CERTYX



AUTONOMOUS CERTIFICATE LIFECYCLE MANAGEMENT

Erste Schritte

Zehn Schritte von der ersten Anmeldung bis zu Ihrem SIEM

SPRACHE
Deutsch

REVISION
8550060f

DATUM
1. November 2026

Inhalt

1 Konto absichern 3
2 Team hinzufügen 4
3 Festlegen, wer gewarnt wird 5
4 TLS-Richtlinie prüfen 6
5 Zertifikate einbinden 7
6 Agenten verbinden 8
7 Auf Wichtiges reagieren 9
8 Erneuerungen planen 10
9 Ereignisse an Ihr SIEM senden 11
10 CERTYX mitnehmen 12

Eine empfohlene Reihenfolge für die ersten Tage mit CERTYX, nachdem Ihre Organisation Zugang erhalten hat: Konto absichern, Team hinzufügen, festlegen, wer gewarnt wird, Richtlinie prüfen, Zertifikate einbinden, Agenten verbinden, auf Warnungen reagieren, Erneuerungen planen, Ereignisse an Ihr SIEM senden und Smartphones autorisieren.

> Bildschirmfotos und Video zeigen Beispieldaten.

1 Konto absichern

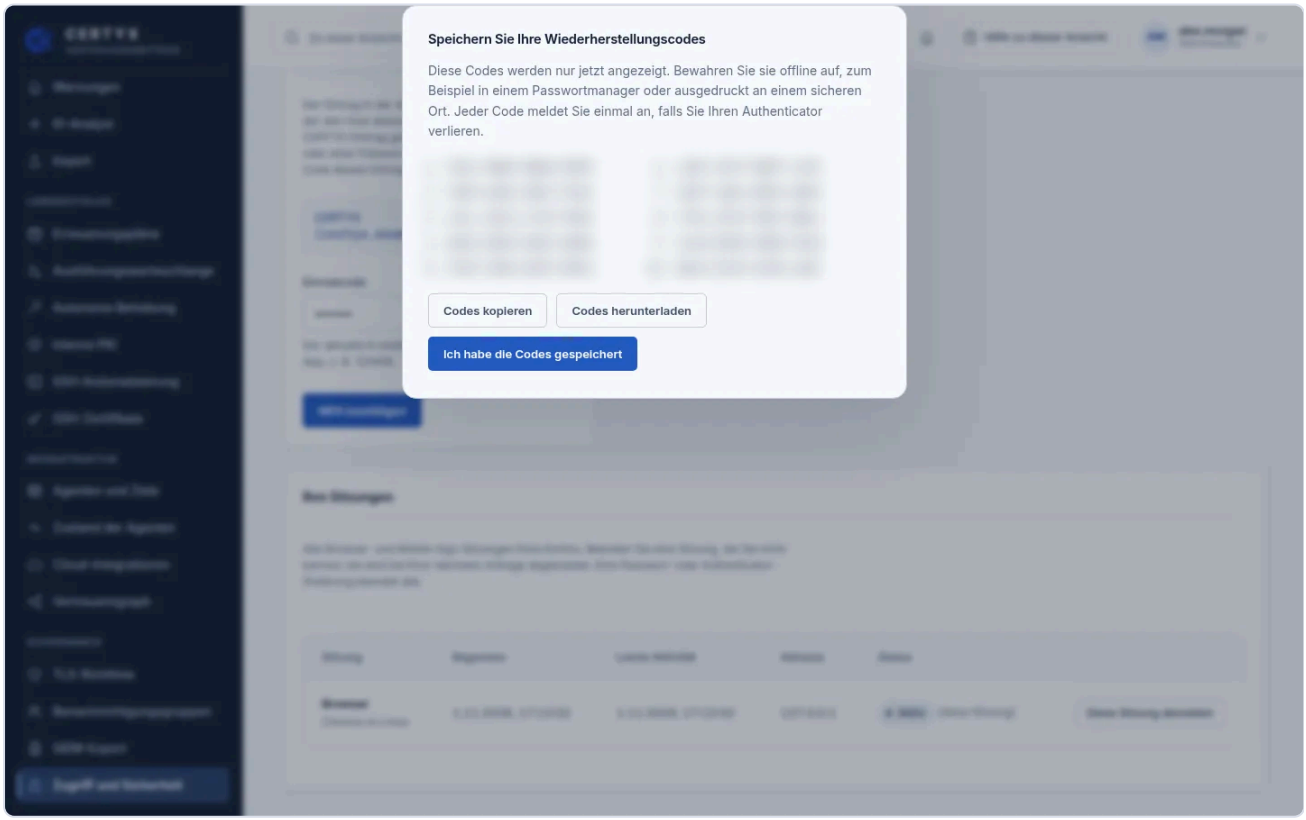
MFA aktivieren und Wiederherstellungscodes aufbewahren

WARUM

Ihr Konto steuert die Zertifikate und Freigaben Ihrer Organisation. Ein zweiter Faktor stoppt jeden, der Ihr Passwort kennt.

SO GEHT'S

1. Öffnen Sie Zugriff und Sicherheit. Wenn Sie sich per Unternehmensanmeldung (SSO) anmelden, verwaltet Ihr Identitätsanbieter die MFA und dieser Schritt gilt als erledigt.
2. Wählen Sie „MFA aktivieren" und fügen Sie das Geheimnis Ihrer Authenticator-App hinzu.
3. Geben Sie den sechsstelligen Code aus der App ein und wählen Sie „MFA bestätigen".
4. Kopieren oder laden Sie die zehn Wiederherstellungscodes herunter, bewahren Sie sie offline auf und wählen Sie „Ich habe die Codes gespeichert".
5. Melden Sie sich erneut mit Passwort und MFA-Code an.



