CERTYX

AUTONOMOUS CERTIFICATE LIFECYCLE MANAGEMENT

Getting started

Ten steps from the first sign-in to your SIEM

LANGUAGE	REVISION	DATE
English	8550060f	1 November 2026

Contents

1 Secure your account 3
2 Add your team 4
3 Decide who gets warned 5
4 Check the TLS policy 6
5 Bring in your certificates 7
6 Connect an agent 8
7 Act on what needs attention 9
8 Plan renewals 10
9 Send events to your SIEM 11
10 Take CERTYX with you 12

A suggested order for the first days with CERTYX after your organization receives access: secure your account, add the team, decide who is warned, check the policy, bring in certificates, connect agents, act on alerts, plan renewals, send events to your SIEM and authorize phones.

> Screenshots and video use sample data.

1 Secure your account

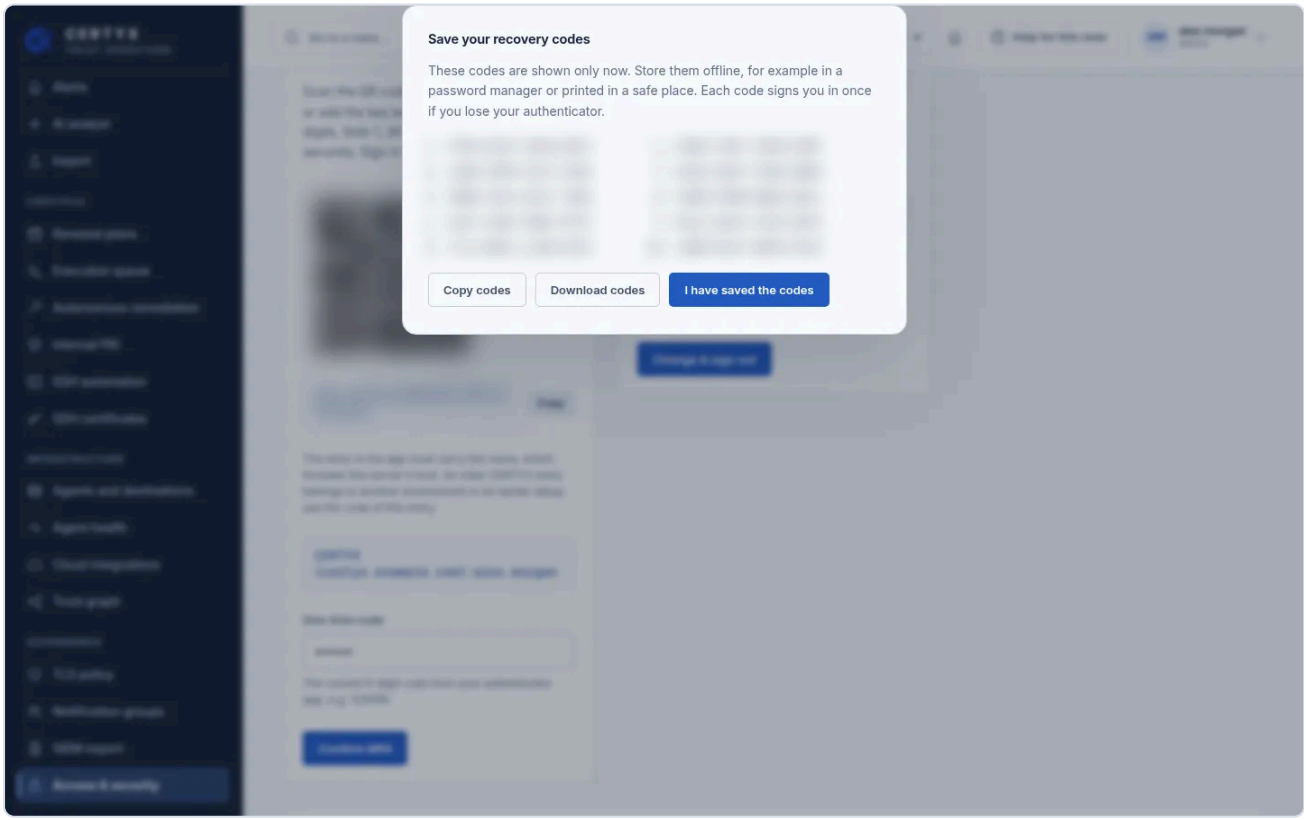
Turn on MFA and keep the recovery codes

WHY

Your account controls your organization's certificates and approvals. A second factor stops anyone who learns your password.

HOW

1. Open Access & security. If you sign in with company sign-in (SSO), your identity provider manages MFA and this step counts as done.
2. Select Enable MFA and add the secret to your authenticator app.
3. Enter the six-digit code from the app and select Confirm MFA.
4. Copy or download the ten recovery codes, keep them offline and select I have saved the codes.
5. Sign in again with your password and MFA code.



