SSO Identity Provider Integration

SYSPRO 8

Reference Guide

Published: January 2024

SYSPRO

CONTENTS

SSO Identity Provider Integration

SSO Identity Provider Integration

Exploring

Where it fits in?

Enhancing user convenience while fortifying system security, the **SSO Identity Provider Integration** feature empowers users to access SYSPRO using trusted identity providers, creating a unified and secure authentication flow.

Once authenticated, SYSPRO users are automatically logged in, without them having to enter the traditional SYSPRO username and password.

Functionality

With **SSO Identity Provider Integration**, you can login to the ***SYSPRO Web UI (Avanti)*** or ***SYSPRO Desktop*** using one (or more) of the following identity providers:

- Google
- Microsoft
- LinkedIn

In addition, **Multi-Factor Authentication** (MFA) inherently becomes a part of your SSO solution, thereby strengthening your security posture.

Benefits

This feature addresses a significant challenge faced by larger organizations who need to manage multiple employees and credentials and provides the following benefits:

- Enhanced security measures
- Reduced administrative burden associated with managing user credentials and passwords
- Simplified user experience

Navigation

The programs related to this feature are accessed from the **Program List** of the SYSPRO menu:

- *Program List* > *Administration* > *Security* > *Authentication*

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Terminology

Single Sign-on (SSO)

A robust authentication mechanism designed to minimize the vulnerabilities associated with traditional username and password combinations by integrating a trusted authentication technology. This enables users to seamlessly access SYSPRO using a single set of credentials, eliminating the need for multiple logins and reducing the risk of unauthorized access.

Within SYSPRO, the following single sign-on methods are available:

- SSO using Active Directory
  - This method is ideal for sites using the ***SYSPRO Desktop*** user interface, as each user has to login to their Windows client environment. This option allows a site to leverage the user authenticated by Windows to login to SYSPRO.
  - This option is not suitable for users using the ***SYSPRO Web UI (Avanti)*** as users can connect via any device (such as a phone or tablet) where Windows authentication is not appropriate.
- SSO Identity Provider Integration
  - Each Identity provider allows various additional validation over the traditional user name and password, including the use of authenticator applications, and other forms of Multi-Factor Authentication. These providers are often already in use across the organization, so users are already comfortable using these common dialogs.
  - The **SSO Identity Provider Integration** works across the ***SYSPRO Desktop*** and ***SYSPRO Web UI (Avanti)*** user interfaces, providing a consistent experience across SYSPRO interfaces and the rest of the organization.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Starting

Prerequisites

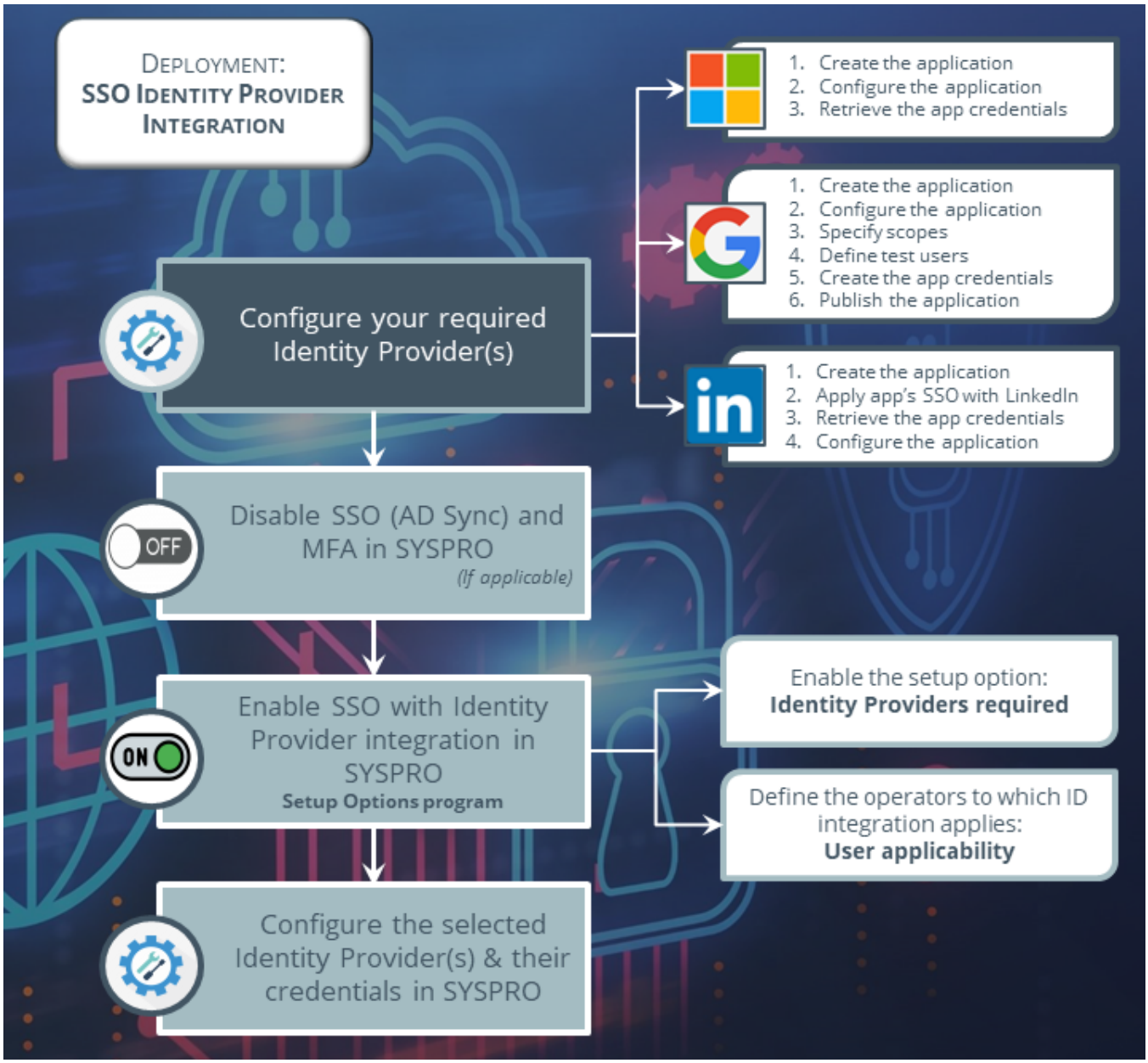
Setup Options

To use this feature, the following setup option(s) must be enabled:

Setup Options > System Setup > Login

- Identity providers required
- User applicability

Deploying



Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Identity Provider Configuration

The following explains how to configure each of the supported identity providers:

Microsoft

When selecting to use **Microsoft** as your identification provider, proceed as follows for the provider configuration:

Step 1: Create the application

1. From your browser, navigate to the following URL:

   https://portal.azure.com/

2. Sign into the **Microsoft Azure** portal with your appropriate credentials.
3. Navigate to the **Azure Active Directory** resource:
   a. Select to add an **App Registration**.

   > For detailed explanations on this process, refer to the following **Microsoft** documentation:
   >
   > https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app#register-an-application

   b. Indicate an appropriate name for the application.

   > **FOR EXAMPLE:**
   >
   > SYSPRO Authentication

   > Users of your application might see the display name when they use the app, for example during sign-in. You can change the display name at any time and multiple app registrations can share the same name. The app registration's automatically generated Application (client) ID, not its display name, uniquely identifies your app within the identity platform.

   c. Select the supported account types:

   - **Accounts in any organizational directory**

     Select this option if you want users in any Azure Active Directory (Azure AD) tenant to be able to use your application. This option is appropriate if, for example, you're building a software-as-a-service (SaaS) application that you intend to provide to multiple organizations.

     This type of app is known as a multitenant application in the **Microsoft**

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

- identity platform.

d. Against the **Redirect URI** field, select **Public client/native (mobile & desktop)**.

e. Select **Register** to complete the initial app registration.

Once registration completes, the Azure portal displays the app registration's **Overview** pane.

Step 2: Configure the application

Once your application has been registered, navigate to the **Authentication** section from the **Manage** menu:

1. From the **Platform configurations**, select **Add a platform**.
2. From the **Configure platforms** screen, proceed as follows for single sign-on access within the SYSPRO Web UI (Avanti) and/or SYSPRO Desktop:

Web

a. Select **Web**.

b. Within the **Redirect URIs** section, add `http://localhost` to the entry.

You will add more to this entry in a later step.

c. Within the **Implicit grant and hybrid flows** section, enable the **Access tokens** option.

d. Select **Configure** to complete the platform configuration.

e. Save your changes.

Desktop

a. Select **Mobile and desktop applications**.

b. Enable the **https://login.microsoftonline.com/common/oauth2/nativeclient** option.

c. Select **Configure** to complete the platform configuration.

d. Once your platform has been configured, the Azure portal displays the app registration's **Overview** pane, from where you can view the Application (client) ID. Also called the client ID, this value uniquely identifies your application in the **Microsoft** identity platform.

Record this client ID, as you'll need it later for the configuration within SYSPRO.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

3. From the **Authentication** screen, select the **Web** configuration to add your required URLs within the **Redirect URIs** section.

> **FOR EXAMPLE:**
>
> Your users may access the SYSPRO Web UI (Avanti) from various URLs.
>
> A few examples could be:
>
> - http://localhost/SYSPROAvanti
> - https://zalpusername01/SYSPROAvanti/
> - https://zalpusername01.sysproglobal.com/SYSPROAvanti/

View the following article to learn more about the Microsoft URL restrictions: https://learn.microsoft.com/en-us/azure/active-directory/develop/reply-url

Step 3: Retrieve the application credentials

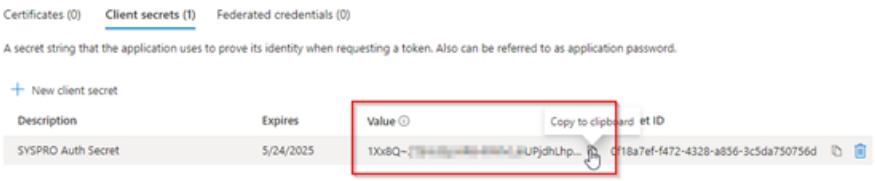
The next step is to retrieve the credentials created for the application (i.e. client secret and client ID):

1. Once your application has been registered, navigate to the **Certificates & secrets** section from the **Manage** menu. This allows you to retrieve the Client Secret required for Web applications.
2. Select the **New client secret** function.
3. Indicate a **Description** for the client secret.
4. Indicate your required period against the **Expires** field.
5. Select the **Add** function.

Once completed, you are returned to the **Certificates & secrets** screen, from where you can retrieve the client secret.

Record this client secret, as you'll need it later for the configuration within SYSPRO.

Ensure to record the **Value** and not the **ID**:



Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Google

When selecting to use **Google** as your identification provider, proceed as follows for the provider configuration:

Step 1: Create the application

1. From your browser, navigate to the following URL:

   https://console.cloud.google.com/

2. Sign into the **Google Cloud** portal with your appropriate credentials.
3. Click the **Select a project** button.
   a. From the **Select a project** screen, select the **NEW PROJECT** option.
   b. At the **Project name** field, indicate an appropriate name for your application.