2 Team hinzufügen

Benutzer mit passenden Rollen

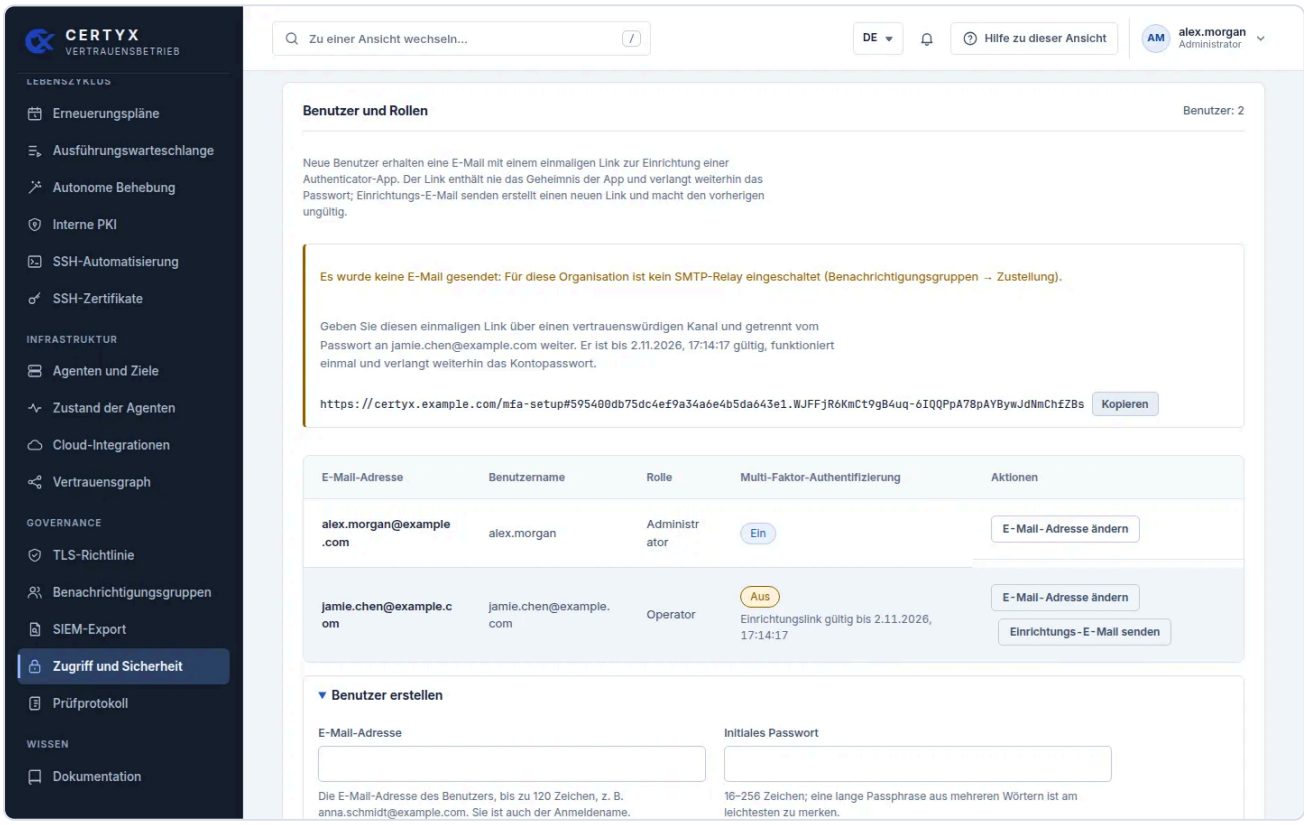
WARUM

Jede Person arbeitet mit einem eigenen Konto, damit jede Änderung und Freigabe einer Person zugeordnet ist.

SO GEHT'S

1. Gehen Sie in Zugriff und Sicherheit zu Benutzer und Rollen.
2. Öffnen Sie „Benutzer erstellen“ und geben Sie die E-Mail-Adresse, ein initiales Passwort mit mindestens 16 Zeichen und eine Rolle ein: Auditor liest, Operator verwaltet Inventar und Pläne, Administrator gibt frei.
3. Wählen Sie „Benutzer erstellen“ und übergeben Sie das initiale Passwort persönlich.
4. Optional: Verbinden Sie unter Unternehmensanmeldung (SSO) Microsoft Entra ID, Okta, einen anderen OpenID-Connect-Anbieter oder SAML 2.0, damit sich Kollegen mit ihrem Firmenkonto anmelden.

> Diesen Schritt erledigen Administratoren. Wenn Sie kein Administrator sind, wenden Sie sich an Ihren.