2 Add your team

Users with the right roles

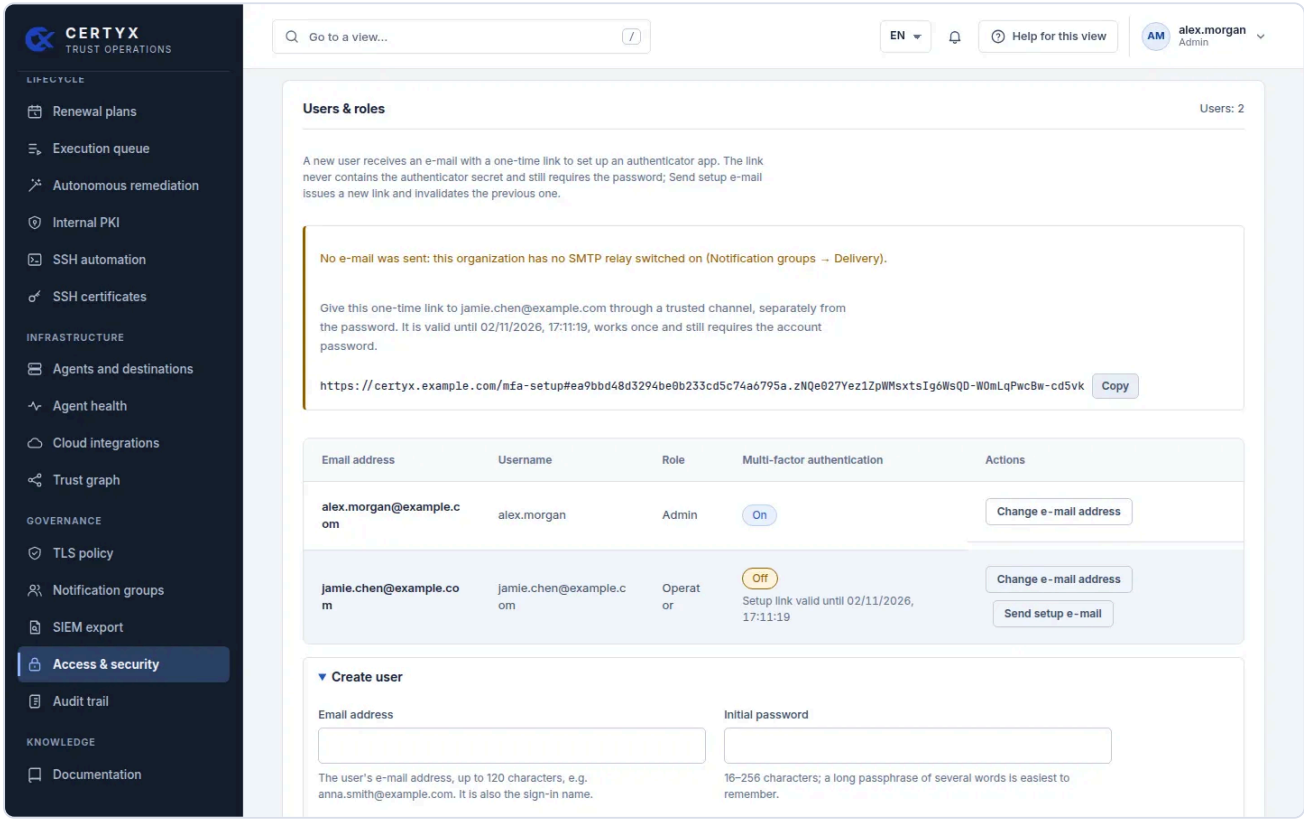
WHY

Each person works with their own account, so every change and approval is attributed to someone.

HOW

1. In Access & security, go to Users & roles.
2. Open Create user and enter the colleague's e-mail address, an initial password of at least 16 characters and a role: Auditor reads, Operator manages inventory and plans, Admin approves.
3. Select Create user and hand over the initial password personally.
4. Optional: in Company sign-in (SSO) connect Microsoft Entra ID, Okta, another OpenID Connect provider or SAML 2.0 so colleagues sign in with their company account.

> Administrators do this step. If you are not an administrator, ask yours.



