FOR IT, INFOSEC, COMPLIANCE AND PROCUREMENT TEAMS

Security and Architecture Overview

Your organization is evaluating Reportworq. This document explains, in plain terms, what the software is, where it runs, what it connects to, and what it needs from your network, so each team in the approval process can do its part quickly. It is not an installation guide.

Executive summary

Reportworq is enterprise reporting and distribution software that you install and run on your own servers. It connects to the systems where your numbers live, such as IBM Planning Analytics, Workday, Oracle and SQL databases, builds formatted reports in Excel, PDF and PowerPoint, and delivers each person the version they are entitled to see through services such as email, Microsoft 365, Google and Box, on a schedule or on demand. It requires no cloud service to run, and it connects to the systems you choose to connect it to (plus a public map service, only when a report includes a map).

WHERE IT RUNS Your servers, on premises or in your own cloud tenant. Windows Server 2016 or later, or 64-bit Linux. A container image is also available.	**HOW PEOPLE USE IT** A web application in a Chromium browser (Chrome or Edge), plus an optional add-in for Excel and PowerPoint.
CLOUD DEPENDENCY None required. Optional services (a cloud relay, hosted AI) are off until you turn them on.	**INTERNET ACCESS** Not required. Runs on an air-gapped server; every online step, including periodic license renewal, has an offline alternative.
WHERE DATA IS STORED A folder on your server or file share (the repository). No separate database server is needed.	**IDENTITY** Built-in accounts, or single sign-on with Microsoft Entra ID, Google or any OpenID Connect provider, whose group claims can manage access.
NETWORK PORTS One web port (default 8600 on Windows, 8080 on Linux) and an internal event hub port one above it.	**WHAT IT CONNECTS TO** What you configure: your data sources and your delivery channels, each with its own credentials.

The most useful thing to know: not every connector, integration or capability described here is something you need. Reportworq brings very little of its own to your network. What it touches is defined by the data sources and delivery channels *you* decide to use, and each of those brings its own, familiar network and authentication requirements. Start with your use case, then read only the sections it involves.

1. Architecture at a glance

Reportworq is a single service that hosts a web server and a job engine. Administrators and authors work in the browser; scheduled jobs pull data from your sources, produce reports, and deliver them to the destinations you configure. Everything it keeps (definitions, outputs, run history, audit logs) lives in its repository.