3 Festlegen, wer gewarnt wird

Empfängergruppen für Ablauf-E-Mails

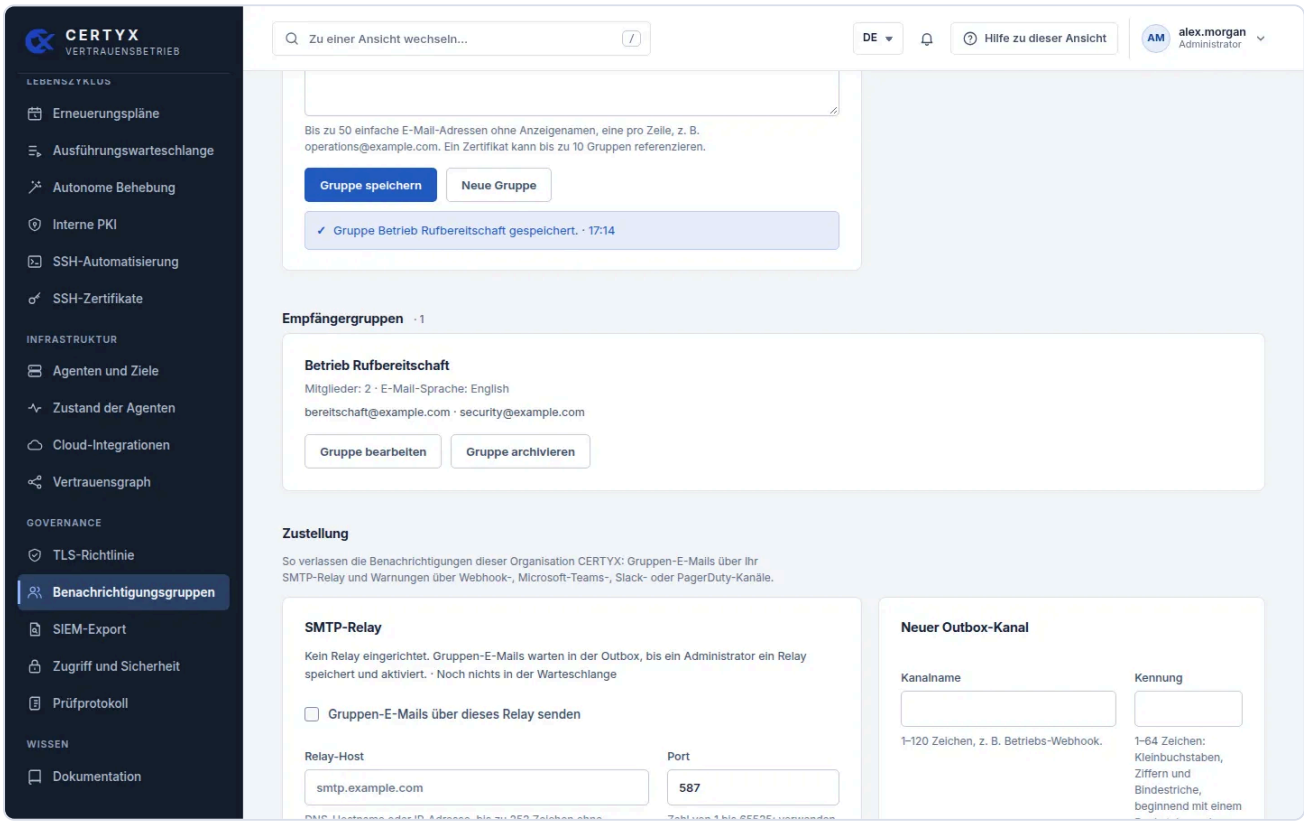
WARUM

Ablaufwarnungen erreichen die Personen, die handeln können, in ihrer Sprache – statt eines gemeinsamen Postfachs.

SO GEHT'S

1. Öffnen Sie Benachrichtigungsgruppen. Oben steht das Formular „Neue Empfängergruppe"; „Neue Gruppe" leert es.
2. Geben Sie einen Gruppennamen ein, zum Beispiel Betrieb Rufbereitschaft, und unter Gruppenmitglieder bis zu 50 E-Mail-Adressen, eine pro Zeile.
3. Wählen Sie die E-Mail-Sprache und dann „Gruppe speichern".
4. Weisen Sie die Gruppe Zertifikaten in deren Details unter Verantwortlichkeitsgruppen zu. E-Mails werden versendet, sobald ein Administrator unter Zustellung ein SMTP-Relay speichert und aktiviert.

> Diesen Schritt erledigen Administratoren. Wenn Sie kein Administrator sind, wenden Sie sich an Ihren.



