

# Best practices for Security and Configuration

Version 1 – Sept 2025





# Contents

<b>Contents</b>	<b>2</b>
<b>Introduction</b>	<b>3</b>
<b>SYSPRO Best Practices Setup</b>	<b>3</b>
Principle of Least privilege	3
Segregation of Duties (SoD) principle	6



# Introduction

In today's digital landscape, ensuring the security and integrity of systems and data is paramount. This document outlines the best practices for security and configuration within the SYSPRO environment. The aim is to identify and mitigate potential vulnerabilities, ensuring that the system is robust against unauthorized access and other security threats. By adhering to the principles and guidelines detailed in this document, organizations can enhance their security posture and protect sensitive information from potential breaches.

## SYSPRO Best Practices Setup

### Principle of Least privilege

Apply the principle of least privilege to the application's file system permissions to ensure users can only access authorized files and directories. Operators should only have permissions enabled for the tasks required.

#### Unrestricted File Modification

It is advised to remove or heavily restrict direct file editing capabilities unless absolutely required.

**Suggested Remediation:** Limit operator activities that aren't essential for operations. Enable access as required.

#### Path Traversal

SYSPRO offers the availability of embedding a browser control in the product. This allows an operator to browse the file system for specific files within the product.

**Suggested Remediation:** We recommend removing access to the browser control for every operator. SYSPRO will consider deprecating this outdated feature in the future.

The unrestricted file modification and path traversal can be remediated with the following configuration options in SYSPRO:

1. Run the **Operator Browse** program.
2. Select an operator and click on **Change** in the toolbar as seen below

Report Preview

Operators

File Edit Options Include

Select

Change (Ctrl+Q)

Operator	Name	Last login	Location	Email	Primary r...	Primary ...	Status	Last SSO ...	Date last ...
MERLE	Merle Franks	Never	Ground Fl...	merlef@O...	Marketing...	MARK	Active		None
MICH	Michelle Lewis	Never	Ground Fl...	michelle...	Order Entr...	SALES	Active		None
MIKE	Michael Young	Never	Second LF...	mikey@O...	Payables ...	FINANC	Active		None
MIRA	Miranda Fenwick	Never	Third Floo...	mirandaf...	Shipping ...	OPS	Active		None
OLGA	Olga Dietermeyer	Never	RM Ware...	olgad@O...	Inventory ...	OPS	Active		None
OZZIE	Oswald McKenna	Never	FG Wareh...	ozziem@...	Maintena...	OPS	Active		None
PARK	Park Jeong	Never	Second Fl...	parkj@Ou...	Receivabl...	FINANC	Active		None
PAT	Pat Webb	More tha...		patw@OU...		ADMIN	Active		None
PENNY	Penny Green	Never	Third Floo...	pennygre...	Assets Bu...	PURCH	Active		None
PETER	Peter Smith	Never	Third Floo...	peters@O...	Purchasin...	PURCH	Active		None
PHIL	Phillip Dandrich	Never	Ground Fl...	phild@Ou...	Chief Exec...	BOARD	Active		None
PIERRE	Pierre Dalen	Never	Second Fl...	pierred@...	Chief Fina...	FINANC	Active		None
ROD	Rod Martin	Never	Second Fl...	rodm@O...	Treasury ...	FINANC	Active		None
ROGER	Roger Nadel	Never	Third Floo...	rogerm@...	Assets Ma...	PURCH	Active		None
RUSS	Russell Howard	Never	First Floor...	russellho...	Research ...	OPS	Active		None
SALLY	Sally Green	Never	FG Wareh...	sallygreen...	Quality In...	OPS	Active		None
SAM	Sam Worx	More tha...		sam@the...	Viewing	VIEW	Active		None
SANDY	Sandra Holford	Never	Second Fl...	sandrah@...	Controller	FINANC	Active		None
SEAN	Sean Harris	Never	Third Floo...	seanharris...	Consuma...	PURCH	Active		None
SPENC	Spencer Jude	Never	Ground Fl...	specejr@...	Marketing...	MARK	Active		None
SVEN	Sven Almgren	Never	Second Fl...	svena@O...	Payables ...	FINANC	Active		None
syspro_basic	syspro_basic	Last 7 days				BASIC	Active		None
syspro_standard	syspro_standard	Last 7 days				ALL	Active		None
T1	Training 1 Administrator	Never	Training R...	TRAIN1@...		ADMIN	Active		None
T10	Training 10 Administrator	Never	Training R...	TRAIN10...		ADMIN	Active		None
T11	Training 11 Administrator	Never	Training R...	TRAIN11...		ADMIN	Active		None
T12	Training 12 Administrator	Never	Training R...	TRAIN12...		ADMIN	Active		None

