



TECHNICAL SPECIFICATION

BeCa IT Authentication for Sage 300

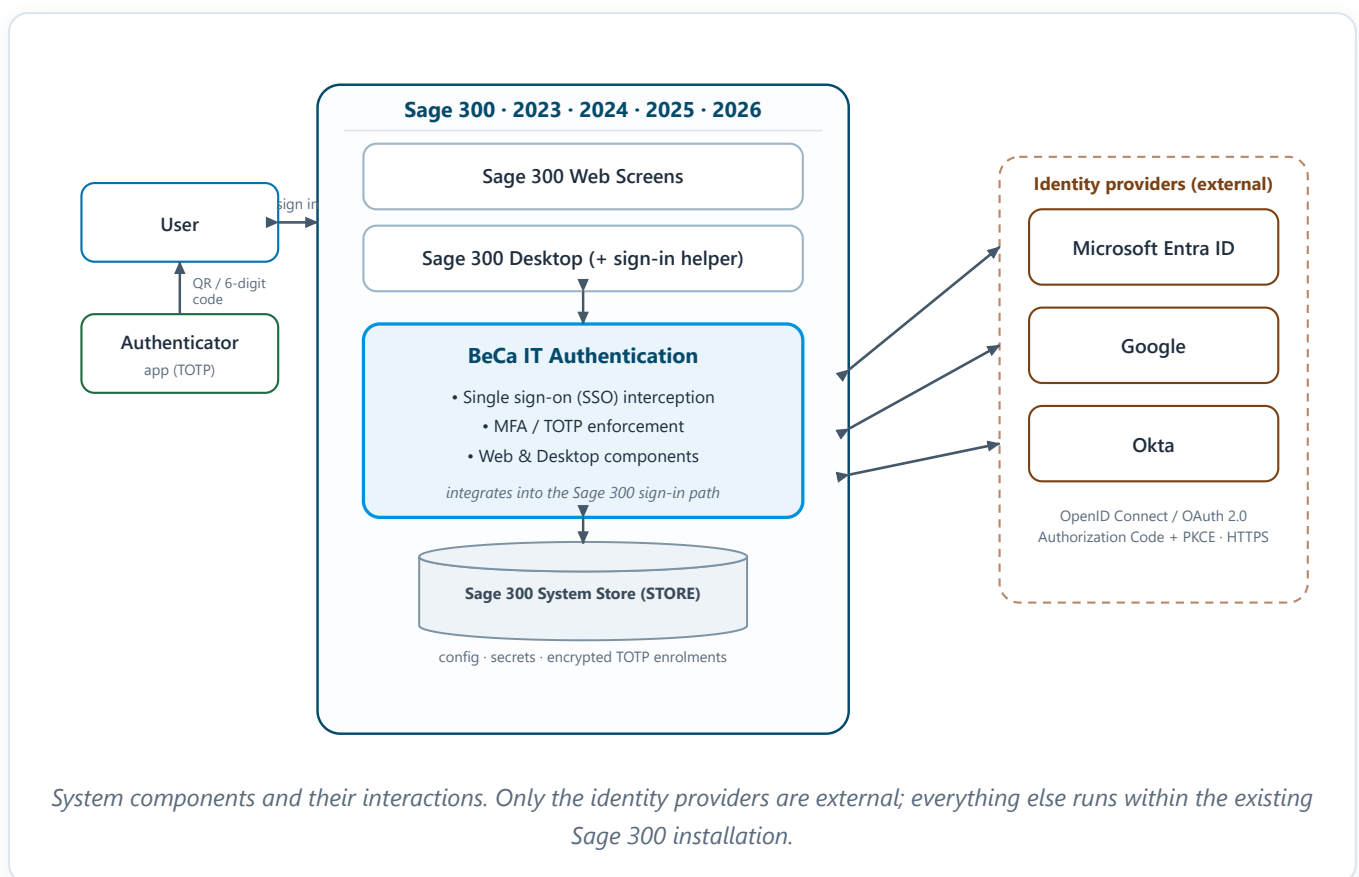
A technical reference for evaluating Single Sign-On (SSO) and Multi-Factor Authentication (MFA) for Sage 300 — standards, identity model, data handling, network posture and licensing.