4 TLS-Richtlinie prüfen

Erneuerungsfenster und Sicherheitsregeln

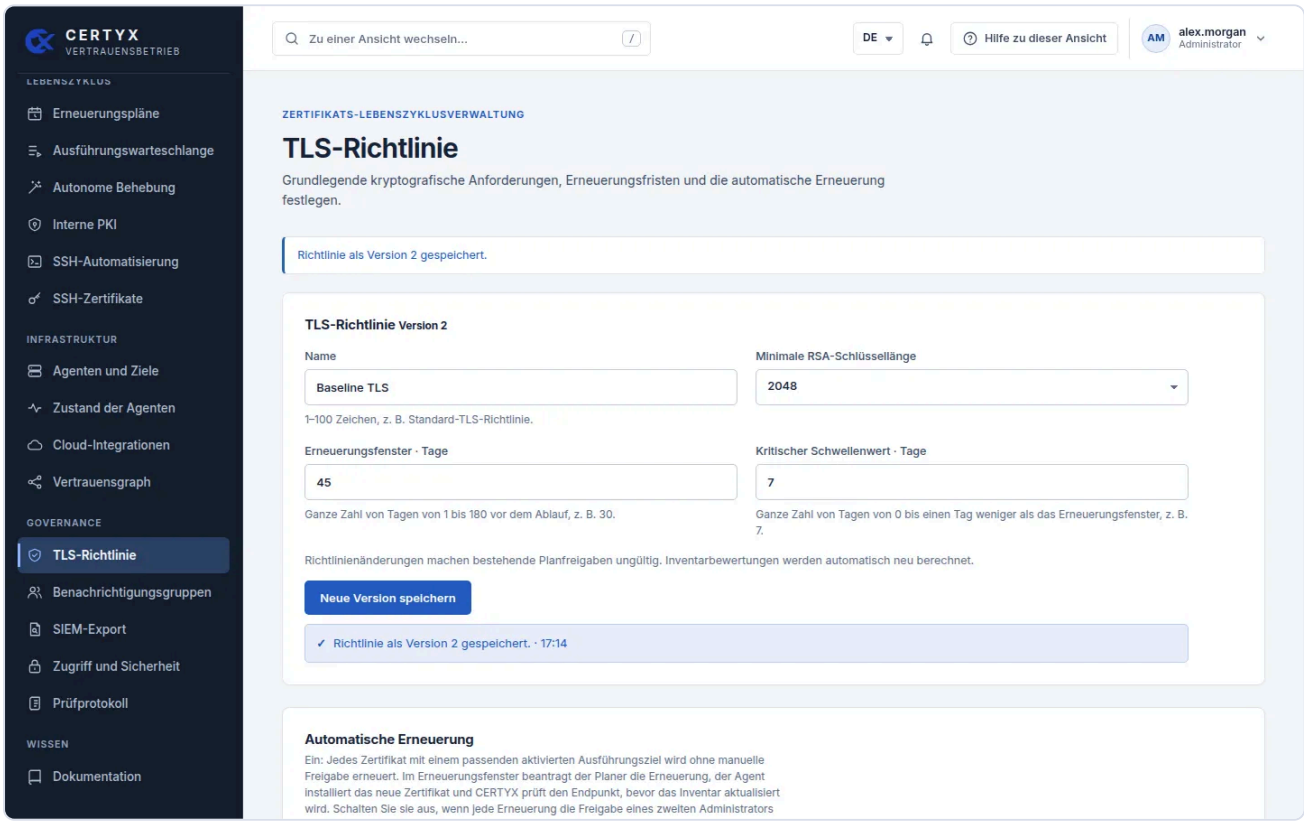
WARUM

Die Richtlinie legt fest, wann ein Zertifikat Aufmerksamkeit braucht und welche Schlüssel und Signaturen zulässig sind.

SO GEHT'S

1. Öffnen Sie TLS-Richtlinie.
2. Prüfen Sie das Erneuerungsfenster und die kritische Schwelle in Tagen.
3. Wählen Sie die minimale RSA-Schlüssellänge. Feste Regeln gelten immer zusätzlich: ECDSA-Schlüssel ab P-256, keine SHA-1- oder MD5-Signaturen und Gültigkeitsprüfungen.
4. Wählen Sie „Neue Version speichern"; jedes Zertifikat wird danach bewertet, und Freigaben bestehender Erneuerungspläne werden ungültig.

> Diesen Schritt erledigen Administratoren. Wenn Sie kein Administrator sind, wenden Sie sich an Ihren.



