

V5 ULTIMATE 5.10

On-Premises Deployment Specification

Planning reference for V5 Ultimate On-Premises, including Customer-managed cloud, and how it differs from Cloud and Private Cloud, which we host and operate. Commercial terms are set by the Master Services Agreement V1.24 and your Order.

DOCUMENT	On-Premises Deployment Specification
PRODUCT	V5 Ultimate, Version 5.10
REVISION	September 28, 2026
SUPERSEDES	Revision v2026.06 (June 23, 2026), withdrawn
COMMERCIAL TERMS	Master Services Agreement V1.24 and your Order
AUDIENCE	Customer IT, Quality and Procurement
OWNER	S.G. Systems, LLC

CONTENTS

In this document

1	Scope and status of this document	10	Validation
2	Deployment options compared	11	Backup, recovery and high availability
3	On-premises topology patterns	12	Logging and monitoring
4	Hybrid patterns	13	Integrations
5	Reference sizing (planning starting points)	14	Support and releases
6	Platform prerequisites	15	Installation approach
7	Network and connectivity	16	Installation checklist (planning)
8	Identity and access	17	Acceptance
9	Data security	18	What this document is not

This is a technical reference. It does not amend the [Master Services Agreement V1.24](#) or your Order, which govern if anything here differs. The current version of this document is at v5ultimate.com/resources/on-prem-specification.

1 Scope and status of this document

This is a technical reference for installing and operating **V5 Ultimate 5.10 On-Premises**, meaning on infrastructure that you (or your contractor) operate. That includes a cloud account, subscription or tenancy that you control, which the MSA calls a **Customer-managed cloud** and treats as On-Premises.

Commercial terms (licence or subscription, fees, support, liability) are set only by the [Master Services Agreement V1.24](#) and your Order. This document is technical only and does not amend them. The On-Premises Licence Addendum of June 6, 2026 is kept as historical text and does not govern current purchases.

Sizing, topology examples, versions and objectives in this document are planning starting points. The delivery format and supported configurations for a release are those in the Documentation for that release (MSA §4.3), and each site's design is confirmed in writing during project design.

This document does not describe **V5 Classic 5.9**. Classic is a separate product with its own technology stack, supplied On-Premises only (MSA §2.1.2). A Classic licence does not include V5 Ultimate; any move is a separate Order with its own scope and fees ([MSA §4.8](#)).

2 Deployment options compared

V5 Ultimate is available as Cloud, Private Cloud or On-Premises. Your Order states which one applies; there is no default. Private Cloud is hosted and operated by us on the same hosting platform and environment, by the same operator, as standard Cloud, with a separate isolated application instance and a separate database for you ([MSA §2.4](#)). A deployment in a cloud account you control is not Private Cloud: it is a Customer-managed cloud, which is On-Premises.

	CLOUD	PRIVATE CLOUD	ON-PREMISES (INCL. CUSTOMER-MANAGED CLOUD)
Who runs the hosting	Us	Us, same platform and operator as Cloud	You or your contractor
Application and database	Shared service	Your own isolated instance and database	Installed in your environment
Security, patching, backups	Us (MSA Section 9)	Us (MSA Section 9)	You (MSA §4.3, §9.4)
Release timing	Our schedule with notice (§8.1(a))	Coordinated; 180-day deferral window (§8.5)	You decide when to apply (§8.1(c))
Service levels	MSA §11.3	MSA §11.4	Software support only (§11.2); no uptime, RPO or RTO
Validation	Your Quality team (§7.2)	Your Quality team (§7.2, §7.2.1)	Your Quality team (§7.2, §10.1)

Private Cloud release deferral (not On-Premises)

For a Private Cloud production instance you may defer a routine, non-security feature release and stay on the prior supported version for up to **180 calendar days** from our written release notice, which includes release notes and impact information. Installation windows are agreed together, and we give at least 30 days' written notice before the window ends. If you supplied a documented validation plan with milestones and need more time, a reasonable extension can be recorded in writing before the window ends. We may require earlier mitigation or upgrade for a critical security vulnerability or active threat, a legal or regulatory requirement, a material incompatibility or end of life of an underlying platform component; urgent security patches may be applied sooner ([MSA §8.5](#)). This window does not apply On-Premises, where you control deployment timing.

3 On-premises topology patterns

The patterns below are the shapes most often discussed in project design. Which ones are supported for a given release, and in what form, is confirmed from the release Documentation.

PATTERN	DESCRIPTION
Linux virtual machine or server	Application and database on customer-operated Linux hosts, on a single host or split between application and database. On Windows Server sites this runs as a Linux guest on Hyper-V, VMware, Nutanix or Proxmox.
Container host	A single Linux host running the application as containers. Suits smaller sites, pilots and validation or sandbox environments.
Container orchestration	A cluster-based deployment for multi-site or high-availability designs, with the database run separately. Scope and supported platforms confirmed per project.
Customer-managed cloud (On-Premises)	The same software installed in your own AWS, Azure or Google Cloud account, using services you operate (for example managed database, key management and object storage). You hold the credentials and operate the environment. Not Private Cloud.
Hybrid	A mix of on-premises and Customer-managed cloud tiers, all operated by you. See Section 4.