   > **FOR EXAMPLE:**
   > SYSPROOAuth

   c. Select the **Create** function.

   Once saved, you are returned to the **Google Cloud** home page and a notification indicates that your application has been created.

Step 2: Configure the application

1. From the **Google Cloud** home page, select the project you have just created.
2. From the hamburger menu, select **APIs & Services**, followed by **OAuth consent screen**.

   From the **OAuth consent screen**:
   a. Indicate the **User Type** as **External**.
   b. Select the **Create** function.
3. The **Edit app registration** screen is displayed. Proceed as follows:

   ### App information

   a. Enter an appropriate name for your application within the **App name** field.

   > **FOR EXAMPLE:**
   > SYSPRO OAuth

   This name is displayed to your users (in the consent screen) when they sign

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

in for the first time.

b. Within the **User support email** field, indicate the email address to which your users can direct any queries.

App logo

a. Optionally upload and assign the logo you want associated with the application.

   This helps your users recognize your app and is displayed on the OAuth consent screen.

b. After you upload a logo, you will need to submit your app for verification.

> For more detailed information regarding the verification, view the following **Google** documentation:
>
> https://support.google.com/cloud/answer/9110914

Developer contact information

a. Within the **Email addresses** field, enter the email address(es) for the developer contact(s).

> These email addresses are for **Google** to notify you about any changes to your project.

4. Select the **SAVE AND CONTINUE** function.

   Once saved, you are moved onto the next step in the Google configuration.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Step 3: Specify your scopes

From the **Scopes** section, you need to specify the scopes that this application will request. SYSPRO only requires read scopes on the user's profile.

Scopes express the permissions that you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account.

For more detailed information regarding scopes, view the following **Google** documentation:

https://developers.google.com/identity/protocols/oauth2/scopes

1. Select the **ADD OR REMOVE SCOPES** function.
2. From the **Update selected scopes** screen, enable the following entries:
   - .../auth/userinfo.email
   - .../auth/userinfo.profile
   - openid
3. Select the **Update** function.

   As the selected scopes are all non-sensitive, they are then displayed within the **Your non-sensitive scopes** section.
4. Select the **SAVE AND CONTINUE** function.

   Once saved, you are moved onto the next step in the Google configuration.

Step 4: Define the test users

While publishing status is set to *Testing*, only test users are able to access the app.

For more detailed information regarding unverified apps, view the following **Google** documentation:

https://support.google.com/cloud/answer/7454865

1. From the **Test users** section, use the **ADD USERS** function to indicate the email addresses of the users who will be testing your application.

   Ensure to add your own email address as well.
2. Select the **SAVE AND CONTINUE** function.

   Once saved, you are presented with a summary of your application's configuration.
3. Select the **BACK TO DASHBOARD** function.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Step 5: Create the required credentials (for desktop and web)

The next step is to create the credentials required for desktop and web access (depending on your requirements).

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID.

For more detailed information regarding OAuth 2.0 configuration, view the following **Google** documentation:

https://support.google.com/cloud/answer/6158849

https://developers.google.com/identity/protocols/oauth2

1. From the hamburger menu, select **Credentials**.

   This navigates you to the **Credentials** screen.

2. Select the **CREATE CREDENTIALS** function, followed by the **OAuth client ID** option.

   This opens the **Create OAuth client ID** screen. Proceed as follows for single sign-on access within the SYSPRO Web UI (Avanti) and/or SYSPRO Desktop:

   ### Web

   a. Within the **Application type** field, select **Web application**.

   b. Enter an applicable name for the OAuth 2.0 client.

   > **FOR EXAMPLE:**
   >
   > SYSPROOAuthWebApp

   This name is only used to identify the client in the console and will not be shown to end users.

   c. Within the **Authorised JavaScript origins** section:

   Specify the appropriate URL host name that users will use to interact with the SYSPRO Web UI (Avanti).

   > **FOR EXAMPLE:**
   >
   > - http://localhost
   > - https://zalpusername01.sysproglobal.com

   d. Within the **Authorised redirect URIs** section:

   Specify the appropriate URL host name that users will use to interact with the SYSPRO Web UI (Avanti).

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

> **FOR EXAMPLE:**
>
> - http://localhost
> - https://zalpusername01.sysproglobal.com

e. Select the **CREATE** function.

Once created, the **OAuth client created** screen is displayed, from where your newly created Client ID and secret are displayed.

> Ensure to record the **Client ID** and the **Client secret**, as you'll need them later for the configuration within SYSPRO.

Desktop

a. Within the **Application type** field, select **Desktop app**.

b. Enter an applicable name for the OAuth 2.0 client.

> **FOR EXAMPLE:**
>
> SYSPROOAuthDesktopApp

This name is only used to identify the client in the console and will not be shown to end users.

c. Select the **CREATE** function.

Once created, the **OAuth client created** screen is displayed, from where your newly created Client ID and secret are displayed.

> Ensure to record the **Client ID** and the **Client secret**, as you'll need them later for the configuration within SYSPRO.

Step 6: Publish your application

Your application is now ready, but currently in a *Testing* phase, which means that access is currently only allowed for the email addresses added within step 4. Therefore, the last step is to publish your application (so that its available for all of your users):

1. From the hamburger menu, select **OAuth consent screen**.
2. Within the **Publishing status** section, select the **PUBLISH APP** function.
3. Confirm the system prompt to proceed with pushing the application to production.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

LinkedIn

When selecting to use **LinkedIn** as your identification provider, proceed as follows for the provider configuration:

Step 1: Create the application

1. From your browser, navigate to the following URL:

   https://developer.linkedin.com/
2. Sign into the **LinkedIn Developers** portal with your appropriate credentials.
3. Select the **My apps** option from the menu.
4. From the **My apps** page, select the **Create app** function:
   a. At the **App name** field, indicate an appropriate name for your application.

