Single Sign-on

SYSPRO 8

Reference Guide

Published: October 2021

SYSPRO

CONTENTS

Single Sign-on

Exploring 1
Starting 3
Solving 7
Using 13

Single Sign-on

Exploring

Where it fits in?

Single Sign-on in SYSPRO provides a simple to setup and robust method of using **Microsoft Active Directory (AD)** to control SYSPRO users.

Once configured, it enables a complete single sign-on experience as SYSPRO users are authenticated by **Windows** and then simply use a shortcut to run SYSPRO without being prompted for a user name and password at the login screen.

It means that a SYSPRO site can use **Microsoft Active Directory (AD)** to add, change, disable and delete operators virtually seamlessly. Any changes to user attributes automatically reflect against the SYSPRO operator without manual intervention.

Navigation

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

- *Program List > Administration > Security*

Terminology

Microsoft Active Directory (AD)

Microsoft Active Directory (AD) is a directory service developed by **Microsoft** for **Windows** domain networks and comprises several services that run on **Windows Server** to manage permissions and access to networked resources.

Organizational unit

An organizational unit (OU) is a subdivision within **Microsoft Active Directory (AD)** into which you can place the following objects:

- Users
- Groups (e.g. Security groups)
- Computers
- Other organizational units

You can create organizational units to mirror your organization's functional or business structure, and each domain can implement its own organizational unit hierarchy.

Security group

Security groups provide an efficient way to assign access to resources on your network:

- Assign user rights to security groups in **Microsoft Active Directory (AD)**.
- Assign permissions to security groups for resources.

Starting

Prerequisites

The following setup options must be configured to use this feature:

Setup Options

Setup Options > *System Setup* > *Login*

- Single sign-on:
  - Active Directory sync required
  - AD sync service endpoint
  - Review email required
  - Failure email required
  - Success email required

Setup Options > *System Setup* > *Connectivity*

- Email/SMTP settings:
  - SMTP server IP address
  - Outgoing email address
  - Username
  - Password
  - Server port
  - Use SSL

Restrictions and Limits

- SYSPRO operators cannot be enabled for simultaneous use of **Multi-Factor Authentication** and:
  - Single Sign-on (i.e. the operator is defined as an Active Directory user)
  - Concurrent usage (i.e. the **Allow concurrent use of this operator** option is enabled against the operator in the **Operator Maintenance** program)
- Currently, **Single Sign-on** is not supported with the following platforms:
  - SYSPRO Espresso
  - SYSPRO Supply Chain Portal
  - SYSPRO Avanti (when using local Active Directory)