3 Decide who gets warned

Notification groups for expiry e-mails

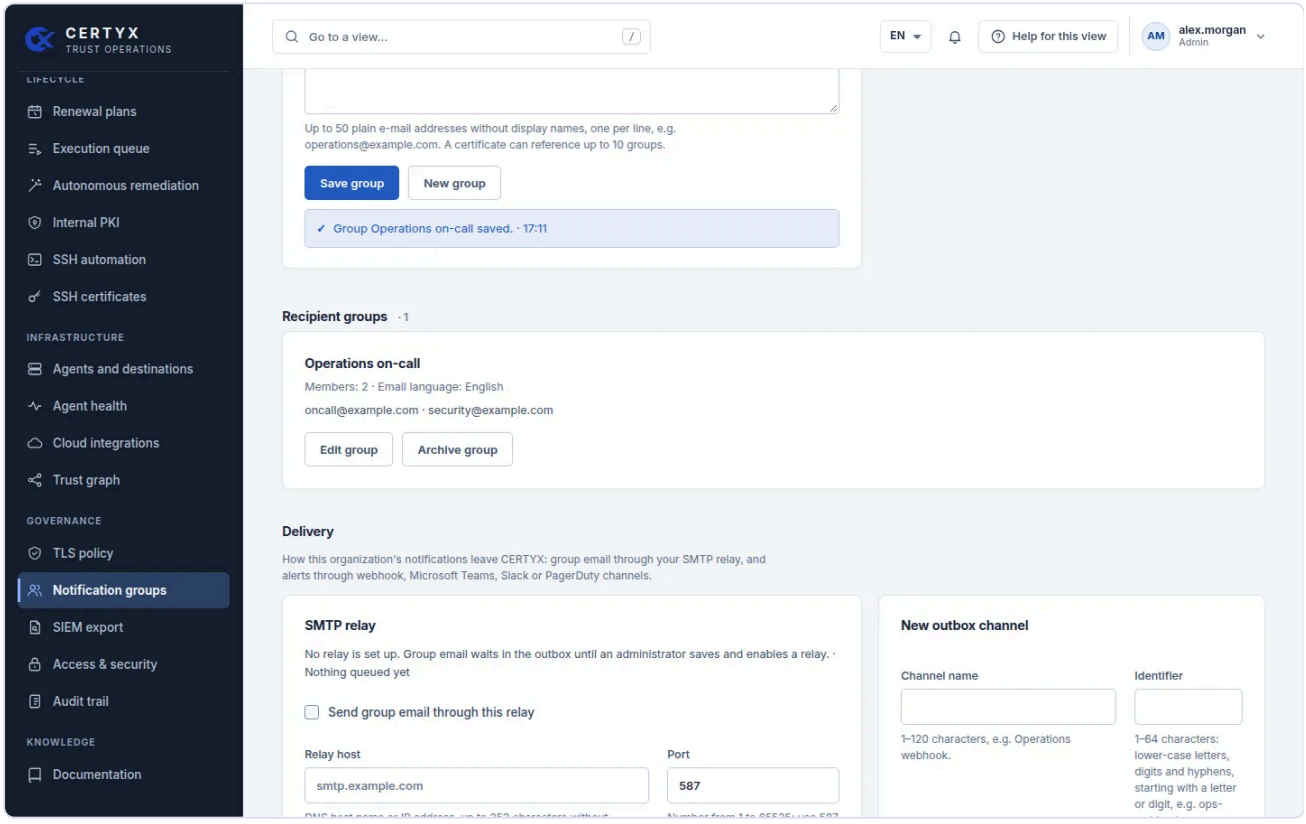
WHY

Expiry warnings reach the people who can act, in their language, instead of one shared inbox.

HOW

1. Open Notification groups. The New recipient group form is at the top; New group clears it.
2. Enter a Group name, for example Operations on-call, and up to 50 e-mail addresses in Group members, one per line.
3. Choose the Email language and select Save group.
4. Assign the group to certificates under Responsibility groups in their details. E-mails leave CERTYX once an administrator saves and enables an SMTP relay under Delivery.

> Administrators do this step. If you are not an administrator, ask yours.