5 Zertifikate einbinden

Zertifikat importieren oder Domain hinzufügen

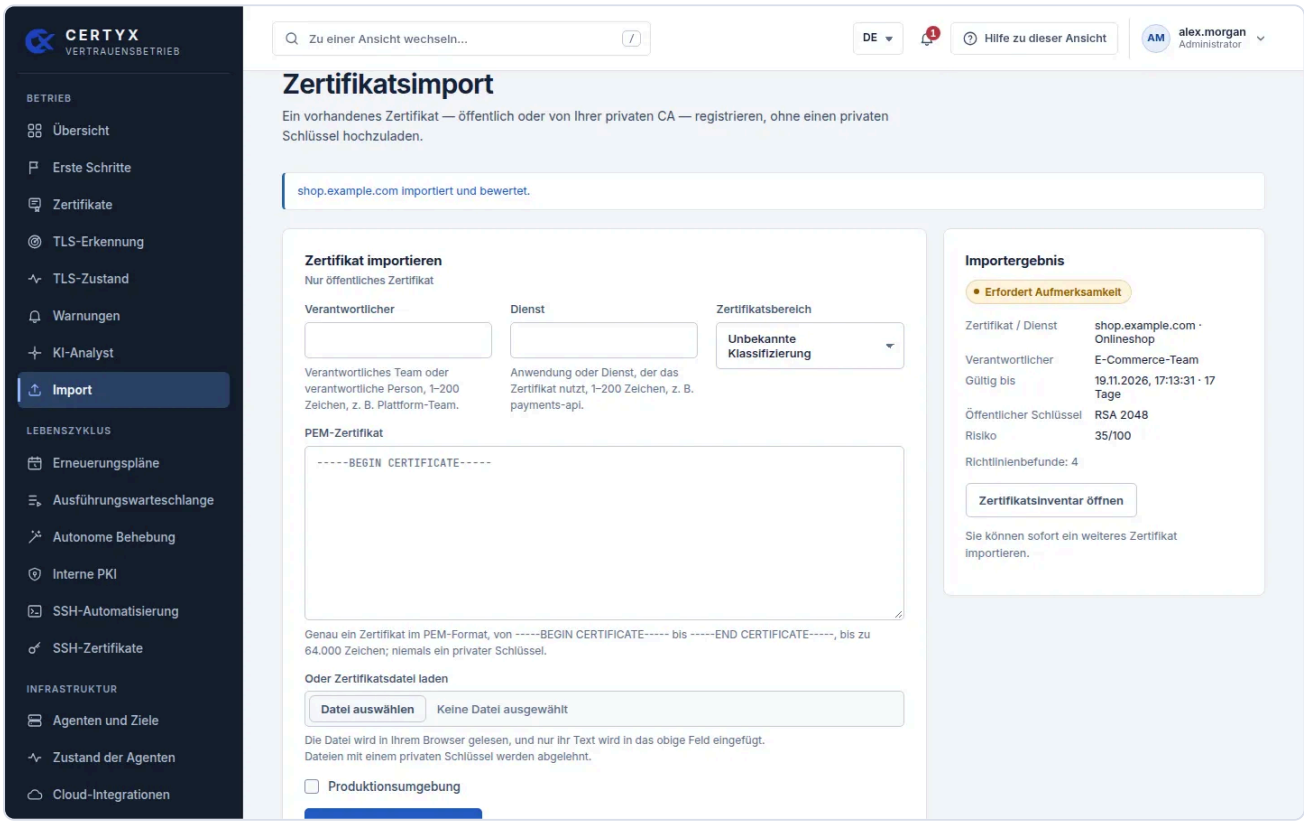
WARUM

Verwalten lässt sich nur, was sichtbar ist. Beginnen Sie mit den wichtigsten Diensten.

SO GEHT'S

1. Öffnen Sie Import, fügen Sie ein öffentliches Zertifikat im PEM-Format ein oder laden Sie eine Zertifikatsdatei, und tragen Sie Verantwortlichen und Dienst ein.
2. Wählen Sie „Importieren und bewerten“: Das Zertifikat wird gespeichert und anhand der Richtlinie geprüft.
3. Um ein Zertifikat von einem laufenden Server zu lesen, wählen Sie „Domain hinzufügen“ unter Zertifikate; das öffnet die TLS-Erkennung.
4. Für ganze Netze registrieren Sie einen Agenten (nächster Schritt) oder verbinden Cloud-Integrationen.

> Diesen Schritt erledigen Operatoren und Administratoren. Ihre Rolle kann das Ergebnis lesen; bitten Sie für Änderungen einen Operator oder Administrator.



6 Agenten verbinden

Netze scannen und Erneuerungen bereitstellen

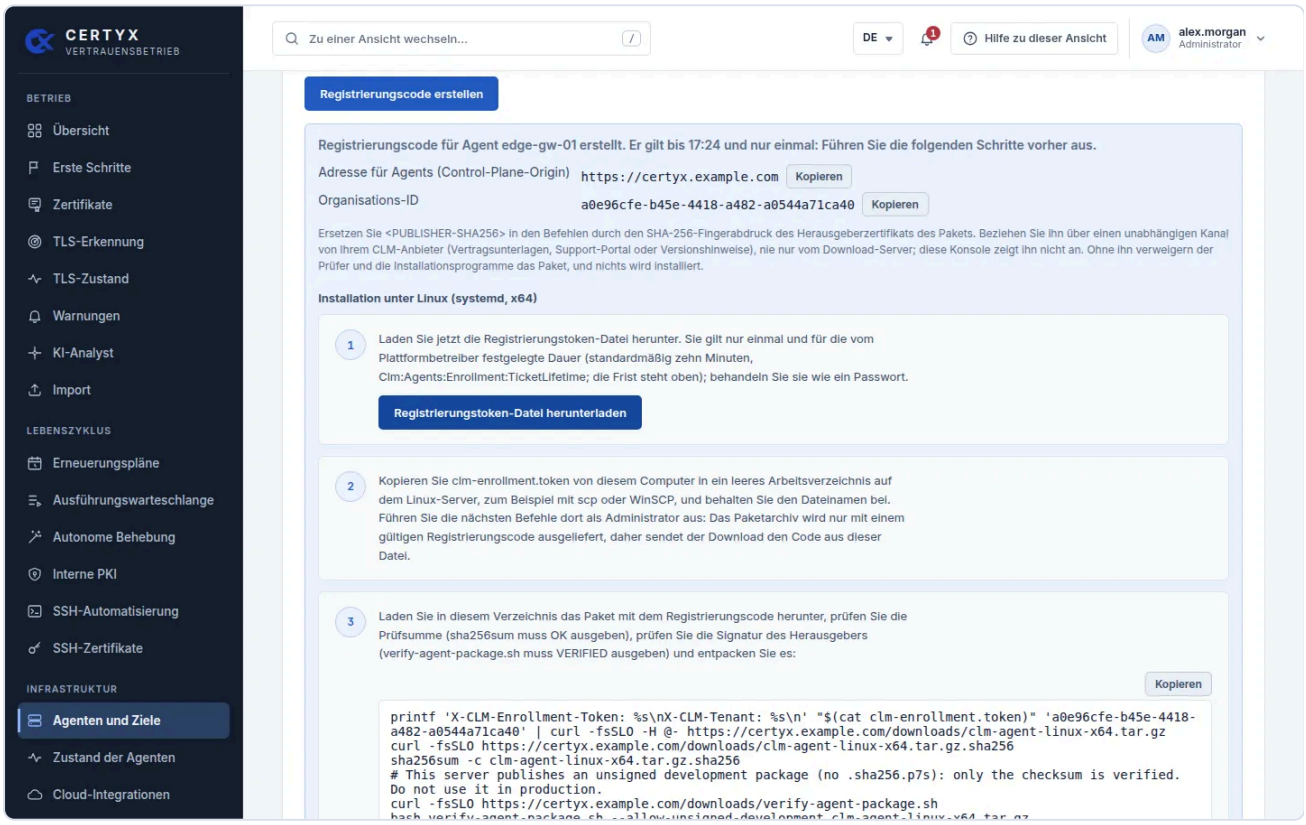
WARUM

Ein Agent in Ihrem Netz findet Zertifikate auf jedem freigegebenen Host und Port und installiert später erneuerte.