Applies to Sage 300 **2023, 2024, 2025, 2026** and **2027** · 2023 PU2 → 2027 · Document revision 2026-09

BeCa IT Authentication adds two optional, independently licensed functions to an existing Sage 300 installation. Each is described in its own section below. They install alongside Sage 300, require no changes to Sage 300's own program files, and can be removed cleanly, returning Sage 300 to its original sign-in.

- **SSO** — sign in to Sage 300 with an existing Microsoft Entra ID, Google, or Okta account, on both Sage 300 Web Screens and Sage 300 Desktop.
- **MFA** — a 6-digit, time-based Authenticator-app code added on top of the normal Sage 300 sign-in, for all Sage 300 users.

System components & interactions. The diagram below shows the parts involved and how they communicate. BeCa IT Authentication sits inside the Sage 300 sign-in path: it delegates authentication to the customer's identity provider over standard OpenID Connect, enforces the Authenticator code, and reads its settings and secrets from the Sage 300 system store. The identity providers are the only external parties, reached over outbound HTTPS.



Contents

1. [Single Sign-On \(SSO\)](#)
2. [Multi-Factor Authentication \(MFA\)](#)

Companion documents: the *Administrator Guide* (install / configure / remove) and the *Registration & Authentication Workflow* (step-by-step enrolment and sign-in flows).

1 Single Sign-On (SSO)

SSO lets a user sign in to Sage 300 with their existing organisational identity instead of a Sage 300 password. Authentication is delegated to the customer's own identity provider; Sage 300 then runs as that person's own Sage 300 user.

1.1 — Scope & supported surfaces

Sage 300 versions	2023 PU2 through 2027 — the 2023, 2024, 2025, 2026 and 2027 lines (every Product Update in that range; new PUs onboarded as they ship). Each release ships a version-matched installer; an installer refuses to run on a Sage 300 version it was not built for.
Sign-in surfaces	Sage 300 Web Screens (in the browser) and Sage 300 Desktop (the Windows client). Both are supported by the same configuration.
Identity providers	Microsoft Entra ID, Google, and Okta. The design is OpenID Connect-based and extensible to other OIDC providers.
Provisioning model	Each person signs in as their own Sage 300 user. No shared or service account is used; Sage 300 security, audit and licence counts are unchanged.

1.2 — Standards & sign-in flow

SSO uses the **OpenID Connect / OAuth 2.0 Authorization Code** flow with **PKCE** (Proof Key for Code Exchange, RFC 7636). The product never sees or stores the user's identity-provider password; the provider performs authentication and returns a signed token.

SURFACE	REDIRECT ENDPOINT	NOTES
Web Screens	<code>https://<your-sage300-host>/SSO/Callback</code>	Handled by the existing Sage 300 web site over HTTPS — no new inbound port is opened . Must match the address users browse to (public or internal both work).

SURFACE	REDIRECT ENDPOINT	NOTES
Desktop (Entra / Google)	<code>http://127.0.0.1</code> (loopback)	A sign-in helper opens the system browser and listens on an ephemeral loopback-only port for the duration of the sign-in. Nothing is exposed off the machine. Per RFC 8252 §7.3 , Entra and Google ignore the port when matching a registered <code>http://127.0.0.1</code> redirect, so the helper may bind any free port.
Desktop (Okta)	<code>http://127.0.0.1:<port></code> (loopback)	Okta matches <code>redirect_uri</code> as an exact literal string, port included — it does not apply RFC 8252 §7.3. The sign-in helper therefore binds a port from a fixed, administrator-configured set (<code>OktaLoopbackPorts</code> , default <code>8765</code>), and each port in that set must also be registered in the Okta Native app as a bare <code>http://127.0.0.1:<port></code> authority. On a terminal server (RDS), the set is widened so concurrent Desktop sign-ins each get a free port.