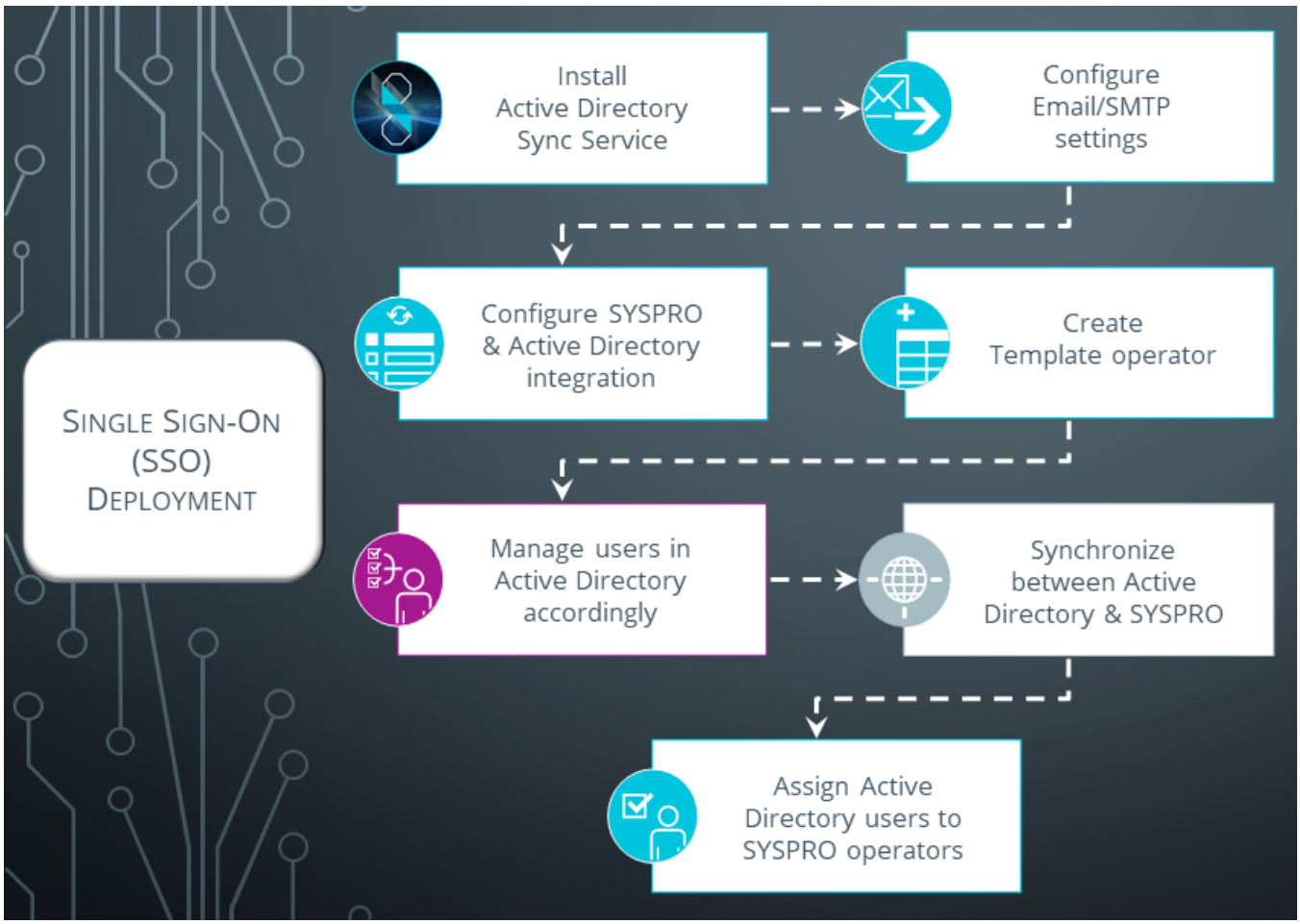
SYSPRO Avanti supports **Single Sign-on** capabilities if you use **Microsoft Azure Active Directory B2C**.

Security

You can secure this feature by implementing a range of controls against the affected programs. Although not all these controls are applicable to each feature, they include the following:

- You restrict operator access to *activities* within a program using the **Operator Maintenance** program.
- You can restrict operator access to the *fields* within a program (configured using the **Operator Maintenance** program).
- You can restrict operator access to *functions* within a program using passwords (configured using the **Password Definition** program). When defined, the password must be entered before you can access the function.
- You can restrict access to the eSignature *transactions* within a program at operator, group, role or company level (configured using the **eSignature Setup** program). Electronic Signatures provide security access, transaction logging and event triggering that gives you greater control over your system changes.
- You can restrict operator access to *programs* by assigning them to groups and applying access control against the group (configured using the **Operator Groups** program).
- You can restrict operator access to *programs* by assigning them to roles and applying access control against the role (configured using the **Role Management** program).

Deploying



How to enable Single Sign-on

1. Install the **SYSPRO 8 Active Directory Sync Service** using the **SYSPRO Installer** application.

   This requires you to define an endpoint for the **SYSPRO 8 e.net Communications Load Balancer**, which is used to communicate with your SYSPRO instance.

2. From the **Setup Options** program:
   - Ensure that your SMTP configuration is defined within the **EMAIL/SMTP SETTINGS** section (*Setup Options* > *System Setup* > *Connectivity*).
   - Enable and configure the integration between SYSPRO and **Microsoft Active Directory (AD)** within the **SINGLE SIGN-ON** section (*Setup Options* > *System Setup* > *Login*).

You must define the **AD SYNC SERVICE ENDPOINT** which indicates the location of the **SYSPRO 8 Active Directory Sync Service**. This is the same endpoint that was configured when the service was installed. Use the **Test Connection** function once you have entered the endpoint to ensure the entry is correct.