Administration

3. Select the **Security** tab on the right pane for the operator as seen below.

Operator Maintenance

File Edit Contact Password

New X Operator: syspro\_stand Notepad Printers... Contact...

Operator Details

Security

Personal

Operator syspro\_standard

Operator name syspro\_standard

Network user name syspro\_standard

Operator group ALL

Subgroup Define list...

Location

Email

Information

SQL Server authentication

SQL login

Use system-wide SQL user details

Use operator specific SQL user details

Use generated SQL user details

Login name syspro\_standard

Roles

Access Roles

Add Roles Organogram

Role Primary role

Account Manager

Assets Buyer

Assets Manager

Assistant Controller

Bookkeeper

Building Maintenance Engineer

Chief Executive Officer

Chief Financial Officer (CFO)

Chief Technical Officer

Status - Changing operator: syspro\_standard

Defaults Options Timeout Security E.net

Activities

Selection List

Configure activities Edit

Fields

Selection All

Configure fields Edit

Menus

Enable standard SYSPRO menus

Password

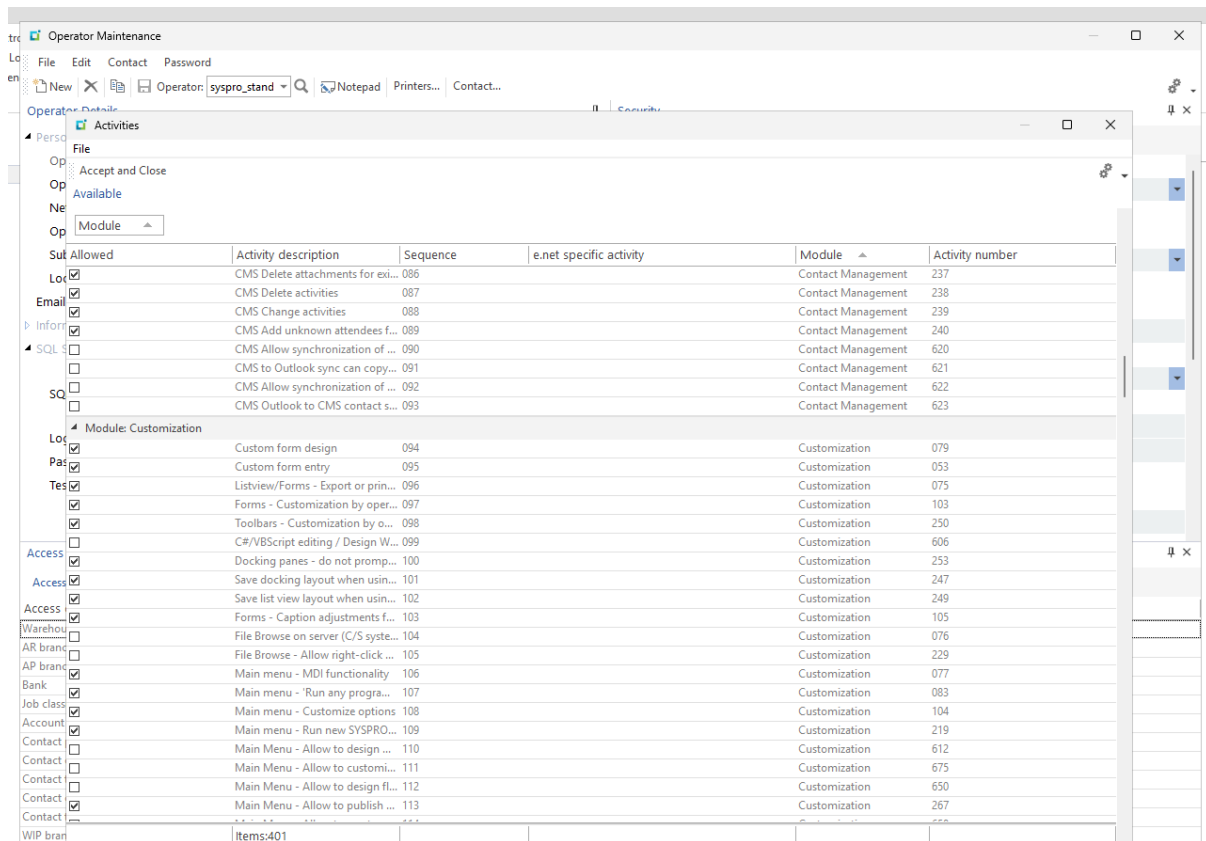
Number of login attempts Lockout after 5 failed login attempts

