ERPAdvance asia

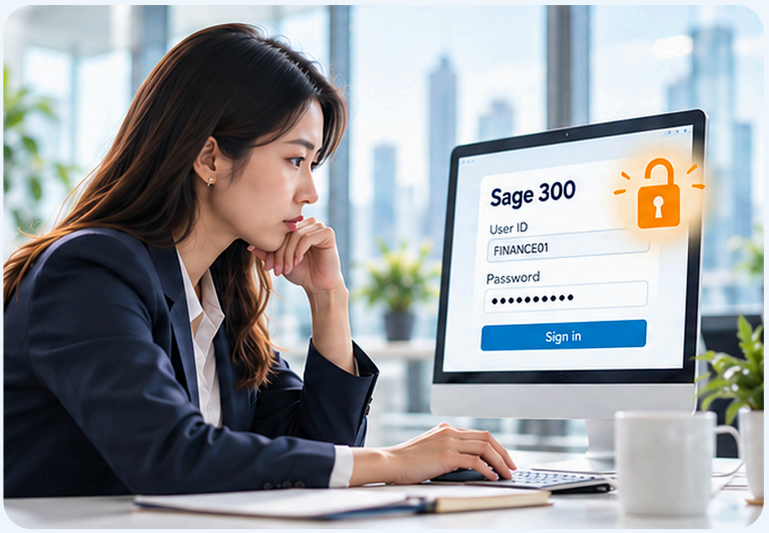
DEVELOPED BY beca

SAGE 300 LOGIN SECURITY

Could someone misuse your Sage 300 login?

A stolen login can put your business at risk.

What they can see or do depends on that user's access rights.



Protect your Sage 300 login with SSO and MFA

For Sage 300 Web Screens and Desktop

BeCa IT Authentication

Why protect the Sage 300 login?

Sage 300 holds sensitive financial, customer and supplier information. If sign-in relies only on a user ID and password, stolen credentials could allow someone to access the system as that user.

Possible business impact

- Unauthorised transactions
- Customer, supplier or payroll data leaked
- Disruption at busy times, such as month-end

Cyber insurance

- Insurers may ask if you use MFA
- Missing or misstated security controls may affect cover or claims, depending on policy terms

Audit and regulatory impact

- Shared logins, or ex-staff who can still log in
- Missing MFA on remote access
- Weak access controls may raise audit findings
- Possible regulatory fines after a data breach

Disruption to your team

- Checking affected transactions
- Restoring systems and data
- Explaining the incident to customers or suppliers

~88% of breaches in the Basic Web Application Attacks category involved stolen credentials

Verizon DBIR 2025

>99% lower risk of account compromise with MFA in a study of Microsoft accounts

Microsoft Research, 2023

Industry research, not Sage 300 or BeCa IT product test results.

A password on its own is no longer enough. Page 2: what SSO and MFA are, and how they help.

What are SSO and MFA?

SSO Single sign-on - one work login

Sign in to Sage 300 with the Microsoft, Google or Okta work account your staff already use.

1. Choose Microsoft, Google or Okta sign-in
2. The work account checks who you are
3. Sage 300 opens as your own Sage 300 user

Having Microsoft 365 does not add SSO to Sage 300 by itself - BeCa IT adds the connection.

MFA Multi-factor authentication

Add a 6-digit authenticator code at sign-in - similar to an extra check in online banking.

1. Sign in with your password, or with SSO
2. Enter the 6-digit code from your phone app
3. Sage 300 opens

Works with Microsoft or Google Authenticator and similar apps. No SMS fees. Never share a code.

Use **SSO, MFA or both**. Already use MFA on your work account? Your partner can check whether it also covers Sage 300.

How they help

Extra protection if a password is stolen

MFA also asks for a code from the user's own phone.

Fewer passwords

One work login for staff, fewer Sage 300 password resets for IT.

Control sign-in in one place

Disable leavers' work accounts and Sage 300 access. End active sessions as part of offboarding.

Same access rights

Existing Sage 300 permissions and audit trails remain unchanged.

Clear answers for auditors

Show auditors and insurers how sign-in to Sage 300 is protected.

Web Screens and Desktop

Protect sign-in on both Sage 300 Web Screens and Desktop.

Which fits you?

SSO

Use your existing work account to simplify Sage 300 access and manage sign-in centrally.

MFA

Keep your Sage 300 login and add a code from an authenticator app.

SSO + MFA

Use work-account sign-in with MFA. Your partner can advise whether existing MFA is sufficient.

Simple to set up

- ✓ No new servers, no Sage 300 code changes
- ✓ Removing it restores the original sign-in
- ✓ Settings stay in your own Sage 300 database
- ✓ Supported Sage 300 releases from 2023 PU2. Confirm your version and Product Update.

Next step: talk to your Sage 300 partner

Ask for a demo and a quotation. Tell them your Sage 300 version, how many users you have, and whether you use Microsoft, Google or Okta. ERPAdvance Asia and BeCa IT support your partner with setup.

No partner yet? Contact us
contact@erpadvanceasia.com
WhatsApp +65 8168 3926