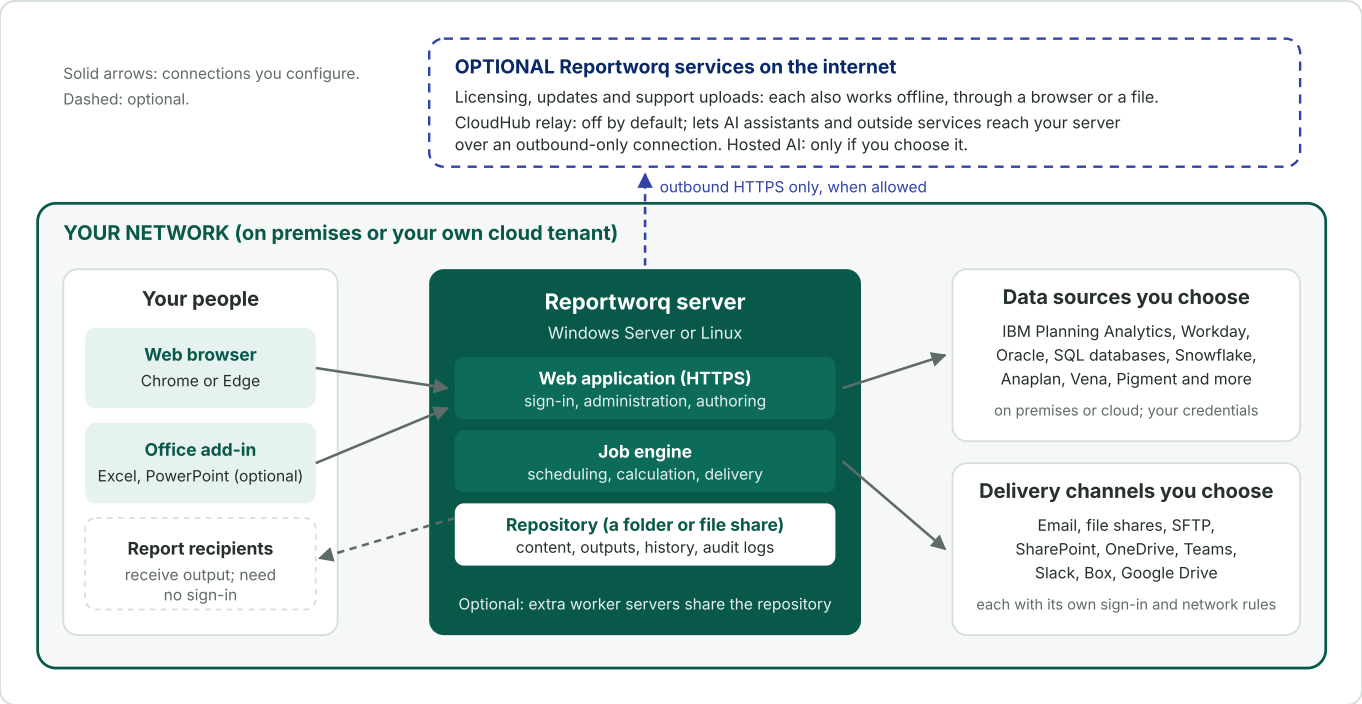


Figure 1. A typical single-server deployment. The server initiates the connections to your data sources and delivery channels; nothing outside your network needs an inbound path to it unless you choose to publish it.

Deployment options

Option	What it is
Windows Server	The standard install: an installer (MSI) and a Windows service that hosts the web application and the job engine. Windows Server 2016 or later.
Linux	The same application as a tarball run under systemd, or as a Docker container. A current 64-bit distribution such as Ubuntu. Feature parity with Windows.
Your Azure tenant	The container image on Azure App Service or Container Apps, with the repository on an Azure Files share. Single-tenant: it is your instance, in your subscription.
Load-balanced cluster	For high volume: one main server plus worker servers that share the repository on a network share. Each job runs whole on one server. Licensed separately.

Server sizing

Size the server for the workload. The baseline is a 4-core x64 CPU at 2 GHz or faster, **32 GB of RAM** (plus about 2 GB for each job running at the same time; the default is four), and 10 GB of free disk that grows with the repository. No GPU is needed. On Linux, the .NET runtime is bundled; a few font and rendering libraries are installed from the distribution. Reportworq 6 can run beside an existing Reportworq 5 on the same server.

More in the documentation: System requirements, Deployment topology.

2. What Reportworq connects to: your choice

Reportworq integrates with many systems, but **each integration is an option, not a requirement**. A connection exists only once an administrator configures it, and it uses the credentials and network path you give it. Your existing rules for that system (firewall rules, service accounts, app registrations, API keys) apply unchanged. Beyond them, the only outside service Reportworq contacts for report content is a public map service, and only when a report includes a map (see section 5).

Data sources

Most organizations connect Reportworq to **one primary source** and perhaps a few supporting ones. The catalog includes IBM Planning Analytics (self-hosted, IBM Cloud and IBM SaaS), SQL Server, ODBC and OLE DB databases, Snowflake, Oracle EPM Cloud, Power BI and Analysis Services, Workday Adaptive Planning and Workday, Anaplan, Vena and Pigment, plus drivers for systems such as Salesforce, NetSuite, Databricks, SAP HANA, Dynamics 365 and Google BigQuery. Through its connectivity partner, Reportworq has access to some 250 data sources in all, and any of them not yet in the product can be added. A source may be on your network or in the cloud; either way the server needs a network route to it and an account on it.

Source	How Reportworq authenticates
IBM Planning Analytics (self-hosted)	Native Planning Analytics security, Windows integrated security (Active Directory), or IBM Cognos (CAM). Needs the Planning Analytics REST port open from the Reportworq server.
IBM Planning Analytics (IBM Cloud / SaaS)	A non-interactive service user, or a tenant ID and API key.
Workday Adaptive Planning	An Adaptive Planning user name and password, an Adaptive authentication token, or Workday OAuth (client ID, secret and refresh token). HTTPS to the Adaptive Planning API.
Workday (Financial Management, HCM)	A Workday integration user with OAuth or Basic credentials, reading web-service-enabled custom reports (or WQL, REST or SOAP). HTTPS to your Workday tenant.
SQL Server, ODBC, OLE DB	A connection string with a database account (stored encrypted).
Other cloud platforms	The platform's own API credentials: an API key, a service account, or OAuth, as the vendor requires.

More in the documentation: Connector catalog, Connect IBM Planning Analytics, Connect Workday Adaptive Planning, Connect Workday.

Delivery channels and integrations

Channel	Authentication	Network
Email	Your SMTP relay, Microsoft 365 (OAuth or Graph), or SendGrid	SMTP (25 or 587) or HTTPS
Network folder	The Reportworq service account's own file permissions	SMB to the share
SFTP	Server address, user name and password	SSH (22) to the server
SharePoint, OneDrive, Teams	A Microsoft Entra app registration (see section 3)	HTTPS to Microsoft 365

Slack	A Slack app's bot token, with scopes to post messages and files and to look up channels	HTTPS to Slack
Box	A Box server-to-server app (client credentials)	HTTPS to Box
Google Drive, Google Cloud Storage	Google OAuth credentials or a service-account key	HTTPS to Google
IBM Planning Analytics	Writes output back to a Planning Analytics application folder	As for the data source

Job-run notifications are sent by email. Recipients of a report do not need a Reportworq account.