4 Check the TLS policy

Renewal window and security rules

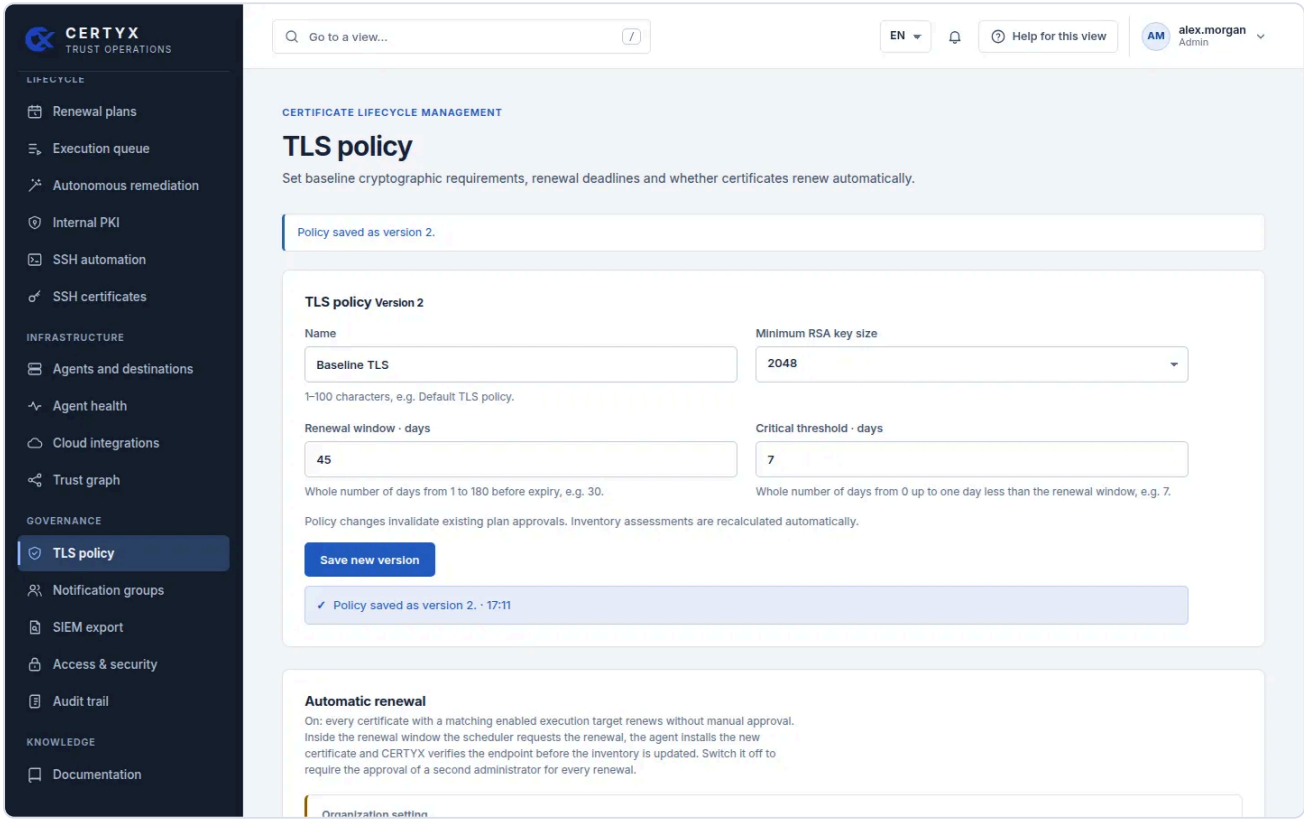
WHY

The policy decides when a certificate needs attention and which keys and signatures are acceptable.

HOW

1. Open TLS policy.
2. Check the renewal window and the critical threshold in days.
3. Choose the minimum RSA key size. Fixed rules always apply as well: ECDSA keys of at least P-256, no SHA-1 or MD5 signatures, and validity checks.
4. Select Save new version; every certificate is assessed against it, and approvals of existing renewal plans become invalid.

> Administrators do this step. If you are not an administrator, ask yours.