SO GEHT'S

1. Öffnen Sie Agenten und Ziele.
2. Geben Sie eine Agenten-ID ein und wählen Sie „Registrierungscode erstellen".
3. Installieren Sie den Agenten auf einem Linux- oder Windows-Server mit den Befehlen, die nach dem Erstellen des Codes angezeigt werden; Details enthält die Installationsanleitung für den Agenten.
4. Laden Sie unter Automatische Netzwerkerkennung das Netzwerkprofil des Agenten, legen Sie die autorisierten CIDRs fest und wählen Sie „Netzwerkprofil speichern"; „Zustand der Agenten" zeigt, ob der Agent sich meldet.

> Diesen Schritt erledigen Administratoren. Wenn Sie kein Administrator sind, wenden Sie sich an Ihren.



7 Auf Wichtiges reagieren

Übersicht, Warnungen und Verantwortliche

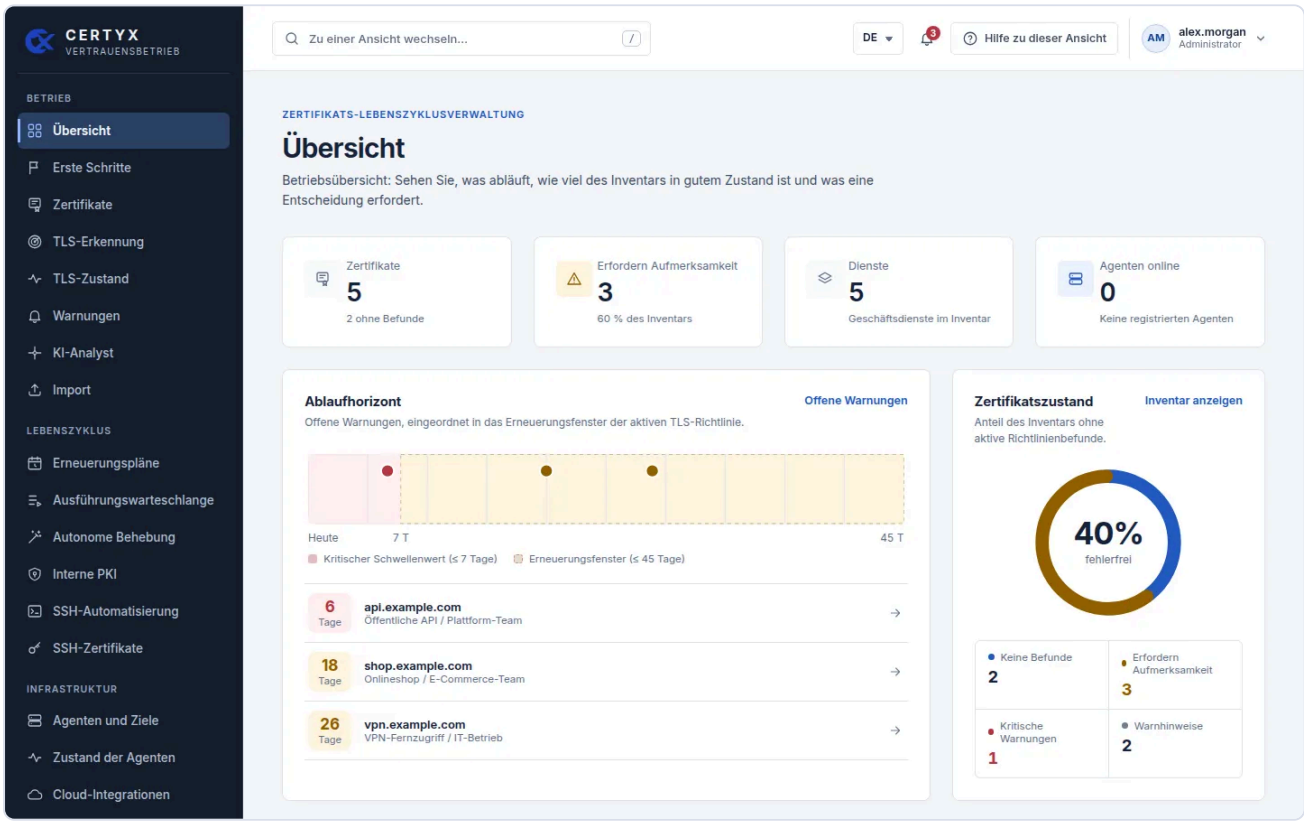
WARUM

Zertifikate mit Verantwortlichem werden bearbeitet; die Übersicht zeigt, wo Sie beginnen.