More in the documentation: Destinations, Distribution overview.

3. Microsoft 365 and the Office add-in

Microsoft 365 integrations

Anything Microsoft-based (Entra ID sign-in, Microsoft 365 email, SharePoint, OneDrive and Teams) uses **one app registration that your administrator creates in your own Microsoft Entra tenant**. It is single-tenant and owned by you. It uses delegated permissions, granted by your administrator's consent, and an administrator can remove any permission for a feature you do not use. The redirect addresses point back to your own Reportworq server, which must be served over HTTPS for these features to work.

The Office add-in (Excel and PowerPoint)

The add-in lets authors build and refresh reports inside Excel and PowerPoint. It is listed in Microsoft's Office Store (AppSource), and your Microsoft 365 administrator deploys it to the users who need it through Centralized Deployment in the Microsoft 365 admin center, or through a trusted add-in catalog. Users sign in to **your** Reportworq server from the add-in, and their report data flows between Office and that server. The add-in's user interface files are served from `officeaddin.reportworq.com` to the user's Office client. The add-in is optional: an organization that does not deploy it loses nothing on the server side.

More in the documentation: Microsoft 365 setup, The Office add-ins.

4. Cloud services: none required, some available

Reportworq does not require any cloud component to run. Two optional services exist for customers who want them.

CloudHub relay Off by default

A Reportworq-operated relay that lets services outside your network reach your on-premises server **without an inbound firewall rule or a public address**. Your server opens an outbound HTTPS connection to the relay and requests come back down it. It supports:

- AI assistants (Microsoft 365 Copilot and desktop clients using the Model Context Protocol, MCP) reaching the distribution jobs you have published to them;
- automation platforms calling the Reportworq REST API to start a job.

It is a convenience, not the only route: you can instead publish the MCP endpoint through your own reverse proxy. An administrator enables or disables CloudHub at any time.

AI features Off until configured

AI features are opt-in. An administrator adds a connection to the AI provider of your choice (OpenAI, Azure OpenAI, Amazon Bedrock or Google Gemini) **using your own account and key**, or chooses Reportworq AI, a

hosted option brokered through your license that is intended for trials and demonstrations, not production use. When a user runs an AI feature, the data it needs is sent to the provider you configured; in the Office add-in, nothing is sent until the user acts. Every AI prompt and response is recorded in an administrator-only audit log.

More in the documentation: AI integration overview (CloudHub and MCP), Connect an AI provider.

5. Internet access and air-gapped operation

Reportworq runs on a server with no internet access. It contacts Reportworq-operated services for a small number of things, and each one has an offline path. The one thing an offline server must not forget is license renewal.

Purpose	With an internet connection	Without one
License activation	Activates automatically against the Reportworq licensing service.	Manual activation: the server shows a request code, an administrator exchanges it for a response code on the Reportworq documentation site from any machine with a browser, and pastes it back.
License renewal	Once a day the server renews its license and reports usage information with it. If the service cannot be reached, the failure is logged and the server keeps running.	Repeat the manual code exchange approximately once a year (Reportworq support can confirm your license's renewal date) and after each upgrade to a new minor version (for example 6.1 to 6.2). A license that is not renewed in time lapses, and jobs stop running until it is renewed.
Updates and patches	Settings, Update Reportworq lists available versions and installs the latest release, a hotfix, or a specific version, in the application.	Download the patch file on another machine, carry it over, and apply it on the same screen with Update with a patch file.
Support diagnostics	At the push of a button, an administrator uploads a diagnostics packet (logs, and optionally repository data and job history, as the administrator chooses) securely to the Reportworq support desk. The upload is authenticated with your license key and asks for confirmation first. Uploaded files are kept for 30 days, then deleted automatically.	Download the same packet through the browser and send it by any channel your policy allows.
Product news	The administrator console shows headlines from the public Reportworq forum, fetched once a day.	The panel is simply empty.

CloudHub and Reportworq AI contact the internet only if you enable them (section 4). Integrations with cloud services (Microsoft 365, Google, Slack, Box, cloud data sources) need routes to those services, as described in section 2, and single sign-on with Entra ID or Google needs a route to that identity provider.

Maps in reports

When a report contains a map chart, the server fetches map tiles from OpenStreetMap (or another public tile service the author names), and looks up place names with OpenStreetMap's geocoding service. **The place names a map searches for, which can come from report data, are sent to that service.** Without access, maps draw without background tiles and the rest of the report is unaffected. If your policy does not allow this, block the hosts below or do not use map charts.

