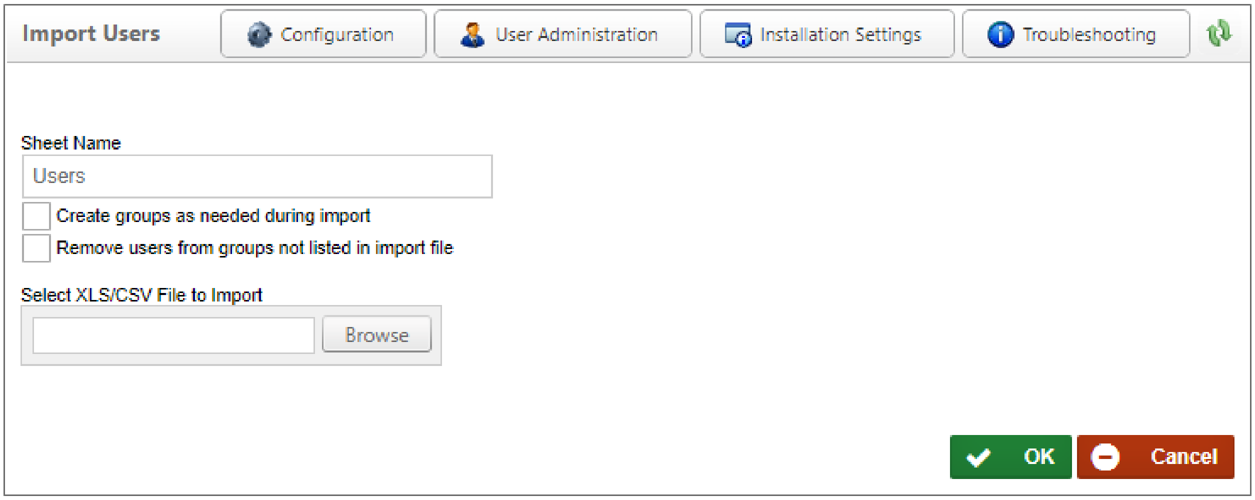
Similarly, you can use your own Excel or CSV file to import new users. If you are importing users via your own Excel or CSV file, you must, as a minimum, have a

UserID column for each record, but BP Logix recommends that you have the following columns in your file, with the appropriate data for the users in each row:

- UserID
- UserName
- EmailAddress

When using an Excel file for the import, the user data must be on a worksheet named "Users".

To import the file into the target system, navigate to the Users page again. Once there, click the Import Users action link. You'll be prompted for the Excel or CSV file to import.



Sheet Name
Users

□ Create groups as needed during import
□ Remove users from groups not listed in import file

Select XLS/CSV File to Import

When importing an Excel file with users there are a couple options available.

- Create groups as needed during import
- Remove users from groups not listed in import file

The first option will automatically create and groups in the “Groups” column if they don't exist. The default is to add users to groups that exist, but not to create the groups. The second option will remove a user from an group that isn't listed in their “Groups” column.

Once you have selected the import file and set the desired properties for the import, click the OK button to begin the import. All of the users in the import file will be imported to the target system.

Using Multi-Factor Authentication (MFA)

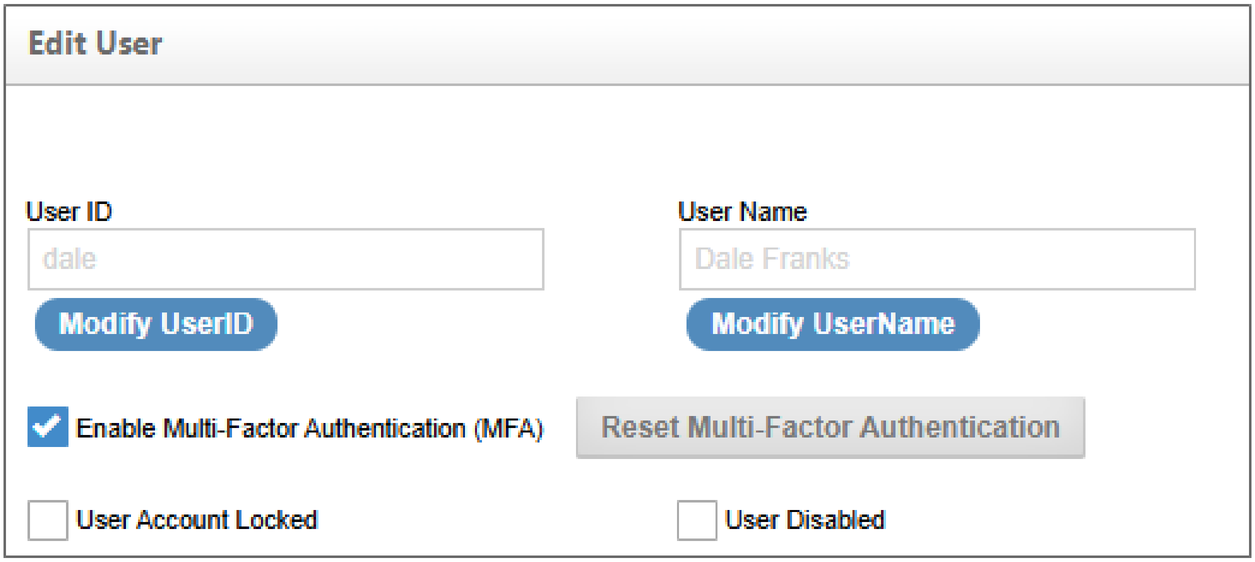
Process Director v6.1.300 and higher enables the use of Multi-Factor Authentication (MFA) for Built-in user accounts. Previously, MFA was only available for other account types, such as SAML or Windows accounts, that implemented MFA as part of the external authentication system. With the addition of MFA to Built-In accounts, all user account types can implement this heightened authentication method for increased security.

MFA generally relies on the use of an in dependent device, such as a tablet or phone, to supply an authentication token that is used to log in, in addition to the user name and password. The authentication token is supplied via an MFA app on the mobile device that refreshes the token every minute. There are several popular authenticator apps available, as well as stand-alone authentication devices (though they are rarely used). The only requirement for the MFA authentication app is that it's compliant with Google Authenticator. One popular authentication app, available for both Android and iOS devices, is **Authy**, which can be obtained easily from your mobile device's app store.

With MFA enabled, the user must have access to both their computer, as well as a separate device that provides an authentication token, in order to log into Process Director.

Implementing MFA

In the Edit User page of the User Administration section, each user account has two MFA properties available, the most important of which is the Enable Multi-Factor Authentication (MFA) property.



Edit User

User ID: dale

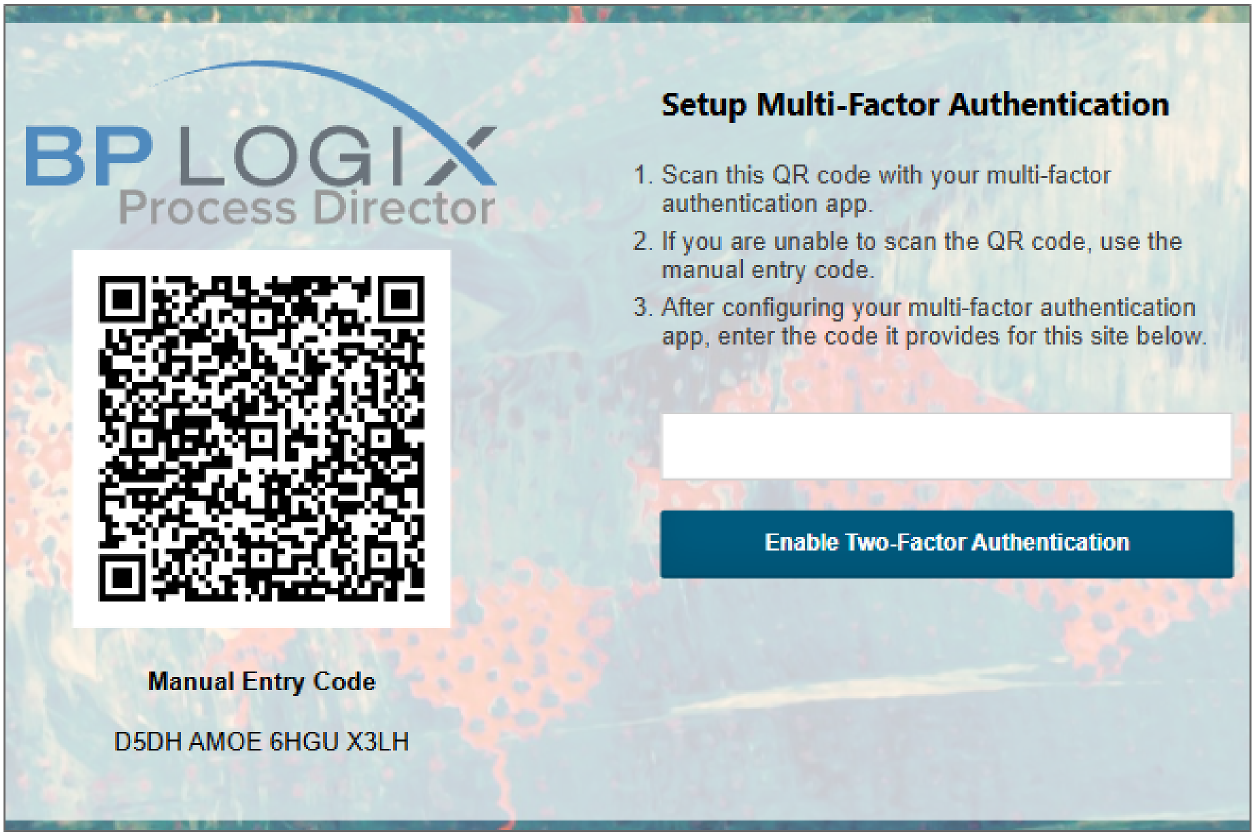
User Name: Dale Franks

☑ Enable Multi-Factor Authentication (MFA)

□ User Account Locked

□ User Disabled

The Enable Multi-Factor Authentication (MFA) property will, when checked, activate the use of MFA for the specified user account, once the Edit User page is updated. Once activated, the user will, on their next login, be presented with an MFA activation screen immediately after attempting to log in with their existing user name and Password.



Setup Multi-Factor Authentication

1. Scan this QR code with your multi-factor authentication app.
2. If you are unable to scan the QR code, use the manual entry code.
3. After configuring your multi-factor authentication app, enter the code it provides for this site below.

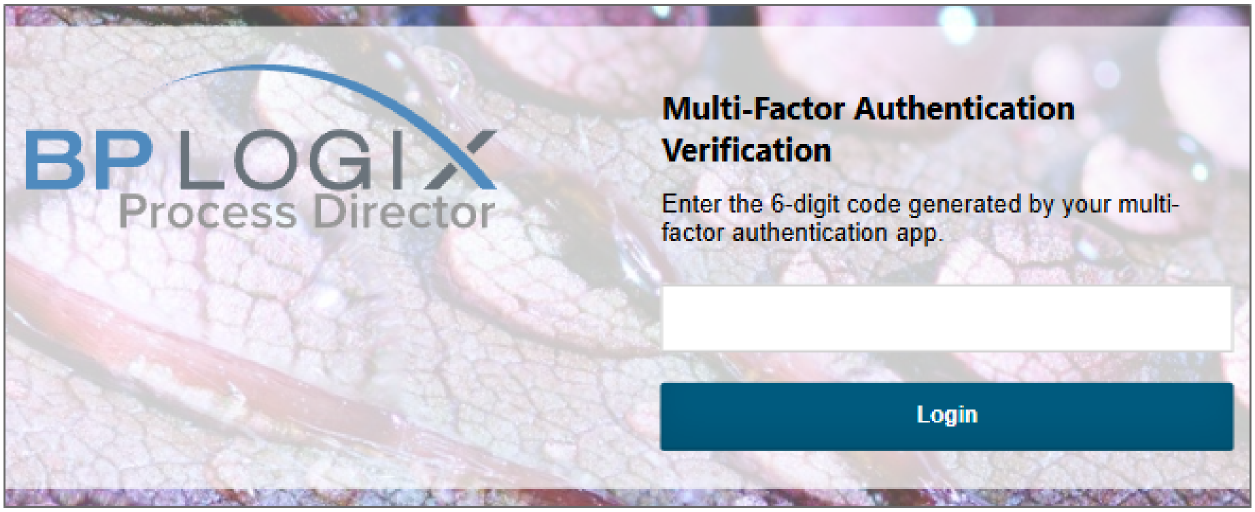
Manual Entry Code

D5DH AMOE 6HGU X3LH

The activation screen displays a QR code that, when scanned in the user's authentication app, will create an MFA account for the Process Director installation. (A manual MFA entry code is also displayed below the QR code to manually enter into the authenticator app, if needed. Generally the authentication app simply enables you to scan the QR code.)

Once the MFA account is created and accessible in the authenticator app, a 6-digt authorization token will be displayed, which will refresh every 60 seconds with a new token. Once the token appears in the authentication app, the user can enter it into the text box provided, then click the Enable Two-Factor Authentication button. Assuming the token has been entered correctly, the user will be logged into Process Director automatically.

On every subsequent login, the user will enter their user name and password, after which they'll be directed to the MFA verification screen. The user will enter the 6-digit token from their authenticator app to complete their login.



Multi-Factor Authentication Verification

Enter the 6-digit code generated by your multi-factor authentication app.

Once activated, the user will not be able to log into Process Director without the token provided by the authentication app.

For Process Director v6.1.400 and higher, the "Remember Me" check box will appear on the main Login page enables the user to pause the system from requesting the MFA token for 30 days before asking for it again.

As mentioned, the 6-digit authentication token is refreshed with a new token in the authenticator app every 60 seconds. Process Director will, however, continue to respect the old token during a brief grace period if the refresh occurs prior to clicking the Login button. Once the token has been entered, and the Login button clicked, the user login is complete.

Resetting MFA

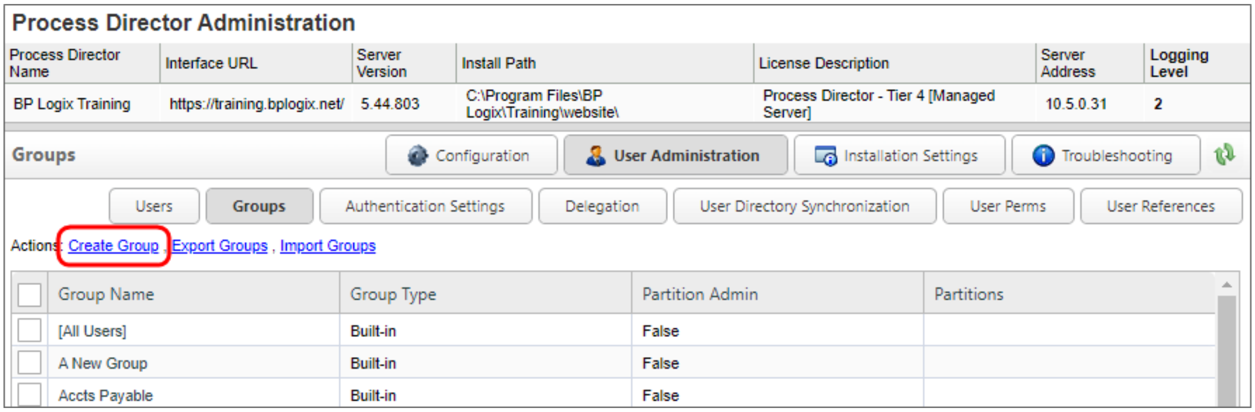
In cases where the user loses their mobile device, or switches to a new authentication app, the user will have to create a new MFA account in their authenticator app to log in again. To enable this, the Edit User page has a Reset Multi-Factor Authentication button. When clicked, this button will terminate the existing token sequence. The user, on their next login, will once again see the MFA activation screen, which will enable them to create a new MFA account in their authentication app, and log into the system again with the correct token for their new MFA account.

Group Administration

Process Director supports groups. A **group** provides a collection of users according to organization, geographic location, role, or any other type of categorization. Any permissions or task assignments that can be given to an individual user can also be given to a group. Group administration can be accessed via the Groups page, which is located in the User Administration section of the IT Admin area.

Adding a New Group

Click on the Create Group action link at the top of then Groups page. Doing so will open the Create Group dialog, which will prompt you to enter a Name for the new group.



Process Director Administration

Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
BP Logix Training	https://training.bplogix.net/	5.44.803	C:\Program Files\BP Logix\Training\website\	Process Director - Tier 4 [Managed Server]	10.5.0.31	2

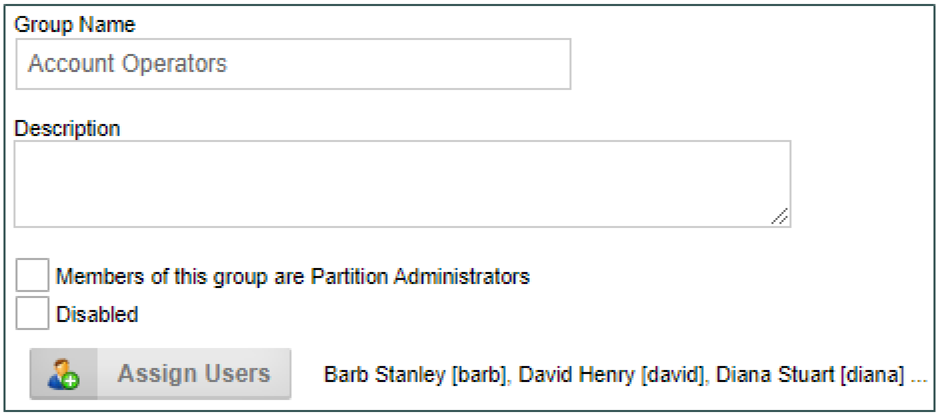
Groups

Actions: Create Group , Export Groups , Import Groups

	Group Name	Group Type	Partition Admin	Partitions
□	[All Users]	Built-in	False	
□	A New Group	Built-in	False	
□	Accts Payable	Built-in	False	

Adding Users to a Group

The previous step adds the new group to the Groups list on the Groups page. To add users to this group, click on the Edit hotlink of the group to configure it. When the group definition page opens, click the Assign Users button.



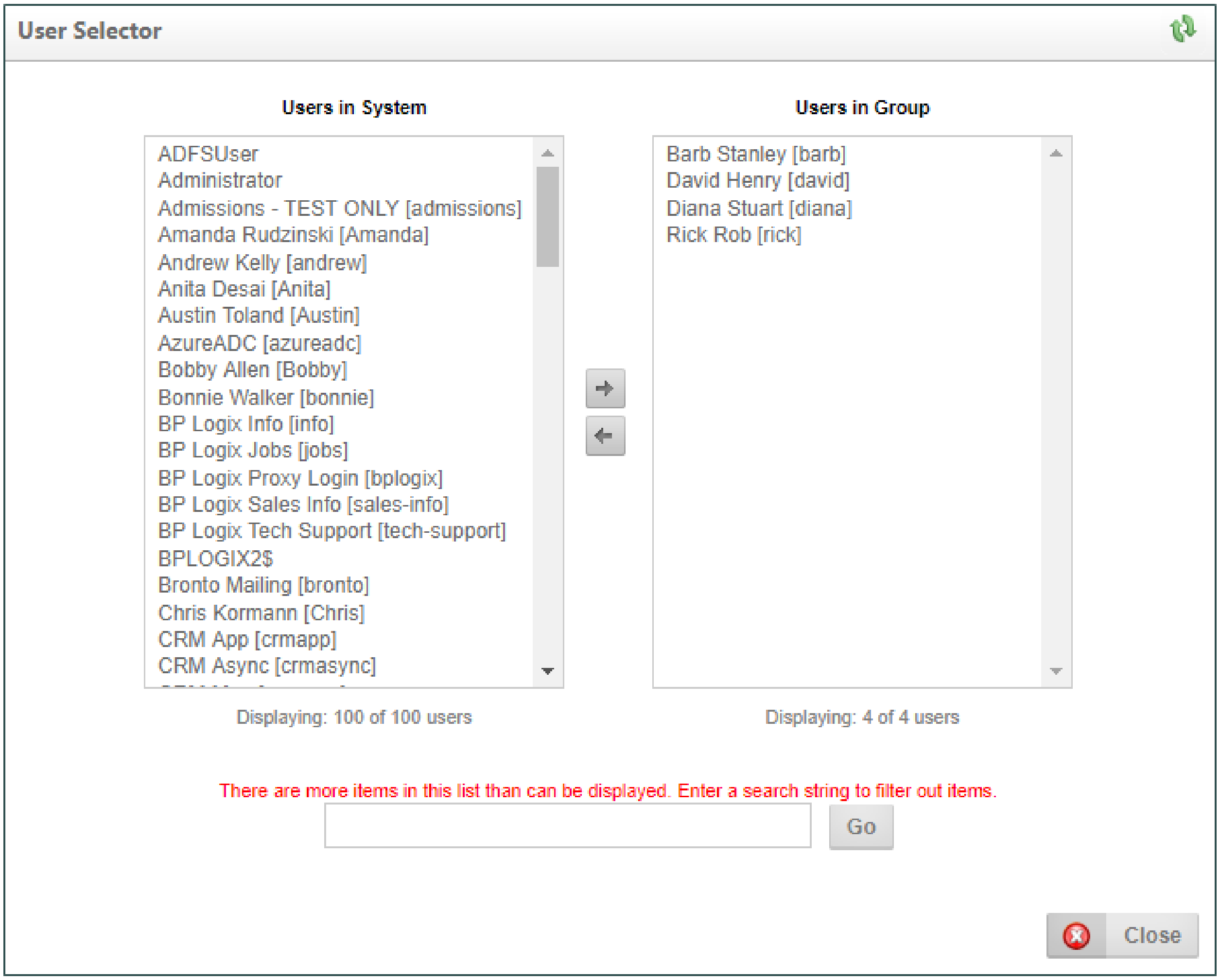
Group Name
Account Operators

Description

□ Members of this group are Partition Administrators
□ Disabled

Barb Stanley [barb], David Henry [david], Diana Stuart [diana] ...

A User Selector window will appear. Select the users that you want to add to the group from the Users in System pane, then click on the arrow that point to the right to add the selected users to the Users in Group pane. To remove a user from a group, select the users from the Users in Group pane and click on the arrow button that points to the left.


User Selector

Users in System

ADFSUser
Administrator
Admissions - TEST ONLY [admissions]
Amanda Rudzinski [Amanda]
Andrew Kelly [andrew]
Anita Desai [Anita]
Austin Toland [Austin]
AzureADC [azureadc]
Bobby Allen [Bobby]
Bonnie Walker [bonnie]
BP Logix Info [info]
BP Logix Jobs [jobs]
BP Logix Proxy Login [bplogix]
BP Logix Sales Info [sales-info]
BP Logix Tech Support [tech-support]
BPLOGIX2$
Bronto Mailing [bronto]
Chris Kormann [Chris]
CRM App [crmapp]
CRM Async [crmasync]

Displaying: 100 of 100 users

Users in Group

Barb Stanley [barb]
David Henry [david]
Diana Stuart [diana]
Rick Rob [rick]

Displaying: 4 of 4 users

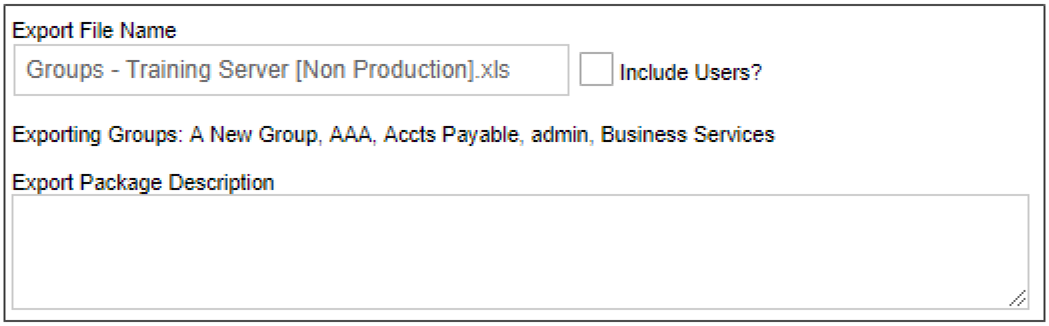
There are more items in this list than can be displayed. Enter a search string to filter out items.

Once a group has been created, an additional property, Members of this Group are Partition Administrators, will make all group users partition administrators automatically when checked. These users will have full control to create, modify, or delete Process Director objects in the Partitions of which they are a member, irrespective of any permissions that are set in the Content List.

Once created, groups should not be deleted from the system. Deleting the group will, just as with users, delete all of the historical data referring to the group. Instead, BP Logix strongly recommends that you check the Disabled property to disable the group. This will remove the group from all task assignments, Business Rules, etc., while retaining the historical data.

Exporting Groups

Built-in Groups can be exported between systems using Excel files. To export groups, select one or more groups from the Group List, then click on the Export Groups action link. An export box will appear that enables you to specify the name of the Excel file to which the list of selected users will be exported. A default name will be provided, but you can edit the default, at your discretion.



Export File Name

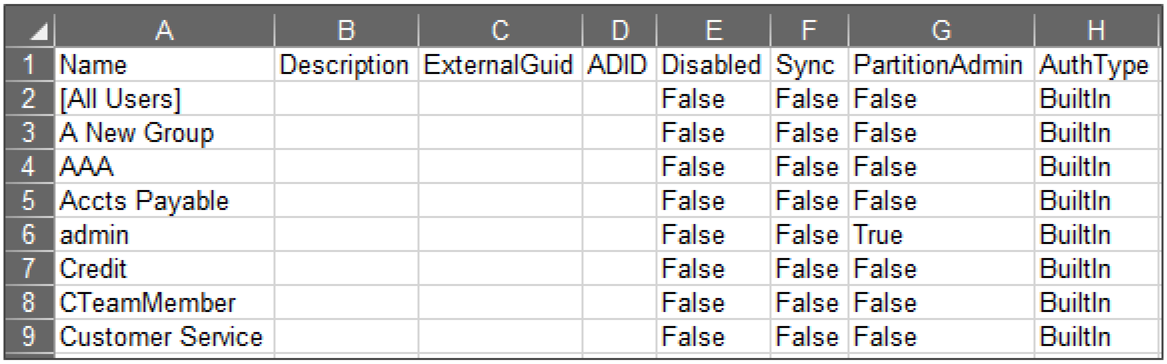
Groups - Training Server [Non Production].xls

□ Include Users?

Exporting Groups: A New Group, AAA, Accts Payable, admin, Business Services

Export Package Description

Once exported, the groups will be saved to an Excel Spreadsheet.



	A	B	C	D	E	F	G	H
1	Name	Description	ExternalGuid	ADID	Disabled	Sync	PartitionAdmin	AuthType
2	[All Users]				False	False	False	BuiltIn
3	A New Group				False	False	False	BuiltIn
4	AAA				False	False	False	BuiltIn
5	Accts Payable				False	False	False	BuiltIn
6	admin				False	False	True	BuiltIn
7	Credit				False	False	False	BuiltIn
8	CTeamMember				False	False	False	BuiltIn
9	Customer Service				False	False	False	BuiltIn

The spreadsheet containing the exported groups can be imported into another system, using the Import Groups action link.

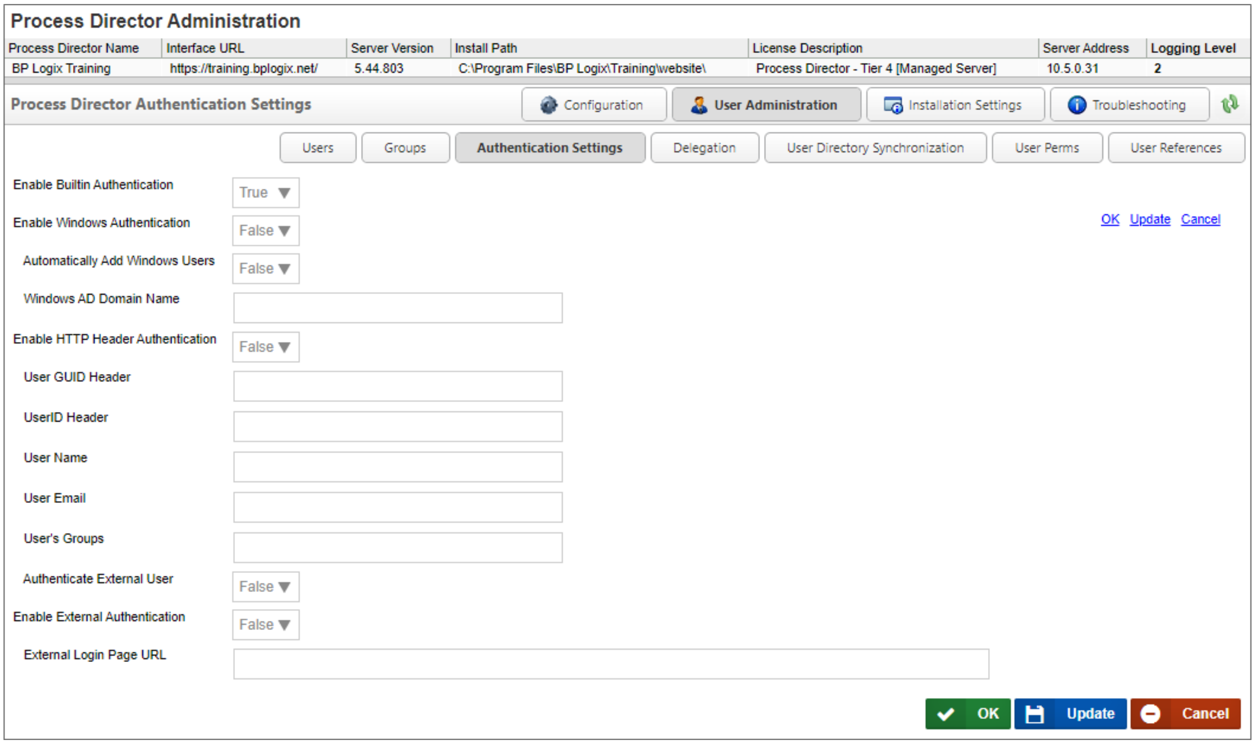
Exporting Groups and Users

An additional export property, Include Users?, will use the User Export feature to export the users and groups together. In that case, the output will use the Export Users feature to export both users and groups in one spreadsheet. Importing that file into another system will import both the users and groups in one import via the Import Users link on the User Administration page, rather than the Import Groups link on the Group Administration page.

Continue

Continue to the documentation for the Authentication Settings page.

Authentication Settings



Process Director Administration

Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
BP Logix Training	https://training.bplogix.net/	5.44.803	C:\Program Files\BP Logix\Training\website\	Process Director - Tier 4 [Managed Server]	10.5.0.31	2

Process Director Authentication Settings

Enable Builtin Authentication	True
Enable Windows Authentication	False
Automatically Add Windows Users	False
Windows AD Domain Name	
Enable HTTP Header Authentication	False
User GUID Header	
UserID Header	
User Name	
User Email	
User's Groups	
Authenticate External User	False
Enable External Authentication	False
External Login Page URL	

The Authentication Settings page enables you to determine the authentication methods available to users. As a default, Built-In authentication is automatically enabled. Other Authentication settings can be configured so that NTLM, Single-Sign-On, etc., are enabled.

Enable Built-In Authentication

This is the standard Process Director option, and is set to true by default.

Enable Windows Authentication

When set to true, this setting enables Windows authentication, so that Single Sign-On is used to authenticate users via their Windows identity.

Automatically Add Windows Users

When set to true, new Windows users will be automatically added to Process Director.

Windows AD Domain Name

The Active Directory domain name for the domain from which to add windows users to process Director.

Enable HTTP Header Authentication

When set to true, this setting enables authentication through the HTTP header, enabling users to log in via NTLM through an identity that is set in the HTTP header of the page request when a user navigates to Process Director with their browser. All users log in with a single identity specified in the header settings.

User GUID Header

The value of the User GUID to use in the HTTP Header.

UserID Header

The value of the UserID to use in the HTTP Header.

User Name

The value of the User Name to use in the HTTP Header.

User Email

The value of the User email address to use in the HTTP Header.

User's Groups

A comma-separated list of Groups to which the User should be assigned to use in the HTTP Header.

Authenticate External User

This setting determines whether external users, i.e., users that aren't listed in the User database, should be authenticated.

Enable External Authentication

This setting, when set to true, enables you to use a login page outside of Process Director.

External Login Page URL

The URL of the external login page.

Authentication Types

Users must access Process Director with a User ID and password. A User ID must exist in the Process Director database before a login can occur. Process Director supports four types of user authentication methods.

Built-in

This authentication method uses Process Director to authenticate users. This is the default authentication method. These users must be added to the Process Director database using the web based System Administration.

Windows Domain Security

This authentication mechanism uses your Microsoft Windows Domain to authenticate users. These users will be automatically added to the Process Director database after being successfully authenticated by your Windows Domain Server.

LDAP

This authentication mechanism uses your LDAP server (e.g. Active Directory) to authenticate users. These users will be automatically added to the Process Director database after being successfully authenticated.

External

External users are those that are authenticated by a third party system. This includes products such as CA CleverPath Portal, CA Siteminder, Cafesoft Cams, and other external authentication systems using Process Director APIs. External users are automatically kept synchronized with the third party authentication system on every login.

More information about setting up authentication settings can be found in the User Authentication Options and SAML 2.0 (Federated Identity) Support sections of the Installation Guide.

Continue

Continue to the documentation for the Delegation page.

User Delegation

Process Director features two methods of delegating tasks. Standard Delegation enables you to assign all tasks from a delegator to a specified delegate, automatically assigning the tasks to the delegate while the delegation is active. Shared

Delegation enables you to share tasks, by enabling the delegate to complete tasks that are assigned to the delegator on an optional basis. Using Standard Delegation always assigns all tasks to the delegate, while Shared Delegation enables the delegate to view and complete tasks on an *ad hoc* basis.

Standard Delegation

Tasks assigned to one user can be delegated to another user. When using standard delegation, all of the delegated tasks will be assigned directly to the delegated user until such time as the delegation is revoked. There are three primary ways in which delegation can be assigned, two of which are performed at the administrative level. The remaining delegation method can be performed by users by modifying their own profiles, and we will address this method first.

When a user delegates to another that is already running in the same step/activity, the original user is canceled and the other user is left running. When undelegating, there is an option that will allow the original canceled user to be restarted if that step/activity is still running. To enable this option, set the fEnableUndelegationRestart custom variable to "true". If this option isn't set, then the delegated user's task will be canceled, but the original user's task *won't be restarted*, and the task will be canceled for both users.

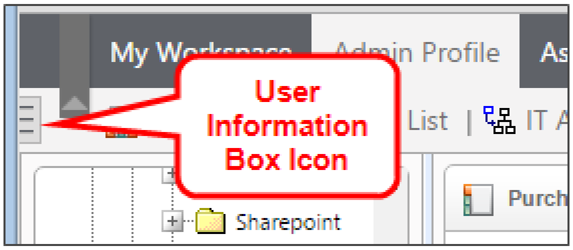
For Process Director v4.03 and higher, the system will prevent users from delegating tasks to a user who is already delegating tasks to them. In other words, if User A is delegating tasks to User B, User B will be prevented from delegating tasks to User A. This loop checking only prevents a direct delegation loop between two users, and won't prevent indirect delegation loops that involve three or more persons.

For Process Director v5.26, delegation was extended to enable a disabled user to still delegate to another user. This will better handle implementations where a disabled user is listed in a form field that is being used to assign to a task. The task will have the delegate assigned to it so it can continue.

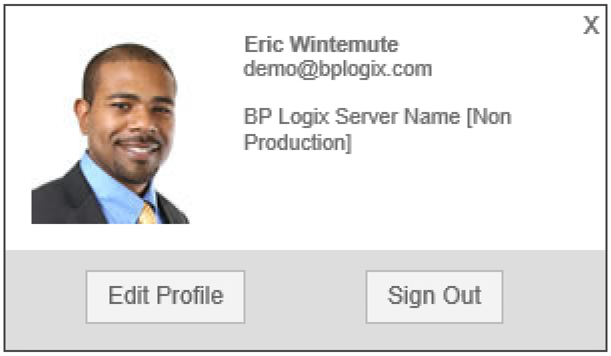
Delegation by the user

Users may delegate their own tasks to another user by modifying their user profile via the following procedure.

First, open the user information box by clicking the user menu icon located at the top left corner of the Process Director interface.



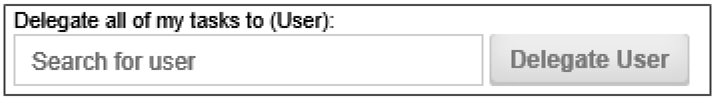
When you click the icon, the user information box will appear.



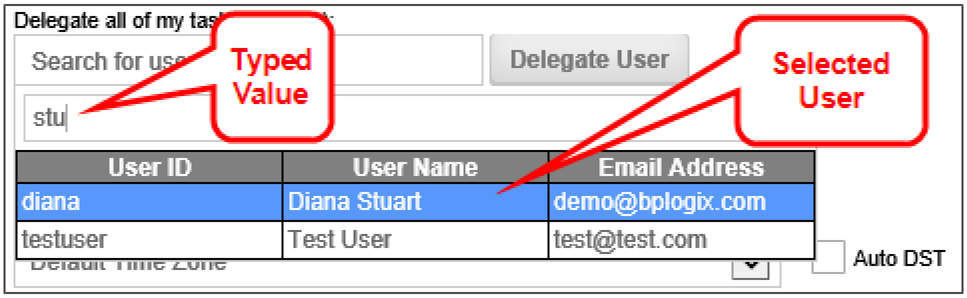
Eric Wintemute
demo@bplogix.com

BP Logix Server Name [Non Production]

Once the user Information box appears, click the Edit Profile button to open your User Profile page. On the User Profile, there is a delegation picker displayed.



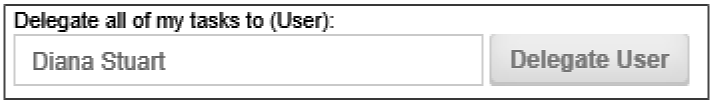
Select the User Picker to open the type ahead box and begin typing a user name to expand the type ahead dropdown containing the list of matching users. Select a user to which to delegate by choosing the user from the type ahead dropdown. You can use the arrow keys to scroll the selection cursor up and down, then press the [ENTER] key to make your selection, or you can select the user with your mouse.



stu

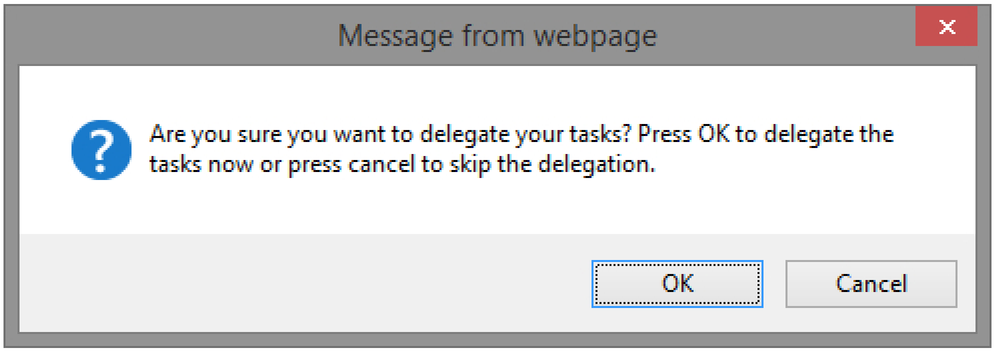
User ID	User Name	Email Address
diana	Diana Stuart	demo@bplogix.com
testuser	Test User	test@test.com

Once the user list type ahead has closed, the selected user will now appear in the delegation user picker. Confirm the delegation by clicking the Delegate User button.



Delegate all of my tasks to (User):
Diana Stuart

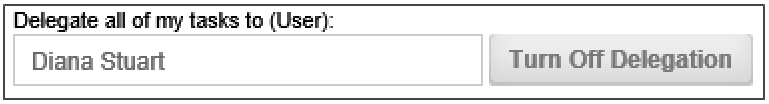
A confirmation dialog box will appear to ask you to confirm the delegation.



Message from webpage

Are you sure you want to delegate your tasks? Press OK to delegate the tasks now or press cancel to skip the delegation.

Click the OK button to confirm the delegation. The dialog box will close, the delegation will take effect.



Delegate all of my tasks to (User):
Diana Stuart

You can end the delegation by clicking the Turn Off Delegation button. Again, a dialog box will appear that asks you to confirm that you wish to turn off the delegation. Click the OK button to turn off delegation to the previously selected user.

When you have made the appropriate delegation decision, click the OK button at the bottom right of the User Profile screen to close it.

ⓘ The Standard Delegation functionality can be removed from the user profile page by setting the fTurnOffDelegation Custom Variable to "true" in the Custom Vars file.

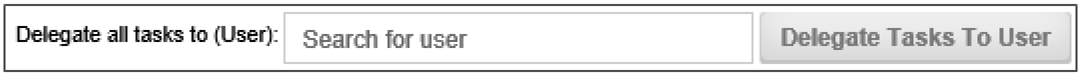
Delegation by Administrators

Administrators can perform delegation on behalf of users by making the delegation change in the User Profile for a specific user, or in the User Administration section's Delegation page.

Edit User Profile

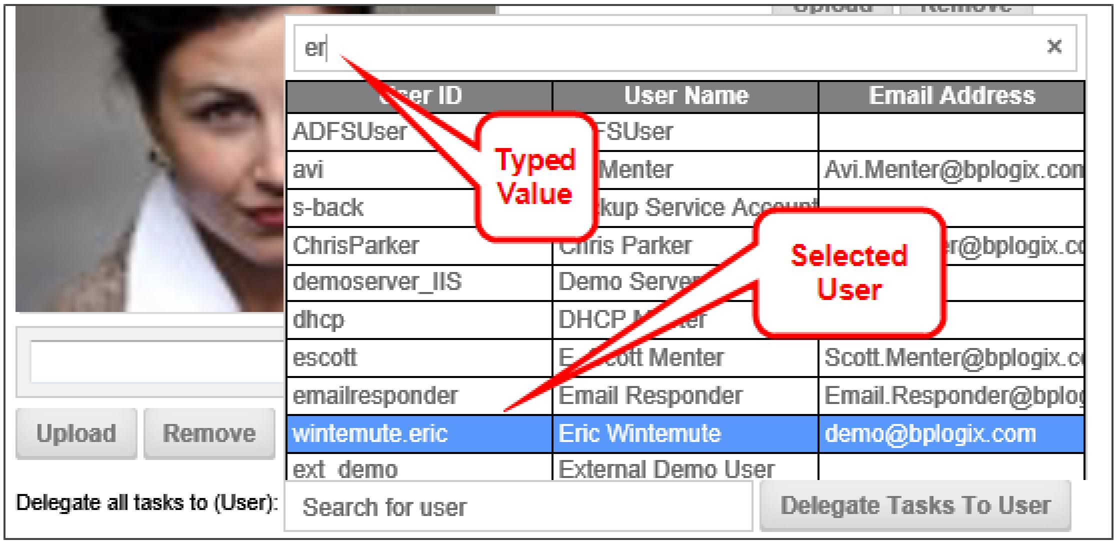
From the Users page of the User Administration area, open the Edit User screen of the user for which you wish to perform delegation. There is a User Picker labeled

Delegate all tasks to (User).



Delegate all tasks to (User): Search for user

Select the User Picker to open the type ahead box and begin typing a user name to expand the type ahead dropdown containing the list of matching users. Select a user to which to delegate by choosing the user from the type ahead dropdown. You can use the arrow keys to scroll the selection cursor up and down, then press the [ENTER] key to make your selection, or you can select the user with your mouse.

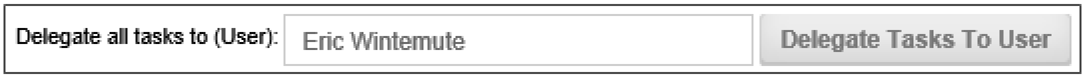


er

User ID	User Name	Email Address
ADFSUser	FSUser	
avi	Menter	Avi.Menter@bplogix.con
s-back	kup Service Account	
ChrisParker	Chris Parker	r@bplogix.c
demoserver_IIS	Demo Serve	
dhcp	DHCP M ter	
escott	E ott Menter	Scott.Menter@bplogix.c
emailresponder	Email Responder	Email.Responder@bplog
wintemute.eric	Eric Wintemute	demo@bplogix.com
ext_demo	External Demo User	

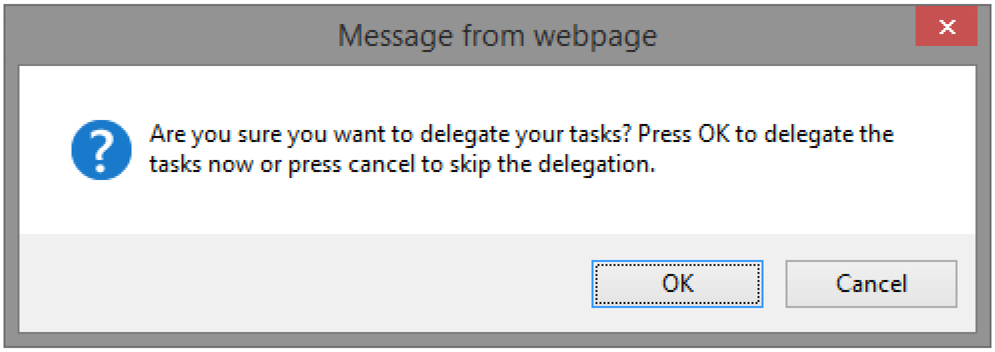
Delegate all tasks to (User): Search for user

Once the user list type ahead has closed, the selected user will now appear in the delegation user picker. Confirm the delegation by clicking the Delegate Tasks to User button.



Delegate all tasks to (User): Eric Wintemute

A confirmation dialog box will appear to ask you to confirm the delegation.

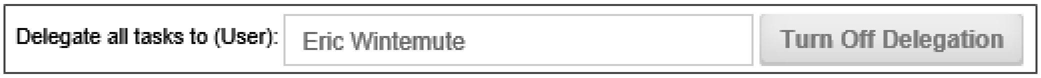


Message from webpage

Are you sure you want to delegate your tasks? Press OK to delegate the tasks now or press cancel to skip the delegation.

Click the OK button to confirm the delegation. The dialog box will close, the delegation will take effect.

You can end the delegation by clicking the Turn Off Delegation button. Again, a dialog box will appear that asks you to confirm that you wish to turn off the delegation. Click the OK button to turn off delegation to the previously selected user.

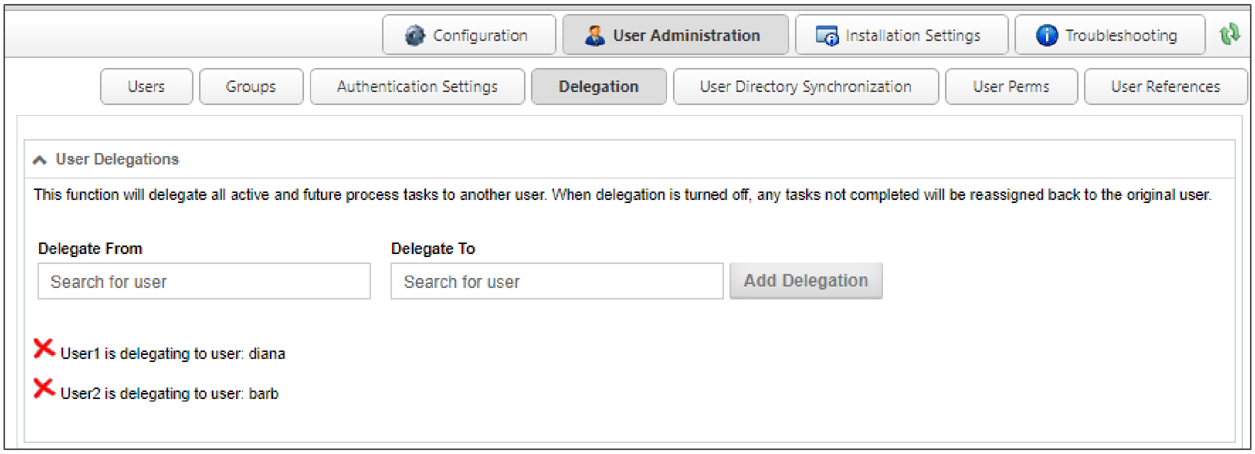


Delegate all tasks to (User): Eric Wintemute

When you have made the appropriate delegation decision, click the OK button at the bottom right of the Edit User screen to close it.

Delegation Page

In the Delegation page of the User Administration section, you can set or remove multiple delegations. The screen also displays the currently active delegations in the User Delegations section of the page, as displayed in the example below.



This function will delegate all active and future process tasks to another user. When delegation is turned off, any tasks not completed will be reassigned back to the original user.

Delegate From: Search for user

Delegate To: Search for user

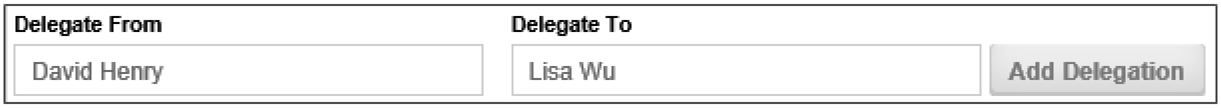
User1 is delegating to user: diana

User2 is delegating to user: barb

Setting Delegation

Use the User Pickers to select the from whom the tasks should be delegated, and the user to whom tasks should be delegated.

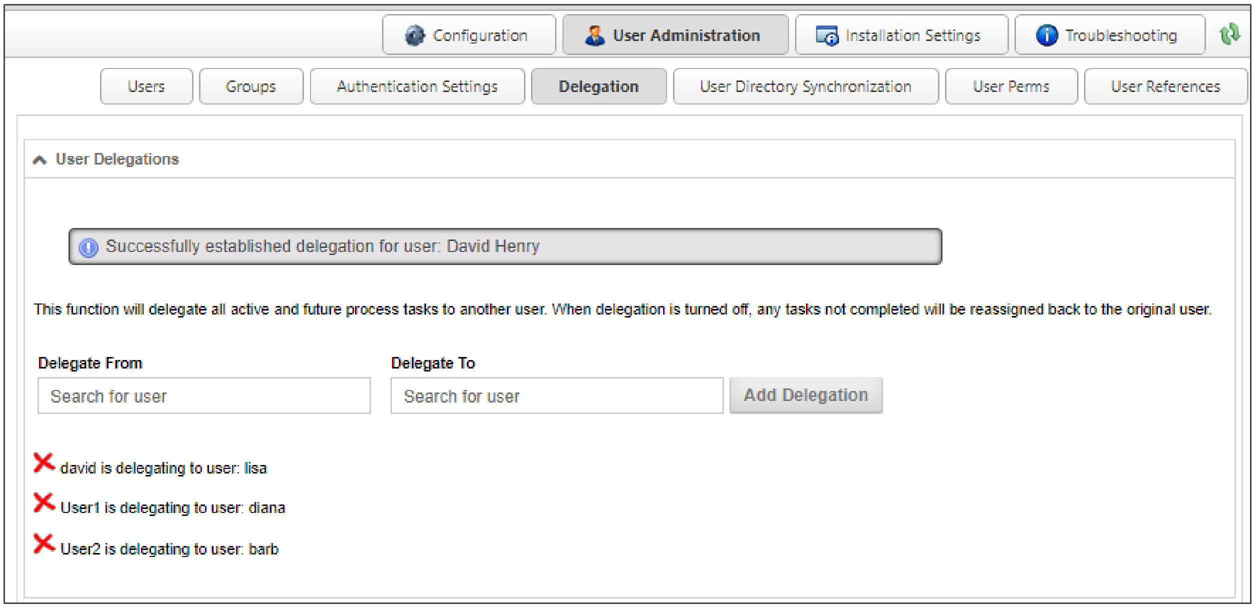
Once you have set both users for the delegation, click the Add Delegation button to create the delegation.



Delegate From: David Henry

Delegate To: Lisa Wu

The delegation will be created immediately, and will appear in the delegation list at the bottom of the Delegation page, and a message will appear notifying you that the delegation has been successfully created.



Successfully established delegation for user: David Henry

This function will delegate all active and future process tasks to another user. When delegation is turned off, any tasks not completed will be reassigned back to the original user.

Delegate From: Search for user

Delegate To: Search for user

✕ david is delegating to user: lisa

✕ User1 is delegating to user: diana

✕ User2 is delegating to user: barb

Removing Delegation

To remove a delegation, simply click the delete icon (✕) next to the delegation you wish to remove. The delegation will be canceled and a message will appear that notifies you that the delegation has been removed.

Shared Delegation

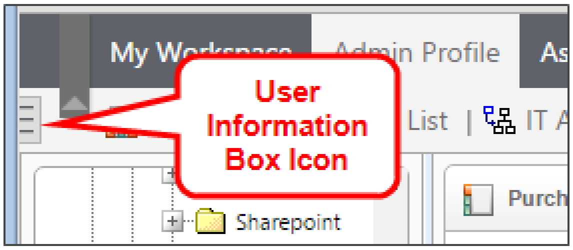
In addition to the standard delegation described above, users of Process Director v5.12 and higher can also implement shared delegation. Unlike standard delegation, shared delegation enables specified users to complete tasks for the delegator, but doesn't automatically assign tasks to the delegate. Instead, shared delegation gives the delegate access to the delegator's tasks, so that the delegate can complete them, if necessary or desired.

Delegates can be selected by the user, or by an administrator, using the procedures described below.

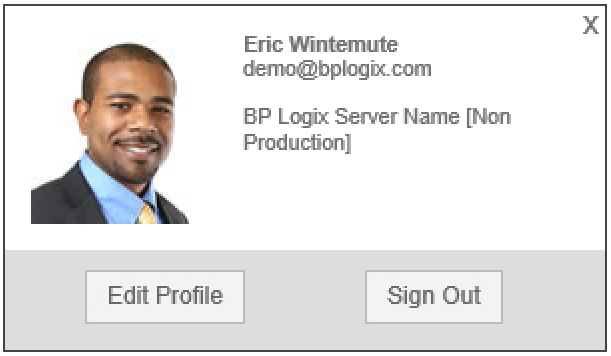
Delegation by the user

Users may share their own tasks to another user by modifying their user profile via the following procedure.

First, open the user information box by clicking the user menu icon located at the top left corner of the Process Director interface.

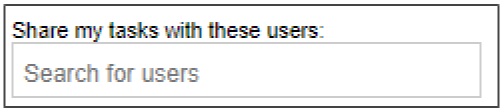


When you click the icon, the user information box will appear.


Eric Wintemute
demo@bplogix.com

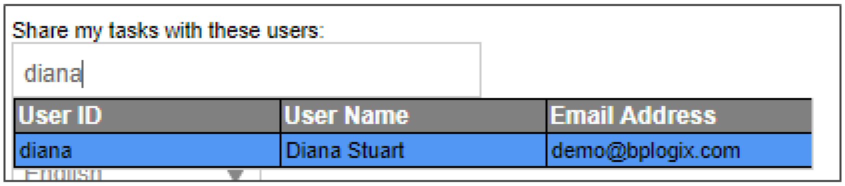
BP Logix Server Name [Non Production]

Once the user Information box appears, click the Edit Profile button to open your User Profile page. On the User Profile page, there is a Share my tasks with these users User Picker displayed.


Share my tasks with these users:

Search for users

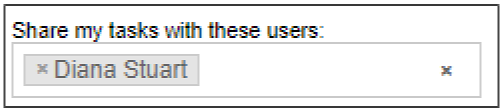
Select the User Picker to open the type ahead box and begin typing a user name to expand the type ahead dropdown containing the list of matching users. Select a user to which to delegate by choosing the user from the type ahead dropdown. You can use the arrow keys to scroll the selection cursor up and down, then press the [ENTER] key to make your selection, or you can select the user with your mouse.


Share my tasks with these users:

diana

User ID	User Name	Email Address
diana	Diana Stuart	demo@bplogix.com

Once the user list type ahead has closed, the selected user will now appear in the delegation user picker, and tasks will be shared once the profile is saved.



Share my tasks with these users:

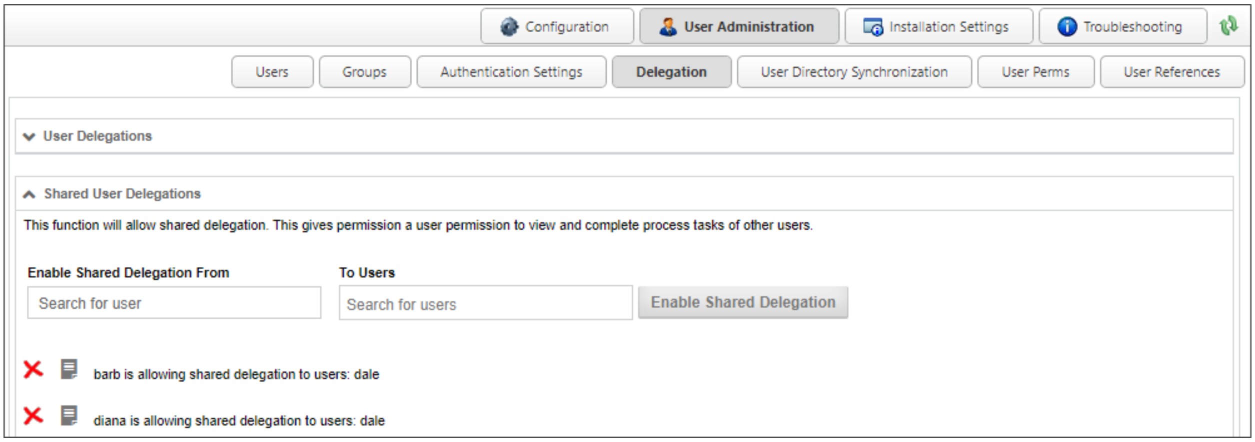
You can end the delegation by clicking the "X" icon that appears next to the delegates name, or clear ALL delegates by clicking the "X" icon that appears on the right side of the user picker.

When you have made the appropriate delegation decision, click the OK button at the bottom right of the User Profile screen to save and close the user profile.

The Shared Delegation functionality can be removed from the user profile page by setting the fTurnOffSharedDelegation Custom Variable to "true" in the Custom Vars file.

Delegation by Administrators

In the Delegation page of the User Administration section, you can set or remove multiple shared delegations. The screen also displays the currently active shared delegations in the Shared User Delegations section of the page, as displayed in the example below.



This function will allow shared delegation. This gives permission a user permission to view and complete process tasks of other users.

Enable Shared Delegation From: Search for user

To Users: Search for users

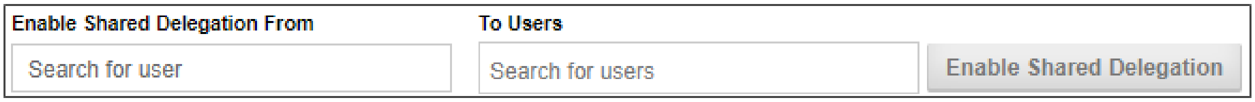
barb is allowing shared delegation to users: dale

diana is allowing shared delegation to users: dale

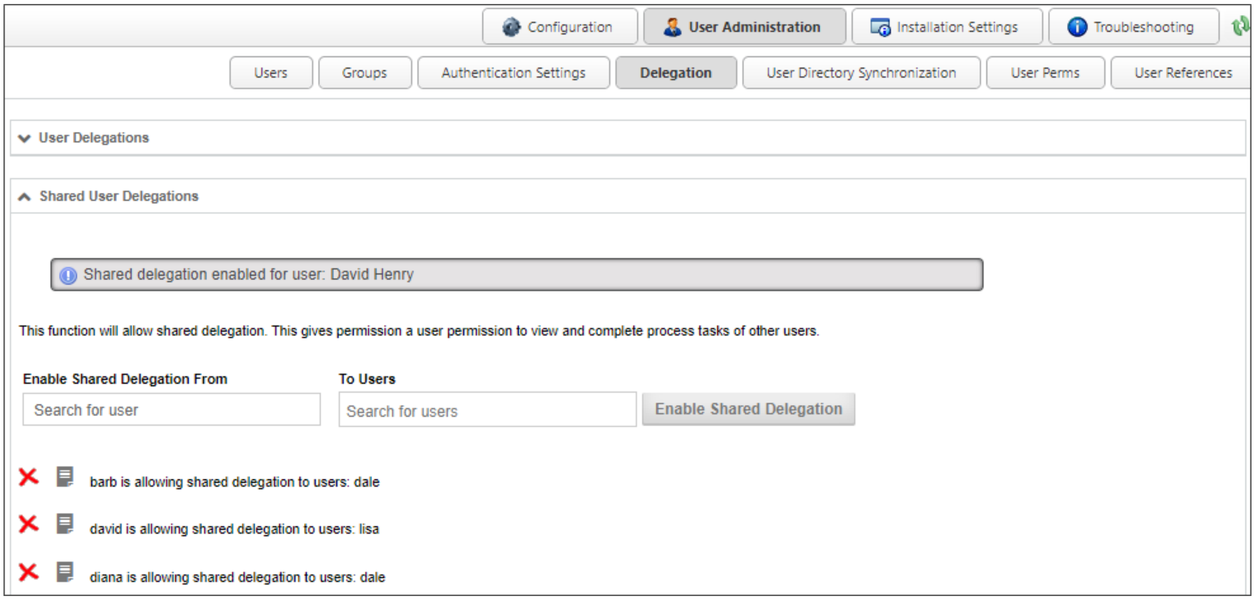
Setting Delegation

Use the User Pickers to select the from whom the tasks should be shared, and the user to whom tasks should be shared.

Once you have set both users for the delegation, click the Enable Shared Delegation button to create the delegation.



The delegation will be created immediately, and will appear in the delegation list at the bottom of the Delegation page, and a message will appear notifying you that the delegation has been successfully created.



Shared delegation enabled for user: David Henry

This function will allow shared delegation. This gives permission a user permission to view and complete process tasks of other users.

✕ barb is allowing shared delegation to users: dale

✕ david is allowing shared delegation to users: lisa

✕ diana is allowing shared delegation to users: dale

Removing Delegation

To remove a delegation, simply click the delete icon (✕) next to the delegation you wish to remove. The delegation will be canceled and a message will appear that notifies you that the delegation has been removed.

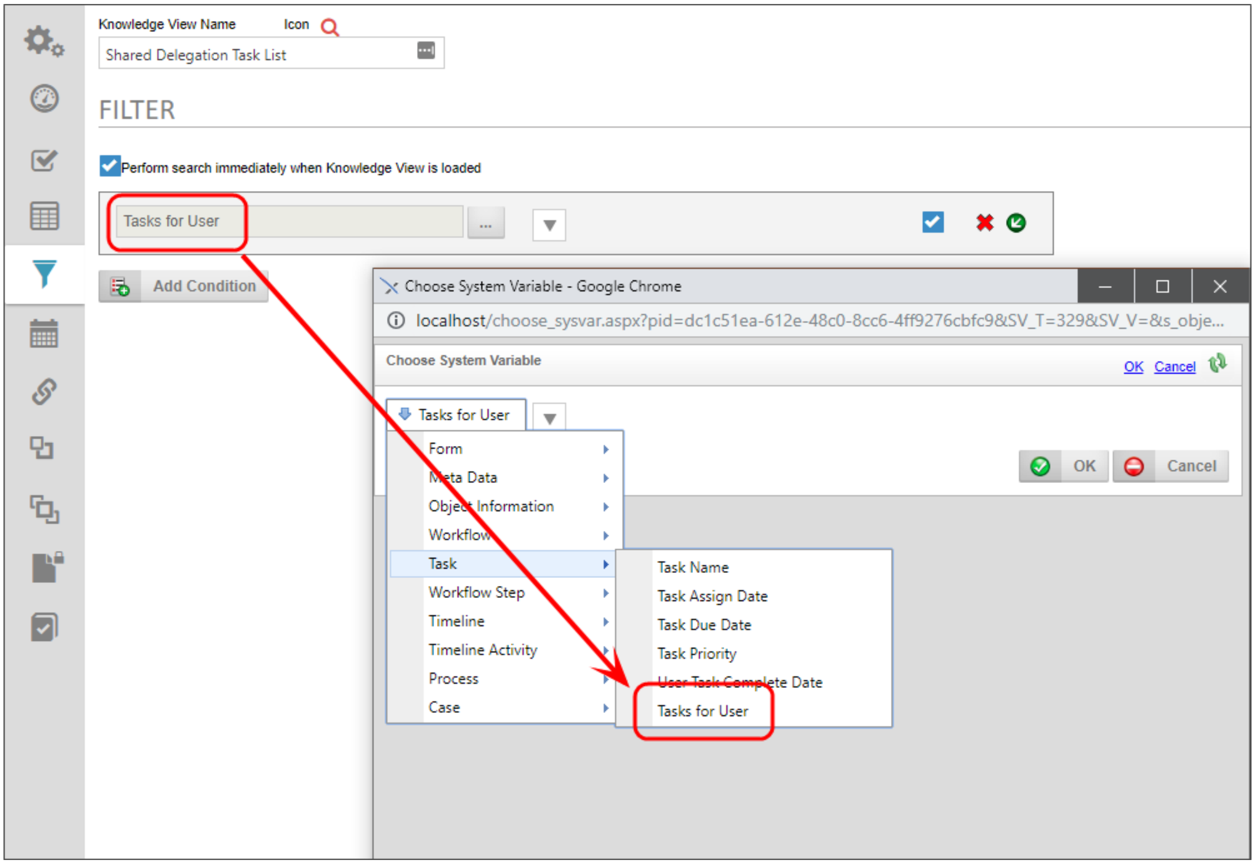
Selecting Tasks for Delegation

In order to enable a delegate to retrieve and complete shared tasks, the tasks must be specifically designated as shared tasks. On the Advanced tab of the User Timeline Activity type, there's an Allow Task Sharing property check box. This property check box must be checked or the task won't be shared with the delegate. This property enables you to implement task sharing on a per-task basis, which the default method for task sharing in the system.