SO GEHT'S

1. Öffnen Sie die Übersicht: ablaufende Zertifikate, offene Warnungen und Agentenzustand auf einen Blick.
2. Öffnen Sie Warnungen und beginnen Sie mit den kritischen.
3. Öffnen Sie ein Zertifikat unter Zertifikate, legen Sie Verantwortlichen und Dienst fest und wählen Sie „Verantwortlichkeit speichern", damit jede Warnung einen Zuständigen hat.
4. Wählen Sie bei erledigten Warnungen „Bestätigen".

> Diesen Schritt erledigen Operatoren und Administratoren. Ihre Rolle kann das Ergebnis lesen; bitten Sie für Änderungen einen Operator oder Administrator.



8 Erneuerungen planen

Von einer zweiten Person freigegeben

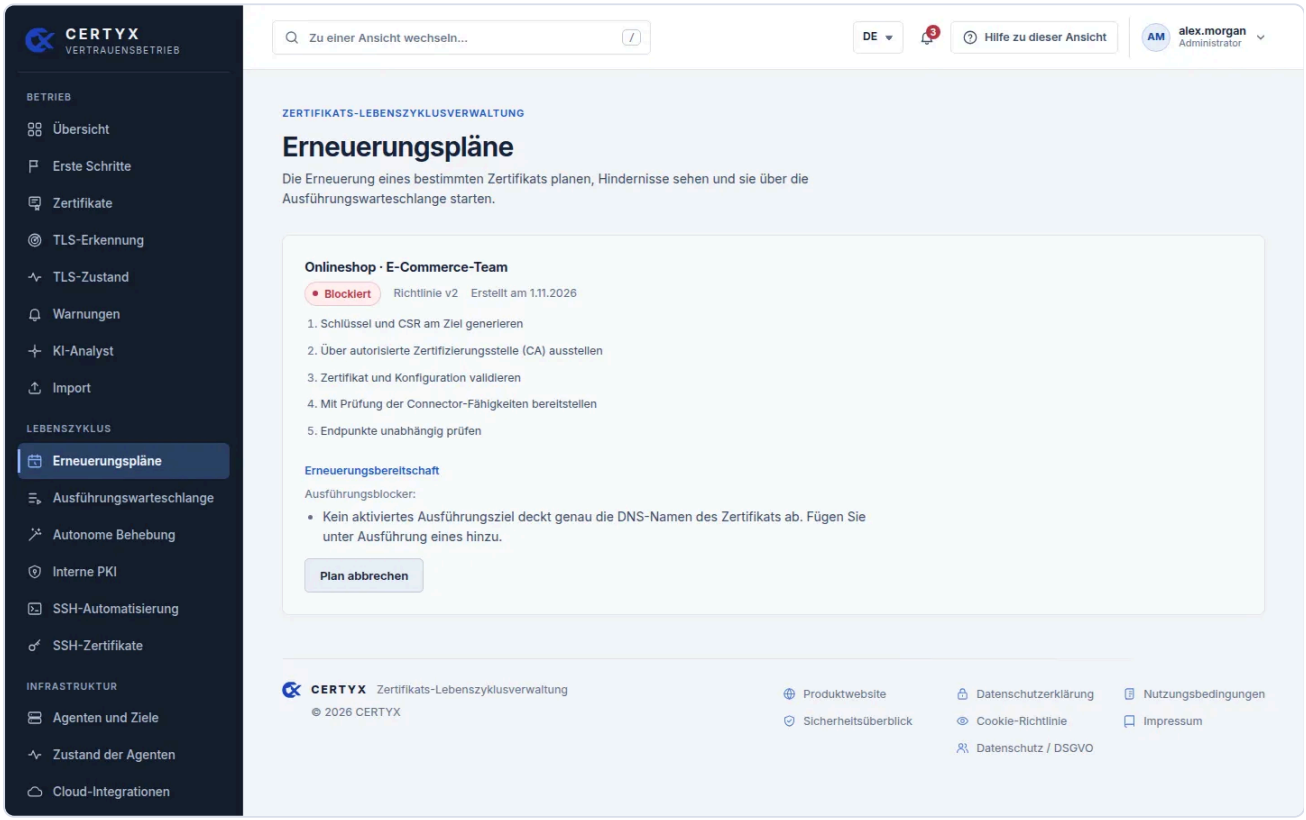
WARUM

Erneuerungen werden vorausgeplant und von einer zweiten Person freigegeben, bevor sich auf Ihren Servern etwas ändert.

SO GEHT'S

1. Öffnen Sie unter Zertifikate ein bald ablaufendes Zertifikat und wählen Sie „Erneuerung planen".
2. Öffnen Sie Erneuerungspläne: Der Plan zeigt seine Phasen und alles, was ihn blockiert, etwa ein fehlendes Bereitstellungsziel oder fehlenden Agentenkontakt.
3. Ein Administrator wählt „Plan freigeben", wodurch ein Ausführungsauftrag angefordert wird; ein zweiter Administrator wählt „Auftrag als zweite Person genehmigen".
4. Mit einem verbundenen Agenten, einem Bereitstellungsziel und einer konfigurierten Zertifizierungsstelle erneuert, verteilt und prüft die Ausführungswarteschlange das Zertifikat.

> Diesen Schritt erledigen Operatoren und Administratoren. Ihre Rolle kann das Ergebnis lesen; bitten Sie für Änderungen einen Operator oder Administrator.