3. From the **Operator Maintenance** program (*SYSPRO Ribbon bar* > *Setup* > *Operators*) define an operator template.

   This is required when using the **Add operator** option in the **Active Directory User Management** program as a template operator is used when creating a new operator for assignment to an Active Directory user.

4. In **Microsoft Active Directory (AD)** add the appropriate users to the `SYSPRO.ERP` security group.

   Once the **SYSPRO 8 Active Directory Sync Service** is running, any Active Directory users that are added to the `SYSPRO.ERP` security group are added to the AdmSsoUsers table.

   Either wait for the **SYSPRO 8 Active Directory Sync Service** to run (this defaults to running every 12 hours) or select the **Sync Now** option in the **Active Directory User Management** program to force an immediate synchronization with **Microsoft Active Directory (AD)** to update the operator list.

   An email notification will be sent indicating that there are one or more Active Directory users that can be reviewed and linked to an existing or new SYSPRO operator.

5. From the **Active Directory User Management** program (*Program List* > *Administration* > *Security*) assign SYSPRO operators to Active Directory users accordingly.

   New `{Unassigned}` Active Directory users can be managed as follows:

   - Link to an existing SYSPRO operator.

     An informational icon clearly indicates when an existing user has a network user name matching the Active Directory network user name.

   - Add a new SYSPRO operator.

     You select a template, define the new operator code, location and default company and the operator is then added and linked to the Active Directory user.

   - Mark as 'hidden'.

     Optionally hide one or more Active Directory users from the list of items for later review.

     You can use the filter options to see the hidden Active Directory users.

Solving

FAQs

Active Directory management

Can I rename the security group in Microsoft Active Directory (AD)?

You can rename the `SYSPRO.ERP` security group in **Microsoft Active Directory (AD)** by adding a suffix to the group name.

> **FOR EXAMPLE:**
>
> `SYSPRO.ERP.ACCOUNTS`

When you install the **SYSPRO 8 Active Directory Sync Service** (using the **SYSPRO Installer** app) ensure that you enter this suffix at the **Security Group Suffix** parameter field.

If required, you can update the suffix after installing the **SYSPRO 8 Active Directory Sync Service**:

1. Create a `custom.config` file:

   To create a `custom.config` file, make a copy of the `SYSPRO.AD.Sync.Service.exe.config` file and rename it to `custom.config`.

   The `custom.config` file can then contain the entry you want to modify and the startup node. Any entries not contained in the `custom.config` file are retrieved from the original `SYSPRO.AD.Sync.Service.exe.config` file.

   You should ideally stop the service while you do this, otherwise the configurations will be picked up at the next poll interval.

2. Update the `ADSecurityGroup` key's value with the new security group name.

What attributes are updated in Microsoft Active Directory (AD)?

None. The synchronization between SYSPRO and **Microsoft Active Directory (AD)** is a one-way service.

SYSPRO operators defined as **AD Managed** are managed by **Microsoft Active Directory (AD)** and updated accordingly in SYSPRO automatically when the **SYSPRO 8 Active Directory Sync Service** runs.

The following operator attributes are managed by **Microsoft Active Directory (AD)** and cannot be maintained in SYSPRO for Active Directory operators:

- Operator name
- Operator email address
- Network user name
- Operator status (i.e. `ACTIVE`, `DISABLED` or `REMOVED`)

What happens if a user is removed from the SYSPRO.ERP security group in Microsoft Active Directory (AD)?

A user who is removed from the `SYSPRO.ERP` security group in **Microsoft Active Directory (AD)** is automatically disabled within SYSPRO when the **SYSPRO 8 Active Directory Sync Service** synchronizes with **Microsoft Active Directory (AD)**.

Synchronization

What permissions are required for the service user?

The **SYSPRO 8 Active Directory Sync Service** must be run as a named user that has `READ` permission to access **Microsoft Active Directory (AD)**.

What variables are passed to the email templates when synchronization occurs?

If you have configured receiving emails in the **System Setup** program (**Review email required**, **Failure email required**, **Success email required**) the following variables are passed to the email templates when the Microsoft Active Directory (AD) synchronization takes place:

- `$SsoUserCount$`

  Count of users added for review.
- `$SsoOpChanged$`

  Count of operators with changes (e.g. email, name).
- `$SsoOpActivated$`

  Count of operators whose status has changed to active from disabled or removed.
- `$SsoOpDisabled$`

  Count of operators whose status has changed to disabled.
- `$SsoOpRemoved$`

  Count of operators whose status has changed to removed.
- `$FailedMsg$`

  If the synchronization fails, then this contains the message as written to the log file.