You can, however, universally implement task sharing by setting the fSharedDelegationAllProcesses Custom Variable to "true". Conversely, you can completely disable task sharing by adding the appropriate disabling subroutine to the Custom Vars file.

Viewing Shared Delegations

Since tasks don't automatically get assigned to delegates when they are shared, the delegate must have a method to view the shared tasks that are available for completion. You must, therefore, provide a Task List Knowledge View to the delegates that applies a specific Filter to enable the delegates to view the shared tasks. On the Filter tab of the Knowledge View, you must use the Task >> Tasks for User system variable as the filter. This variable can also be accessed via the Task User system variable.


Knowledge View Name: Shared Delegation Task List

FILTER

☑ Perform search immediately when Knowledge View is loaded

Tasks for User

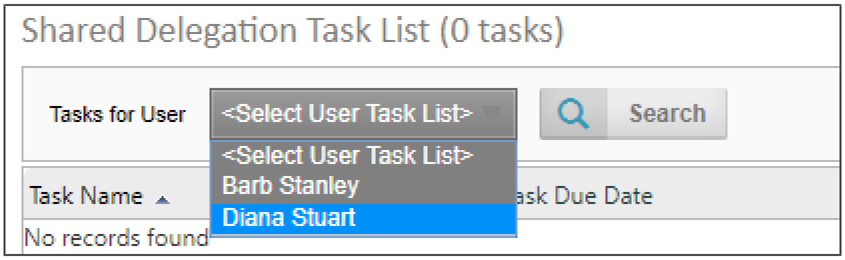
Choose System Variable - Google Chrome

localhost/choose_sysvar.aspx?pid=dc1c51ea-612e-48c0-8cc6-4ff9276cbfc9&SV_T=329&SV_V=&s_obje...

Choose System Variable

Tasks for User

When the Knowledge View runs, this filter will display a dropdown to enable the delegate to choose the delegator for whom the tasks should be viewed. The dropdown will only show users who have active tasks that have been delegated to the current user.



You can use the dropdown to select the desired delegator, then click the Search button to retrieve the tasks for that delegator. Once the tasks appear, the user can choose the tasks to complete, just as would be done in the default Task List.

For Process Director v5.26 and higher, Shared Delegation also supports delegation to unauthenticated users. This enables tasks assigned to anonymous users to appear in the task user dropdown in the Knowledge View filter, when the current user is the shared delegate owner in that activity.

Continue

Continue to the documentation for the User Directory Synchronization page.

User Directory Synchronization

If you are using an LDAP directory (e.g. Microsoft Active Directory) to authenticate your users, their User ID will be automatically added to the Process Director database when they first login. Process Director automatically synchronizes the user and group information when the login occurs. This happens transparently to the user. If you are using Windows Domain security to authenticate users you can still configure Process Director to synchronize user information with your LDAP server. This allows your users to authenticate against the Windows Domain, but still have their email address and user name (Alias) synchronized with the LDAP settings.

There are a couple of limitations to using this technique alone. It requires that a user logs into Process Director before it “knows” of that user and the groups the user belongs to. This means that you can't add users to a Timeline activity, or specify users in permissions until after that user logs into Process Director. Additionally, users or groups that are changed or removed in LDAP will still exist in the Process Director database.

To address these scenarios, there is a user directory synchronization utility that will synchronize your LDAP user information with Process Director. For **Active Directory** synchronization specifically, please see the Creating an Active Directory Sync Profile topic. For generic **LDAP synchronization**, please see the Creating an

LDAP Sync Profile topic. The synchronization utility will only synchronize attributes such as the name and email address, but won't copy over any passwords. Passwords are only stored on your LDAP server – the LDAP server is responsible for authentication.

How Directory Synchronization Works

In your LDAP or Active Directory database, each user account is assigned a unique value via a GUID. For example, in Active Directory, this value will be the **SID** for each account. This is the value that Process Director will use to uniquely identify each user account. Similarly, each synchronization profile you create in Process Director will also be assigned a unique GUID, known as the **ADID**. Finally, in each Process Director user account, another GUID, the **UserUID** will be assigned to the Process Director user account when it's created. These three, unique GUIDs govern how the synchronization process works.

Initial Provisioning

When you first provision users via a directory synchronization, which we'll simply call a "sync", a new Process Director user account will be created for each user contained in the sync. Inside Process Director, the new user account will be assigned a UserUID, Additionally, the SID (or other unique GUID) for each user account in your directory service will be stored as the External GUID, along with the ADID. So, each synced user account record will store all three of these unique identifiers.

Subsequent Synchs

For all subsequent synchs, three things will happen:

1. Each existing user account will match the External GUID and Synchronization profile to the corresponding values returned by the running sync. If any changes have been made to the user's attributes in the directory service, those changes will be updated for the existing users.
2. If the sync contains a user that does not exist in Process Director, a new user account will be created for that user.
3. If an existing user has been removed from the Directory Service, and is no longer available for syncing, Process Director will mark that user as disabled, (assuming that you haven't configured the Synchronization Profile to prevent disabling users).

At the conclusion of each sync, the active users in Process Director will match the active users contained in your directory service.

Synchronization Issues

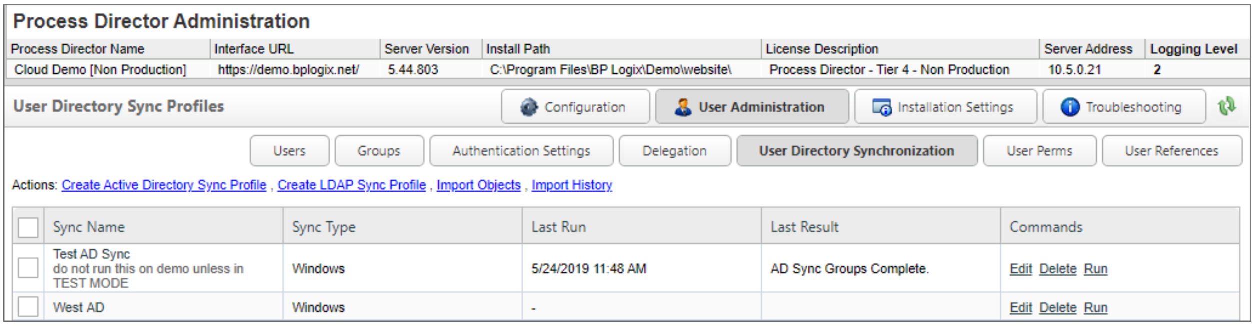
Because each Process Director user is specifically identified with both an AD/LDAP user and a Synchronization Profile, proper configuration is very important in ensuring that synchronization is accomplished correctly. Since that is so, there are some issues with synchronization about which you should be aware.

- If you sync the same AD user in two different synchronization profiles, the SID will be the same for the user, but the ADID will be different. In that case, Process Director will create two different user accounts for the same user. Thus, if you create multiple user sync profiles, you must ensure that each profile synchronizes a unique group of users.
- Similarly, once a user profile has been created, and users synced with it, the best practice, if changes need to be made, is to edit the existing sync profile. If you inactivate a user profile, and create a new profile that syncs the same users, new Process Director user accounts will be created for those users. Their original accounts, remember, are already associated with the sync Profile that originally created their Process Director accounts.
- It is possible, in AD, to have multiple SIDs for the same user. For instance, a user who has left and returned to your organization over time might have multiple AD SIDs for their original and new accounts. In AD, both of these SIDs can be unified into a single user identity via linking an attribute such as their network user name, e.g., Jane.Doe. Process Director, however, cannot perform this same type of account unification. Each SID uncovered during the sync will result in the creation of a separate user account. So, again, it's important to ensure that the sync profile only includes the AD account with the current SID to create a single account for that user.
- Every sync profile contains a property, Do Not Disable, that will, when checked, prevent users and/or groups from being disabled when a sync runs. When this property is checked, users removed from AD/LDAP will remain as active users in Process Director. It's important to ensure that this setting is ***unchecked*** if you want to ensure that your Process Director users correctly mirror your current AD/LDAP users.
- Inactive users are never deleted by a sync. Instead, inactive AD/LDAP users are disabled. BP Logix strongly recommends that you ***never*** delete a user account. User records are top-level records in the Process Director database, and cannot

be deleted without removing all of the child records associated with the user record. Thus, deleting a user would delete all records of that user's activity in the system. Disabled users, on the other hand, ***do not count against your license***, and ***cannot access Process Director***. But their historical activity is maintained and is auditable in the system.

Creating an Active Directory Sync Profile

This utility can be run manually, or scheduled to perform an automatic synchronization. To perform the synchronization, navigate to User Administration > User Directory Synchronization. Each sync configuration is a profile. Each profile will, after running, display when the synchronization was last performed, and the result of the synchronization.



Process Director Administration

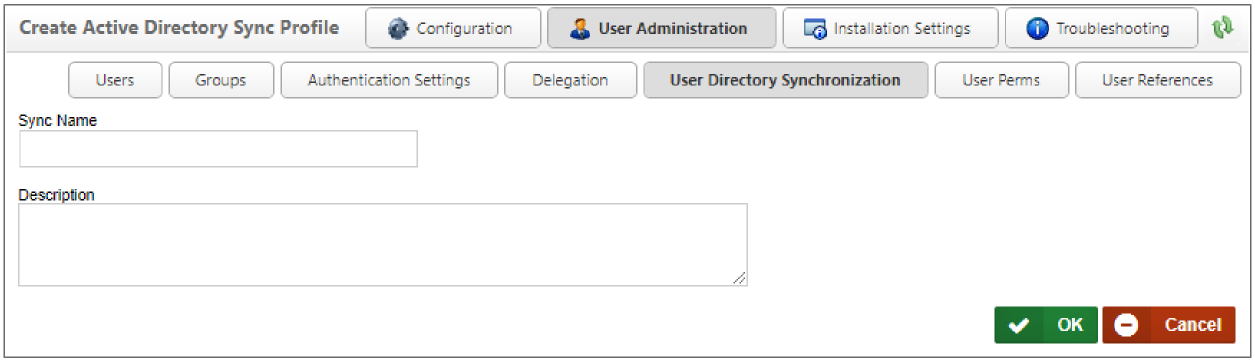
Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
Cloud Demo [Non Production]	https://demo.bplogix.net/	5.44.803	C:\Program Files\BP Logix\Demo\website\	Process Director - Tier 4 - Non Production	10.5.0.21	2

User Directory Sync Profiles

Actions: Create Active Directory Sync Profile , Create LDAP Sync Profile , Import Objects , Import History

□	Sync Name	Sync Type	Last Run	Last Result	Commands
□	Test AD Sync do not run this on demo unless in TEST MODE	Windows	5/24/2019 11:48 AM	AD Sync Groups Complete.	Edit Delete Run
□	West AD	Windows	-		Edit Delete Run

You can create many profiles to sync specified users or groups of users. These profiles will be saved to the database so you may run them at any time. You can create a profile by selecting the Create Active Directory Sync Profile link. Clicking this link will open the Create Active Directory Sync Profile window, into which you can enter the Sync Name and Description of the profile, then click the OK button to open the configuration screen for the new profile.

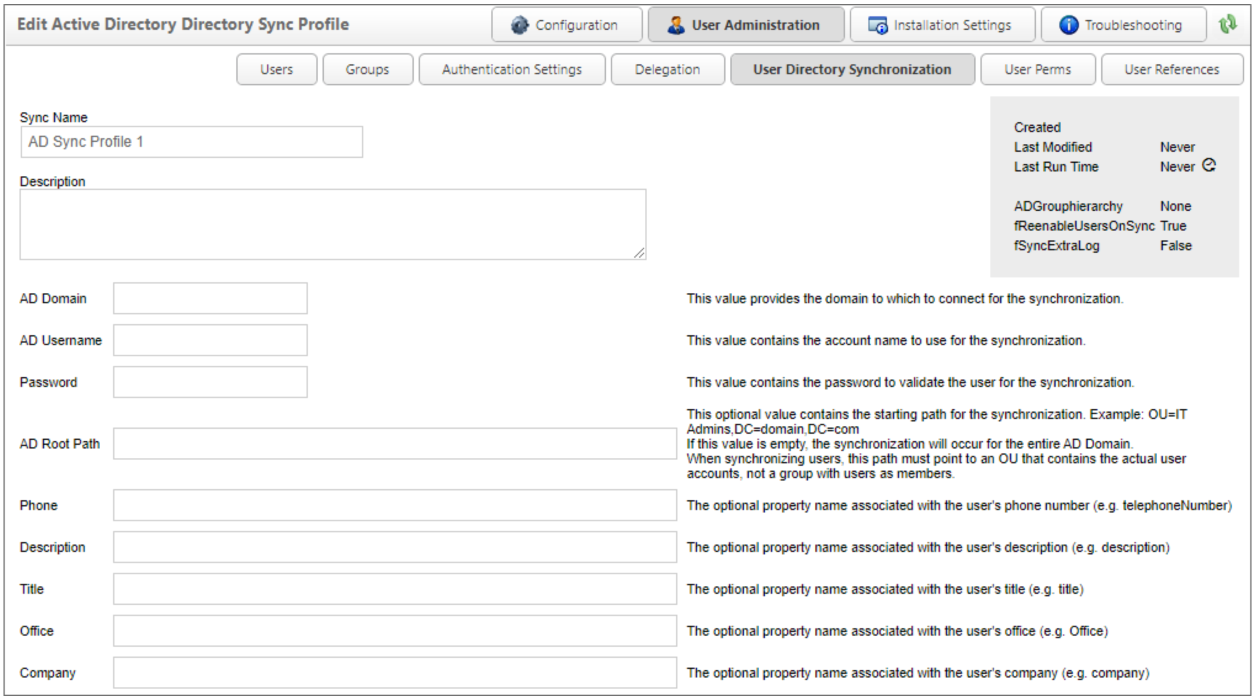


Create Active Directory Sync Profile

Sync Name

Description

Configure the profile by selecting the appropriate values for the settings displayed, then click the OK button to save the settings to the profile.



Sync Name: AD Sync Profile 1

Description

Created	
Last Modified	Never
Last Run Time	Never
ADGrouphierarchy	None
fReenableUsersOnSync	True
fSyncExtraLog	False

AD Domain	This value provides the domain to which to connect for the synchronization.
AD Username	This value contains the account name to use for the synchronization.
Password	This value contains the password to validate the user for the synchronization.
AD Root Path	This optional value contains the starting path for the synchronization. Example: OU=IT Admins,DC=domain,DC=com If this value is empty, the synchronization will occur for the entire AD Domain. When synchronizing users, this path must point to an OU that contains the actual user accounts, not a group with users as members.
Phone	The optional property name associated with the user's phone number (e.g. telephoneNumber)
Description	The optional property name associated with the user's description (e.g. description)
Title	The optional property name associated with the user's title (e.g. title)
Office	The optional property name associated with the user's office (e.g. Office)
Company	The optional property name associated with the user's company (e.g. company)

Synchronization Profile Properties #

The following properties are configurable in the Active Directory Sync Profile.

Sync Name

The name of the profile that will appear in the list of available profiles on the User Directory Synchronization page.

Description

An optional, brief description of the profile's purpose.

AD Domain

The Active Directory Domain with which you wish to synchronize.

AD Username

The Active Directory User name that has permissions to pull data from the domain with which you wish to synchronize.

Password

The password associated with the AD Username.

From the Phone Field to the Custom Number Field

A list of fields that can be mapped to Active Directory fields to store the relevant data contained in Active Directory.

Secure

This option forces the synchronization to use a secure connection (SSL).

Test Connection Settings

This button, when clicked, will make a test connection to the specified AD Domain to ensure the connection works properly.

Sync Objects

A series of check boxes that enable you to choose which object types to sync. There are three checkboxes available to configure:

- **Users:** Will sync only AD users in the specified AD domain.
- **Groups:** Will sync only AD Groups in the specified AD domain, without syncing the user membership for the groups.
- **User Group Memberships:** When syncing Groups, this setting ensures that the users will be assigned to the Groups of which they are members in AD.

Limit Users to Group

This optional value will synchronize only the users within the specified Active Directory group.

Limit Groups to Group

This optional value will limit the synchronization only to the groups within the specified Active Directory group.

Add Objects to Partitions

This optional dropdown value lists the partitions that exist on the installation, and enables you to specify the partition to which to add the synchronization objects.

Add Users to Groups

This optional value specifies to which Process Director groups to add the synchronization users.

Do Not Disable

This option indicates that the synchronization will add new objects from an AD Sync, but will NOT disable already existing users or groups which the sync doesn't find.

Remove Users From Groups

This option indicates that the synchronization will remove users from groups in Process Director when they are removed from the AD group.

Add as Day Pass Users

This option indicates that the synchronized users should be added as licensed day pass users. This option is only relevant to installations licensed for user passes.

Debug Mode

This option runs the synchronization in "Debug Mode" - providing more verbose logging.

Test Mode

This option causes the synchronization to fetch all the object to synchronize without adding them to Process Director.

Interactively Run This Sync Profile

Clicking this button will manually run the Synchronization. By default, the Sync will run in Test Mode, so you'll need to be sure to uncheck the Test Mode property to run an actual sync.

Manual Execution of an Active Directory Sync Profile

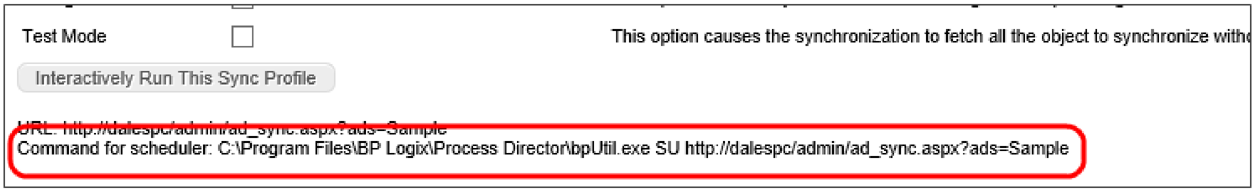
To execute a profile, navigate to the User Directory Synchronization page and select the Run command from the profile you'd like to run. This will display the AD Sync Run page. The AD Sync Run page displays the profile configuration with the option of changing your settings for that run instance.

If the synchronization occurs successfully, you'll see the number of users and groups that were synchronized.

Scheduled Execution of an Active Directory Sync Profile

To automatically schedule the profile to run at regular intervals (for example, every night at midnight) use the Microsoft Windows Scheduled Tasks utility. This utility enables you to schedule and test commands executed on a regular basis.

Do not schedule IEXPLORE.EXE because the web browser will never close. Rather, use the bputil.exe command to run the web page. Process Director has created this path for you. Navigate the AD Sync Run Page and copy and paste the URL under Directory Connection to the Windows Scheduler.



Test Mode □ This option causes the synchronization to fetch all the object to synchronize with

URL: http://dalespc/admin/ad_sync.aspx?ads=Sample
Command for scheduler: C:\Program Files\BP Logix\Process Director\bpUtil.exe SU http://dalespc/admin/ad_sync.aspx?ads=Sample

For example, enter this command in the “Run” dialog box to schedule the synchronization:

```
"PATH\bputil.exe" SU "http://localhost/WD/admin/ad_sync.aspx?ads=Profile_Name"
```

where PATH is the installation directory for Process Director (e.g. c:\Program Files\BP Logix\Process Director\). Enter the appropriate credentials in the Windows Scheduler when prompted. Use the “Schedule” tab to set the times to run the command. Consult the Microsoft help for more information on this utility.

> **You must enclose the URL to ad_sync.asp in double quotes.**

User Synchronization

AD users will be created in the Process Director database when synchronization is performed and when the user logs in. The user ID, display name, email address and organization hierarchy will be kept in sync. If a user is renamed in AD it will be reflected in the Process Director database during a login or a synchronization operation. If a user is deleted in AD, the user will be disabled in the Process Director database. It is recommend that the user ID be left as disabled instead of deleting it so that the user history is maintained (e.g. processes they participated in, documents they modified, etc.).

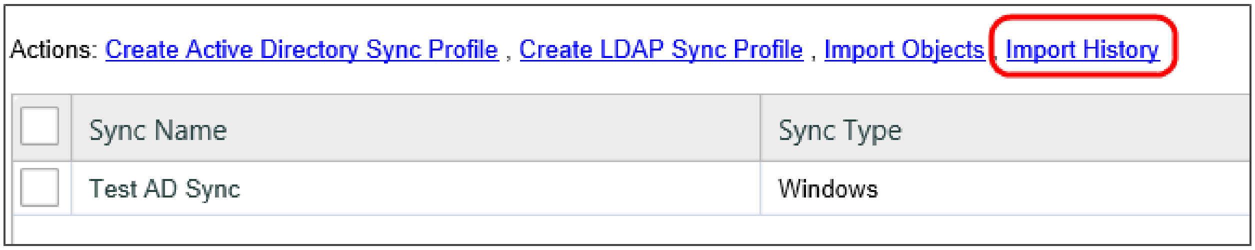
Group Synchronization

The integration will synchronize the AD groups. These will be created as groups in Process Director. When using AD groups, if you delete or rename groups in AD they'll be removed from the Process Director database. When renaming an AD group, you should rename it in the Process Director User Administration Group section first. This isn't required for AD users.

For more information on User or Group synchronization, please see the topic on User Directory Synchronization.

Active Directory Synchronization Log #

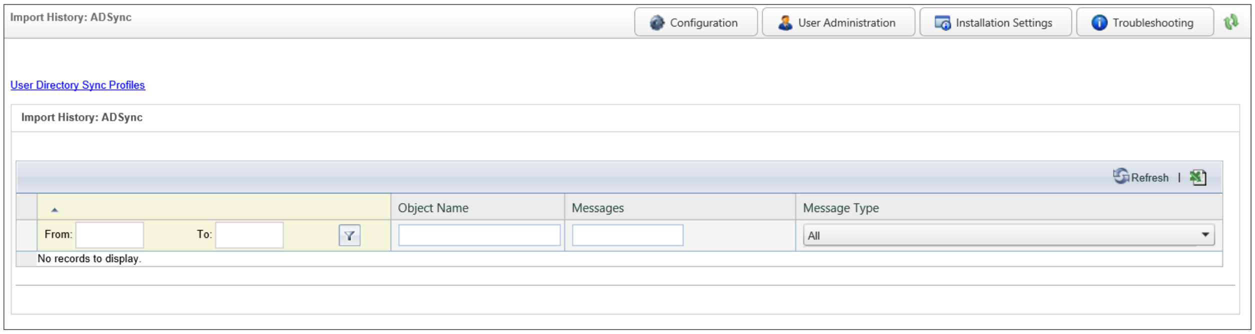
Installations that use the Auditing component have access to a Synchronization log that is saved to the database when an Active Directory synchronization is run. The link to this page is available from the Import History action link at the top of the User Directory Synchronization page.


Actions: Create Active Directory Sync Profile , Create LDAP Sync Profile , Import Objects , Import History

□	Sync Name	Sync Type
□	Test AD Sync	Windows

This link opens a searchable log page to view all of the log events generated during a synchronization.

> **❗ Please be aware that larger organizations may have—depending on the size and frequency of the synchronizations—a huge number of log entries, which can return a massive amount of data and degrade system performance. The number of records returned, however, can be restricted by setting the nMaxADSyncLogEvents and fKeepADSyncInfoLogs custom variables.**



	Object Name	Messages	Message Type
From: To:			All

No records to display.

A number of filters are available on the page to assist you with searching for specific entries.

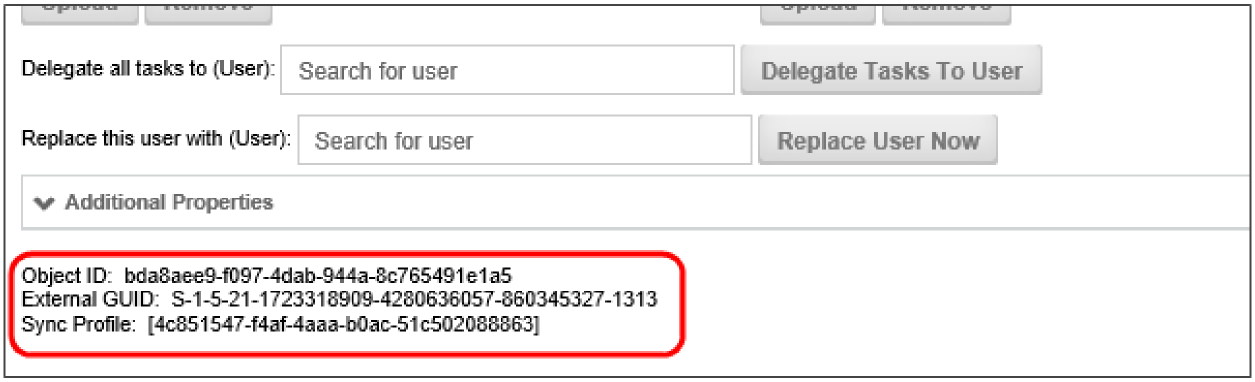
- **From/To:** You can perform a search only for log entries that occurred between specified dates. An additional Filter button provides you with appropriate date conditions to apply to the From/To criterion.
- **Object Name:** You can search for entries that have specific text in the object name, such as a username.
- **Messages:** You can search for entries that have specific text in the log Message.
- **Message Type:** You can search for specific message types by selecting the appropriate message type from the dropdown control. Available message types are All, Info, Warning, and Error.

When you configure the options, clicking the Refresh button will reload the log files that match your conditions. An Export to CSV button is also available to export the log results to a CSV file that can be opened in Microsoft Excel.

You can return to the AD Synchronization page by clicking the User Directory Sync Profiles action link.

Synchronization Issues #

When a user is managed via an Active Directory Synchronization, some extra information about the user is available at the bottom of the user's account profile.



Object ID: bda8aee9-f097-4dab-944a-8c765491e1a5
External GUID: S-1-5-21-1723318909-4280636057-860345327-1313
Sync Profile: [4c851547-f4af-4aaa-b0ac-51c502088863]

The Object ID is the user's internal UID in Process Director. The External GUID is the user's SID in Active Directory, which is copied over to Process Director, and placed in the sExternalGuid field of the record in the tblUser database table for this user, and links the user's Process Director ID to the Active Directory ID for this user. Finally, the Sync Profile is the ID of the Synchronization Profile that is used to synchronize this user.

When a user is synchronized, once, they are permanently associated with a specific Active Directory account and Sync Profile.

This association can be lost under some circumstances:

- The user leaves the organization, and is removed from AD. The user will be disabled, but not deleted, on the next AD Sync. If the user returns to the organization, and a new AD account is created, then the user will appear as a NEW user in Process Director, and the existing account won't be reassociated.
- Similarly, If you move the user to a different AD Sync profile, the same thing will happen, because Process Director will assume that the user in the new AD Sync profile is a different user. Again, a new account will be created, and the old account disabled.

In such cases you may want to reassociate the same Process Director user with the changed AD Account, so that you can maintain continuity with the Process Director user's different profiles or AD Accounts.

In such cases, the solution we would recommend is creating an admin form that allows a user ID and new AD GUID or Profile ID to be entered and have it update the tblUser database table. This form would update the Process Director sExternalGUID and/or oADID fields in the table tblUser within the Process Director database for the affected user. The form can save the original GUIDs from tblUser in the form instance, just in case there was a mistake made. Also, that would provide an audit trail of changes. You can then delete the new user from Process Director.

> ❗ **This is an advanced solution, so you should use due caution in implementing it. We *very strongly* advise you to contact us for Direct Assistance in creating this solution unless you are absolutely sure you know how to implement it.**

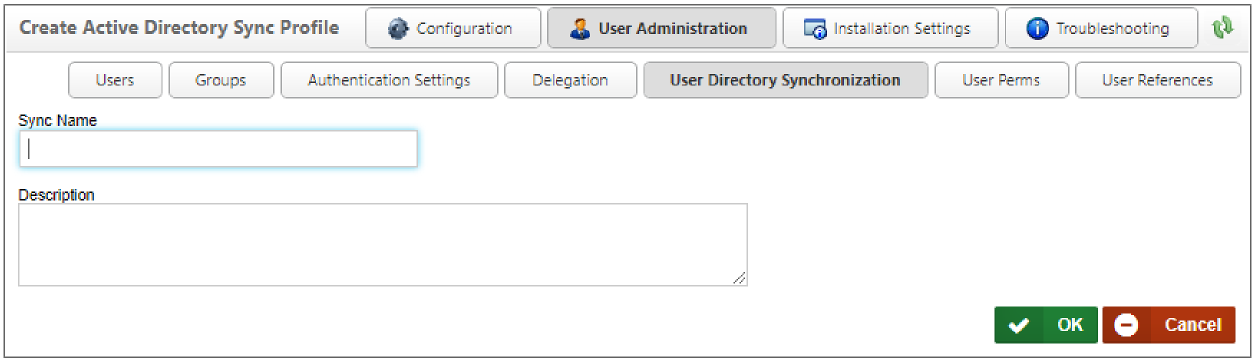
Continue

Continue to the documentation for the Creating an LDAP Sync Profile, User Perms, and User References pages, all of which are included in the main User Administration topic.

Creating an LDAP Sync Profile

This utility can be run manually, or scheduled to perform an automatic synchronization. To perform the synchronization, navigate to User Administration > User Directory Synchronization. Each sync configuration is a profile. Each profile will, after running, display when the synchronization was last performed, and the result of the synchronization.

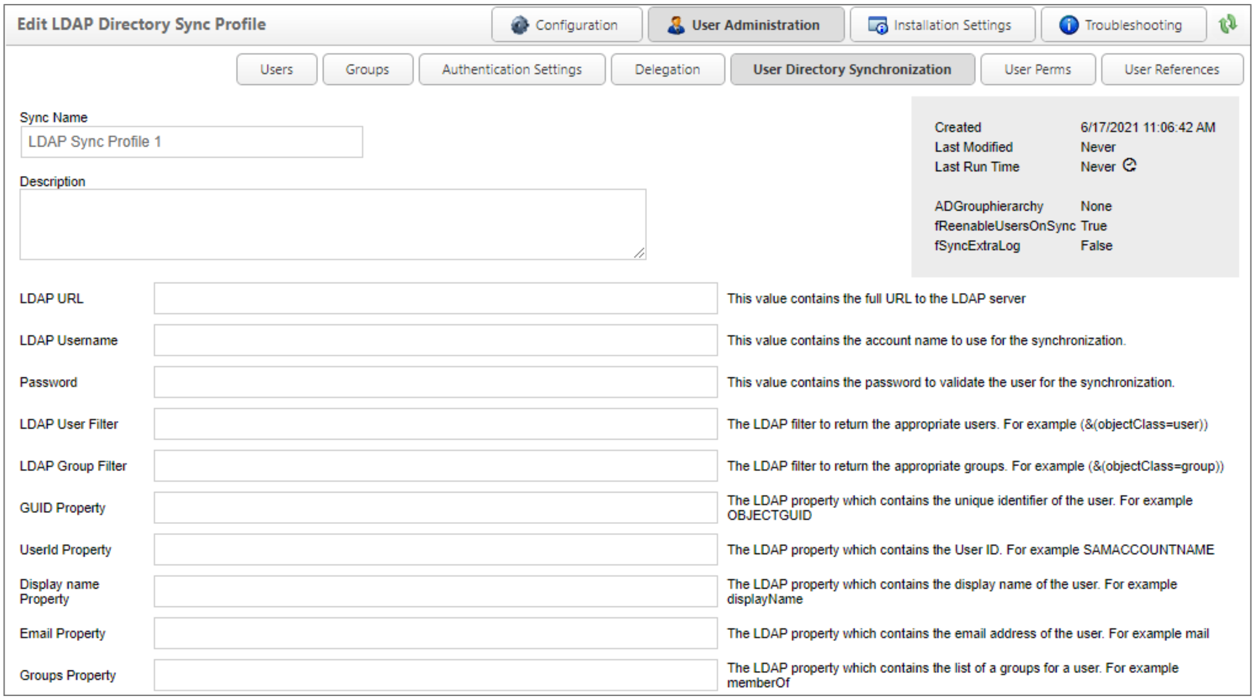
You can create many profiles to sync specified users or groups of users. These profiles will be saved to the database so you may run them at any time. You can create a profile by selecting the Create LDAP Sync Profile link. Clicking this link will open the Create Active Directory Sync Profile page (This is the same page that's used to create a new AD Sync profile), into which you can enter the Sync Name and Description of the profile, then click the OK button to open the configuration page for the new profile.



Sync Name

Description

Configure the profile by selecting the appropriate values for the settings displayed, then click the OK button to save the settings to the profile.



Sync Name
LDAP Sync Profile 1

Description

Created	6/17/2021 11:06:42 AM
Last Modified	Never
Last Run Time	Never
ADGrouphierarchy	None
fReenableUsersOnSync	True
fSyncExtraLog	False

LDAP URL	This value contains the full URL to the LDAP server
LDAP Username	This value contains the account name to use for the synchronization.
Password	This value contains the password to validate the user for the synchronization.
LDAP User Filter	The LDAP filter to return the appropriate users. For example (&(objectClass=user))
LDAP Group Filter	The LDAP filter to return the appropriate groups. For example (&(objectClass=group))
GUID Property	The LDAP property which contains the unique identifier of the user. For example OBJECTGUID
UserId Property	The LDAP property which contains the User ID. For example SAMACCOUNTNAME
Display name Property	The LDAP property which contains the display name of the user. For example displayName
Email Property	The LDAP property which contains the email address of the user. For example mail
Groups Property	The LDAP property which contains the list of a groups for a user. For example memberOf

Synchronization Profile Properties #

The following properties are configurable in the Active Directory Sync Profile.

Sync Name

The name of the profile that will appear in the list of available profiles on the User Directory Synchronization page.

Description

An optional, brief description of the profile's purpose.

LDAP URL

The URL of the LDAP server with which you wish to synchronize.

LDAP Username

The LDAP User name that has permissions to pull data from the domain with which you wish to synchronize.

LDAP Group Filter

The LDAP filter to use, if any, to return only users in groups that match the filter.

Password

The password associated with the LDAP Username.

LDAP User Filter

The LDAP filter to use, if any, to return only users that match the filter.

GUID Property

The LDAP property that contains the unique identifier for each user.

UserId Property

The LDAP property that contains the UserID.

From the Display Name to the Custom Number Field

A list of fields that can be mapped to LDAP fields to store the relevant data contained in the LDAP Directory.

LDAP Options

This property consists of a series of check boxes you can check to select specific options to use during the Synchronization.

> **These properties are specific to LDAP server access and/or binding. Please consult your LDAP administrator to determine which settings are appropriate, based on your LDAP server's configuration, as some of these settings are mutually exclusive.**

- **Secure:** Use the Secure LDAP service to run the synchronization.
- **Encryption:** Use the STARTTLS (LDAP over TLS) service for the synchronization.
- **Secure Sockets Layer:** Use the LDAPS (LDAP over SSL) service for the synchronization.
- **ReadOnlyServer:** Specifies that a writable server isn't required, and to allow connection to a read-only cache/replica of the writable server.
- **Anonymous:** Enables anonymous binding.
- **FastBind:** Enables the server to process concurrent bind requests on the same connection.
- **Signing:** Enables the server to the server to reject Simple Authentication and Security Layer binds that don't request signing, or to reject LDAP simple binds that are performed on a clear-text connection.
- **Sealing:** Sealing encrypts the LDAP payload data to avoid transmitting it in clear-text.
- **Delegation:** Use the delegate account to perform the synchronization.
- **ServerBind:** Invokes the LDAP ServerBind method to determine how access to the LDAP server will be allowed.

Sync Objects

A series of check boxes that enable you to choose which object types to sync. There are three checkboxes available to configure:

- **Users:** Will sync only users in the specified LDAP directory, based on the LDAP User/Group Filter you configure.
- **Groups:** Will sync only AD Groups in the specified LDAP directory, based on the LDAP User/Group Filter you configure. This setting will not sync the user membership for the groups.

- **User Group Memberships:** When syncing Groups, this setting ensures that the users will be assigned to the Groups of which they are members in the LDAP directory.

Limit Users to Group

This optional value will limit the users to sync to only the users within the specified group.

Limit Groups to Group

This optional value will limit the groups to sync to only the groups within the specified group.

Add Objects to Partitions

This optional dropdown value lists the partitions that exist on the installation, and enables you to specify the partition to which to add the synchronization objects.

Add Users to Groups

This optional value specifies to which Process Director groups to add the synchronization users.

Do Not Disable

This option indicates that the synchronization will add new objects from an LDAP Sync, but will NOT disable already existing users or groups which the sync doesn't find.

Remove Users From Groups

This option indicates that the synchronization will remove users from groups in Process Director when they are removed from the LDAP group.

Add as Day Pass Users

This option indicates that the synchronized users should be added as licensed day pass users. This option is only relevant to installations licensed for user passes.

Debug Mode

This option runs the synchronization in "Debug Mode" - providing more verbose logging.

Test Mode

This option causes the synchronization to fetch all the object to synchronize without adding them to Process Director.

Interactively Run This Sync Profile

Clicking this button will manually run the Synchronization. By default, the Sync will run in Test Mode, so you'll need to be sure to uncheck the Test Mode property to run an actual sync.

Operation of the LDAP Sync Profile

While the configuration settings for Active Directory and LDAP synchronization profiles are slightly different, all synchronization operation operate identically. For information on synchronization methods, Synchronization Logs, and synchronization issues, please refer to the Creating an Active Directory Sync Profile topic, or these specific sections of that topic:

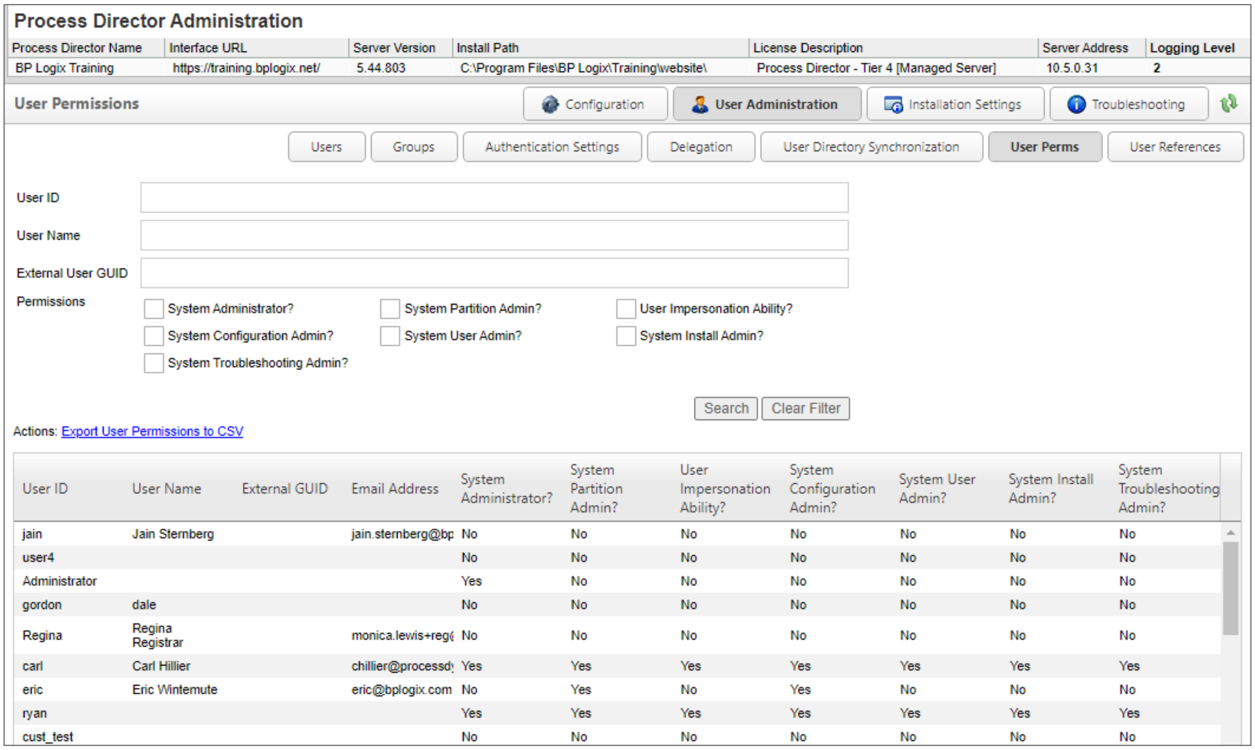
- Manual Execution
- Scheduled Execution
- Synchronization Log
- Synchronization Issues

Continue

Continue to the documentation for the Creating an AD Sync Profile, User Perms, and User References pages, all of which are included in the main User Administration topic.

User Perms

Administrators of Cloud installations or on-Premise installations with the Compliance Option will notice an additional User Perms page in the User Administration section.



Process Director Administration

Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
BP Logix Training	https://training.bplogix.net/	5.44.803	C:\Program Files\BP Logix\Training\website\	Process Director - Tier 4 [Managed Server]	10.5.0.31	2

User Permissions

User ID

User Name

External User GUID

Permissions

□ System Administrator? □ System Partition Admin? □ User Impersonation Ability?
□ System Configuration Admin? □ System User Admin? □ System Install Admin?
□ System Troubleshooting Admin?

Actions: Export User Permissions to CSV

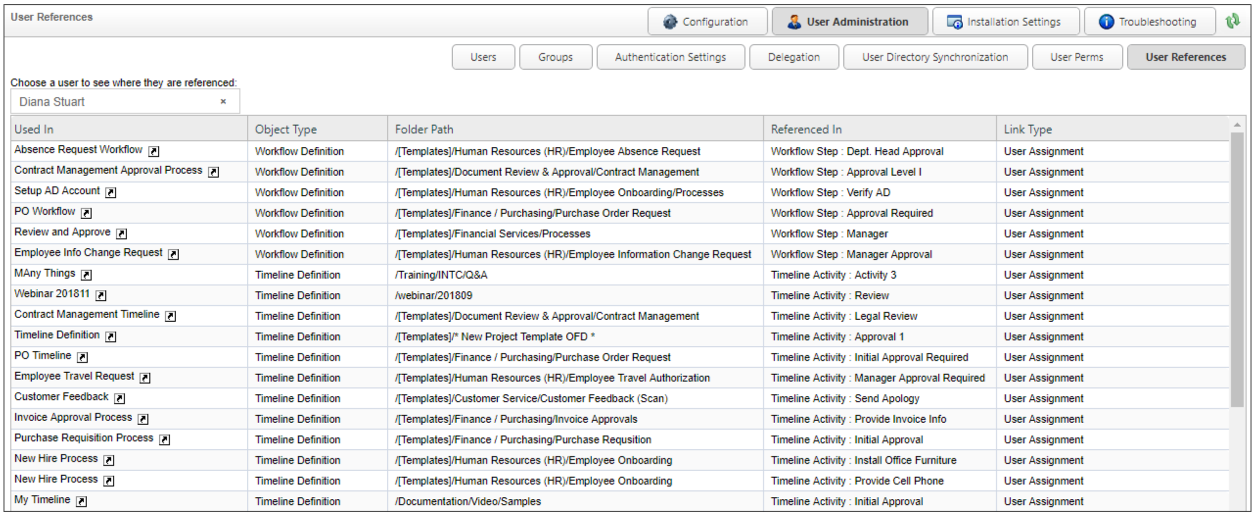
User ID	User Name	External GUID	Email Address	System Administrator?	System Partition Admin?	User Impersonation Ability?	System Configuration Admin?	System User Admin?	System Install Admin?	System Troubleshooting Admin?
jain	Jain Sternberg		jain.sternberg@bp	No	No	No	No	No	No	No
user4				No	No	No	No	No	No	No
Administrator				Yes	No	No	No	No	No	No
gordon	dale			No	No	No	No	No	No	No
Regina	Regina Registrar		monica.lewis+reg(	No	No	No	No	No	No	No
carl	Carl Hillier		chillier@processd\	Yes	Yes	Yes	Yes	Yes	Yes	Yes
eric	Eric Wintemute		eric@bplogix.com	No	Yes	No	Yes	No	No	No
ryan				Yes	Yes	Yes	Yes	Yes	Yes	Yes
cust_test				No	No	No	No	No	No	No

The User Perms page enables you to find users and view a report of permissions that are applicable to that user.

The top section of the page provides a number of search fields that you can fill out to filter the number of objects returned by the search. The filter criteria will accept all or part of a User ID or User Name, or the GUID of an external user. Once you have entered the filter criteria you desire, click the Search button to see a list of all the objects that match your filter criteria.

User References

For Process Director v5.12 and higher, administrators have the ability to find all references in the system for a particular user from the User References page.



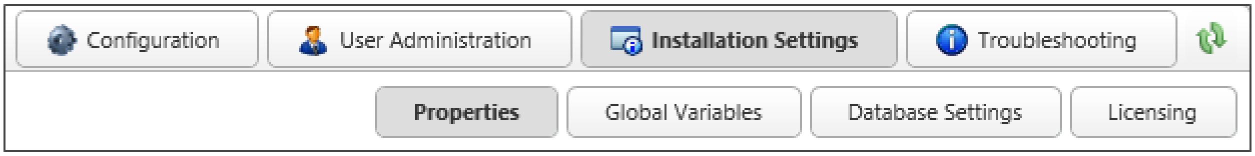
Choose a user to see where they are referenced: Diana Stuart

Used In	Object Type	Folder Path	Referenced In	Link Type
Absence Request Workflow	Workflow Definition	/[Templates]/Human Resources (HR)/Employee Absence Request	Workflow Step : Dept. Head Approval	User Assignment
Contract Management Approval Process	Workflow Definition	/[Templates]/Document Review & Approval/Contract Management	Workflow Step : Approval Level I	User Assignment
Setup AD Account	Workflow Definition	/[Templates]/Human Resources (HR)/Employee Onboarding/Processes	Workflow Step : Verify AD	User Assignment
PO Workflow	Workflow Definition	/[Templates]/Finance / Purchasing/Purchase Order Request	Workflow Step : Approval Required	User Assignment
Review and Approve	Workflow Definition	/[Templates]/Financial Services/Processes	Workflow Step : Manager	User Assignment
Employee Info Change Request	Workflow Definition	/[Templates]/Human Resources (HR)/Employee Information Change Request	Workflow Step : Manager Approval	User Assignment
MAny Things	Timeline Definition	/Training/INTC/Q&A	Timeline Activity : Activity 3	User Assignment
Webinar 201811	Timeline Definition	/webinar/201809	Timeline Activity : Review	User Assignment
Contract Management Timeline	Timeline Definition	/[Templates]/Document Review & Approval/Contract Management	Timeline Activity : Legal Review	User Assignment
Timeline Definition	Timeline Definition	/[Templates]/* New Project Template OFD *	Timeline Activity : Approval 1	User Assignment
PO Timeline	Timeline Definition	/[Templates]/Finance / Purchasing/Purchase Order Request	Timeline Activity : Initial Approval Required	User Assignment
Employee Travel Request	Timeline Definition	/[Templates]/Human Resources (HR)/Employee Travel Authorization	Timeline Activity : Manager Approval Required	User Assignment
Customer Feedback	Timeline Definition	/[Templates]/Customer Service/Customer Feedback (Scan)	Timeline Activity : Send Apology	User Assignment
Invoice Approval Process	Timeline Definition	/[Templates]/Finance / Purchasing/Invoice Approvals	Timeline Activity : Provide Invoice Info	User Assignment
Purchase Requisition Process	Timeline Definition	/[Templates]/Finance / Purchasing/Purchase Requsition	Timeline Activity : Initial Approval	User Assignment
New Hire Process	Timeline Definition	/[Templates]/Human Resources (HR)/Employee Onboarding	Timeline Activity : Install Office Furniture	User Assignment
New Hire Process	Timeline Definition	/[Templates]/Human Resources (HR)/Employee Onboarding	Timeline Activity : Provide Cell Phone	User Assignment
My Timeline	Timeline Definition	/Documentation/Video/Samples	Timeline Activity : Initial Approval	User Assignment

To see all of the objects that reference a user, simply select the desired user from the Choose a user to see where they are referenced User Picker. Once you select the user, the references will automatically be retrieved and listed in a bottom part of the page.

Installation Settings

This section of the IT Admin area enables you to set and change the general settings that control the overall operation of your Process Director installation.



NOTE: For Cloud customers, some settings may be hidden from user accounts that aren't specified as Managed Users.

The Installation Settings section contains four different pages for configuring the Process Director installation. You can navigate to the documentation for each page by using the Table of Contents displayed in the upper right corner of the page, or by using the links below.

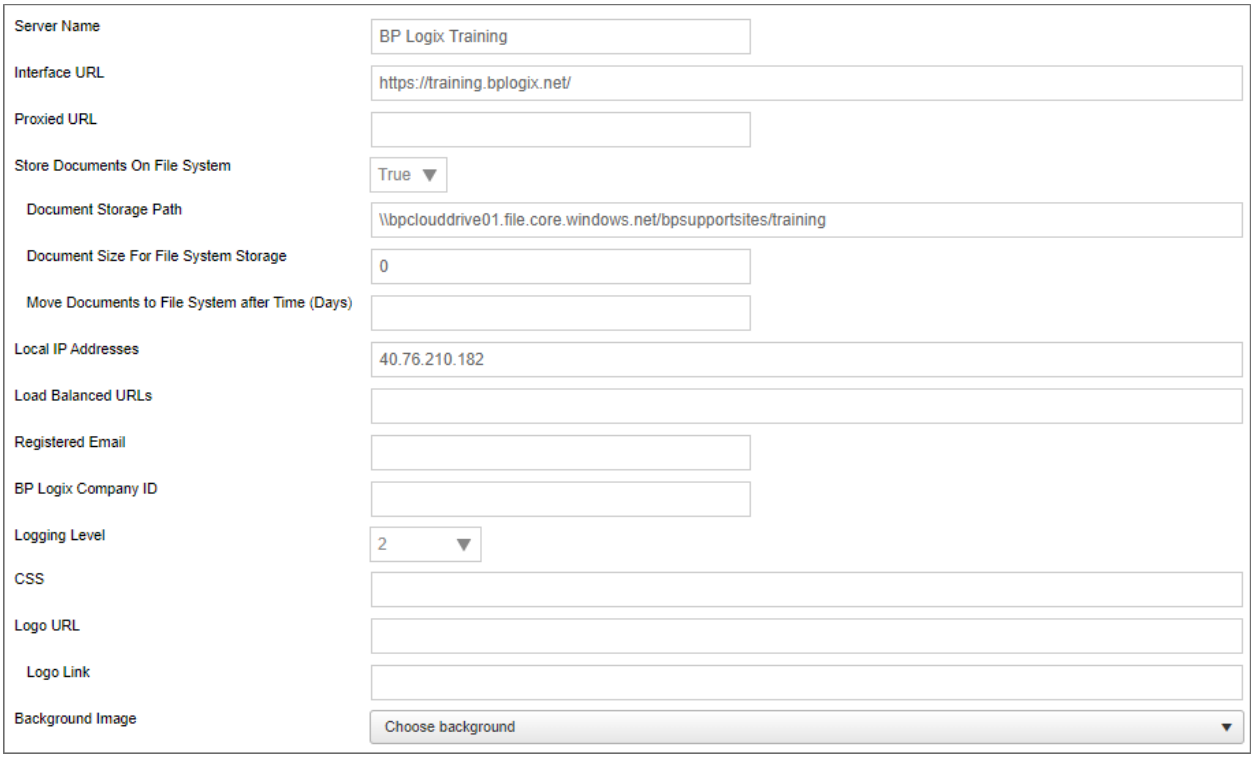
Properties: General system properties.

Global Variables: Variables that set general system options.

Database Settings: Sets the connection to the Process Director database.

Licensing: Validates and stores your Process Director licensing information.

Properties



Server Name	BP Logix Training
Interface URL	https://training.bplogix.net/
Proxied URL	
Store Documents On File System	True ▼
Document Storage Path	\\bpclouddrive01.file.core.windows.net/bpsupportsites/training
Document Size For File System Storage	0
Move Documents to File System after Time (Days)	
Local IP Addresses	40.76.210.182
Load Balanced URLs	
Registered Email	
BP Logix Company ID	
Logging Level	2 ▼
CSS	
Logo URL	
Logo Link	
Background Image	Choose background ▼

The Properties page lists the basic options to configure the Process Director Server, which helps maximize the flexibility of Process Director. Below is the list of options available on the Properties page.

Server Name

The name for the Process Director installation.

Interface URL

Specifies the actual host name that can be used to connect to Process Director.

Proxy URL

Specifies the URL of your proxy server, if you have one in use.

Store Documents on File System

Enables you to store documents on the server file system. Setting this option will require you to set the Document Storage Path and Document Size for File System Storage properties. For more information about storing documents in the Process

Director database as opposed to the file system, see the Storing Attachments topic.

There are times when you may want to store the binary data on a file system, instead of in the database. For example, if you are dealing with very large digital assets/documents, or a large number of them, storing them on the file system may be better. If your database gets too large with document data, it can slow functions like your database backups. When binaries are stored on the file system, you still will have entries in the internal document tables, but the BLOB column will be empty. It is transparent to the implementers and end-users where the document binaries are stored.

Document Storage Path

Actual file path to store files.

Document Size for File System Storage

Enables you to set the minimum size requirement of the file to be stored on the file system. If you want to store ALL files in the file system, set the value of this property to 0.

Move Documents to File System after Time (Days)

For Process Director v6.00.100 or higher, this property will accept a properly formatted date to move all documents with file dates prior to the specified date to file storage.

Local IP Addresses

Enables you to add a comma separated list of IP addresses that have permission to the IT Admin area of Process Director.

Load balanced URLs

Process Director incorporates load balancing to share the processing load between multiple Process Director installations. This property takes a comma-separated list of URLs that are part of the load balancing scheme.

Registered Email

This is an email address to use as a fallback "From" address for process notifications if one of the primary email addresses isn't available. The "From" address for a process notification is set by the first value ***that isn't empty*** from the following list:

1. The value manually configured in an email template's EmailData Control.
2. The value configured the Workflow From Email Address setting in the Installation Settings > Global Variables section.
3. If administratively Canceled, the email of the administrator that performed the operation.
4. The email of the Process Initiator.
5. The value configured in the Registered Email Address.
6. As a final fallback: tech-support@bplogix.com

> ⓘ **For users of Process Director v5.27 and higher, Process Director enables the use of address strings with a Display Name component (e.g. "Test User <test@example.com>").**

BP Logix Company ID

This property stores the 5-digit customer number that BP Logix assigns to each customer. While largely optional, this field is used to send Logs via email on the logs page.

Logging Level

Enables you to set a specific logging level that may provide more information in the logs.

CSS

Enables you to specify a custom CSS file. It is recommended to place the CSS file in the custom directory of the Process Director install.

Logo URL

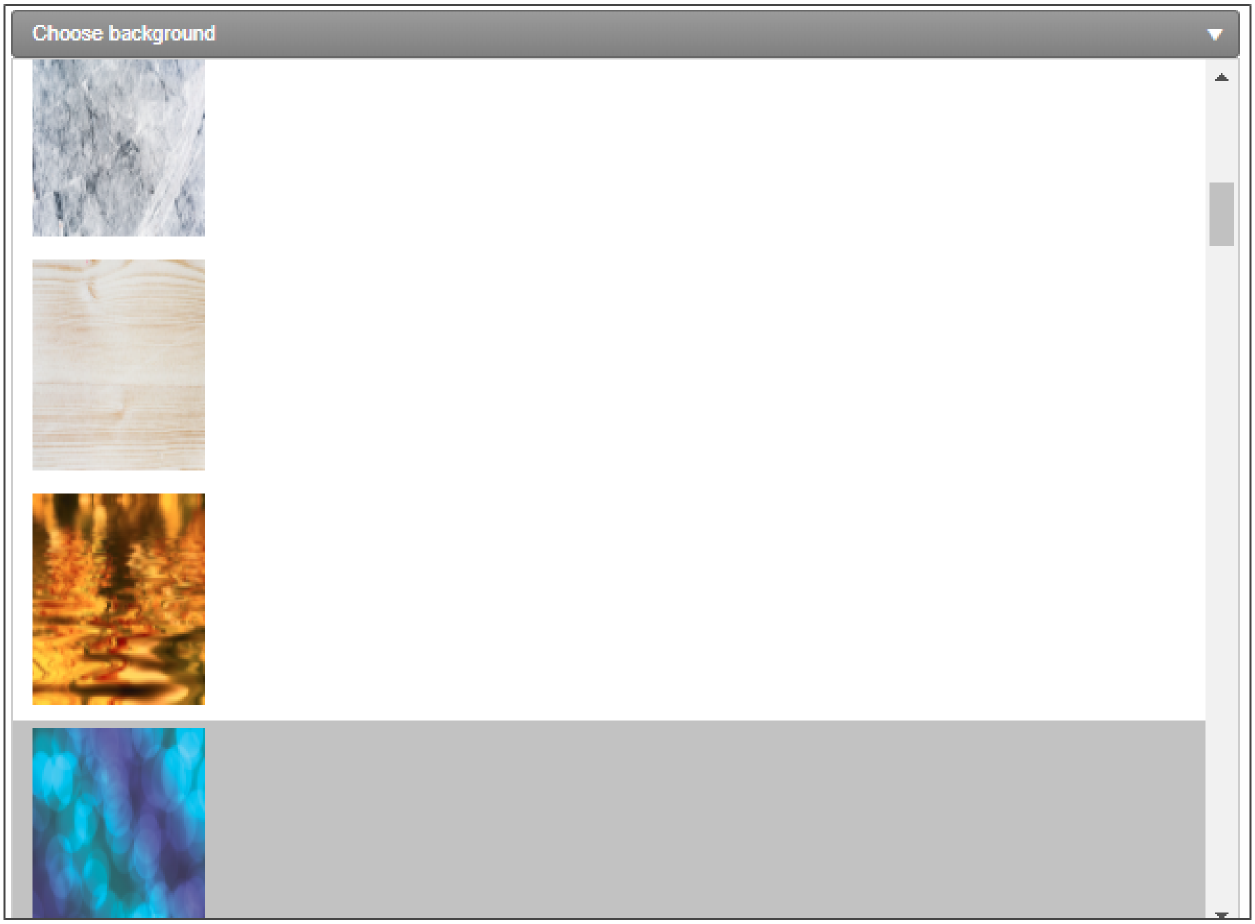
Enables you to specify an image to replace the logo throughout the system. Additionally you can specify a hotlink for the logo.

Logo Link

Enables you to specify a URL to which users will be sent if they click the logo image.

Background Image

Enables you to specify a pre-defined background image to display in the background of the Login page. A number of stock images are displayed in the dropdown control enabling you to select the desired background image.



Background Image Sizing

Enables you to specify how the background image will appear on the login page. The following options are available:

- Cover: The image will expand to fill the entire page background.
- Center: The image will appear in its actual size, centered on the page vertically and horizontally.
- Tile: The image will appear in its actual size, aligned to the top left of the window, and will tile vertically and horizontally.
- Tile X: The image will appear in its actual size, aligned to the top left of the window, and will tile along the X-axis only.

- Tile Y: The image will appear in its actual size, aligned to the top left of the window, and will tile along the Y-axis only.

Home Page Top Height

Enables you to adjust the height of the top navigation bar.

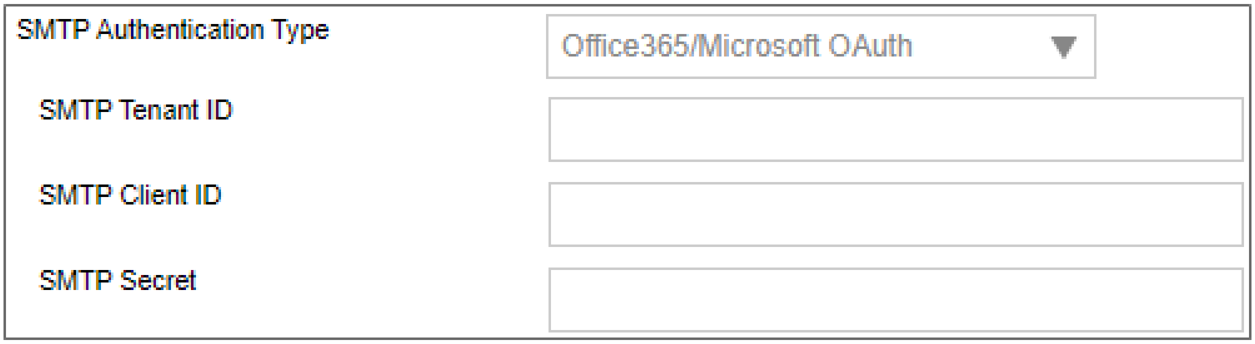
Home Page Logo Width

Enables you to specify the width of the logo displayed at the top right of the page.

SMTP Authentication Type

For Process Director v5.44.1103, this property enables an OAuth-based connection to Azure services by setting this property to "Office365/Microsoft OAuth". When set to this authentication type, three additional settings will appear:

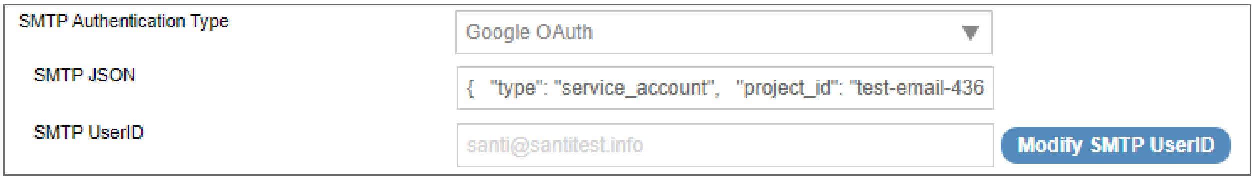
- SMTP Tenant ID
- SMTP Client ID
- SMTP Secret



SMTP Authentication Type	Office365/Microsoft OAuth ▼
SMTP Tenant ID	
SMTP Client ID	
SMTP Secret	

Please see the Microsoft OAuth for SMTP topic for more information on the configuration and use of this Authentication Type and its associated properties.

For Process Director v6.1.300 and higher, Google OAuth has been added as an Authentication Type.



SMTP Authentication Type	Google OAuth ▼
SMTP JSON	{ "type": "service_account", "project_id": "test-email-436
SMTP UserID	santi@santitest.info

The Google OAuth authentication requires two properties.

- SMTP JSON: This property consists of a JSON snippet, provided by your Google Console. The JSON must be pasted into this property, and will be used to send the appropriate JSON authentication data to Google.
- SMTP UserID: This property is the Google UserID, usually an email address, to log into the specific inbox that will be used to send messages via Google.

SMTP Host

Enables you to set a host name or IP address for the SMTP Host. By default it will use the local SMTP server. Setting this property also allows you to set the SMTP Port, SMTP UserID, and SMTP Password, and SSL Required properties.

You do have some different options for sending mail from the system.

1. Using “relay” through your existing mail server (e.g. Azure/Exchange, etc.)
   - This method requires that your mail server enables relay. This can be controlled by IP address and/or the use of credentials to connect to your SMTP mail server.
   - If your mail server can't return quickly from a large number of mail request, this could slow the end user experience in Process Director when the completion of a form results in process emails being sent out. To work around this, you can use option #3. This will perform a store and forward that won't be delayed with slowdowns in the email server responding.
2. Using the local IIS SMTP server to send the emails directly to the recipients
   - This method will send emails from the local SMTP server. It may be necessary to setup a DNS SPF, DKIM or reverse DNS record for this server so recipients don't flag these emails as SPAM.
3. Using the local IIS SMTP server to relay through your mail server using the “Smart Host” configuration.
   - This method requires that your mail server enables relay from this IP address. It will forward all emails through your mail server using a store/forward technique, allowing retries.
4. Relaying through a mail provider (e.g. SMTP.com)
   - This method requires that a provider be created and that recipients will allow emails sent from this domain to be received.

BP Logix recommends that you enable your mail server to accept mail relay from the IP Address of the process Director server, and set the SMTP host to the mail server name, e.g., relay.domain_name.com. This will provide the most direct connection to your mail server, and enable your mail server to impose organizational policies, and return error messages to Process Director.

SMTP Port

The SMTP port used to send email. The default SMTP port is 25 for unencrypted connections. For encrypted connections, BP Logix recommends using port 587 and enabling the SSL Required property.