Failed login attempts 0

Operator locked out

4. Select **List** at the **Selection** field within the Activities section.
5. Click on the **Edit** hyperlink to configure activities.

The following modal window is displayed:



6. Disallow the following high impact activities by unchecking the specific rows:
  - Activity 229: File Browse – Allow right-click over files
  - Activity 631: Allowed to upload files to the server
  - Activity 694: Allow copy files to server
  - Activity 695: Allowed to clone company
  - Activity 304: System Setup
  - Activity 076: File Browse on server
  - Activity 176: SYSPRO Browser – Manual URL address entry
7. Click on **Accept and Close** in the toolbar button to save these operator configuration options.

# Segregation of Duties (SoD) principle

A security infrastructure admin separation model is a strategy based on the Segregation of Duties (SoD) principle, which divides administrative tasks among different roles and accounts to prevent single individuals from having total control over sensitive systems or data. This model creates multiple admin accounts (privileged and unprivileged), limits their use for specific tasks (e.g., using a non-admin account for daily work and a privileged account only for administrative actions), and uses separate systems or jump boxes for management, thereby reducing the risk of fraud, errors, and unauthorized access. This principle should be applied when setting up an operator hierarchy. This will mitigate the vulnerability of the following issues.

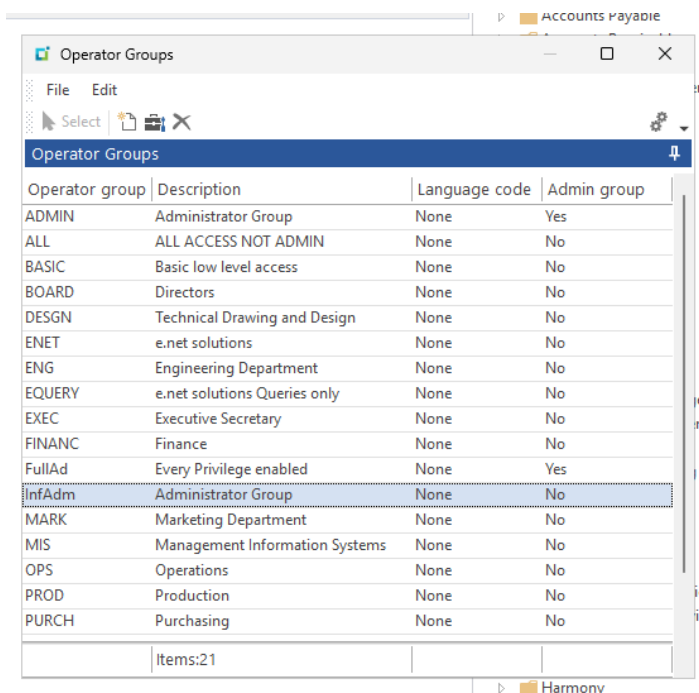
## Preventing Credential Exposure and Broken Access Control

It is advised to separate infrastructure settings from product usage settings by defining access to these options for role specific administrators.