What is the default synchronization schedule?

The `PollInterval` is set to default every `12 hours`, but can be changed if required.

The minimum setting is `0.30` minutes.

SYSPRO operators

How do I create a Template operator?

An operator **Template** is required when adding a new SYSPRO operator for an Active Directory user in the **Active Directory User Management** program.

1. Open the **Operator Maintenance** program.

   Reset your toolbar to ensure all the latest options are visible.

2. From the **Edit** menu, select **Maintain templates**.
3. Enter the template code in the **Template** field on the toolbar and press `TAB`.
4. Enter details for the following mandatory fields on the **Operator Details** pane:
   - Operator name (this becomes the template description)
   - Operator group
5. Configure any security groups, roles and other attributes that you require against the template.
6. Enter any remaining information that you require as defaults for the operator template, or accept the defaults provided.
7. Save the operator template.

   Template operator codes are prefixed with `__Template_` and their operator type records as **Template**.

What functions are available after Active Directory users are assigned to SYSPRO operators?

The following functions become available in the **Active Directory User Management** program after linking an Active Directory user to a SYSPRO operator:

- **Delink operator** (delinks the operator from the Active Directory user but retains the SYSPRO operator code)
- **Delete operator** (completely removes the SYSPRO operator)

What if an operator is delinked in SYSPRO, but remains part of the security group in Microsoft Active Directory (AD)?

An operator who is delinked in the **Active Directory User Management** program remains visible in the program as they are still part of the AdmSsoUsers table.

If you don't want to see delinked operators in the **Active Directory User Management** program, highlight the operator and select the **Hide Users** option from the toolbar menu.

Platform related

How does Single Sign-on work in SYSPRO Avanti?

From ***SYSPRO 8 2021 R1***, ***SYSPRO Avanti*** supports **Single Sign-on** capabilities when using **Microsoft Azure Active Directory B2C**.

Administrators can use **Microsoft Active Directory (AD)** to add, change, disable and delete operators virtually seamlessly and any changes to user attributes automatically reflect against the operator without manual intervention.

Once configured, it enables a complete single sign-on experience as operators are authenticated by **Windows** via the **Microsoft Azure Active Directory B2C** login page configured for their organization. Operators can then use their email address to log into ***SYSPRO Avanti*** and engage as normal.

Upon logging out, operators are signed-out of **Microsoft Azure Active Directory B2C** and redirected back to the **Microsoft Azure** portal.

The **Single Sign-on** session lifetime settings are configured and maintained within the **Microsoft Azure** platform.

How do I enable Single Sign-on for SYSPRO Avanti?

The following prerequisites are required to use the SSO capabilities in ***SYSPRO Avanti***:

- A registered certificate for the ***SYSPRO Avanti*** server is required to run **Single Sign-on**.
- A customer account must be registered with **Microsoft Azure Active Directory B2C** and configured with the correct redirect URL back to the specific ***SYSPRO Avanti*** instance.
- The relevant tags within the `Web.config` file of the **SYSPRO Avanti Web Service** service must be updated accordingly.
- As AD users are mapped to SYSPRO operators, each operator's configured email address must match their registered email address within the **Microsoft Azure Active Directory B2C** portal.

The **SYSPRO Cloud Services** team are responsible for enabling **Single Sign-on** for customers in a ***SYSPRO Cloud ERP*** environment.

To enable **Single Sign-on** in ***SYSPRO Avanti*** (when using **Microsoft Azure Active Directory B2C**) you need to edit the `Web.config` file of the **SYSPRO Avanti Web Service**.

This `Web.config` file is located in the root folder where ***SYSPRO Avanti*** is installed for **Internet Information Services (IIS)** (e.g. `\inetpub\wwwroot\SYSPROAvanti`).

The following tags must be added within the `<Configuration><AppSettings>` section and defined with your specific details:

- `<add key="ida:IsB2Cauth" value="true" />`

  This is used to determine if SSO must be used for ***SYSPRO Avanti***. Therefore, SSO is only enabled within ***SYSPRO Avanti*** if this flag is present and defined as "true".

