Multi-Factor Authentication

SYSPRO 8

Reference Guide

Published: September 2020

SYSPRO
Simplifying your Success

CONTENTS

Multi-Factor Authentication

Multi-Factor Authentication

Exploring

Where it fits in?

Multi-Factor Authentication is a process that identifies a user by validating two or more authentication methods from independent credential categories. This ensures that a user is only granted access after successfully presenting two or more pieces of evidence to the authentication mechanism.

In SYSPRO, the traditional user name and password has been bolstered by the addition of Email and Google authentication to improve security during the login process.

- **Email authentication** sends an email to MFA-defined operators containing a Time-based One-time Password (TOTP) required as part of login verification.
- **Google authentication** uses an app to generate a QR code for first time user configuration and a Time-based One-time Password (TOTP) is required as part of the verification process for subsequent logins.

Navigation

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

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

Terminology

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is the process of identifying a user by validating two or more methods of authentication from independent credential categories.

This authentication method ensures that a user is only granted access after successfully presenting two or more pieces of evidence to an authentication mechanism.

The three most commonly used authentication factors are:

- Knowledge: something only the user knows (e.g. a user name and password, a PIN or answers to security questions).
- Possession: something the user has (e.g. a smart-phone, Time-based One-time Password (TOTP) or smart card).
- Inherence (or biometrics): something unique that proves the user's identity (e.g. a fingerprint, iris scan or voice recognition).

The principle of **Multi-Factor Authentication** is that there is no perfect authentication factor. Any one factor that is implemented will have its strengths and weaknesses. For this reason, the concept of **Multi-Factor Authentication** is that a second or third factor compensates for the weakness of the other factors and vice-versa.

Time-based One-time Password (TOTP)

The Time-based One-Time Password algorithm (TOTP) is an extension of the HMAC-based One-Time Password algorithm (HOTP) which generates a unique one-time password based on the current time.

It has been adopted as **Internet Engineering Task Force standard RFC 6238**, is the cornerstone of **Initiative For Open Authentication (OATH)**, and is used in a number of two-factor authentication systems.

The one-time password must validate over a range of times between the authenticator and the authenticated because of latency (both network and human) and unsynchronized clocks.

Both the authenticator and the authenticatee compute the TOTP value, then the authenticator checks if the TOTP value supplied by the authenticated matches the locally-generated TOTP value.

Some authenticators allow values that should have been generated before or after the current time in order to account for slight clock skews, network latency and user delays.

Starting

Prerequisites

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

System Setup

SYSPRO Ribbon bar > Setup > General Setup

MULTI-FACTOR AUTHENTICATION

- Multi-factor authentication required
- Authentication methods

EMAIL/SMTP SETTINGS

This configuration is required if you select to use the **Email authentication** method.

- SMTP server IP address
- Outgoing email address
- Username
- Password
- Server port
- Use SSL

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 can restrict operator access to *activities* within a program (configured 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).

Restrictions and Limits

- **Multi-Factor Authentication** is not currently available for the following (i.e. an operator configured for **Multi-Factor Authentication** won't be able to login to these platforms):
  - SYSPRO Supply Chain Portal
  - SYSPRO Espresso
- SYSPRO operators cannot be enabled for simultaneous use of **Multi-Factor Authentication** and **Single Sign-on** (Active Directory user).

Solving

FAQs

What auditing capabilities are available for Multi-Factor Authentication?

The following auditing and logging capabilities are available to ensure that **Multi-Factor Authentication** is managed and tracked correctly:

MFA operator status

The system automatically records when **Multi-Factor Authentication** is enabled, disabled, suspended or resumed for an operator using the **MFA Operator Configuration** program.

These entries are stored in the `AdmMfaAuthEnabled` table and you can use the **System Audit Query** program to view the history.

This table includes which operator changed the authentication status and the operator that was changed.

MFA operator methods

The system automatically tracks each operator's configured authentication method when they use the **Multi-Factor Authentication Setup** program.

These entries are stored in the `AdmMfaAuthConfig` table.

MFA login history

This program lets you view the history of successful MFA authentications for the company.

SYSPRO automatically tracks each time an operator successfully authenticates themselves to SYSPRO through **Multi-Factor Authentication** and logs which authentication method is used. Its purpose is to assist system administrators in effectively managing system security.

The entries are stored in the `AdmMfaAuthHistory` table which records each time an operator successfully logs into SYSPRO using **Multi-Factor Authentication**. It includes the date and time they were prompted for the additional authentication, as well as the method used to login and the computer name from which this was done. The **MFA Operator History Query** program lets you view the history.

Although failed login attempts are not currently logged, this will be addressed in a later software release.

What rules apply to operators logging in with Multi-Factor Authentication?