**Suggested Remediation:** When implementing SYSPRO, the operator access levels should be setup in a manner that does not allow a single point of failure to take hostage of the entire system. Some potential configuration options to consider:

- Set up firewalls in Azure. Only allow inbound/outbound communication to allowed machines/servers using well defined rules in Azure Network Interfaces.
- Create well defined Operator Groups with specific permissions enabled and applying the Segregation of Duties (SoD) principle. This can be done as follows:

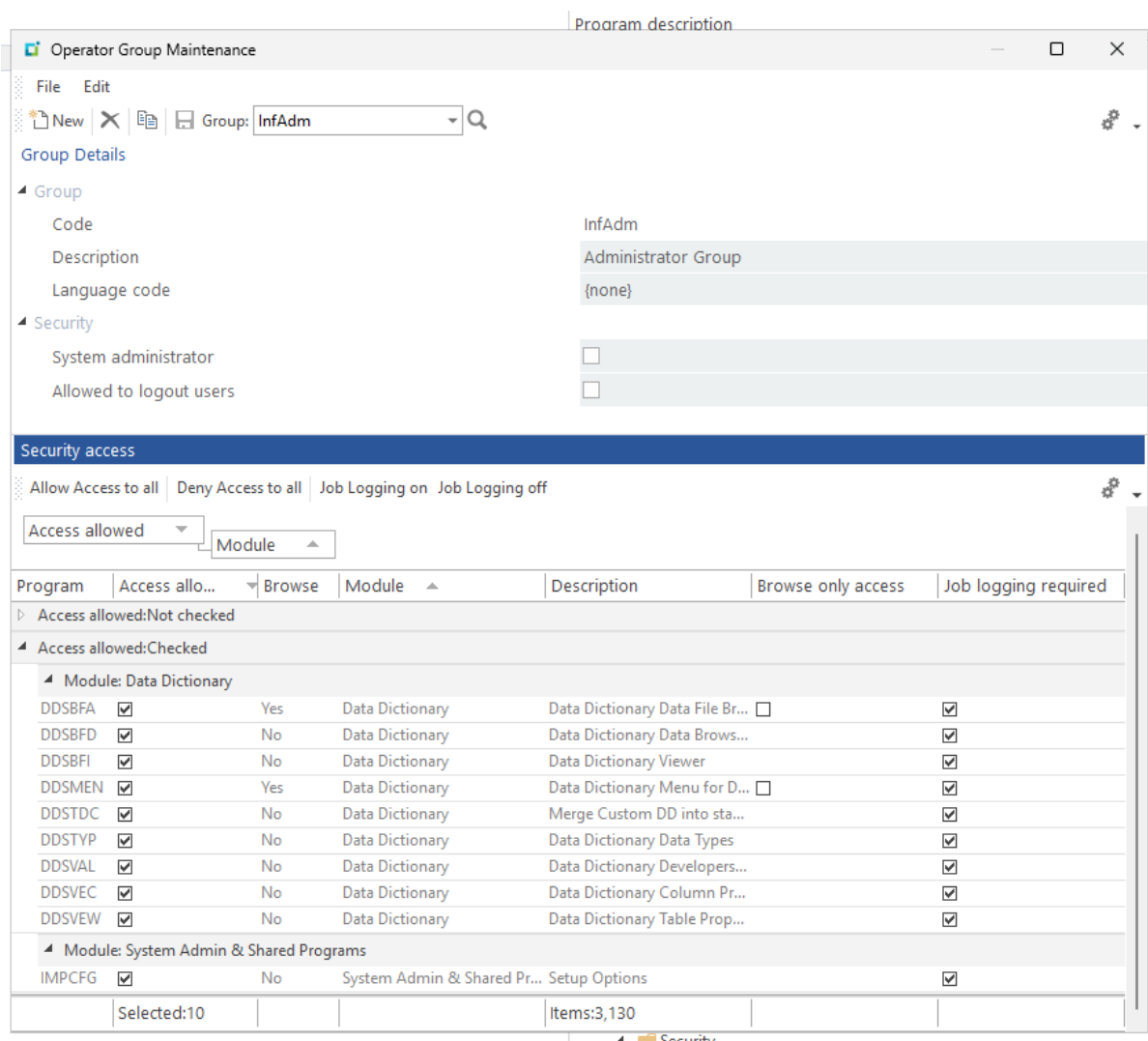
1. Run the **Operator Browse** program.