   > **FOR EXAMPLE:**
   >
   > SYSPRO OAuth

   b. Within the **LinkedIn Page** field, indicate the URL for your company's LinkedIn page that will be associated with your app.

   > **FOR EXAMPLE:**
   >
   > https://www.linkedin.com/company/syspro/mycompany/

   For more detailed information regarding LinkedIn page associations, view the following **LinkedIn** documentation:

   https://www.linkedin.com/help/linkedin/answer/a548360

   c. At the **App logo** section, upload the appropriate logo that will be displayed to users when they authorize with your application.
   d. Familiarize yourself with the LinkedIn **Legal agreement** and select the **I have read and agree to these terms** option.
   e. Select the **Create app** function.

   Once created, you are returned to the **Products** page.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Step 2: Apply the application's sign in with LinkedIn

The next step is to apply the sign in with LinkedIn capability:

For more detailed information regarding sign in with LinkedIn, view the following documentation:

https://learn.microsoft.com/en-us/linkedin/consumer/integrations/self-serve/sign-in-with-linkedin

1. From the **Additional available products** list, select the **Request access** option against the **Sign In with LinkedIn** product.
2. A confirmation window is displayed, from where you can familiarize yourself with the LinkedIn terms of use.

   Select the **I have read and agree to these terms** option, followed by the **Request access** function.

Once created, you are returned to the **Products** page.

Step 3: Retrieve the application credentials

Once your application has been defined with single sign-on, you need to retrieve the credentials created for the application (i.e. client secret and client ID):

1. While still in your newly created application, navigate to the **Auth** page.
2. Within the **Application credentials** section, take note of the **Client ID** and **Client Secret**.

Ensure to record the **Client ID** and the **Client secret**, as you'll need them later for the configuration within SYSPRO.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Step 4: Configure the application

For access to LinkedIn member data, your application must be authenticated. LinkedIn relies on the industry standard **OAuth 2.0 protocol** for granting access.

For more detailed information regarding OAuth 2.0 authorization for the LinkedIn API, view the following documentation:

https://learn.microsoft.com/en-us/linkedin/shared/authentication/authentication

Proceed as follows while still in your newly created application:

1. Within the **Auth** page, navigate to the **OAuth 2.0 settings** section.
2. Select the edit function (i.e. pencil icon) against the **Authorized redirect URLs for your app** option.

   This will allow you to add your redirect URLs for the web and/or desktop requirements.
3. Select the **+ Add redirect URL** function.

Web

Specify the appropriate URL host name that users will use to interact with the SYSPRO Web UI (Avanti).

> **FOR EXAMPLE:**
>
> - http://localhost/SYSPROAvanti
> - http://zalpusername01/SYSPROAvanti/
> - https://zalpusername01.sysproglobal.com/SYSPROAvanti/

Desktop

Specify `http://locahost` as the URL host name that users will use to interact with the SYSPRO Desktop.

These redirect URLs for both web and desktop are case-sensitive.

4. Once you've added the appropriate redirect URLs, select the **Update** function.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

SYSPRO Configuration

Once you have completed your application configuration with the required the identity provider (s), the final step is to configure SYSPRO to support the selected provider integration:

1. Launch ***SYSPRO 8 2023*** (or later) and open the **Setup Options** program (*SYSPRO Ribbon bar > Setup*).
2. Navigate to the **Login** form within the **System Setup** category (*Setup Options > System Setup > Login*).
3. Ensure that the following setup options are disabled:
    - Active Directory sync required
    - Multi-factor authentication required

    The **SSO Identity Provider Integration** feature supersedes the previous methods of **SSO using Active Directory** and **Multi-Factor Authentication**.

    Therefore, it is necessary to disable these previous capabilities, before enabling the new **SSO Identity Provider Integration**, as the use of both methods simultaneously is not possible.
4. Within the **SINGLE SIGN-ON IDENTITY PROVIDERS** section, enable the **IDENTITY PROVIDERS REQUIRED** option.
5. Against the **USER APPLICABILITY** option, indicate to which operators this integration applies:
    - **All operators except "Admin"**

      This dictates that all operators require Identity Provider Authentication when logging into SYSPRO, except for SYSPRO operators with the operator code ADMIN.

      Be careful when selecting this option if you don't have an ADMIN operator.
    - **All operators except administrators**

      This dictates that all operators require Identity Provider Authentication when logging into SYSPRO, except for SYSPRO administrators.

      This is useful if the identity provider's system is not available (e.g. due to temporary network or provider unavailability) and operators can't access the defined authentication method in order to login to SYSPRO. An administrator can then still access SYSPRO (without requiring validation by the

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

- authentication methods that have been configured) to suspend the Identity Provider Authentication and allow operators to login.

  Therefore, all administrators should use strong operator passwords.

- **Specific operators**

  This dictates that Identity Provider Authentication only applies to specific operators.

  Select the **Define specific operators** hyperlink to indicate the operators to which this Identity Provider authentication applies (using the **Single Sign-On Operator Configuration**[1] program).

6. Select the **Configure identity providers** hyperlink.

   This opens the **Single Sign-On Provider Configuration**[2] program, from where you can configure your selected identity provider(s):

   a. Select your required provider from the listview, followed by its configuration hyperlink within the **Configure** column.

   b. Within the configuration screen, define your requirements for the Desktop authentication and/or Web authentication, as per your organization's requirements:

      Desktop authentication

Field	Action
Enabled	This option must be enabled to allow desktop authentication using the selected identity provider.
Default provider	Enable this option against the identity provider that you require as the default for desktop authentication. This option cannot be enabled for more than one provider at a time.