Where the identity provider supports it, a tenant/hosted-domain restriction can be applied (single-tenant Entra app registration; optional Google Workspace hosted-domain; for Okta, the org authorization server is itself selected by the org domain, e.g. `acme.okta.com` — a customer needing a custom authorization server instead configures `acme.okta.com/oauth2/default` in the same field, with no code change). Group or policy restrictions on Okta sign-in are enforced Okta-side. This confines sign-in to the customer's own directory.

1.3 — Identity mapping model

A Microsoft, Google, or Okta identity is matched to a Sage 300 user through Sage 300's native **Windows authentication** fields. The provider is represented as the **Windows Domain**, and the user's sign-in id (UPN / email) as the **Windows User Name**:

SAGE 300 USER FIELD	MICROSOFT ENTRA	GOOGLE	OKTA
Authentication Method	Windows (or Both , to also allow a Sage 300 password)		
Windows Domain	<code>MICROSOFT</code>	<code>GOOGLE</code>	<code>OKTA</code>
Windows User Name	the Entra sign-in id (UPN), e.g. <code>JANE@CONTOSO.COM</code>	the Google account, e.g. <code>JANE@CONTOSO.COM</code>	the Okta login (<code>preferred_username</code> claim), e.g. <code>JANE@CONTOSO.COM</code>

This mapping uses only Sage 300's standard user record — there is no separate user directory to maintain inside the product, and removing the product leaves the Sage 300 users intact.

1.4 — Configuration & storage

All SSO settings are configured once, system-wide, in the **Admin tool** and stored in the Sage 300 **system store** (the `STORE` system database) — not in any individual company database. Settings therefore apply across all companies in the installation.

Per provider	Enable flag, Authority/Tenant, Client ID, and Client Secret (and, for Google and Okta, separate web and desktop client credentials, since both require two app registrations — Google's two OAuth clients, and Okta's confidential Web app plus public Native app, an Okta app's type being fixed at creation; Google also has an optional hosted domain). Okta is stored as provider rows <code>OKTA</code> (org domain and HMAC key), <code>OKTA:W</code> (web client id/secret) and <code>OKTA:D</code> (desktop/native client id — no secret, since it is a public PKCE client).
Okta Loopback Ports	The fixed set of loopback ports the Desktop sign-in helper may bind for Okta (default <code>8765</code> ; see 1.2). Each port must also be registered as a bare <code>http://127.0.0.1:<port></code> redirect in the Okta Native app; the set is widened on a terminal server so concurrent Desktop sign-ins each get a free port.
Integrity key	An HMAC key generated in the Admin tool. It is used to integrity-protect the identity assertion handed to Sage 300 so it cannot be altered in transit between the product's components.
Password fallback	Allow Password Login (Web Screens) accepts a list of CIDR ranges. Empty = password sign-in allowed from anywhere; set = only listed networks may use a Sage 300 password, everyone else must use SSO.
Secrets at rest	The client secret and HMAC key are held in the Sage 300 system store, readable only by the Sage 300 service account and administrators, consistent with how Sage 300 stores its own connection secrets.

1.5 — Security model

- **No inbound ports.** Web sign-in reuses the existing Sage 300 HTTPS site; Desktop sign-in uses a transient loopback-only listener. The product opens no new externally reachable port.
- **No password handling.** The provider authenticates the user; the product receives a standards-based token, never the provider password.
- **Tamper-evident assertion.** The identity passed into Sage 300 is bound with an HMAC so it cannot be forged or modified between components.

- **Least exposure.** Sign-in can be restricted to the customer’s own tenant/hosted domain, and password fallback restricted by network.
- **Clean removal.** Uninstalling restores Sage 300’s original sign-in with no residual configuration in Sage 300’s own files.