Operator group	Description	Language code	Admin group
ADMIN	Administrator Group	None	Yes
ALL	ALL ACCESS NOT ADMIN	None	No
BASIC	Basic low level access	None	No
BOARD	Directors	None	No
DESGN	Technical Drawing and Design	None	No
ENET	e.net solutions	None	No
ENG	Engineering Department	None	No
EQUERY	e.net solutions Queries only	None	No
EXEC	Executive Secretary	None	No
FINANC	Finance	None	No
FullAd	Every Privilege enabled	None	Yes
InfAdm	Administrator Group	None	No
MARK	Marketing Department	None	No
MIS	Management Information Systems	None	No
OPS	Operations	None	No
PROD	Production	None	No
PURCH	Purchasing	None	No

## 2. Create a new group or edit an existing group

In this example, we are looking at the *InfAdm* group highlighted in the above image.



3. In the **Operator Group Maintenance** program above, this operator group only has access to infrastructure settings. Any operator that belongs to this group is unable to perform business operations and can't access setup options for business processes.
4. This operator group also does not have system administrator privileges and is unable to sign out other operators. Access to these Operator and Group Maintenance programs have been restricted to only be accessible by a "Super Admin" operator that implements SYSPRO and creates the security access model.
5. Strictly defining program and activity access across the product will mitigate risk of any damage done.
6. It is advised that access to the **Setup Options**, **Group Maintenance** and **Operator Browse** programs be denied. Access to the System Setup activity should also be denied for all non-

essential operators. This mitigates the risk of one compromised operator having the ability to hijack the system.

## Password Sent Via Email

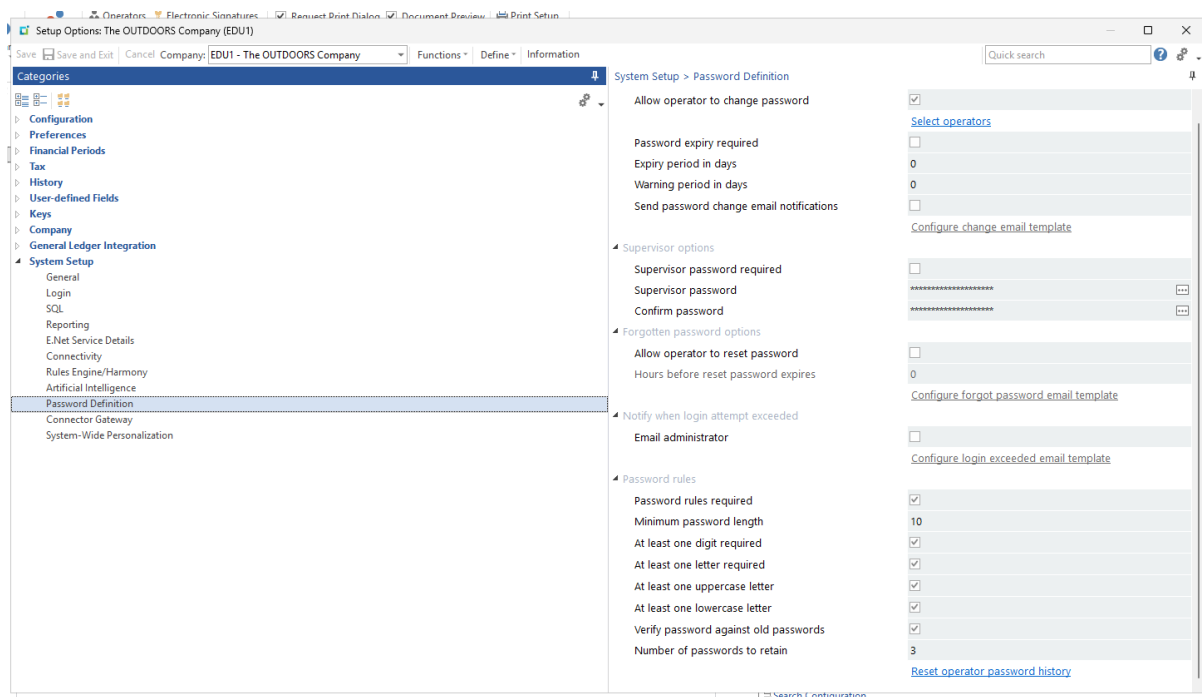
The standard forgot password feature is a basic implementation for on-premise sites with limited security requirements and a minimized setup complexity need.