9 Ereignisse an Ihr SIEM senden

Passend zu Ihrer Lizenz

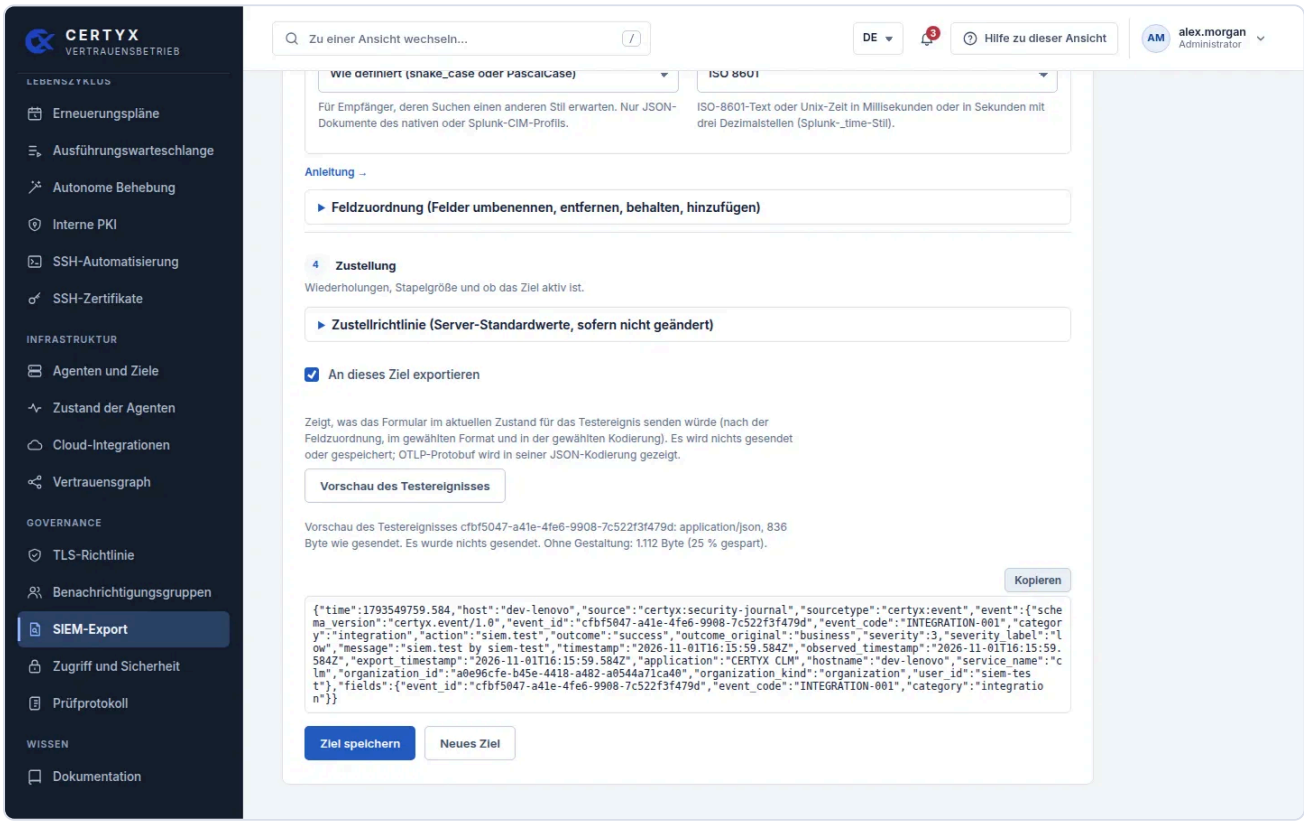
WARUM

Ihr Sicherheitsteam sieht jede Anmeldung, Änderung und jeden Fehler in Splunk, QRadar, Sentinel, Elastic oder jedem anderen SIEM, und Sie entscheiden, wie groß jedes Ereignis ist, damit keine SIEM-Lizenz verschwendet wird.

SO GEHT'S

1. Öffnen Sie SIEM-Export und geben Sie einen Namen und eine Kennung für das Ziel ein.
2. Wählen Sie den Transport Ihres SIEM, zum Beispiel Splunk HTTP Event Collector, und geben Sie Adresse und Token ein.
3. Wählen Sie unter Form und Größe Ausgewogen oder Sparsam; Vorschau des Testereignisses zeigt, wie viele Byte jedes Ereignis spart.
4. Speichern Sie, dann Verbindung prüfen und Testereignis senden.

> Diesen Schritt erledigen Administratoren. Wenn Sie kein Administrator sind, wenden Sie sich an Ihren.



10 CERTYX mitnehmen

Smartphones für Ihr Team autorisieren

WARUM

Warnungen und Freigaben auf dem Smartphone – nur auf Geräten, die Ihr Administrator autorisiert hat.

SO GEHT'S

1. Gehen Sie in Zugriff und Sicherheit zu Mobilgeräte.
2. Wählen Sie den Benutzer und „Aktivierungscode erzeugen"; Ihre Sitzung muss mit MFA angemeldet sein.
3. Der Benutzer installiert CERTYX aus dem App-Store Ihrer Organisation, scannt den QR-Code oder gibt den Code ein und meldet sich mit seinem Konto und MFA oder per Unternehmensanmeldung an.
4. Wählen Sie bei einem verlorenen Gerät „Zugriff widerrufen"; die App darauf funktioniert sofort nicht mehr.

> Diesen Schritt erledigen Administratoren. Wenn Sie kein Administrator sind, wenden Sie sich an Ihren.