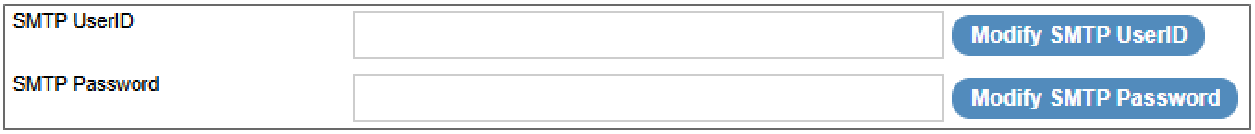
For more information on SMTP connections to Microsoft Azure, please see Microsoft's documentation on this topic.

SMTP UserID/Password

SMTP UserID: The User Name for the email account that will be used to send email.

SMTP Password: The Password for the email account that will be used to send email.

For Process Director v6.1.200 and higher, both of these fields are now disabled by default. Some password managers can automatically insert unwanted values into user name and password fields automatically, without the user being aware of it. To prevent this inadvertent and unwanted behavior, these fields cannot be edited unless the user enables them by clicking one of the Modify buttons next to the field value.


SMTP UserID
SMTP Password

Clicking one of the Modify buttons will enable its associated field, so that the field can be edited.

SSL Required

Determines whether the connection to the SMTP server will require SSL to encrypt the UserID and password when sent to the SMTP server. This setting is required to be enabled when using encrypted connections.

Web Service Enabled

Enables you to enable or disable Web Services for the system. Additionally you can add restrictions. Setting this property allows you to set the Require Web Service Authentication and Web Service Restrictions properties.

Require Web Service Authentication

Determines whether authentication is required to use a web service.

Web Service Restrictions

A comma-separated list of IP Addresses that you enter into this field, which will restrict access to web services to only requests from the IP Addresses entered. Leaving this field blank will allow universal access to web services.

In addition to a comma-separated list of IP Addresses, this field also supports CIDR notation for an IP Address range, e.g., "10.1.1.0/24" will use all IP Addresses between 10.1.1.0 and 10.1.1.24.

Number of Custom Icons

Enables you to set the number of custom icons that you can use in the Process Director interface. The default setting is 0. If you create any custom icons, you must set this value to the exact number of custom icons that you have created. For information on creating custom icons, please see the Creating Custom Icons topic.

Enable trust MFA for 30 days

This property, when set to true, will enable the system to limit requests for MFA authentication confirmation to once every thirty days. This setting is somewhat out of order, and it appears below the M365 CDA settings at the bottom of the page.

Microsoft 365 CDA Installation Settings

For Process Director v6.1.300 and higher, the product supports the use of Microsoft 365 for CDA. All prior versions can use only the third-party document editing service provided by OnlyOffice. The implementation of M365 for CDA requires several properties be configured on the Installation Settings > Properties page.

Microsoft 365 SharePoint CDA Site URL

The URL of the SharePoint/M365 site that hosts the office installation.

Microsoft 365 SharePoint CDA Root Folder

The root folder in which the documents will be stored for access via CDA.

Microsoft 365 Tenant ID

a. The ID of the Tenant in which the registered application resides in Azure/Entra. Creation of an application requires the existence of a Tenant.
b. The Tenant ID is displayed as the Directory (tenant) ID property on the Overview page of your AAD Application in Azure, but this value will also be displayed following `login.microsoft.com/...` in the Endpoint URLs that the App references.

Like SMTP, This is an OAuth property to enable authentication with Microsoft.

Microsoft 365 CDA Client ID

a. The ID of the Application in SharePoint.
b. This value is displayed as the Application (client) ID property on the Overview page of your application from the "Site" application registration.

Microsoft 365 CDA Client Secret

The client secret or application password the administrator created to use with the application.

Microsoft 365 CDA Advanced options (optional)

A list of options to pass to your M365 system, using JSON format.

❗ **This property should only be configured at the direction of BP Logix support personnel.**

For Process Director v6.1.305 and higher, some additional properties have been added.

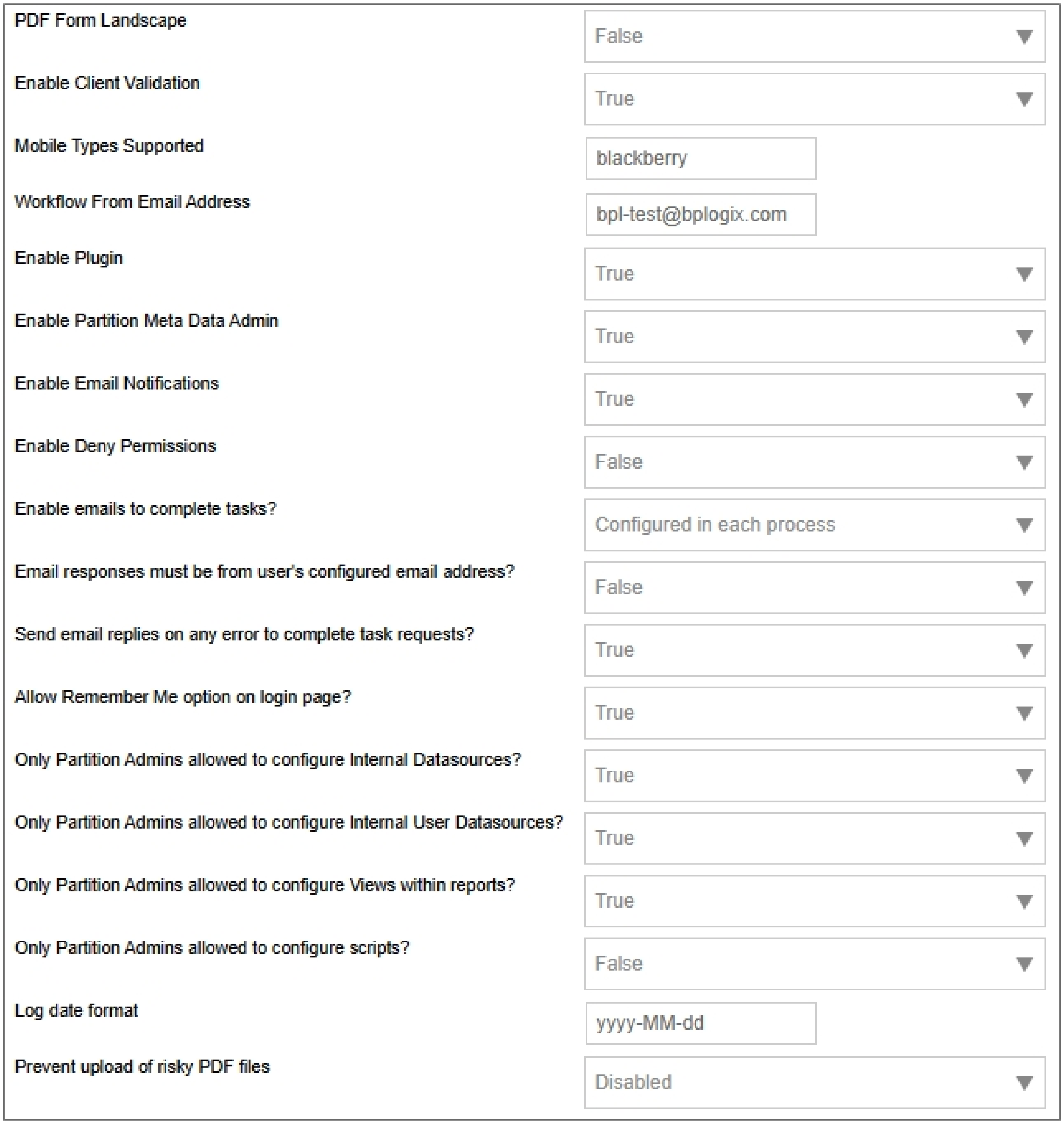
Microsoft 365 CDA Certificate

This property enables you to upload the certificate required to accept document uploads for use as attachments to be edited via M365 CDA.

Microsoft 365 CDA Certificate Password

The password needed to access the uploaded certificate.

Global Variables



PDF Form Landscape	False
Enable Client Validation	True
Mobile Types Supported	blackberry
Workflow From Email Address	bpl-test@bplogix.com
Enable Plugin	True
Enable Partition Meta Data Admin	True
Enable Email Notifications	True
Enable Deny Permissions	False
Enable emails to complete tasks?	Configured in each process
Email responses must be from user's configured email address?	False
Send email replies on any error to complete task requests?	True
Allow Remember Me option on login page?	True
Only Partition Admins allowed to configure Internal Datasources?	True
Only Partition Admins allowed to configure Internal User Datasources?	True
Only Partition Admins allowed to configure Views within reports?	True
Only Partition Admins allowed to configure scripts?	False
Log date format	yyyy-MM-dd
Prevent upload of risky PDF files	Disabled

The Global Variables page enables specific options to be enabled or disabled throughout the system.

PDF Form Landscape

Setting this value to "True" will set the landscape aspect ratio as the default for all PDF conversions.

Enable Client Validation

Setting this value to "True" will allow the Process Director installation to use client-side validation. The data that the user enters is validated in the user's browser before being sent to the server. If the validation fails, the user can correct the data immediately. Only data that passes client-side validation is sent to the server, which helps reduce server load. Without client validation, all data must be sent to the server for validation, which may require multiple round trips to the server before the data passes validation. Client-side validation removes the need for these round trips to the server for invalid data.

Mobile Types Supported

Enables you to specify the type of mobile devices supported by Process Director by entering a comma-separated list of HTTP types. The default is "blackberry". Available HTTP types include: Android, iPad, iPhone, etc.

Workflow from Email Address

Enables you to specify the default “from” email address for a process. If this value is set, ALL emails sent from a Process Timeline will be sent from this email address. This field will accept a display-formatted email address, using the format:

```
Display Name <username@domain.com>
```

Enable Plug-in

Enables or disables the client plug-in for Process Director.

Enable Partition Meta Data Admin

Enables you to enable or disable the partition Meta Data administration for Process Director.

Enable Email Notifications

Enables you to enable or disable email notifications for running processes. If this property is disabled, Process Director won't send any emails.

Enable Deny Permissions

If this property is set to "True", permissions can be set to deny users access to Process Director objects.

Enable emails to complete tasks?

Enables you to allow users to complete tasks via email. This option can be enabled in two ways. Setting this value to "Yes" will enable all tasks to be completed via email. Setting this value to "Configured in each process" will enable process designers to determine whether completion by email should be allowed on a given process.

Email responses must be from user's configured email address?

Setting this value to "True" will ensure that Process Director will only accept task responses sent from the email address specified in the user's profile. Responses from any other email address will be ignored. If users will respond from alternate email addresses, then this value must be set to "False".

Send email replies on any error to complete task requests?

If set to "True", any validation error that arises when a task response is submitted will send an email notification to the sender of the original error.

Allow Remember Me option on login page?

Setting this value to "True" will enables the "Remember Me" option on the login page. When the user checks the "Remember Me" check box on the login page, the user won't need to type in a password on subsequent logins.

Only Partition Admins allowed to configure Internal Datasources?

Setting this value to "True" ensures that only Partition Admins will be allowed to configure a Datasource to use the Internal database.

Only Partition Admins allowed to configure Internal User Datasources?

Setting this value to "True" ensures that only Partition Admins will be allowed to configure a Datasource to use the Internal User database.

Only Partition Admins allowed to configure Views within reports?

Setting this value to "True" ensures that only Partition Admins will be allowed to configure a View within a Report Definition.

Only Partition Admins allowed to configure scripts?

Setting this value to "True" ensures that only Partition Admins will be allowed to configure scripts for Forms, Process Timelines, and Knowledge Views.

Log Date Format

Available in Process Director v6.0.11 and higher, this property enables you to set a date format to apply to log entries. This property accepts all of the standard date format placeholders, as described in the System Variable Parameters topic's DateTime System Variables section. For instance, setting the Log Date Format to `yyyy-MM-dd` would display the date portion of a log entry as `2023-11-21` for a log entry made on November 21, 2023. You do not need to add a time format to this property. Times in the log entry timestamps are automatically formatted as `HH:mm:ss`, and are added to the date automatically.

> ❗ **Any change to this setting will NOT take effect in Process Director until the system has been restarted. This property is only recognized and implemented as part of the startup process. Once the system is restarted, log entries will use the specified format for dates.**

Prevent upload of risky PDF files

Available in Process Director v6.1.300 and higher, setting this value to "True" will scan all PDF file uploads for malicious code, such as Cross-Site Scripting attacks, and prevent the documents from being uploaded to the system.

Enable Workflow

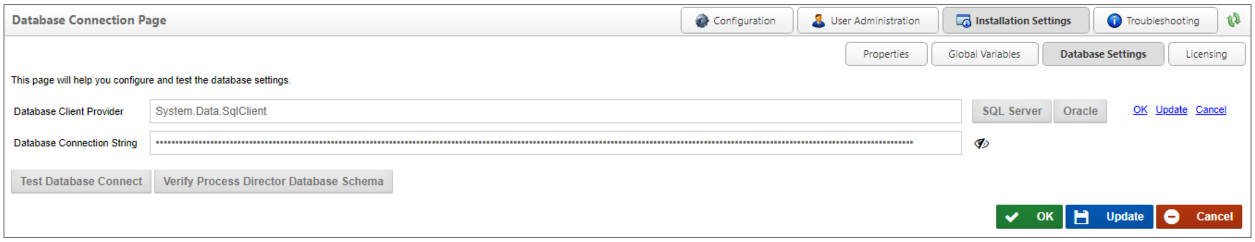
For Process Director v6.1.500, the ability to create new Workflow definitions is disabled by default. This property enables you to enable Workflow objects for creation in the Create New menu of the Content List.

***BP Logix strongly recommends that you do NOT use Workflows. You should use the Process Timeline object as the process model for all new applications.* The Workflow object is the legacy process model used in early versions of Process Director, and has been deprecated. It remains in the product *solely* for backwards compatibility, and hasn't received any new functionality updates since Process Director v4.5. For Process Director v6.1.500, Workflow creation is disabled by default in the product, though it can be re-enabled via a setting on the Global Variables page of the IT Admin area.**

Database Settings

The Database Settings page allows you to set the database connection string and database client provider. Once you have entered your connection strings, ensure that you saved your settings. You may also test the connection by clicking the Test Database Connect button. This will return a valid statement or return an error. The Verify Process Director Database Schema button will run a test on the database to ensure that the data schema for the Process Director database you've selected is compatible with the version of Process Director you have installed.

For Process Director v6.0.100 and higher, the header text, Database Connection Page, has been changed to Database Settings, to match the page name specified on the navigation button.



This page will help you configure and test the database settings.

Database Client Provider: System.Data.SqlClient

Database Connection String: ••

As a security enhancement to Process Director v6.0 and higher, passwords in connection strings and password fields are obfuscated by

default, and will not display unless the "Eye" icon adjacent to the field is clicked, which will show the password in clear text.

Licensing

You must add a license key after installation to activate Process Director from the Licensing page.

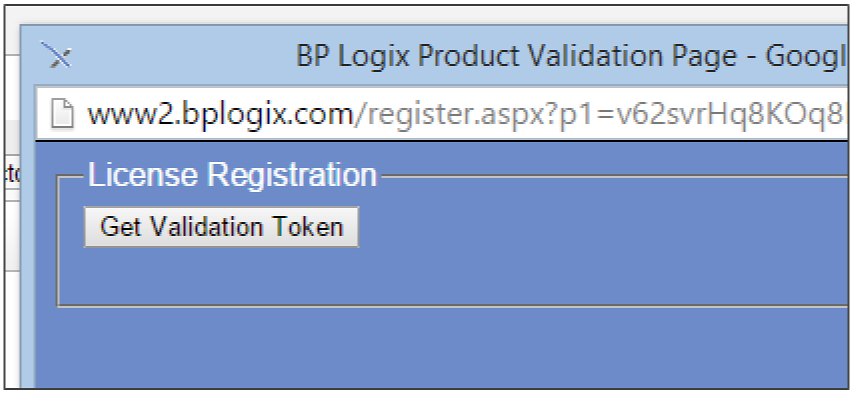
1. Enter the license key that was sent from BP Logix into the License Key text box.
2. Generate a Validation Token using either
   a. The Get Validation Token button which launches a web page that displays the validation token, or
   b. Pasting the Validation URL displayed on the Licensing page into any Internet connected browser.
3. Copy the Validation Token displayed on the registration page that was opened in Step 2, and paste it into the Validation Token text box on the Licensing page.
4. Validate the token by clicking the Validate Token button to complete the registration.

❗ The Validation Token is generated from an evaluation of certain technical characteristics of the server on which Process Director is installed. Each Validation Token is specific to the server that requested the token. Validation Tokens can't be transferred from one server to another, as each token is unique to the server that generated it.

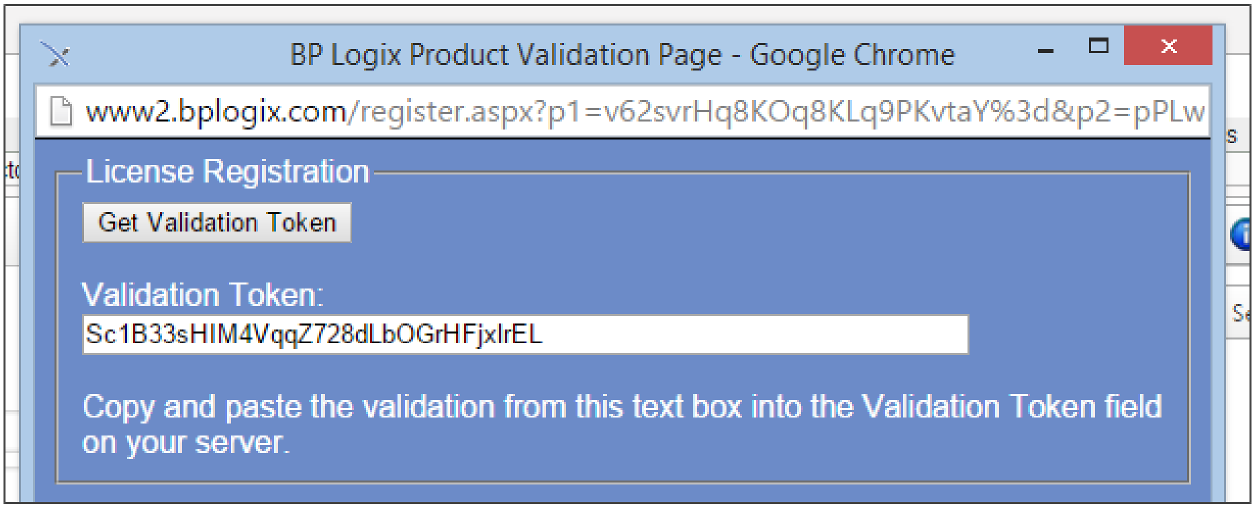
Reregistering your License

Some Process Director licenses have an expiration date, and this requires that the license be reregistered to keep using the software after the registration expires. To reregister your license, go to the Licensing page of the Installation Settings section, and perform the following procedure:

1. Click the Get Validation Token button, which will launch the **BP Logix Product Validation Page** as a pop-up web page.


BP Logix Product Validation Page - Googl
www2.bplogix.com/register.aspx?p1=v62svrHq8KOq8
License Registration
Get Validation Token

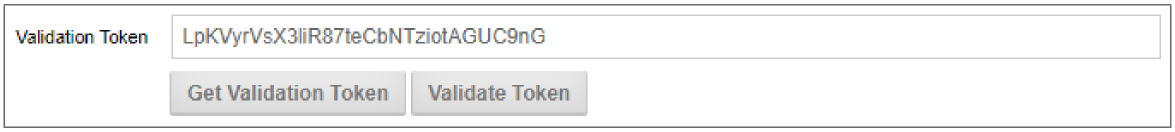
2. Click the Get Validation Token button on the pop-up web page, which will create new validation token for your license.


BP Logix Product Validation Page - Google Chrome
www2.bplogix.com/register.aspx?p1=v62svrHq8KOq8KLq9PKvtaY%3d&p2=pPLw
License Registration
Get Validation Token

Validation Token:
Sc1B33sHIM4VqqZ728dLbOGrHFjxIrEL

Copy and paste the validation from this text box into the Validation Token field on your server.

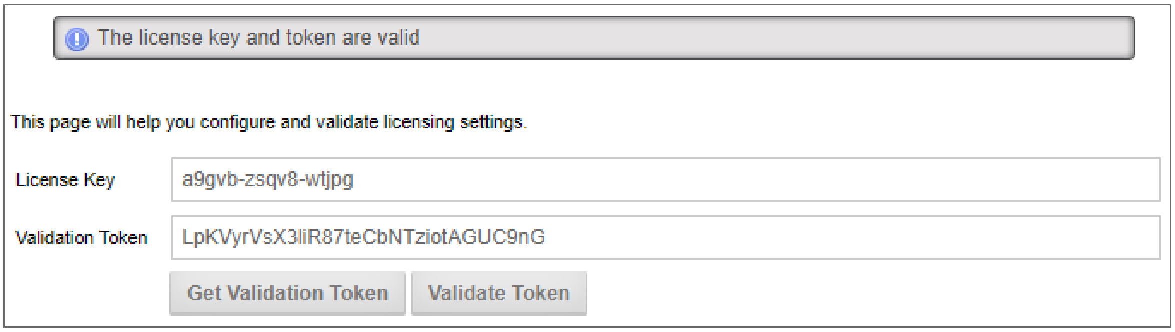
3. Copy the new validation token from the Pop-up web page, and paste it into the Validation Token field on the Licensing page. (You can now close the pop-up page.)



Validation Token LpKVyrVsX3liR87teCbNTziotAGUC9nG

4. Click the Validate Token button to validate the new license token. When you do, a status message will appear letting you know that the license and token

are valid.



The license key and token are valid

This page will help you configure and validate licensing settings.

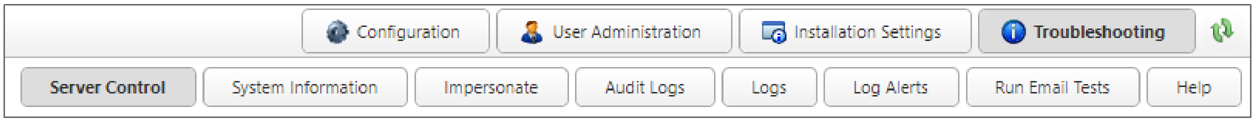
License Key: a9gvb-zsqv8-wtjpg

Validation Token: LpKVyrVsX3liR87teCbNTziotAGUC9nG

Your Process Director license has now been properly re-registered.

Troubleshooting

The Troubleshooting section contains the various pages needed for troubleshooting issues with Process Director. This section provides you with an easier way to troubleshoot issues with the server and processes. The logs can be read here without going to the logs folder, and can be submitted to technical support with a single button click.



The section also provides basic information about your Process Director installation, including its name, Interface URL, Server Version, Install Path, License Description, Server IP Address, and Logging Level.

Troubleshooting Pages

The Troubleshooting section's pages can be accessed via Table of Contents displayed on the upper right section of this page, or by using one of the links below:

Server Control: A list of links that invoke various server actions.

System Information: Provides a display of relevant server statistics.

Live Stats: Displays current performance statics on a continuing basis.

Impersonate: Enables you to impersonate other users.

Audit Logs: Enables access to the Audit logs saved in the Process Director Database, when this feature is configured for appropriately licensed installations.

Logs: Enables access to the system logs.

Log Alerts**:** Enables you to set alerts for specific events that might occur in the log files.

Run Email Tests: Enables sending test emails from the system.

Help: From the Troubleshooting section, clicking the Help button will open a new browser tab that displays the documentation web site for Process Director at https://doc.bplogix.com. There is no need for further documentation about this link.

Server Control

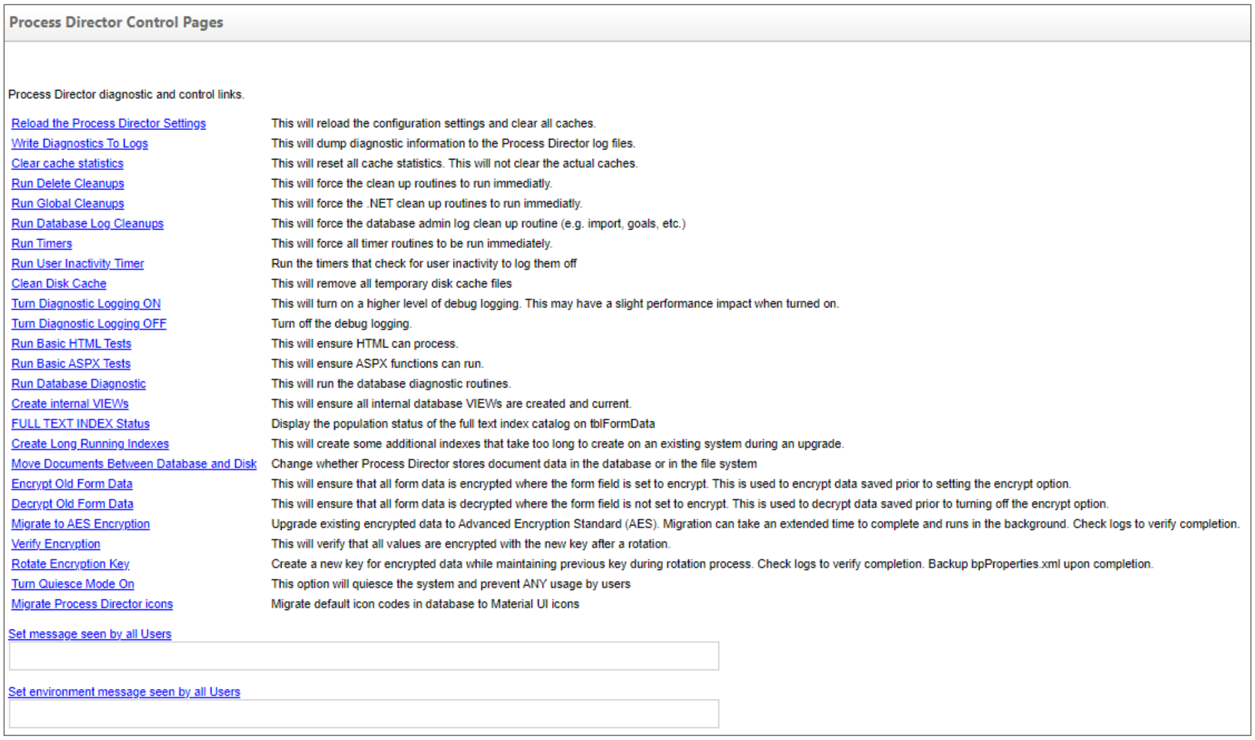
The Server Control page enables you to run various tests and cleanups to ensure that Process Director is running properly. Most of the server control items are self-explanatory, but a few require a bit more elaboration.

You can set a message that will be seen by all users when they log into Process Director. You can choose not to send a message by leaving the text field blank and clicking Set message seen by all Users.

The Turn Quiesce Mode On link will disable Process Director for end users, but not administrators. Quiesce mode enables administrators to make changes to the Content List, import applications, and do other administrative tasks, while preventing non-administrative users from accessing Forms or other objects. This function is useful for making administrative changes that might disrupt users. When turning Quiesce Mode on, you can also provide a message using the Set message seen by all Users link to notify them that some administrative activity is in progress, and their access to the system is temporarily suspended.

For Process Director v5.45 and higher, an input field is displayed when clicking Set environment message seen by all Users. This input field enables administrators to specify a message to be displayed to inform users if the system on which they're working is a Development, Staging, or Production system. The visual presentation of this message is also customizable, as described in the UI Customization topic.

For Process Director v6.1.0 and higher, a new control link, Migrate Process Director icons, will update any existing default object icons used in previous versions of the product to the most recent default icons.



Process Director Control Pages

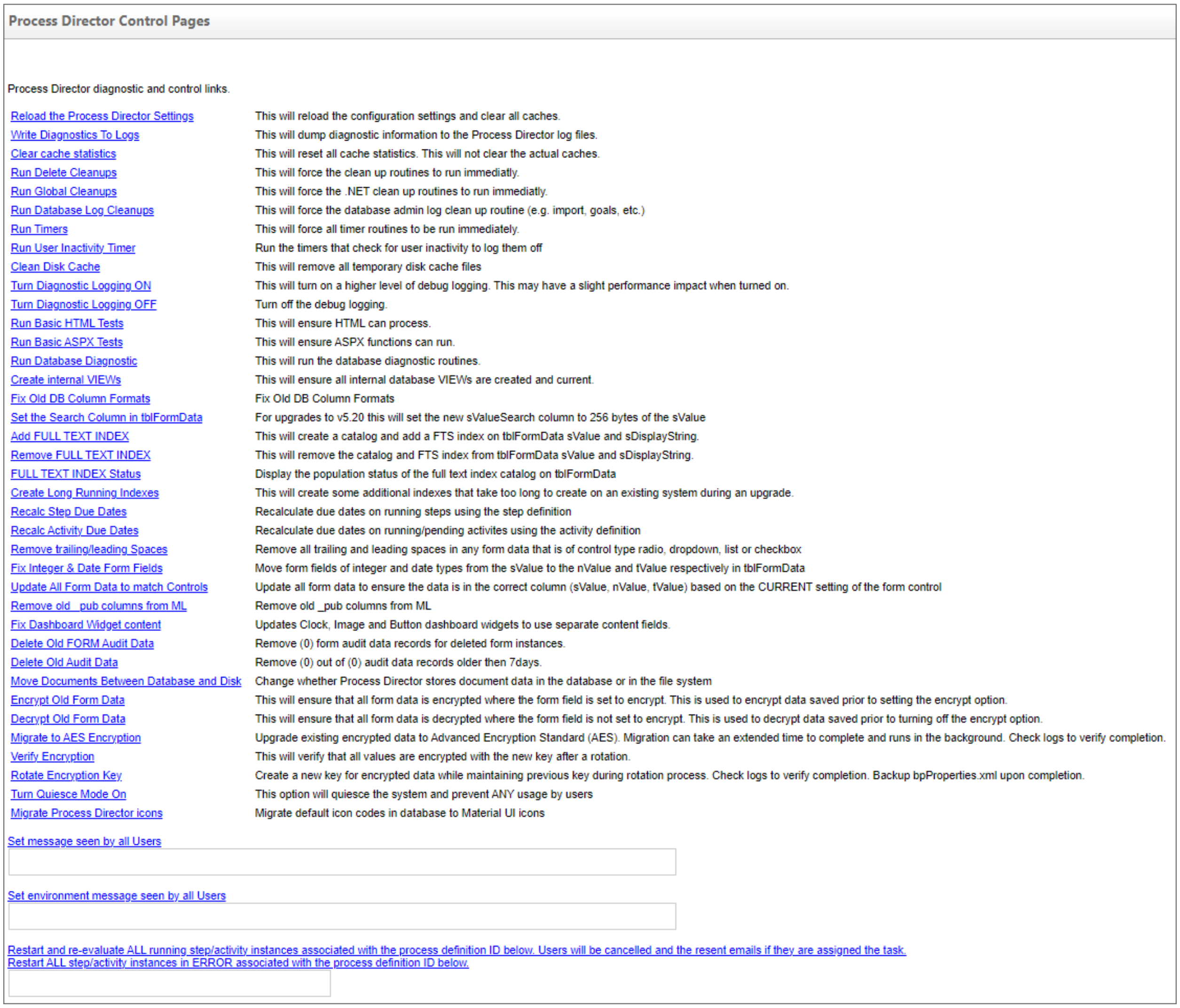
Process Director diagnostic and control links.

Reload the Process Director Settings	This will reload the configuration settings and clear all caches.
Write Diagnostics To Logs	This will dump diagnostic information to the Process Director log files.
Clear cache statistics	This will reset all cache statistics. This will not clear the actual caches.
Run Delete Cleanups	This will force the clean up routines to run immediatly.
Run Global Cleanups	This will force the .NET clean up routines to run immediatly.
Run Database Log Cleanups	This will force the database admin log clean up routine (e.g. import, goals, etc.)
Run Timers	This will force all timer routines to be run immediately.
Run User Inactivity Timer	Run the timers that check for user inactivity to log them off
Clean Disk Cache	This will remove all temporary disk cache files
Turn Diagnostic Logging ON	This will turn on a higher level of debug logging. This may have a slight performance impact when turned on.
Turn Diagnostic Logging OFF	Turn off the debug logging.
Run Basic HTML Tests	This will ensure HTML can process.
Run Basic ASPX Tests	This will ensure ASPX functions can run.
Run Database Diagnostic	This will run the database diagnostic routines.
Create internal VIEWs	This will ensure all internal database VIEWs are created and current.
FULL TEXT INDEX Status	Display the population status of the full text index catalog on tblFormData
Create Long Running Indexes	This will create some additional indexes that take too long to create on an existing system during an upgrade.
Move Documents Between Database and Disk	Change whether Process Director stores document data in the database or in the file system
Encrypt Old Form Data	This will ensure that all form data is encrypted where the form field is set to encrypt. This is used to encrypt data saved prior to setting the encrypt option.
Decrypt Old Form Data	This will ensure that all form data is decrypted where the form field is not set to encrypt. This is used to decrypt data saved prior to turning off the encrypt option.
Migrate to AES Encryption	Upgrade existing encrypted data to Advanced Encryption Standard (AES). Migration can take an extended time to complete and runs in the background. Check logs to verify completion.
Verify Encryption	This will verify that all values are encrypted with the new key after a rotation.
Rotate Encryption Key	Create a new key for encrypted data while maintaining previous key during rotation process. Check logs to verify completion. Backup bpProperties.xml upon completion.
Turn Quiesce Mode On	This option will quiesce the system and prevent ANY usage by users
Migrate Process Director icons	Migrate default icon codes in database to Material UI icons

Set message seen by all Users

Set environment message seen by all Users

Additional troubleshooting options are available on this tab when in Debug Mode.



Process Director Control Pages

Process Director diagnostic and control links.

Reload the Process Director Settings	This will reload the configuration settings and clear all caches.
Write Diagnostics To Logs	This will dump diagnostic information to the Process Director log files.
Clear cache statistics	This will reset all cache statistics. This will not clear the actual caches.
Run Delete Cleanups	This will force the clean up routines to run immediatly.
Run Global Cleanups	This will force the .NET clean up routines to run immediatly.
Run Database Log Cleanups	This will force the database admin log clean up routine (e.g. import, goals, etc.)
Run Timers	This will force all timer routines to be run immediately.
Run User Inactivity Timer	Run the timers that check for user inactivity to log them off
Clean Disk Cache	This will remove all temporary disk cache files
Turn Diagnostic Logging ON	This will turn on a higher level of debug logging. This may have a slight performance impact when turned on.
Turn Diagnostic Logging OFF	Turn off the debug logging.
Run Basic HTML Tests	This will ensure HTML can process.
Run Basic ASPX Tests	This will ensure ASPX functions can run.
Run Database Diagnostic	This will run the database diagnostic routines.
Create internal VIEWs	This will ensure all internal database VIEWs are created and current.
Fix Old DB Column Formats	Fix Old DB Column Formats
Set the Search Column in tblFormData	For upgrades to v5.20 this will set the new sValueSearch column to 256 bytes of the sValue
Add FULL TEXT INDEX	This will create a catalog and add a FTS index on tblFormData sValue and sDisplayString.
Remove FULL TEXT INDEX	This will remove the catalog and FTS index from tblFormData sValue and sDisplayString.
FULL TEXT INDEX Status	Display the population status of the full text index catalog on tblFormData
Create Long Running Indexes	This will create some additional indexes that take too long to create on an existing system during an upgrade.
Recalc Step Due Dates	Recalculate due dates on running steps using the step definition
Recalc Activity Due Dates	Recalculate due dates on running/pending activites using the activity definition
Remove trailing/leading Spaces	Remove all trailing and leading spaces in any form data that is of control type radio, dropdown, list or checkbox
Fix Integer & Date Form Fields	Move form fields of integer and date types from the sValue to the nValue and tValue respectively in tblFormData
Update All Form Data to match Controls	Update all form data to ensure the data is in the correct column (sValue, nValue, tValue) based on the CURRENT setting of the form control
Remove old _pub columns from ML	Remove old _pub columns from ML
Fix Dashboard Widget content	Updates Clock, Image and Button dashboard widgets to use separate content fields.
Delete Old FORM Audit Data	Remove (0) form audit data records for deleted form instances.
Delete Old Audit Data	Remove (0) out of (0) audit data records older then 7days.
Move Documents Between Database and Disk	Change whether Process Director stores document data in the database or in the file system
Encrypt Old Form Data	This will ensure that all form data is encrypted where the form field is set to encrypt. This is used to encrypt data saved prior to setting the encrypt option.
Decrypt Old Form Data	This will ensure that all form data is decrypted where the form field is not set to encrypt. This is used to decrypt data saved prior to turning off the encrypt option.
Migrate to AES Encryption	Upgrade existing encrypted data to Advanced Encryption Standard (AES). Migration can take an extended time to complete and runs in the background. Check logs to verify completion.
Verify Encryption	This will verify that all values are encrypted with the new key after a rotation.
Rotate Encryption Key	Create a new key for encrypted data while maintaining previous key during rotation process. Check logs to verify completion. Backup bpProperties.xml upon completion.
Turn Quiesce Mode On	This option will quiesce the system and prevent ANY usage by users
Migrate Process Director icons	Migrate default icon codes in database to Material UI icons

Set message seen by all Users

Set environment message seen by all Users

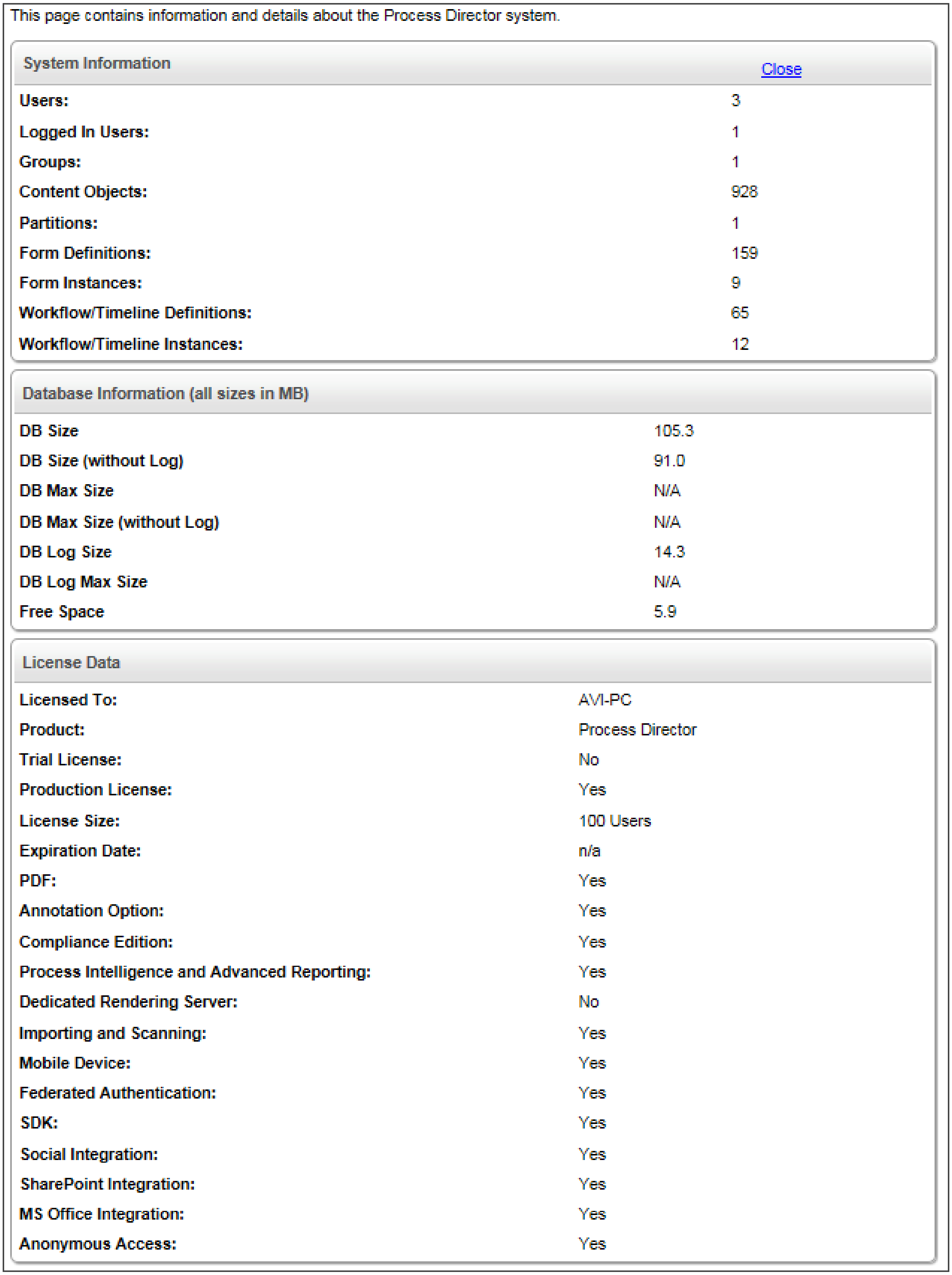
Restart and re-evaluate ALL running step/activity instances associated with the process definition ID below. Users will be cancelled and the resent emails if they are assigned the task.
Restart ALL step/activity instances in ERROR associated with the process definition ID below.

The additional debug mode operations all have explanatory text describing their usage as well.

For Process Director v6.1.500 and higher, the Set Message seen by all users or the Set environment message seen by all Users properties on the Server Control page of the IT Admin area will parse System Variables.

System Information

The System Information page displays information regarding the number of objects and users on this installation of Process Director, characteristics of the hard drive that Process Director is installed on, and licensing information.



This page contains information and details about the Process Director system.

System Information

Users:	3
Logged In Users:	1
Groups:	1
Content Objects:	928
Partitions:	1
Form Definitions:	159
Form Instances:	9
Workflow/Timeline Definitions:	65
Workflow/Timeline Instances:	12

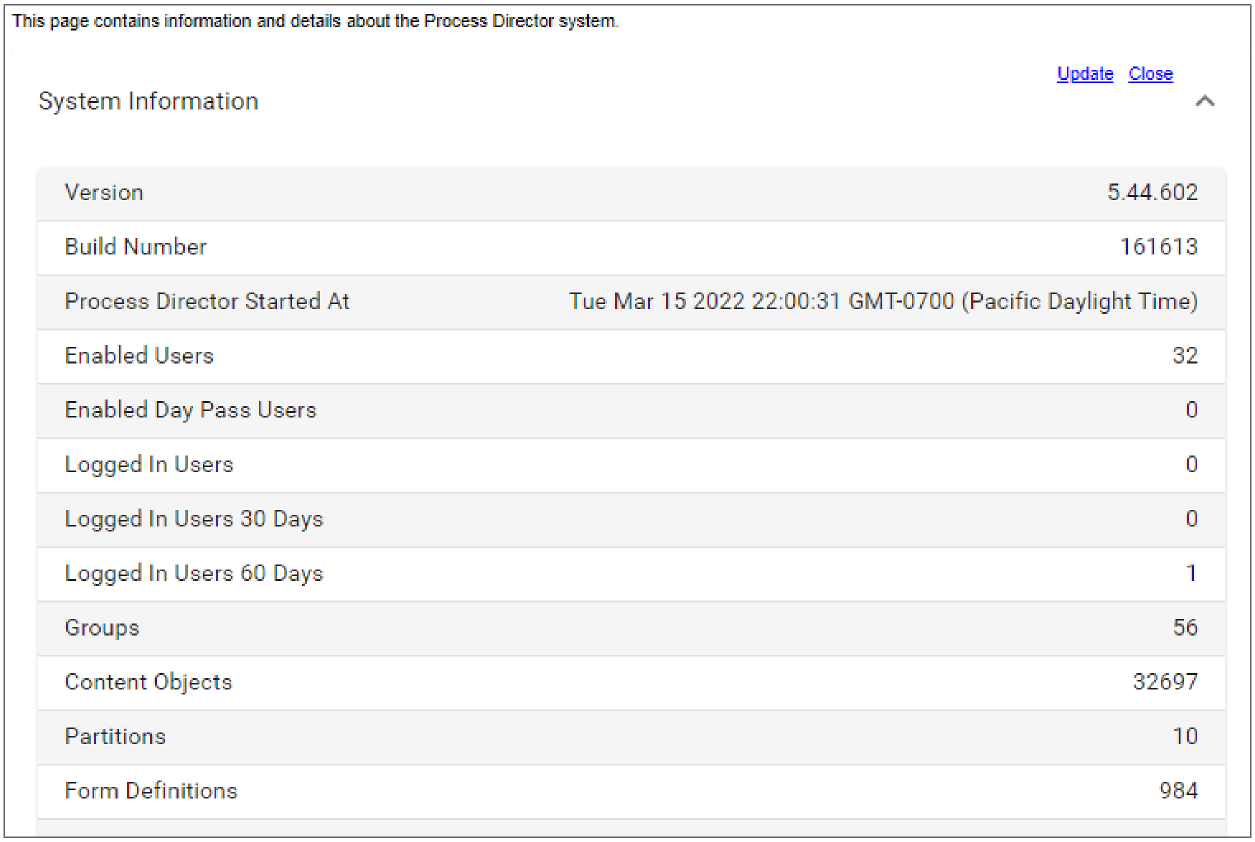
Database Information (all sizes in MB)

DB Size	105.3
DB Size (without Log)	91.0
DB Max Size	N/A
DB Max Size (without Log)	N/A
DB Log Size	14.3
DB Log Max Size	N/A
Free Space	5.9

License Data

Licensed To:	AVI-PC
Product:	Process Director
Trial License:	No
Production License:	Yes
License Size:	100 Users
Expiration Date:	n/a
PDF:	Yes
Annotation Option:	Yes
Compliance Edition:	Yes
Process Intelligence and Advanced Reporting:	Yes
Dedicated Rendering Server:	No
Importing and Scanning:	Yes
Mobile Device:	Yes
Federated Authentication:	Yes
SDK:	Yes
Social Integration:	Yes
SharePoint Integration:	Yes
MS Office Integration:	Yes
Anonymous Access:	Yes

Process Director v5.44.602 and higher also has an updated version of this page with a more modern look.



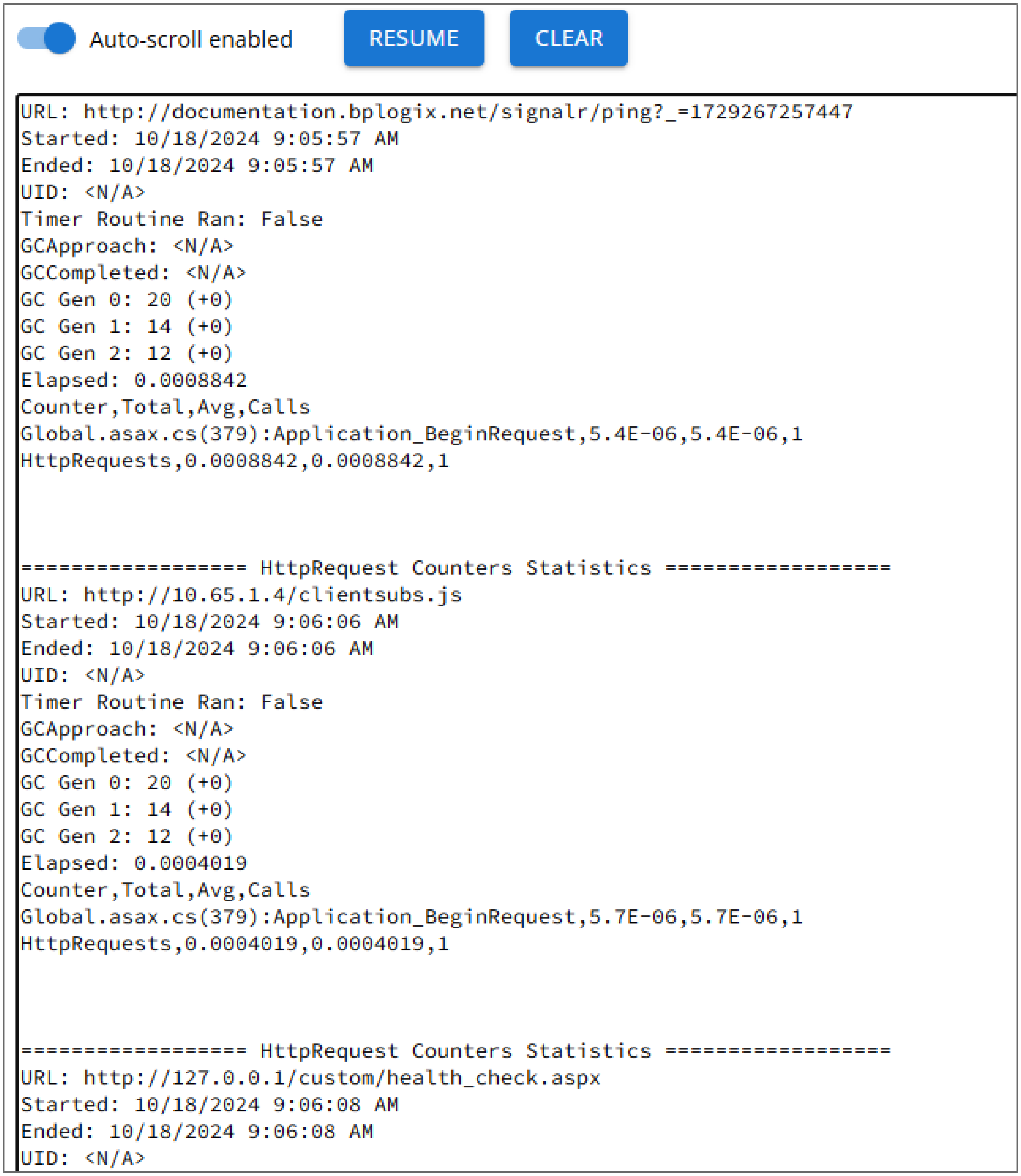
This page contains information and details about the Process Director system.

System Information

Version	5.44.602
Build Number	161613
Process Director Started At	Tue Mar 15 2022 22:00:31 GMT-0700 (Pacific Daylight Time)
Enabled Users	32
Enabled Day Pass Users	0
Logged In Users	0
Logged In Users 30 Days	0
Logged In Users 60 Days	1
Groups	56
Content Objects	32697
Partitions	10
Form Definitions	984

Live Stats

For Process Director v6.1.300 and higher, the Troubleshooting section of IT Admin contains a Live Stats page that continually refreshes to display current performance statistics for the system.



```
URL: http://documentation.bplogix.net/signalr/ping?_=1729267257447
Started: 10/18/2024 9:05:57 AM
Ended: 10/18/2024 9:05:57 AM
UID: <N/A>
Timer Routine Ran: False
GCApproach: <N/A>
GCCompleted: <N/A>
GC Gen 0: 20 (+0)
GC Gen 1: 14 (+0)
GC Gen 2: 12 (+0)
Elapsed: 0.0008842
Counter,Total,Avg,Calls
Global.asax.cs(379):Application_BeginRequest,5.4E-06,5.4E-06,1
HttpRequests,0.0008842,0.0008842,1



================== HttpRequest Counters Statistics ==================
URL: http://10.65.1.4/clientsubs.js
Started: 10/18/2024 9:06:06 AM
Ended: 10/18/2024 9:06:06 AM
UID: <N/A>
Timer Routine Ran: False
GCApproach: <N/A>
GCCompleted: <N/A>
GC Gen 0: 20 (+0)
GC Gen 1: 14 (+0)
GC Gen 2: 12 (+0)
Elapsed: 0.0004019
Counter,Total,Avg,Calls
Global.asax.cs(379):Application_BeginRequest,5.7E-06,5.7E-06,1
HttpRequests,0.0004019,0.0004019,1



================== HttpRequest Counters Statistics ==================
URL: http://127.0.0.1/custom/health_check.aspx
Started: 10/18/2024 9:06:08 AM
Ended: 10/18/2024 9:06:08 AM
UID: <N/A>
```

There are some health check system events that run on a recurring basis to poll various performance counters. The results of this polling are displayed in a continuous scroll on this page. The three primary health check polls are:

- A ping to the SignalR service,
- A `clientsubs` JavaScript poll, and,
- A custom health check page, health_check.aspx.

Examples of results from all three of these are shown in the example screenshot above. Each statistics block displays the length of time it takes for various processes to complete on the system. The time for completion is given in seconds. Ideally, completion should take only a decimal fraction of a second, e.g.:

```
Elapsed: 0.0008842
```

Often, the fractions are presented in scientific notation, e.g.:

```
Global.asax.cs(379):Application_BeginRequest,5.4E-06
```

In the example above, the elapsed time would be 0.0000054 seconds.

At the top of the Live Stats page, there are three controls to manipulate the display of the performance statistics.

Auto-Scroll Enabled is a switch control that's turned on by default. This setting enables the page to continually scroll as new statistics are reported. Because the reporting occurs frequently, you may wish to turn this switch off to stop the automatic scrolling, in order to concentrate on a specific section of the stats, without having the continuously scroll out of view. Turning this switch off does not stop the reporting from being presented on the page, it merely stops the automatic scrolling when new results are reported.

A Pause button, when clicked, will pause the reporting completely. When paused, this button will be replaced by a Resume button that can be clicked to resume the statistics reporting.

A Clear button erases all of the current statistics from the screen, and starts over with a blank page.

When this page is first opened, the reporting window will have no data initially. Statistics posting does not begin until the page is opened. It may take a few seconds for the first polling results are displayed.

When reporting performance issues via Tech Support, you may be asked to open this page, let it run for a few minutes, then copy and paste the results into a text file, which you can then attach to the support ticket.

Troubleshooting Pages

The Troubleshooting section's pages can be accessed via Table of Contents displayed on the upper right section of this page, or by using one of the links below:

Server Control: A list of links that invoke various server actions.

System Information: Provides a display of relevant server statistics.

Impersonate: Enables you to impersonate other users.

Audit Logs: Enables access to the Audit logs saved in the Process Director Database, when this feature is configured for appropriately licensed installations.

Logs: Enables access to the system logs.

Log Alerts**:** Enables you to set alerts for specific events that might occur in the log files.

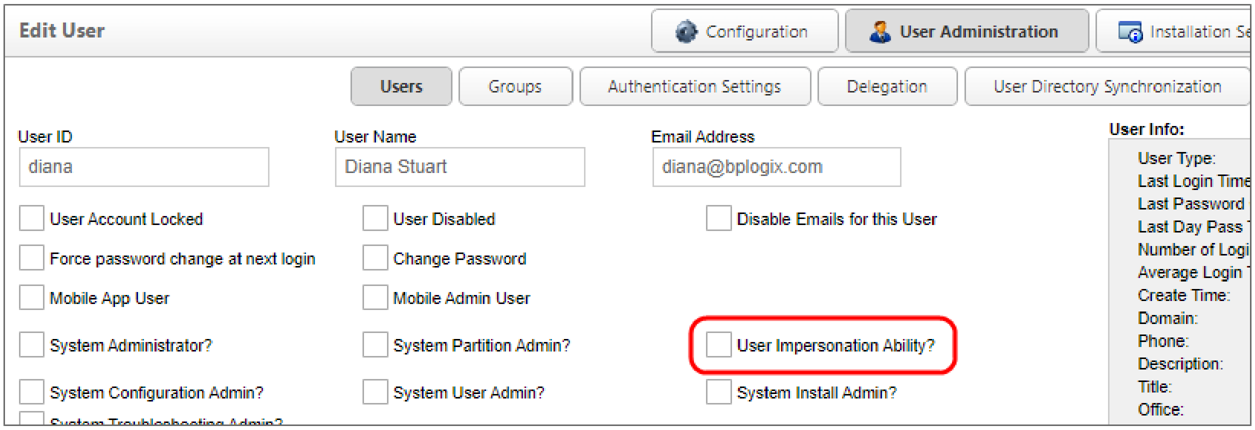
Run Email Tests: Enables sending test emails from the system.

Help: From the Troubleshooting section, clicking the Help button will open a new browser tab that displays the documentation web site for Process Director at https://doc.bplogix.com. There is no need for further documentation about this link.

User Impersonation

For Cloud installations, or on-premise installations that use the Compliance Edition or Subscription licenses, Process Director allows some users to impersonate other users. Impersonation allows a user to act as another user, seeing and completing the tasks to which he is assigned, leaving his name on routing slips when doing so, etc. Impersonating a user is almost exactly the same as being logged in as that user, except that the impersonation will appear in the audit log. This feature is useful to assist users with problems they are having, or to debug problems you can't replicate with another user.

To grant a user the ability to impersonate other users, navigate to the User Administration section of the IT Admin area, access the Users page, and click on the user whom you'd like to grant the ability. When the user's profile opens, you'll see a checkbox that says User Impersonation Ability?. Check the box.



Edit User

User ID: diana

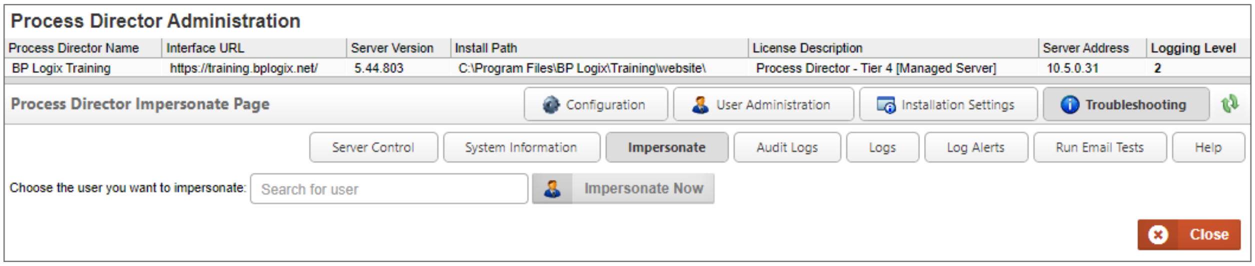
User Name: Diana Stuart

Email Address: diana@bplogix.com

□ User Account Locked
□ User Disabled
□ Disable Emails for this User
□ Force password change at next login
□ Change Password
□ Mobile App User
□ Mobile Admin User
□ System Administrator?
□ System Partition Admin?
□ User Impersonation Ability?
□ System Configuration Admin?
□ System User Admin?
□ System Install Admin?
□ System Troubleshooting Admin?

User Info:
User Type:
Last Login Time
Last Password
Last Day Pass
Number of Logi
Average Login
Create Time:
Domain:
Phone:
Description:
Title:
Office:

To impersonate another user, go to the Impersonate page of the Troubleshooting section. There you'll see a Choose the user you want to impersonate user picker. Select the user whom you'd like to impersonate this user, and click the Impersonate User button.



Process Director Administration

Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
BP Logix Training	https://training.bplogix.net/	5.44.803	C:\Program Files\BP Logix\Training\website\	Process Director - Tier 4 [Managed Server]	10.5.0.31	2

Process Director Impersonate Page

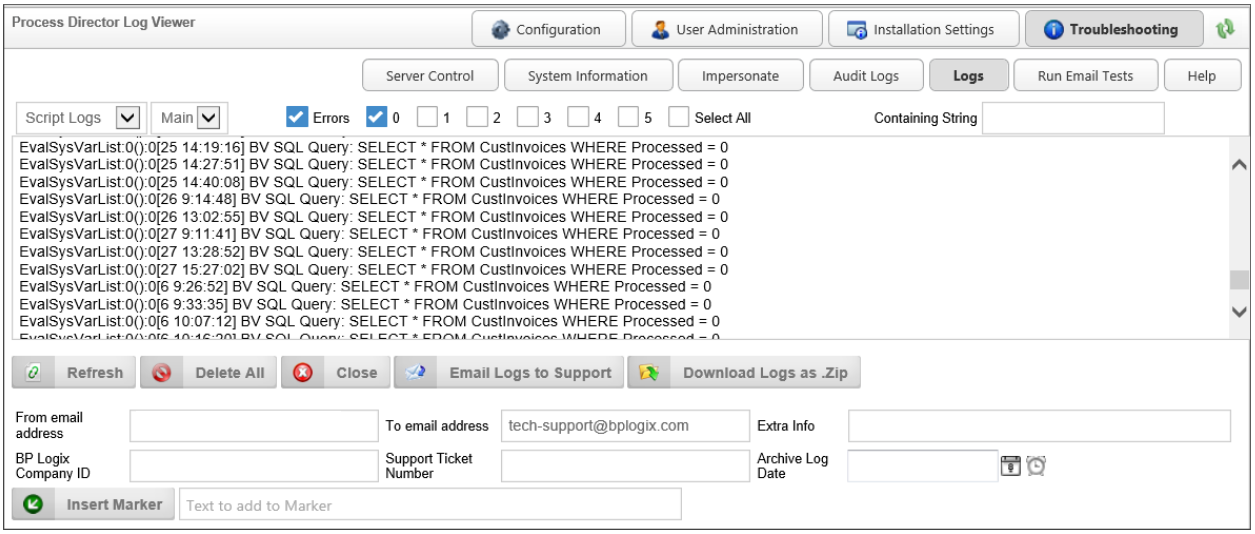
Choose the user you want to impersonate: Search for user

When impersonating another user, you'll use your own credentials to complete tasks that require reauthentication, so you don't need to know the impersonated user's password to complete tasks.

> **For Process Director v5.13 and higher, a user can't impersonate anyone who has System Administrator permissions, unless the user also has System Administrator permissions.**

Logs

For Cloud installations, or On-Premise installations that use the Compliance Option, Process Director provides a number of logging functions, all of which are available through the Logs page of the IT Admin area's Troubleshooting section. Once you've navigated to the Troubleshooting section, you can open the Logs page by clicking the Logs button located in the upper right portion of the screen.



Script Logs | Main | ☑ Errors ☑ 0 □ 1 □ 2 □ 3 □ 4 □ 5 □ Select All | Containing String

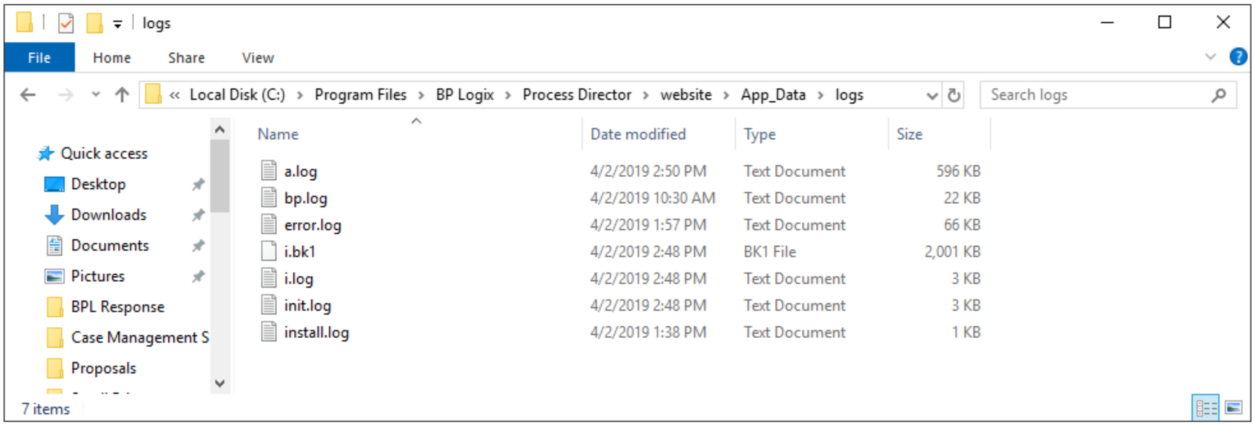
```
EvalSysVarList:0():0[25 14:19:16] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
EvalSysVarList:0():0[25 14:27:51] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
EvalSysVarList:0():0[25 14:40:08] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
EvalSysVarList:0():0[26 9:14:48] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
EvalSysVarList:0():0[26 13:02:55] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
EvalSysVarList:0():0[27 9:11:41] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
EvalSysVarList:0():0[27 13:28:52] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
EvalSysVarList:0():0[27 15:27:02] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
EvalSysVarList:0():0[6 9:26:52] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
EvalSysVarList:0():0[6 9:33:35] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
EvalSysVarList:0():0[6 10:07:12] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
EvalSysVarList:0():0[6 10:16:20] BV SQL Query: SELECT * FROM CustInvoices WHERE Processed = 0
```

From email address | To email address: tech-support@bplogix.com | Extra Info

BP Logix Company ID | Support Ticket Number | Archive Log Date

Text to add to Marker

The most recent log files are available for view in this page's log reader. All of the log files are also available from within your Process Director installation in the `%InstallationDirectory%\website\App_Data\logs` folder.



« Local Disk (C:) › Program Files › BP Logix › Process Director › website › App_Data › logs

Search logs

Name	Date modified	Type	Size
a.log	4/2/2019 2:50 PM	Text Document	596 KB
bp.log	4/2/2019 10:30 AM	Text Document	22 KB
error.log	4/2/2019 1:57 PM	Text Document	66 KB
i.bk1	4/2/2019 2:48 PM	BK1 File	2,001 KB
i.log	4/2/2019 2:48 PM	Text Document	3 KB
init.log	4/2/2019 2:48 PM	Text Document	3 KB
install.log	4/2/2019 1:38 PM	Text Document	1 KB

The log files are saved in a comma-separated text format. If you change the file extension of the logs from ".log" or ".bkX" to ".csv", they can generally be opened in Excel for easier reading than opening the text log file in Notepad.