**Suggested Remediation:** It is recommended to implement Single Sign On (SSO) for a more secure experience when using SYSPRO. Refer to the [Syspro authentication overview](#) document on Single Sign On (SSO).

The **Forgot Password** option can also be disabled for the application, by following these steps:

1. Run the **Setup Options** program.
2. Navigate to System Setup > Password Definition.

The window should now look like the following:



3. Ensure that the **Allow operator to reset password** option is disabled (as seen above).



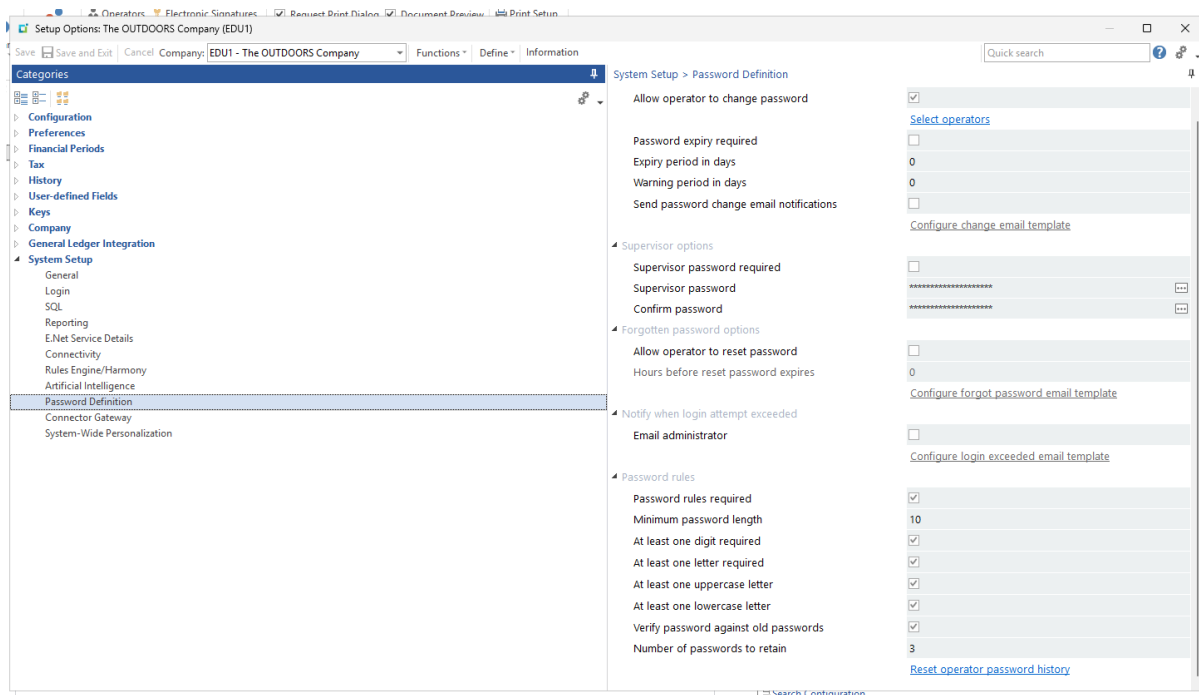
## Preventing Weak Passwords

SYSPRO offers the user the ability to dictate password policies for operators. To ensure that an operator does not have a password that is easily obtainable, a strong password policy should be enforced.

**Suggested Remediation:** The following password policy should be enforced at a minimum:

1. Run the **Setup Options** program.
2. Navigate to System Setup > Password Definition.

The window should look like the following:

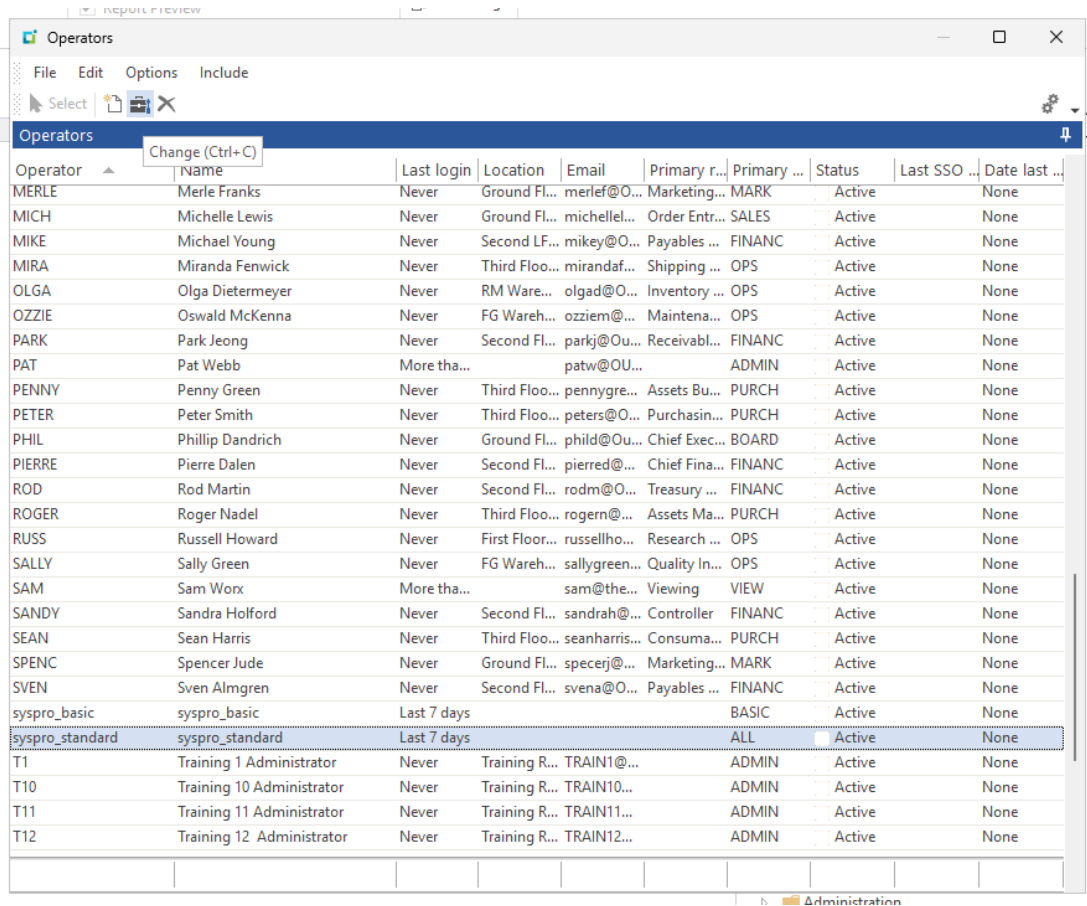


3. Ensure the password rules are set up as seen in the above image.

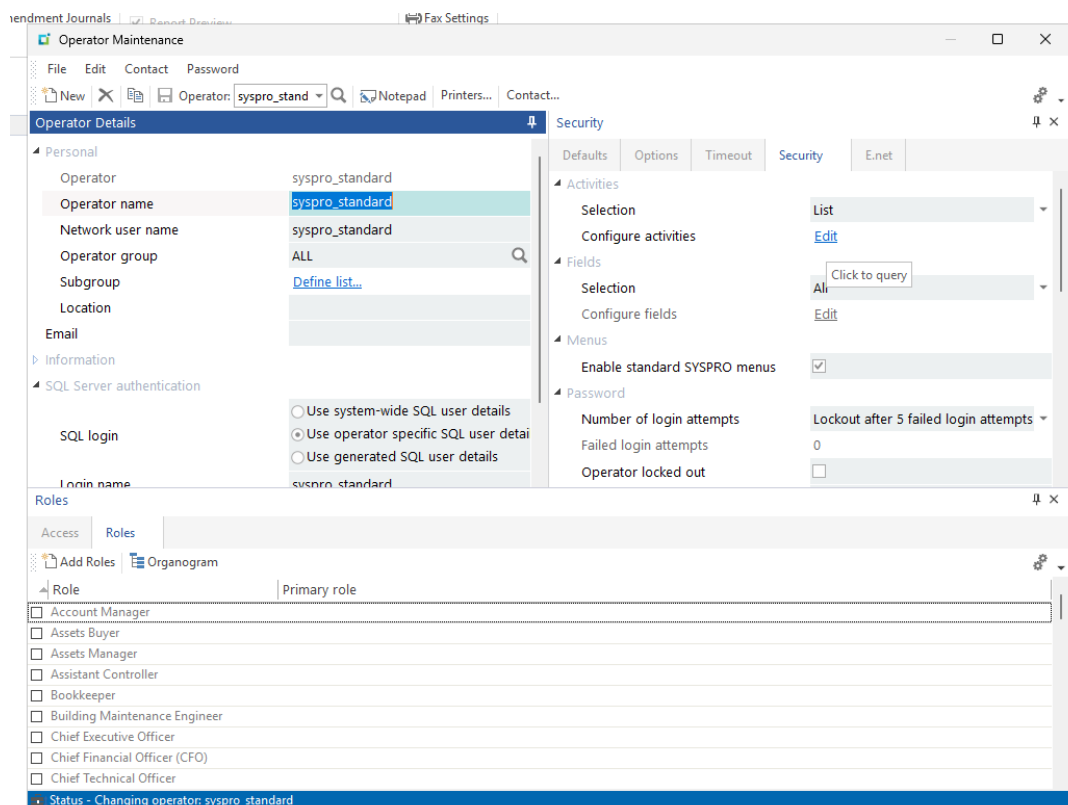
The following criteria are used to assess the strength of a password:

- Avoid using dictionary words or phrases derived from the username
- Ensure the password is at least 10 characters long (14 characters recommended for applications handling sensitive data).
- The password contains uppercase and lowercase letters, numbers, and non-alphanumeric special characters
- Additionally, passwords must be changed periodically, which should be enforced by the system. This can be enforced by enabling the **Password expiry required** option seen above. A suitable password expiry period should be defined.
- Lockout operators after 5 failed attempts in **Operator maintenance**.

4. The operator should be locked out after 5 failed attempts to prevent brute force attacks on a user's system.
  - a. Run the **Operator Browse** program.
  - b. Select an operator and click on **Change** in the toolbar as seen below:



- c. Select the **Security** tab on the right pane for the operator as seen below.



- d. Ensure that the **Number of login attempts** for the **Password** section is set to **Lockout after 5 failed login attempts** as seen above.

## Preventing Sensitive Data Exposure from SQL Server

MS SQL Server offers the option to encrypt network communication between the SQL Server & the SQL Client Application (SYSPRO). This provides the same benefits as using HTTPS instead of HTTP.

Connection encryption should always be enabled in production and testing to ensure the data is not intercepted or changed in transit. Unencrypted connections may be used in development, but it is strongly suggested that developers get used to enabling this feature in their development environments as well.