[1]Program: IMPSSP
[2]Program: IMPSSI

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Field	Action
Client ID	Indicate the Client ID created during your setup of the identity provider:  = This is your desktop client ID generated using the **Azure App Registration** portal.  = This is your desktop client ID generated using the **Google Developer** Console.  = This is your client ID generated using the **LinkedIn Developer Network** portal.
Client secret	Indicate the Client Secret created during your setup of the identity provider:  = *Not applicable for desktop authentication.*  = This is your desktop client secret generated using the **Google Developer** Console.  = This is your client secret generated using the **LinkedIn Developer Network** portal.

Web authentication

Field	Action
Enabled	This option must be enabled to allow web authentication using the selected identity provider.
Default provider	Enable this option against the identity provider that you require as the default for web authentication.  This option cannot be enabled for more than one provider at a time.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Field	Action
Client ID	Indicate the Client ID created during your setup of the identity provider: = This is your web client ID generated using the **Azure App Registration** portal. = This is your web client ID generated using the **Google Developer** Console. = This is your client ID generated using the **LinkedIn Developer Network** portal.
Client secret	Indicate the Client Secret created during your setup of the identity provider: = This is your web client secret generated using the **Azure App Registration** portal. = This is your web client secret generated using the **Google Developer** Console. = This is your client secret generated using the **LinkedIn Developer Network** portal.

c. Once you have completed your provider configuration, use the **Test connection** hyperlink to ensure all entries are valid and that the connection to each provider is configured correctly.

7. Exit the program.
8. Restart SYSPRO for your changes to take effect.

Considerations:

If you enable and configure SSO Identity Provider Integration using the SYSPRO Web UI (Avanti):

- You may need to refresh your browser and restart your SYSPRO Web UI (Avanti) instance for changes to take effect.

If you enable and configure SSO Identity Provider Integration using the SYSPRO Desktop UI:

- You must restart your SYSPRO Web UI (Avanti) instance for changes to reflect in the Web UI.
- This applies to enabling the capability, as well as any changes made to the Identity Provider configuration.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Restrictions and Limits

- The **SSO Identity Provider Integration** feature supersedes the previous methods of **SSO using Active Directory** and **Multi-Factor Authentication**.

  Therefore, it is necessary to disable these previous capabilities, before enabling the new **SSO Identity Provider Integration**, as the use of both methods simultaneously is not possible.
- This functionality is not yet available with the following user interfaces, but is planned for a later release:
  - SYSPRO Espresso
  - e.net Solutions

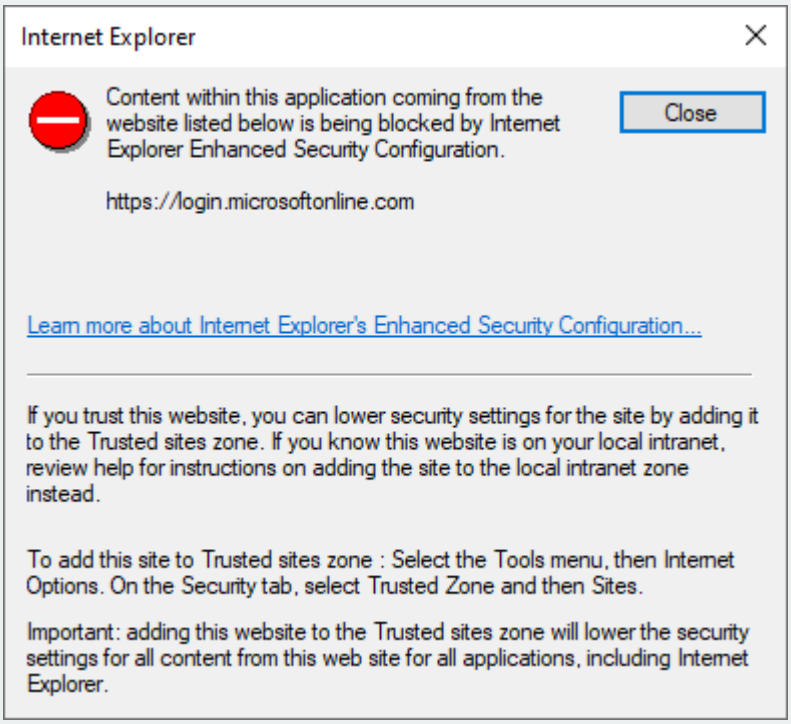
Hints and Tips

- When using Microsoft authentication:

  Certain Microsoft URLs may need to be added to the Trusted Sites zone within your internet options.

  FOR EXAMPLE:

  If a URL is currently blocked (i.e. not a Trusted Site), then an error message similar to the following example is displayed when an operator attempts to login using Microsoft:



Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Solving

FAQs

Configuration & Usage

What happens if I enable SSO Identity Provider Integration without enabling any identity providers?

If **SSO Identity Provider Integration** is enabled (i.e. the **IDENTITY PROVIDERS REQUIRED** setup option is enabled) but no Desktop UI providers have been enabled:

- Operators are prompted with the latest login dialog (which includes the identity providers) however their only choice available will be the standard SYSPRO Authentication (i.e. username and password).

If **SSO Identity Provider Integration** is enabled but no Web UI providers have been enabled:

- Operators are prompted with the latest login dialog however no identity provider authentication is displayed. Therefore, their only choice will be the standard SYSPRO Authentication (i.e. username and password).

How does SSO Identity Provider Integration impact operator timeouts?

A timeout occurs when an operator remains inactive within the system for a specified period. In such cases, to maintain security, the operator may be prompted to re-enter their password before they can continue using the system. This measure is in place to prevent unauthorized access in case an operator leaves their application unattended for an extended period.