- `<add key="ida:Tenant" value="yourcloud.onmicrosoft.com" />`

  This indicates the Azure tenant address, as recorded within your **Microsoft Azure** configuration.

- `<add key="ida:TenantId" value="YourUniqueTenantId" />`

  This indicates your Azure tenant ID, as recorded within your **Microsoft Azure** configuration.

- `<add key="ida:ClientId" value=" YourUniqueClientId " />`

  This indicates your Azure client ID, as recorded within your **Microsoft Azure** configuration.

- `<add key="ida:ClientSecret" value="YourClientSecret" />`

  This indicates your Azure secret used by the client (i.e. avanti web app) as recorded within your **Microsoft Azure** configuration.

- `<add key="ida:AadInstance" value="https://Yourcloud.b2clogin.com/tfp/{0}/{1}" />`

  This is used to determine the Active Directory Instance.

- `<add key="ida:RedirectUri" value="https://YourCompany.com/SYSPROAVANTI_companyID/" />`

  This indicates the redirect URI (i.e. Avanti uri) after successful authentication on the Azure portal.

- `<add key="ida:SignUpSignInPolicyId" value="b2c_1_susi" />`

  This indicates your sign in policy as configured within **Microsoft Azure**.

To ensure the setup works correctly, ensure that none of these tags are duplicated within the `Web.config` file.

How do I enable Single Sign-on for SYSPRO Point of Sale?

From ***SYSPRO 8 2021 R2***, **Single Sign-on** capabilities are available with ***SYSPRO Point of Sale*** when running in ***SYSPRO Avanti***.

The following requirements must be met to use the SSO capabilities:

- A registered certificate for the ***SYSPRO Point of Sale*** server is required to run **Single Sign-on**.
- A customer account must be registered with **Azure B2C** and configured with the correct redirect URL back to the specific ***SYSPRO Point of Sale*** instance.
- ***SYSPRO Point of Sale*** users must be configured with an email address for the system to identify the correct operator.

To enable **Single Sign-on** functionality in ***SYSPRO Point of Sale*** (when running in ***SYSPRO Avanti***) add the following tags within the `Web.config` file located in the `\inetpub\wwwroot\SYSPRO8POS_xxxx\SYSPROPOSAVANTI` folder (where `xxxx` is your company code):

- `<add key="ida:IsB2Cauth" value="true" />`
- `<add key="ida:Tenant" value="yourcloud.onmicrosoft.com" />`
- `<add key="ida:TenantId" value="yourUniqueTenantId" />`
- `<add key="ida:ClientId" value=" yourUniqueClientId " />`
- `<add key="ida:ClientSecret" value="YourClientSecret" />`
- `<add key="ida:AadInstance" value="https://yourcloud.b2clogin.com/tfp/{0}/{1}" />`
- `<add key="ida:RedirectUri" value="https://yourCompany.com/SYSPRO8POSAVANTI_EDU1/" />`
- `<add key="ida:SignUpSignInPolicyId" value="b2c_1_susi" />`
- `<add key="ida:EditProfilePolicyId" value="b2c_1_edit_profile" />`
- `<add key="ida:ResetPasswordPolicyId" value="b2c_1_reset" />`