Available Logs

Process Director makes the following logs available:

LOG FILE	DESCRIPTION
Script Logs	Records information from scripts when using the bp.logs methods.
Internal logs	Records internal system status information.
Init Logs	Records when various components of functions are initiated.
Audit Logs	Records changes made to data or processes.
Email Logs	Records data about email messages sent from Process Director. (For users of the Compliance edition only.)

You can switch between each of these logs by using the dropdown control located above the Log Viewer, at the far left of the screen. To the immediate right of the log type dropdown is a log file dropdown that gives you access to the current log ("Main") and the four most recent backups. Process Director sets a default log file size of 2MB, so that, when the main log reaches 2MB, it is saved as backup 1, and a new empty Main log is started. Process Director saves the old backup 1 log as backup 2, and so on as the changes ripple down through the log backup numbers.

To the right of the log file dropdown, you'll see check boxes that you can use to select if you wish to see logged errors only, and which logging level you'd like to see. Logging is documented at six different levels, Level 0 through Level 5. Level 0 is the default level for logging. Each logging level creates logs at an increasingly detailed scale, with Level 5 being the most detailed level, and level 0 being the least detailed. Nearly all debugging you'll need to do on a regular basis can be done using Level 0 or Level 1 logging. On occasion, system problems may require more detailed logging, but you should be aware that higher levels of logging detail can impact system performance. Using higher levels of logging is usually done in conjunction with assistance from BP Logix, and isn't usually necessary otherwise.

Additionally, for users of the Compliance Edition, Cloud, or Subscription licenses, some audit logging is also sent to the Windows Event Log. From the Windows Event Log Viewer, you can configure automated actions, such as email notifications, to occur when certain events are logged. For information on this functionality, and how to edit the events sent to the Windows Event log, please see the Audit Logging Variables section of the Developer's Guide.

For Process Director v6.00 and higher, the date/time formats displayed for log events have been reformatted to use common date/time formats for greater readability.

Log Events

Some standard events will show up in the log files, based on actions taken by either Process Director users, or by Process Director as processes move through their life cycle. The table below enumerates and describes these standard log events.

LOG EVENT	APPEARS IN A LOG WHEN
AddAppEvent	A new application event was added to a Form or Process Timeline definition.
AddGroupToPartition	A user group was added to a partition to enable access to that partition by members of the group.
AddUserToGgroup	A user is added into a group.
AddUserToPartition	A user was added to a partition to enable access to that partition.
AdminPageAccess	A user directly accesses an admin page from the installation server.
AdminPageUpdate	A change was made to an IT Admin page's data.
AdminReplaceUser	An administrator uses the "replace user" function.
AnonymousAccess	An anonymous user accessed the system.
AttachmentAdded	Any time an attachment is added to a Form instance (v5.34 and higher).
AttachmentRemoved	Any time an attachment is removed from a Form instance (v5.34 and higher).
AuthenticateFailed	A user types the wrong password when

LOG EVENT	APPEARS IN A LOG WHEN
	attempting to log in, or to access to admin page without privileges
CancelActivity	A Timeline Activity is canceled.
CancelDocumentCheckout	A user canceled an attempt to check out a document or document attachment.
CancelStep	A Workflow Step is canceled, e.g. an administrator right clicking on a step and clicking "Cancel".
CaseDataChange	The data stored in a Case instance was changed.
CaseModeEntered	A user opened a case instance in case context.
CheckoutDocument	A document or document attachment was checked out, usually for editing.
CreateGroup	A group is created (Group Admin).
CreateObject	A Content List object of is created or an object is created from an object instance.
CreateUser	A user is created (User Admin).
DelegateOff	A user ends delegation.
DelegateOn	A user sets delegation to other users.
DeleteAppEvent	An application event was deleted by a user.
DeleteGroup	A group is deleted (Group Admin).
DeleteObject	A Content List object of is deleted or an object is deleted from an object instance.
DeleteUser	A user is deleted (User Admin).
DownloadDocument	A user downloads documents from application.
ExportObjects	When an XML file is exported.
FormDataChange	When a Form is filled out by a user. This is used when form field auditing is active on a

LOG EVENT	APPEARS IN A LOG WHEN
	form instance. The log entry shows the changes to all the form fields, including the old values, the new values, and who changed the Form.
ImpersonateOff	When impersonate is off.
ImpersonateOn	When impersonate is on (Someone uses impersonate function).
ImportObjects	When an XML file is imported.
JumpToStep	A task is moved to non-connected task with a Jump to Step Custom Task.
Login	A user logs in
Logoff	A user logs off
MoveObject	A Content List object or an object from an object instance is moved.
NotSet	Not categorized into the following
ObjectLock	A Content List object was automatically locked for editing.
ObjectUnlock	A Content List object was automatically unlocked from editing.
ObjectUnlockOther	A Content List object was manually unlocked
PasswordChange	A user changes the password.
PermissionAdded	A permission is added to a user (User Admin).
PermissionDeniedAdmin	A user attempts to view admin pages to which the user doesn't have permissions.
PermissionDeniedDelete	A user attempts to delete object to which the user doesn't have permissions.
PermissionDeniedExecute	A user attempts to run an object to which the user doesn't have permission.
PermissionDeniedModify	A user attempts to modify an object to which the user doesn't have permission.

LOG EVENT	APPEARS IN A LOG WHEN
PermissionDeniedView	A user attempts to view object to which the user doesn't have permission.
PermissionGiven	An application elevates a user's permissions.
PermissionRemoved	A permission is removed from a user (User Admin).
PermissionReplicated	This occurs when the user clicks on the "Replicate Permissions to Child Objects" button.
PermissionUpdated	A user edits and updates an existing permission record.
ReInit	The Process Director installation was reinitialized, usually from a suspended state after period of inactivity.
RemoveGroupFromPartition	A user group was removed from a partition.
RemoveObjectFromParent	Any content object is removed from a parent, e.g. removing an attachment from a process.
RemoveUserFromGroup	A user is removed from a group.
RemoveUserFromPartition	A user was removed from a partition.
RestartActivity	A Timeline Activity is restarted.
RestartTimeline	A Process Timeline instance is restarted.
RestartWorkflow	A Workflow instance is restarted.
RollbackActivity	A Timeline Activity is rolled back.
RollbackDocument	An edited document or document attachment was rolled back to an earlier version of the document.
Signature	A user enters data into an eSign signature control on a Form.
StopStep	A Workflow Step is stopped without completing it.
StopWorkflow	A Workflow instance is stopped.

LOG EVENT	APPEARS IN A LOG WHEN
SyncEnd	Sync is finished.
SyncStart	Sync is run/started.
TaskCompleted	A process task is completed by a user.
TaskReassigned	A user is reassigned to a process task.
TaskRemoved	A running task is removed from a running process.
UpdateAppEvent	An application event was changed by a user.
UpdateDocumentProps	A user updated the properties of a document or document attachment.
UpdateObject	A Content List or object instance object is updated.
UpdateUser	A user profile is updated (User Admin).
UserDisabled	A user is disabled (User Admin/ Setting).
UserEnabled	A disabled user is enabled.
UserLockedOut	A user was locked out of the system, usually as the result of authentication failures.
ViewCaseData	A user viewed the data for a Case instance.
ViewForm	Any time a user opens a form instance. The flag fAuditFormViews must be enabled, i.e., set to "True" in the vars file, for this to appear. This may add strongly to the servers load when in use.
ViewFormData	When someone accesses form data other than through the normal viewing of a form instance (e.g. through SDK calls).
WebService	A web service is run (Process Director access to Web Service).

Searching the Logs

At the top of the Log Viewer, to the right of the logging levels check boxes, you'll see a text box labeled Containing String. If you enter text into this text box, then hit the [ENTER] key, Process Director will search the current log for log entries that match the text you have typed into the text box.

Emailing Logs

On occasion, you may run into issues that you requires assistance from BP Logix to debug. In those cases, a technical support representative may ask you to attach your log files to your technical support ticket. In this case, there is a button located below the log reader that is labeled Email Logs. Below this button, you'll see text boxes into which you can enter email addresses to which to send the logs from your Process Director installation. In addition, there is a text box for you to enter other information you'd like to appear in the text of your email. If these are filled out correctly, you can click the Email Logs button to send the logs in a zipped file.

Enter your email address, and send the logs to yourself. When you receive the email, download the zipped log files to your computer, then attach the zipped log files to your support ticket.

Sending Logs to Support

If you have an active support ticket, you can automatically attach the logs to your tech Support ticket by entering your BP Logix Company ID and the Support Ticket number into the fields provided, then clicking the Email Logs to Support button.

Additionally, you can send specific archive logs by selecting a date from the Archive Log Date control, which will attach the logs from 1 day before to 1 day after the specified date.

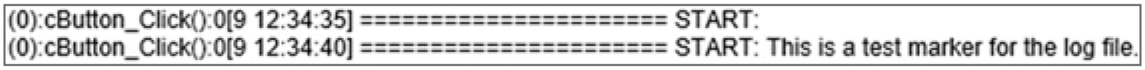
Downloading the log file

You can download the zipped log files for your own use and analysis by clicking the Download Logs as .Zip button.

Log Markers

At the bottom of the Log Viewer, you'll see an Insert Marker button. Clicking this button will insert a marker into the log file. You can fill in the text box next to the "Insert marker" button to include some custom text in the marker.

You may find it useful to insert a marker when dealing with logs that contain a lot of information, and which are updated frequently by Process Director. For instance, when testing a function, you might insert a marker with custom text before running the test. The marker makes it easier to return to the log and find where your test started.



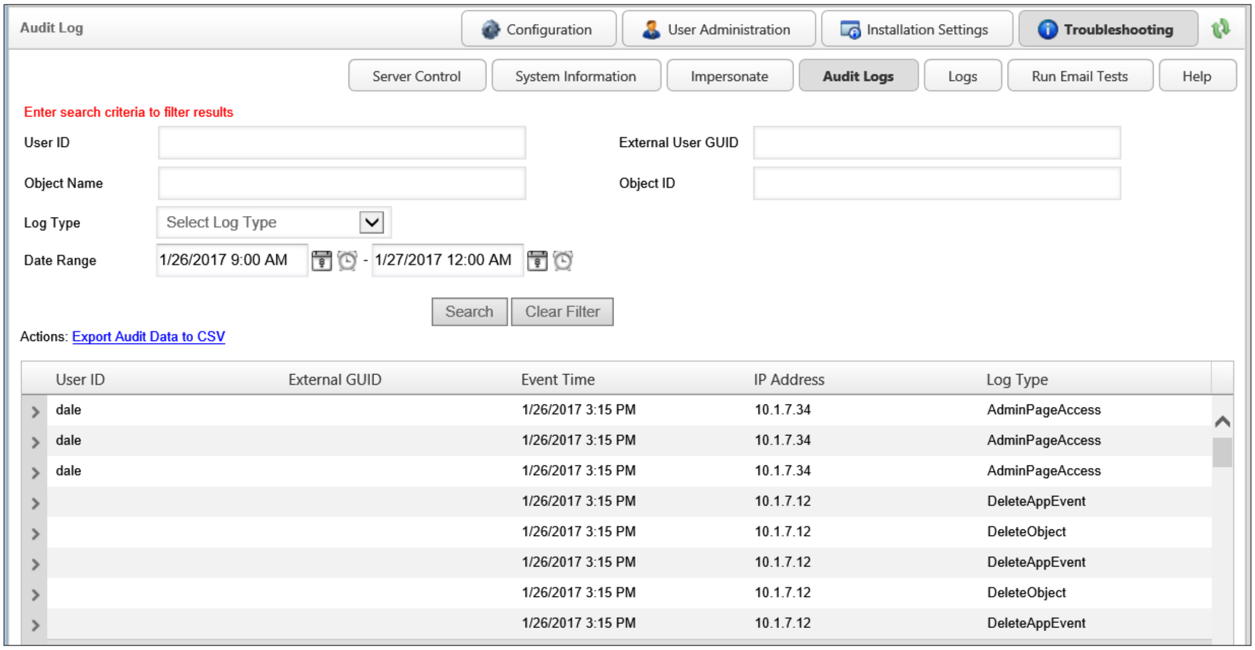
```
(0):cButton_Click():0[9 12:34:35] ====================== START:
(0):cButton_Click():0[9 12:34:40] ====================== START: This is a test marker for the log file.
```

The example above demonstrates two markers. The first marker is the default marker that is inserted in the log file when you click the Insert marker button. The second example is a marker where the following custom text has been inserted:

```
This is a test marker for the log file.
```

Audit Logs

In addition to storage in the file system, users of the Compliance edition—which includes cloud-based installations—can have audit logs written into the Process Director internal database for easier access to the logs to view, search, and export audit logs. This functionality is available from within the Troubleshooting section of the IT Admin area via the Audit Logs button.



Enter search criteria to filter results

User ID

External User GUID

Object Name

Object ID

Log Type: Select Log Type

Date Range: 1/26/2017 9:00 AM - 1/27/2017 12:00 AM

Actions: Export Audit Data to CSV

User ID	External GUID	Event Time	IP Address	Log Type
dale		1/26/2017 3:15 PM	10.1.7.34	AdminPageAccess
dale		1/26/2017 3:15 PM	10.1.7.34	AdminPageAccess
dale		1/26/2017 3:15 PM	10.1.7.34	AdminPageAccess
		1/26/2017 3:15 PM	10.1.7.12	DeleteAppEvent
		1/26/2017 3:15 PM	10.1.7.12	DeleteObject
		1/26/2017 3:15 PM	10.1.7.12	DeleteAppEvent
		1/26/2017 3:15 PM	10.1.7.12	DeleteObject
		1/26/2017 3:15 PM	10.1.7.12	DeleteAppEvent

The top portion of the Audit Logs page provides search fields to find the relevant portions of the log files stored in the database. Below the search fields is a link to export the search data to a CSV file. Exporting the data to CSV format enables users to open the exported data in Excel for further analysis, providing a much easier way to analyze audit logs than the text-based log files. The bottom portion of the screen displays the returned records from the database. Each returned row has an expansion icon (›) that users can click to expand the row to show log file details for that entry.

If you allow outside users who don't have Process Director user accounts, such as customers or suppliers, to have access to your processes via anonymous access, you can enable audit logging for anonymous users as well. To turn this feature on, you'll need to set the fAuditLogFileOnly variable to "false" in the Custom Variables file. You can limit the number of days log files are stored by setting the nAuditLogDays Custom Variable, to keep the audit table at a manageable size, as it grows quickly.

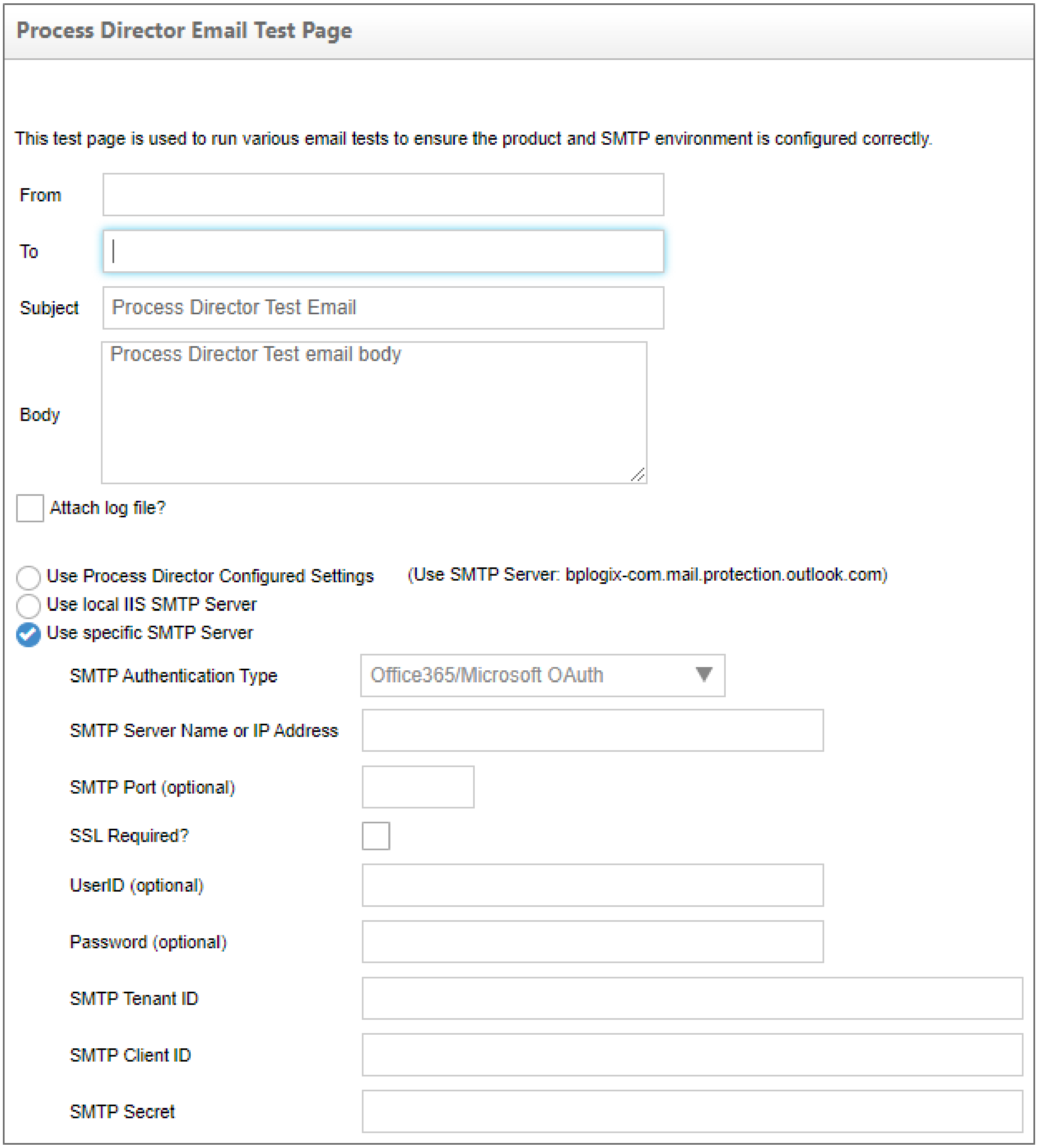
Run Email Tests

The Run Email Tests page enables you to configure a number of options for sending a test email. This page enables you to set up an email and have Process Director send it, testing Process Director’s ability to send emails. The email body and content can be configured, as well as the server from which the email is sent.

From the Troubleshooting section, you can navigate to the Run Email Tests page by clicking the Run Email Tests button.

This page is very important when troubleshooting email issues in Process Director. In general, if an email is successfully sent from this page, then you can be relatively certain that the email features of Process Director are operating correctly. If the tests are sent correctly, from this page, but you are still having email delivery issues, you may wish to check other possibilities, such as issues with your email server.

For Process Director v5.44.1103, the Run Email Tests page is configured to use Microsoft Modern Authentication by setting the configuration to Use Specific SMTP Server, the setting the SMTP Authentication Type property to "Office 365/Microsoft OAuth".



Process Director Email Test Page

This test page is used to run various email tests to ensure the product and SMTP environment is configured correctly.

From	
To	
Subject	Process Director Test Email
Body	Process Director Test email body

□ Attach log file?

○ Use Process Director Configured Settings (Use SMTP Server: bplogix-com.mail.protection.outlook.com)
○ Use local IIS SMTP Server
● Use specific SMTP Server

SMTP Authentication Type	Office365/Microsoft OAuth
SMTP Server Name or IP Address	
SMTP Port (optional)	
SSL Required?	□
UserID (optional)	
Password (optional)	
SMTP Tenant ID	
SMTP Client ID	
SMTP Secret	

There are several configurable properties you can set for each email test you wish to run.

From

The email address from which the email is sent.

To

The email address to which to send the test.

Subject

The Subject of the test email message. A simple default value is supplied, as illustrated in Figure 65.

Body

The Body of the test email message. A simple default value is supplied, as illustrated in Figure 65.

Attach Log File?

A check box that, when checked, will send a log file as an attachment to the email.

Use Process Director Configured Settings

A radio button that, when selected will send the test email using the SMTP settings that have been configured for the Process Director installation.

Use local IIS SMTP Server

A radio button that, when selected, will send the test email using the locally configured SMTP server for the IIS installation that is running on the local machine containing the Process Director installation.

Use specific SMTP Server

A radio button that, when selected, enables you to specify a different SMTP server. When this option is selected, the following SMTP properties for the server will be enabled:

- **SMTP Server Name or IP Address:** The SMTP server you wish to use to send the email.
- **SMTP Port:** The port number to use for sending SMTP email.
- **User ID:** The UserID for the email inbox to use
- **Password:** The Password for the email inbox to use.

For Process Director v5.44.1103 and higher, additional OAuth settings are available for use with Microsoft Modern Authentication. If you wish to use the OAuth connection that is set on the Properties page of the Installation Settings section, you do not need to reconfigure them here. You can simply leave the Use Process

Director Configured Settings property selected; however, you can use this setting to use a different email server or inbox than the one configured on the Properties page.

- **SMTP Tenant ID:** The Azure Tenant ID.
- **SMTP Client ID:** The Azure Client ID for the Registered AAD App.
- **SMTP Secret:** The Azure Client Secret.

For more information on configuring Azure for Process Director, Please see the SharePoint Datasources topic.

Use SSL?

A check box that, when checked, will send the test email via the encrypted SSL layer, if applicable.

UserID (optional)

The User ID of the email account from which to send the email.

Password (optional)

The Password for the user account from which to send email.

Once you have configured the test email settings, you can send the test email by clicking the Send button.

Microsoft OAuth for SMTP

For Process Director v5.44.1100, additional properties have been added to enable the SMTP settings to access an Azure Exchange365 server using Microsoft's OAuth-based Modern Authentication method. In most cases, the OAuth properties will be set on the Properties page of the Installation Settings section. If so, the appropriate OAuth SMTP settings configured there will be applied to any email tests that are run from this page, when the Use Process Director Configured Settings property is true.

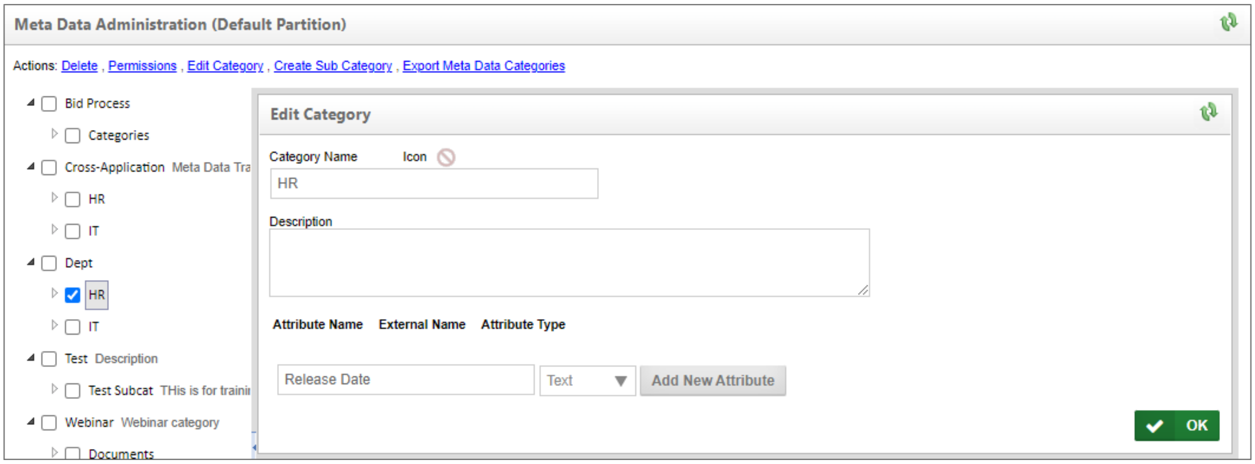
You can, however, also use custom OAuth settings on the email test by selecting the Use Specific SMTP Server option. This option will also display the properties for the SMTP Authentication Type, SMTP Tenant ID, SMTP Client ID, and SMTP Secret, just as they're displayed in Installation Settings. You can configure the appropriate OAuth values here and use them to run the email test. Of course, you must have the appropriate settings configured in Azure prior to using this feature. This feature may be useful for testing a new Exchange server that uses different properties for the OAuth settings, prior to modifying the existing SMTP OAuth properties in Installation Settings.

Help

From the Troubleshooting section, clicking the Help button will open a new tab that displays the Product Documentation web site for Process Director.

Meta Data Administration

The Meta Data Administration section, which is separate from the IT Admin section, enables you to configure the category hierarchy for this partition. Each category can have attributes that contain variable data. A category can be assigned to any object in the partition (e.g., documents, Forms, and Process Timelines). For more information about creating and using Meta Data, please refer to the Meta Data topic in the Implementer's Guide, which covers the use of the Meta Data Administration section in detail.



Meta Data Administration (Default Partition)

Actions: Delete , Permissions , Edit Category , Create Sub Category , Export Meta Data Categories

- □ Bid Process
  - □ Categories
- □ Cross-Application Meta Data Tra
  - □ HR
  - □ IT
- □ Dept
  - ☑ HR
  - □ IT
- □ Test Description
  - □ Test Subcat THis is for trainii
- □ Webinar Webinar category
  - □ Documents

Edit Category

Category Name: HR

Icon

Description

Attribute Name | External Name | Attribute Type

Release Date | Text | Add New Attribute

OK

A button that links to the Meta Data Administration section can be added to any administrative workspace via adding it from the Top Navigation Buttons tab of the Workspace's properties page.

Common Admin Actions

In addition to configuration activities one might perform in the IT Admin area of Process Director, there are several additional tasks an administrator might need to perform. This section of the documentation specifies the most common tasks that might need to be performed. You can navigate to each topic that addresses these tasks using the Table of Contents displayed on the upper right section of this page, or by using one of the links below:

Activity Checking: Ensuring that IIS Remains active, and that timer events are fired within a specified time frame.

Backing up the System: Recommendations for creating full backups of a Process Director Installation.

Creating Custom Icons: Instructions for creating and using custom icons that are **not** installed as part of Process Director.

Direct URL Access to Objects: Enabling users to access Process Director objects directly via their dynamic URL, instead of using fixed navigation buttons or links (From the Implementer's Reference Guide).

Folder Permissions: Setting and replicating user permissions on Content List folders.

Load Balancing: Implementing and configuring Load Balanced installations of Process Director.

Securing Process Director: Recommended security configuration for Process Director installations.

Storing Attachments: Recommendations and configuration for storing document attachments created during processes.

Test Server Methodology: Recommendations for performing development, QA, and production releases for applications.

Working with BP Logix Tech Support: General instructions for submitting technical support requests to BP Logix.

Activity Check Page

Process Director runs as a virtual directory in IIS and processes all time-related events only when activity is present on the system (e.g. Users are actively working on the system). Process Director doesn't have a constantly running timer service; **Timers can only be called when IIS is active and it is processing web page requests**. So, while Process Director is a near real-time system on an active installation, it is **not** a real-time system. Time-based events like condition evaluations, due date checks, activity notification schedules, and so forth are only prompted when the timer checks run. On an active system, of course, user activity prompts the time checks to run more frequently. Conversely, on an inactive system, like a development or staging system, the lack of user activity means that timer checks will run far less frequently.

Additionally, if there are no active users, IIS goes inactive and shuts down after 20 minutes of inactivity, by default. We want to avoid that during business hours, but still leave some time for IIS to restart on its own during a period of inactivity. So, we have provided an activity check page in the installation folder, named activity_check.aspx.

The activity check page does a couple things. First, it keeps IIS active so it doesn't shut down and need to restart during the business day. Second, it prompts the timer checks to invoke all of the time based events like due date checks, etc., so, even on an inactive system, time checks will still occur on a regular basis when the activity check runs, even if no users are on the system.

For on-premise installations, BP Logix recommends setting the activity check page to run every 15 minutes for a duration of 15 hours to cover the entire business day. Setting the activity check timer to 15-minute intervals will prevent IIS from shutting down every 20 minutes if the system has no active users, while ending the checks after 15 hours allows IIS to shut down the Application Pool at night, when the system isn't active. This configuration also ensures that timer checks will run within fifteen minutes of the expected time.

❗ **BP Logix implements the appropriate activity check scheduling for installations that reside in the BP Logix Cloud.**

While the activity check page is running, it tells Process Director that timer process should NOT occur under the context of a user, but only occur in the context of the running activity_check.aspx page. If timer processing occurs under the context of a user, they may see their session hang while the activity check processing is occurring, but setting the timer context to the activity check page will avoid this. Time checking will reset to user context when the activity check is complete.

To run the activity check page on a scheduled basis, you can set the following command in the Windows Scheduler utility to be run according to the highlighted schedule above:

```
PATH\bputil.exe" SU "http://localhost/activity_check.aspx"
```

In this example, PATH is the installation directory for Process Director (e.g. c:\Program Files\BP Logix\Process Director\).

There are a number of URL parameters that you can apply to the URL for the activity check page above that will enable the activity check to check specific processes. Only one of these URL parameters can be used at any time.

- **WFID:** A specific Workflow definition.
- **WFINSTID:** A specific Workflow instance.
- **PRID:** A specific Process Timeline definition.
- **PRINSTID:** A specific Process Timeline instance.

For instance, you can do an activity check on a Workflow definition by using the command

```
PATH\bputil.exe" SU "http://localhost/activity_check-
.aspx?WFID=XXXXXX"
```

❗ **The activity check page can't be run from a remote host. It can only be executed from the local server where Process Director is installed, or run remotely when logged in as an administrator. Assuming that the remote host is a secure server, however, you can add the remote server to the list of "local IPs" in the installation settings to cause Process Director to treat the remote host as a local host.**

When the activity check page runs, Process Director will determine which timer processing functions need to occur. (There are a few things like GOALS that will be evaluated EVERY time the activity check runs because they are low-impact.) You can control the timer functions by setting custom variables in the vars.cs customization file. These timer functions are NOT controlled by the frequency that the activity_check.aspx page is scheduled.

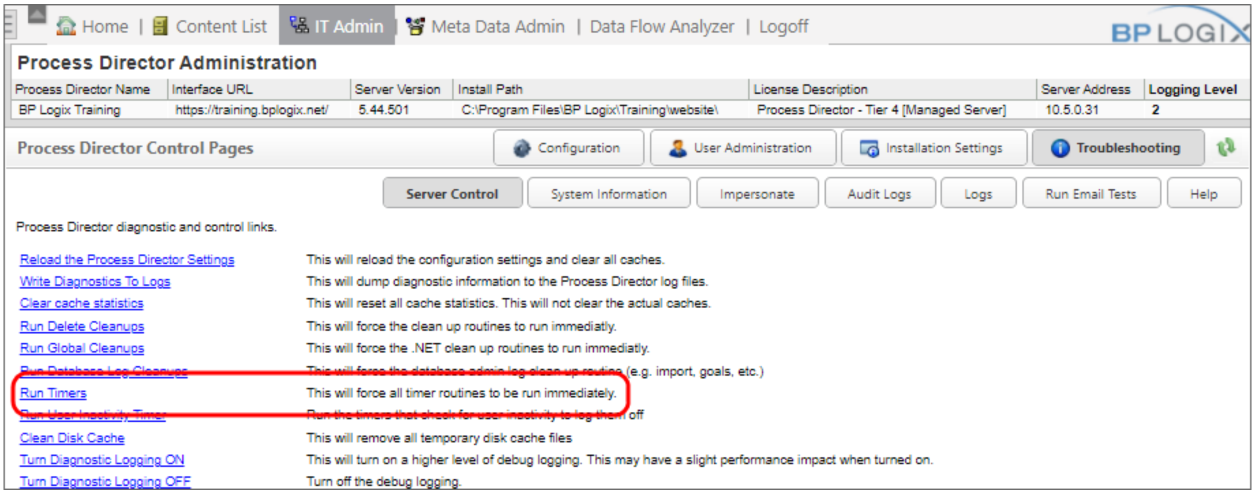
There are several Custom Variables that control the amount of time to wait between different types of timer processing. These Custom Variables, examples of their configuration, and other details, are provided in the Activity Checking Custom Variables topic of the Developers Guide.

There are ways for force the timer processing to occur without being governed by the Custom Variables. Instead, you can pass special URL parameters on the activity_check.aspx URL query string. For example, you can pass a Workflow definition

ID (WFID) on the URL, which tells Process Director to process all timers for all running Workflow instances under that definition. This should be used with care to prevent excessive resource utilization if used too often. The following URL Parameters are available to run timers on specific objects:

- STINSTID
- ACTINSTID
- WFINSTID
- PRINSTID
- WFID
- PRID
- MLID

Timers can also be manually forced from the Troubleshooting page of the IT Admin area, by clicking the Run Timers action link.



Process Director Administration

Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
BP Logix Training	https://training.bplogix.net/	5.44.501	C:\Program Files\BP Logix\Training\website\	Process Director - Tier 4 [Managed Server]	10.5.0.31	2

Process Director Control Pages

Process Director diagnostic and control links.

Reload the Process Director Settings	This will reload the configuration settings and clear all caches.
Write Diagnostics To Logs	This will dump diagnostic information to the Process Director log files.
Clear cache statistics	This will reset all cache statistics. This will not clear the actual caches.
Run Delete Cleanups	This will force the clean up routines to run immediatly.
Run Global Cleanups	This will force the .NET clean up routines to run immediatly.
Run Database Log Cleanups	This will force the database admin log clean up routine (e.g. import, goals, etc.)
Run Timers	This will force all timer routines to be run immediately.
Run User Inactivity Timer	Run the timers that check for user inactivity to log them off
Clean Disk Cache	This will remove all temporary disk cache files
Turn Diagnostic Logging ON	This will turn on a higher level of debug logging. This may have a slight performance impact when turned on.
Turn Diagnostic Logging OFF	Turn off the debug logging.

Process Director v4.52 and higher implements advanced timer checking to ensure that new instances of a running timer can't be created until the current instance of the running timer has completed.

Backing up the system

Process Director is a database-driven application, which means that the vast majority of the data you need to backup is stored in a SQL Server or Oracle database. Backing up that data should already be included as part of your normal database maintenance, when you back up the database server on a recurring basis. In addition to the database data, however, Process Director is also customizable through the use of the vars file and various resource files. Backing up the database doesn't include those customizations.

In order to perform a full backup of a Process Director installation you must back up the following items:

1. The Process Director database from SQL Server/Oracle.
2. All contents of the `Program Files\BP Logix\Process Director\website\custom` folder. This folder contains the customization file, vars.cs.ascx, along with other user-created custom files, such as any custom icons you've created.
3. The `Program Files\BP Logix\Process Director\website\app_Data\bpProperties.xml` file.
4. Any localization or string files you have created. These localization string files will have a file extension of "resx", and will be located in the `Program Files\BP Logix\Process Director\website\app_Data\` folder.
5. By default, Process Director stores document attachments in the database; however, you can elect to have Process Director store document attachments in the file system, rather than in the database. If you elect to store documents in the file system, you'll need to back up the folders that you use to store document attachments.

Creating Custom Icons

Process Director comes with many standard icons you can use to customize the icons displayed for buttons, Content List objects, Timeline Activity results, etc. In addition, you can create your own custom icons, as desired, to further customize the product's interface. Custom icons must meet the following criteria to display properly in Process Director:

- The icon file must be a GIF image, and be sized precisely at 16x16 pixels. Alpha transparency for these GIF images is supported.
- The icon file names must use sequential numbers. So if you have created three custom icons, the file names must be "1.gif", "2.gif", and "3.gif". If the icons aren't sequentially numbered, any missing numbers will display as broken images in the Process Director Interface. This means that if you delete a custom

icon, all of the icon file names must be renumbered if the numbering sequence is broken by the deletion.

- The icon files must be uploaded into the `\%Installation Directory%\custom\icons` folder of your Process Director installation (e.g., `C:\Program Files\BP Logix\Process Director\website\custom\icons`). **Only** custom icon files should be placed in this directory.

Once the criteria above have been met, and the GIF images have been loaded into the custom images folder, you must go to the Properties page of the Installation Settings section, and set the Number of Custom Icons setting to equal the number of icons you have created. Every time you add or delete an icon, this setting must be reset to the new number of existing icons. If you do not, then a new icon added to the system won't be displayed at all, and a deleted icon will display as a broken image.

Once you have uploaded and properly configured the custom icon settings, your custom icons will be displayed in the Icon Picker, In a Custom Icons section at the bottom of the Older Built-In Icons tab.

Direct URL Access to Objects

Most objects in Process Director have a unique URL that is specified in the Properties or Options tab of the object's definition. Workspaces and Documents, however, each share a generic URL, and specific Workspaces or documents are identified via a URL parameter, as described below.

Workspaces

Hotlinks can be used to directly access a specific workspace on the system. To access a workspace directly use the following syntax:

```
https://servername.com/home.aspx?profile=profile_name
```

Where "servername.com" is the host where Process Director is installed and "profile_name" is the name of the workspace. A user must be a member of the workspace for the page to be displayed.

Documents

Hotlinks can be used to directly access and download documents on the system. You may access a single document, or multiple documents. A number of

URL parameters can be used to define how you'd like to access the document(s).

OPTION	DESCRIPTION
Did	The Document ID of the document(s) you wish to download.
Path	The Partition path to the document.
Zipname	The name of the file to save as a zip file when downloading the document(s).
Inline	Setting this parameter to "Inline=1" will open the document in the same window (if it is web viewable).
Viewable	Setting this parameter to "Viewable=1" tells the system to open the web viewable version of the document, and is only used when Process Director is creating a web viewable rendition (e.g. PDF).
Height	The height in pixels to make the popup window to display the document.
Width	The width in pixels to make the popup window to display the document.

Examples

Download Via URL (Multiple Documents)

```
https://servername.com/download.aspx?DL=DID1,DID2
```

Where "servername.com" is the host where Process Director is installed and "DL" is the document ID of the document(s) you wish to download. In the example above, two documents would be downloaded by specifying two Document IDs as URL parameters. The specified documents would be zipped and downloaded in a single ZIP archive.

Open Via Path (Single Document)

```
https://servername.com/download.aspx?path=/Partition/Folder1/Folder2/document
```

Where "servername.com" is the host where Process Director is installed and "path" is the Partition path to the document.

Open Inline Option

You can optionally select to view the document inline in the browser, rather than downloading the document, by using the "inline" URL Parameter. This option is useful for files such as images, that can be viewed directly in the browser. For instance:

```
https://servername.com/download.aspx?path=/Partition/Folder1/Folder2/image.png&inline=1
```

In this example, the image.png file would be downloaded and displayed in the browser, rather than downloaded to your local file system as a file.

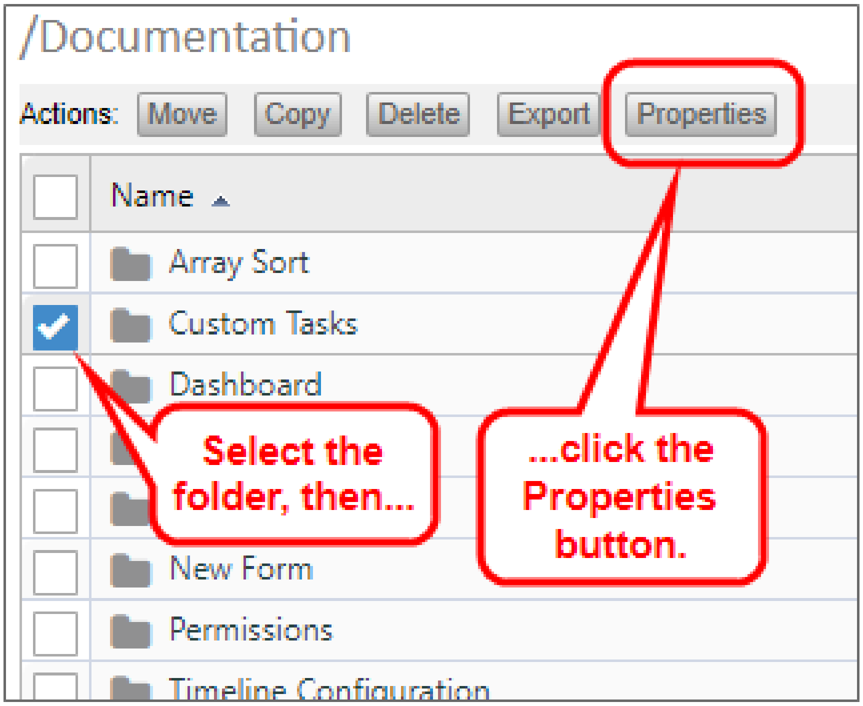
This function is available to end users only through

- Administrators providing the URL to a user;
- Server-side scripting; or
- Client-side JavaScript to construct the URL with the appropriate document IDs, such as from a Knowledge View displayed on a form.

Folder Permissions

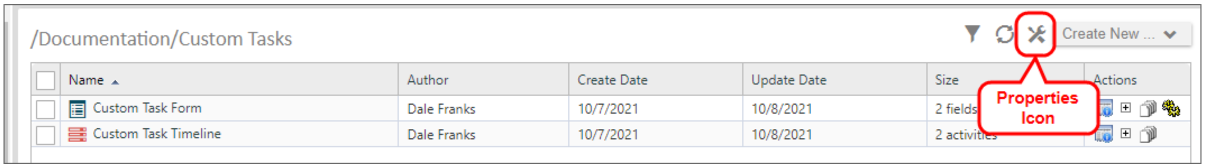
In the Content List, at the level of each folder, you may set permissions for that folder by

- Checking the checkbox next to the folder, then clicking on the Permissions link located at the top left of the Content List.


/Documentation
Actions: Move Copy Delete Export Properties
Select the folder, then...
...click the Properties button.

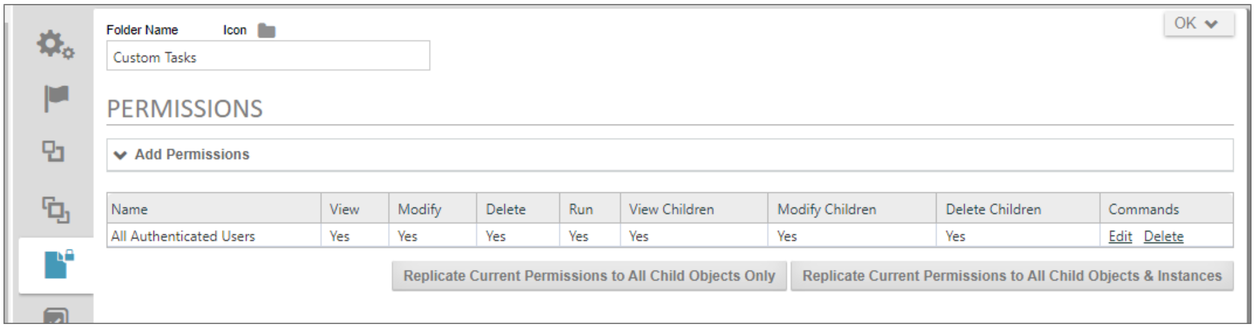
	Name ▲
□	Array Sort
☑	Custom Tasks
□	Dashboard
□	
□	
□	New Form
□	Permissions
□	Timeline Configuration

- Navigate to the folder, then click the properties icon when your inside the folder.



□	Name ▲	Author	Create Date	Update Date	Size	Actions
□	Custom Task Form	Dale Franks	10/7/2021	10/8/2021	2 fields	
□	Custom Task Timeline	Dale Franks	10/7/2021	10/8/2021	2 activities	

With either method, once the properties screen opens, you can navigate to the Permissions tab of the object definition.


OK
Add Permissions
Replicate Current Permissions to All Child Objects Only
Replicate Current Permissions to All Child Objects & Instances

Folder Name: Custom Tasks

PERMISSIONS

Name	View	Modify	Delete	Run	View Children	Modify Children	Delete Children	Commands
All Authenticated Users	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Edit Delete

You can add, edit, or delete folder permissions from this screen. A fully-detailed explanation of permissions is documented in the Permissions topic of the Implementer's Reference.

Replicating Permissions to Child Objects

You have the ability to replicate all permissions of the parent folder to all of the child objects in the folder. You have two options for doing so.

First, you can Replicate permissions to all child objects, which won't only overwrite the existing permissions on definition objects, it will also overwrite permissions on all of the form and process instances—including those instances that are active and in-progress. This may completely change the ability of users to complete active process or Form instances, so you should exercise caution in using this option in the production environment.

You also have the option, though, to replicate the permissions to child all child objects except for Form, Workflow, and Process Timeline instances. This is probably the preferred option for replicating folder permissions in the production environment where there are active processes running. Future process and form instances will be created under the new permissions regime, but existing instances will still run under the permissions regime that was valid when they were created.

Load Balancing, Standby, and Rendering Options

Customers can license load balancing, rendering servers, and hot standby systems as installation options.

Process Director installations that use multiple servers can implement load balancing between machines to ensure that processing is evenly distributed across all machines in the installation. This prevents one machine from being overloaded with processing tasks while the other machines sit idle. When configuring Process Director to run in a load balanced environment, see the settings below.

Each load balanced system must be licensed separately, and you'll be given a unique license key for each load balanced system that will be used on the register page.

The **hot standby** is a redundant method in which one system runs simultaneously with an identical primary Process Director system. Both systems have identical data and either point to the same database, or point to a replicated database. A hot standby is also known as hot spare. In the hot standby configuration, the backup system typically only processes traffic when the primary system goes down. This redirection of traffic to the backup server is controlled by the customer, who may use specialty devices to detect the loss of the primary server and automatically redirect traffic to the hot standby. In a hot standby configuration, ensure that any changes that are made to the configuration files on the local server are made on all systems. This includes the following configuration that is referenced in the backup procedures topic in this document.

The difference between a hot standby and a load balanced (LB) configuration is that a LB deployment requires a load balancing device that sits in front of the Process Director web applications. This device is responsible for sending traffic to one system or the other, based on each system's capabilities and configuration. In a load balanced configuration. all the servers must be pointing to the same database server. Replication shouldn't be used except to create a hot standby of the database.

Custom Var Settings

Implementing load balancing requires that some specific settings be mirrored on all machines in the installation. All Process Director servers that participate in the load balancing scheme should have the following settings made in the **PreSetSystemVars** function in the Custom Vars file on each machine.

```
public override void PreSetSystemVars(BPLogix.WorkflowDirector.SDK.bp bp)
{
    // Record cache
    tbl.tblProjectInstance.StaticCache.Enabled = false;
    tbl.tblProjActivityInst.StaticCache.Enabled = false;
    tbl.tblProjActivityUserInst.StaticCache.Enabled = false;
    tbl.tblProjActivityNotifyInst.StaticCache.Enabled = false;
    tbl.tblWfInstance.StaticCache.Enabled = false;
    tbl.tblWfStepInst.StaticCache.Enabled = false;
    tbl.tblWfStepUserInst.StaticCache.Enabled = false;
    tbl.tblWfStepNotifyInst.StaticCache.Enabled = false;
    tbl.tblObject.StaticCache.Enabled = false;
    tbl.tblDocument.StaticCache.Enabled = false;
    tbl.tblDocumentOnly.StaticCache.Enabled = false;
    tbl.tblContent.StaticCache.Enabled = false;

    // Read-only cache
    tbl.tblProjectInstance.StaticCache.EnabledDirtyRead =
true;
    tbl.tblProjActivityInst.StaticCache.EnabledDirtyRead =
true;
    tbl.tblProjActivityUserInst.StaticCache.EnabledDirtyRead =
true;
    tbl.tblProjActivityNotifyInst.StaticCache.EnabledDirtyRead
= true;
    tbl.tblWfInstance.StaticCache.EnabledDirtyRead = true;
    tbl.tblWfStepInst.StaticCache.EnabledDirtyRead = true;
    tbl.tblWfStepUserInst.StaticCache.EnabledDirtyRead = true;
    tbl.tblWfStepNotifyInst.StaticCache.EnabledDirtyRead =
true;
    tbl.tblObject.StaticCache.EnabledDirtyRead = true;
    tbl.tblDocument.StaticCache.EnabledDirtyRead = true;
    tbl.tblContent.StaticCache.EnabledDirtyRead = true;
    tbl.tblDocumentOnly.StaticCache.EnabledDirtyRead = false;
}
```

Installation Settings

All Process Director servers that participate in the load balancing scheme should have the following settings implemented on the Installation Settings page of the IT Admin area.

In the Load Balanced URLs field, enter the URL of each server that participates in the load balancing scheme, separating each URL with commas.

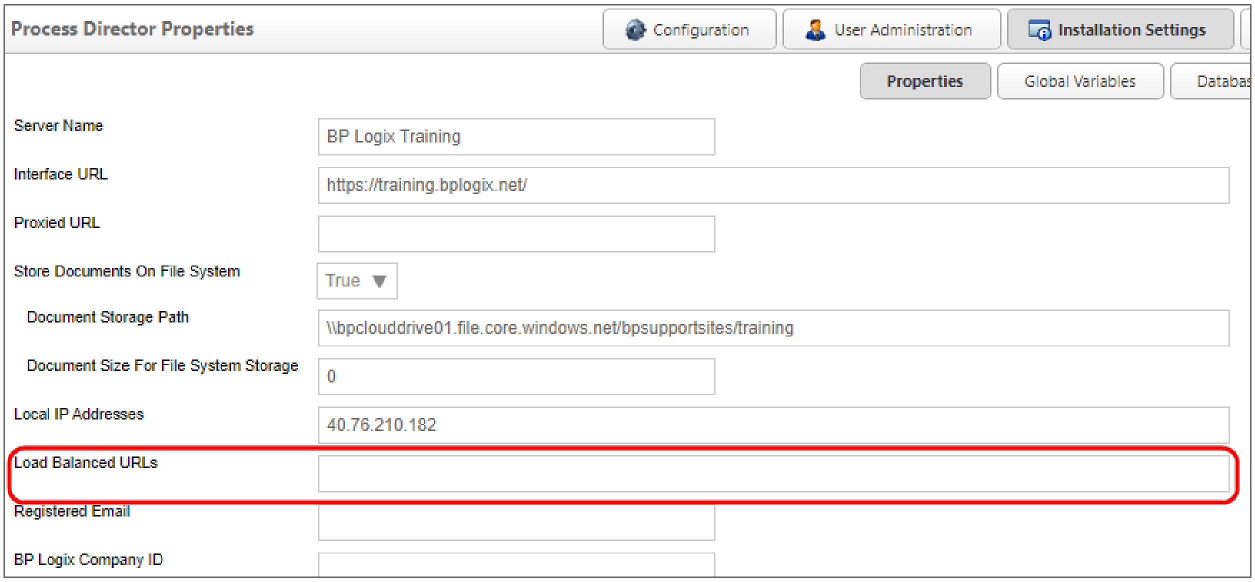
Each URL should be the URL of another Process Director server in the load balancing scheme. The system should be accessible behind the load balancing device, and each URL should be a direct connection to the other server, without going through the load balancing device.

Ensure that the Web Service Enabled property is set to "true" on the Installation Settings page on both systems. If Require Web Service Authentication is set to "true", you also need to add the IP addresses of all Process Director servers in the load balancing scheme to the list of IP Addresses in the Web Service Restrictions property of the primary Process Director installation.

For Process Director v5.44.700 and higher, the update to AES Encryption in the product requires an extra step to generate the appropriate `<machineKey>` configuration setting in the web.config file for all servers that participate in the load balancing scheme. Prior to this version, the value of the `<machineKey>` element was hard-coded. With the use of AES encryption, this is no longer the case.

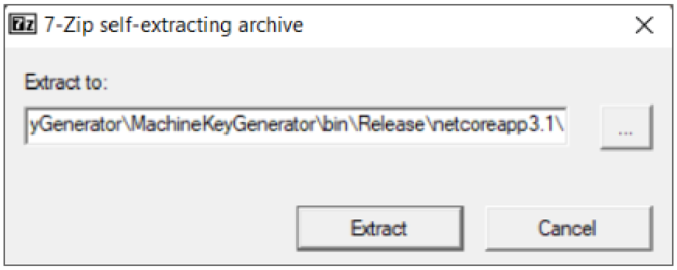
Thus, customers who utilize two or more servers with PD installed as part of a load balancing scheme must generate validation and encryption keys and update the

`<machineKey>` XML element in the web.config files for all PD instances. This ensures each server uses the same keys, which enables data encrypted by one server to be decrypted by the other. So, for the **first** upgrade to v5.44.700 or higher, you'll need to follow the procedure below to apply the proper keys to all machines in the load balancing scheme:



Server Name	BP Logix Training
Interface URL	https://training.bplogix.net/
Proxied URL	
Store Documents On File System	True
Document Storage Path	\\bpclouddrive01.file.core.windows.net/bpsupportsites/training
Document Size For File System Storage	0
Local IP Addresses	40.76.210.182
Load Balanced URLs	
Registered Email	
BP Logix Company ID	

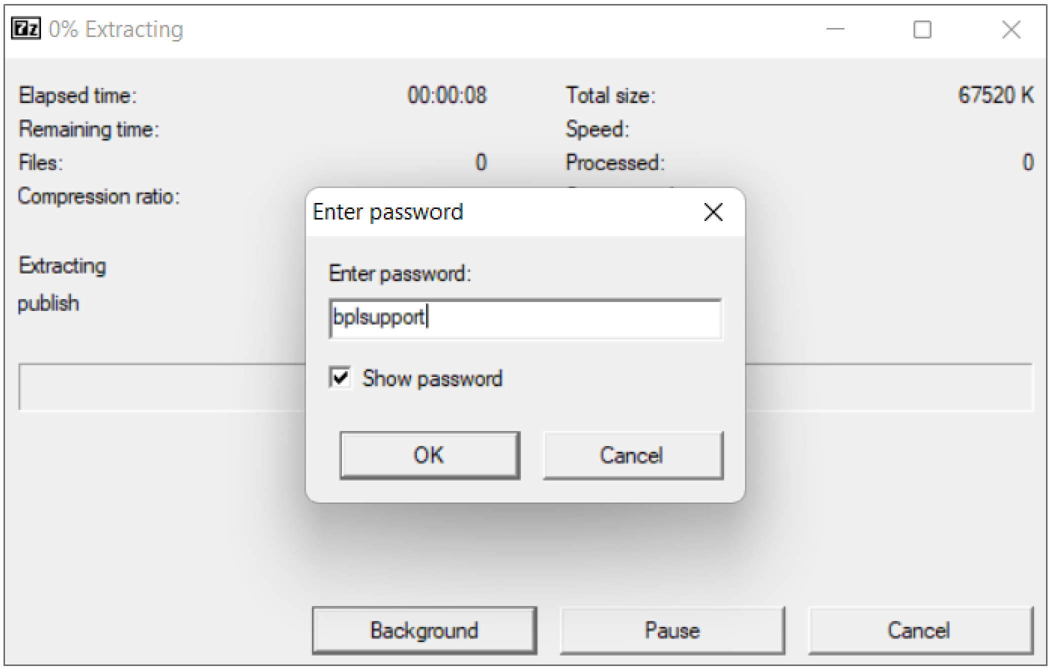
1. BP Logix will provide you with an application, **MachineKeyGenerator.exe**, that generates the Machine Key value.
2. Run the application and choose a location to which to extract the files, the click the Extract button.



Extract to: yGenerator\MachineKeyGenerator\bin\Release\netcoreapp3.1\

3. When prompted, enter the password “bplsupport”. Some anti-virus systems automatically reject unprotected self-extracting ZIP/7-ZIP archives, so the

password has been applied this file to help prevent this automatic rejection.



0% Extracting

Elapsed time: 00:00:08
Remaining time:
Files: 0
Compression ratio:
Total size: 67520 K
Speed:
Processed: 0

Extracting
publish

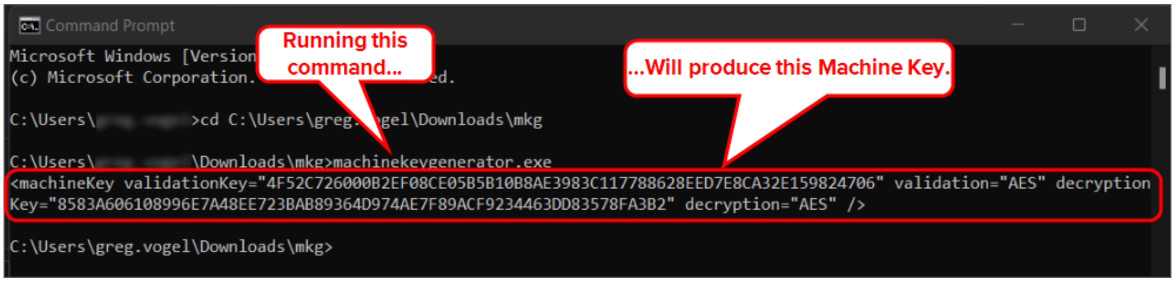
Enter password

Enter password:

bplsupport

☑ Show password

4. Using the Command Window, navigate to the folder into which you extracted the files, then run MachineKeyGenerator.exe.



Command Prompt

```
Microsoft Windows [Version
(c) Microsoft Corporation.                    ed.

C:\Users\[redacted]>cd C:\Users\greg.[redacted]gel\Downloads\mkg

C:\Users\[redacted]\Downloads\mkg>machinekeygenerator.exe
<machineKey validationKey="4F52C726000B2EF08CE05B5B10B8AE3983C117788628EED7E8CA32E159824706" validation="AES" decryption
Key="8583A606108996E7A48EE723BAB89364D974AE7F89ACF9234463DD83578FA3B2" decryption="AES" />

C:\Users\greg.vogel\Downloads\mkg>
```

5. Copy the entire `machineKey` XML element that is circled above, i.e., everything within and including the `<` and `>` characters.
6. Paste the value into each PD instance's web.config file to replace the existing `<machineKey>` element .

Once you're done, the web.config file should look something like this:

```
<configuration>
  ...
  <system.web>
    <machineKey
      validationKey="296E3FA02E766C1653678F909F4ED863254058D7A6C65C206A8B36A5681D4EE8E4A681B0463296B4CFB567D310F0F15520B3B699EDEFFE2E7420B36E5A876073" validation="HMACSHA512"
      decryptionKey="8583A606108996E7A48EE723BAB89364D974AE7F89ACF9234463DD83578FA3B2" decryption="AES"
    />
    ...
  </system.web>
  ...
</configuration>
```

Once all web.config files have been updated with the new `<machineKey>`, each machine in the load balancing scheme should be able to encrypt/decrypt any data from any of the machines in the load balanced installation.

After this procedure has been performed for the first upgrade, on every **subsequent** upgrade:

- The `<machineKey>` element will need to be generated and re-added, or,
- You can save the value of the `<machineKey>` element before the upgrade and re-apply it after.

Either way, manual modification of all web.config files will be required.

Additional AES encryption configuration requirements for upgrading your system are discussed in the Upgrading to a New Version section of the Installation Guide's Reinstall/Upgrades/Moving Hosts topic.

Load Balancing Devices

On your load balancing device, you can configure the device to check the following URL to determine if a particular server is unresponsive:

```
http://HOSTNAME/admin/test_aspx.aspx
```

In the example above, replace "HOSTNAME" with the name of the Process Director server you wish to test. You should configure the load balancer to test this URL only during business hours, to allow the server's Internet Information Server to restart the Application Pool at night, when server activity is reduced.

Rendering Server

One very specific type of load balancing that Process Director can provide is the use of a Rendering Server. The Rendering Server maintains a full installation of Process Director, and is linked to the same database at the production server. Unlike the production server, however, users can't log into the rendering server or view a content list. Its sole purpose is to transfer some processor-intensive activities away from the production Process Director server. You can use the Rendering server to perform the following activities:

- Advanced Reporting
- Asynchronous processes. The call for asynchronous processing is made by Implementers when they select the Asynchronous Operations property for Process Timeline activities of the Process, Script, or Custom Task type.

Rendering Server Setup/Configuration

To set up the rendering server, install Process Director just as you'd on a production server, using the same setup and database settings. When you apply the Rendering Server license key, the Process Director installation is automatically converted to a Rendering Server.

To associate the Rendering Server with a Production server, open the Custom Variables file on the Rendering Server, and set the BaseURLFromRenderingServer system variable to the URL of the production server for which the rendering options will be processed.

Example

```
public override void SetSystemVars(BPLogix.WorkflowDirector.SDK.bp bp)
{
    bp.Vars.BaseURLFromRenderingServer = "http://productionserver.com";
}
```

Next, on the production server, set the ReportRemoteURL system variable to the base URL for the Rendering Server.

Example

```
public override void SetSystemVars(BPLogix.WorkflowDirector.SDK.bp bp)
{
    bp.Vars.ReportRemoteURL = "http://renderingserver.com";
}
```

Once the appropriate variables have been set on each server, the rendering server will provide the processing for rendering operations.

Securing Process Director

Like any system that is exposed publicly, whether it's to the Internet or to a corporate intranet, security should be a primary administrative concern. There are a number of security practices that can be implemented to protect a Process Director installation from unauthorized access. This especially important for systems that may contain sensitive data such as Personally Identifiable Information (PII) or data that is covered under HIPAA.

Process Director includes a number of features and settings that assist you with tightening security to the product. To properly secure your Process Director installation, consider implementing the practices below.

Cross Site Scripting Protection

For users of Internet Explorer, Chrome, or Safari, Process Director v3.54 and higher implements cross-site scripting protection by implementing the XSS filter in the HTTP header, with the setting:

```
X-XSS-Protection: 1; mode=block
```

When the browser detects a cross-scripting attempt, it will stop rendering the page completely, rather than attempting to sanitize the attack and render the page.

! The Firefox browser does not support cross-site scripting protection via the XSS filter.

Starting with Process Director v3.78, Cross-Site Request Forgery (CSRF) protection is enabled by setting the fEnableReferrerProtection custom variable. When set to "true," this variable enables Process Director to screen for CSRF by ensuring that the HTTP Referrer header is valid.

HTTP Strict Transport Security

For Process Director v4.54 and higher, HTTP Strict Transport Security (HSTS) has been implemented to protect against "man in the middle" attacks, like protocol downgrade or cookie hijacking attacks. The HSTS setting is sent to the browser via an HTTPS response header field named "Strict-Transport-Security", and specifies a time period during which the browser can only access the server via a secure transport layer.

Properties Settings

On the Properties page of the Installation Settings section of the IT Admin area, there are two properties to which you should pay special attention.

Interface URL

Consider configuring your Process Director installation to use SSL. SSL encrypts all data moving between the client and the server. To do so, you'll need to acquire an SSL certificate for the server, and configure the certificate via IIS. Once you have properly configured SSL, you can set the Interface URL setting to use the HTTPS URL for your Process Director installation, preventing anyone from capturing clear-text data being sent in transit to or from your Process Director installation.

Local IP Addresses

The Local IP Addresses setting enables you to add a comma separated list of IP addresses that have permission to access the IT Admin area of Process Director as if they were a local user. Ensure that this setting only includes IP addresses from which you want to grant full administrative permissions without authentication.

By default, this setting is empty, which only allows localhost users to access the IT admin area of the product without authenticating (e.g. http://localhost/admin/). Adding additional IP addresses widens the range of users who might be granted unrestricted administrative access, thus reducing security.

If Process Director is running behind a firewall, additional care should be taken setting this value. If you add the IP address of the firewall, this effectively treats all access through the firewall as a local access.

Certain functions that would normally require system administrator privileges (for example: enabling debug mode, editing users) are available for users logged in to the server directly and connecting to the Process Director server using the “localhost” convention.

Web Service Enabled

If you don't need to make any calls to Process Director's web services, this property should be set to its default value of "False". The web service API calls can be used to enable administrative functionality, so if the web services aren't needed, they should be turned off completely. If you do require web services to run, then you should restrict access to the web services to only the IP addresses that requires access to them by setting the Web Service Restrictions setting appropriately, as described below.

Web Service Restrictions

This property contains a comma-separated list of IP Addresses, and will restrict access to web services to only the IP Addresses entered. Leaving this field blank will allow universal access to web services with authentication.

Ensure that you are restricting web service calls only to IP addresses to which you want to give full administrative permission. Again, web service API calls can enable administrative functionality, so access should be restricted to only those trusted servers. To lock the system down more securely than the default, set this value to 127.0.0.1, which will allow only local access to the Web Services API, which is useful if you have no other server applications that use Web Services.

Custom Variable Settings

When using Cloud installations or on-Premise installations with the Compliance Edition, Process Director will keep an external audit trail of all activity. There are configuration options that should understand so that the settings you are using are implemented by design, rather than simply using the product defaults.

These values are configured in the /custom/vars.cs.asmx file in the PreSetSystemVars() function. Detailed information on how to set custom variables, with the appropriate syntax, are available in the Developer's Guide.

