Certivo Compliance Platform
Secure Configuration Guide

Field	Value
Document Title	Certivo Compliance Platform — Secure Configuration Guide
Provider	Certivo, Inc.
Service Name	Certivo Compliance Platform
Application URL	https://app.gov-cloud.certivo.com/
Service Model	SaaS
Deployment Model	Government-Only Cloud — AWS GovCloud (US)
Version	1.1.2
Status	Approved
Document Owner	Certivo Security / Compliance
Approved By	Kunal Chopra
Effective Date	Oct-21-2026
Next Review Date	Aug-09-2027
Security Contact	security@certivo.com

1. Purpose

This guide describes the minimum security settings and practices recommended for customers using the Certivo Compliance Platform. It is intended to help customer administrators and users configure and use the service securely in accordance with their organization's security requirements and applicable regulatory obligations.

This guide does not replace Certivo's internal security documentation, System Security Plan, or FedRAMP authorization package. It is a customer-facing reference document.

2. Secure Account Access

- Access the Certivo Compliance Platform only through the approved application URL: https://app.gov-cloud.certivo.com/
- Create a separate, individual account for each user. Do not share accounts.
- Use a strong, unique password for each account. Do not reuse passwords across services.
- Multi-factor authentication (MFA) is required for every user. Each user signs in with a password and a second factor: an authenticator app or a passkey. Certivo recommends a passkey, which resists phishing.
- Grant each user only the access required for their specific job responsibilities (least privilege).
- Review administrator and privileged-user access at least quarterly.
- Remove access promptly when a user leaves the organization or changes responsibilities.
- Do not use generic, shared, or service accounts for human user access.

3. Administrator Access

- Limit administrative access to authorized personnel only.
- Use individual administrator accounts. Do not share administrator credentials.
- Do not expose administrative services, database services, or internal management interfaces directly to the public internet.
- Use the approved secure administrative access method for any privileged operations.
- Log and review all administrative actions.
- Review privileged access at least quarterly and remove access that is no longer required.
- Notify Certivo security immediately if an administrator account is suspected to be compromised.

4. Integration and API Security

- Use HTTPS/TLS for all integrations with the Certivo platform.
- Use a separate credential or API token for each integration or system connection.
- Store credentials and tokens in an approved secrets-management system. Do not store them in plaintext files, spreadsheets, source code, screenshots, tickets, or email.
- Rotate credentials and tokens when personnel, systems, or responsibilities change, and at least annually.
- Disable unused integrations and revoke unused credentials promptly.
- Limit each integration to the minimum permissions it requires to function.
- Monitor integration activity for unexpected or unauthorized access patterns.

5. Data Protection

- Upload only information required for the applicable compliance activity.
- Do not upload passwords, private keys, API tokens, or unrelated sensitive information.
- Restrict access to uploaded documents using user roles and business need.
- Use encrypted HTTPS/TLS connections when transmitting data to Certivo.
- After downloading a report or document, customers are responsible for storing it only in approved locations, applying their own access and retention requirements, and preventing unauthorized redistribution.
- Do not place Certivo data in an unapproved public location, personal storage, or unauthorized system.
- Encryption note: Certivo production data at rest is encrypted. Stored documents in Amazon S3 use Amazon S3-managed server-side encryption (SSE-S3) with the AES256 algorithm. The database and its backups, and the disks of the servers that run the platform, are encrypted with AWS-managed AWS KMS keys. Any change to the encryption design requires a separate approved change with validation evidence. Customers transmitting data to Certivo must use encrypted HTTPS/TLS connections.
- Platform note: This guide does not state that Certivo currently enforces customer-side classification, retention, or redistribution controls after a file has been downloaded.

6. Secure Document Processing

- Upload documents only from trusted and authorized sources.
- Confirm that each document belongs to the correct supplier, product, part, or compliance record before uploading.
- Review extracted information for accuracy before using it in a compliance record.
- Report suspicious files, incorrect extraction results, or unauthorized access to Certivo immediately.

No application feature of the Certivo Compliance Platform uses Amazon Bedrock, and the AWS GovCloud (US) account holds no Amazon Bedrock resources (Security Lead's evidence record of 14 August 2026, recorded 13 October 2026). The platform therefore presents no Bedrock-generated results. Earlier versions of this guide asked customers to review AI-generated and AI-assisted results before using them; those statements (two in this section and one in section 7) were withdrawn in version 1.1.2.

7. Customer Responsibilities

Customers are responsible for the following within their Certivo tenant:

- Managing Certivo users, roles, and access permissions;
- Protecting passwords, credentials, and API tokens;
- Removing access when it is no longer required;
- Reviewing administrator and integration access at least quarterly;
- Uploading only authorized and appropriately classified information;
- Protecting exported Certivo information after download according to their own internal requirements;
- Reporting suspected security incidents, unauthorized access, or data exposure promptly; and
- Following their organization's applicable data-handling, information-security, and regulatory requirements.

Certivo is responsible for the security of the platform infrastructure, including the AWS GovCloud environment, network controls, encryption at rest and in transit, audit logging, and availability. Customers are responsible for the security of their own accounts, users, credentials, uploaded data, and exported information after download.

8. Reporting a Security Concern

Report suspected unauthorized access, data exposure, credential compromise, suspicious files, or any other security concern to Certivo immediately.

Security Contact: security@certivo.com

Trust Center: https://trust-gov.certivo.com/

Do not include passwords, private keys, API tokens, or other secrets in the initial security report. Certivo will provide a secure channel for sharing sensitive details if required.

9. Document Control

Field	Value
Document Title	Certivo Compliance Platform — Secure Configuration Guide
Version	1.1.2
Status	Approved
Document Owner	Certivo Security / Compliance
Approved By	Kunal Chopra
Effective Date	Oct-21-2026
Next Review Date	Aug-09-2027
Security Contact	security@certivo.com
Public Location	Certivo Trust Center, https://trust-gov.certivo.com/ (Resources: Certivo Secure Configuration Guide)
Access Method	Public HTTPS access; no authentication required

10. Version History

Version	Date	Change	Approved by
1.1	Aug-09-2026	Approved version.	Kunal Chopra
1.1.1	Oct-08-2026	Corrections only: section 2 now states that MFA is required (authenticator app or passkey), replacing a statement that MFA was planned; the encryption note in section 5 now covers the database, backups and server disks as well as stored documents; the Trust Center address in sections 8 and 9 is the AWS GovCloud Trust Center, https://trust-gov.certivo.com/; section numbering corrected.	Kunal Chopra
1.1.2	Oct-21-2026	Correction only: section 6, "Secure Document and AI-Assisted Processing", renamed "Secure Document Processing"; its two bullets asking customers to review AI-generated and AI-assisted results removed and a statement added at the end of the section that no application feature uses Amazon Bedrock and the account holds no Amazon Bedrock resources (Security Lead's evidence record of 14 August 2026, recorded 13 October 2026); section 7, the bullet "Reviewing automated and AI-assisted results before using them in compliance decisions;" removed (decision 28 of 19 October 2026); the Version, Status and Effective Date fields updated. Nothing else changed.	Kunal Chopra