

Security

Last updated: October 2026 · Describes Primentra 1.2026.10.11

Online version: <https://primentra.com/security>

This page answers the questions a security review asks about Primentra. Where we can, each answer says where you can check it. Send questions to info@primentra.com.

AT A GLANCE

Where it runs	On your own Windows server, with your own SQL Server
Our access to your data	None. The product sends no master data to us
Certifications	None. No SOC 2 report and no ISO 27001 certificate
Outside penetration test	None so far
Single sign-on	Not available yet
Security contact	info@primentra.com

1. Certifications and testing

Do you hold a security certification?

No. We have no SOC 2 report and no ISO 27001 certificate. We hold no other security certification.

Has an outside company tested Primentra?

No. No outside company has run a penetration test on Primentra.

How do you test security yourselves?

- Code changes get an AI-assisted code review and security review before we push them. A hook in our development tools refuses a push that holds unreviewed code.
- A secret scan (gitleaks) runs before each commit. It refuses a commit that holds a password or a key.
- The release build stops when one of its checks fails. It upgrades a database from every released version to the new schema. It runs `npm audit` on the shipped packages. It runs the

end-to-end test suite, more than 200 test files, against a separate test database.

- The person who builds a release can skip a check with an explicit setting. The build log then marks that check as skipped. That person can also narrow the end-to-end run to a short critical set, and the log then names that scope.

2. Hosting and data location

Where does Primentra run, and where is our data?

Primentra runs on your own Windows server. Your master data lives in a SQL Server database that you create and manage. We do not host Primentra. The product gives us no access to your server or your database. See [Security & Compliance](#).

What does Primentra send outside our network?

The Primentra server opens two kinds of outbound connection: to your SQL Server, and to your mail server if you set up email. It sends no telemetry and no usage data. It does not call home for the licence. The server checks the licence key itself, against an Ed25519 signature.

One request goes out from the browser. When an administrator uses Primentra, the browser asks the GitHub releases API (`api.github.com`) once a day if a newer version exists. The request carries no Primentra data. To stop it, switch off **Check for new versions** in General Settings.

The browser loads scripts, styles and fonts from your Primentra server only, and the Content Security Policy enforces this. Since version 1.2026.10.11, Primentra does not ask the browser for its location.

Does Kraaitje B.V. ever receive our master data?

No. Nothing in the product sends master data to us. We hold your contact and order details, as any supplier does. The [Privacy Policy](#) describes them.

3. Sign-in and sessions

How does Primentra store passwords?

Primentra hashes each password with scrypt and a random 16-byte salt. It stores the salt and the hash, never the password. It compares hashes in constant time. A user who changes or resets their own password must use at least 8 characters. When an administrator sets a password for a user, Primentra does not check its length. See [Account Security](#).

What stops password guessing?

- After 5 failed sign-ins in a row, Primentra locks the account. The lock ends every open session of that account.
- Only an administrator can unlock a user. **Forgot password?** changes the password but does not remove the lock.
- An administrator account unlocks itself after 30 minutes. Without this, an attacker could lock out every administrator.
- The server accepts 10 failed sign-ins per client address in 15 minutes. After that it refuses sign-ins from that address until the 15 minutes are over.
- The audit log records each failed sign-in. It also records attempts with an email address that has no account.

How do password reset links work?

A reset link is valid for 30 minutes and works once. A new request cancels the earlier link.

Primentra builds the link from the application address an administrator set, never from the address in the request. When the link is used, every session of that account ends. The server accepts 5 reset requests per client address per hour.

A sign-in link in a welcome email is valid for 72 hours and also works once.

How long does a session last?

A session ends after a period without activity. The default is 24 hours. An administrator sets it under **Session Timeout** in General Settings. See [Sessions & Timeouts](#).

The session token is a 256-bit random value. The server keeps sessions in memory, so a restart of the service ends all sessions. The browser keeps the token in local storage and sends it in the `Authorization` header. Primentra sets no session cookie.

When does Primentra end a user's sessions?