When a timeout occurs, the SSO Identity Provider Integration comes into effect and is used to authenticate the operator again before granting further access. This authentication step ensures that the operator is indeed the legitimate user and helps maintain the overall security.

How does SSO Identity Provider Integration enhance eSignature security?

When a particular transaction is configured with the highest level of security settings, the operator is required to provide their password each time the transaction is initiated. Moreover, the system allows the administrator to set up an alternative operator password for added flexibility.

During each eSignature password request, the SSO Identity Provider Integration is used for the authentication process. Prior to permitting the transaction to proceed, the system relies on the identity provider to verify the operator's credentials.

This authentication step ensures that only authorized personnel can execute critical transactions, bolstering the overall security and integrity of the eSignature process.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

How does SSO Identity Provider Integration enhance the Supply Chain Portal?

The **SYSPRO Supply Chain Portal** utilizes the **Web authentication** settings (as defined within the **Setup Options** program - *Setup Options* > *System Setup* > *Login*) and performs in the same manner as the SYSPRO Web UI (Avanti).

The only difference when logging in via the SYSPRO Supply Chain Portal, is the absence of the company sign-in page, as this doesn't apply in a portal environment.

Therefore, once you configure the **Web authentication** settings, both the SYSPRO Web UI (Avanti) and SYSPRO Supply Chain Portal will automatically utilize the SSO Identity Provider Integration capability.

How does SSO Identity Provider Integration impact command line prompts in the SYSPRO Desktop?

With the integration of the SSO Identity Provider Integration, command line prompts in the ***SYSPRO Desktop*** retain their functionality while gaining the added benefit of enhanced authentication options:

When launching the ***SYSPRO Desktop***, users can still pass command line parameters as they did before. These parameters allow users to log in to SYSPRO by selecting their user name, password, company ID, and other relevant information, and even specify a program to run with its associated parameters.

However, with the introduction of the `/OPER=` parameter, the identity provider prompt is now set to **SYSPRO Authentication**, and the operator's code and password, as well as company-specific information, are validated. This means that if an operator is required to authenticate using an SSO identity provider, the validation process will fail, and the user will be prompted to enter the required provider's credentials.

For users who do not need to be authenticated through an SSO identity provider, the existing command line prompts continue to function seamlessly. They can provide the necessary parameters as before without any changes to their workflow.

> **FOR EXAMPLE:**
>
> Let's consider the case of the ADMIN user. The following command line parameters can still be used:
>
> `/OPER=ADMIN /PASS=USERSECRET /COMP=EDU1 /CPAS=COMPANYSECRET`
>
> These parameters will work smoothly, allowing the ADMIN user to access the ***SYSPRO Desktop*** as intended.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

How does SSO Identity Provider Integration affect the Forgot Password functionality?

When SSO Identity Provider Integration is enabled, the Forgot Password process performs as follows:

SYSPRO Desktop:

1. When presented with the SYSPRO login dialog, select **SYSPRO Authentication** from the **Identity Provider** drop-down.
2. Enter your traditional user name and password.
3. Select the **Forgot Password** option.
4. A system message prompts you to confirm this request. Select **OK** to proceed.
5. From the **Forgot Password Email Confirmation** screen, enter your email address, followed by the **Send Email** function.

   The system then verifies your entry against the email address defined against your SYSPRO operator code, before sending the email.

SYSPRO Web UI (Avanti):

1. When presented with the SYSPRO Sign in dialog, enter your traditional user name and password.
2. Select the **Forgot password** option.
3. From the **Forgot password** screen, enter your email address, followed by the **Request password** function.

   The system then verifies your entry against the email address defined against your SYSPRO operator code, before sending the email.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

SYSPRO Authentication Methods

What is the difference between SSO using Active Directory and SSO Identity Provider Integration?

SSO using Active Directory:

- This method is ideal for sites using the ***SYSPRO Desktop*** user interface, as each user has to login to their Windows client environment. This option allows a site to leverage the user authenticated by Windows to login to SYSPRO.
- This option is not suitable for users using the ***SYSPRO Web UI (Avanti)*** as users can connect via any device (such as a phone or tablet) where Windows authentication is not appropriate.

SSO Identity Provider Integration:

- Each Identity provider allows various additional validation over the traditional user name and password, including the use of authenticator applications, and other forms of Multi-Factor Authentication. These providers are often already in use across the organization, so users are already comfortable using these common dialogs.
- The **SSO Identity Provider Integration** works across the ***SYSPRO Desktop*** and ***SYSPRO Web UI (Avanti)*** user interfaces, providing a consistent experience across SYSPRO interfaces and the rest of the organization.

View the following topic for more information regarding the various authentication methods available in SYSPRO 8:

SYSPRO Authentication

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Microsoft SQL Server Related

Where is SSO Identity Provider Integration data stored in SQL?

The following SQL tables within the system database contain information related to **SSO Identity Provider Integration**:

- AdmSsoProviders (`Admin SSO Identity Providers`)

  This table records the following data:

  - SSO identity providers available
  - Indicators as to whether Desktop and/or Web UI authentication applies
  - Default identity provider for each user interface

- AdmSsoAttributes (`Admin SSO Identity Provider Attributes`)

  This table records the following data:

  - Attributes associated with each identity provider (e.g. secret key)

- AdmSsoUserXref (`Admin SSO User Cross Reference`)

  This table records the following data:

  - Cross references between the SSO user ID and SYSPRO operator
  - The date and time that the definition was created for the operator (i.e. `DateAdded`)
  - The date and time of each operator's last login using the identity provider (i.e. `DateLastLogin`)

- AdmOperator (`Admin Operator`)

  This table includes the following data:

  - `OperatorSsoStatus` status flag indicating whether SSO is used (i.e. `Enforced`, `Disabled`, `Paused`)

- AdmCurrentUsers (`Users Currently Using SYSPRO`)

  This table includes the following data:

  - `AuthType` (i.e. Authentication type) - defined as **S** when using an identity provider
  - `SsoProviderName` contains the name of the identity provider
  - `SsoProviderDesc` indicates the description of the identity provider

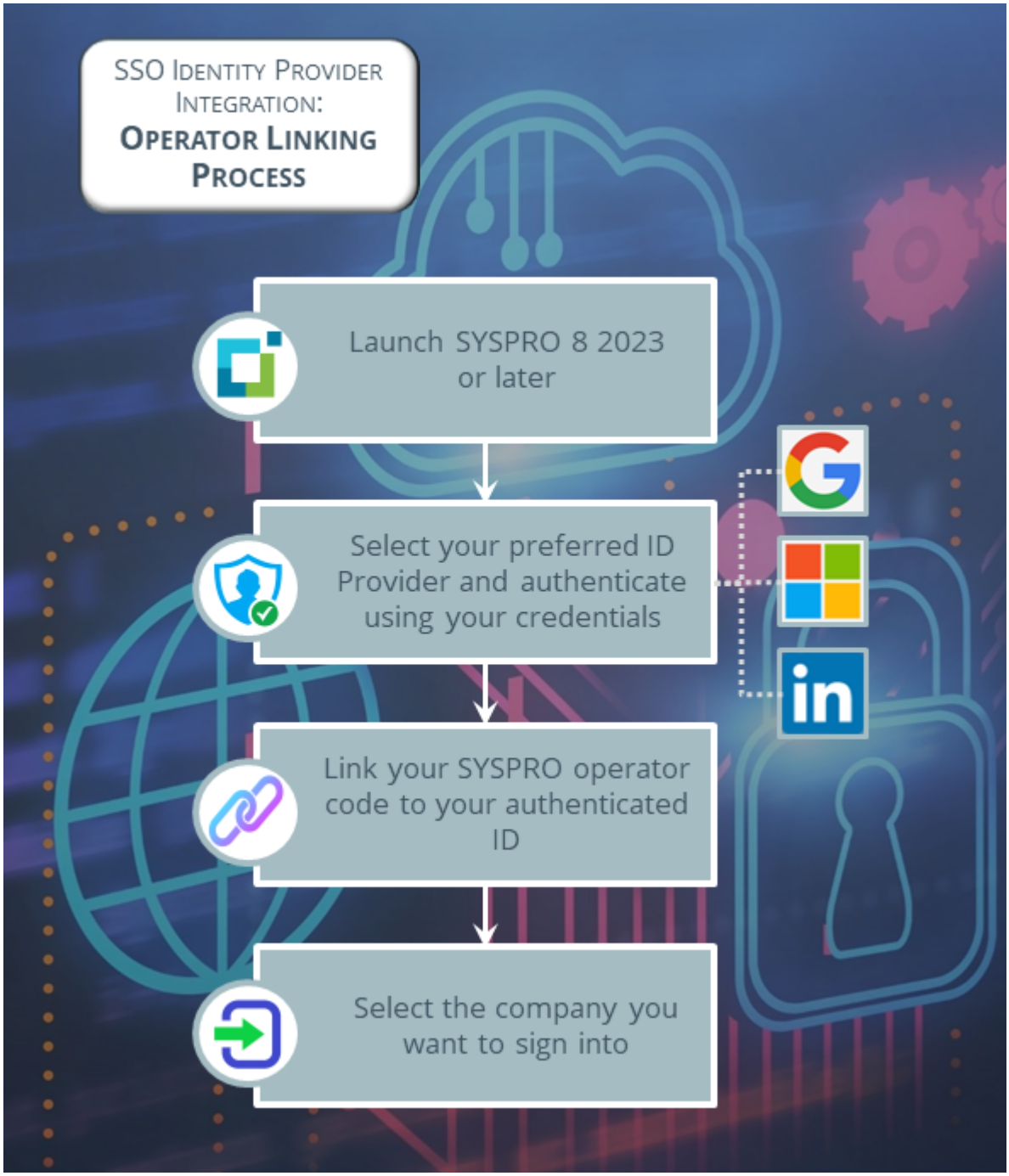
  The `AuthType` entry in this table is only stored for the duration of the user(s) being logged in.

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Using

Process

Operator Linking



Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Once the administrator has enabled the **SINGLE SIGN-ON IDENTITY PROVIDERS** capability and configured at least one identity provider, your operator login process is as follows:

1. An operator launches ***SYSPRO 8 2023*** (or later) in either the ***SYSPRO Web UI (Avanti)*** or ***SYSPRO Desktop*** user interface.

   The login dialog is displayed to the operator and presents as follows in each of the UIs:

   - SYSPRO Desktop:

     The login dialog contains an **Identity Provider** drop-down with the a list of all identity providers enabled by the system administrator, as well as a *SYSPRO authentication* entry that allows the entry of a user name and password.

     > The SYSPRO authentication option (i.e. traditional user name and password) is useful for administrators and other operators where Single sign-on identity providers has been disabled or paused.

   - SYSPRO Web UI (Avanti):

     The login dialog contains login buttons for each of the identity providers enabled by the system administrator. In addition, operators currently not enabled for Single sign-on identity providers have the ability to login using the user name and password.

   > Operators who have been configured to use Single sign-on identity providers are prevented from using the standard SYSPRO Authentication (i.e. traditional user name and password).

2. The operator selects their identity provider of choice (if more than one available and configured by the administrator) and authenticates themselves using their account credentials with that provider.