5 Bring in your certificates

Import a certificate or add a domain

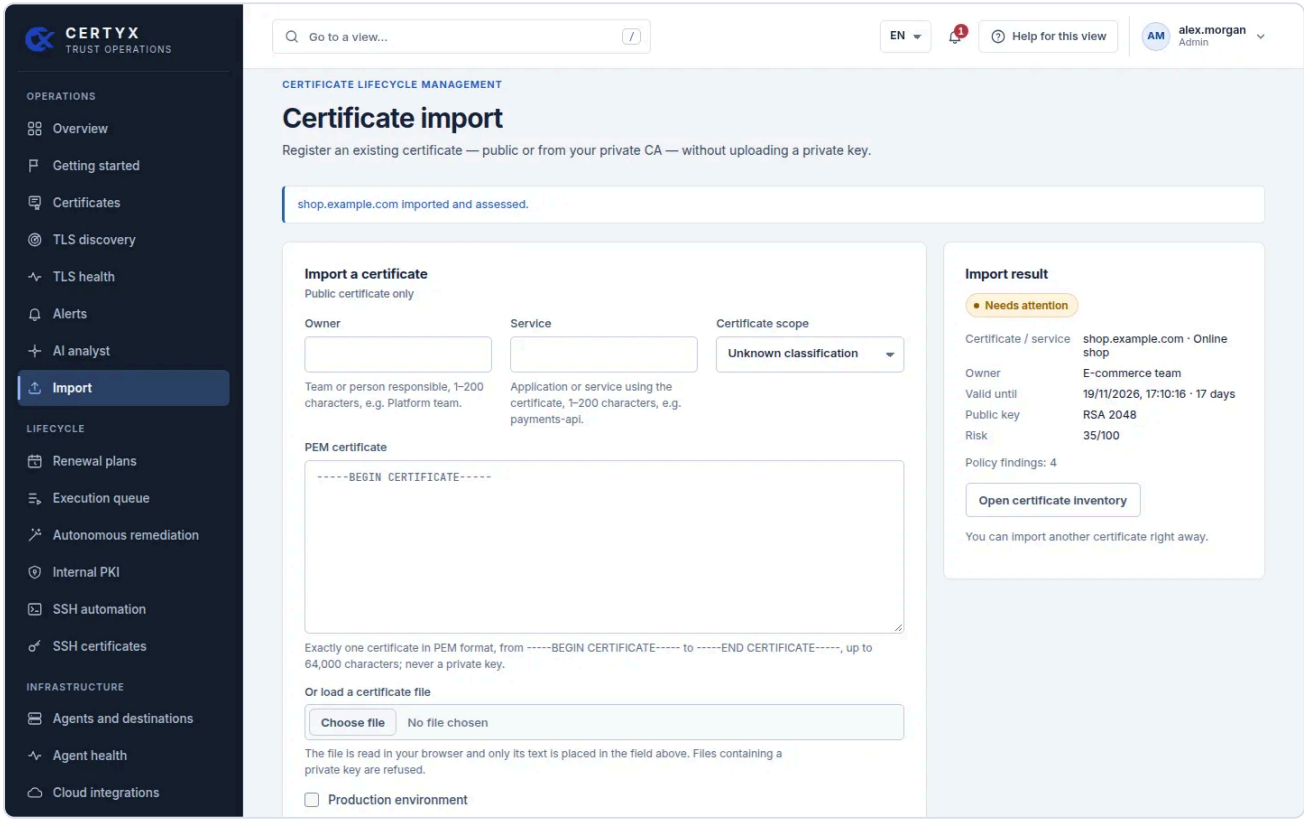
WHY

You can only manage what you can see. Start with the services that matter most.

HOW

1. Open Import, paste a public certificate in PEM format or load a certificate file, and enter its owner and service.
2. Select Import & assess: the certificate is stored and checked against the policy.
3. To read a certificate from a live server, select Add domain in Certificates; it opens TLS discovery.
4. For whole networks, enroll an agent (next step) or connect cloud integrations.

> Operators and administrators do this step. Your role can read the result; ask an operator or administrator to change data.