Auditing Variables

fAuditLogFileOnly

This variable determines whether Process Director will write audit log information only to the text log files. The variable defaults to "True", meaning that it won't write any audit logging information to the Process Director database. Setting this variable to "False" will cause the audit data to be written to the Process Director database, in addition to the log files.

Documentation: fAuditLogFileOnly

nArchiveLogDays

This variable sets the number of days to keep the zipped audit log files. The default value is 30 days. Log files are stored in the /website/App_Data/logs_archive/ folder. Any log files older than the number of days specified by this setting will be deleted.

Documentation: nArchiveLogDays

nAuditLogDays

This is the number of days to keep the audit log data in the Process Director database. The default value is 30 days. Any audit data older than the specified value will be removed from the database.

Documentation: nAuditLogDays

fAuditFormAPICalls

This variable determines whether Process Director will write an audit log for changes made by APIs. The default value is "True", which means that Process Director will log an audit record of API calls resulting in a change to form data. While we generally recommend that this value remain set to the default value of "True", please note that this setting can have an effect on server performance for applications rapidly performing large numbers of API-based form field changes.

Documentation: fAuditFormAPICalls

fAuditFormViews

This variable determines whether Process Director will write an audit log for all form views. This can result in a tremendous amount of audit logging when the value is set to "True". The default for this variable is "False".

Documentation: fAuditFormViews

User Authentication Variables

If you are using built-in user authentication with Cloud installations or on-Premise installations with the Compliance Edition, BP Logix recommends that you use the password enforcement options. This will require that any user passwords conform to the enforcement options.

PwdStrength

This variable controls password complexity. It should be configured to use at least PasswordStrength.Medium. The default value for this variable is PasswordStrength.None. See the topic for the PwdStrenth custom variable for more information.

Testing Variables

fTestMode

This variable sets the Process Director installation to Test Mode when set to "True", and will allow a user to login as any other user without a password. The default value for this variable is "False". Ensure that this custom variable is always set to "False" in your production system. The variable should also be set to "False" on your development and test systems, except for those times when it is explicitly needed, after which, it should be set back to "False".

Documentation: fTestMode

User Settings

Users can be given administrative privileges in the User Administration section of the IT Admin area. There are some privileges that are very sensitive, and so should be used very sparingly, and only with an understanding of the capabilities these settings will give the user. Also, remember that these privileges can be given indirectly by granting them to a group to which the user is also a member.

On production systems, the best practice is to give no administrative rights to any “normal” user. Instead, build in a privileged user identity for each administrator, to which they should explicitly log in for the purpose of executing administrative tasks, and for no other reason.

System Administrator

This permissions setting gives the user access to the functions in the IT Admin area. With this privilege, a user can give any user any type of permission. Essentially, this permissions setting gives full control of the Process Director installation to the user, or any other user they choose to designate.

System Partition Admin

This permissions setting gives the user full permission to every object in the Content List of the partition for which administrator access is granted. All other permissions settings in the Content List of the specified partition are ignored for this user.

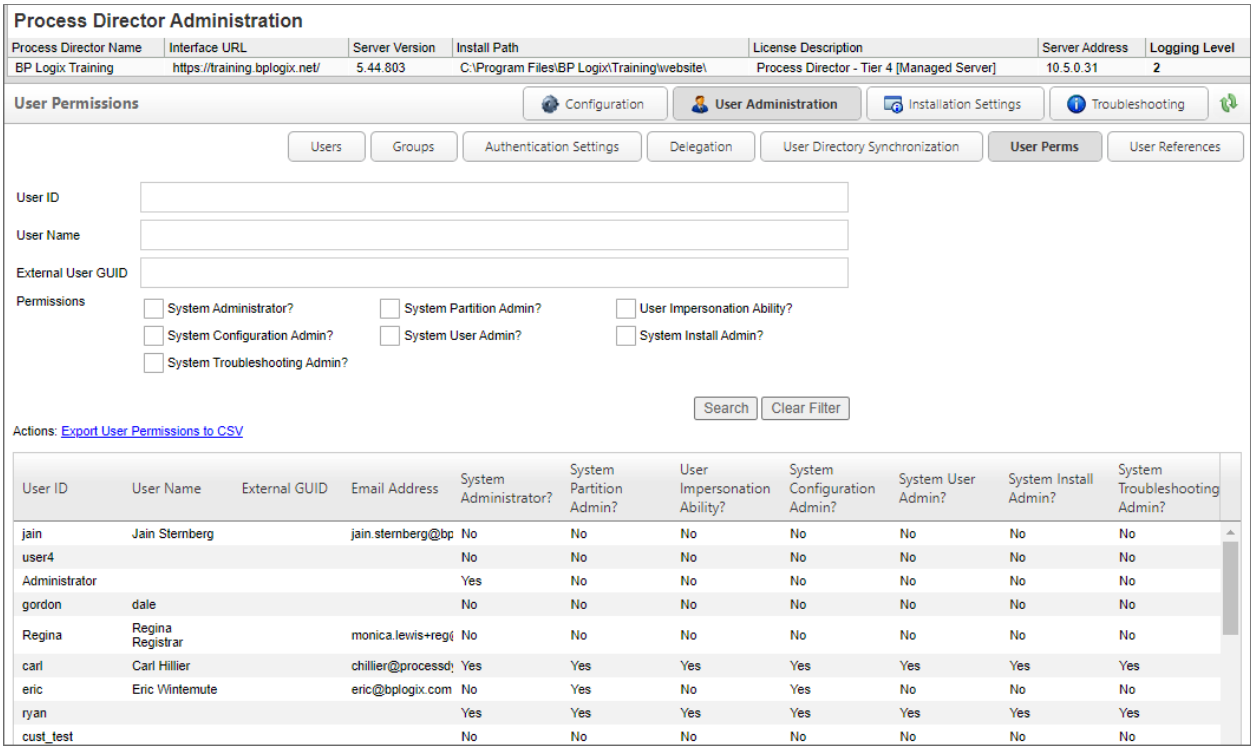
User Impersonation Ability

This permissions setting allows a user to impersonate any other user and take on their complete identity and privileges. Administrators should be extremely careful about who is granted user impersonation permission, though Process Director v5.13 and higher prevents non-administrators from assuming any administrative permissions via impersonation.

User Permissions Page

Administrators of Cloud installations or on-Premise installations with the Compliance Edition will notice an additional User Perms page in the User

Administration section of the IT Admin area.



Process Director Name	Interface URL	Server Version	Install Path	License Description	Server Address	Logging Level
BP Logix Training	https://training.bplogix.net/	5.44.803	C:\Program Files\BP Logix\Training\website\	Process Director - Tier 4 [Managed Server]	10.5.0.31	2

User ID

User Name

External User GUID

Permissions
☐ System Administrator? ☐ System Partition Admin? ☐ User Impersonation Ability?
☐ System Configuration Admin? ☐ System User Admin? ☐ System Install Admin?
☐ System Troubleshooting Admin?

Actions: Export User Permissions to CSV

User ID	User Name	External GUID	Email Address	System Administrator?	System Partition Admin?	User Impersonation Ability?	System Configuration Admin?	System User Admin?	System Install Admin?	System Troubleshooting Admin?
jain	Jain Sternberg		jain.sternberg@bp	No	No	No	No	No	No	No
user4				No	No	No	No	No	No	No
Administrator				Yes	No	No	No	No	No	No
gordon	dale			No	No	No	No	No	No	No
Regina	Regina Registrar		monica.lewis+reg(	No	No	No	No	No	No	No
carl	Carl Hillier		chillier@processdi	Yes	Yes	Yes	Yes	Yes	Yes	Yes
eric	Eric Wintemute		eric@bplogix.com	No	Yes	No	Yes	No	No	No
ryan				Yes	Yes	Yes	Yes	Yes	Yes	Yes
cust_test				No	No	No	No	No	No	No

The User Perms page enables you to find users and view a report of permissions that are applicable to that user.

The top section of the user permissions screen provides a number of search fields that you can fill out to filter the users returned by the permissions search. The filter criteria will accept all or part of a User ID or User Name, or the GUID of an external user. Once you have entered the filter criteria you desire, click the Search button to see a list of all the users that match your filter criteria, as well as the permissions granted to the users.

The User Perms page is very useful for manually auditing the permissions granted to any user.

Built-In User Authentication Options

When using Cloud installations or on-Premise installations with the Compliance Edition, there are several callout points in the /custom/vars.cs.asmx file that allow you to control access to the system, password changes, etc.

More detail on these functions can be found in the Developer's Guide.

CanLogin()

This function is called when a user attempts to login, and can be used to reject a login, to redirect the user to another page, or to limit certain users to specific IP addresses.

LoginComplete()

This function is called when the login is successful.

ForgotPassword()

This function is called when the user clicks on the “I forgot my password” link on the login page. This is only for built-in users.

ValidatePassword()

This function is called when a user attempts to set or change their password, allowing for custom complexity requirements.

Audit Log Monitoring

When using Cloud installations or on-Premise installations with the Compliance Edition, and when storing audit logs in the database, you can search for various events. In the Troubleshooting section of the IT Admin area, there is an Audit Logs page containing a search function that allows you to find specific audit log types. BP Logix recommends that you periodically check audit logs for certain privilege changes to ensure that these privileges are the ones expected on the production system.

- AdminPageAccess
- PermissionAdded
- PermissionRemoved
- PermissionUpdated
- PermissionReplicated
- UpdateUser
- AdminPageAccess
- ImpersonateOn

Content List Permissions

When setting up permissions in the Content List on a production system you want to grant only the minimum permissions required. For instance, users don't need to be explicitly given View or Modify permission to form instances to participate in a process task. The system will automatically grant them the appropriate level of permission on the form instance to complete a task that is assigned to them. When the user completes the task, the configured permissions are then used for that form instance.

Permissions shouldn't generally be configured on individual objects in the Content List, except in special cases that require that level of granularity. Normally, permissions should only be configured at the folder level. Preparation and thought is necessary during the initial implementation to ensure that you structure the objects across folders based on object types and how permissions will be established.

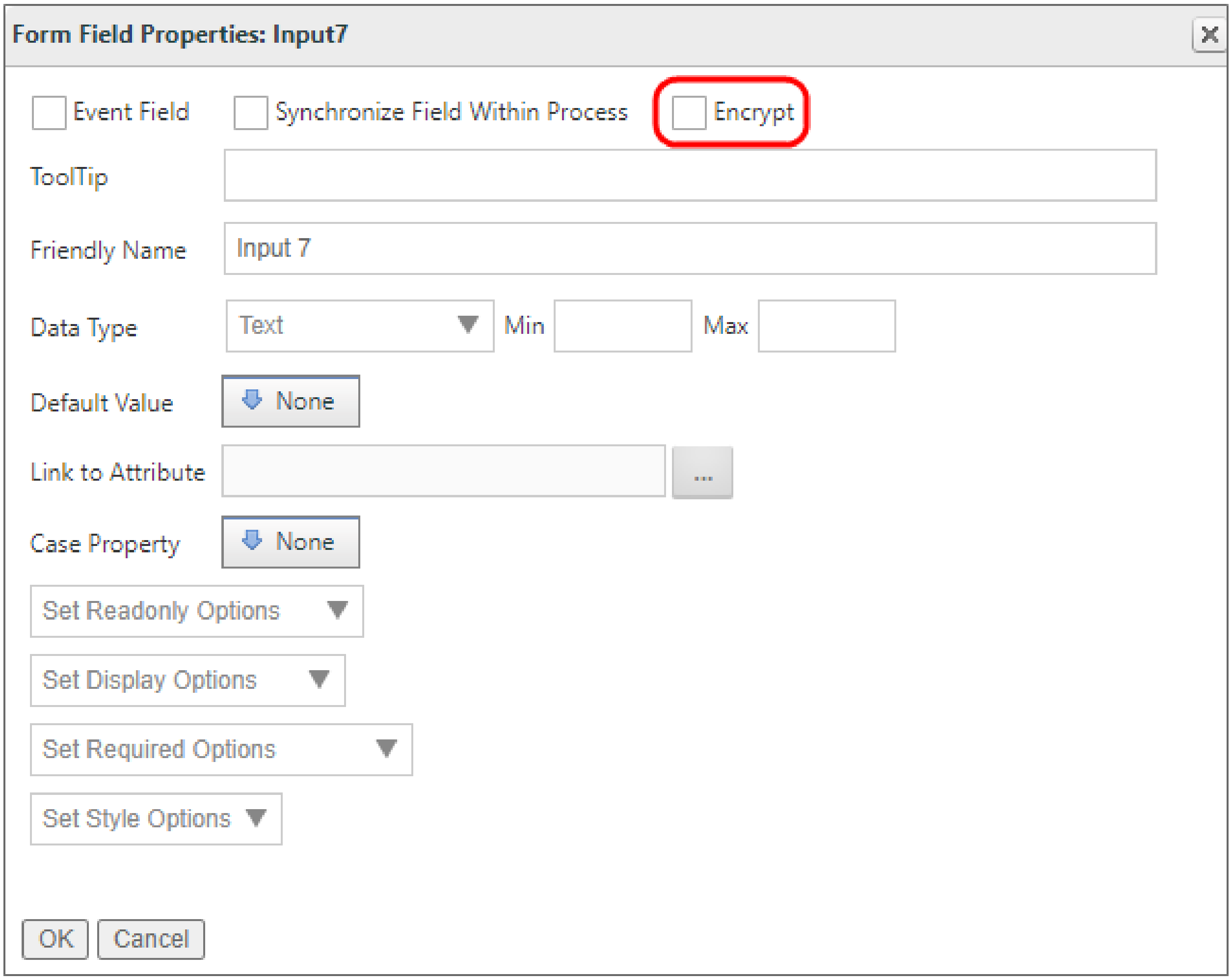
For example, don't create a folder that contains all Knowledge Views and Reports and then configure the permissions on each individual object to identify who is able to run it. Instead create multiple folders and group the objects by the type of access required. For instance, you might create an “Admin Knowledge Views” folder that only administrators can access, and a “Knowledge Views” folder than can be accessed by other end users. Segregating the access by folder will assist in the deployment of new objects from a non-production system to your production system, because:

1. Imported objects inherit the permission of the parent folder into which objects are being imported, and
2. Permissions aren't carried across in the XML export.

Your production system shouldn't grant delete permission to any users. Instead, have a limited set of partition administrator users, as partition administrators can perform functions in the Content List regardless of its configured permissions. Users should only login with these partition administrator user IDs when performing specific administrative functions, like deleting objects or importing XML files from a non-production system.

Data Encryption

When using Cloud installations or on-Premise installations with the Compliance Edition, you have the option to encrypt fields using the Form Field Properties settings of a control, which is located in the Form Controls tab of every Form definition. Simply select the Encrypt check box.



Form Field Properties: Input7

□ Event Field □ Synchronize Field Within Process □ Encrypt

ToolTip

Friendly Name: Input 7

Data Type: Text Min Max

Default Value: None

Link to Attribute

Case Property: None

Checking the Encrypted Field check box will cause Process Director to save the field value in an encrypted format in the database. You may wish to consider this for fields that contain passwords, PII, HIPAA, or other sensitive data. Keep in mind, however, that you may not be able to search for data stored in encrypted form.

Storing Attachments

You have two choices when it comes to storing documents, such as file attachments, in Process Director: internal database or file system storage.

The default method of document storage is to store the documents in the Process Director internal database, in a binary field. For most users, this is the recommended option, for a number of reasons.

- Backing up the Process Director database automatically backs up the stored documents, so the number of required backups is reduced.

- Outside users can't inadvertently access the documents outside of Process Director to alter, move, or delete them.
- Performance, in most cases, will be superior, because there is no need to access files on separate network locations, and drag them across the network.
- Document administration can be performed from a single location.

For some users, however, there are use cases where storing documents in a separate file system makes more sense, such as:

- You store very large files, such as high-definition video files. It is more efficient to store these files on a File System, rather than to transform them to binary database storage and back, which imposes performance delays that file system storage doesn't.
- You have a need for the files to be accessed from outside of Process Director.
- You have a large number, i.e., in the hundreds of thousands, of documents, which greatly increases the time needed for a database backup.

Obviously, when documents are stored on a separate file system, you must perform two backups, one of the database, and one of the file system. And, of course, it may be possible for malicious users to get into the file system and alter or delete the documents, so extra security considerations apply. There are configuration options in the administrative settings that allow you to control the size of documents that should be stored on the file system. This is useful if you only want to store very large documents external to the database but maintain the advantages of using the database storage for all other documents. However, it is recommended to decide on one approach or the other, and if storing files on the file system, set the size to `0` so that all documents binaries are stored as files.

Ultimately, the decision whether to store documents in process Director or a file system depends on your use case, the size and number of documents you expect to store, your network bandwidth, and the backup requirements that will be imposed under each alternative. This is decision best made in consultation with your internal IT professionals.

Whichever choice you make, Process Director will handle the stored documents in a way that is transparent to your users.

There is a built-in Process Director function that enables documents to be moved according to the current configuration of the system. You have to go into “debug mode” in the client browser and navigate to the IT Admin area's Troubleshooting section. There will be a link that will move documents back/forth from the file system to the database. This can take quite some time, and if canceled in the middle, it can be restarted and it will continue safely where is left off.

Some internal documents will always be stored in the database regardless of the installation settings, for example, form definitions.

Test Server Methodology

Process Director can be installed on a development or test/staging server to create and test applications without affecting your production environment. Applications can be exported from a test server and imported to the production server. See the Importing/Exporting Content topic in the Implementer's Reference.

The safest option is to create a new, blank database for your test installation. You'll, once the test server is set up properly, have to manually export all of your existing object definitions from the Production server to the Test server.

When you want to set up a Test server, follow these steps:

1. Create a new, blank Test database
    a. Create a blank database on SQL Server to host your test installation.
2. Ensure that the database settings for Process Director are using the connection string for the test database and not the production database.
3. Run the test server diagnostics using the online Administrative functions under Troubleshooting.
4. Enter the test license key and token again on the test server in the online Administrative section under the Installation > Licensing.
5. Navigate to the installation tab in the Administration section and ensure the Interface URL in the Installation Settings is pointing to the test server (if any values were configured).
6. Turn off email notifications on the test server using the Administrative section and changing the Email Notification option in the Installation tab.
   This setting is important because emails sent to users from the test system may be confusing. The other option is to replace all email addresses in the database with another email address for testing. This can be done by setting the TestUserEmailscustom variable in the installation's vars.cs.ascx file. This variable allows you to route all process emails (task list emails, notifications,

etc) to a single user. Use this setting with caution. It should only be used on non-production systems to test processes and Forms.

7. To test the system by logging in as different users, turn off security for all users on the TEST system at the database layer, and set the `fTestMode` variable to "true" in the vars.cs file. In this mode, Windows Integrated authentication is disabled. This mode allows anyone to log into the server without a password. Use this setting with caution. It should only be used on non-production systems to test processes and Forms.
8. You can now export Content List items from the Production server, and import them into the Test server.

For test servers, if you enable users to recover passwords, you should be aware that, when using the TestUserEmails custom variable, password reset emails will ***not*** be sent to the configured Test User Email address. Exempting the Test User Email address is done for security purposes, because anyone with access to the test email account would gain the ability to access the account of any user that submits a "Forgot password" request. Password reset emails are, instead, sent directly to the requesting user.

Custom Variables Code Sample

```
public override void SetSystemVars(BPLo-
gix.WorkflowDirector.SDK.bp bp)
{
    bp.Vars.fTestMode = true;
    bp.Vars.TestUserEmails = User.GetUserByUserID(bp, "my_
test_id");
}
```

After the above steps are completed, you can modify existing Processes on the test system and export them. The exported Processes can be then imported into the production server.

Using Production Data

When you are ready, you have an additional option to use production data on your Test server by importing your existing Production database into the Test database. This will provide an exact mirror of your Production installation, however, it may expose sensitive data to users in the test environment.

Exercise extreme caution when selecting this option, to avoid a breach of sensitive data.

To reproduce your production data on the Test database for Process Director **v5.44.700 and higher** follow the steps below. For versions **below v5.44.700**, steps 1, 3, 6, and 7 are not needed, as those version do not implement AES encryption.

1. Be sure web access to the test system is disabled during this process to prevent any users from accessing the system during this process.
2. Backup the database on the test server and save Process Director license key and token.
3. Backup your existing bpProperties.xml file in the App_Data folder.
   a. Save the value for Database Connection String from /admin/db.aspx. Using the UI allows you to view the un-encrypted value.
4. Turn off email notifications on the test server by setting the TestUserEmails flag in the installation's vars.cs.ascx file. This variable allows you to route all process emails (task list emails, notifications, etc) to a single user. Do this prior to copying over the Production database to ensure that users don't receive a plethora of notifications from the Test database when the import is complete.
5. Copy the Process Director production database to the test server. This WILL overwrite your existing test database, if applicable. All of your existing process director objects in the Production database will be available in the Test database.
6. Copy the sEncryptionKeyDoNotModify and sCheckValue XML elements from the production bpProperties.xml to the test server bpProperties.xml.
   a. You will need to set all the following values to empty (if used) and then reconfigure them in the administrative UI because you are changing the system's encryption key: sSMTPPassword2, sSMTPSecret, sSMTPClientID, sSMTPTenantID. Once configured, these values can be restored using the IT Admin pages AFTER saving bpProperties.xml.
7. After saving bpProperties.xml, restore the value of the Database Connection String from 3(a) using /admin/db.aspx page.
8. If you are storing documents on a Windows file system instead of the Process Director database, ensure you make a copy of that file system to the appropriate location for the new system.

9. Copy any other Custom variables you are using in the Production installation's custom vars file to the Test server's custom vars file. Do NOT copy the vars file itself, just the text of the vars settings from the Production vars file to the Test vars file.
10. Copy any other customized process scripts or other file-based customizations from these production directories to the test server:
    `\Program Files\BP Logix\Process Director\website\custom\*.*`
11. Re-enter your license key information on the Test Server.

You may wish to re-import the production data on a recurring basis, like once a year, or once every six months, so that changes to existing Processes can be tested based on a recent copy of the Production environment.

Tenant-Based SharePoint Configuration

Tenant-based SharePoint installations have a complex and more cumbersome access model than Site-based installations. Tenant-based installations, therefore, require a different process to set up and configure:

1. Create a certificate to authenticate Process Director with Azure.
    a. Using Microsoft’s certreq.exe, installed on all modern Windows OS versions.
    b. Using PowerShell, also included with all modern Windows OS versions.
2. Add Process Director as a Registered Application in Azure.
    a. Add the public key certificate to the Process Director application in Azure.
    b. Configure the appropriate Azure settings.

In this topic, we'll address each of these required steps in detail. Additional information about this topic can also be obtained from Microsoft's online documentation.

❗ **You cannot configure any OAuth settings for SharePoint Datasources or SMTP Email in Process Director until you have created and registered an Azure Active Directory Application in Azure by completing the steps described in this topic.**

Create a certificate to authenticate Process Director with Azure

Microsoft prefers the use of certificates for authentication. Each certificate includes both the public and private keys used to encrypt data. The public key (in a CER file) is used by SharePoint Online to authenticate Process Director. The private key is packaged in a password-protected PFX file and is used by Process Director to authenticate with Azure Services. There are two methods that can be used on Windows-based systems to create a proper certificate.

- Using Microsoft’s certreq.exe, installed on all modern Windows OS versions.
- Using PowerShell, also included with all modern Windows OS versions.

> **Keep in mind that certificates expire after a set period of time. Most organizations specify the maximum length of time certificates should be used. By default, the instructions that follow will generate certificates valid for one year. You should, therefore, generate and install new certificates well before existing certificates expire. This implies that your organization also has a mechanism in place to be reminded when expiration is approaching, to ensure that service interruptions don't occur.**

Creating a Certificate with certreq.exe

This method of certificate creation might be preferred if you’re less comfortable with command-line operations and don’t intend to automate the generation of certificates. Microsoft's online documentation has additional information about certreq.exe.

Instructions

First, using a text editor like Notepad, copy and paste the following text into a new document:

```
[Version]
Signature = "$Windows NT$"

[Strings]
szOID_ENHANCED_KEY_USAGE = "2.5.29.37"
szOID_KEY_ENCIPHERMENT = "1.3.6.1.5.5.7.3.1"

[NewRequest]
Subject = "cn=BP Logix Process Director"
```

```
MachineKeySet = false
KeyLength = 2048
HashAlgorithm = Sha1
Exportable = true
RequestType = Cert

KeyUsage = "CERT_KEY_ENCIPHERMENT_KEY_USAGE"
; The following values can be changed to generate certificates
that expire
; sooner or later depending on your organizations needs. The
default is 1 year.
ValidityPeriod = "Years"
ValidityPeriodUnits = "1"

[Extensions]
%szOID_ENHANCED_KEY_USAGE% = "{text}%szOID_KEY_ENCIPHERMENT%"
```

Once you've done so, save the document as an INF file in a folder on your system, e.g., `c:\Users\Some.User\Documents\PD Certificate\CertReq.inf`.

Open the Windows Command Prompt. You can press the [WINDOWS] key, type "cmd", then select the "Command Prompt" application.

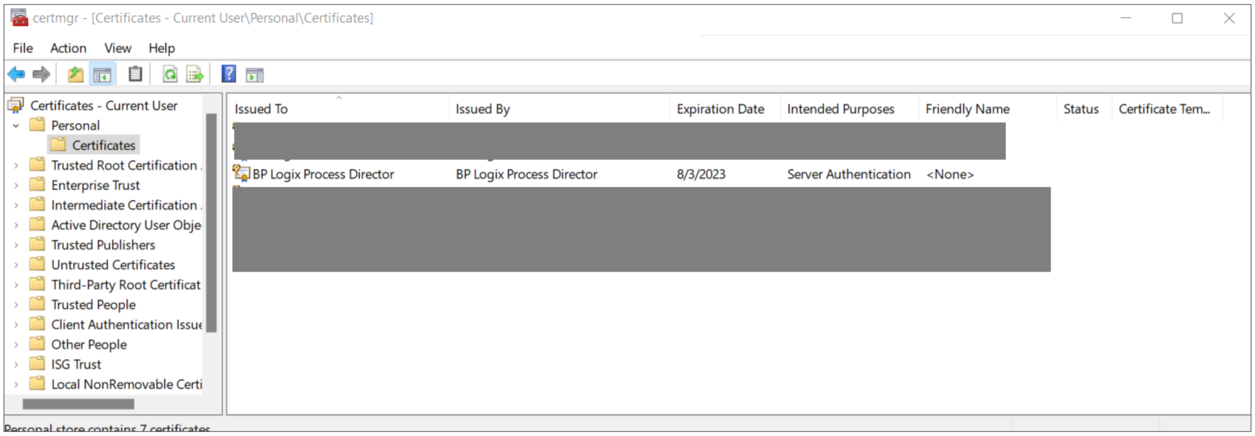
In the Command Prompt, open the directory in which you installed the INF by using the cd command, and the folder path to the INF file, then pressing the [ENTER] key. Using the example above, you'd need to type:

```
cd c:\Users\Some.User\Documents\PD Certificate\
```

Once the directory changes, type the following and press the [ENTER] key to run the certreq application.

```
certreq -new certreq.inf PublicKey.cer
```

Running the certreq application will create the certificate, and add it to the Windows Certificate Manager. To continue, you'll need to open the Certificate Manager to access the new certificate. To open the Certificate Manager, you can press the [WINDOWS] key, type "certmgr", then select the "Manage computer certificates" option. When the Certificate Manager opens, you'll need to navigate to the `Personal\Certificates` folder, where you should see the certificate issued to and by BP Logix Process Director.

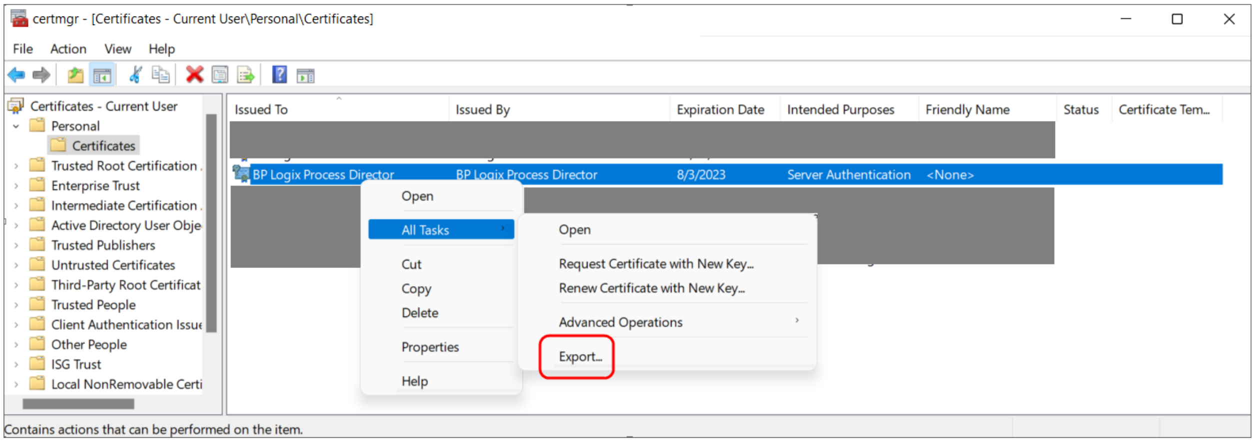


certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issue
Other People
ISG Trust
Local NonRemovable Certi

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
[redacted]						
BP Logix Process Director	BP Logix Process Director	8/3/2023	Server Authentication	<None>		
[redacted]						

Personal store contains 7 certificates.

Right-click that certificate and then select All Tasks > Export.

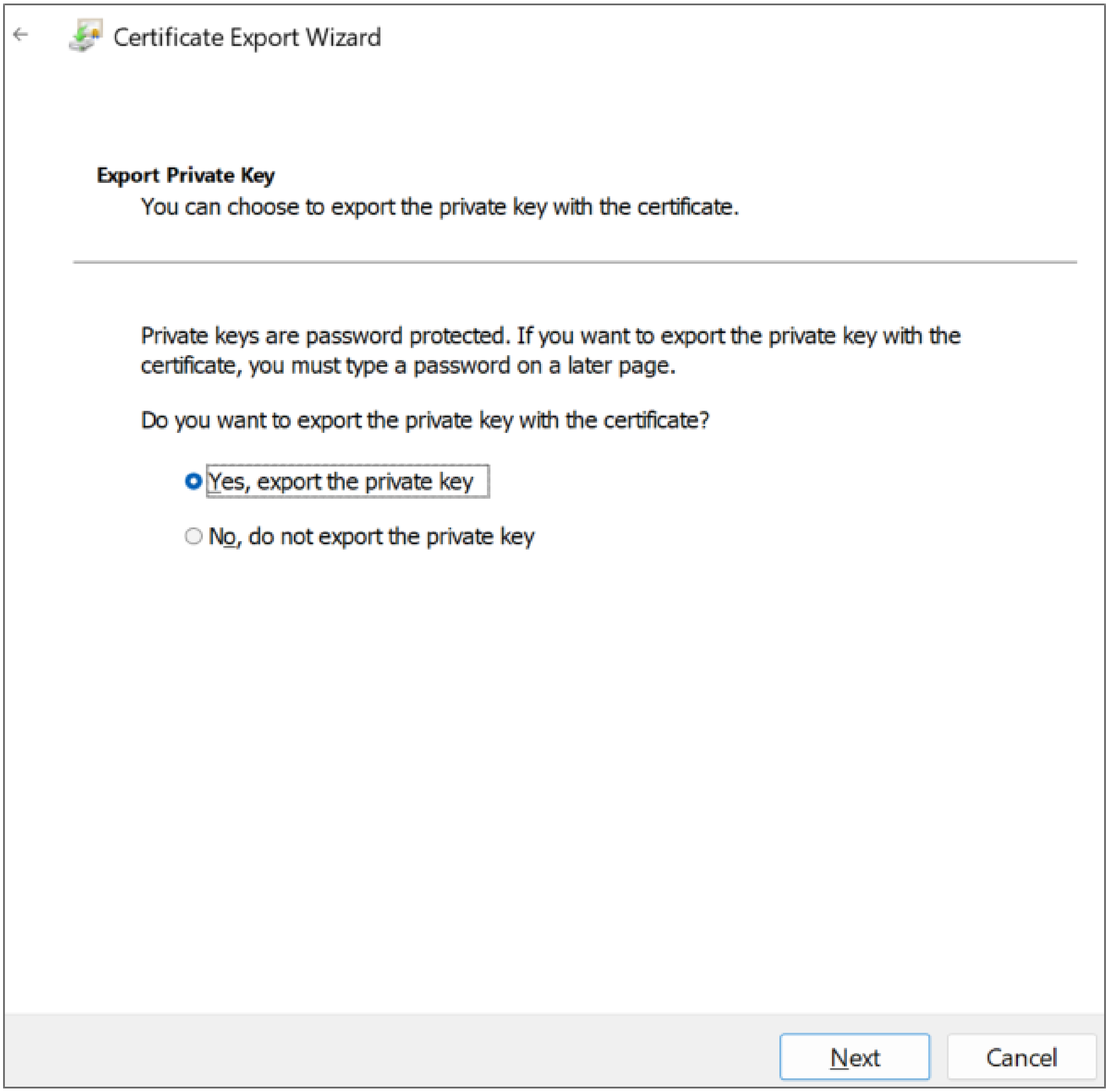


certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issue
Other People
ISG Trust
Local NonRemovable Certi
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Advanced Operations
Export...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
[redacted]						
BP Logix Process Director	BP Logix Process Director	8/3/2023	Server Authentication	<None>		
[redacted]						

Contains actions that can be performed on the item.

The Certificate Export Wizard will open. On the first screen, click the Next button. On the Export Private Key screen, select Yes, export the private key, then click the Next button.



Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

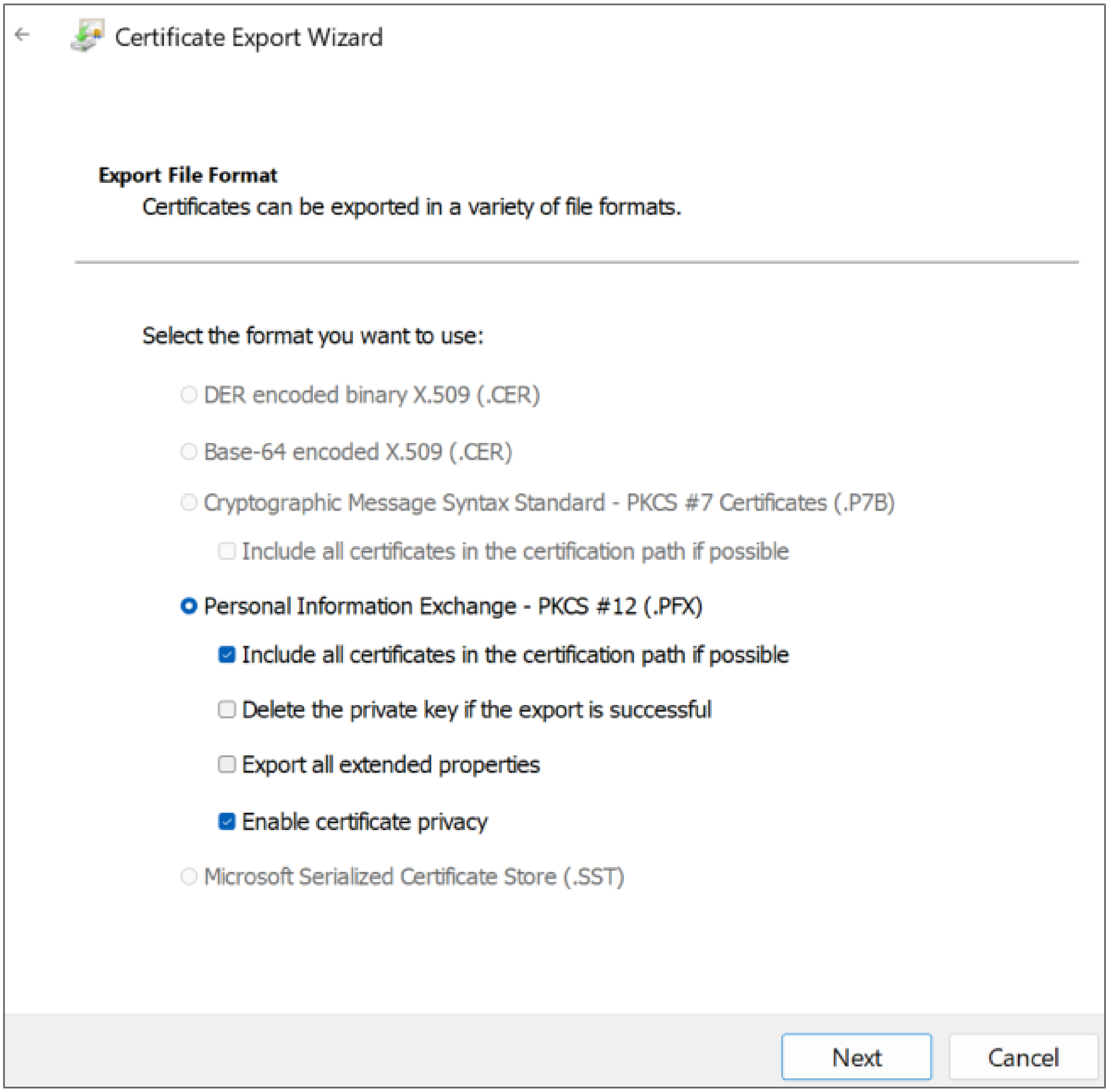
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

On the Export File Format screen of the Wizard, Ensure that you select the following options:

- Personal Information Exchange - PKCS #12 (.PFX)
- Include all certificates in the certification path, if possible
- Enable certificate privacy



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

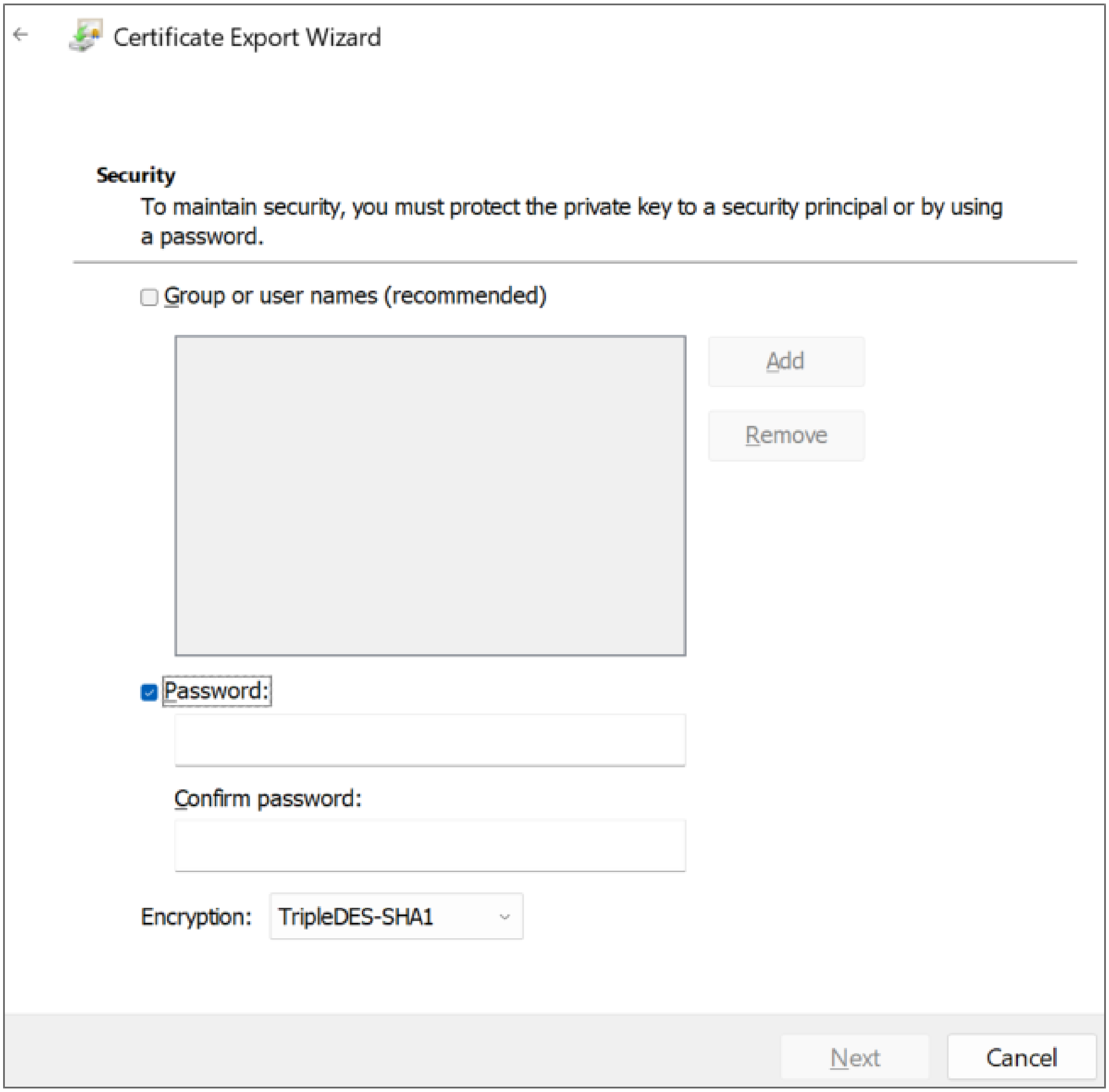
☑ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

On the Security screen, check Password as the security protocol and enter a password twice.

> ⓘ **Be sure to store this password securely, you'll need it in future steps.**

> ! **Be sure to use a long, sufficiently complex password in line with your organization’s cryptographic standards.**



Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

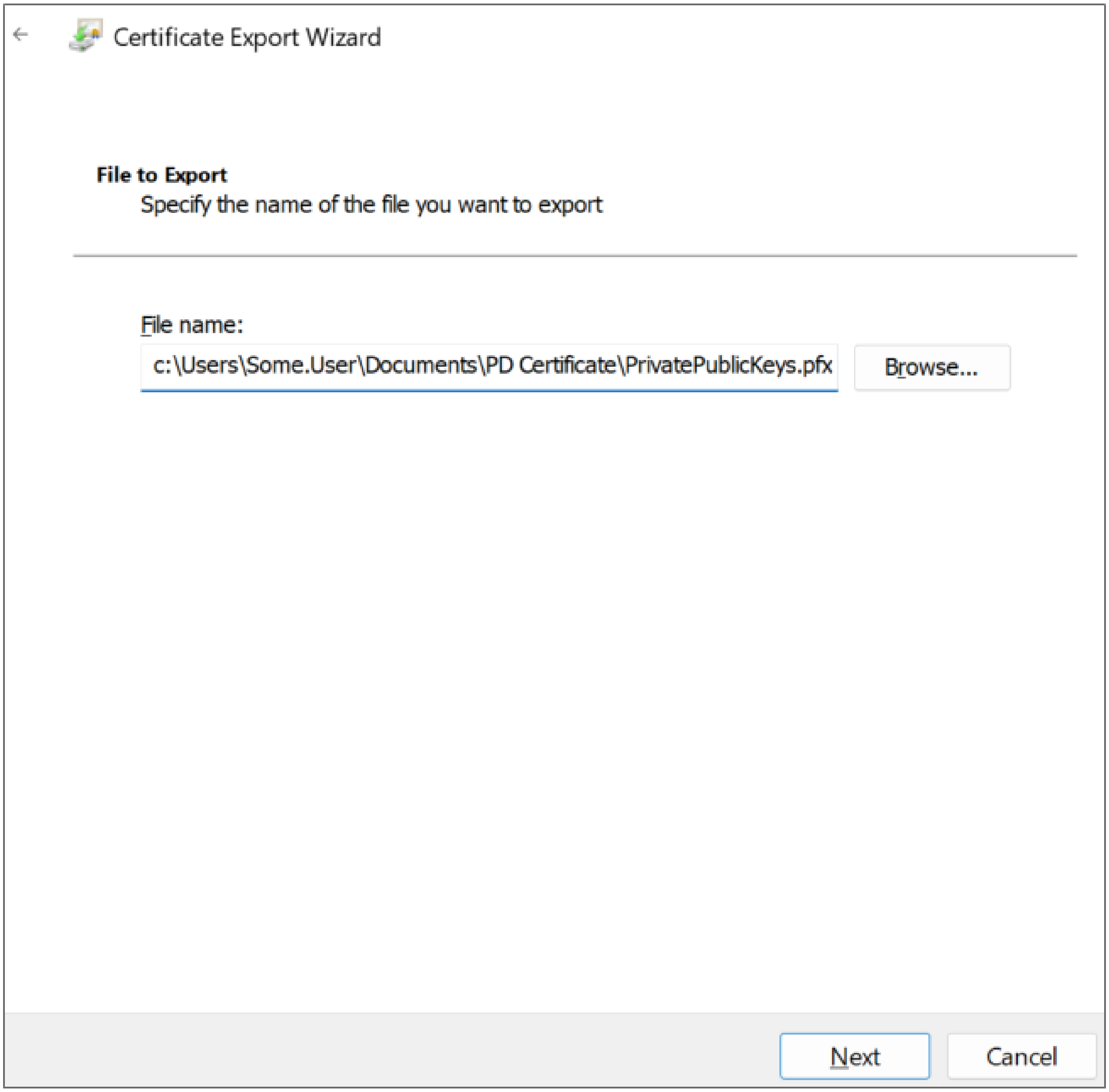
☐ Group or user names (recommended)

☑ Password:

Confirm password:

Encryption: TripleDES-SHA1

On the File to Export screen, store the resulting PFX file in the same folder as you stored the CertReq.Inf and PublicKey.Cer files, then click the Next button.



File to Export

Specify the name of the file you want to export

File name:

c:\Users\Some.User\Documents\PD Certificate\PrivatePublicKeys.pfx

Click the Finish button on the next Wizard screen, then OK to finish the Wizard and close it.

BP Logix recommends that you remove the certificate installed in the Certificate Manager by right-clicking it and then selecting Delete followed by Yes to delete it in the confirmation dialog.

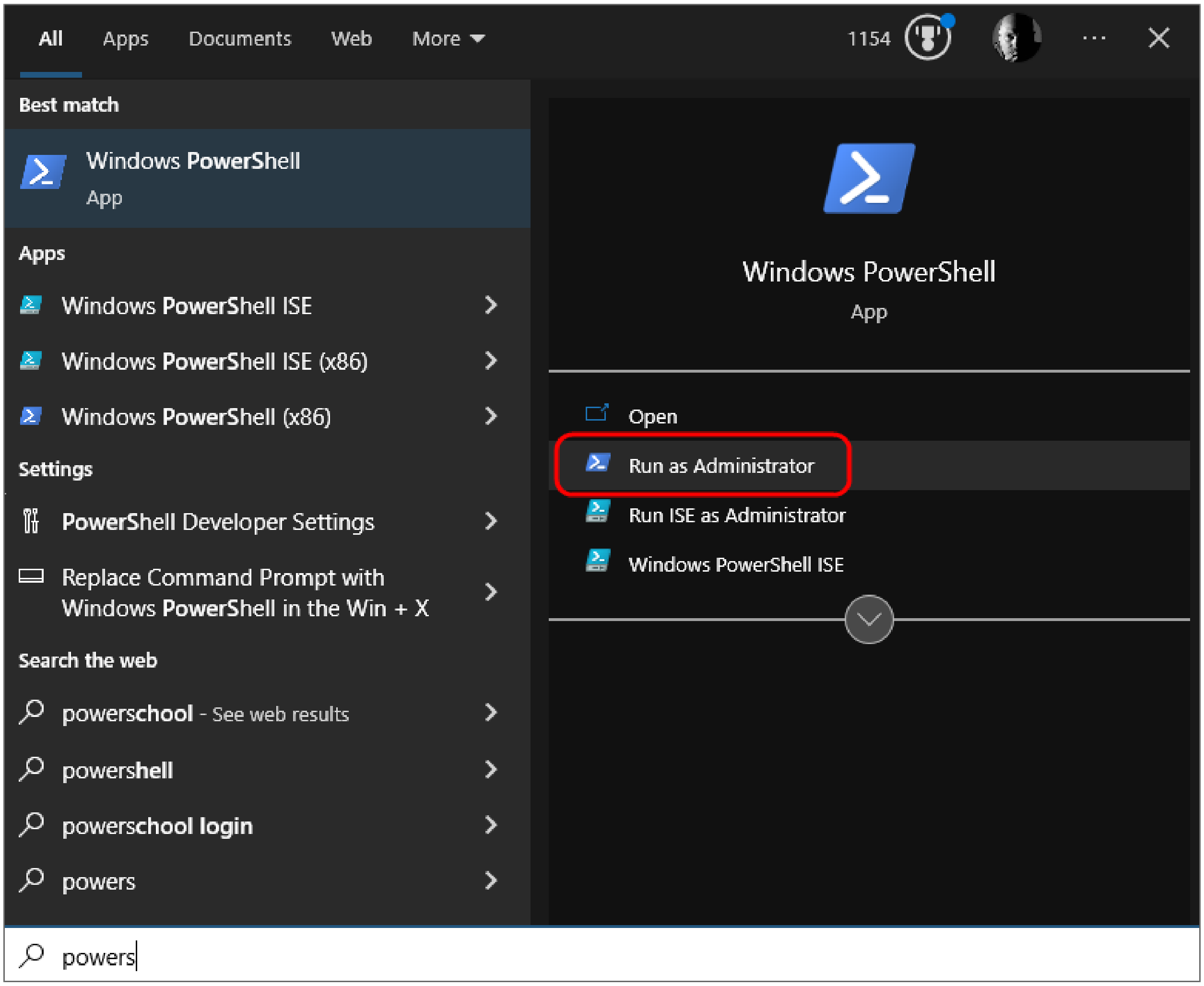
Keep both the PublicKey.cer and PrivatePublicKeys.pfx files handy for subsequent steps in this setup process. You should also archive them in a secure, backed up location as well.

Creating a Certificate with PowerShell

PowerShell is a command line application that's included with all modern versions of Windows. You can choose this method if you’re comfortable with PowerShell and might want to automate certificate generation on a recurring basis.

Instructions

Open PowerShell by pressing the [WINDOWS] key, typing "PowerShell" then selecting the Run as Administrator option to open Windows PowerShell.



In PowerShell, create or navigate to the directory you'd like to use to store the certificate files. Once you're in the desired directory, run the following command:

```
$cert = New-SelfSignedCertificate -CertStoreLocation Cer-
t:\LocalMachine\ -KeyUsage KeyEncipherment
    -KeyAlgorithm rsa -KeyLength 2048 -subject "BP Logix
```

```
Process Director"
    -DnsName "BP Logix Process Director" -Type SSLServer-
Authentication
    -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1")
```

Next, run these commands in PowerShell, replacing `<password>` with a password of your choosing. Ensure the passowrd is cryptographically secure, in accordance with your organization’s standards. Be sure to also store this password securely, as you'll need it in future steps.

```
$pwd = ConvertTo-SecureString -String '<password>' -Force -
AsPlainText
$path = 'cert:\LocalMachine\My\' + $cert.Thumbprint
```

Finally, run these commands to create the .PFX and .CER files. Modify the `<path>` value to store the file in a location of your choosing.

```
Export-PfxCertificate -cert $path -FilePath <path>\Priv-
atePublicKeys.pfx -Password $pwd
Export-Certificate -cert $path -FilePath <path>\PublicKey.cer
```

Keep both the PublicKey.cer and PrivatePublicKeys.pfx files handy for subsequent steps in this setup process. You should also archive them in a secure backup location as well.

Add Process Director to Azure

To add Process Director as an application in your Azure Active Directory portal at the Tenant level, complete the steps below after signing into your Azure portal (portal.azure.com):

1. Register Process Director as an Application

A. If you have access to multiple tenants, use the Directories + subscriptions filter in the top menu to switch to the tenant in which you want to register the application.
B. Search for and select Azure Active Directory.
C. Under Manage, select App registrations > New registration.
D. Enter a display Name for your application, e.g., “Process Director”. This name can be changed later, if needed.

E. Specify who can use the application. Typically, only accounts in this organizational directory should be used. See the Microsoft documentation titled Quickstart: Register an application with the Microsoft identity platformfor more information.
F. Add the Redirect URI, which is the URI for your Process Director installation, e.g., https://myorg.bplogix.net.
G. Click the Register button to register the application.

2. Add Your Public Key Certificate

To add your public key certificate to the Process Director application in Azure, complete the steps below.

A. In the Azure portal, in App registrations, select the Process Director application you created previously, e.g., “Process Director”, as in step 1D, above.
B. Select Certificates & secrets > Certificates > Upload certificate.
C. Select the PublicKey.cer file you created earlier.
D. Upload the certificate file to Azure.

Your AAD Application should now be properly registered and secured with a certificate.

Conclusion

Congratulations! Assuming that you've correctly followed the instructions above, you've now configured an Azure Integration with Process Director. To complete the integration, you'll need to perform some additional, specialized configuration in Azure, which is covered in the Create a Sharepoint data source topic.

Working with BP Logix Technical Support

BP Logix maintains a technical support system that operates primarily through the BP Logix support site. All technical support tickets should be submitted through the support web site.

There are a some best practices to keep in mind when submitting a support ticket. These practices will make it easier for our support specialists to help you, and reduce the amount of time it takes to resolve your issue.

- Process Director is updated on a regular basis, with both formal releases, and patch updates. These patches may contain resolutions to the issue you are experiencing, and updating the product will eliminate the issue. If you are on an older version of Process Director, then first upgrade to the most recent version, which is available on the Downloads page of the BP Logix support site, and see if the upgrade fixes the issue you're experiencing. In general, you should always be using the most recent version of the product.

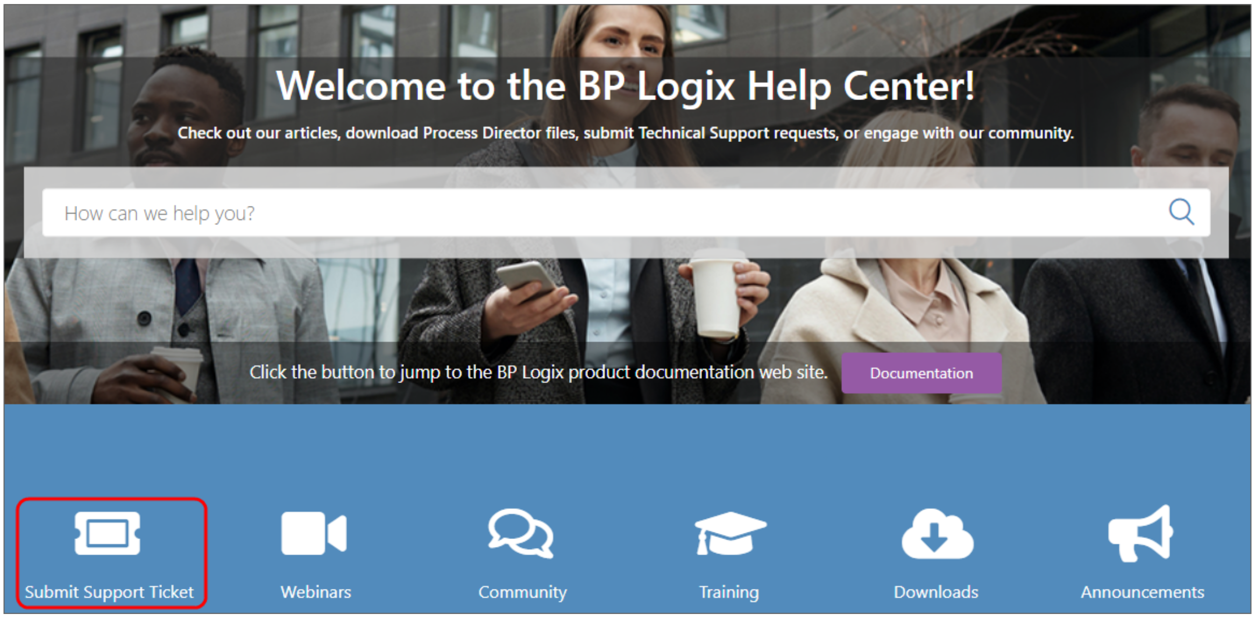
- When describing your issue, please remember that our support specialists don't know how your project is configured, the nature of your processes, or what you are trying to accomplish. The only thing they know is what you tell them in the Description field, so please provide them with adequate information to understand the issue. Doing so will help minimize the amount of back and forth it will take for the support specialist to understand your issue.
- Be sure to attach any relevant screen shots or, if the issue generates a Process Director error, attach your log files to the ticket, as described in the Logs topic.
- It is extremely helpful if you can create a small sample project that replicates your issue, export it from Process Director, and attach the exported XML file to the ticket. There is a good chance that the support specialist will ask you for such a project, so attaching it when you first submit the ticket will eliminate that round of troubleshooting conversation. Also, if you can't replicate the issue in a small project, then it may not be a Process Director issue, but rather an issue of improperly configuring the project where you are experiencing the problem.
- While we do wish to help you, please remember that the tech support ticket is for actual errors or other problems with Process Director itself. It isn't designed for use as a means of learning how to perform a configuration task. We are happy to schedule a Direct Assistance session with you to provide you with instruction in how to use a particular feature or perform a complex configuration, but please reserve support tickets for actual issues with the product. Also, if you don't know how to perform a particular task, remember that we have fairly extensive documentation on how to administer Process Director and implement projects, so there's an excellent chance that your answer can be found there.

Registering at the Support Site

For most customers, two Support users are allowed to register at the support web site. You must contact your sales representative to submit names to be added to the list of Support Site users. Once BP Logix registers your user account, you'll be able to fully access the support site.

Submitting a Support Ticket

From the home page of the support site, you can create a new ticket by clicking the Submit Support Ticket button to open the Submit a Support Request form.


Welcome to the BP Logix Help Center!
Check out our articles, download Process Director files, submit Technical Support requests, or engage with our community.
How can we help you?
Click the button to jump to the BP Logix product documentation web site.
Documentation
Submit Support Ticket
Webinars
Community
Training
Downloads
Announcements

This button won't display unless you are logged into the Support Site.

The Submit a Support Request form contains the following fields to fill out:

Subject: A brief title to describe the nature of the issue.

Description: Please provide as detailed a description of the issue as possible.

Selected Severity: A dropdown control containing various severity levels, based on the issue's impact on your production environment. Please don't overstate the severity of the issue.

Vaccine Tracker Issue: A check box to indicate this is an issue with the pre-built Vaccine Tracker application.

Process Director Version: A dropdown from which you can select the version of Process Director you're running.

Attachments: This is a good place for you to provide additional information, such as screen shots, log files, etc.

Once you've filled out the support ticket, click the Submit button to submit it. Submitting the ticket instantly sends it to the support queue, making it visible to all of the support specialists.

Miscellaneous Administration Notes

SQL Server Issues

Replication

SQL Server's running replication may fail if Process Director is upgraded in a way that alters the database schema. This is because an ALTER query can't be performed on the database if replication is enabled. If the upgrade fails, you may see a SqlException error with the following message: “You can only specify the READPAST lock in the READ COMMITTED or REPEATABLE READ isolation levels”.

If the upgrade fails, perform the following procedure:

1. Set the nDBTransIsolationLevel variable in your vars file to IsolationLevel.RepeatableRead.
2. Then, click on the Verify Process Director Database Schema button in the IT Admin settings.
3. After the database schema has been verified, remove the nDBTransIsolationLevel variable from your custom vars file, and add to the top of the vars file the following line: `<%@ Import Namespace=”System.Data” %>`

Full-Text Search

Process Director supports Full Text Searching (FTS) of documents. It utilizes the FTS Indexing in SQL Server. The Full-Text engine must be installed, enabled and configured in SQL Server.

These steps will create a Full-Text Index in SQL Server and start the population of the index. The population needs to be run to index new documents added to the system. This can be configured to run automatically (e.g. through the scheduler), or can be configured to update the index every time a document is added/removed from the server. To perform a manual population, under the Process Director database entry, click on the [Storage] Full-Text Catalogs entry and right click on the BPLogixFTS catalog in the right side pane, and choose the menu item Start

Incremental Population. On SQL Server 2008 set the Population Schedule for the new FTS index.

1. Open the SQL Server Management Studio.
2. Expand the Process Director database and right click on the tblObject table. Select the "Full-Text Index Table -> Define Full-Text Index" menu entries.
3. Using the Full-Text Indexing Wizard, select the default Unique Index by pressing the Next button.
4. Set Columns and Document Types: Under the Available columns item, select the checkbox next to bObjectData. Under the column named “Document type column” set the value to sFileType for the bObjectData row just selected. Press Next to continue.
5. Enter the appropriate change tracking. Press Next to continue.
6. Enter a catalog name (e.g. BPLogixFTS). Press Next until the wizard completes.
7. Create an optional population schedule. Press Next to continue.
8. Set IFilters: IFilters are needed to index the various document/file types. If Microsoft Office is installed on the server where Process Director is installed, an IFilter is automatically included for Office documents allowing them to be indexed. PDF documents require the Adobe Acrobat IFilter (e.g. Adobe PDF IFilter 11) to be installed. The 64-bit version of the IFilter can be downloaded from the Adobe web site. (Adobe currently bundles a 32-bit PDF IFilter with Adobe Acrobat® 11 as well as the free Adobe Reader® 11 software.) The Acrobat IFilter must be installed prior to creating the index. If the index already exists, delete it, install the Adobe IFilter and recreate the index. Additionally, the Adobe IFilter requires that the "bin" folder be added to the PATH environmental variable. For more information on the Acrobat IFilter and SQL Server see the relevant documentation from Adobe.

Windows and SQL Server will natively support .DOC, .XLS and .PPT file types, however to support .DOCX, .XLSX, and .PPTX files, you'll need to install the Office Filter pack

Refer to the vendor of the document/file format for information on IFilters, or use third party IFilter products for common file types such as ZIP, JPG and TIFF.

Refer to the SQL Server documentation for scheduling options and detailed configuration and tuning information for the full-text engine.

You should be aware, however, that FTS isn't a panacea for all text search issues. The way FTS is configured by default may result in unexpected search results if you aren't aware of the default configuration. For example, when using FTS on SQL Server there is a default list of “Stop Words” that Microsoft identifies as items that are ***not significant*** when doing FTS indexing. So, by default, if you are searching for something like “Activity 1” using FTS, SQL Server will ***not*** find it using the following syntax:

```
SELECT tblObject.oDID FROM tblObject WHERE CONTAINS(bObjectData,
N'"%Activity 1%*"')
```

But if you were searching for “Activity 1A”, that ***would*** work using the same syntax:

```
SELECT tblObject.oDID FROM tblObject WHERE CONTAINS(bObjectData,
N'"%Activity 1A%*"')
```

Why? Because the indexing lists the trailing number (1) in the first example in the ‘system’ Stop Word list, and so does ***not*** include the trailing number as part of the search criterion in the first example.

To see what Stop Word list is used by tblObject, issue this SQL command:

```
SELECT
    ft_c.name AS [Catalog],
    s.name AS [Schema],
    o.name AS [Table],
    [StopList] =
    CASE
        WHEN ft_i.stoplist_id IS NULL THEN 'None'
        ELSE ISNULL(ft_sl.NAME, 'System')
    END
FROM
    sys.fulltext_indexes AS ft_i LEFT OUTER JOIN
    sys.fulltext_stoplists AS ft_sl ON ft_sl.stoplist_id = ft_
i.stoplist_id INNER JOIN
    sys.fulltext_catalogs AS ft_c ON ft_c.fulltext_catalog_id
= ft_i.fulltext_catalog_id INNER JOIN
    sys.objects AS o ON o.object_id = ft_i.object_id INNER
JOIN
    sys.schemas AS s ON s.schema_id = o.schema_id
```

To see the list of all stop words for English:

```
SELECT * FROM sys.fulltext_system_stopwords WHERE language_id
= 1033;
```

To turn off the use of stop words in SQL Server for tblObject:

```
ALTER FULLTEXT INDEX ON tblObject SET STOPLIST = OFF
```

To use "system" stop words in SQL Server for tblObject:

```
ALTER FULLTEXT INDEX ON tblObject SET STOPLIST = SYSTEM
```

SQL Queries Run Slowly After Upgrading to SQL Server 2014

In SQL Server 2014, Microsoft changed how SQL commands are evaluated. If, while running SQL Server 2008/2012, you created a SQL view that contains array fields for a form definition, this query will run more slowly if you subsequently upgrade your database to SQL Server 2014. This is **only** an issue on SQL Server 2014 with views that map columns in an array. Views that map array fields will need to be dropped and recreated after the upgrade to SQL 2014. When you recreate the view from the form definition, it will append a new "trace flags" option that will tell SQL Server 2014 to use the older logic from SQL Server 2008/2012, and eliminate the performance deficiency.