Outbound destinations for your firewall

Host	Used for	Needed?
`quelock.reportworq.com`	Licensing, the daily license check, the update catalog and downloads, support uploads, Reportworq AI	Optional
`api.reportworq.com`	CloudHub relay, only when enabled	Off by default
`tile.openstreetmap.org` `nominatim.openstreetmap.org`	Map tiles and place-name lookups, only when a report contains a map chart (an author may name another public tile service)	Maps only
`forum.reportworq.com`	Product news headlines in the administrator console	Optional
`officeaddin.reportworq.com`	Office add-in user interface, loaded by users' Office clients (not by the server)	Add-in only
Your chosen services	Microsoft 365, Google, Slack, Box, cloud data sources, AI providers	As configured

All of these are reached over HTTPS, outbound only.

More in the documentation: Licensing and manual activation, Update Reportworq, Log diagnostics and support.

6. Security controls

Identity and sign-in

- One sign-in method at a time: built-in Reportworq accounts, or single sign-on through **Microsoft Entra ID, Google, or any OpenID Connect provider** you run.
- With single sign-on, your identity provider enforces your policies, including multi-factor authentication.
- **Manage access from your identity provider.** Role and group claims from your SSO provider can drive Reportworq roles and group membership, so adding or removing someone in your directory grants or removes their Reportworq access at their next sign-in, with no separate user list to maintain. To cut access at once, disable the account in Reportworq as well.
- Built-in accounts have password complexity, expiry and lockout rules. Passwords are stored as one-way hashes.
- SAML and LDAP are not supported directly; connect through an OpenID Connect provider.

Access control

- Roles separate administrators, authors and users; only administrators change security.
- **A new installation starts open:** everyone who can sign in holds the Administrator role, the root folder and the default workspace, so the first administrator can set up. Remove those All Users grants before you connect your directory, and with Entra ID, require user assignment on the app registration.
- Content lives in workspaces with folder and item permissions; groups can be managed in Reportworq or driven by your identity provider.
- Bursting sends each recipient only the slice of a report meant for them.
- A built-in security audit report shows who can see what.

Auditing

- Administrator-only audit logs record configuration, security and sign-in changes (with before and after values), every job run, every AI interaction, and every AI assistant (MCP) request.
- Retention is configurable; logs export to Excel.

Data at rest

- Everything Reportworq keeps lives in its repository, a folder on the server or a network share, with embedded databases for history and audit. **No database server is required**, and backing up the folder backs up the system.
- Output and run-history retention is set by job or folder and enforced automatically.
- Stored credentials (data source passwords, API keys, tokens) are encrypted at rest with AES-256. Restrict access to the repository folder at the operating-system level.
- A secret-rotation API (off by default) lets tools such as CyberArk or HashiCorp Vault rotate stored credentials.

Data in transit

- The web application is served over HTTPS with your own certificate. A new Windows install starts on HTTPS (port 8600) with a self-signed certificate; on Linux and in containers (port 8080) you enable HTTPS in configuration or put your TLS reverse proxy or load balancer in front.
- TLS versions and ciphers follow the operating system's policy.
- The event hub port (web port plus one, 8601 by default) carries internal traffic between Reportworq processes and servers **without encryption or authentication**. Firewall it so that only Reportworq servers can reach it.

Programmatic access

- The REST API requires a named API key, each tied to one workspace. The AI assistant (MCP) endpoint is set to off, an instance-wide API key, or OAuth scoped to the signed-in user. Both can be turned off.
- Script Runner (licensed with the API) lets job authors run C# scripts at points in a job. Scripts run on the server under the service account, so grant job-editing rights accordingly.

More in the documentation: Sign-in and single sign-on, Accounts, groups and entitlements, Audit logs, Secret rotation.

7. A checklist for your teams

Team	What to confirm
IT / infrastructure	A Windows or Linux server sized for the workload; a service account; the web port open to users; HTTPS certificate; backups of the repository folder; for an offline server, who renews the license and when.
Network	Routes from the server to the data sources and delivery channels you will use. Outbound HTTPS to the hosts above only for what you want (online licensing, updates, support uploads, maps). The event hub port closed to everything but Reportworq servers.
Identity	Your sign-in choice; if Microsoft-based, one Entra app registration and administrator consent. Remove the open All Users grants first.
InfoSec	The optional services you will allow (CloudHub, AI provider, map services), who may edit jobs and scripts, access to the repository folder, and audit log retention.
Desktop / Microsoft 365	Whether to deploy the Office add-in, and to which users.
Procurement	License entitlements: capabilities, connectors and cluster nodes are enabled per license.

Learn more at docs.reportworq.com (system requirements, deployment topology, sign-in, licensing, updates, audit logs). Questions: support@reportworq.com. Describes Reportworq 6 as of November 2026; capabilities may change between releases.