   > Depending on the provider, this may include a Multi-Factor Authentication check.
   >
   > **FOR EXAMPLE:**
   >
   > The Microsoft identity provider may ask for confirmation using the mobile-based **Authenticator** app.

3. Once authentication has succeeded, the operator is presented with the **Single Sign-On Link Dialog**, from where they can link their SYSPRO operator code to their authenticated ID:

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

a. The operator enters their correct operator code within the **User name** field.

   This could be an operator code, network user name or email address; depending on the organization's specific parameters and licensing options.

b. The operator enters the password associated with their operator code within the **Password** field.

c. The operator then selects the **Link operator** function.

Once these credentials are validated, a row is added to the AdmSsoUserXref (`Admin SSO User Cross Reference`) system-wide table and contains the following information:

- SYSPRO operator code
- SSO provider type (e.g. Microsoft)
- Unique user string returned from the identity provider

This creates a cross-reference between the SYSPRO operator code and the authenticated user string, which is then used for subsequent authentication attempts.

4. Once the operator has been linked, the **Company Sign In** page is displayed, from where the operator can select the company they want to access and enter the applicable password.
5. The operator selects the **Sign in to company** function and is then logged into SYSPRO.

Considerations

- Operators can link more than one identity provider to their SYSPRO operator code.
- When a SYSPRO operator code is linked to an SSO identity provider, the flags against the operator record are set to indicate that SSO authentication is in-force.
- In the scenario that someone can no longer login using a specific identity provider, the system administrator can login and use the **Single Sign-On Operator Configuration**[1] program to allow the SYSPRO Authentication (i.e. traditional user name and password) to be used.

  This is achieved by disabling or pausing SSO for the operator.

  An alternative option (e.g. if the Single sign-on identity providers is not set 'per operator') is for an administrator to use the **Force SSO registration at next login** option within the **Operator Maintenance** program.

  Enabling this option removes the operator's previous SSO history and forces the operator to re-authenticate their SSO Identity Provider login details the next time they login to SYSPRO.

[1] Program: IMPSSP

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Subsequent Logins

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Once an operator has linked their SYSPRO operator code with one of the identity providers and authenticated themselves successfully, their subsequent login experience is as follows:

1. An operator launches ***SYSPRO 8 2023*** (or later) in either the ***SYSPRO Web UI (Avanti)*** or ***SYSPRO Desktop*** user interface.
2. From the login dialog, the operator selects their preferred identity provider (with which they have already linked their operator code) to authenticate their access into SYSPRO.

   SYSPRO validates this authentication by checking the entries defined against the operator within the AdmSsoUserXref (`Admin SSO User Cross Reference`) table.

3. The **Company Sign In** page is displayed, from where the operator can select the company they want to access and enter the applicable password.
4. The operator selects the **Sign in to company** function and is then logged into SYSPRO.

Considerations

- If an operator is defined to use Single sign-on identity providers for their authentication (and they have logged in at least once using one of the identity providers) then all subsequent logins must use an identity provider for their authentication. Therefore, they can no longer log into SYSPRO using their traditional user name and password after linking their operator code to an identity provider.

  The only exception to this, is if their Single sign-on identity providers authentication has been paused or disabled by the administrator (using the **Single Sign-On Operator Configuration**[1] program).
- If an operator cancels out from the authentication dialog, they are returned to the main login screen.
- If an operator defined to use Single sign-on identity providers attempts to use an alternative user interface where no identity providers have been enabled, then they will not be able to login to that user interface.

[1] Program: IMPSSP

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Affected programs

The following indicates areas in the product that may be affected by implementing this feature:

Setup programs

Setup Options

Setup Options > *System Setup* > *Login*

The **Login System Setup** form includes a **SINGLE SIGN-ON IDENTITY PROVIDERS** section that lets you configure the following setup options:

- Single sign-on identity providers
- User applicability

In addition to the above options:

- The **Define specific operators** hyperlink allows you to indicate the operators to which this Identity Provider authentication applies (using the **Single Sign-On Operator Configuration**[1] program).
- The **Configure identity providers** hyperlink lets you configure your selected identity provider(s) (using the **Single Sign-On Provider Configuration**[2] program).

Single Sign-On Provider Configuration

Program List > *Administration* > *Security* > *Authentication*

This program lets administrators configure the following Identity Providers available for use within SYSPRO:

- Google
- Microsoft
- LinkedIn

Single Sign-On Operator Configuration

Program List > *Administration* > *Security* > *Authentication*

This program lets administrators configure Identity Provider authentication per operator.

[1]Program: IMPSSP
[2]Program: IMPSSI

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

Affected business objects

The following indicates the business objects that are affected by this feature:

Setup objects

COM Setup Operator Delete

The **COM Setup Operator Delete** business object is used to remove the applicable entries from the AdmSsoUserXref (i.e. `Admin SSO User Cross Reference`) table when you delete an operator.

Transaction objects

Post System Setup Options

The **POST SYSTEM SETUP OPTIONS**[1] business object is used to record your configuration of the **SINGLE SIGN-ON IDENTITY PROVIDERS** options.

COM Operator Copy Transaction

The **COM Operator Copy Transaction** business object is used to copy the SSO status flag when you copy an operator record.

Query objects

Query System Setup Options

The **QUERY SYSTEM SETUP OPTIONS**[2] business object is used to query your configuration of the **SINGLE SIGN-ON IDENTITY PROVIDERS** options.

[1]Business object: COMTSY
[2]Business object: COMQSY

Copyright © 2023 Syspro Ltd. All rights reserved. All trademarks are recognized

SYSPRO™

www.syspro.com

Copyright © SYSPRO. All rights reserved.
All brand and product names are trademarks or
registered trademarks of their respective holders.