Event	Sessions that end
The user changes their own password	All other sessions of that user
A password reset link is used	All sessions of that user
An administrator sets a new password for the user	All sessions of that user

Event	Sessions that end
The account is locked, disabled or deleted	All sessions of that user, and unused sign-in links from welcome emails

While a session is in use, the server checks the account in the database every 5 minutes. If the account is disabled, locked or deleted, the session ends.

4. Single sign-on

Do you support Active Directory or single sign-on?

Not yet. Today each user has a Primentra account with its own password. We are building Active Directory sign-in. The blog post [Active Directory SSO for an on-premises MDM](#) describes the plan.

5. Permissions

How do you control who sees and changes what?

Permissions come from roles only. There are no permissions per user. A role grants Create, Read, Update and Delete per model or per entity. Per column, a role grants None, Read or Write. None hides the column from that role in the grid, in search, in exports and in the REST API. When a user has several roles, the highest level wins.

The server checks the permission on every request. It refuses a request without permission with HTTP 403. See [Roles & Permissions](#).

What can administrators and moderators do?

A role with the Administrator flag gives full access and skips the permission checks. Primentra refuses any change that would leave no active administrator.

Moderator is a level in the permission matrix. It gives full data access and configuration rights, only for the models and entities where you set it. See [Administrator & Moderator](#).

Can we check what a user can see?

Yes. With [Preview As](#), an administrator sees Primentra with the permissions of a user or a role. A preview is read-only. The [Permissions Report](#) shows the result across users and entities.

Where do these permissions not apply?

Primentra enforces them for Primentra users. They do not apply to staging tables, to integration views, or to a person with a SQL login to the database. Keep secret columns out of integration

views, and control who gets a SQL login.

6. Audit log

What does the audit log record?

- Saves, deletes and imports of data. For a save in the data grid, the entry holds the old and the new value of each changed field. For a delete, it holds a full copy of each deleted row.
- Each permission change, with the role, the scope and the old and new setting.
- Each approval step, from submit to approve, force approve, reject or send back.
- Sign-ins and failed sign-ins, lockouts and unlocks, sign-outs and password changes.
- Changes to users, API users and API keys, and switching the REST API on or off.

Each entry holds the user and the time in UTC. Primentra writes a data save and its audit entry in the same database transaction, so a failed save leaves no entry. See [Audit Log](#).

Does it record who read or exported data?

No. The audit log does not record reads, searches or exports.

How long do you keep audit entries?

90 days by default. An administrator sets **Audit Log Retention** in General Settings, from 1 to 9999 days. A SQL Server Agent job deletes older entries. Without that job, Primentra deletes nothing. You can export the log as JSON, CSV or XLSX. See [Data Retention](#).

Can someone change an audit entry?

Primentra has no function to change or delete one entry. Only the retention cleanup deletes entries. Primentra does not sign the entries, so a person with write access to the database can change the table.

7. REST API

How do you store API keys?

Primentra shows a new key once. It stores a SHA-256 hash of the key, and the first 12 characters so you can recognize the key in a list. Each key belongs to an API user, and the roles of that user decide what the key may do. An API user cannot sign in with a password.

How do we revoke a key?

Disable the API user, delete it, or regenerate the key. The old key then stops working. You can also give a key an expiry date.

To stop all API access, switch off **Enable REST API** in General Settings. Every request with a key then gets HTTP 503. If the server cannot read that setting and has no earlier value, it refuses API requests. See [REST API](#).

Is the API rate limited?

Partly. On `/api/v1`, the server accepts 300 requests per minute per key. A key also works on the other `/api` routes, and those have no rate limit for key requests.

8. Encryption

Is traffic between the browser and Primentra encrypted?

That depends on your setup. The Primentra service serves plain HTTP. For HTTPS, put IIS in front of it with a certificate that your users trust. See [Production Deployment \(IIS\)](#).

Primentra does not send an HSTS header, on purpose. Many installations run on plain HTTP inside the company network, and HSTS would lock browsers out of them. If you serve Primentra over HTTPS only, you can add HSTS in IIS.