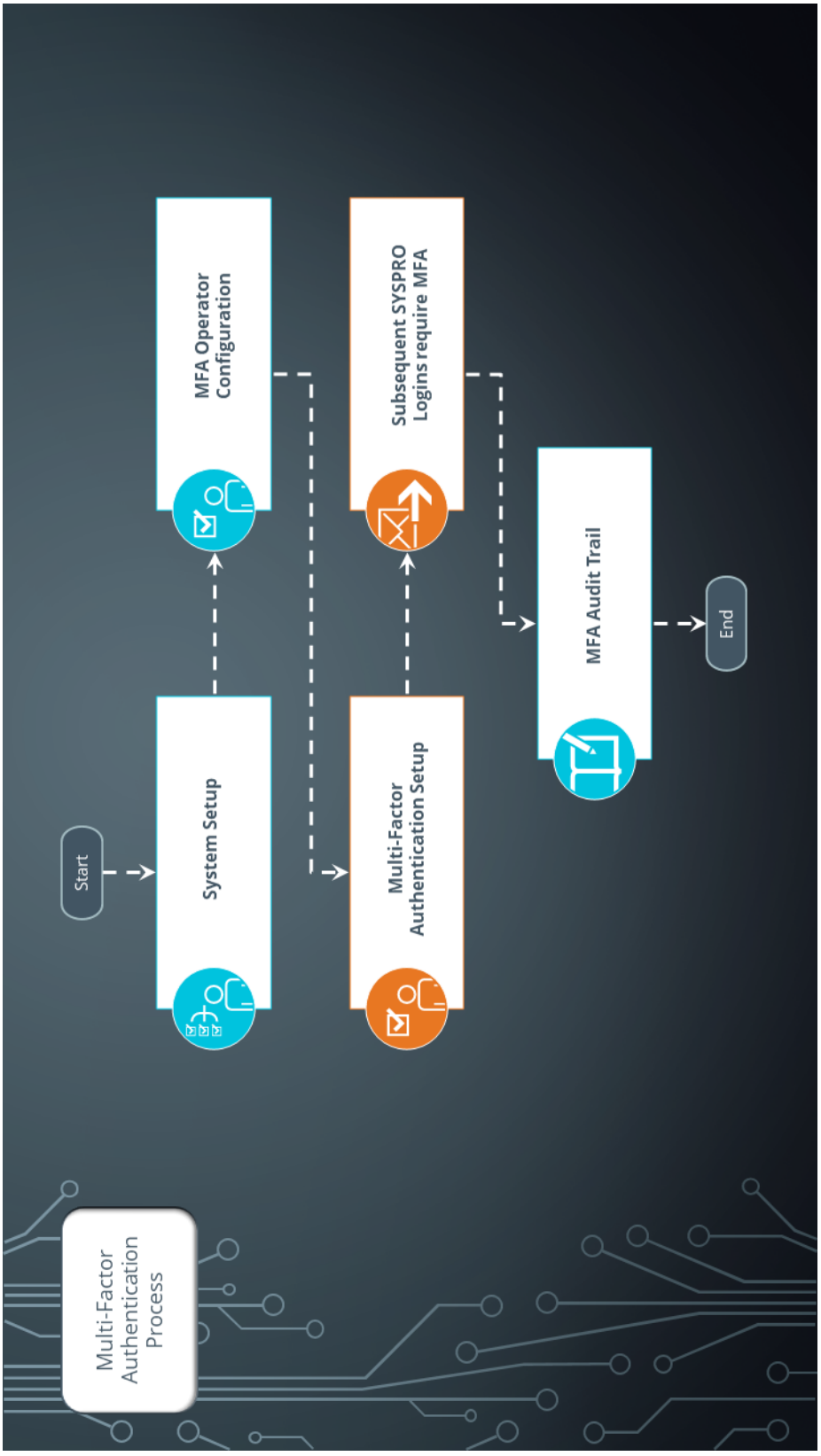
When you login as an operator requiring **Multi-Factor Authentication**, the following rules apply to the `AdmOperator` table of your system-wide database:

- The `AuthenticationType` entry must be **M** (indicating multi-factor authentication).
- The `OperatorType` entry must be **N** (indicating normal operator).
- The `OperatorStatus` entry must be **A** (indicating active).
- The operator code cannot be prefixed with underscores (e.g. __BOT)
- The operator cannot be locked out (i.e. the `OperatorLockedOut` entry must contain spaces and not an **L** entry).

Can MFA-defined operators access applications that use e.net?

An operator code that is configured for **Multi-Factor Authentication** can't be used to access applications that use e.net.

Using



Process

The following describes how a system administrator configures **Multi-Factor Authentication** in SYSPRO:

1. From the **MULTI-FACTOR AUTHENTICATION** pane of the **System Setup** program, indicate that **Multi-Factor Authentication** is required against all, or specific operators.
2. Use the **MFA Operator Configuration** program to view and configure additional MFA requirements (e.g. enabling, disabling, suspending or resuming an operator's MFA requirement).
3. Once MFA is enabled for operators, they are automatically prompted by the **Multi-Factor Authentication Setup** program when next they login to SYSPRO.

   Operators use this program to configure and validate their preferred authentication method.
4. Each subsequent login to SYSPRO requires the one-time, time-based pin from the configured MFA method, before the operator's login is validated.
5. Use the **System Audit Query** program to review an audit log of all operators enabled for **Multi-Factor Authentication**.

Affected Programs

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

System Setup

SYSPRO Ribbon bar > Setup > General Setup

The program includes a **Multi-Factor Authentication** pane that lets you configure additional login authentication for SYSPRO operators.

Multi-Factor Authentication Setup

Program List > Administration > Security

This is a new program that lets operators configure their authentication method when first logging into SYSPRO (after Multi-Factor Authentication has been enabled).

MFA Operator Configuration

Program List > Administration > Setup

This is a new program that lets administrators configure Multi-Factor Authentication per operator.

The program lets you perform a number of Multi-Factor Authentication actions for an operator (e.g. enable, disable, suspend or resume).

System Audit Query

Program List > Administration > Security

The program includes auditing and logging capabilities for all operators who have been configured for Multi-Factor Authentication.

You can view when Multi-Factor Authentication is enabled, disabled, suspended or resumed for an operator, as well as which operator changed the authentication status.

MFA Operator History Query

Program List > Administration > Security

This program lets you view the history of successful MFA authentications for the company.

SYSPRO automatically tracks each time an operator successfully authenticates themselves to SYSPRO through **Multi-Factor Authentication** and logs which authentication method is used. Its purpose is to assist system administrators in effectively managing system security.

MFA Operator History

Program List > Administration > Setup > Reports

This report lets you generate a log of operators that have authenticated themselves to SYSPRO via Multi-Factor Authentication, according to your specified criteria.

www.syspro.com