General

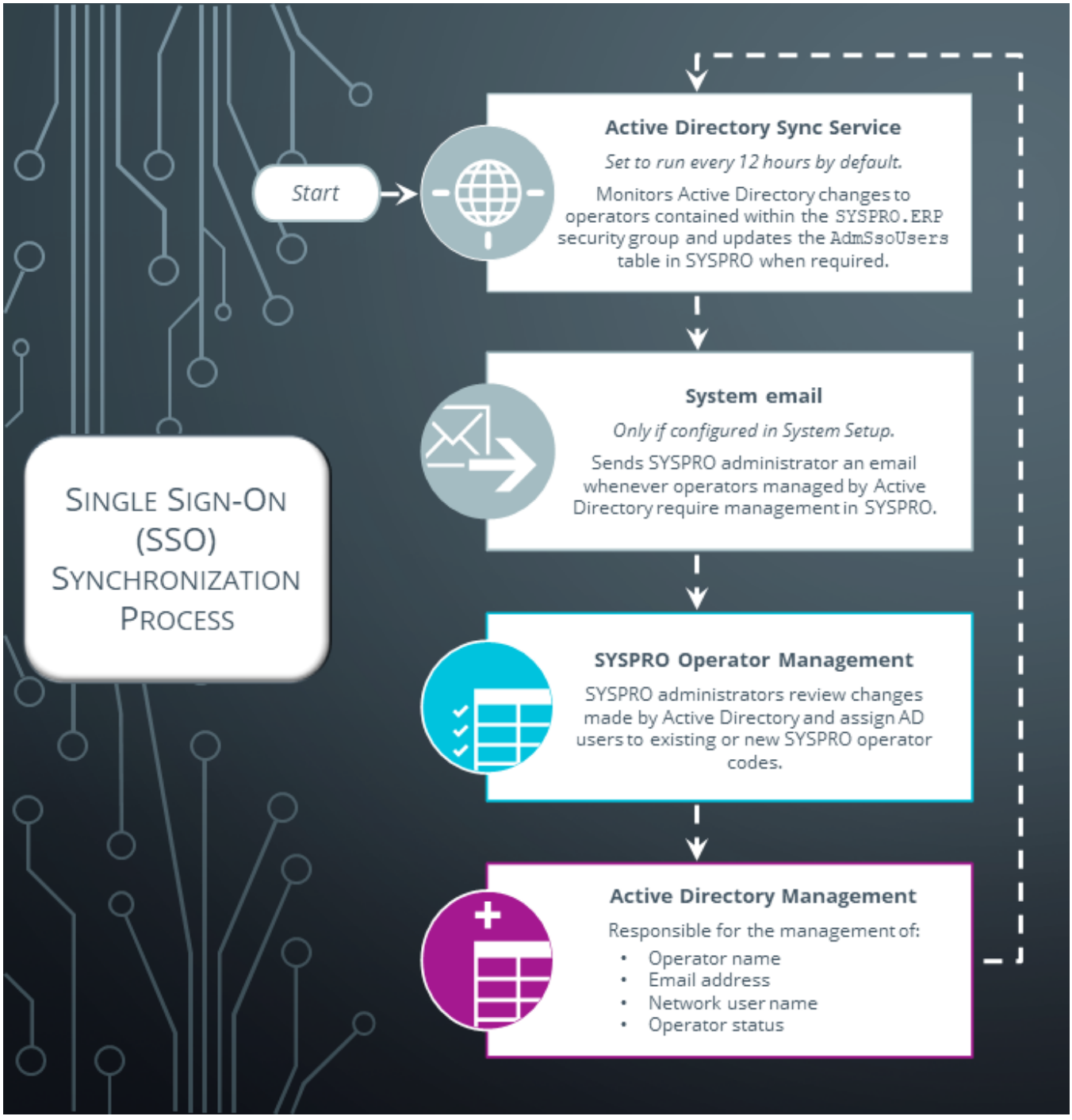
Why are SMTP details required to use Single Sign-on?

SMTP details are required if you have configured any of the following email options from the **Connectivity System Setup** form of the **Setup Options** program (*Setup Options* > *System Setup* > *Connectivity*):

- Review email required
- Failure email required
- Success email required

Using

Process



The synchronization process occurs once you have enabled **Single Sign-on** and added the relevant users to the `SYSPRO.ERP` security group in **Microsoft Active Directory (AD)**.

When an Active Directory user belongs to the SYSPRO.ERP security group, they are assumed to be personnel in the organization who have access to the SYSPRO ERP application and are therefore SYSPRO operators. This is important because Active Directory users on many sites include personnel who use additional applications and don't necessarily require access to SYSPRO.

1. The **SYSPRO 8 Active Directory Sync Service** interrogates **Microsoft Active Directory (AD)** to read all users contained within the SYSPRO.ERP security group, either by direct membership or via a nested group.

   This lets you take advantage of an existing Active Directory security grouping (if it exists) without having to duplicate existing groups.

   The service provides an audit trail of all updates that occur and stores this information in the AdmSsoUserSyncLog table of your system-wide database.

   The service updates the SYSPRO AdmSsoUsers table, which updates the users linked to SYSPRO operators shown in the **Active Directory User Management** program.

2. The **Active Directory User Management** program lets you to assign Active Directory users to existing SYSPRO operator codes, or to create new SYSPRO operator codes to which you want to assign Active Directory users.