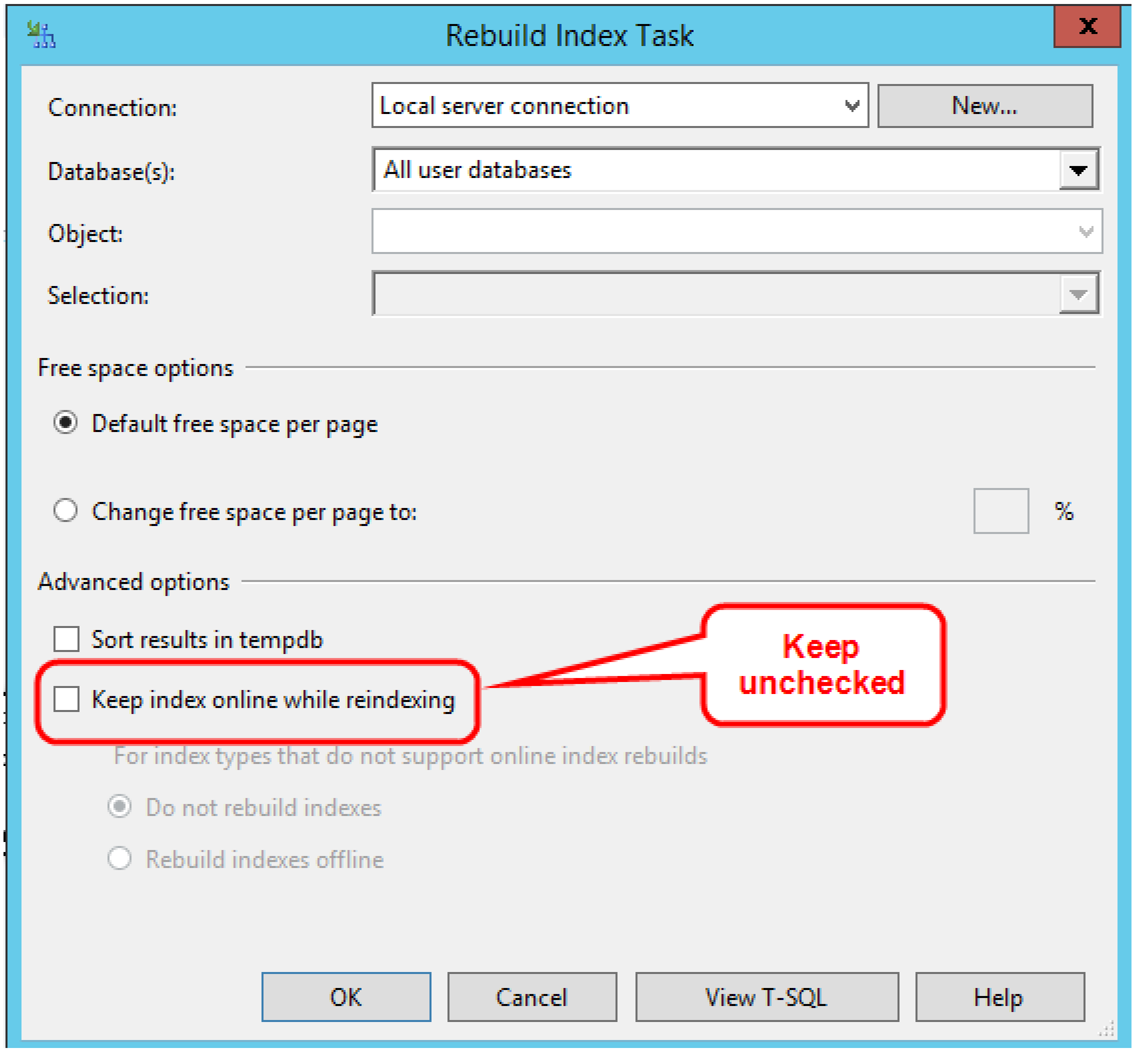
SQL Server Escape Bug

A bug in SQL Server can cause a performance problem with Knowledge Views searching for form data using "contains". To work around this, the product will now match any special wildcard characters in your search filter with any character. You can re-enable the exact matching using special characters by setting the fEnableSQLEscape Custom Variable that we created to help mitigate this SQL Server bug to 'true". The new variable exists to enable the ESCAPE, but **ensure your SQL Server version is patched at the appropriate level**. The variable can be enabled in the Custom Vars file in the PresetSystemVars() function.

See the MS KB article: https://support.microsoft.com/en-us/kb/2698639 for more information. It is important to note that the bug effects more than the SQL Server versions listed in the KB article (e.g. SQL Server 2014 is also effected).

Rebuilding Database Indexes

You should, as part of your regular SQL Server maintenance, have a maintenance plan for rebuilding database indexes and statistics on a recurring basis. We recommend doing this weekly. For the “Rebuild Index Task” in SQL Server we recommend that the check box labeled “Keep index online while reindexing” is NOT checked.



Connection: Local server connection

Database(s): All user databases

Object:

Selection:

Free space options

● Default free space per page

○ Change free space per page to: %

Advanced options

□ Sort results in tempdb

□ Keep index online while reindexing

For index types that do not support online index rebuilds

● Do not rebuild indexes

○ Rebuild indexes offline

Keep unchecked

IIS Issues

SMTP with IIS/Exchange Server

On Windows 2003, the SMTP email notification can use the IIS SMTP server or Microsoft Exchange Server. If you are running Microsoft Exchange Server on Process Director host, this will be used as the SMTP host instead of the IIS SMTP Server. Microsoft Knowledge Base articles Q238956 and Q228465 have additional information regarding the configuration and troubleshooting.

To use Exchange Server you still have to install IIS SMTP. After it is installed change the "Pickup" parameter: This IIS command will display the current "Pickup" directory:

```
%WINDIR%\system32\inetsrv\adminsamples\ADSUTIL set SMTPsvc/1/PickupDirectory
```

Use the following command to change the "Pickup" directory to Exchange Server:

```
%WINDIR%\system32\inetsrv\adminsamples\ADSUTIL set SMTPsvc/1/PickupDirectory X:\exchsrvr\imcdata\Pickup
```

where X: is the drive where Exchange Server is installed. To revert back to the original IIS SMTP configuration run the "set" command again with the directory value displayed on the first command (e.g. c:\inetpub\mailroot\pickup).

On Windows 2003, "Smart Host" on the IIS SMTP Server allows the SMTP server to point to another mail server to forward its emails.

Improving IIS Performance

Occasionally, you may notice that Internet Information Service (IIS) loads Process Director pages very slowly. Normally when IIS starts an Application Pool, it checks the Certificate Revocation List (CRL) for managed assemblies that have an Authenticode signature to confirm that the signature is valid. Performing the CRL check requires the .NET framework to connect to the Internet to access the CRL. This can cause long delays in loading .NET applications in IIS.

Edit the Config file for ASP.NET to prevent IIS from checking the Certificate revocation List. . Turning the CRL check option off means that if a signed .NET application has it certificate revoked it will still load. This is usually fine, however, because a) you should already be properly managing the applications that are on your server, and b) anyone who has an access level that allows them to put a revoked application on your server already has enough access to perform far more malicious acts.

Open the config file for ASP.NET, which should be located in the root folder of the framework version you are using. For example, if you are running the .NET Framework v2.0, in the 64-bit environment, the config file should be found at:

```
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\aspnet.config
```

Edit the Config file to stop the CRL check by adding this tag to the `<runtime>` section of the config file:

```
<generatePublisherEvidence enabled="false"/>
```

Browser Issues

Underscore Bug

Some versions of Internet Explorer don't support domain names or server names with an underscore in the URL. While general browsing in IE still works, all session and browser cookies are ignored. With cookies ignored, login to Process Director using internal user names doesn't work. The product checks for underscores in the domain name to detect this problem. This is, however, a bug in Microsoft IE, not Process Director. Using Chrome, Firefox, or Safari will allow users to log in properly.

Integrated Browser Security Issues

There is a known IE problem that happens when some ASP pages in IIS are running “Integrated Browser Security” (NTLM) and other pages aren't (the other pages are just using normal anonymous user access). There are bugs in the browser that can cause posted form data to be stripped. In some cases it appears whenever the client cache is cleared (which can happen automatically on occasion, with things like virus scanners). The Microsoft Knowledge base contains an article discussing the problem. There are two ways to work around this problem.

Option 1

Use Regedt32 on the client machine and go to this branch:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet
```

On the Edit menu, Add Value name DisableNTLMPreAuth as a type REG_DWORD and set the data value to 1 (true).

Option 2

Configure all pages in your virtual directory to use “Integrated Browser Security”. This means that the logged in users won't be running as the “anonymous” user id (IUSR_hostname), but instead the web pages will be run under the context of the authenticated user.

"Internet Explorer can't display the webpage" error

A user sees the error “Internet Explorer can't display the webpage” on long running web page requests. Either remove the following registry key or set it to decimal 60000 on the CLIENT PC:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ReceiveTimeout
```

This may need to be repeated as certain applications may reset this to a 10000 (10 seconds). If this doesn’t work, you may want to try connecting to other, smaller pages and test your internet connection.

Microsoft Edge/Windows 10

A bug in Windows 10 and Microsoft Edge causes new windows to open *behind* parent windows, rather than on top of them. As a workaround, for Process Director v4.5, we have added the following line to the Custom Variables file:

```
bp.Vars.nFormOpenProps = FormOpenProps.UseFullScreen;
```

This will force JavaScript to open the new window in a maximized fashion, therefore pushing the new window to the top of the other windows.

This should be an acceptable temporary workaround until Microsoft corrects the bug.

Virus Scanners

Some virus scanners that are configured to scan in real-time can cause delays on the system. This tends to happen when they are monitoring the Process Director logs directory. Process Director will write audit logs and internal logs to the log files on disk. For example if you are using Microsoft Security Essentials you may see the CPU being used by “msmpeng.exe” when running Process Director forms and Process Timelines. If you are seeing this problem, exclude the following folder from the real-time scanning:

```
\Program Files\BP Logix\Process Director\website\App_Data\
```

This is the folder that contains the log files that are being written to when the system is being used.

TIFF Files

TIFF file formats aren't natively supported in most browsers. To display a TIFF file in a browser or embedded on a Form you must install a TIFF ActiveX viewer (e.g.

www.alternatiff.com, QuickTime, etc.). These viewers are provided by and supported by their respective companies. Once a TIFF viewer is installed on all users PC's, you can configure Process Director to display the TIFF files inline, instead of as a popup window in another application. This is done by adding the following lines to Process Director configuration file named vars.cs.ascx. Add to the PreSetSystemVars() function in vars.cs.ascx

```
bp.Vars.EmbedDocumentTypes.Add("tiff");
bp.Vars.EmbedDocumentTypes.Add("tif");
```

The vars.asp configuration file is located in the c:\Program Files\BP Logix\Process Director\website\custom\ directory.

DDE and Excel

If you are unable to open Excel documents from Process Director or, upon trying to open an Excel document, ensure that DDE is enabled in Microsoft Excel. See Microsoft's documentation on this error for more information and instructions on how to enable DDE.

You should also verify that Process Director is listed as a trusted site on Internet Explorer.

Document Downloading Issues

Process Director can store any file type. These files and documents can be viewed in the browser or downloaded to your PC. Windows Server, however, won't allow unregistered file types to be downloaded. The browser may display the following message:

HTTP Error 404 - File or directory not found.

For information on how to configure new file types in Windows IIS, refer to the Microsoft Knowledge Base article on this issue.

Installation with Multiple IP addresses

Using two NIC’s (IP addresses) that can connect to the product presents configuration choices. The ideal configuration is to have a single DNS name that all users can access. This problem can occur when trying to have different IP’s for the intranet and Internet access.

Here are some of the configuration options to connect to the product from multiple interfaces:

Option 1

If multiple interfaces exist and users can only access the server using one of them, you'll have to remove the “Interface URL” configuration from the installation settings. Additionally you'll have to modify all email templates to display two URL’s, one for accessing the system externally and the other for accessing the system internally.

Option 2

Use proxy DNS technique that uses the same name that point to different IP’s depending on where the user is located (e.g. internal users resolve the name to the internal IP, and external users resolve the name to the Internet address).

Coordinated Universal Time (UTC)

Process Director's internal timekeeping is always conducted in UTC, including all process timekeeping, start/end dates/times, etc. As such, Process Director doesn't store local times. Process Director will generally convert the UTC time to your local time automatically when the dates/times are displayed, but the actual saved dates are in UTC time (Greenwich Mean Time).

Resource Strings

Inside the Process Director interface, most control labels are generated by Resource Strings that are located in the Resources.resx file that is located in the %InstalDir%\website \App_GlobalResources folder. Occasionally, after a Windows Update reboot, this file will, for reasons still unknown, be deleted. If this occurs, you'll see an error message similar to the following:

Error processing source URL: http://xyz.bplogix.net/admin/admin.aspx

Source: System.Web

Message: The resource object with key '___somestring___' was not found

The other error you'll occasionally see is an exception accessing a function `toString()`, which is the system trying to retrieve a string resource from the Resources.resx file that can't be found.

To recover from these errors, just reinstall Process Director to restore the Resources.resx file.

Simultaneous Windows and LDAP Authentication

You can configure a Process Director installation to have both Windows and LDAP authentication enabled at the same time. To enable this, you have to **enable** Windows and LDAP authentication, but **disable** Integrated Windows authentication and **disable** the function that automatically adds users after they initially authenticate through Windows or LDAP. To configure the system in this way, the following flags must be set in the PreSetSystemVars() method of the custom variable file.

```
bp.Vars.fAuthTryAllAuthTypes = true;
bp.Vars.fAuthWindowsIntegrated = false;
bp.Vars.fAuthWindowsAutoAdd = false;
bp.Vars.fAuthLDAPAutoAdd = false;
```

Force TLS 1.2 on outgoing HTTP connections

For Process Director v5.34 and higher, the default the SSL cipher used for *outgoing* web requests will use TLS 1.2 instead of 1.0 or 1.1, which have been deprecated for security reasons. This can be changed back by setting this in the vars:

```
System.Net.ServicePointManager.SecurityProtocol = Sys-
tem.Net.SecurityProtocolType.Ssl3|Sys-
tem.Net.SecurityProtocolType.Tls;
```

AES Encryption for Process Director v5.44.700 and Higher

Process Director v5.44.700 and higher implements AES encryption. This encryption change provides higher security, but it does affect the migration process the first time--and ONLY the first time--you install v5.44.700 or higher from v5.44.600 or lower (except for load-balanced installations). Upgrading from v5.44.700 to any higher version will require no special action for most customers.

Please refer to the Upgrading to a Newer Version section of the Reinstall/Upgrades/Moving Hosts topic of the Installation guide, which covers the upgrade process for most customers.

Customers who manage a load-balanced installation are subject to some additional considerations, which are documented in the Installation Settings section of the Load Balancing, Standby, and Rendering Options topic of the System Administration Guide.

On-premise customers who decide NOT to upgrade to v5.44.700, should also make a specific change to their installation. BP Logix recommends that you manually edit your installation's web.config file to direct Internet Information Server to provide an auto-generated cryptographic key that will be unique to your installation.

To do so, you should edit the machineKey configuration setting in the system.web section of the web.config file so that it looks like the example highlighted in red below.

```
<configuration>
    // Some other configuration settings may appear here
    <system.web>
        <machineKey
            validationKey="AutoGenerate,IsolateApps" validation="HMACSHA512"
            decryptionKey="AutoGenerate,IsolateApps" decryption="AES" />
        // Some other configuration settings may appear here
    </system.web>
    // Some other configuration settings may appear here
</configuration>
```

Once you have made this change and saved the web.config file, the system will recompile and new AES encryption keys will be automatically generated for your installation.

Tenant-Based SharePoint Configuration

Tenant-based SharePoint installations have a complex and more cumbersome access model than Site-based installations. Tenant-based installations, therefore, require a different process to set up and configure:

1. Create a certificate to authenticate Process Director with Azure.
   a. Using Microsoft’s certreq.exe, installed on all modern Windows OS versions.
   b. Using PowerShell, also included with all modern Windows OS versions.
2. Add Process Director as a Registered Application in Azure.
   a. Add the public key certificate to the Process Director application in Azure.

b. Configure the appropriate Azure settings.

In this topic, we'll address each of these required steps in detail. Additional information about this topic can also be obtained from Microsoft's online documentation.

❗ You cannot configure any OAuth settings for SharePoint Datasources or SMTP Email in Process Director until you have created and registered an Azure Active Directory Application in Azure by completing the steps described in this topic.

Create a certificate to authenticate Process Director with Azure

Microsoft prefers the use of certificates for authentication. Each certificate includes both the public and private keys used to encrypt data. The public key (in a CER file) is used by SharePoint Online to authenticate Process Director. The private key is packaged in a password-protected PFX file and is used by Process Director to authenticate with Azure Services. There are two methods that can be used on Windows-based systems to create a proper certificate.

- Using Microsoft’s certreq.exe, installed on all modern Windows OS versions.
- Using PowerShell, also included with all modern Windows OS versions.

❗ Keep in mind that certificates expire after a set period of time. Most organizations specify the maximum length of time certificates should be used. By default, the instructions that follow will generate certificates valid for one year. You should, therefore, generate and install new certificates well before existing certificates expire. This implies that your organization also has a mechanism in place to be reminded when expiration is approaching, to ensure that service interruptions don't occur.

Creating a Certificate with certreq.exe

This method of certificate creation might be preferred if you’re less comfortable with command-line operations and don’t intend to automate the generation of certificates. Microsoft's online documentation has additional information about certreq.exe.

Instructions

First, using a text editor like Notepad, copy and paste the following text into a new document:

```
[Version]
Signature = "$Windows NT$"

[Strings]
szOID_ENHANCED_KEY_USAGE = "2.5.29.37"
szOID_KEY_ENCIPHERMENT = "1.3.6.1.5.5.7.3.1"

[NewRequest]
Subject = "cn=BP Logix Process Director"
MachineKeySet = false
KeyLength = 2048
HashAlgorithm = Sha1
Exportable = true
RequestType = Cert

KeyUsage = "CERT_KEY_ENCIPHERMENT_KEY_USAGE"
; The following values can be changed to generate certificates
that expire
; sooner or later depending on your organizations needs. The
default is 1 year.
ValidityPeriod = "Years"
ValidityPeriodUnits = "1"

[Extensions]
%szOID_ENHANCED_KEY_USAGE% = "{text}%szOID_KEY_ENCIPHERMENT%"
```

Once you've done so, save the document as an INF file in a folder on your system, e.g., `c:\Users\Some.User\Documents\PD Certificate\CertReq.inf`.

Open the Windows Command Prompt. You can press the [WINDOWS] key, type "cmd", then select the "Command Prompt" application.

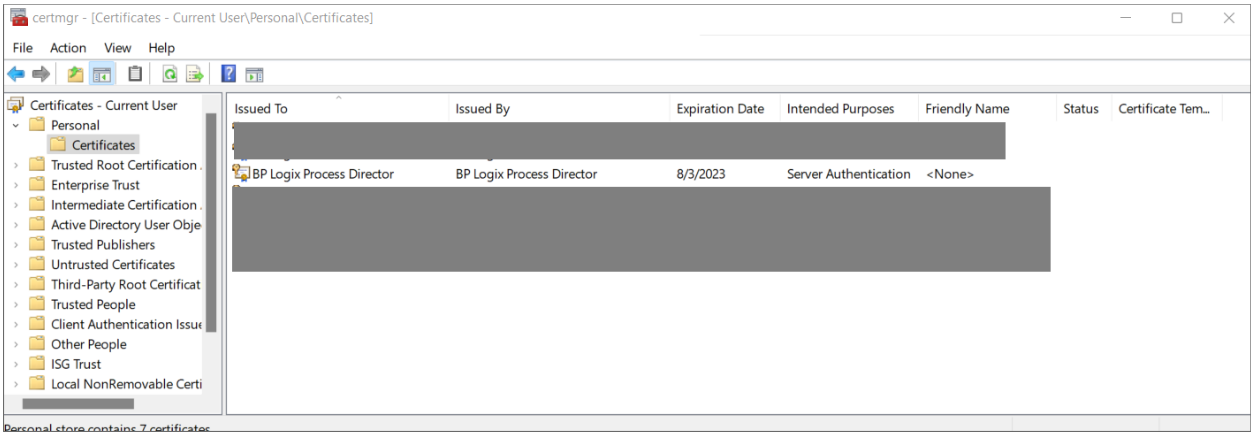
In the Command Prompt, open the directory in which you installed the INF by using the cd command, and the folder path to the INF file, then pressing the [ENTER] key. Using the example above, you'd need to type:

```
cd c:\Users\Some.User\Documents\PD Certificate\
```

Once the directory changes, type the following and press the [ENTER] key to run the certreq application.

```
certreq -new certreq.inf PublicKey.cer
```

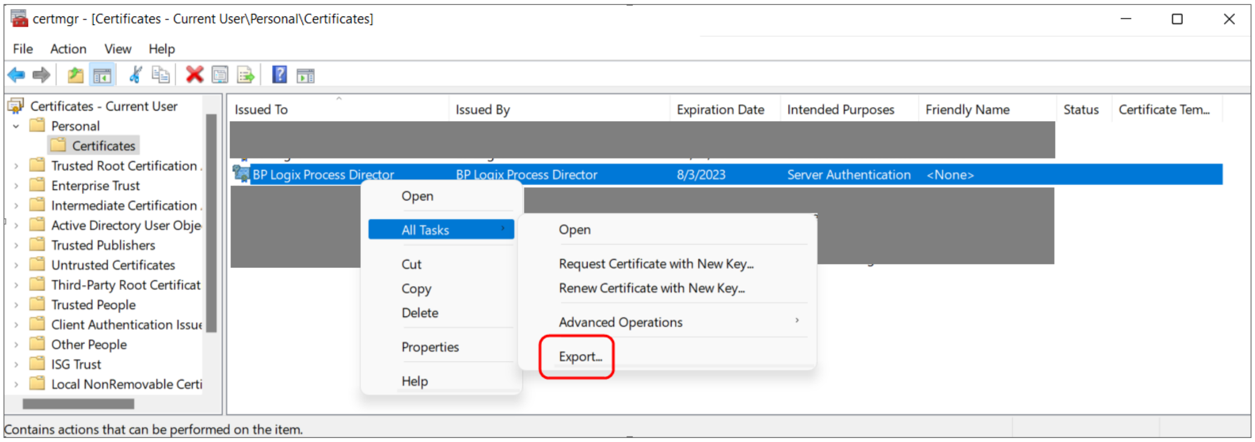
Running the certreq application will create the certificate, and add it to the Windows Certificate Manager. To continue, you'll need to open the Certificate Manager to access the new certificate. To open the Certificate Manager, you can press the [WINDOWS] key, type "certmgr", then select the "Manage computer certificates" option. When the Certificate Manager opens, you'll need to navigate to the `Personal\Certificates` folder, where you should see the certificate issued to and by BP Logix Process Director.


certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issue
Other People
ISG Trust
Local NonRemovable Certi

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
[redacted]						
BP Logix Process Director	BP Logix Process Director	8/3/2023	Server Authentication	<None>		
[redacted]						

Personal store contains 7 certificates.

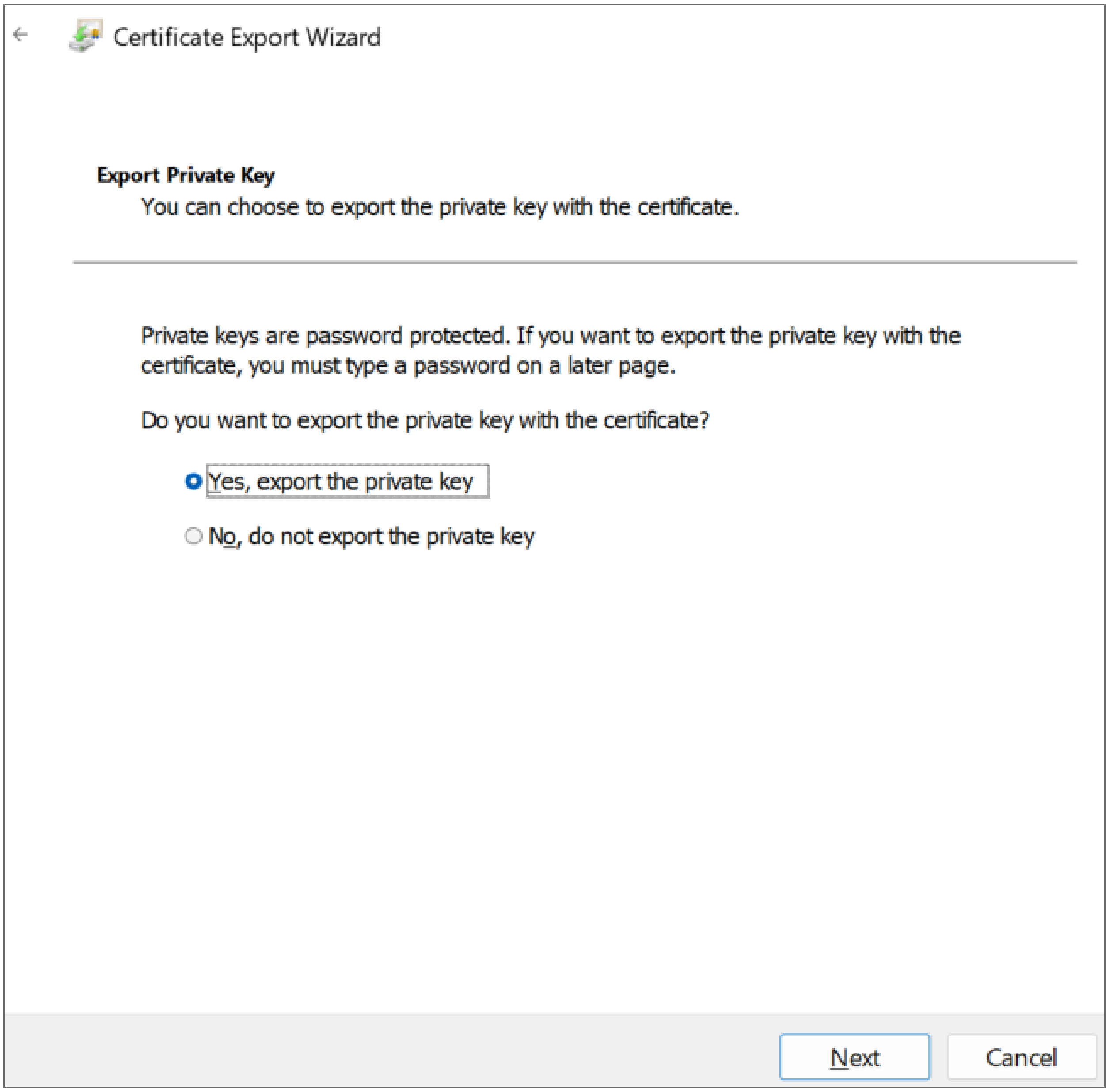
Right-click that certificate and then select All Tasks > Export.


certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issue
Other People
ISG Trust
Local NonRemovable Certi
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Advanced Operations
Export...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
[redacted]						
BP Logix Process Director	BP Logix Process Director	8/3/2023	Server Authentication	<None>		
[redacted]						

Contains actions that can be performed on the item.

The Certificate Export Wizard will open. On the first screen, click the Next button. On the Export Private Key screen, select Yes, export the private key, then click the Next button.



Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

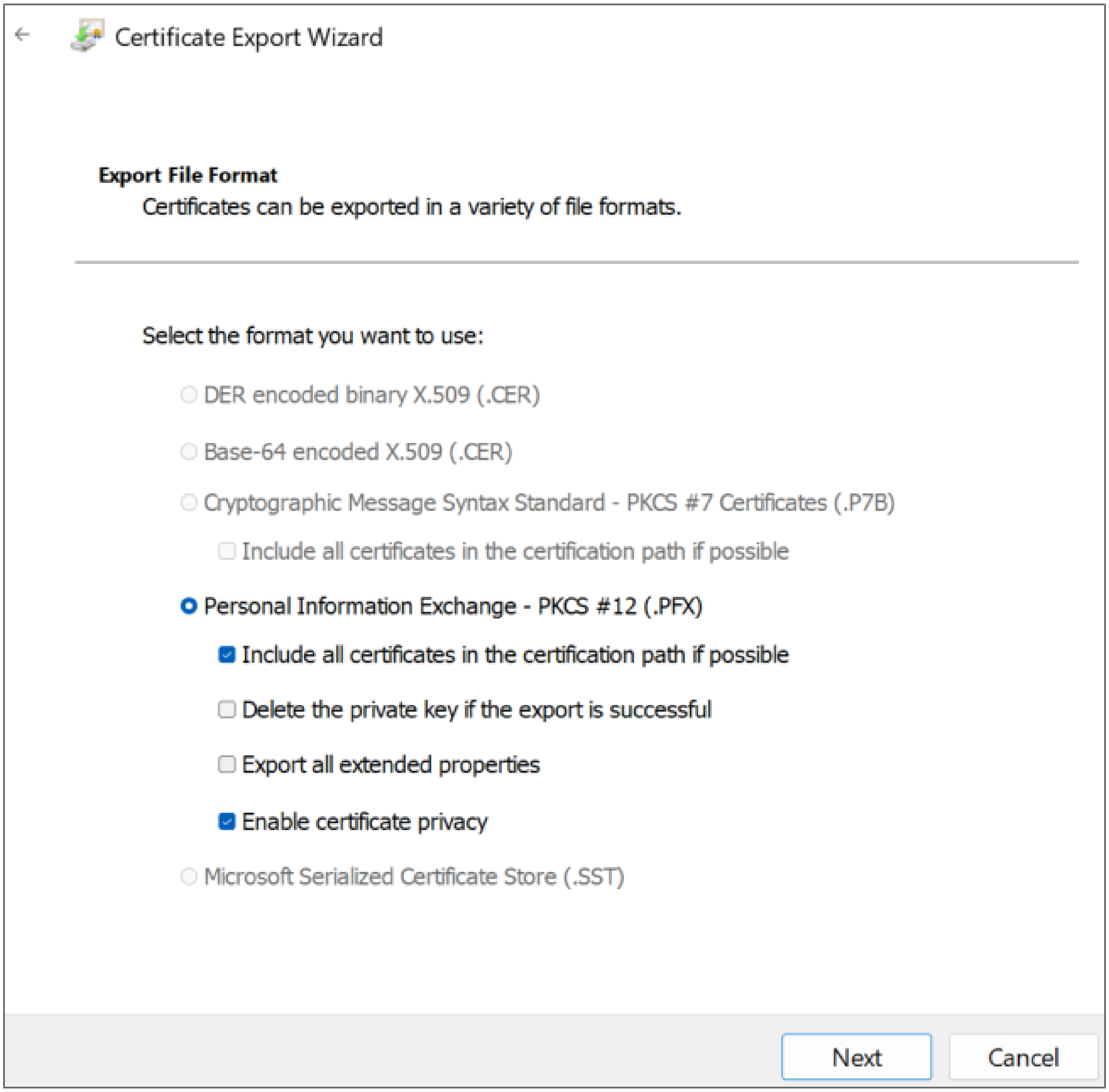
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

On the Export File Format screen of the Wizard, Ensure that you select the following options:

- Personal Information Exchange - PKCS #12 (.PFX)
- Include all certificates in the certification path, if possible
- Enable certificate privacy



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

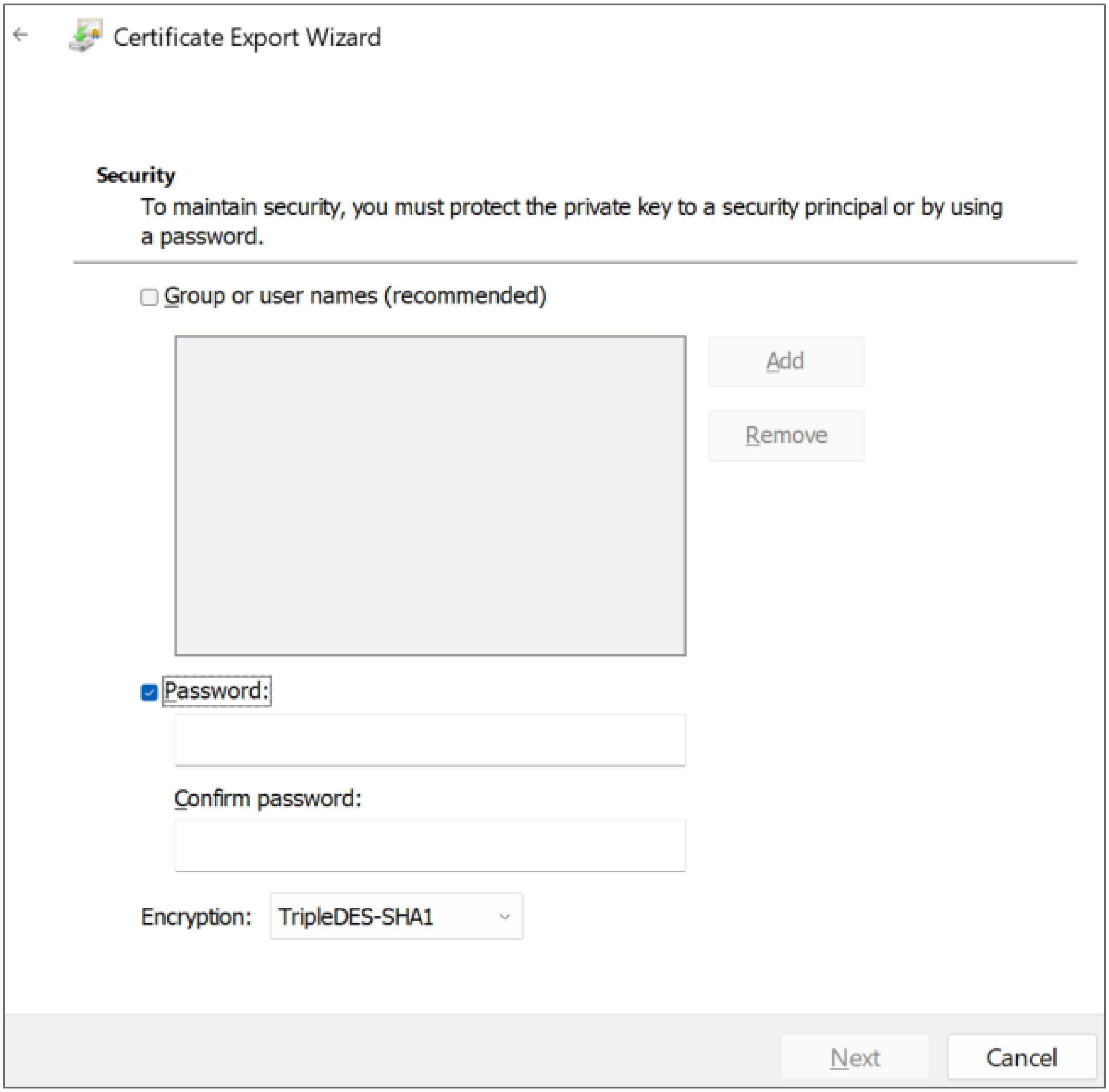
☑ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

On the Security screen, check Password as the security protocol and enter a password twice.

Be sure to store this password securely, you'll need it in future steps.

Be sure to use a long, sufficiently complex password in line with your organization’s cryptographic standards.



Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

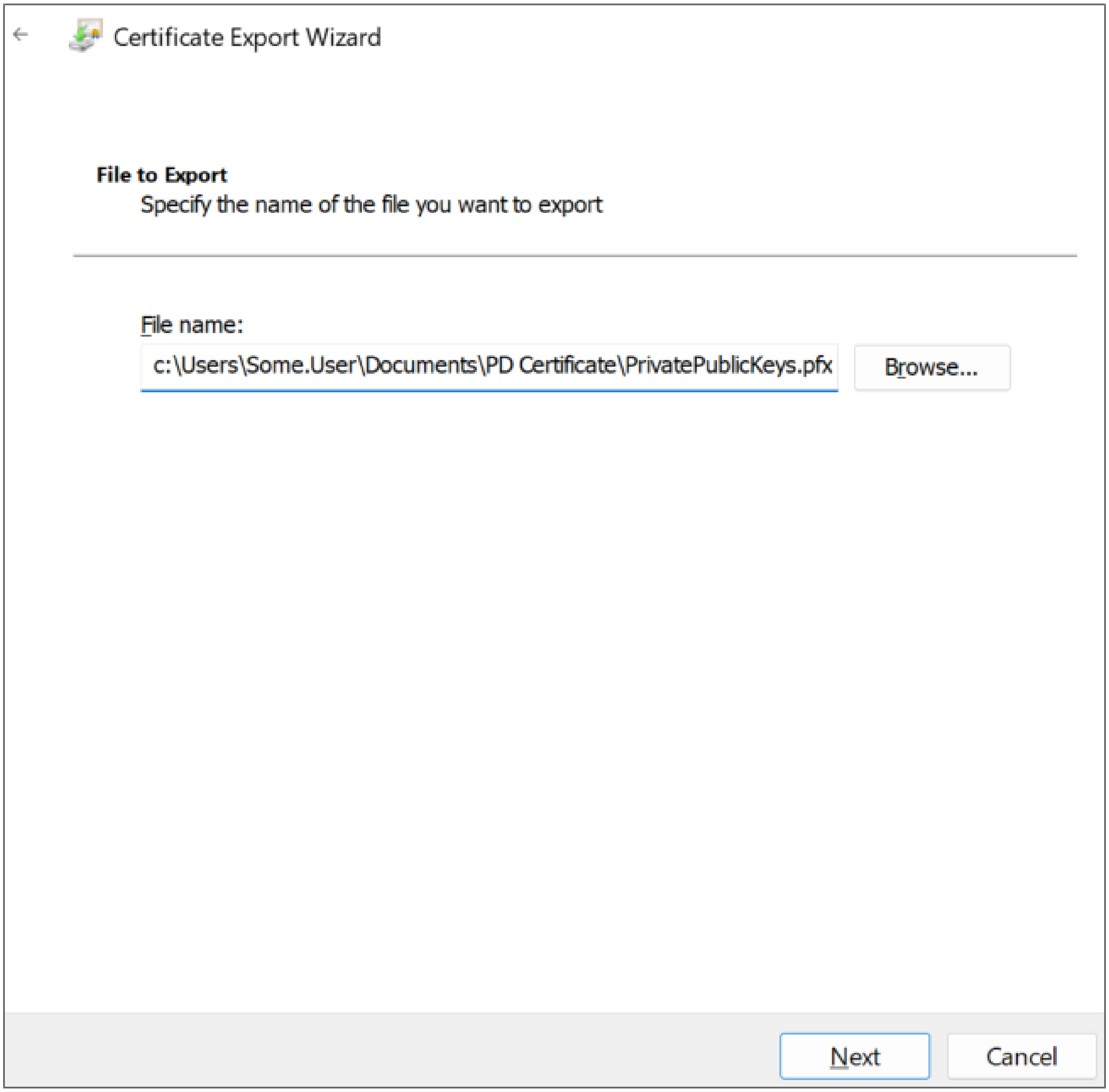
☐ Group or user names (recommended)

☑ Password:

Confirm password:

Encryption: TripleDES-SHA1

On the File to Export screen, store the resulting PFX file in the same folder as you stored the CertReq.Inf and PublicKey.Cer files, then click the Next button.



File to Export
Specify the name of the file you want to export

File name: c:\Users\Some.User\Documents\PD Certificate\PrivatePublicKeys.pfx

Click the Finish button on the next Wizard screen, then OK to finish the Wizard and close it.

BP Logix recommends that you remove the certificate installed in the Certificate Manager by right-clicking it and then selecting Delete followed by Yes to delete it in the confirmation dialog.

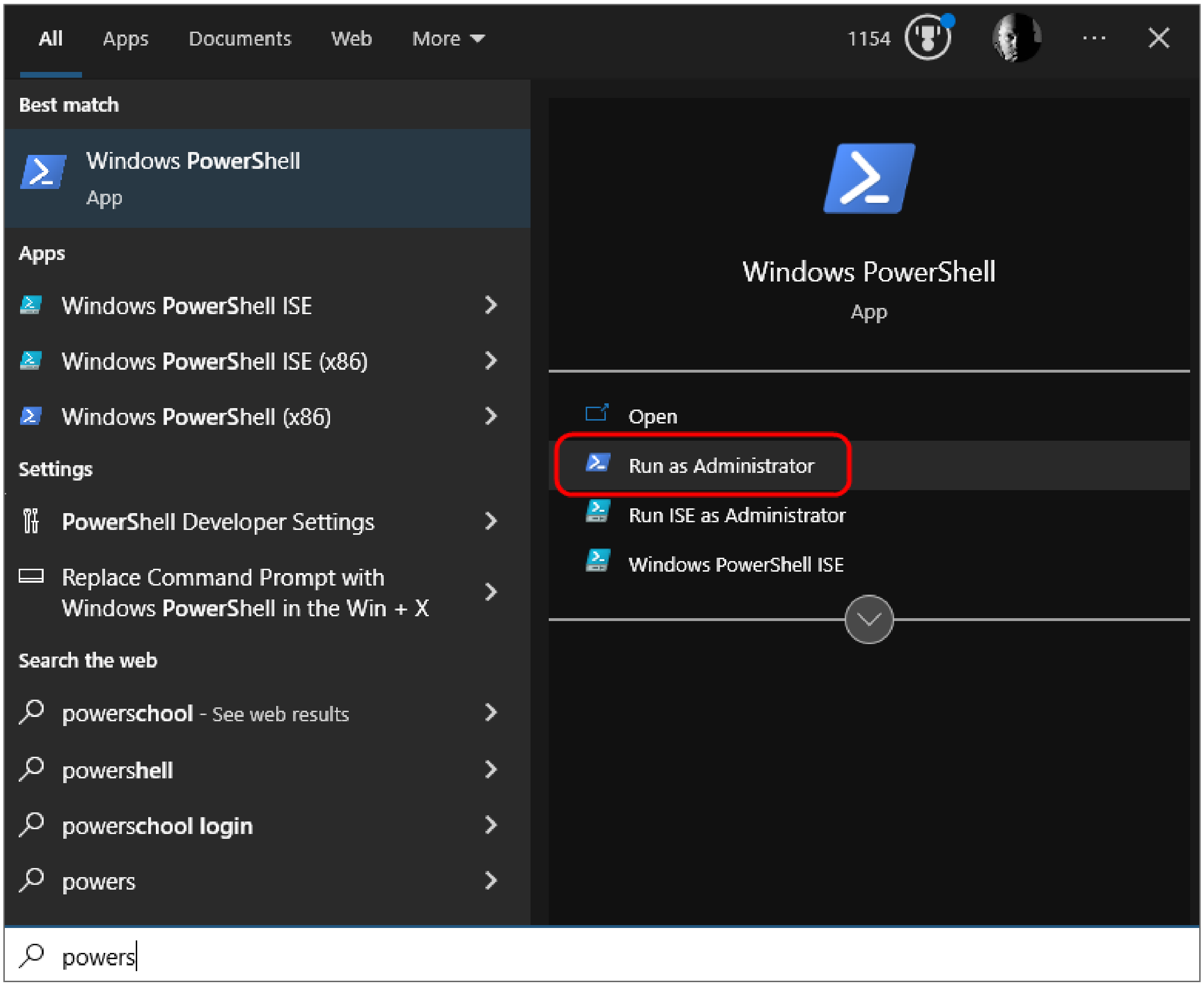
Keep both the PublicKey.cer and PrivatePublicKeys.pfx files handy for subsequent steps in this setup process. You should also archive them in a secure, backed up location as well.

Creating a Certificate with PowerShell

PowerShell is a command line application that's included with all modern versions of Windows. You can choose this method if you’re comfortable with PowerShell and might want to automate certificate generation on a recurring basis.

Instructions

Open PowerShell by pressing the [WINDOWS] key, typing "PowerShell" then selecting the Run as Administrator option to open Windows PowerShell.



In PowerShell, create or navigate to the directory you'd like to use to store the certificate files. Once you're in the desired directory, run the following command:

```
$cert = New-SelfSignedCertificate -CertStoreLocation Cer-
t:\LocalMachine\ -KeyUsage KeyEncipherment
    -KeyAlgorithm rsa -KeyLength 2048 -subject "BP Logix
```

```
Process Director"
    -DnsName "BP Logix Process Director" -Type SSLServer-
Authentication
    -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1")
```

Next, run these commands in PowerShell, replacing `<password>` with a password of your choosing. Ensure the passowrd is cryptographically secure, in accordance with your organization’s standards. Be sure to also store this password securely, as you'll need it in future steps.

```
$pwd = ConvertTo-SecureString -String '<password>' -Force -
AsPlainText
$path = 'cert:\LocalMachine\My\' + $cert.Thumbprint
```

Finally, run these commands to create the .PFX and .CER files. Modify the `<path>` value to store the file in a location of your choosing.

```
Export-PfxCertificate -cert $path -FilePath <path>\Priv-
atePublicKeys.pfx -Password $pwd
Export-Certificate -cert $path -FilePath <path>\PublicKey.cer
```

Keep both the PublicKey.cer and PrivatePublicKeys.pfx files handy for subsequent steps in this setup process. You should also archive them in a secure backup location as well.

Add Process Director to Azure

To add Process Director as an application in your Azure Active Directory portal at the Tenant level, complete the steps below after signing into your Azure portal (portal.azure.com):

1. Register Process Director as an Application

A. If you have access to multiple tenants, use the Directories + subscriptions filter in the top menu to switch to the tenant in which you want to register the application.
B. Search for and select Azure Active Directory.
C. Under Manage, select App registrations > New registration.
D. Enter a display Name for your application, e.g., “Process Director”. This name can be changed later, if needed.

E. Specify who can use the application. Typically, only accounts in this organizational directory should be used. See the Microsoft documentation titled Quickstart: Register an application with the Microsoft identity platformfor more information.
F. Add the Redirect URI, which is the URI for your Process Director installation, e.g., https://myorg.bplogix.net.
G. Click the Register button to register the application.

2. Add Your Public Key Certificate

To add your public key certificate to the Process Director application in Azure, complete the steps below.

A. In the Azure portal, in App registrations, select the Process Director application you created previously, e.g., “Process Director”, as in step 1D, above.
B. Select Certificates & secrets > Certificates > Upload certificate.
C. Select the PublicKey.cer file you created earlier.
D. Upload the certificate file to Azure.

Your AAD Application should now be properly registered and secured with a certificate.

Conclusion

Congratulations! Assuming that you've correctly followed the instructions above, you've now configured an Azure Integration with Process Director. To complete the integration, you'll need to perform some additional, specialized configuration in Azure, which is covered in the Create a Sharepoint data source topic.

SharePoint Data Sources

The purpose of the SharePoint data source is to connect to a SharePoint List to retrieve documents or data. **This datasource is a core feature of the product, and is *not* related to the use of the Collaborative Document Authoring (CDA) feature with Microsoft 365 (M365) in any way.** CDA for M365 is a separately licensed feature, with its own setup and configuration process.

With the implementation of Microsoft's move to **Modern Authentication**, using the Microsoft identity platform, logging into cloud-based versions of SharePoint is no longer possible by simply using a user name and password. Legacy installations that user older versions of SharePoint may still do so, but SharePoint has largely implemented an OAuth-based authentication scheme, with additional security provided by the use of encryption certificates.

In Process Director v5.44.1000, Modern Authentication for SharePoint was implemented using the SharePoint OAuth Datasource, which only gives access to SharePoint at the Tenant (organizational) level.

For Process Director v5.44.1103, The SharePoint OAuth Datasource was renamed to SharePoint OAuth (Tenant), while a new Datasource SharePoint OAuth (Site), was added to give access to SharePoint at the Site level, rather than at the entire tenant.

The existing SharePoint Datasource, which uses the simple username/password authentication scheme, is still available for customers who are using older versions of SharePoint. This legacy authentication method should be relevant to only a very small minority of customers, and has been renamed to SharePoint Legacy.

❗ This update to the SharePoint Datasources will require updating the SharePoint Custom Tasks!

Configuring a SharePoint OAuth (Tenant) Datasource

Modern Authentication provides much more secure access to SharePoint, but does require a more complex setup process for Tenant-based SharePoint installations.

Create the Registered Application for the Tenant

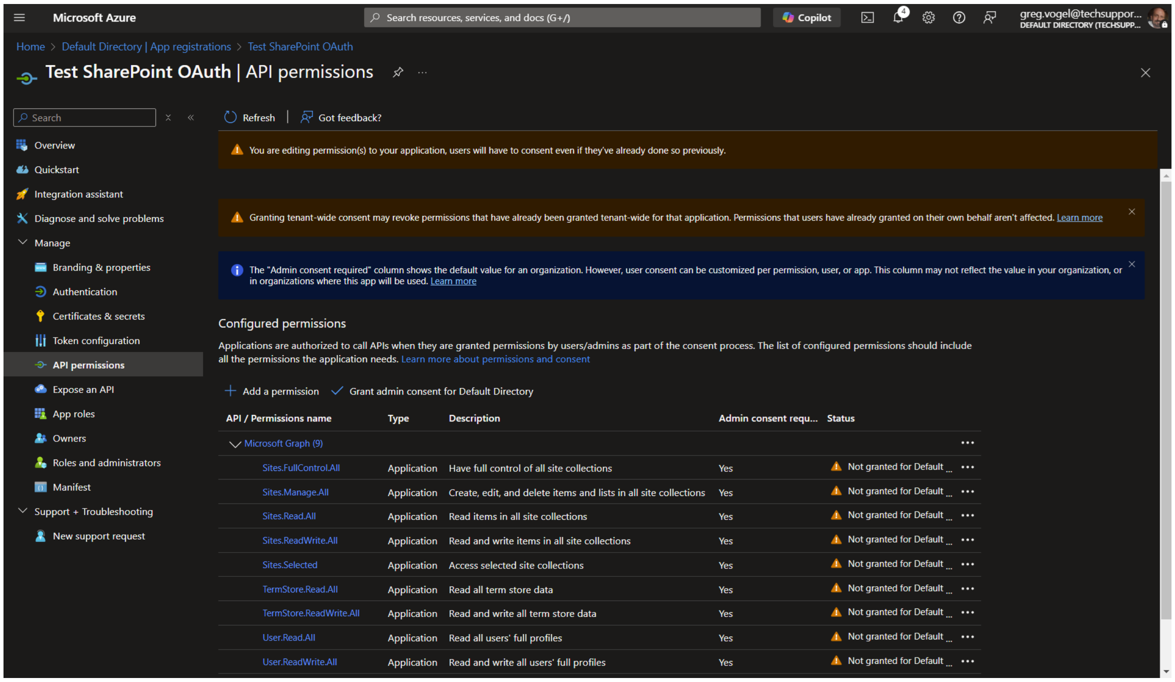
To set up Modern Authentication between SharePoint and Process Director, you must first create a Registered Application in Microsoft Entra. Please see the Tenant-Based SharePoint Configuration topic for instructions on how to complete this task.

Once you've created the Registered Application, you can begin the process for configuring SharePoint Online, as described below.

Configure SharePoint Online permissions

To configure the application to use SharePoint with Process Director, you'll need to perform the following configuration steps:

1. If you have access to multiple tenants, use the Directories + subscriptions filter in the top menu to switch to the tenant in which you want to register the application.
2. Search for and select Azure Active Directory.
3. Under Manage, select App registrations, then select your Process Director application. In this example, we'll use “Test SharePoint OAuth” as the Registered Application name, though, of course, the name you use may vary.
4. Click API permissions.
5. Click Add a permission and add all permissions displayed below to the SharePoint section of the API Permissions area:



You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. Learn more

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for Default Directory

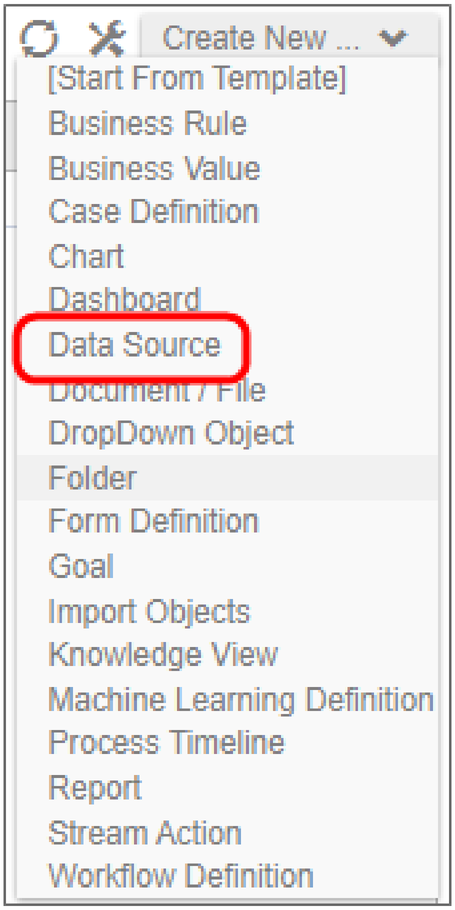
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (9)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	Not granted for Default ...
Sites.Manage.All	Application	Create, edit, and delete items and lists in all site collections	Yes	Not granted for Default ...
Sites.Read.All	Application	Read items in all site collections	Yes	Not granted for Default ...
Sites.ReadWrite.All	Application	Read and write items in all site collections	Yes	Not granted for Default ...
Sites.Selected	Application	Access selected site collections	Yes	Not granted for Default ...
TermStore.Read.All	Application	Read all term store data	Yes	Not granted for Default ...
TermStore.ReadWrite.All	Application	Read and write all term store data	Yes	Not granted for Default ...
User.Read.All	Application	Read all users' full profiles	Yes	Not granted for Default ...
User.ReadWrite.All	Application	Read and write all users' full profiles	Yes	Not granted for Default ...

Create the SharePoint OAuth (Tenant) Datasource

Now that the application has been fully registered in Azure, and the appropriate SharePoint API permissions have been set, you can create the SharePoint OAuth Datasource in Process Director. Be sure to keep the Azure window open, however, as you'll need to transfer some information from Azure to configure the SharePoint OAuth Datasource. Ensure you've opened the Entra admin center window to the Overview tab of the App registrations page of your Process Director integration app. In this example, we'll use the "Test SharePoint OAuth" application we used in the steps above.

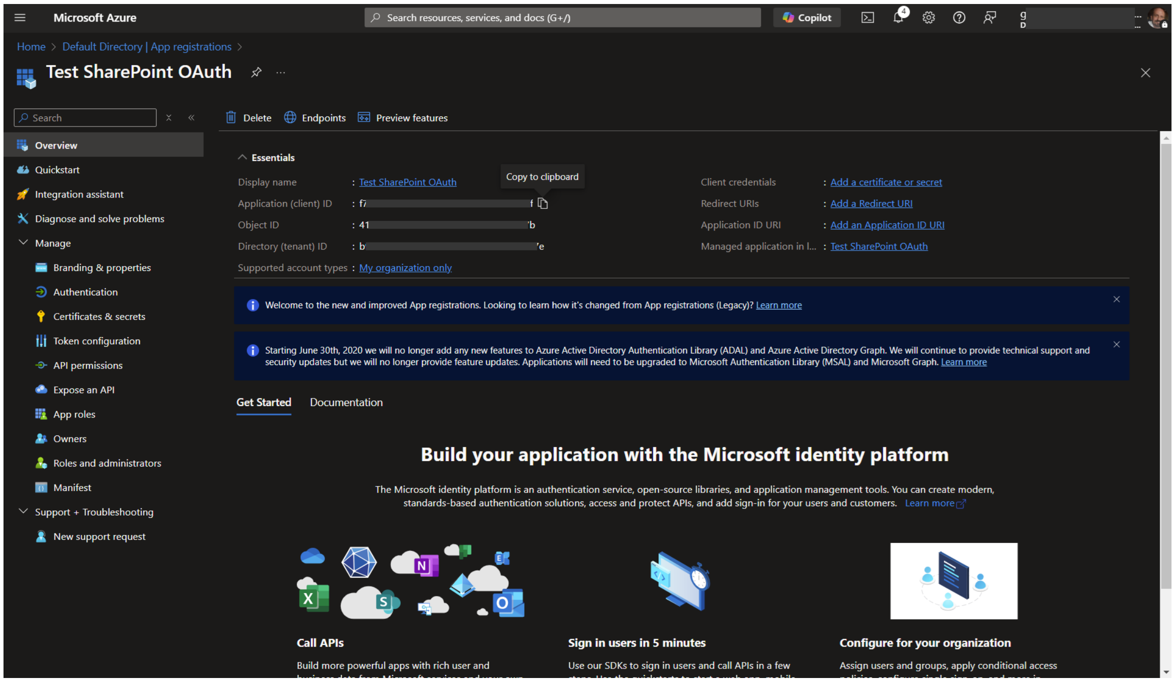
Instructions

1. Navigate to the Process Director folder in which you want to store the new Datasource, then select Data Source from the Create New menu.



2. In the Create New Data Source screen, enter an Name for the Datasource, then click the OK button to create the Datasource and open its configuration screen.
3. On the Properties tab of the Datasource definition, change the Datasource Type to "SharePoint OAuth (Tenant)".
4. Set the SharePoint Site URL to the URL your SharePoint Online server.
5. To set the Client ID property, go to the Azure window, and using the "Copy to Clipboard" icon, copy the value in the Application (client) ID property, then

paste it into the Client ID Property of the Datasource definition.



Display name : Test SharePoint OAuth
Application (client) ID : f7[redacted]f
Object ID : 41[redacted]b
Directory (tenant) ID : b[redacted]e
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : Test SharePoint OAuth

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

Call APIs

Build more powerful apps with rich user and

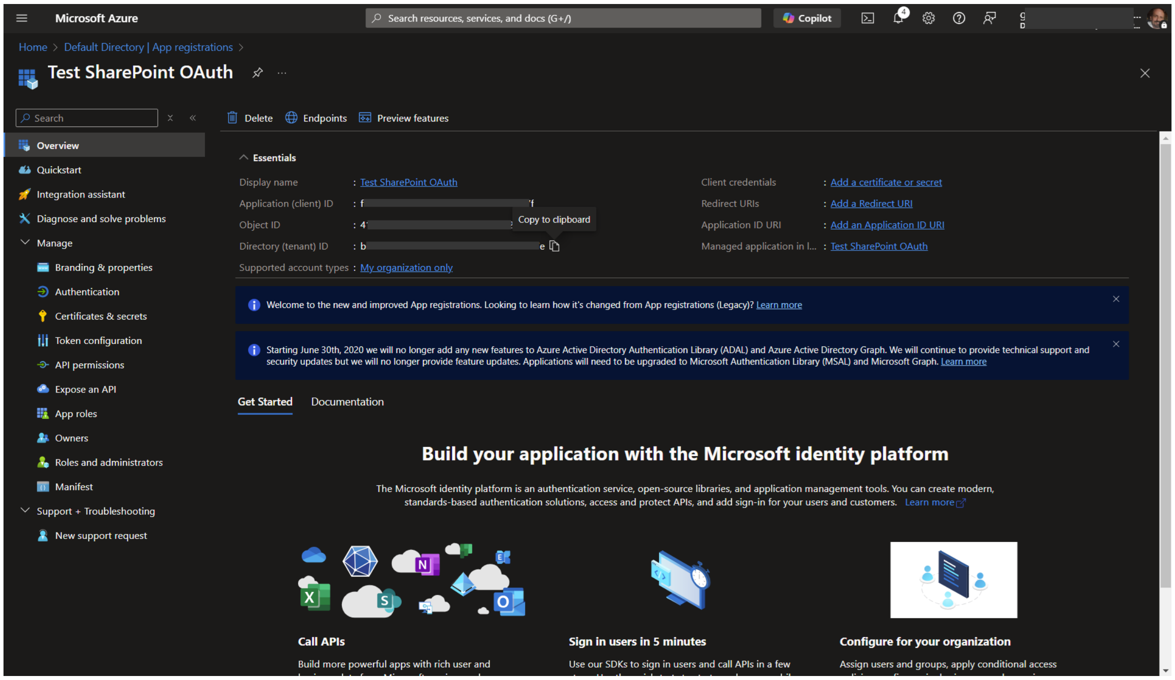
Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few

Configure for your organization

Assign users and groups, apply conditional access

6. Similarly, you'll need to copy the value of the Directory (tenant) ID property in Azure to the Tenant ID property of the Datasource definition.



Display name : Test SharePoint OAuth
Application (client) ID : f[redacted]f
Object ID : 4[redacted]
Directory (tenant) ID : b[redacted]e
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : Test SharePoint OAuth

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

Call APIs

Build more powerful apps with rich user and

Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few

Configure for your organization

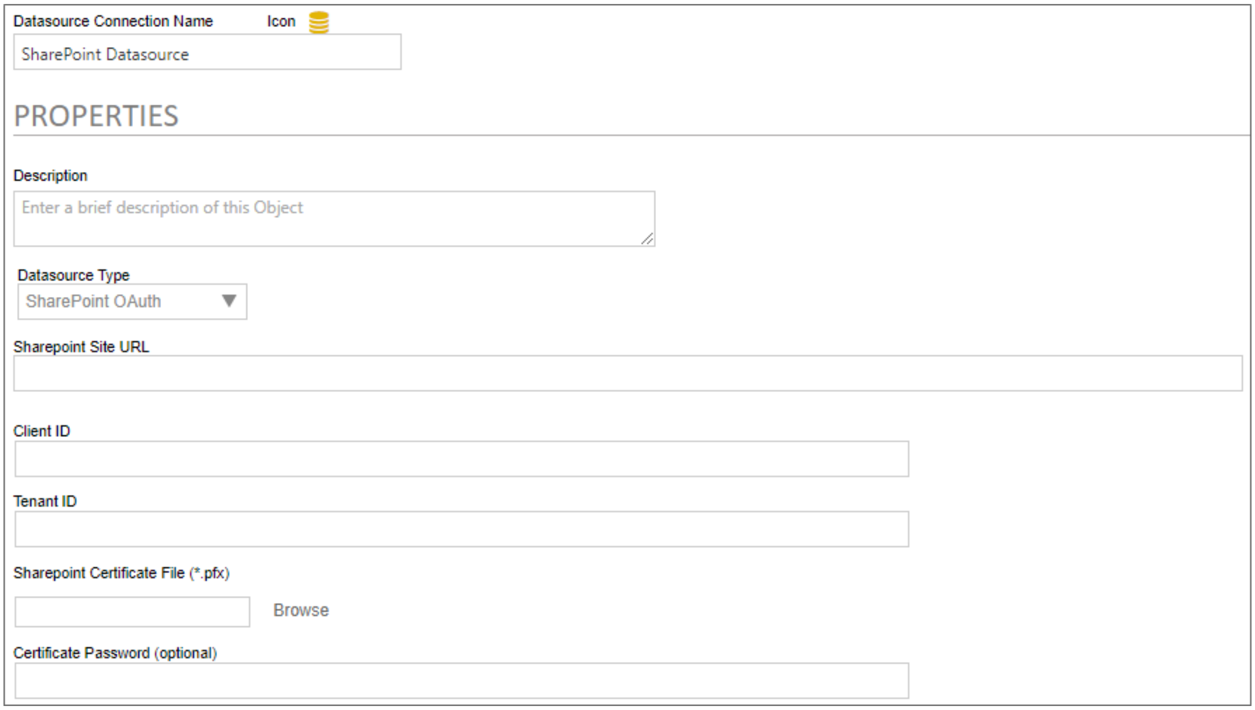
Assign users and groups, apply conditional access

7. To set the certificate to use for this Datasource, click the Browse button for the SharePoint Certificate File property, then locate and select the

PrivatePublicKeys.pfx file you created earlier (either with certreq.exe or PowerShell).

8. Enter the certificate Password that you created for the PrivatePublicKeys.pfx file.
9. Click the OK button to save your changes, then update the Datasource definition by selecting Update from the OK dropdown menu at the upper right corner of the page.
10. Click the Test Connection button to ensure that the Datasource can connect properly to SharePoint.

SharePoint OAuth (Tenant) Datasource Properties



Datasource Connection Name: SharePoint Datasource

Icon

PROPERTIES

Description: Enter a brief description of this Object

Datasource Type: SharePoint OAuth

Sharepoint Site URL

Client ID

Tenant ID

Sharepoint Certificate File (*.pfx)

Certificate Password (optional)

In addition to the standard Description property, setting the Datasource Type property to *SharePoint OAuth* enables configuration of the connection properties listed below.

SharePoint Site URL

The fully-qualified URL that connects to the SharePoint installation.

Client ID

The value of the Application (client) ID property contained in the App Registration screen in Azure.

Tenant ID

The value of the Directory (tenant) ID property contained in the App Registration screen in Azure.

SharePoint Certificate File

A Content Picker than enables you to browse to and upload the certificate (.PFX) file to Azure.