4 Hybrid patterns

Hybrid means a deployment that spans your own site infrastructure and your own cloud tenancy. Every tier is operated by you. Common shapes to discuss in project design:

- **Application on site, data in your cloud.** Application and operator stations on the plant network, close to scales and printers; database and file storage in your cloud account. Needs a stable, adequately sized site-to-cloud link; behaviour when the link is lost is confirmed during design.
- **Site edge with central application.** A site node connects local devices while the main application and database run in your cloud account. Whether and how local operation continues through a network outage is confirmed during design; it is not assumed.
- **On-site primary with cloud recovery.** Production on site, with a standby copy in your cloud account for disaster recovery. Your recovery objectives are set and tested by you.
- **Multi-site.** Some sites on-premises, others in your cloud account, with shared single sign-on and reporting and per-site data residency as you design it.

The project design records which tier runs where, who owns the link between them, and how your validation covers each part.

5 Reference sizing (planning starting points)

Starting points for one production site and one environment (production, validation or sandbox), covering application and database unless split. Allow roughly 25% more per additional concurrent site. Final sizing depends on sites, concurrent users, throughput, retention and any high-availability design, and is confirmed in project design.

TIER	CONCURRENT USERS	VCPU	RAM	STORAGE (YEAR 1)
Small (single line or pilot)	up to 25	4	16 GB	200 GB SSD
Medium (one plant)	25 to 100	8	32 GB	500 GB SSD
Large (multi-line plant)	100 to 300	16	64 GB	1 TB NVMe
Enterprise (multi-site, HA)	300+	2 × 16 (app) + 16 (db)	128 GB+	2 TB+ NVMe, replicated

6 Platform prerequisites

COMPONENT	PLANNING BASELINE
Operating system	Linux server. Supported distributions and versions are listed in the release Documentation.
Database	PostgreSQL, operated by you (self-managed or your cloud provider's managed service). Supported versions per the release Documentation.
File storage	S3-compatible object storage or local storage for attachments and backups, operated by you.
Web access	Your reverse proxy or load balancer terminating TLS; TLS 1.2 minimum, TLS 1.3 recommended.
Browsers	Current versions of mainstream browsers for office users and operator stations.

Windows Server sites

There is no Windows-native build of the V5 Ultimate application tier. On a Windows Server site, the recommended pattern is a Linux virtual machine on your existing host (Hyper-V, VMware, Nutanix or Proxmox), which keeps your Windows team in charge of the host. Docker Desktop is a Windows 10/11 client product and is not supported on Windows Server, so it must not be used as the host runtime. Any other arrangement is not a standard configuration and would need to be scoped separately.

7 Network and connectivity

- **Inbound:** HTTPS (443/tcp) from office users, operator stations and integrated systems on your network.
- **Internal:** application to database (for PostgreSQL, 5432/tcp by default) and to file storage, inside the deployment network.
- **Optional outbound:** your identity provider, your mail relay for notifications, and any ERP or other integration endpoints you configure.
- **Devices:** scales, label printers, scanners and sensors on the same network segment as the application, or routed through a gateway you control.
- **Air-gapped sites:** an air-gapped On-Premises deployment is available as an option. Some analytics features may be unavailable without outbound connectivity, and licence enforcement described in the Documentation still applies (MSA §14.5).

8 Identity and access

- SAML single sign-on with identity providers such as Okta, Microsoft Entra ID and Google Workspace.
- SCIM user provisioning is listed as coming soon and is not currently available.
- Role-based access control, unique user identities and electronic signatures, configured to your procedures.
- Operator accounts can be limited to shop-floor use without administration access, as configured.

9 Data security

- **In transit:** TLS on external connections, terminated at your proxy or load balancer.
- **At rest:** encryption provided by your database, volume or cloud storage encryption, using keys you manage. We do not hold your keys for an On-Premises deployment.
- **Audit trail:** regulated actions such as signatures, overrides and record changes are written to an audit trail designed not to be editable through the application.
- **Secrets:** database credentials and keys held in your secret store (for example container or cluster secrets, or a cloud or third-party vault), not in plain files in production.
- **Responsibility:** for On-Premises you are responsible for infrastructure security, backups and disaster recovery; we have no access to your data except as you authorise (MSA §9.4).

10 Validation

V5 Ultimate 5.10 (and V5 Classic 5.9) have each been independently assessed by Dr. Bob McDowall. Each assessment is limited to the version, scope and findings in its report and is available on request under confidentiality ([MSA §7.1](#)). You may use the 5.10 assessment as supporting evidence in your own validation of that version. It is not regulatory approval or certification, and it does not validate your instance, configuration or deployment, or any later version.