6 Connect an agent

Scan your networks and deploy renewals

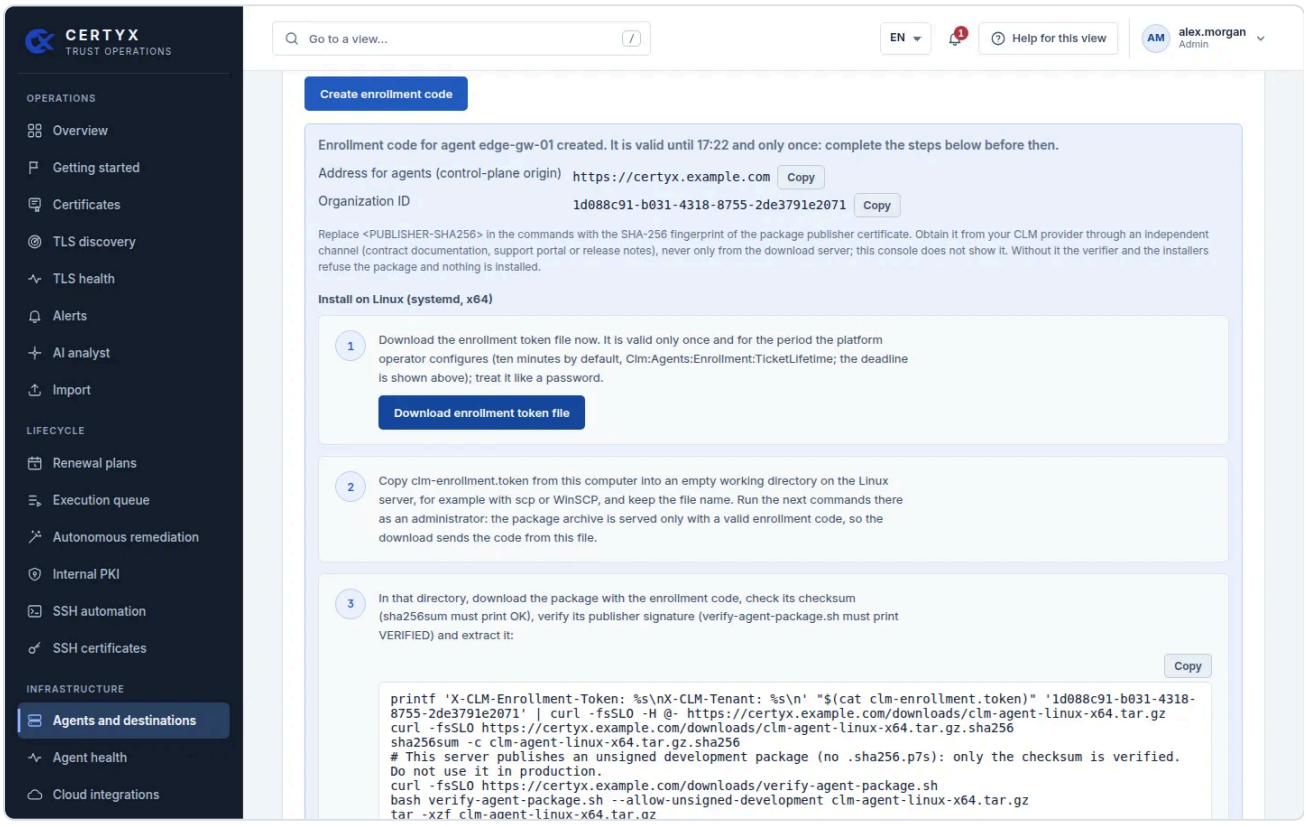
WHY

An agent inside your network finds certificates on every approved host and port, and later installs renewed ones.

HOW

1. Open Agents and destinations.
2. Enter an agent ID and select Create enrollment code.
3. Install the agent on a Linux or Windows server with the commands shown after the code is created; the Agent installation guide has the details.
4. Under Automatic network discovery, load the agent's network profile, set Authorized CIDRs and select Save network profile; Agent health shows whether the agent reports in.

> Administrators do this step. If you are not an administrator, ask yours.



7 Act on what needs attention

Overview, alerts and owners

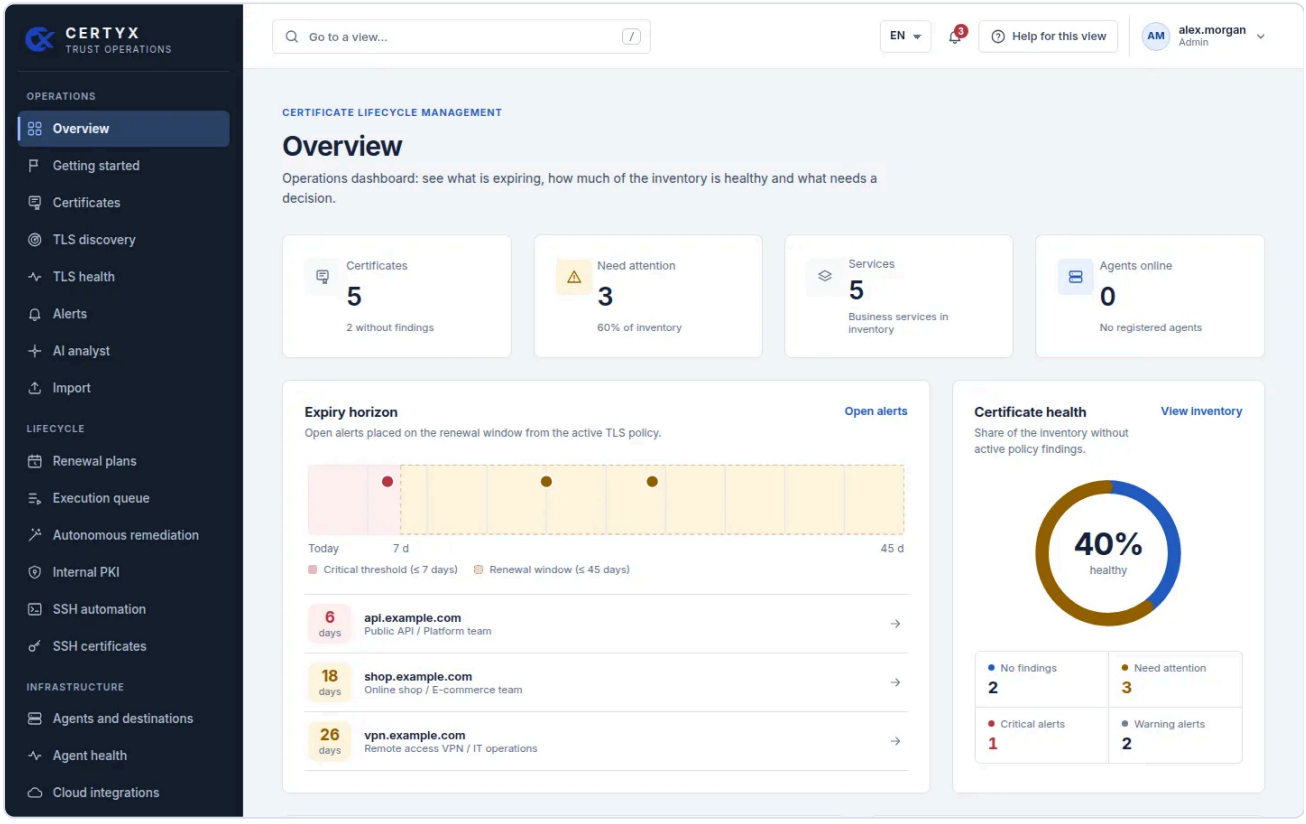
WHY

Certificates with an owner get handled; the overview tells you where to start.