Certificate Password

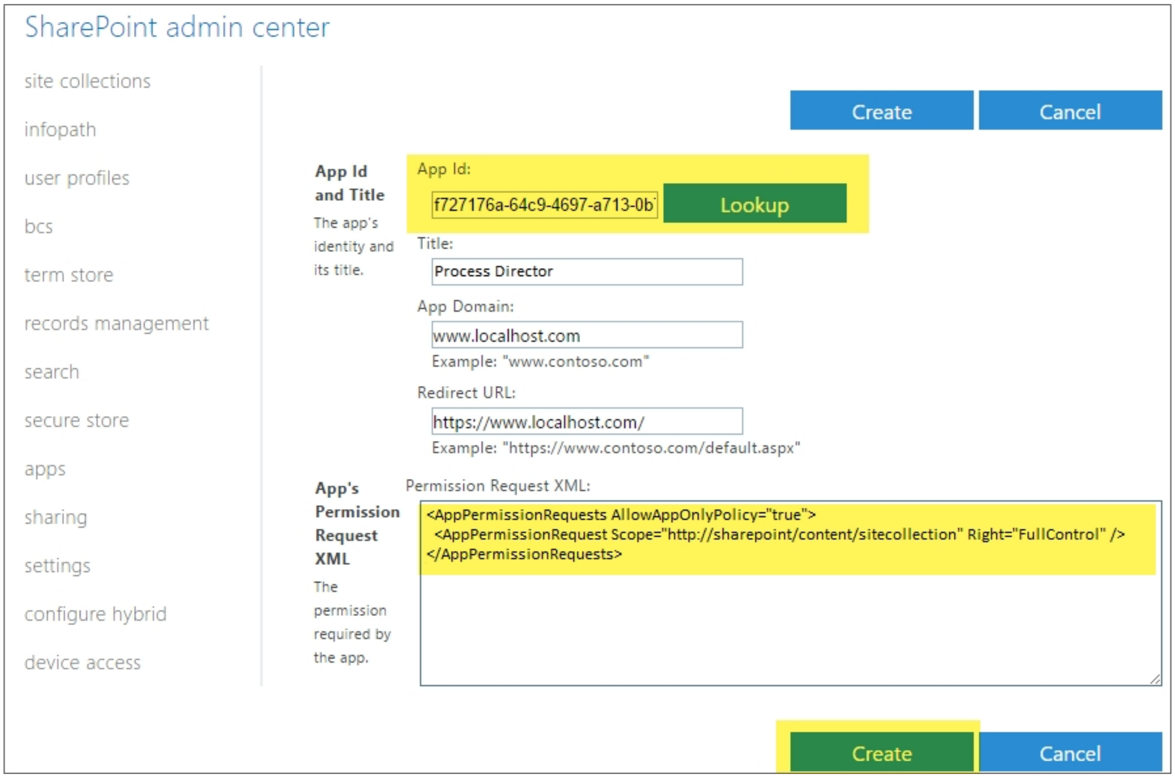
The password that you configured for the certificate (.PFX) file when you created it.

Configuring the SharePoint OAuth (Site) Datasource

Configuring the SharePoint OAuth (Site) Datasource is far less complex than configuring the tenant-level Datasource, and requires no certificate to be created or uploaded to Azure. To add Process Director as an application in your Azure Active Directory portal at the Site level, complete the steps below after signing into your Azure portal (portal.azure.com):

1. Configure SharePoint Site Permissions

1. Navigate to the site you want to configure access for in your tenant. This is typically of the form `https://mytenant.sharepoint.com`, replacing “mytenant” with the appropriate name.
2. Adjust the URL to `https://mytenant.sharepoint.com/_layouts/15/appregnew.aspx`.
    a. Click the buttons to generate both a Client Id as well as a Client Secret.
    b. Select the Client Id value, copy the text and store the value somewhere safe to be used in later steps in this guide.
    c. Select the Client Secret value, copy the text and store the value somewhere safe to be used in later steps in this guide.
3. Now you need to grant permissions to newly registered app (AKA principal). Navigate to
   `https://mytenant-admin.sharepoint.com/_layouts/15/appinv.aspx`.
   It’s important to note the addition of “-admin” to your site's normal name.



App Id and Title
The app's identity and its title.

App Id: f727176a-64c9-4697-a713-0b

Title: Process Director

App Domain: www.localhost.com
Example: "www.contoso.com"

Redirect URL: https://www.localhost.com/
Example: "https://www.contoso.com/default.aspx"

App's Permission Request XML
The permission required by the app.

Permission Request XML:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
 <AppPermissionRequest Scope="http://sharepoint/content/sitecollection" Right="FullControl" />
</AppPermissionRequests>
```

a. Add your Client Id as App Id.
b. Add the XML as shown, reproduced here to aid in copy and paste. Note, there are other, more restrictive options that can be considered listed in Table 1 at Microsoft's documentation topic, Add-in permissions in SharePoint. Be careful using other values as it may prevent Process Director from working correctly.

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
     <AppPermissionRequest Scope-
e="http://sharepoint/content/sitecollection" Right-
t="FullControl" />
</AppPermissionRequests>
```

c. Set the Title to “Process Director”.
d. Set App Domain to the fully qualified domain name of you Process Director deployment.
e. Set the Redirect URL to the URL of your Process Director deployment.

4. Click Create.
5. Click Trust It in the follow-up prompt.

2. Configure the Datasource

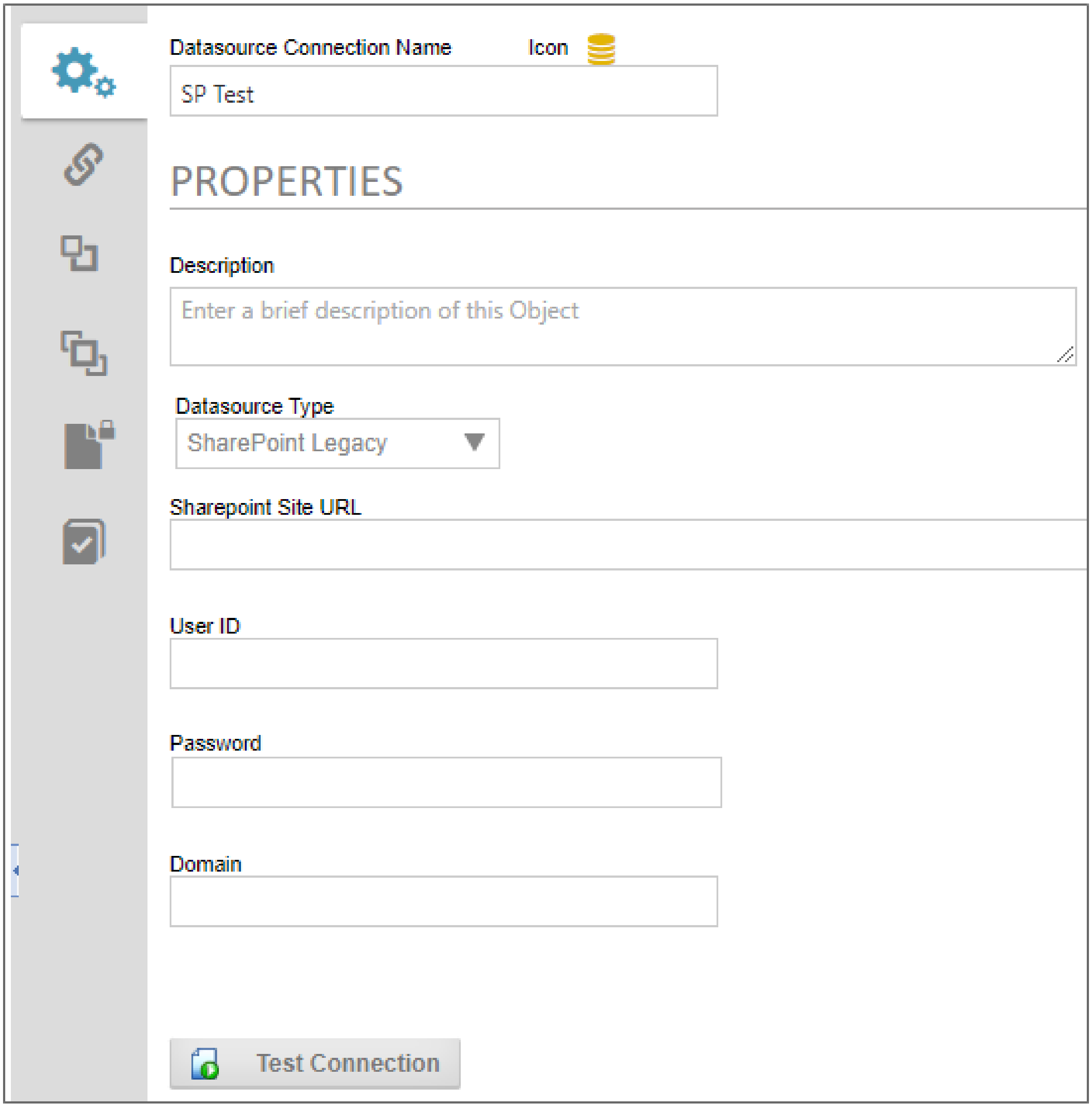
1. In a Process Director Content List folder, select Data Source from the Create New menu.
2. Supply a Name and click OK to open the new Datasource definition.
3. Set the Datasource Type drop-down to "SharePoint OAuth (Site)".
4. Add the SharePoint Site URL for your SharePoint Online installation.
5. Add the Client ID (AKA Application Id) and Client Secret from SharePoint that you set aside in the steps for **Configure SharePoint Site Permissions** above.
6. Click OK then select the Update item from the OK menu at the top right corner of the page to save the configuration.
7. Click theTest Connection button to test your connection to the SharePoint site.

A successful test means that your Datasource is correctly configured and is connecting to the SharePoint site correctly.

Assuming that you've correctly followed the instructions above, you've now configured both SharePoint Online and Process Director. You can now use this Datasource and the SharePoint Custom Tasks in Process Director to integrate your SharePoint sites and data with Process Director.

Sharepoint Legacy Datasource

For connections to pre-OAuth versions of SharePoint, the SharePoint Legacy datasource type enables you to create a datasource connection to the SharePoint server.



Datasource Connection Name: SP Test

Icon

PROPERTIES

Description: Enter a brief description of this Object

Datasource Type: SharePoint Legacy

Sharepoint Site URL

User ID

Password

Domain

There are four properties to configure to create this datasource.

The Sharepoint Site URL property enables you to enter the fully qualified URL of the Sharepoint server to which you wish to connect.

The User ID must be the user ID for a valid SharePoint User, while the Password property will be the password for the specified user. The Domain property is the SharePoint domain that contains the specified user.

Once you've configured the datasource, you can click the Test Connection button and a message banner will appear, notifying you whether the connection was successful.

Other Datasource Types

To see more information about different Datasource Types and their configuration, please refer top the following topics:

- **Common Datasources**
- **Excel Datasources**
- **File Datasources**
- **Social Datasources**

Microsoft OAuth for SMTP

To configure integration between Azure and Process Director, you'll first need to create an Registered Application for Process Director, if you do not have one. Once the Registered Application has been created, you'll need to perform some additional configuration to the Registered Application's settings in Azure.

First, in the Authentication area, you'll need to set the Allow public client flows property to: `Yes (On)`

Unfortunately, there are many factors that might impact the remaining Registered Application settings you'll need to use. Since that is so, you may wish to reference Microsoft's explanation of SMTP OAuth implementation.

Depending on your Azure installation, as well as your organization's policies, there are different configuration settings that you might need to implement, in order to enable your Registered Application to enable Process Director to use OAuth to send mail messages. **BP Logix cannot, therefore, definitively describe what settings might be required to make your Azure installation accept OAuth authentication, as we have no knowledge of, or access to, your Azure configuration.**

We strongly recommend that you refer to the Microsoft documentation topic on this subject: How to set up a multifunction device or application to send emails using Microsoft 365 or Office 365.

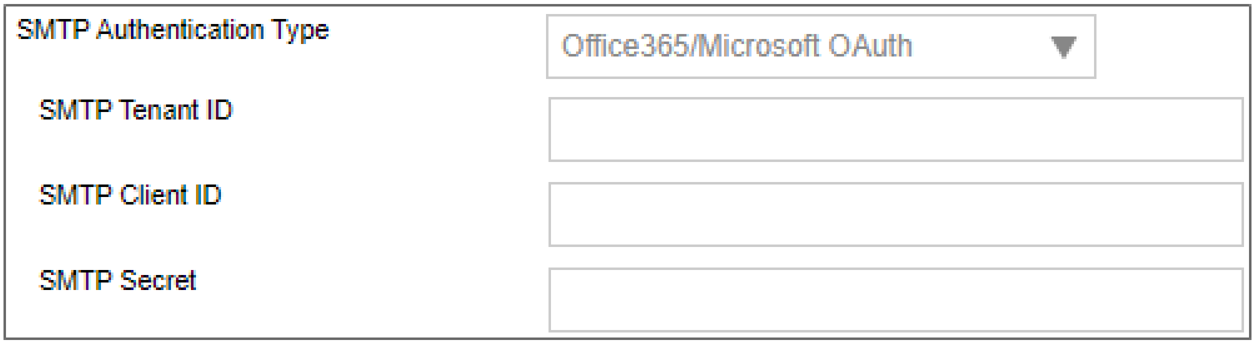
We can provide some common configuration suggestions that have worked for our customers in the past, though ***we cannot guarantee that these settings will work with your specific Azure configuration***.

1. If it's available for your Azure installation, in the Office 365 Exchange Online section of the API Permissions area, you can set the permissions `SMTP.AccessAsUser.All`. This setting is not available for all installations. This setting seems to have been deprecated for recent installations of Azure, in lieu of #2, below.
2. In the Office 365 Exchange Online area, enable the `SMTP.SendAsApp` property. You may also need to enable `IMAP.SendAsUser.All` to true.
3. In the Microsoft Graph section of the API Permissions area, you can enable the following permissions: `Microsoft.Graph Delegated SMTP.Send` and `Delegated User.Read`.
4. For more comprehensive email access, you can set `Microsoft.Graph Delegated IMAP.AccessAsUser.All`.

If no combination of the settings above work for you, you may need to contact your Microsoft Azure technical support representative to assist you with configuring the correct AAD App permissions for your installation.

> ⓘ **For more information on authentication permissions, please refer to the Microsoft Graph Permissions Reference from Microsoft. Please be aware that BP Logix has an extremely limited ability to assist you with troubleshooting your Azure installation or settings.**

Once configured, you'll need to get the following properties from the Registered Application's settings to transfer to the corresponding OAuth settings for the "Office365/Microsoft OAuth" SMTP Authentication Type, which is found on the Properties page of the Installation Settings section of the IT Admin area.:



SMTP Authentication Type	Office365/Microsoft OAuth ▼
SMTP Tenant ID	
SMTP Client ID	
SMTP Secret	

1. SMTP Tenant ID
   1. The ID of the Azure Tenant in which the Registered Application resides (Creation of a Registered App requires the existence of a Tenant)
   2. The Tenant ID is displayed as the Directory (tenant) ID property on the Overview page of your Registered Application in Azure, but this value will also be displayed following `login.microsoft.com/...` in the Endpoint URLs that the App references
2. SMTP Client ID
   1. The ID of the Registered Application
   2. This value is displayed as the Application (client) ID property on the Overview page of your Registered Application.
3. SMTP Secret
   1. The client secret or application password the administrator created to use with the Registered Application.
4. UserID/Password
   1. Some installations may require that you provide a valid UserID and Password to connect to an email account on your system for sending mail messages, as part of the authentication.

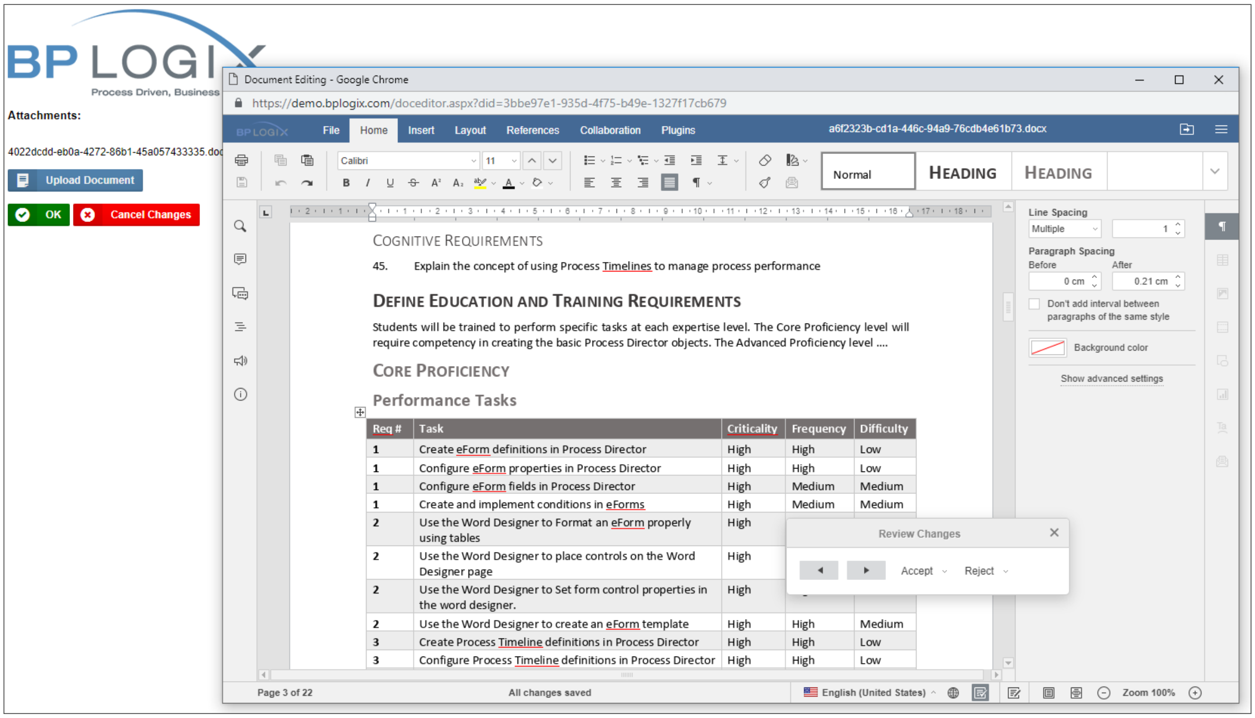
Some Azure configurations may also be configured to require a specific email address be used to send ***all*** mails as the "From" email address. In that case, you will *at least* need to go to the Global Variables page and set the Workflow From Email Address property to the email address you've specified in Azure. You may also wish to set that email address for the Registered Email property on this page (Properties), as a backup to the Global Variables setting.

Be advised that, with this configuration, ALL email addresses sent from the system MUST use the specified email address as the From address. This means that any custom email addresses you configure elsewhere, such as the "From Email" property of a Email Data control in an email template, *will not send email messages*.

Collaborative Document Authoring

For users of Process Director v5.13 and higher, document attachments may be annotated using Collaborative Document Authoring.

Collaborative Document Authoring is a separately licensed component that is only available for Cloud installations.



COGNITIVE REQUIREMENTS

45. Explain the concept of using Process Timelines to manage process performance

DEFINE EDUCATION AND TRAINING REQUIREMENTS

Students will be trained to perform specific tasks at each expertise level. The Core Proficiency level will require competency in creating the basic Process Director objects. The Advanced Proficiency level ....

CORE PROFICIENCY

Performance Tasks

Req #	Task	Criticality	Frequency	Difficulty
1	Create eForm definitions in Process Director	High	High	Low
1	Configure eForm properties in Process Director	High	High	Low
1	Configure eForm fields in Process Director	High	Medium	Medium
1	Create and implement conditions in eForms	High	Medium	Medium
2	Use the Word Designer to Format an eForm properly using tables	High		
2	Use the Word Designer to place controls on the Word Designer page	High		
2	Use the Word Designer to Set form control properties in the word designer.	High		
2	Use the Word Designer to create an eForm template	High	High	Medium
3	Create Process Timeline definitions in Process Director	High	High	Low
3	Configure Process Timeline definitions in Process Director	High	High	Low

Please see the documentation for the ShowAttach control to see how to enable Collaborative Document Authoring for attachments.

Collaborative Document Authoring is a cloud-based service, OnlyOffice, that opens a number of file formats in an online editor for collaborative authoring and editing, change tracking, etc. The documentation for the Document, Spreadsheet and Presentation editors is available at the OnlyOffice documentation web site.

The following file formats can be authored in the OnlyOffice editors:

- Document Editor: DOCX, TXT, ODT, or RTF files.
- Spreadsheet Editor: XLSX, ODS, or CSV files.
- Presentation Editor: PPTX or ODP files.

Microsoft 365 and CDA

For Process Director v6.1.300 and higher, CDA can optionally be used in conjunction with Microsoft 365 (M365), rather than the OnlyOffice service. M365 was formerly called "Office 365" until 2025, when it was renamed. M365 is an online service that provides online access to, storage for, and use of all the productivity applications that have been part of the Microsoft Office software suite for many years, such as Microsoft Word®, Excel®, PowerPoint®, etc.

Additional configuration is required to use M365 as the editor for CDA documents.

- First, you must set up the configuration in Azure/Entra to create the appropriate SAML setup and application endpoints, as described in the Configuring Microsoft 365 for CDA topic of the System Administrator Guide.
- Next, the Properties page of the Installation Settings section of the IT Admin area has several properties that must be configuredto create the connection to both the M365 installation and the shared SharePoint site root folder in which document attachments will be stored. These properties also require supplying the OAuth settings for the Registered Application in Azure/Entra.

The configuration of M365 CDA is a stand-alone process and is completely unrelated to other, similar features, such as OAuth for SMTP through Microsoft Azure or the SharePoint Datasource object, both of which will require their own, unique settings and configuration.

Configuring Azure for Microsoft 365 (M365)

For Process Director v6.1.300 and higher, Collaborative Document Authoring (CDA), can be implemented using the online version of Microsoft 365 (M365). Setting up M365 CDA is a relatively complex process. This process will require setup within your Azure/Entra instance, and will, in most cases, also require some assistance from BP Logix. BP Logix recommends that you read this guide thoroughly before executing the steps provided. Key information can be overlooked if you're not careful.

In order to provide optimal security, confining Process Director to a single SharePoint site, you'll need to create two different application registrations in Microsoft Entra. The first “Full Scope” registration is used only during initial configuration. The second “Site” registration is configured through the “Full Scope” registration and is the application registration that Process Director will utilize, once configured.

There are several steps to the process of configuration, each of which are linked to a documentation topic below, in the order in which they must be completed. In each topic, we'll specifically designate which steps you must perform as part of your Azure/Entra configuration, and which steps BP Logix must perform to complete the configuration in Process Director. Configuring M365 CDA requires that the steps below must be completed in order.

1. Configure SAML access for PD in Azure.
2. Create and configure “Full Scope” App Registration for PD in Azure/Entra.
3. Create and configure “Site” App Registration for PD in Azure/Entra.
4. Grant proper “Site” App Registration permission.
5. Securely exchange “Site” App Registration and related settings with Process Director.
6. Configure Process Director to leverage the application registration.
7. Configure SharePoint external sharing.

Conclusion

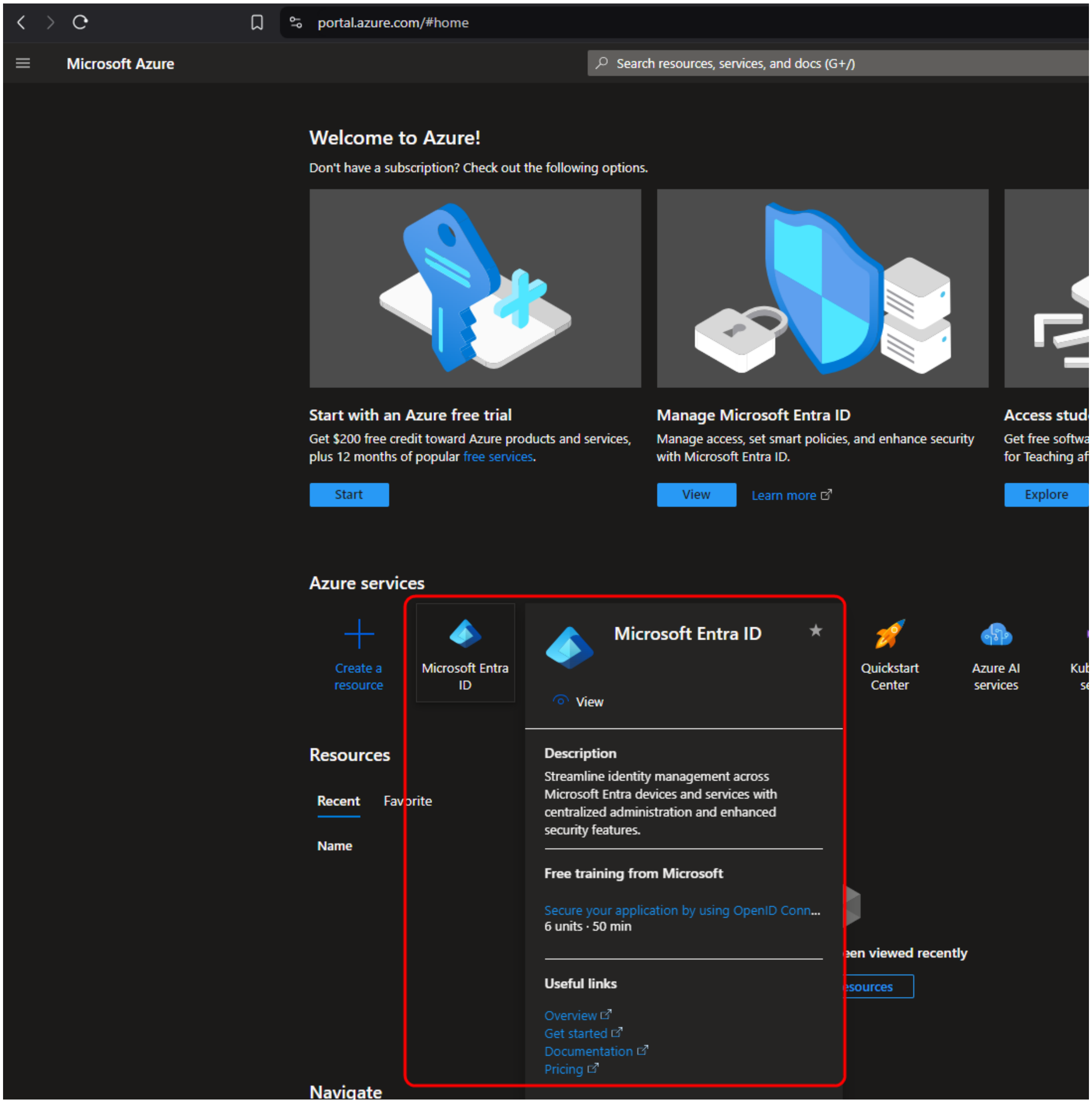
Congratulations! Assuming that you've correctly followed the instructions provided in the topics listed above, you've now configured an Azure/Entra/SharePoint integration with M365 CDA.

Configuring SAML Access for M365 CDA

❗ This topic discusses a product feature in active development, and is subject to change at any time.

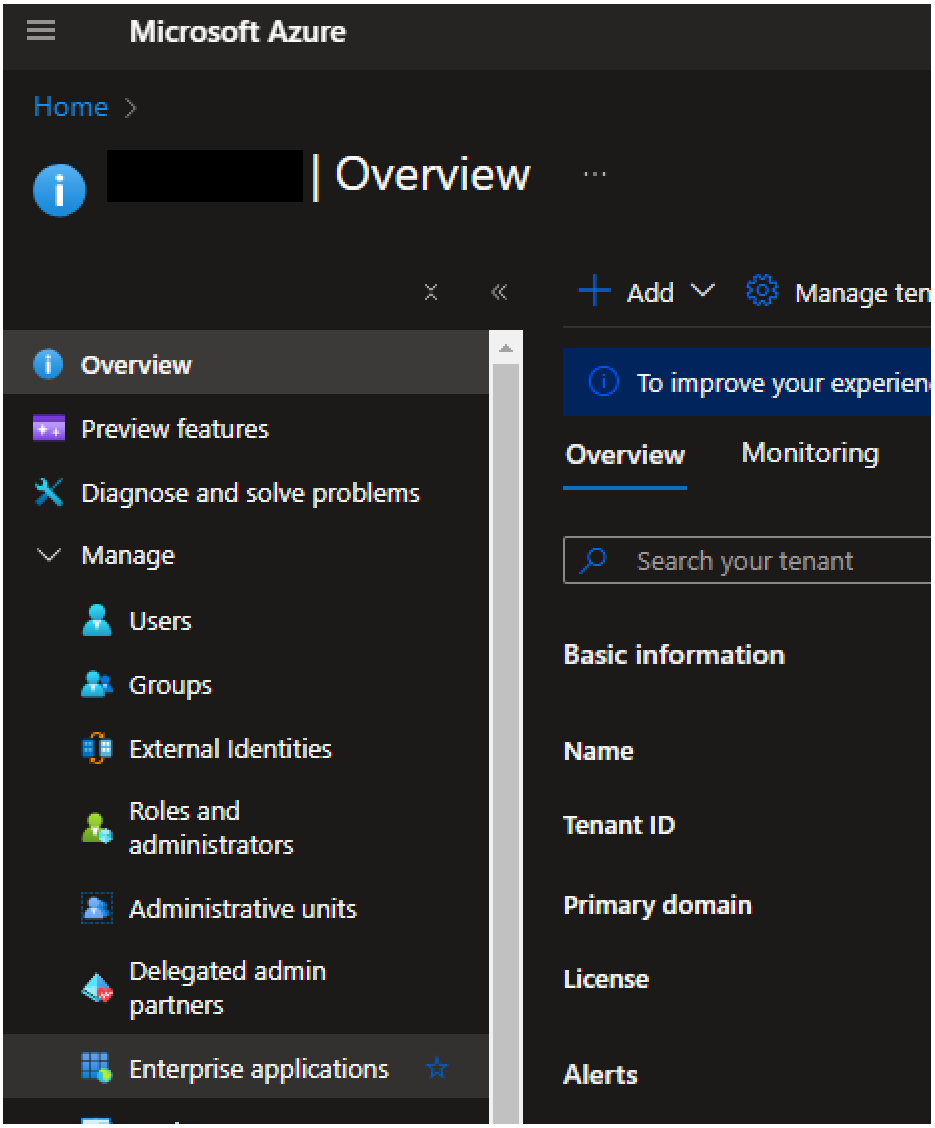
There are several ways to register external applications for use in Azure; however, only Enterprise applications currently support SAML. Thus for this topic, we'll cover the creation of the Enterprise Application for configuring SAML with Process Director.

To begin creating the Enterprise application for SAML integration, first navigate to the Microsoft Entra ID page of your Azure portal.

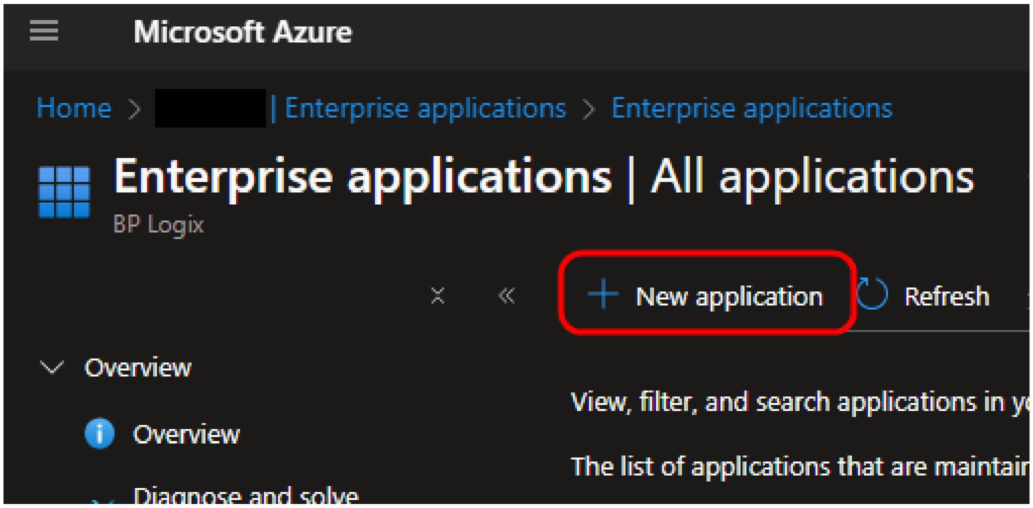


portal.azure.com/#home
Microsoft Azure
Search resources, services, and docs (G+/)
Welcome to Azure!
Don't have a subscription? Check out the following options.
Start with an Azure free trial
Get $200 free credit toward Azure products and services, plus 12 months of popular free services.
Start
Manage Microsoft Entra ID
Manage access, set smart policies, and enhance security with Microsoft Entra ID.
View
Learn more
Access stud
Get free softwa
for Teaching af
Explore
Azure services
Create a resource
Microsoft Entra ID
Microsoft Entra ID
View
Description
Streamline identity management across Microsoft Entra devices and services with centralized administration and enhanced security features.
Free training from Microsoft
Secure your application by using OpenID Conn...
6 units · 50 min
Useful links
Overview
Get started
Documentation
Pricing
Quickstart Center
Azure AI services
Kub
se
Resources
Recent
Favorite
Name
een viewed recently
esources
Navigate

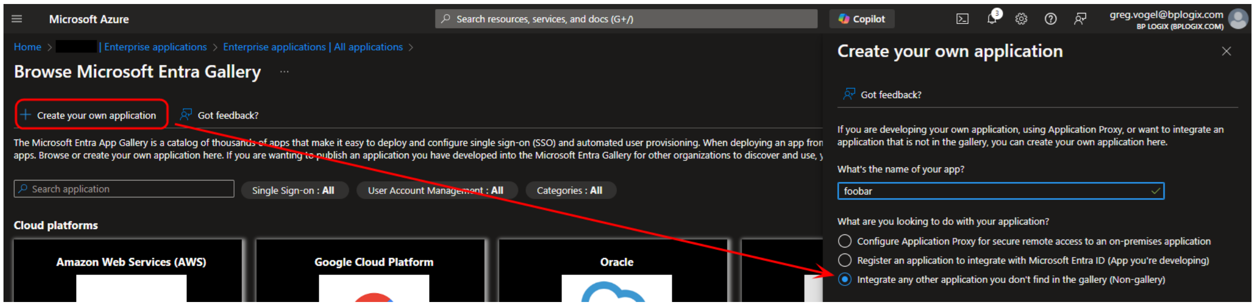
From this page, use the navigation bar on the left side of the screen to navigate to the Enterprise Applications page.



From the toolbar at the top of the page, select the New application button.


Microsoft Azure
Home > [redacted] | Enterprise applications > Enterprise applications
Enterprise applications | All applications
BP Logix
+ New application
Refresh
Overview
Overview
Diagnose and solve
View, filter, and search applications in y
The list of applications that are maintai

Click the Create your own application button, then select the option labeled, Integrate any other application you don't find in the gallery.



Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

greg.vogel@bplogix.com
BP LOGIX (BPLOGIX.COM)

Home > [redacted] | Enterprise applications > Enterprise applications | All applications >

Browse Microsoft Entra Gallery ...

+ Create your own application   Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app fron apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, y

Search application   Single Sign-on : All   User Account Management : All   Categories : All

Cloud platforms

Amazon Web Services (AWS)   Google Cloud Platform   Oracle

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

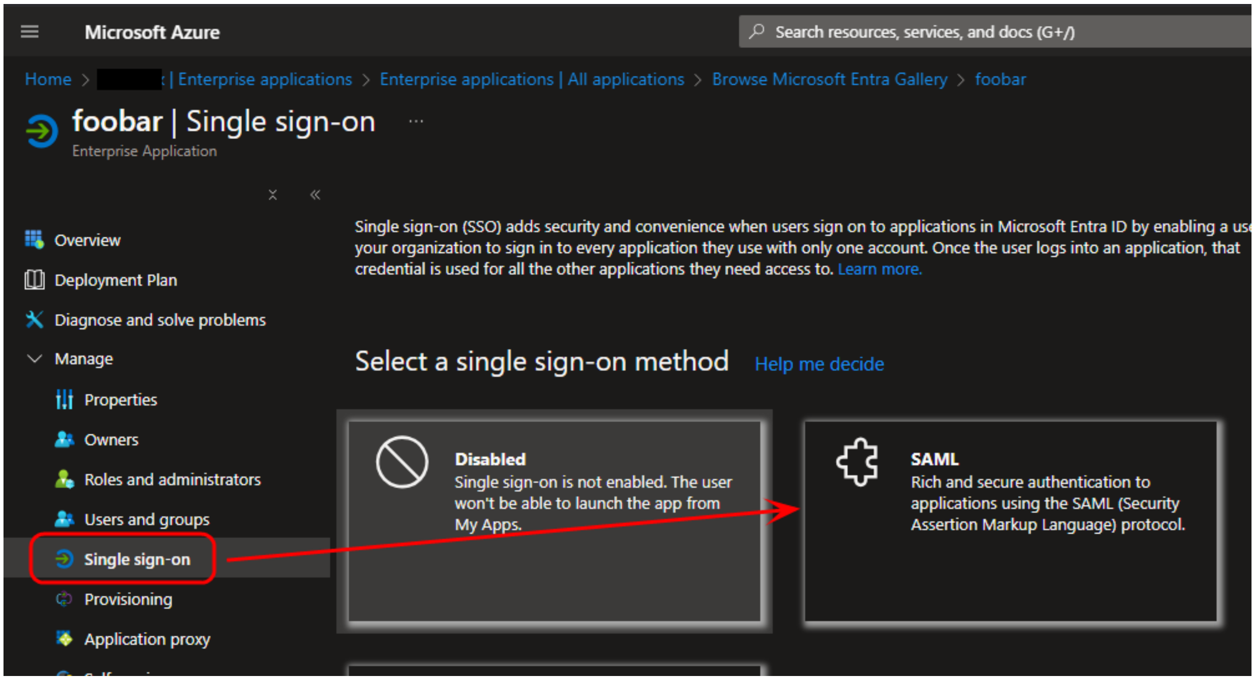
What's the name of your app?

foobar

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application to integrate with Microsoft Entra ID (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

Once the application has been created, you'll need to select the application type. To do so, click the Single sign-on button from the navigation bar on the left side of the page, then click the SAML button that will appear in the main portion of the screen.



Microsoft Azure

Search resources, services, and docs (G+/)

Home > [redacted] | Enterprise applications > Enterprise applications | All applications > Browse Microsoft Entra Gallery > foobar

foobar | Single sign-on ...
Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on
  - Provisioning
  - Application proxy

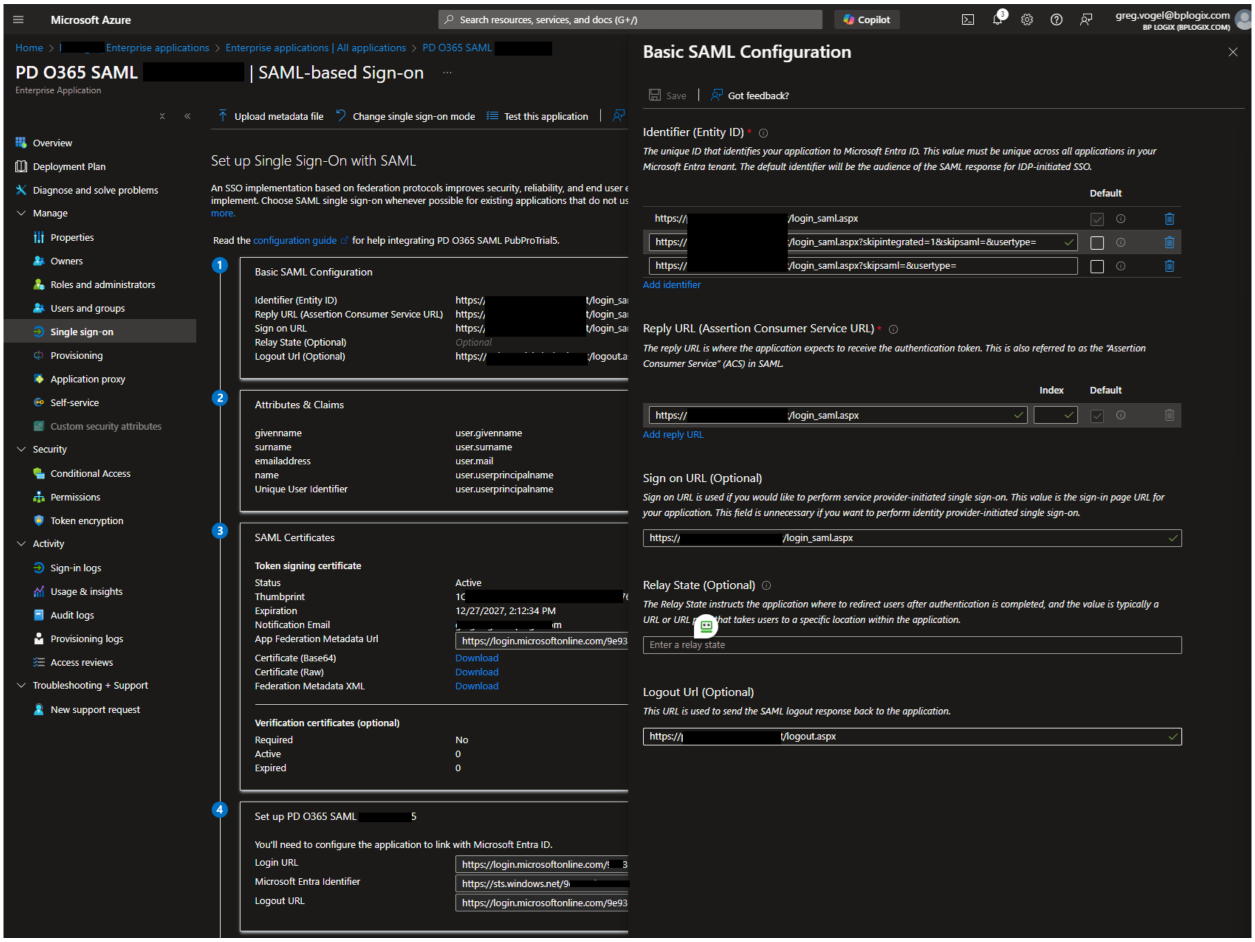
Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a us your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method   Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

On the SAML-based Sign-on page, you'll need to add the appropriate identifying URLS to configure the linkage between Process Director's SAML-related pages and Azure/Entra.



PD O365 SAML [redacted] | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user e
implement. Choose SAML single sign-on whenever possible for existing applications that do not us
more.

Read the configuration guide for help integrating PD O365 SAML PubProTrial5.

1 Basic SAML Configuration

Identifier (Entity ID)	https:/[redacted]t/login_sa
Reply URL (Assertion Consumer Service URL)	https:/[redacted]t/login_sa
Sign on URL	https:/[redacted]t/login_sa
Relay State (Optional)	Optional
Logout Url (Optional)	https://[redacted]/logout.a

2 Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate

Status	Active
Thumbprint	1C[redacted]76
Expiration	12/27/2027, 2:12:34 PM
Notification Email	[redacted]m
App Federation Metadata Url	https://login.microsoftonline.com/9e93
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0
Expired	0

4 Set up PD O365 SAML [redacted]5

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://login.microsoftonline.com/[redacted]3
Microsoft Entra Identifier	https://sts.windows.net/9[redacted]
Logout URL	https://login.microsoftonline.com/9e93

Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://[redacted]/login_saml.aspx	☑
https://[redacted]/login_saml.aspx?skipintegrated=1&skipsaml=&usertype=	□
https://[redacted]/login_saml.aspx?skipsaml=&usertype=	□

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://[redacted]/login_saml.aspx		☑

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

https://[redacted]/login_saml.aspx

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL p that takes users to a specific location within the application.

Enter a relay state

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

https://[redacted]t/logout.aspx

First, you'll need to add the Identifier (Identity ID) URLs that specify where the SAML logins will originate in Process Director. There are three of them that must be configured, using your actual Process Director server domain in place of the `<pdserver.domain>` placeholder text:

1. `https://<pdserver.domain>/login_saml.aspx`
2. `https://<pdserver.domain>/login_saml.aspx?skipintegrated=1&skipsaml=&usertype=`
3. `https://<pdserver.domain>/login_saml.aspx?skipsaml=&usertype=`

You'll then need to set the Reply URL (Assertion Consumer Service URL) property to:

`https://<pdserver.domain>/login_saml.aspx`.

Next, set the Signon URL (Optional) property to:

`https://<pdserver.domain>/login_saml.aspx`.

Finally, set the Logout Url (Optional) property to:

`https://<pdserver.domain>/logout.aspx`.

The remainder of the Azure default property settings can remain unchanged. Click the Save button to save your newly configured application. Keep the page open, however, as we'll want to test the configuration later.

With the application configured in Azure, you'll now need to make the appropriate changes to your Process Director installation to enable SAML sign on for Process Director. **For Cloud customers, this process will most likely be done by BP Logix personnel.** On-Premise customers, however, will have to perform this configuration in their Process Director installation. Please see the appropriate Process Director documentation for configuring SAML 2.0 (Federated Identity) Support in the Installation Guide. This configuration will require setting several SAML Custom Variables in your Custom Variables file.

Once SAML is correctly configured in Process Director, you can return to the Azure Application window. At the bottom of the configuration page, click the Test button. This button will verify that all your changes work by opening a pop-up browser window to perform the connection testing. It will even look up errors you may receive from Microsoft’s login server and provide you help with resolving them.

Once the testing is complete, and you've corrected any SAML configuration or connection errors that may appear, your Process Director server should be fully integrated with Azure for SAML authentication.

With the configuration completed, you'll then need to determine how existing users will be added to Process Director from your SAML system. There are two common methods for adding existing users:

1. Direct import into Process Director via a CSV/Excel file.
2. Enabling Process Director to auto-create user accounts when the user first logs in via SAML.

BP Logix personnel will work with you to determine the most appropriate method for your user provisioning, both initially and on an ongoing basis. There are, as always, pros and cons with both methods, so BP Logix will work with you to determine the user provisioning method that best meets your needs.

With SAML set up properly, you can move to the next step, which is to create and configure the "Full Scope" App Registration in Azure.

Other M365 CDA Configuration Topics

M365 CDA Overview

M365 CDA Configuration Process

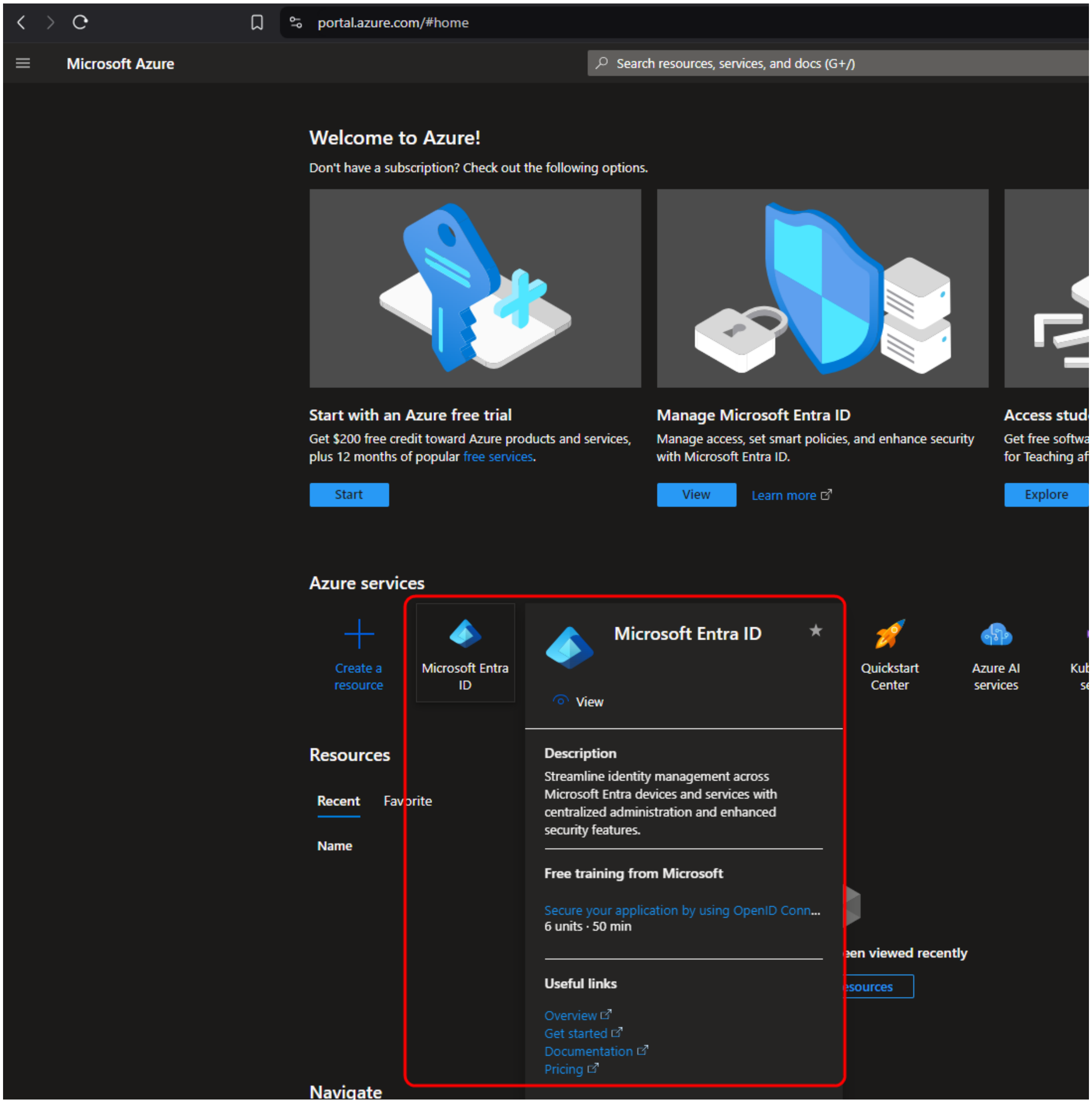
- Create and configure “Full Scope” App Registration for PD in Azure/Entra.
- Create and configure “Site” App Registration for PD in Azure/Entra.
- Grant proper “Site” App Registration permission.
- Securely exchange “Site” App Registration and related settings with Process Director.
- Configure Process Director to leverage the application registration.
- Configure SharePoint external sharing.

Configuring "Full Scope” App Registration

When fully configured, M365 CDA will access a single, specified SharePoint site. In order to create this configuration, you'll need to provide a mechanism to isolate that site. A "Full Scope" application registration in Azure provides this isolation mechanism, which we'll use to create the site-level application later.

The official Azure/Entra proprietary term for creating the entity we're about to configure is *Application (App) Registration*, and that's the term we'll use in this documentation. Your personnel who have IT/IS specialties may refer to this Azure/Entra entity by different names. Most commonly, the generic term *Service Principal* is likely familiar, since it's a generic term that can be used for other cloud providers like AWS and Google Cloud, and is the term commonly used in Internet Security.

To create the "Full Scope" App Registration, first navigate to the Microsoft Entra ID page of your Azure installation.



Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

Manage Microsoft Entra ID

Manage access, set smart policies, and enhance security with Microsoft Entra ID.

Access stud

Get free softwa for Teaching af

Description

Streamline identity management across Microsoft Entra devices and services with centralized administration and enhanced security features.

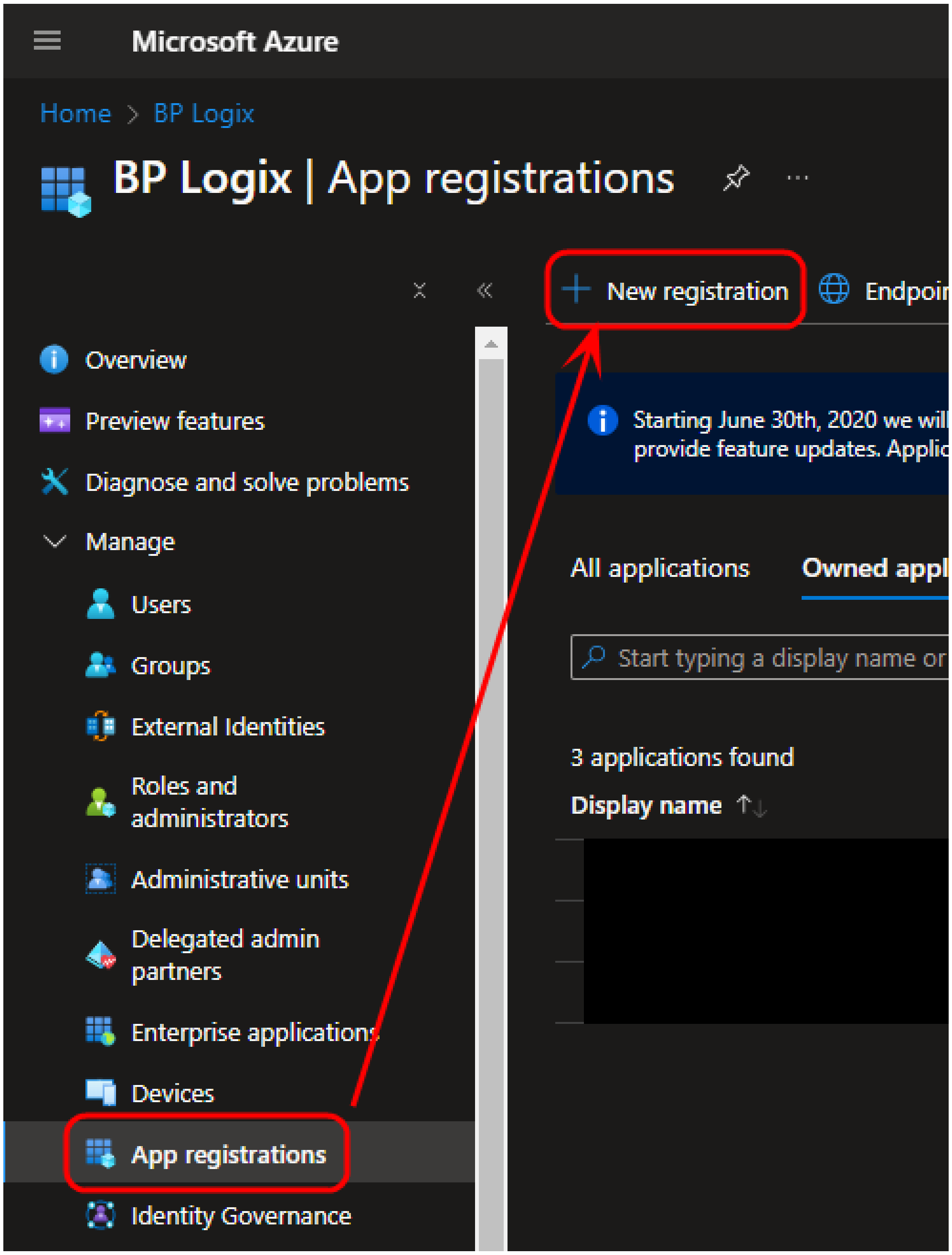
Free training from Microsoft

Secure your application by using OpenID Conn...
6 units · 50 min

Useful links

Overview
Get started
Documentation
Pricing

From this page, use the navigation bar on the left side of the screen to navigate to the App Registrations page. From this page, click the New registration button that appears at the top of the page.

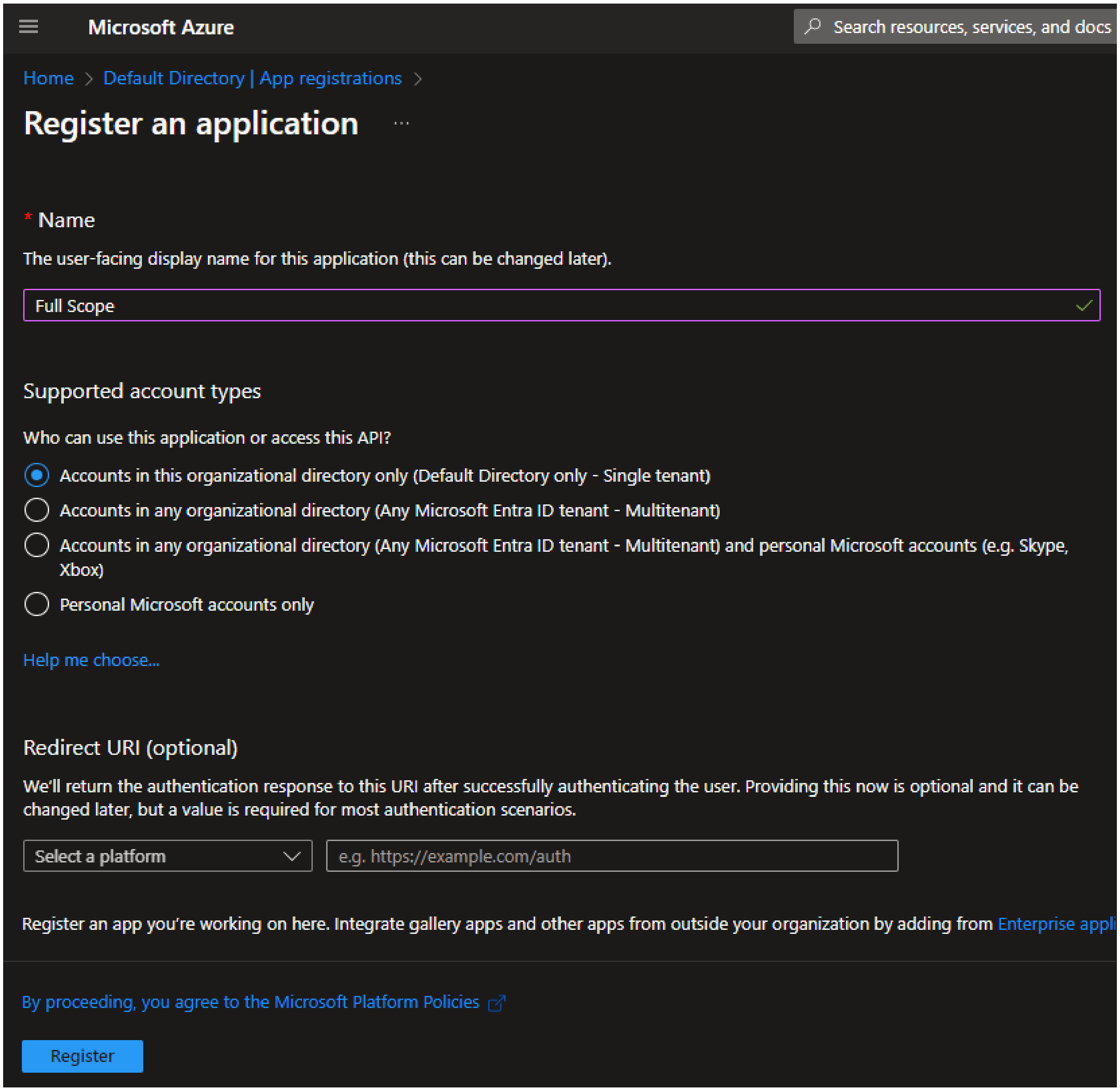


Starting June 30th, 2020 we will provide feature updates. Applic

3 applications found

[redacted]

On the Register an application page, Set the Name of the new application as “Full Scope” (or a suitable name of your choosing but note we refer to it as “Full Scope” in this document). Typically, the default setting of the Supported Account Types property is "Accounts in this organizational directory only" is satisfactory and provides optimal security.



Microsoft Azure
Search resources, services, and docs
Home > Default Directory | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Full Scope

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Default Directory only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

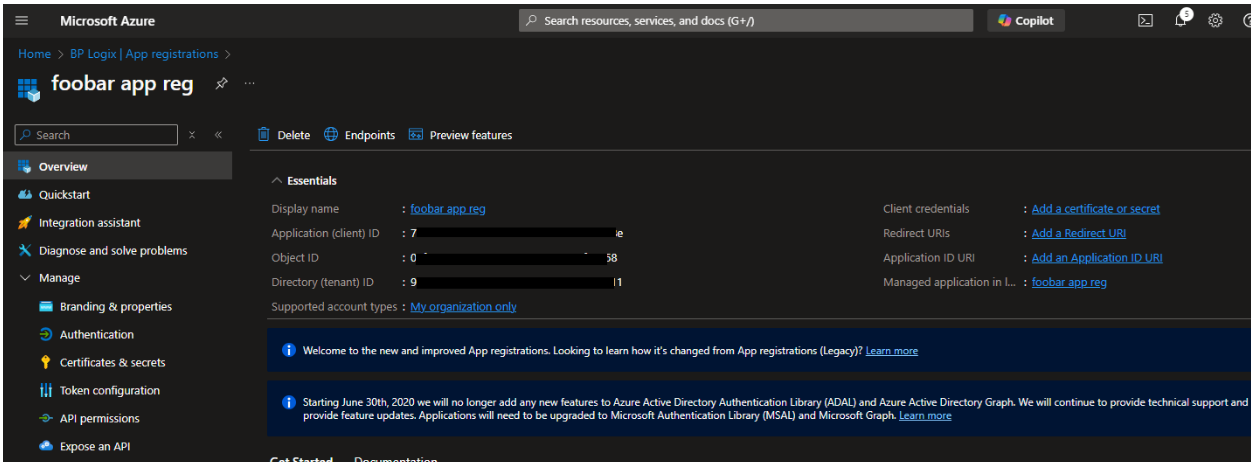
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise appli

By proceeding, you agree to the Microsoft Platform Policies

You can click the Register button at the bottom of the page to register the new application. Once registered, you'll see the Overview page for the new application. Note the Application (client) ID and Directory (tenant) ID properties. These values will be needed later when we grant access to the "Site" level App Registration. They are easily copied when hovering the mouse over each value.



Display name : foobar app reg
Application (client) ID : 7[redacted]e
Object ID : 0[redacted]58
Directory (tenant) ID : 9[redacted]1
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : foobar app reg

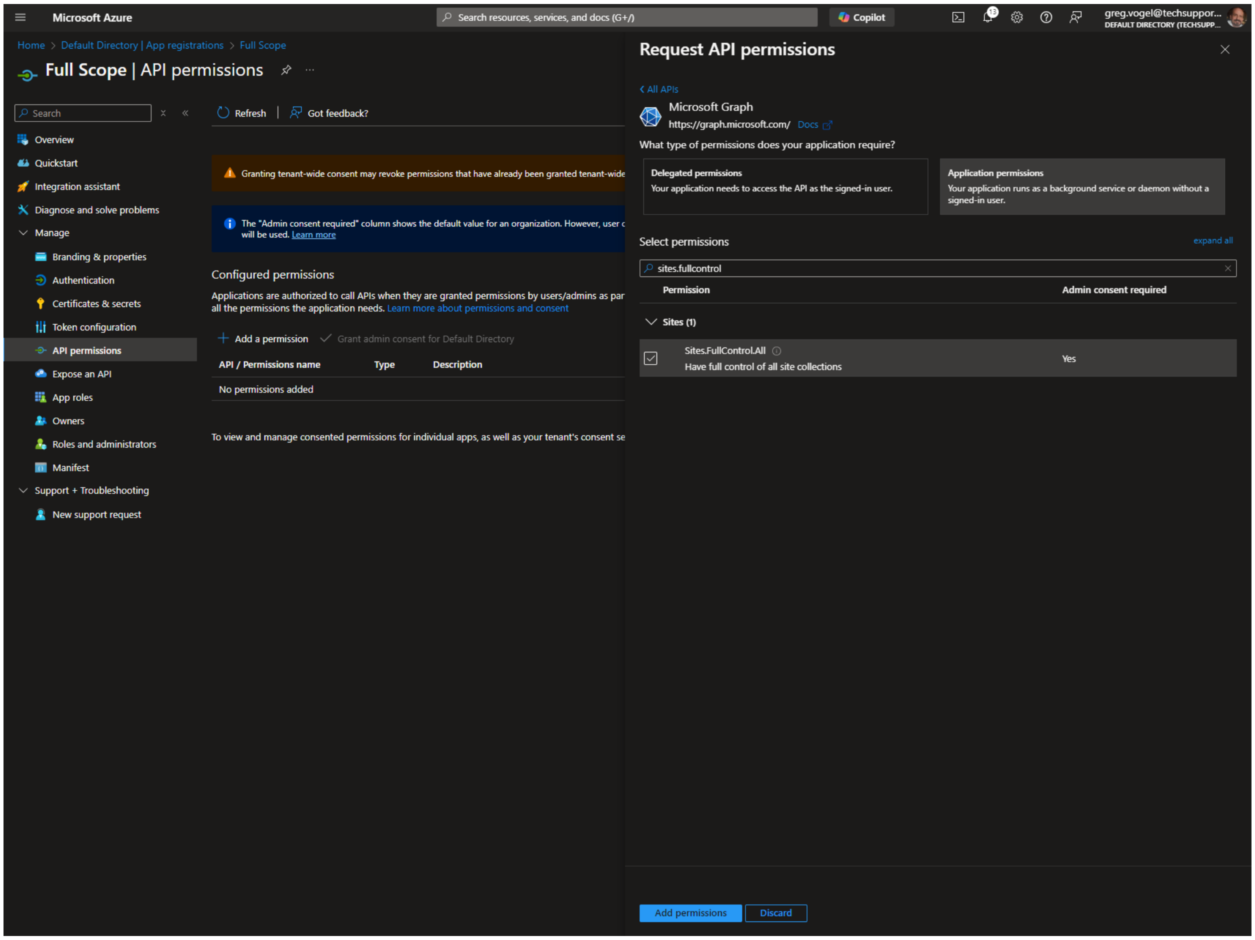
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Next, you'll need to click the API Permissions menu item from the left sidebar of the page to open the API Permissions page. You'll need to edit some of the default permissions for this application.