Your Quality team is responsible for intended-use validation, testing (including IQ, OQ, PQ and UAT as applicable), approval, release and change control (MSA §7.2, §10.1). Validation assistance, including any qualification documentation or help executing it, is provided as described in the MSA and as purchased in your Order.

On-Premises, you decide when to apply a release in your environment (MSA §8.1(c)), so you can validate before production use. Emergency patches are made available with recommended deployment guidance (MSA §8.4).

11 Backup, recovery and high availability

For On-Premises, backup, disaster recovery and availability are yours to design, operate and test. The MSA's uptime, backup, RPO and RTO commitments apply only to hosted services and not to On-Premises (MSA §11.9). For comparison, Private Cloud backup and recovery levels are in MSA §11.4.

- **Backups:** a common design is regular full database backups plus continuous transaction-log archiving to storage you control, encrypted with your keys, with retention set by your record-keeping rules.
- **Recovery objectives:** set by you for each site and proven by restore tests.
- **High availability:** where needed, multiple application instances behind your load balancer and a replicated database, scoped in project design.
- **Drills:** restore into a separate database at go-live and at regular intervals thereafter.

12 Logging and monitoring

- Application logs can be collected by your existing log platform.
- Health checks for your load balancer or orchestrator are described in the release Documentation.
- Monitoring, alerting and capacity management of the infrastructure are operated by you.

13 Integrations

Availability depends on your plan, configuration and connected systems; feasibility for an On-Premises site is confirmed in project design.

- **ERP:** ERP connectors that extend your existing ERP to the shop floor, set up through a guided connect, map, dry-run and go-live process. V5 runs alongside your ERP; it is not an ERP.
- **API:** REST API (read and write) and webhooks.
- **Trading partners:** EDI documents and GS1-128 shipping labels.
- **Devices:** scales, printers, sensors and PLCs, including Mettler SICS, Modbus TCP, OPC-UA, MQTT and Zebra ZPL.
- **Identity:** SAML single sign-on, as in Section 8.

14 Support and releases

For On-Premises we provide remote software support, operational guidance and troubleshooting for defects reproducible in a supported configuration. No uptime is warranted. Target initial response times ([MSA §11.2](#)):

SEVERITY	MEANING	TARGET INITIAL RESPONSE
1	Production down	2 business hours
2	Major impairment	1 business day
3	Minor issue	2 business days
4	Question or request	3 business days

- These are initial response targets, not resolution guarantees. On-site support needs a separate statement of work.
- The former Silver, Gold, Platinum and Diamond support tiers are retired and replaced by this severity-based framework (MSA §11.12).
- Licence or subscription terms, entitlements and any source-code escrow are only those stated in the MSA and your Order.

15 Installation approach

PATH	WHO INSTALLS	WHO VALIDATES	TYPICAL FIT
Customer install	Your IT team, following the release Documentation	Your Quality team	Strong IT teams, sandbox and validation environments, pilots
Assisted install	Our engineer with your IT team, as a purchased service	Your Quality team, with any validation assistance in your Order	First production site, regulated sites, tight deadlines
Mixed	Assisted for production; your team for further environments	Your Quality team	Multi-environment or multi-site rollouts

Services, scope and fees for any assisted work are agreed in your Order or statement of work.

16 Installation checklist (planning)

A planning checklist for the setup engineer. Exact steps, files and commands come from the release Documentation. Record evidence for each step as your validation plan requires.

1. Confirm server specifications against the agreed sizing.
2. Prepare the Linux hosts (on Windows Server sites, the Linux guest virtual machine).
3. Install the container runtime or other prerequisites named in the release Documentation.
4. Install or connect the database and confirm encrypted connections.
5. Create a dedicated database and a non-superuser owner role.
6. Load the release deliverables as described in the Documentation.
7. Apply licence activation as described in the Documentation.
8. Store credentials and keys in your secret store.
9. Configure TLS at your reverse proxy and restrict inbound access to HTTPS.
10. Start the services and confirm the health checks pass.
11. Sign in through a browser and confirm single sign-on with your identity provider.
12. Test an operator sign-in on a representative shop-floor device.

13. Test one printer, scanner and scale per line, where used.
14. Run a backup to your storage and confirm it is encrypted.
15. Restore into a separate database and confirm the records and audit trail match.

17 Acceptance

Acceptance criteria are those in your Order or statement of work. Typical evidence includes the completed installation checklist, your approved test results for an end-to-end signature workflow on a representative record, and a successful restore test.

18 What this document is not

- Not a statement of work or a commercial offer. Scope, pricing and term are in your Order.
- Not a contract term. The MSA V1.24 and your Order govern, and prevail over this document.
- Not a certification or validation of your system. See [Security & Trust](#) for our current security posture.

For a sized proposal or a project design discussion, use the contact form at v5ultimate.com/resources/on-prem-specification.

S.G. Systems, LLC · V5 Ultimate 5.10 · On-Premises Deployment Specification · Revision September 28, 2026.
Supersedes Revision v2026.06 (June 23, 2026). Current version and contact form: v5ultimate.com/resources/on-prem-specification.