HOW

1. Open Overview: expiring certificates, open alerts and agent state at a glance.
2. Open Alerts and start with critical ones.
3. Open a certificate in Certificates, set its owner and service and select Save ownership, so every alert has someone responsible.
4. Select Acknowledge on alerts you have handled.

> Operators and administrators do this step. Your role can read the result; ask an operator or administrator to change data.



8 Plan renewals

Approved by a second person

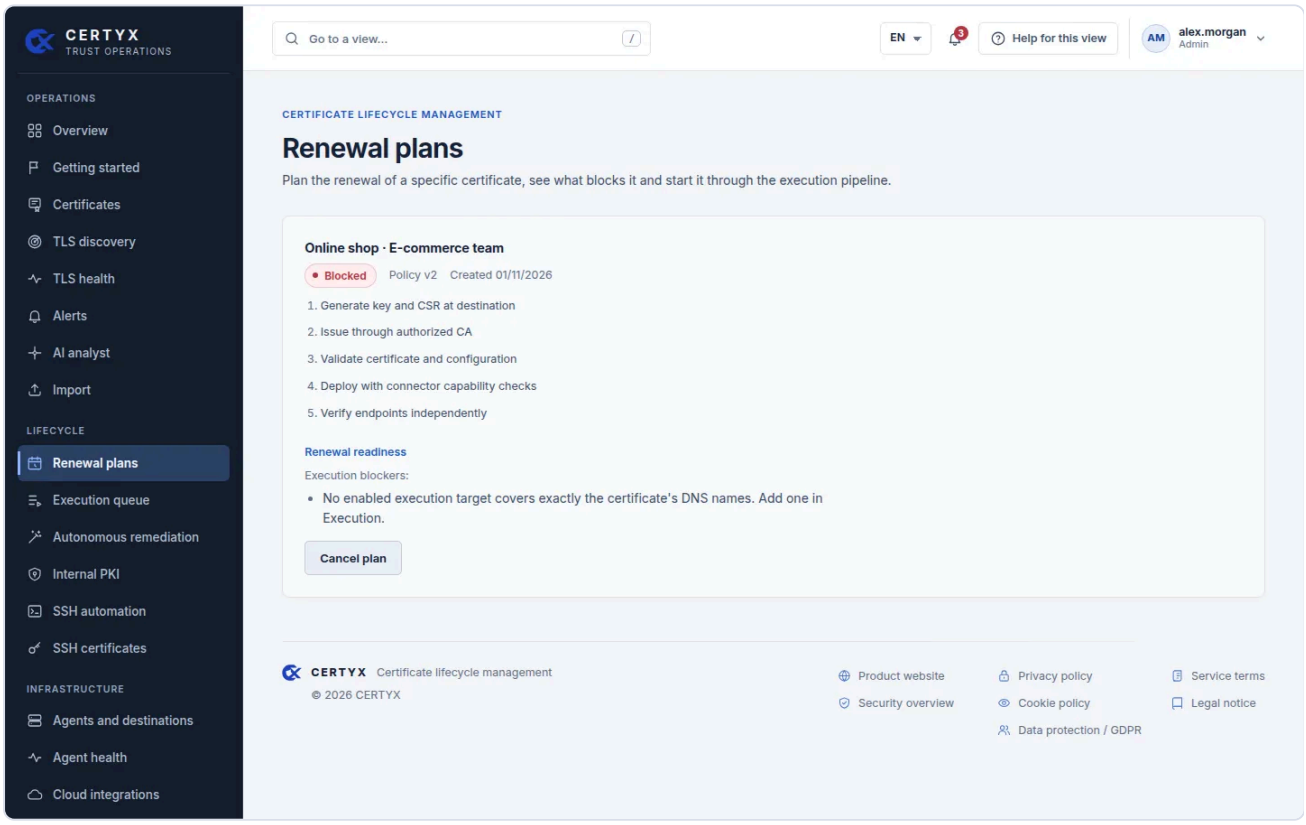
WHY

Renewals are planned ahead and approved by a second person before anything changes on your servers.

HOW

1. In Certificates, open a certificate that expires soon and select Plan renewal.
2. Open Renewal plans: the plan shows its stages and anything that blocks it, such as a missing deployment target or agent contact.
3. An administrator selects Approve plan, which requests an execution job; a second administrator selects Approve job as second person.
4. With a connected agent, a deployment target and a configured certificate authority, the Execution queue renews, deploys and verifies the certificate.