If the `User.Read` permission is shown, you'll need to delete it.

Next, you'll need to click the Add a permission button to open its dialog box. Select Microsoft Graph, then Application Permissions. Once in the Application Permissions section, you'll need to add the `Sites.FullControl.All` permission to the application.



Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide

The "Admin consent required" column shows the default value for an organization. However, user c will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as par all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description
No permissions added		

To view and manage consented permissions for individual apps, as well as your tenant's consent se

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

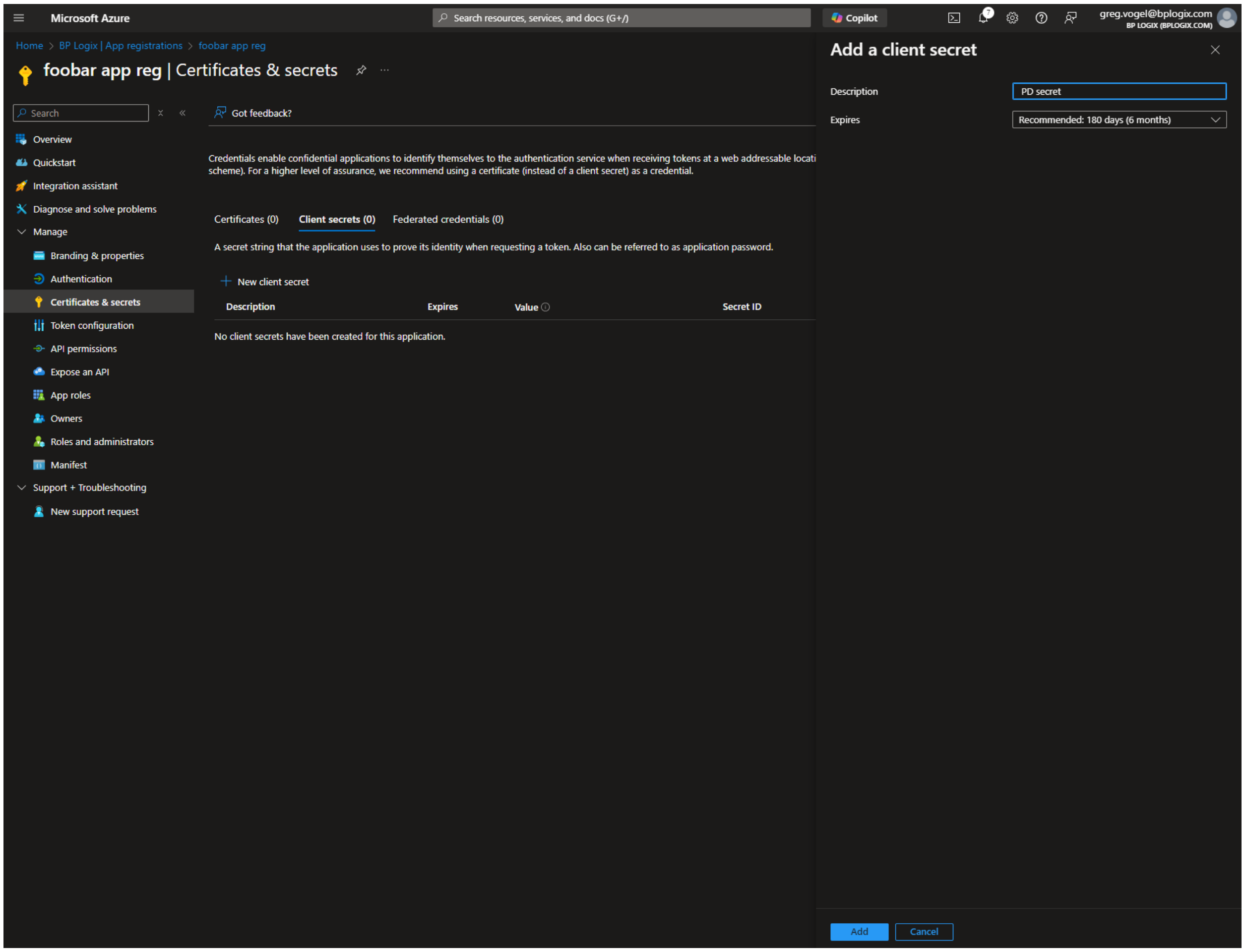
sites.fullcontrol

	Permission	Admin consent required
	Sites (1)	
☑	Sites.FullControl.All Have full control of all site collections	Yes

Once you've done so, click the Add Permissions button at the bottom of the page. Once you do, you'll need to click the Grant admin consent for <Enterprise name> button to confirm the change.

Now that the permissions have been changed, you'll need to create the Client Secret property for the new application. To do so, click the Certificates & secrets navigation menu item on the left sidebar of the page. When the page opens, click the New Client Secret button to create a new client secret. You'll need to provide a Name for the new item. Once you do so, click the Add button.

Once you click the *Add* button, you are presented with the secret *once and only once*. Do not navigate away or refresh the page.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable locati scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

Add a client secret

Description: PD secret

Expires: Recommended: 180 days (6 months)

Click the Copy to clipboard icon and then paste the secret into a secure document or file. Keep the file secret, and store it in a safe and secure place, preferably one that is backed up securely. Losing this value will make it impossible to use the "Full Scope" app to create the site isolation for the M365 CDA integration.

Keep the values for the Client Secret as well as the Client ID and Tenant ID properties for the “Full Scope” App Registration on hand. We'll need them to create and configure the "site" level App Registration, which is the next step in the process.

Other M365 CDA Configuration Topics

M365 CDA Overview

M365 CDA Configuration Process

- Configure SAML access for PD in Azure.
- Create and configure “Site” App Registration for PD in Azure/Entra.
- Grant proper “Site” App Registration permission.

- Securely exchange “Site” App Registration and related settings with Process Director.
- Configure Process Director to leverage the application registration.
- Configure SharePoint external sharing.

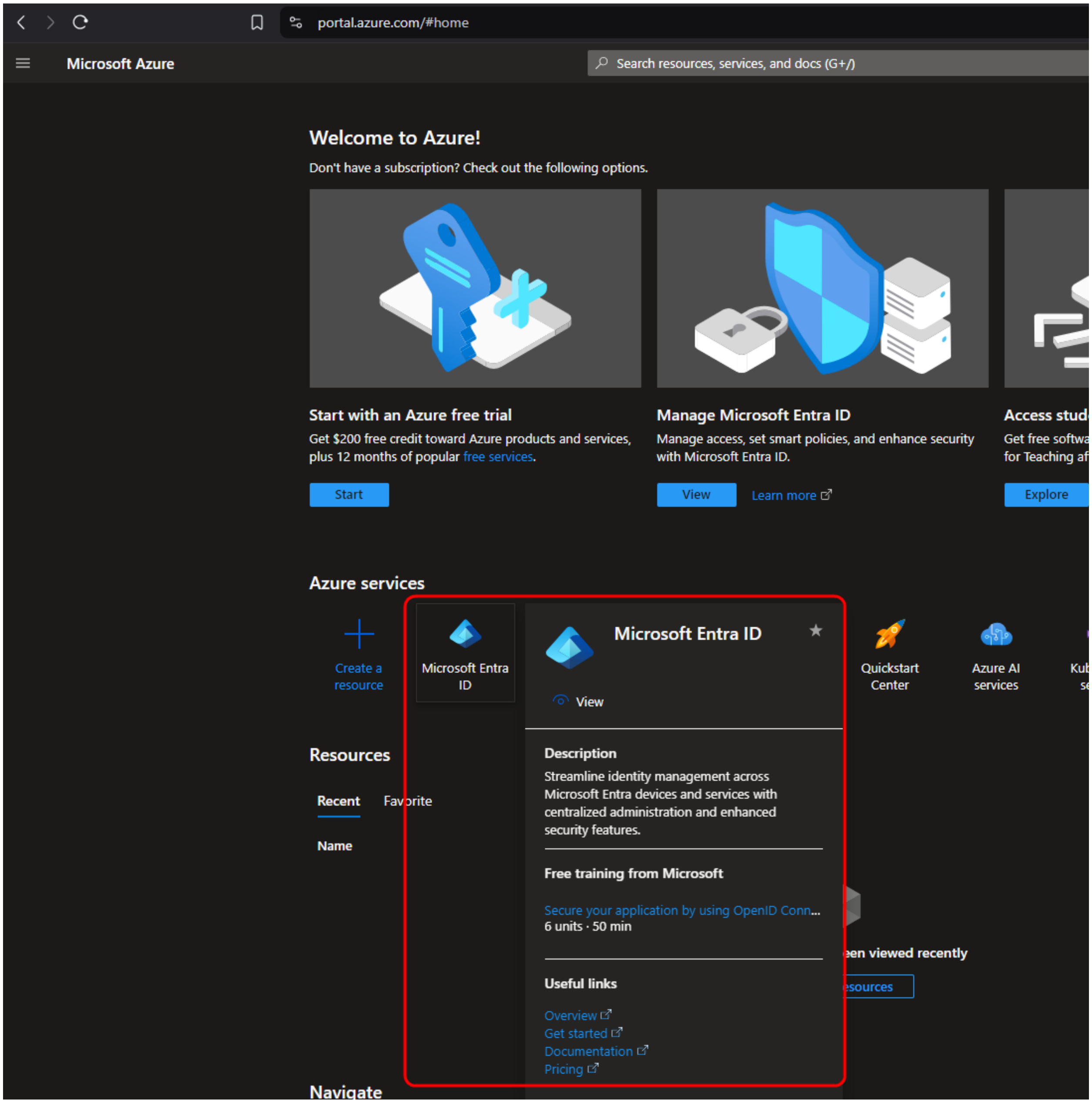
Configuring the "Site" Level App Registration

❗ **This topic discusses a product feature in active development, and is subject to change at any time.**

ⓘ **As mentioned at the end of the previous configuration step, you're going to need to refer to the Client Secret, Client ID, and Tenant ID properties of the "Full Scope" App registration. The "Site" level App registration also has the same properties, with the same property names. To avoid confusion during the configuration, we'll explicitly refer to these properties as "Full Scope" or "Site" when referring to the property names, e.g., Full Scope Client ID, Site Client ID, etc.**

The purpose of the "Site" level App Registration is to enable the Process Director web application server to access your enterprise’s Microsoft 365 (Office Online/M365/SharePoint Online) document storage for the purposes of using it for CDA. The "Site" level application is what CDA will access to enable the use of M365 for the collaborative editing of documents.

To create the "Site" level App Registration, first navigate to the Microsoft Entra ID page of your Azure installation.



portal.azure.com/#home

Microsoft Azure

Search resources, services, and docs (G+/)

Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

Start

Manage Microsoft Entra ID

Manage access, set smart policies, and enhance security with Microsoft Entra ID.

View Learn more

Access stud

Get free softwa
for Teaching af

Explore

Azure services

Create a resource

Microsoft Entra ID

Microsoft Entra ID

View

Description

Streamline identity management across Microsoft Entra devices and services with centralized administration and enhanced security features.

Free training from Microsoft

Secure your application by using OpenID Conn...
6 units · 50 min

Useful links

Overview
Get started
Documentation
Pricing

Quickstart Center

Azure AI services

Kub
se

Resources

Recent Favorite

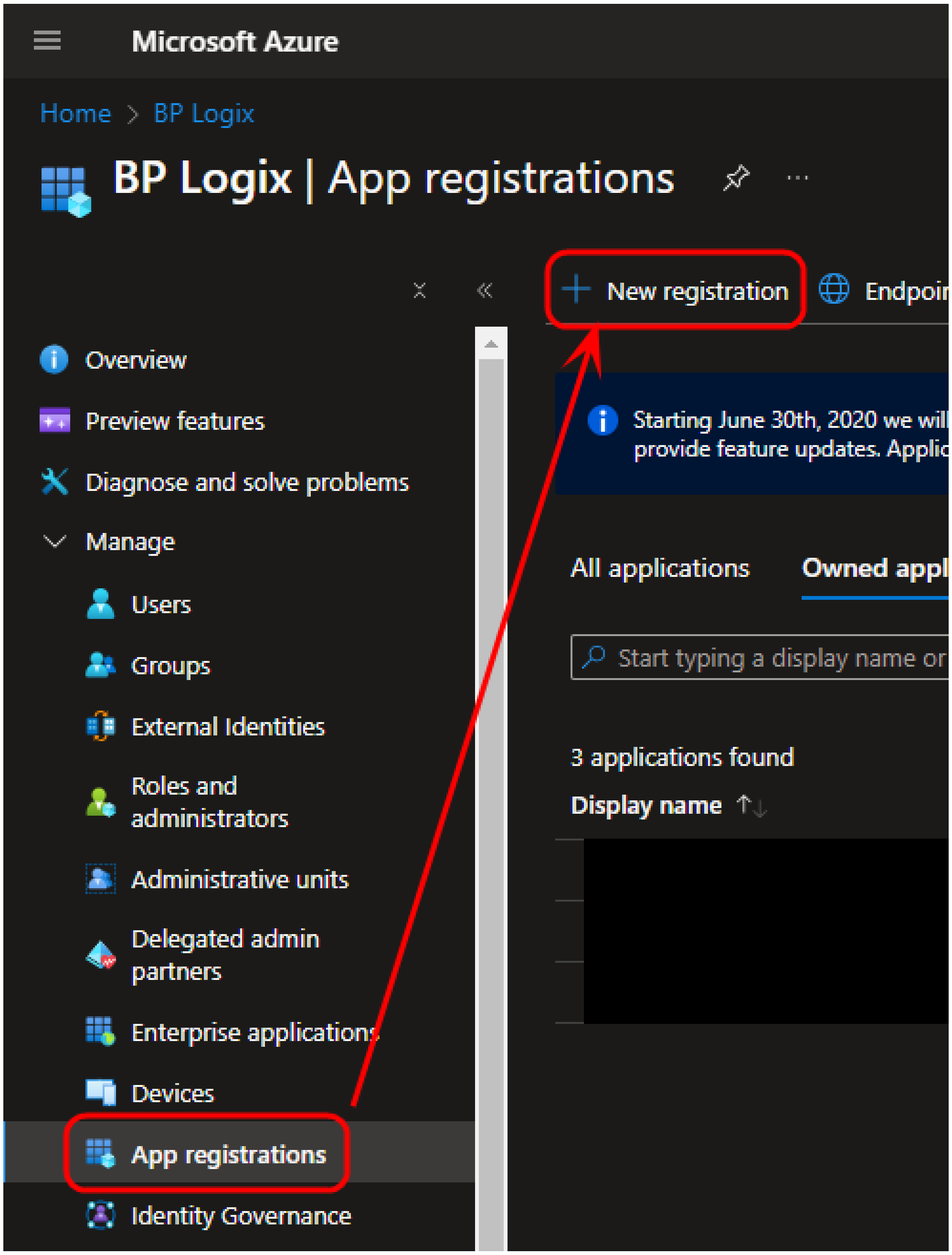
Name

een viewed recently

esources

Navigate

From this page, use the navigation bar on the left side of the screen to navigate to the App Registrations page. From this page, click the New registration button that appears at the top of the page.

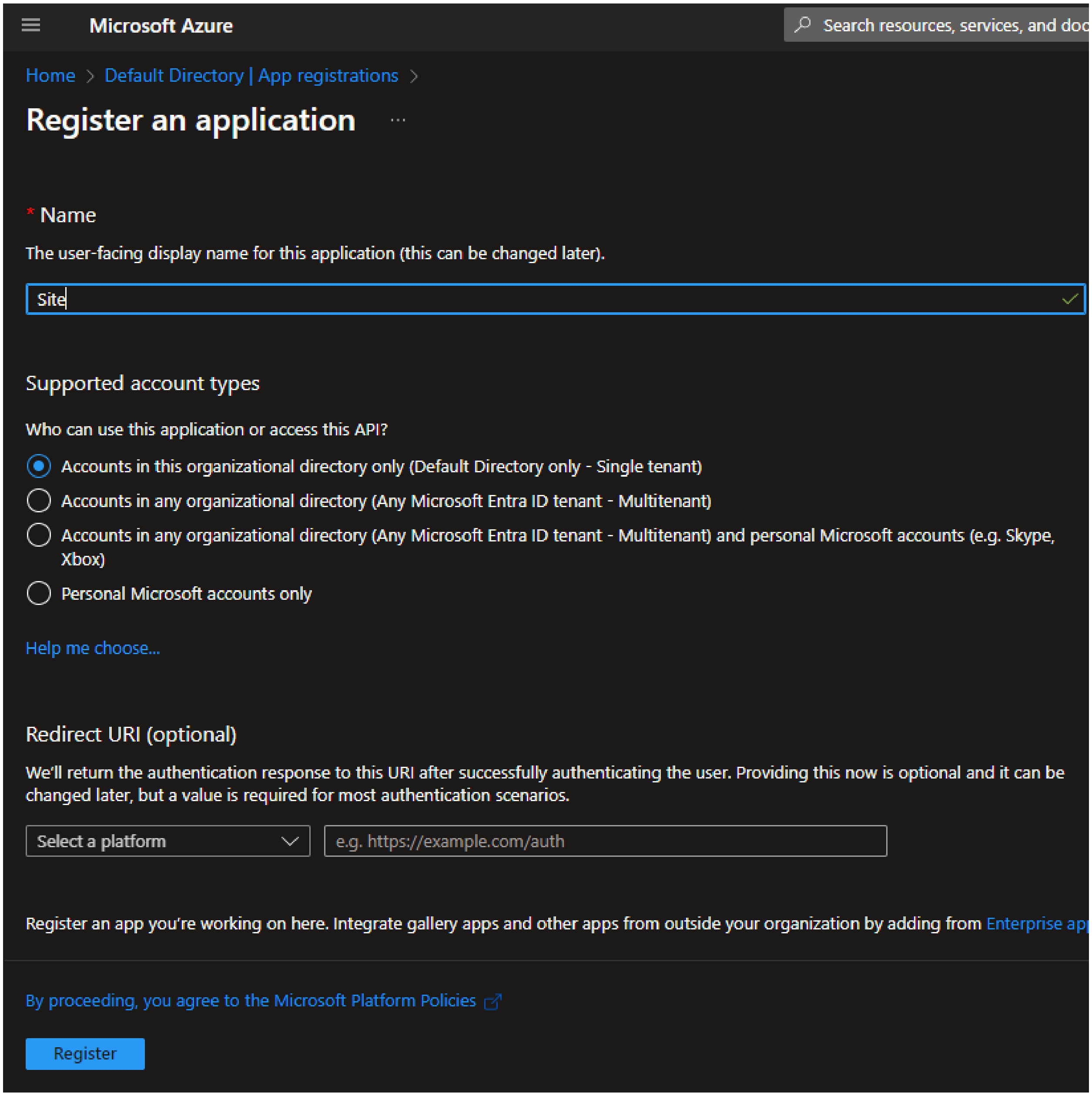


Starting June 30th, 2020 we wil
provide feature updates. Applic

3 applications found

[redacted]

Set the Name property of the new registration to "Site"(or a suitable name of your choosing but we'll refer to it as “Site” in this document), to distinguish it from the "Full Scope" registration you created previously. Typically, the default setting of the Supported Account Types property is "Accounts in this organizational directory only" is satisfactory and provides optimal security.



Microsoft Azure
Search resources, services, and doc
Home > Default Directory | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Site

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Default Directory only - Single tenant)
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

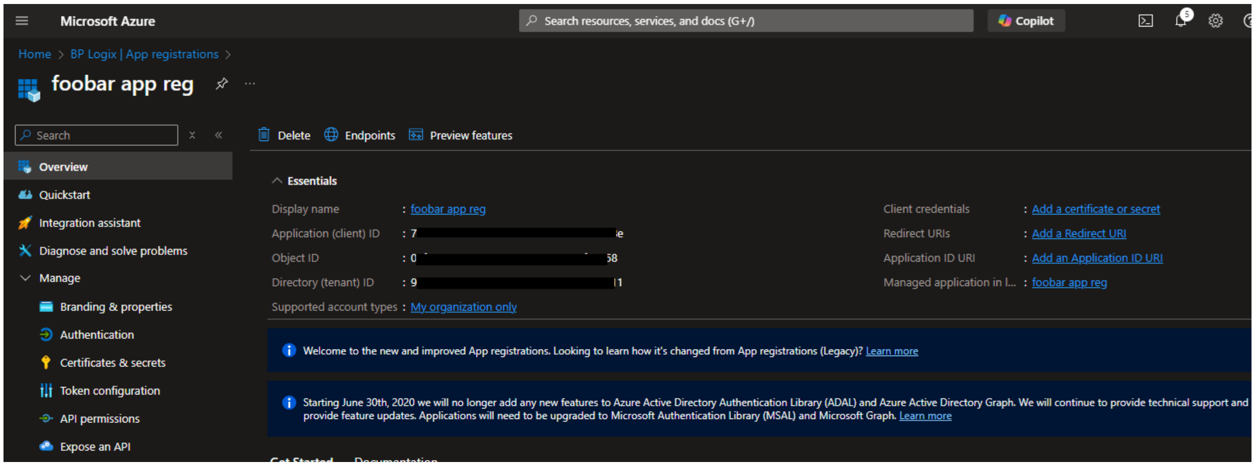
Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise ap

By proceeding, you agree to the Microsoft Platform Policies

You can click the Register button at the bottom of the page to register the application. Once registered, you'll see the Overview page for it. Note the Application (client) ID and Directory (tenant) ID properties. These values are easily copied when hovering the mouse over each value.

As mentioned previously, these are the same property names that are used in the "Full Site" App Registration, so we'll refer to them as Site Client ID and Site Tenant ID for the remainder of this document. Similarly, we'll refer to the Full Scope Client ID and Full Scope Tenant ID for the same properties used by the "Full Scope" App Registration.



Display name	: foobar app reg	Client credentials	: Add a certificate or secret
Application (client) ID	: 7 [redacted] e	Redirect URIs	: Add a Redirect URI
Object ID	: 0 [redacted] 58	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 9 [redacted] 1	Managed application in l...	: foobar app reg
Supported account types	: My organization only		

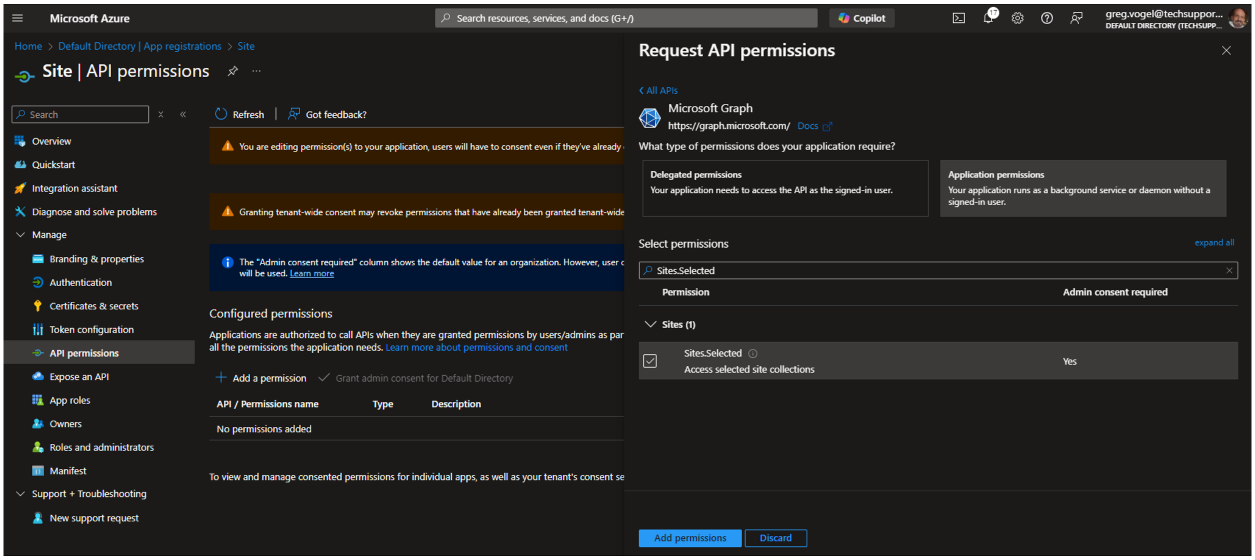
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Next, you'll need to click the API Permissions menu item from the left sidebar of the page to open the API Permissions page. You'll need to edit some of the default permissions for this application.

If the `User.Read` permission is shown, you'll need to delete it.

Next, you'll need to click the Add a permission button to open its dialog box. Select Microsoft Graph, then Application Permissions. Once in the Application Permissions section, you'll need to add the `Sites.Selected` permission to the application.



You are editing permission(s) to your application, users will have to consent even if they've already

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide

The "Admin consent required" column shows the default value for an organization. However, user c will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as par all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for Default Directory

API / Permissions name	Type	Description
No permissions added		

To view and manage consented permissions for individual apps, as well as your tenant's consent se

Request API permissions

‹ All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions — expand all

Sites.Selected

	Permission	Admin consent required
	Sites (1)	
☑	Sites.Selected Access selected site collections	Yes

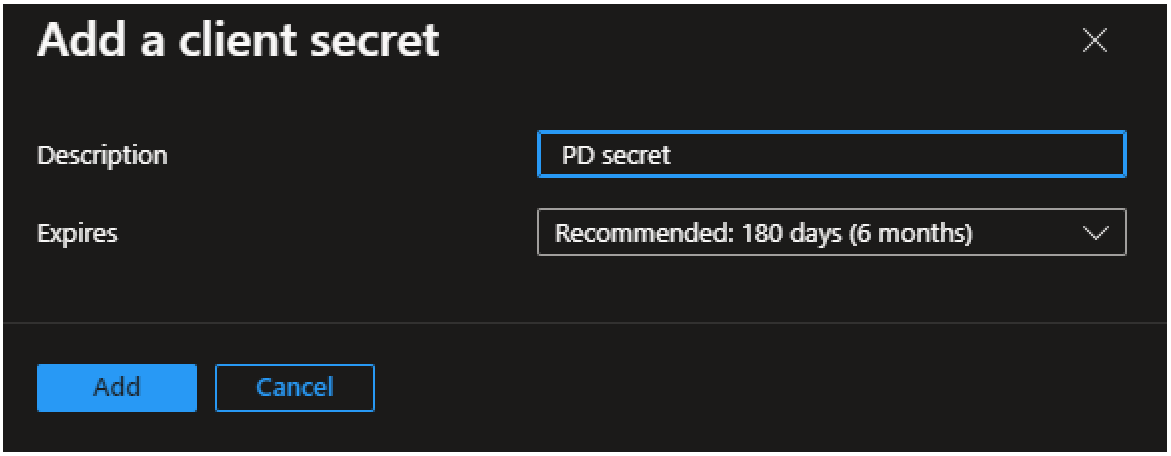
Add permissions | Discard

Once you've done so, click the Add Permissions button at the bottom of the page. Once you do, you'll need to click the Grant admin consent for <Enterprise name> button to confirm the change.

Now that the permissions have been changed, you'll need to create the Client Secret property for the new application. To do so, click the Certificates & secrets navigation menu item on the left sidebar of the page. When the page opens, click the New Client Secret button to create a new client secret. You'll need to provide a Name for the new item.

Additionally you'll need to specify when this Site Client Secret will expire, using the Expires property. This property consists of a dropdown control from which you can select how long the Site Client Secret will remain active.

It’s important to take note of the expiration time chosen. The expiration MUST be communicated to BP Logix. Also, you must provide a new Site Client Secret to BP Logix, on an ongoing basis, before each one expires, to avoid interruptions in service.



Add a client secret

Description: PD secret

Expires: Recommended: 180 days (6 months)

Once you've set the Name and Expires properties, click the Add button to create the new Site Client Secret.

Once you click the *Add* button, you are presented with the secret *once and only once*. Do not navigate away or refresh the page.

Just as you did previously with the Full Scope Client Secret, click the Copy to clipboard icon and then paste the Site Client Secret into a secure document or file. Keep the file secret, and store it in a safe and secure place, preferably one that is backed up securely.

You must provide BP Logix with the values for the Site Client Secret, Site Client ID and Site Tenant ID properties. In addition, you'll need to provide BP Logix with the SharePoint site URL that will be used to access your enterprise's SharePoint environment. Keep in mind that these values are sensitive information, so you'll need to provide them to BP Logix via a secure method. Do NOT send this information via email.

The initial configuration of the "Site" level App Registration is complete. Now you'll need to move to the next step, granting the correct "Site" App Registration permissions.

Other M365 CDA Configuration Topics

M365 CDA Overview

M365 CDA Configuration Process

- Configure SAML access for PD in Azure.
- Create and configure "Full Scope" App Registration for PD in Azure/Entra.
- Grant proper "Site" App Registration permission.
- Securely exchange "Site" App Registration and related settings with Process Director.
- Configure Process Director to leverage the application registration.
- Configure SharePoint external sharing.

Granting "Site" App Registration Permissions

This topic discusses a product feature in active development, and is subject to change at any time.

BP Logix will provide you with a set of Powershell scripts for applying the appropriate permissions to your "Site" level App Registration. These scripts have no additional external dependency; however, prior to running them, you should run the following PowerShell cmdlet:

```
Set-ExecutionPolicy -ExecutionPolicy Bypass
```

Once executed, it should ensure that the scripts provided by BP Logix won't be blocked from running.

Once you've done so, locate the folder into which you extracted the PowerShell scripts provided to you by BP Logix. Start PowerShell in that folder location.

First you must obtain a bearer token from the “Full Scope” App Registration you configured earlier. To obtain the bearer token, run the PowerShell command below. For each parameter in the command, use the "Full Scope" value you obtained earlier (Full Scope Tenant ID, Full Scope Client ID, and Full Scope Client Secret).

```
.\get-access-token.ps1 -tenantId <Full Scope Tenant ID> -clientId <Full Scope Client ID> -clientSecret <Full Scope Client Secret>
```

You'll need to replace the text in angled brackets with the actual values from your "Full Scope" App Registration, e.g.:

```
.\get-access-token.ps1 -tenantId deadbeef-deed-feed-f00d-0123456789ab -clientId 87654321-deed-feed-f00d-0123456789ab -clientSecret dI8AQ~EKNqYwcXf0CJ_lFBJvR6xnDWOZDM4Qbao7
```

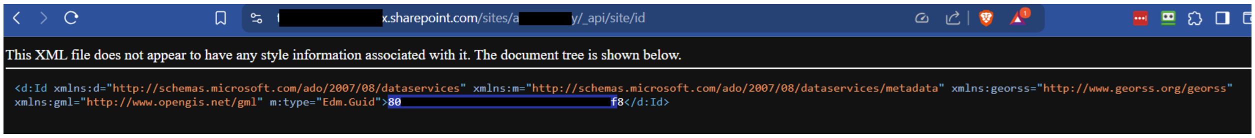
Once you’ve run the script successfully, you’ll have a file named "bearer.txt" in the current folder. The script will also output the bearer token to the console, though it will be truncated, due to its length.

Next you’ll need to obtain the Site ID for the SharePoint site you wish to use with Process Director. Process Director uses a specific path within the site to avoid conflicts with other files, documents, and folders that may be in use.

Using a browser of your choice, login and access the SharePoint site you wish to use. In that same browser, without logging out of SharePoint/Entra, navigate to:

`https://<tenantname>.sharepoint.com/sites/<sitename>/api/site/id`

Once that page loads, it will display some XML values, as shown below.



t[redacted]x.sharepoint.com/sites/a[redacted]y/_api/site/id

This XML file does not appear to have any style information associated with it. The document tree is shown below.

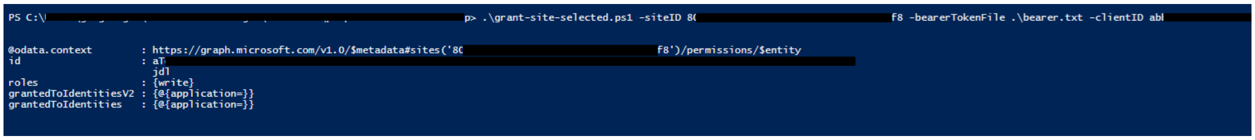
```
<d:Id xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices" xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata" xmlns:georss="http://www.georss.org/georss" xmlns:gml="http://www.opengis.net/gml" m:type="Edm.Guid">80[redacted]f8</d:Id>
```

In the example above, the redacted value that's outlined in blue (starts with “80” and ends with “f8”) is the Site ID. Copy this value and save it.

Now that we have the correct bearer token, and SharePoint Site ID, you'll need to use them, along with the Site Client ID, the file location of the bearer.txt file that contains the bearer token, and the Site Name for the "Site" level App Registration, to run the following PowerShell command.

```
.\grant-site-selected.ps1 -siteID <SharePoint Site ID> -bear-
erTokenFile .\bearer.txt -clientID <Site Client ID> -appName
"Site"
```

Again, you'll need to replace the values in angled brackets above with the appropriate values from your systems. Upon successful completion of the script, you should see the appropriate output in the console, and there should be no red error text.



```
PS C:\[redacted]p> .\grant-site-selected.ps1 -siteID 8([redacted]f8 -bearerTokenFile .\bearer.txt -clientID abl[redacted]

@odata.context        : https://graph.microsoft.com/v1.0/$metadata#sites('80[redacted]f8')/permissions/$entity
id                    : aT[redacted]
                        jdl
roles                 : {write}
grantedToIdentitiesV2 : {@{application=}}
grantedToIdentities   : {@{application=}}
```

The console messages should indicate that the appropriate roles/permissions were granted to the specified "Site" App Registration.

With this complete, you can now securely transmit the configuration information BP Logix needs to configure your system.

Other M365 CDA Configuration Topics

M365 CDA Overview

M365 CDA Configuration Process

- Configure SAML access for PD in Azure.
- Create and configure “Full Scope” App Registration for PD in Azure/Entra.
- Create and configure “Site” App Registration for PD in Azure/Entra.
- Securely exchange “Site” App Registration and related settings with Process Director.
- Configure Process Director to leverage the application registration.
- Configure SharePoint external sharing.

Securely Transmit Configuration to BP Logix

> ❗ **This topic discusses a product feature in active development, and is subject to change at any time.**

The secure online information exchange services mentioned in this topic are suggestions. BP Logix is happy to use other secure services you've vetted and wish to use. Avoid sending any this information in this topic to BP Logix via email or other insecure methods to prevent unnecessarily exposing this sensitive data.

Using a secure online information exchange mechanism (e.g. FireCloud, Kiteworks, ShareFile, onetimescret.com, Privnote, etc.), send BP Logix the following information:

- Site Tenant ID
- Site Client ID
- Site Client Secret
- Site Client Secret Expiration Date (what month/day/year will the secret expire?)
- SharePoint site URL, e.g.: `https://<tenant-name>.sharepoint.com/sites/<site-name>`
- (Optional) SharePoint site folder path: If there’s a specific location within the site where you'd like to store the Process Director data, provide that path here.

Once BP Logix receives this information, we can perform the next step in the process, Configuring your Process Director installation.

Other M365 CDA Configuration Topics

M365 CDA Overview

M365 CDA Configuration Process

- Configure SAML access for PD in Azure.
- Create and configure “Full Scope” App Registration for PD in Azure/Entra.
- Create and configure “Site” App Registration for PD in Azure/Entra.
- Grant proper “Site” App Registration permission.
- Configure Process Director to leverage the application registration.
- Configure SharePoint external sharing.

Configuring Process Director

This topic discusses a product feature in active development, and is subject to change at any time.

Whether you're a Cloud customer of the Process Director platform, or a customer who has purchased a Use Case application, such as PubPro, Approvia, MIRador, etc., BP Logix will configure your Process Director and/or application installation with the values you've securely supplied to us. Please refer to the documentation for the M365 CDA property settings of the Properties page to see the details of the properties that will have to be configured.

You can now move to the final step of the configuration process, Configuring SharePoint External Access.

Other M365 CDA Configuration Topics

M365 CDA Overview

M365 CDA Configuration Process

- Configure SAML access for PD in Azure.
- Create and configure “Full Scope” App Registration for PD in Azure/Entra.
- Create and configure “Site” App Registration for PD in Azure/Entra.
- Grant proper “Site” App Registration permission.
- Securely exchange “Site” App Registration and related settings with Process Director.
- Configure SharePoint external sharing.

Configuring SharePoint for External Access

This topic discusses a product feature in active development, and is subject to change at any time.

To configure SharePoint for external access, there are two procedures you must complete:

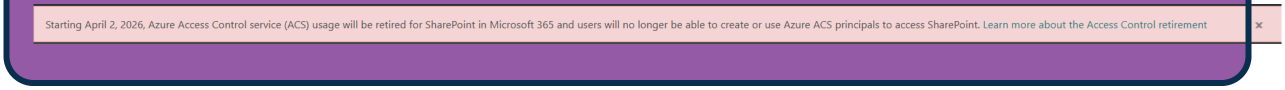
1. Configure SharePoint Review Mode
2. Configure external access.

We'll discuss each step in order, below.

Configure SharePoint Review Mode

You may encounter the following warning on the web page when performing the steps that follow. The BP Logix Team is aware of this issue

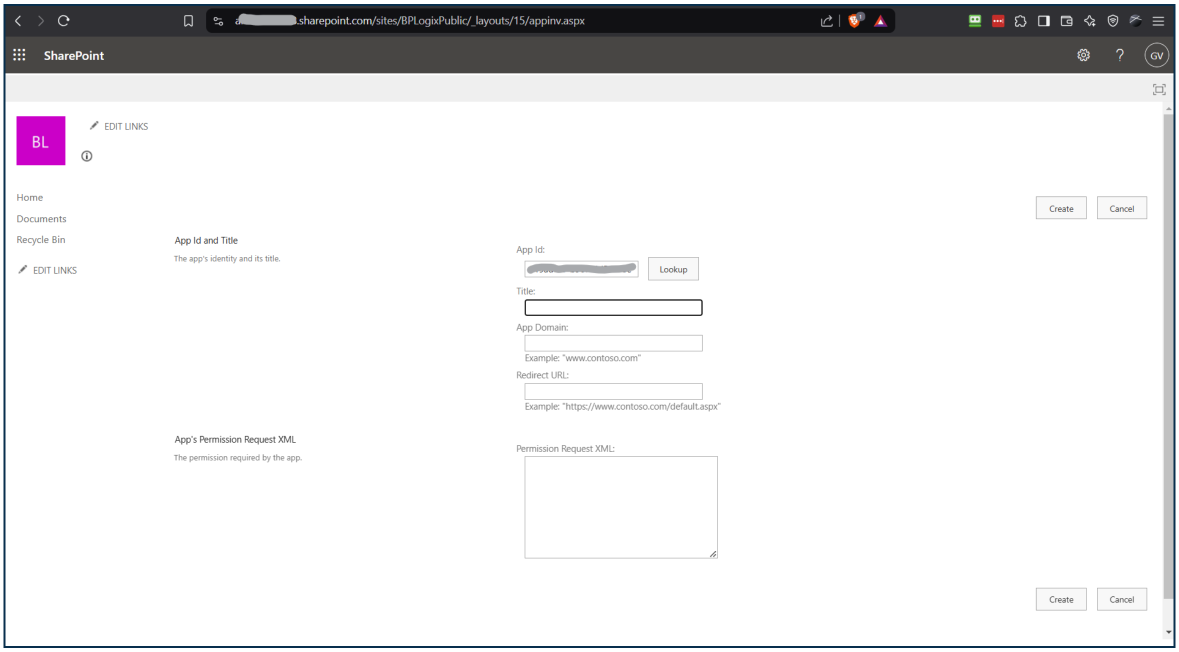
and actively working with Microsoft to prevent any future service disruptions or configurations difficulties before this April 2026 deadline.



Starting April 2, 2026, Azure Access Control service (ACS) usage will be retired for SharePoint in Microsoft 365 and users will no longer be able to create or use Azure ACS principals to access SharePoint. Learn more about the Access Control retirement ×

In order for Process Director to properly create links to Word documents in Review (or “Track Changes”) mode, an additional admin action must be performed. Otherwise, users will encounter errors open forms with attachments intended to be reviewed.

1. Navigate to `https://<your-tenant-name>.sharepoint.com/<“sites” or “teams”>/<your-site-or-team>/_layouts/appinv.aspx`.
2. Enter the Site client ID in the App Id field and then click the Lookup button.

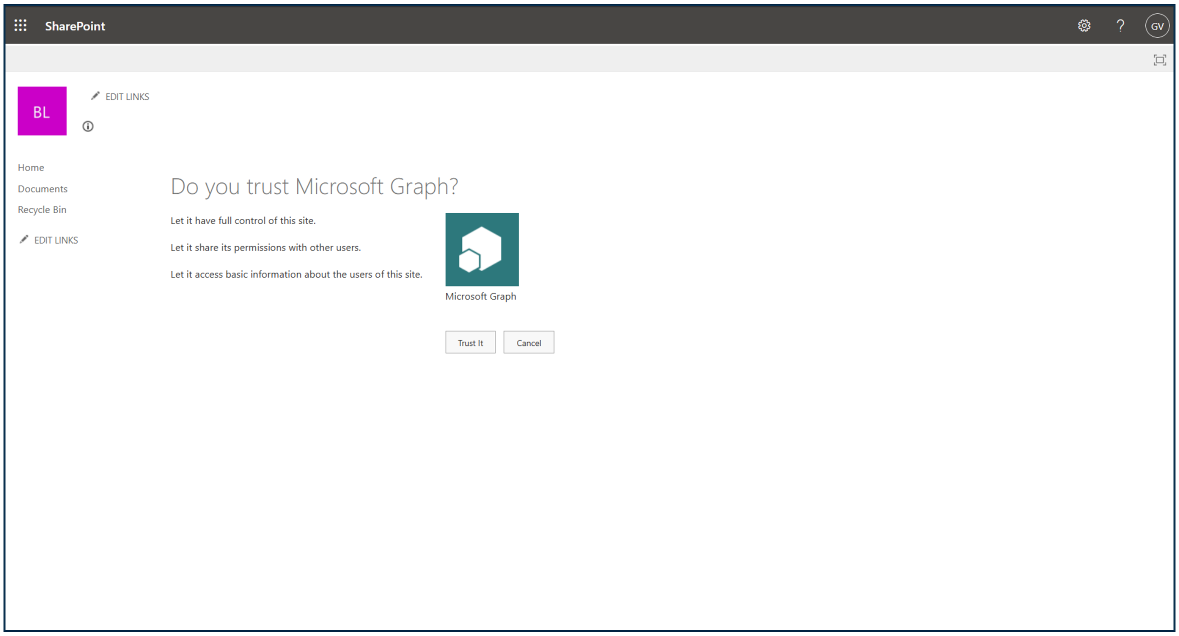

[redacted].sharepoint.com/sites/BPLogixPublic/_layouts/15/appinv.aspx
SharePoint
GV
BL
EDIT LINKS
Home
Documents
Recycle Bin
EDIT LINKS
Create
Cancel
App Id and Title
The app's identity and its title.
App Id:
[redacted]
Lookup
Title:
App Domain:
Example: "www.contoso.com"
Redirect URL:
Example: "https://www.contoso.com/default.aspx"
App's Permission Request XML
The permission required by the app.
Permission Request XML:
Create
Cancel

The Title and possibly some of the other fields should be automatically filled with data related to the app registration.

3. Add `<your-tenant-name>.sharepoint.com` to the App Domain field.
4. Next, paste the following text into the Permission Request XML field, then click the Create button.

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
    <AppPermissionRequest Scope-
e="http://sharepoint/content/sitecollection/web"
     Right="FullControl" />
</AppPermissionRequests>
```

5. Next you'll be asked to confirm the operation by trusting the application. Click the Trust It button.



Do you trust Microsoft Graph?

Let it have full control of this site.

Let it share its permissions with other users.

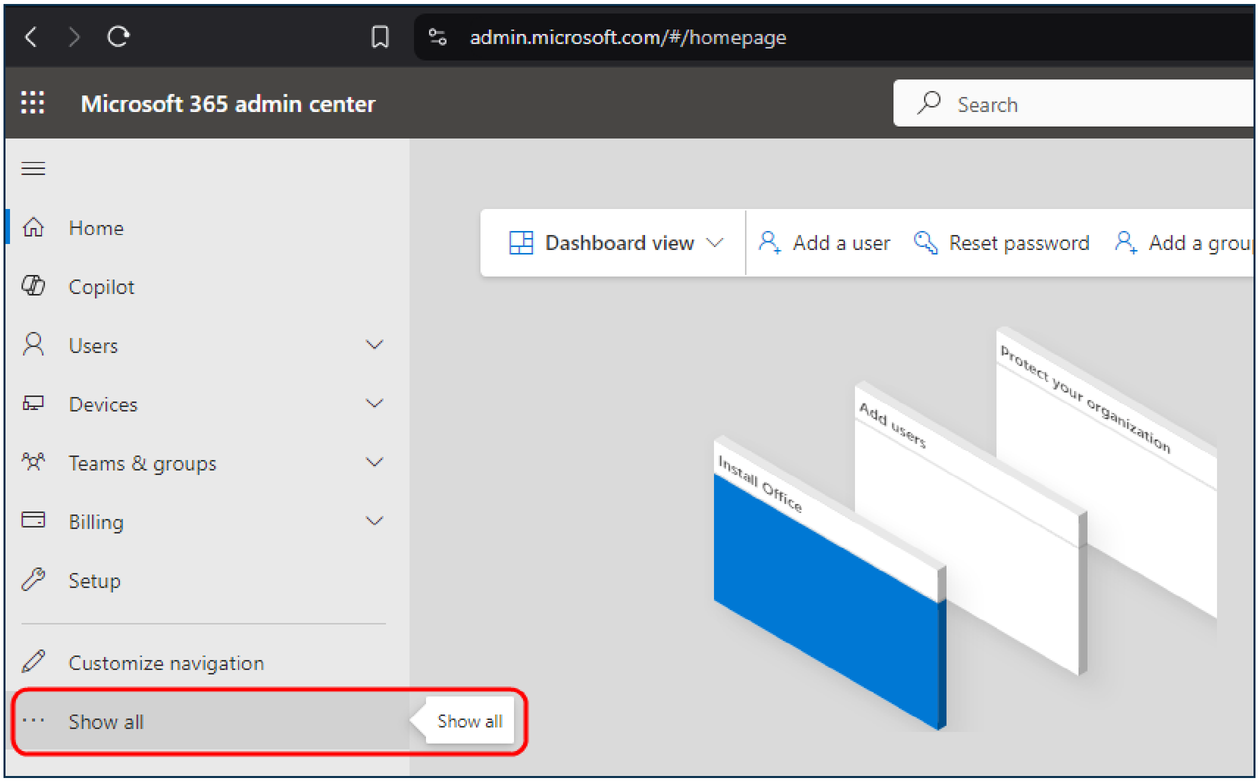
Let it access basic information about the users of this site.

Once you've completed these step, SharePoint should now be configured to enable review mode, which will enable external users to review and edit documents, after yo set up external access below.

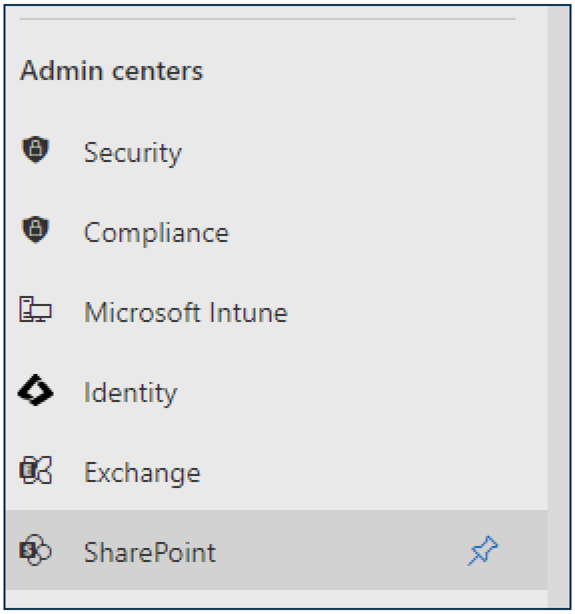
Configure External Access

Once you've configured Azure/Entra, and transmitted the appropriate information to BP Logix, you may need to make some changes to your SharePoint installation to enable its access for CDA, as a final step in this process. For some customers, this won't be necessary, since every user who accesses the documents for CDA will be valid, authenticated users of your Azure/Entra tenant. In many cases, however, you'll need to provide access to the documents for review or editing by users outside of your organization. In that case, you'll need to provide those external users with access to your SharePoint installation, to enable them to participate.

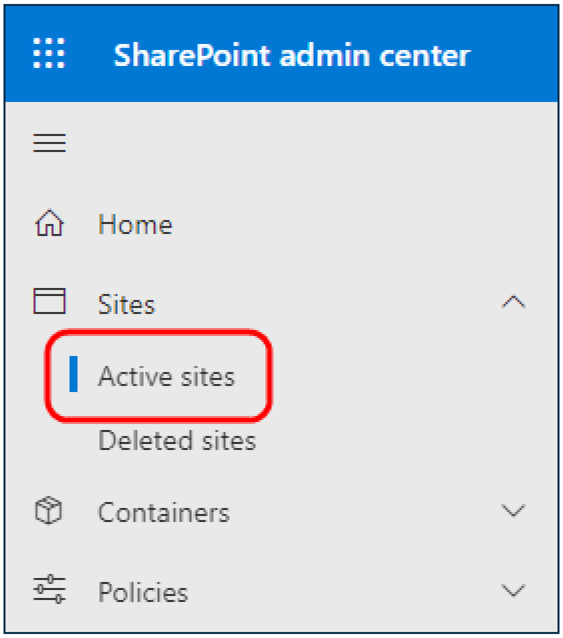
To do so, you'll first need to go to admin.microsoft.com to access your **Microsoft 365 Admin Center**. Once the admin center main page opens, you'll need to click the Show All menu item that appears in the sidebar on the left side of the page. Clicking this item will expand the sidebar to show additional menu items.



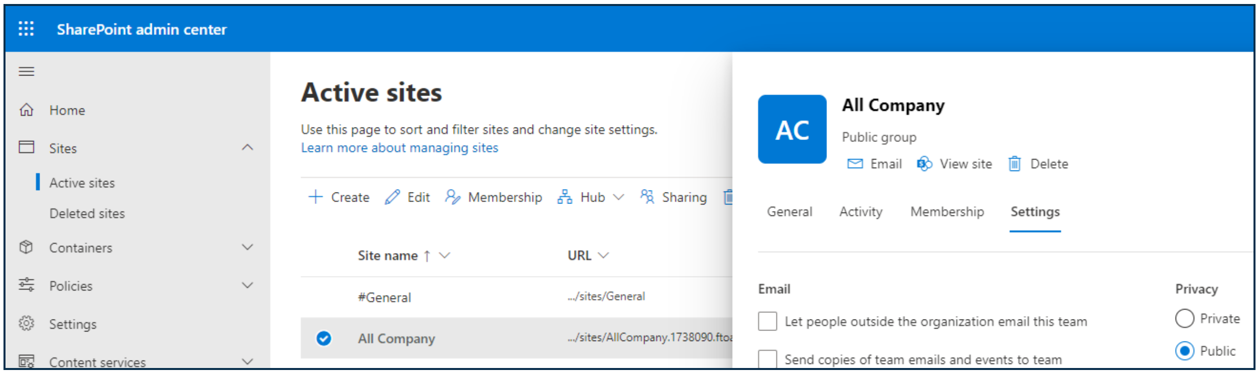
When the new menu items appear, you'll need to scroll down to the Admin Centers section, and select the SharePoint menu item.



Clicking the SharePoint menu item will open a new browser tab to display the **SharePoint Admin Center**. On the left sidebar of the page, you'll need to click the Sites menu to expand it, then select the Active Sites menu item.



Clicking Active Sites will display the Active Sites page, listing all of your currently active SharePoint sites. Find the Web site in the list of sites, and click on it to select and expand it. When you do so, an informational pane for the selected site will appear on the right side of the page.



Active sites

Use this page to sort and filter sites and change site settings.
Learn more about managing sites

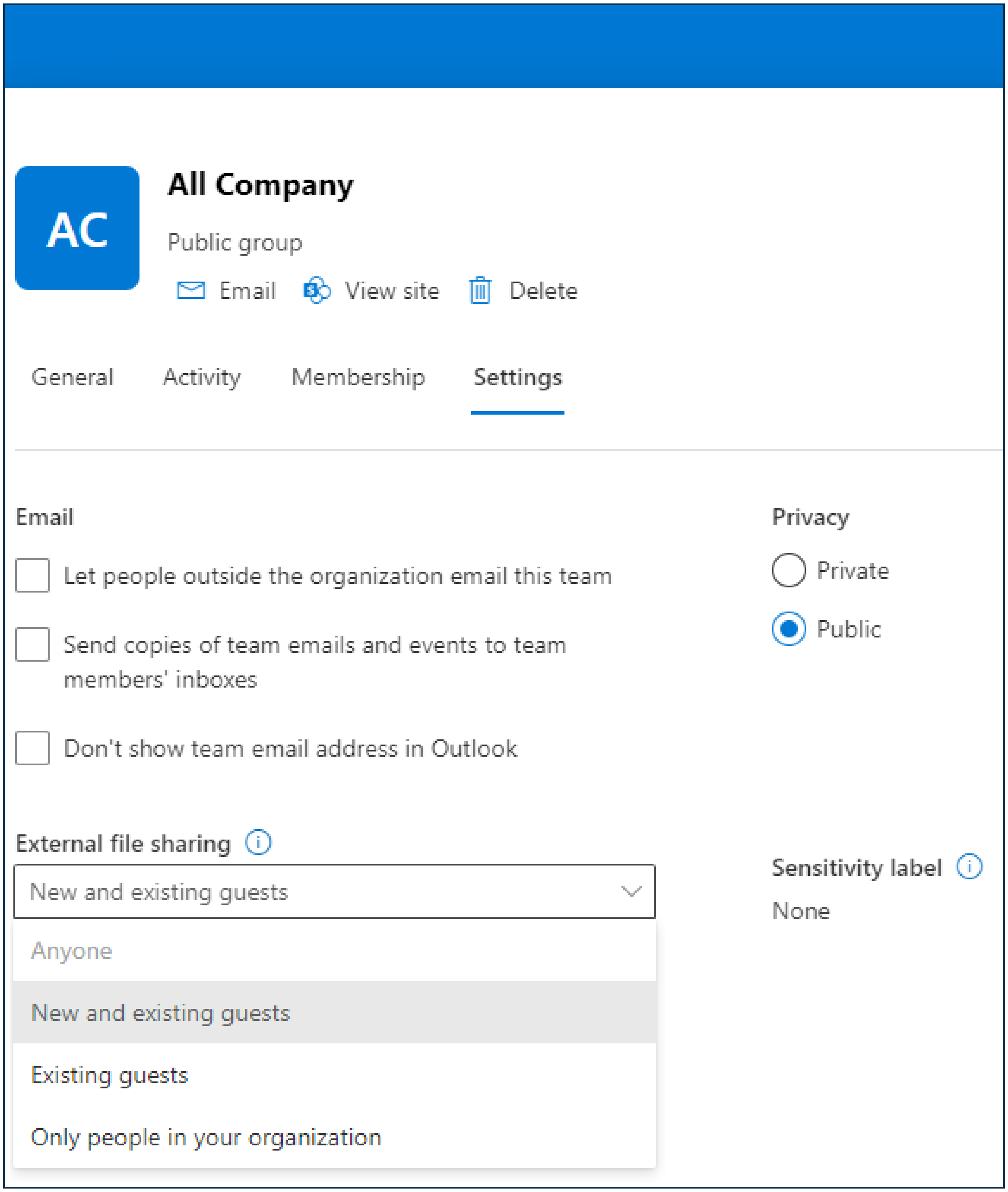
Site name ↑	URL
#General	.../sites/General
All Company	.../sites/AllCompany.1738090.fto

AC All Company
Public group

Email
□ Let people outside the organization email this team
□ Send copies of team emails and events to team

Privacy
○ Private
● Public

In the informational pane, a series of tabs will be displayed, just below the header information and logo. You'll need to click the Settings tab to display its contents.



Email

□ Let people outside the organization email this team

□ Send copies of team emails and events to team members' inboxes

□ Don't show team email address in Outlook

Privacy

○ Private

● Public

External file sharing

New and existing guests

- Anyone
- New and existing guests
- Existing guests
- Only people in your organization

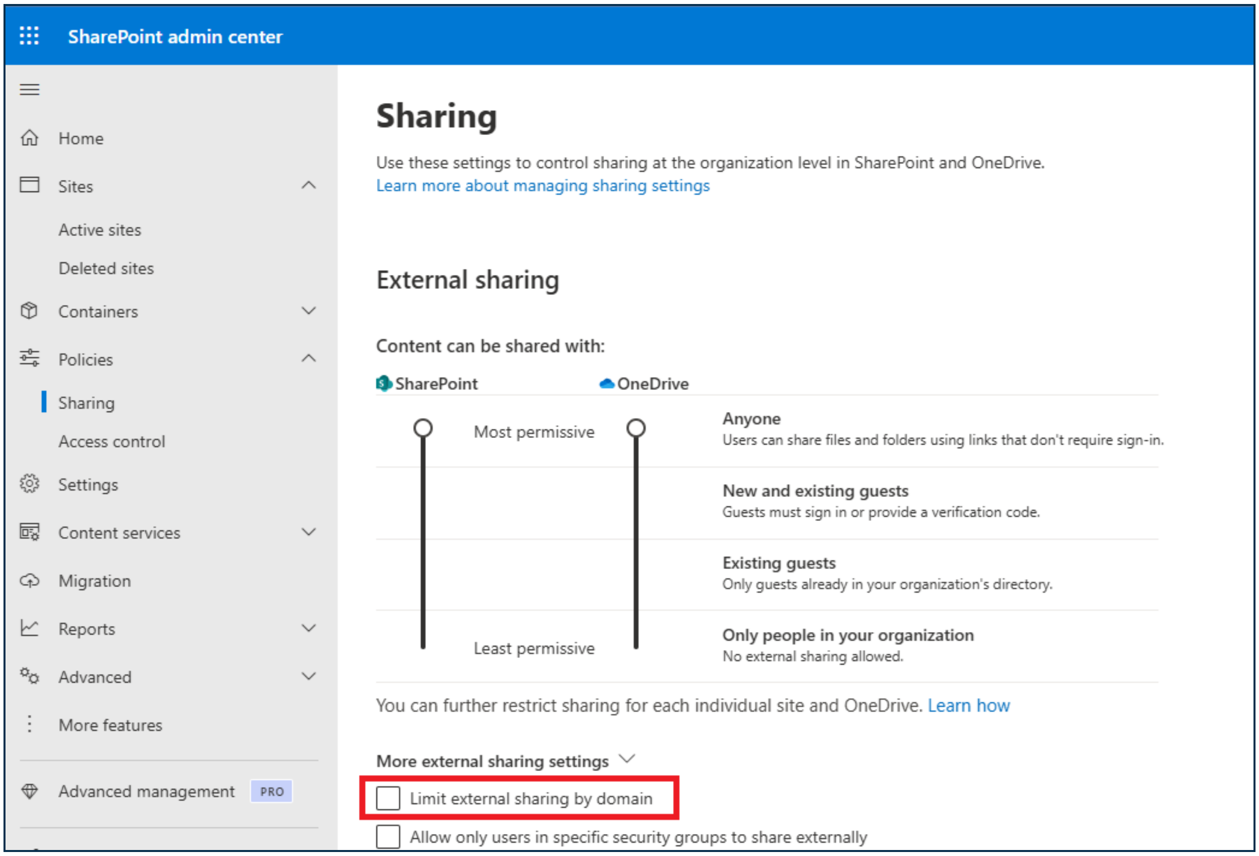
Sensitivity label

None

In the Settings tab, select either *Anyone* or *New and existing guests* from the External file sharing property options. You must choose one of these options to enable external sharing to users from outside of your organization. There are different security implications for each item. *New and existing guests* is a more secure option that verifies external users by sending a one-time password (OTP) to their email address. While more secure, some organizations may find this too cumbersome for their use-case. The Anyone selection enables access to documents without the additional OTP verification. Irrespective of which option you choose, it will require specially crafted URLs to access individual documents. You'll need to refer to Microsoft's SharePoint documentation for more information about that.

External Sharing

In some SharePoint installations, there may be some additional settings that prevent external users, i.e., those outside of your Azure/M365 tenant, from accessing shared documents. This issue can occur if the Limit external sharing by domain property is enabled in your global (tenant-wide) SharePoint settings. This feature resides within the SharePoint Admin Center under Policies > Sharing.



Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive.
Learn more about managing sharing settings

External sharing

Content can be shared with:

SharePoint   OneDrive

Most permissive

Anyone
Users can share files and folders using links that don't require sign-in.

New and existing guests
Guests must sign in or provide a verification code.

Existing guests
Only guests already in your organization's directory.

Only people in your organization
No external sharing allowed.

Least permissive

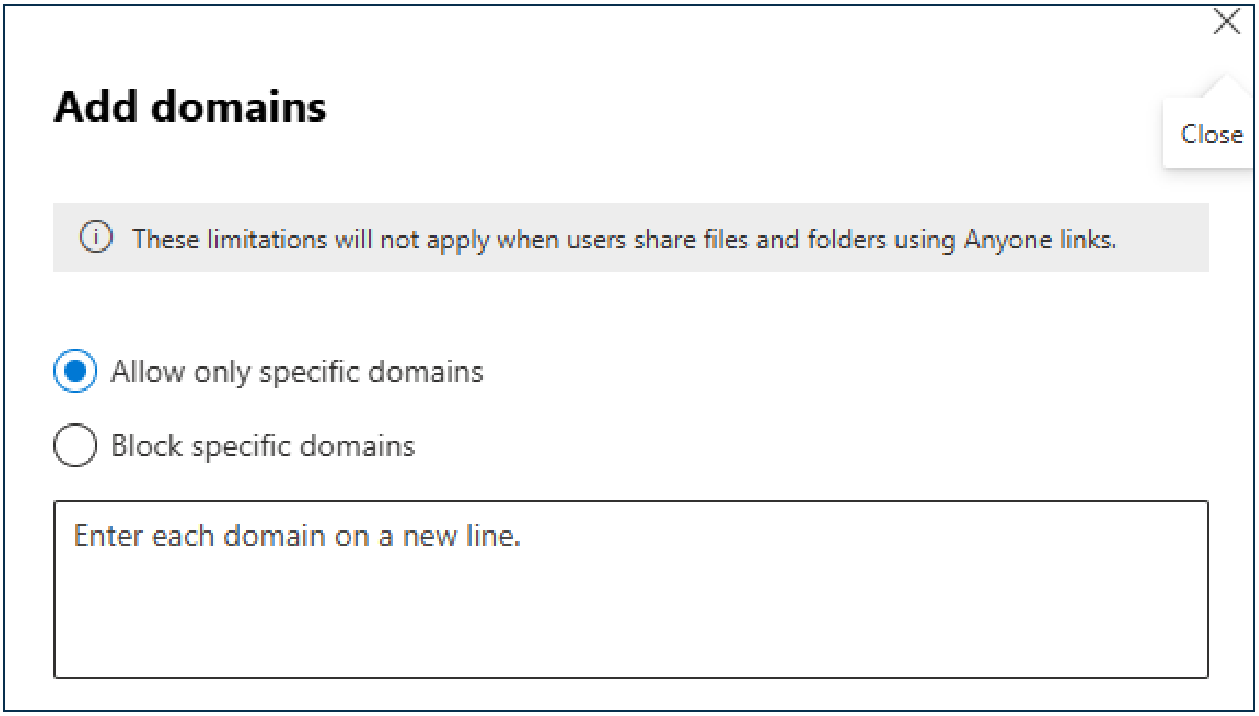
You can further restrict sharing for each individual site and OneDrive. Learn how

More external sharing settings

□ Limit external sharing by domain

□ Allow only users in specific security groups to share externally

Either disable this feature altogether by unchecking it or, if you wish it to remain checked, you must be sure that all of the expected domains for email addresses to be used on the system are included in the Add Domains screen for this property setting. You can also configure the inverse, and exclude specific domains, though, in most cases, this will not be the optimal option.



Add domains

Close

These limitations will not apply when users share files and folders using Anyone links.

● Allow only specific domains

○ Block specific domains

Enter each domain on a new line.

Conclusion

Once you've set the desired External file sharing property option, you can click the Save button to save it. Once saved, the appropriate external users will be able to access the documents they need to access when participating in the editing/collaboration process.

This step, combined with the changes made to your Process Director installation, should fully enable M365 for use with the product's CDA feature.

Other M365 CDA Configuration Topics

M365 CDA Overview

M365 CDA Configuration Process

- Configure SAML access for PD in Azure.
- Create and configure “Full Scope” App Registration for PD in Azure/Entra.
- Create and configure “Site” App Registration for PD in Azure/Entra.
- Grant proper “Site” App Registration permission.
- Securely exchange “Site” App Registration and related settings with Process Director.
- Configure Process Director to leverage the application registration.