The service listens on its port (3001 by default) on all network interfaces of the server. Use the Windows firewall to control who can reach that port.

Is the connection to SQL Server encrypted?

Yes. Primentra always encrypts the connection. By default it accepts the certificate of the server without checking it, so a self-signed certificate works. To require a trusted certificate, clear **Trust Server Certificate** in the database settings.

Is data encrypted at rest?

Primentra adds no encryption of its own to master data. Encryption at rest, such as Transparent Data Encryption (TDE), is a setting of your SQL Server.

Primentra stores passwords as script hashes and API keys as SHA-256 hashes. The configuration file `mds-config.json` holds the SQL password, the SMTP password and the licence key in plain text. When the service starts, it removes read access to that file for the Users and Authenticated Users groups.

9. Application security

Which security headers does Primentra send?

Primentra sets its headers with helmet. The Content Security Policy lets scripts, styles and fonts load from the Primentra server only. The policy allows inline styles, because the interface uses

them. The browser may connect to the Primentra server, and to `api.github.com` for the update check. The policy stops other sites from framing Primentra (`frame-ancestors 'none'`) and blocks plugins (`object-src 'none'`).

In the IIS reverse-proxy setup, IIS serves the application page itself. That page then comes without these headers. The API responses keep them.

How do you prevent SQL injection?

The application reads and writes data through stored procedures, and it passes values as parameters. Some procedures must build SQL text, because SQL Server does not accept a table or view name as a parameter. Those procedures escape each name before they use it. The server code also holds a few fixed SQL statements for health checks and setup. None of them includes user input.

What do error messages show?

When the server fails, the browser gets a general message. The full error and the stack trace go to the server log. Before the error handler writes a request to that log, it replaces fields named like passwords, tokens or keys with `[redacted]` .

10. Third-party packages

How do you manage third-party packages?

The release build installs packages from the lockfile with `npm ci` , so a release ships the exact versions in that file. Before a release, `npm audit` runs, and the build stops on a high or critical finding.

One exception is on record. We use the `xlsx` package (SheetJS) for Excel import. It has two known advisories, GHSA-4r6h-8v6p-xvw6 (prototype pollution) and GHSA-5pgg-2g8v-p4x9 (regular expression denial of service). The npm registry has no fixed version.

Each release includes `THIRD-PARTY-NOTICES.txt` , which lists the bundled packages and their licences.

11. Backups and upgrades

Who makes backups?

You do. Your data lives in your SQL Server, so your SQL Server backups protect it. Primentra makes no backups of its own.

What happens during an upgrade?

The installer replaces the application files. Then an administrator starts the database upgrade in the application. The installer makes no backup, so make a full database backup first. An older version does not open a database that a newer version upgraded. To go back, you restore that backup. See [Upgrading](#).

12. Deleting data

What happens when we delete a user?

Primentra marks the user as deleted and disabled. It removes the role memberships, favorites, hidden entities and personal settings of that user. It ends the sessions and unused sign-in links of that user.

The user record stays in the database, with the email address, the display name and the password hash. Audit entries stay too, and they keep the ID of the user. You cannot delete a system user or the last active administrator.

What happens when we delete rows?

The rows leave the entity at once. The audit log keeps a full copy of each deleted row until the audit retention period ends.

13. Report a vulnerability

Send the report to info@primentra.com. Please include:

- The steps to reproduce the problem.
- The Primentra version. The status bar of the application shows it.
- The impact: what an attacker can read, change or stop.

We confirm that we received your report within 5 working days. Please do not make the problem public before we have fixed it.

We do not take legal action against security research done in good faith. We have no bug bounty and pay no rewards.

Our [security.txt](#) file gives the same contact.

Primentra is a trade name of **Kraaitje B.V.**, a private limited company registered in the Netherlands (KvK 94886806). Registered address: Noordelijke Dwarsweg 90, 2761 GD Zevenhuizen, Netherlands.