> Operators and administrators do this step. Your role can read the result; ask an operator or administrator to change data.



9 Send events to your SIEM

Sized for your licence

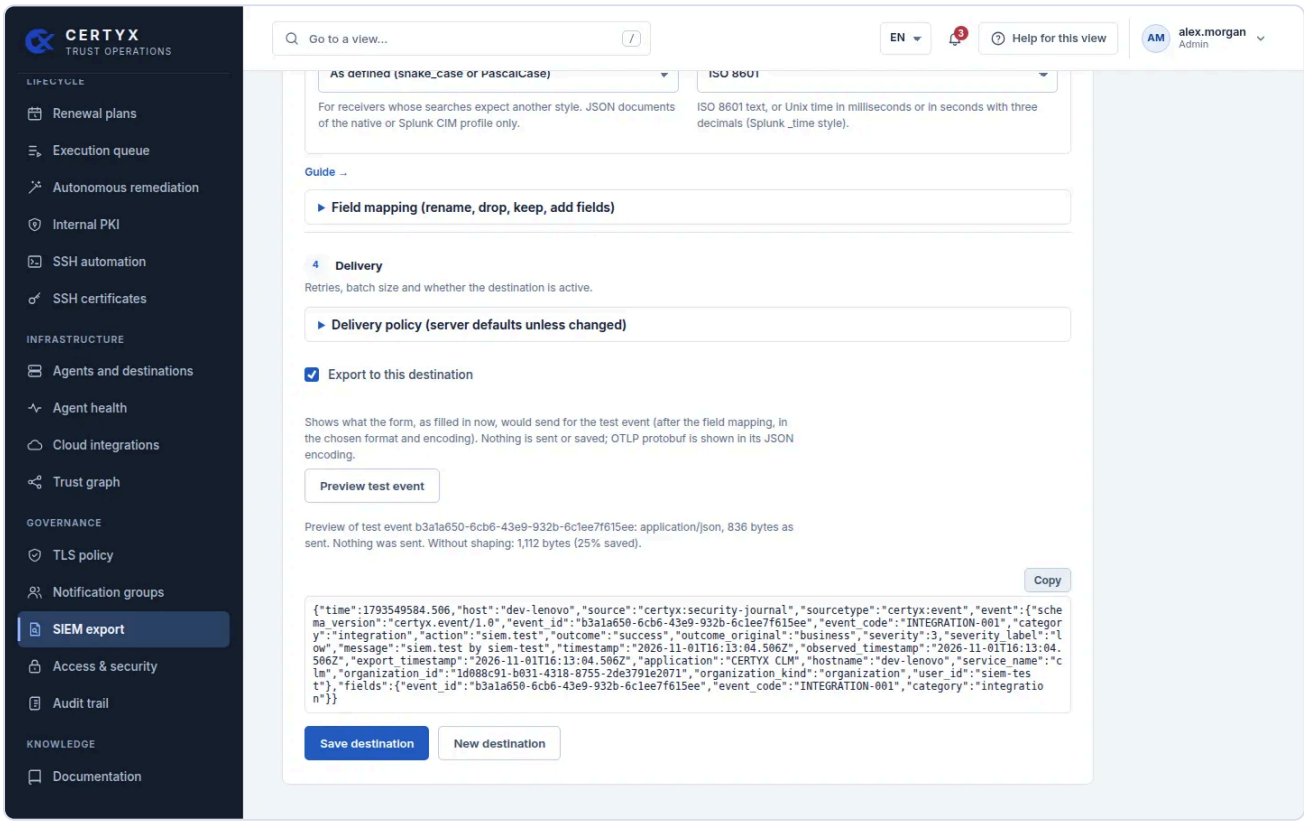
WHY

Your security team sees every sign-in, change and failure in Splunk, QRadar, Sentinel, Elastic or any other SIEM, and you decide how large each event is, so the SIEM licence is not wasted.

HOW

1. Open SIEM export and enter a name and an identifier for the destination.
2. Choose the transport of your SIEM, for example Splunk HTTP Event Collector, and enter its address and token.
3. Under Shape and size choose Balanced or Economical; Preview test event shows how many bytes each event saves.
4. Save, then Check connection and Send test event.

> Administrators do this step. If you are not an administrator, ask yours.



10 Take CERTYX with you

Authorize phones for your team

WHY

Alerts and approvals on the phone, only on devices your administrator authorized.

HOW

1. In Access & security, go to Mobile devices.
2. Choose the user and select Generate activation code; your session must be signed in with MFA.
3. The user installs CERTYX from your organization's app store, scans the QR code or enters the code, and signs in with their account and MFA or with company sign-in.
4. Select Revoke access for a lost device; the app on it stops working immediately.

> Administrators do this step. If you are not an administrator, ask yours.