3. The **SYSPRO 8 Active Directory Sync Service** detects any change against the attributes of operators in the SYSPRO.ERP security group of **Microsoft Active Directory (AD)** during its next synchronization schedule and updates (the AdmSsoUsers table and the relevant operators' details).

   Operator attributes include:

   - Operator name
   - Operator email address
   - Network user name
   - Operator status (i.e. ACTIVE, DISABLED or REMOVED)

4. You are notified via email (if this is configured) that changes requiring your attention have been made in **Microsoft Active Directory (AD)**.

   > **FOR EXAMPLE:**
   >
   > New users are added to the security group in **Microsoft Active Directory (AD)** which require SYSPRO operator assignment.

   This prompts you to run the **Active Directory User Management** program to review the changes and manage accordingly.

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 within the **Setup Options** program includes the following options that let you enable integration between SYSPRO and **Microsoft Active Directory (AD)**:

- Active Directory sync required
- AD sync service endpoint
- Review email required
- Failure email required
- Success email required

Active Directory User Management

Program List > *Administration* > *Security*

This program lets administrators configure and manage the relationship between **Microsoft Active Directory (AD)** users and SYSPRO operators.

The program accesses the AdmSsoUsers table and allows you to:

- View all users added to the `SYSPRO.ERP` security group in **Microsoft Active Directory (AD)**.
- Assign Active Directory users to existing SYSPRO operator codes.
- Create a new SYSPRO operator code to assign to an Active Directory user.
- Force a sync between **Microsoft Active Directory (AD)** and SYSPRO to update the operator list.
- Delink a SYSPRO operator from an Active Directory user.
- Delete a SYSPRO operator that was linked to an Active Directory user.
- Filter, hide or unhide the operators that you want to view.

If a user is removed from the `SYSPRO.ERP` security group in **Microsoft Active Directory (AD)**, they are automatically disabled within SYSPRO when the **SYSPRO 8 Active Directory Sync Service** synchronizes with **Microsoft Active Directory (AD)**.

Operator Maintenance

SYSPRO Ribbon bar > Setup > Operators

The following operator fields related to this feature are available from the **Operator Details** pane:

- **Operator type**

  The operator type *AD Managed* indicates that the operator is managed by **Microsoft Active Directory (AD)** (via the **SYSPRO 8 Active Directory Sync Service**).

- Authentication type

  The authentication type *Windows (W)* indicates that Single Sign-on is enabled for the operator and that **Windows** authentication is used when logging into SYSPRO.

- Operator status

  This indicates the current status of the operator (as recorded in the `OperatorStatus` column of the AdmOperator table:

  - `ACTIVE` indicates that the operator is active in SYSPRO and **Microsoft Active Directory (AD)** and can log into SYSPRO.
  - `DISABLED` indicates that the operator was disabled from **Microsoft Active Directory (AD)** and is therefore not able to log into SYSPRO.
  - `REMOVED` indicates that the operator was removed via **Microsoft Active Directory (AD)** and is therefore not able to log into SYSPRO.

- Status change reason

  This indicates the reason for the operator status not being **Active**.

- Date status changed

  This indicates the date when the operator status was last changed.

Query programs

System Audit Query

Program List > Administration > Security

This program includes auditing and logging capabilities for all operators that are linked to and managed by **Microsoft Active Directory (AD)**, providing an audit trail of all updates that occur, including:

- Operators activated via **Microsoft Active Directory (AD)**
- Operators disabled via **Microsoft Active Directory (AD)**
- Operators removed via **Microsoft Active Directory (AD)**
- Operators details changed via **Microsoft Active Directory (AD)**

Services

SYSPRO 8 Active Directory Sync Service

Program List > Administration > Security

The **SYSPRO 8 Active Directory Sync Service** is used to integrate **Microsoft Active Directory (AD)** to read all users contained within the `SYSPRO.ERP` security group.

The service updates the AdmSsoUsers table, which updates the operators listed in the **Active Directory User Management** program.

This service is installed using the **SYSPRO Installer Application**.

The **SYSPRO 8 Active Directory Sync Service** must be run as a named user that has `READ` permission to access **Microsoft Active Directory (AD)**.

SYSPRO™

www.syspro.com