### Steps to enable SQL Server Connection Encryption

#### Configure MS SQL Server:

The specific steps are dependent on your environment and outside the scope of this article. You will need to consult MS SQL Server documentation on how to enable connection encryption for your SQL Server instance.

You may search online for the topic "Configure SQL Server for connection encryption". The Microsoft article for SQL Server 2025 may be found here: <https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/configure-sql-server-encryption?view=sql-server-ver17>

## Configure SYSPRO:

1. Run the **Setup Options** program.
2. Navigate to the **System Setup** branch and then into the **SQL** branch.
3. The window should look like the following:

System Setup > SQL

- Company database connection
  - Company database authentication
  - SQL Server name
  - SQL Driver to use
  - Encrypted connection string
  - Self-signed server certificate
- System-wide database information
  - System-wide database
- SQL login configuration
  - SQL Login preference
  - Generated SQL user prefix
  - Minimum password length
  - Maximum password length
  - Minimum digits required
  - Minimum letters required
  - Minimum special characters required
- SQL Server administrative information
  - Administrator login
  - Administrator login password

SQL authentication

tcp:ZALPJAMEHEND

SQL Server

☐

☐

DS001\_DB\_900

Use system-wide SQL user details

0

0

0

0

0

sa

\*\*\*\*\*

[Test SQL connection](#)

4. Select the **Encrypted connection string** checkbox.



[syspro.com](https://syspro.com)