1.6 — Licensing

SSO is licensed independently of MFA. A function becomes available only when it is **both enabled and licensed**; an enabled-but-unlicensed function does not appear at sign-in. A configurable reminder banner appears a set number of days before a licence expires (**Expiry Warn Days**); the reminder does not block sign-in. Perpetual and time-limited licences are both supported.

2 Multi-Factor Authentication (MFA)

MFA adds a second factor — a 6-digit code from a standard Authenticator app — to the normal Sage 300 sign-in. It applies to all Sage 300 users once enabled and requires no per-user list.

2.1 — Scope & supported surfaces

Sage 300 versions	2023 PU2 through 2027 — the 2023, 2024, 2025, 2026 and 2027 lines (version-matched installer, as for SSO).
Sign-in surfaces	Sage 300 Web Screens and Sage 300 Desktop.
Coverage	Applies to every Sage 300 user once MFA is enabled — there is no enrolment list to provision. Each user enrolls their own app on first sign-in.
Authenticator apps	Any standards-compliant app — Microsoft Authenticator, Google Authenticator, Authy, 1Password, and others.

2.2 — Standard

MFA implements **TOTP** — Time-based One-Time Password, **RFC 6238** (built on HOTP, RFC 4226). Codes are **6 digits** on a **30-second** window, the de-facto standard supported by every common Authenticator app. Enrolment uses the standard `otpauth://` provisioning URI, presented as a QR code with a manual secret-key fallback.

Algorithm	TOTP / HMAC-SHA1, 6 digits, 30-second period (RFC 6238 defaults).
Enrolment payload	Standard <code>otpauth://totp/</code> provisioning URI, shown as a QR code and as a typed key.

Clock tolerance	A small adjacent-window tolerance is applied so minor device clock drift does not reject valid codes.
------------------------	---

2.3 — Enrolment model

Enrolment is **self-service** and happens automatically the first time a user signs in after MFA is enabled:

1. The user is shown a QR code (with a manual key fallback) to scan in their Authenticator app.
2. The user enters the current 6-digit code once to confirm the pairing.
3. From then on, the user enters a fresh code at each sign-in.

The Authenticator entry is labelled `BeCa IT - <Account Label>` (administrator-set; default `BeCa IT - Sage 300`), so the user can identify it in their app.

2.4 — Configuration & storage

Master Key	Generated once in the Admin tool. It protects the per-user secrets at rest. Regenerating it clears all enrolments — every user re-enrols on next sign-in.
Account Label	The display name shown in users' Authenticator apps.
Per-user secrets	Each user's TOTP secret is stored encrypted at rest (AES, with a per-record initialisation vector) in the Sage 300 system store, never in plaintext and never leaving the server.
Enrolment records	Status and enrolment date per user, kept in the system store and visible in the Admin tool's enrolment manager.

2.5 — Enrolment management

ACTION	EFFECT
Reset	Remove a user's enrolment so they re-pair their Authenticator at next sign-in (e.g. after changing phones).
Revoke	Mark a user's enrolment as revoked.
Revoke All / Restart	Clear every enrolment at once (e.g. after rotating the Master Key).
Refresh	Re-read the current enrolment list from Sage 300.

2.6 — Security model

- **Secrets encrypted at rest.** TOTP secrets are AES-encrypted under the administrator-controlled Master Key and never stored or transmitted in clear text.
- **Server-side only.** Verification happens on the Sage 300 server; the secret never leaves it after enrolment.
- **Administrator control.** Enrolments can be reset, revoked individually, or cleared en masse; rotating the Master Key invalidates all existing enrolments.
- **Standards-based.** Any RFC 6238 Authenticator works; there is no proprietary app or cloud service dependency.

2.7 — Licensing

MFA is licensed independently of SSO and follows the same rule: it is active only when **both enabled and licensed**. The same expiry-reminder banner and perpetual / time-limited licence options apply.