Workato Security Overview

Last updated: November 2023

Workato is committed to providing a highly secure and reliable integration and business automation platform. This includes maintaining the confidentiality of its customers' information and ensuring that customers' information will be available when it is needed. To achieve this we use proven, tested, best-in-class security tools, technologies, practices and procedures.

Compliance

SOC-1 and SOC-2 audited

Workato has successfully completed a Service Organization Controls 2 (SOC-2) Type II audit with a third-party evaluator certified by The American Institute of CPAs (AICPA). This audit uses the Trust Services Principles, published by the AICPA, to evaluate the effectiveness of a service organization's controls with respect to security, availability, processing integrity, online privacy, and confidentiality.

Workato also undergoes an annual SOC-1 Type II audit, focused on financial reporting. SOC-1 examines the internal controls of a service organization and the effect those controls may have on a user entity’s financial statements.

Audit reports are available to current and prospective customers under NDA.

HIPAA

Workato is HIPAA compliant as a Business Associate and is able to sign a Business Associate Agreement (BAA) with customers. Workato obtains an annual HIPAA compliance attestation from an external auditing firm.

PCI

Workato uses PCI Compliant Level 1 audited payment processor Stripe for processing credit card payments for the Workato services.

Hosting Environment and Physical Security

Workato is hosted on public cloud infrastructure from Amazon Web Services (AWS). Amazon maintains high standards of security for their data centers, and has numerous certifications for

their cloud services. Workato is an AWS Partner and adheres to standards and best practices for its cloud environment, including the AWS Well-Architected Framework.

Workato supports hosting in various cloud regions, at the customer's option.

Network Security

The Workato website is only accessible over HTTPS. Traffic over HTTPS is encrypted and is protected from interception by unauthorized third parties. Workato follows current best practices for security, including the use of strong encryption algorithms with a key length of at least 128 bits.

Workato also uses secure protocols for communication with third-party systems: usually HTTPS, but other protocols such as SFTP and FTPS are also supported. For on-premise systems, access requires the installation of an on-premises agent behind the firewall, which communicates outbound to Workato over an encrypted link, using TLS 1.2. No direct inbound access from Workato to customer systems is required.

Workato uses a multi-tier architecture that segregates internal application systems from the public Internet. Public traffic to the website passes through a Web Application Firewall (WAF) and then is routed to interior systems running on private subnets. Interior as well as exterior network traffic uses secure, encrypted protocols. All network access, both within the datacenter and between the datacenter and outside services, is restricted by firewall and routing rules. Network access is recorded into a centralized secure logging system.

Authentication

Clients login to Workato using a password which is known only to them. Password length, complexity and expiration standards are enforced. Passwords are not stored; instead, as is standard practice, only a secure hash of the password is stored in the database.

Workato users can optionally configure their accounts to use Two-Factor Authentication, by means of an authenticator app such as Google Authenticator, Microsoft Authenticator, or Authy.

Workato supports automatic session logout after a period of time. The timeout can be set from 15 minutes up to 14 days. Enterprises can set the appropriate timeout period according to their security needs.

Workato supports integration with 3rd party SAML compliant Single Sign-On (SSO) systems. This allows an enterprise to manage access to Workato as well as other enterprise applications and apply custom authentication schemes and policies. Workato's best practice

recommendation is for customers to utilize SAML for authentication, in which case the customer's identity provider (IdP) controls authentication policies.

Besides SSO, Workato also supports the SCIM standard to automate user provisioning and deprovisioning controlled by the customer's IdP.

When Workato recipes connect to remote systems using user-supplied credentials, where possible this is done using OAuth2 or JWT, and in those cases, no credentials are stored in the Workato system. However, if a remote system requires credentials to be stored in Workato, they are encrypted using a 256-bit key. Customers can also use an external Secrets Manager for credential storage.

Workato's best practice recommendation is for customers to use an integration specific user identity (ISU) with appropriate entitlements/scopes for connection authentication for applications that are part of the recipes.

Access Control and Monitoring

Workato provides platform facilities to control, manage, and monitor user activities within the platform. These include: a robust Role-Based Access Control (RBAC) system; support for separate development, test and production environments; user activity audit logs, and Automation HQ for control and visibility across multiple workspaces.

Application Development

Workato has a comprehensive, documented software development lifecycle process that incorporates security and privacy considerations. That process includes: design and code reviews, scanning for issues in 3rd-party dependencies (SCA), automated code and secret scanning, and unit and integration testing.

Development staff receive regular training on Secure Coding Practices, including avoidance of the OWASP Top Ten Web application vulnerabilities.

Vulnerability and Penetration Testing

Workato engages a qualified 3rd-party to conduct an annual platform level vulnerability and penetration test. Workato also has a program of regular internal vulnerability scanning, and runs a bug-bounty program (currently private).

The results from testing are analyzed and vulnerabilities are addressed based on risk and severity.

Data Privacy

Workato has a public privacy policy, which details the types of personal information we collect, our handling of this information, and our customers' privacy rights. Workato is GDPR compliant and commits to provisions in a Data Protection Addendum for data transfers outside of the EU/U.K. Workato's annual SOC-2 Type II audit includes the Privacy Trust Principle.

At-Rest Protection

All information on the Workato platform is encrypted at rest and in transit. All data stored in the Workato system is encrypted at rest using a strong encryption algorithm (AES-256).

Workato stores a log of transactions for a limited period of time, in order to provide visibility into system activity, facilitate testing and debugging, allow the re-running of failed transactions, and to support long running transactions. The maximum retention period varies by Workato plan and in some plans is configurable. If longer-term retention is required, Workato provides the capability (an optional add-on feature) to stream transaction logs and audit history to an external destination. Supported destinations include S3, Azure Monitor, Azure Blob Storage, or a customer provided HTTP endpoint.

Workato has innovative key management features for securing customer data. Certain sensitive data including transaction data and stored credentials are double-encrypted. All data is encrypted with a global key managed by our cloud providers. These keys are rotated at least annually. In addition, Workato encrypts data with secondary keys whose lifetimes are tied to the configured retention period for the data. For job history, content is encrypted with a key that is specific to the job, a tenant, and a one-hour time window. At the end of the configured retention interval, the key is deleted, effectively erasing the data within the time window by making it unreadable. Subsequently, the data storage is also reclaimed.

Workato's Enterprise Key Management feature allows customers to use their own master encryption keys, maintained within their own AWS account, for encryption of data in the Workato platform.

Data Masking and Zero Retention

Workato provides the ability to mask out sensitive data for additional security. The data masking feature is available in certain Workato plans. It can be applied to individual Workato recipe steps (triggers or actions). The input and output of a masked step are not shown in the job history view within the Workato UI and are also not stored persistently. Masked trigger data must still be persisted, to support retry of a failed recipe; but when masking is enabled for subsequent steps (action steps), data from those steps is only stored transiently in memory.

If desired, zero retention can be selected on a per-recipe basis, in which case data will be held only temporarily in memory during processing. A record of the transaction, including time it was initiated and the result (success or failure), will be stored, but none of the underlying data is persisted.

High Availability

Workato is designed to offer high availability and resilience to service disruption. Technical measures used to ensure high availability include running Workato services in redundant clusters, utilizing multiple redundant cloud Availability Zones, and continuous replication of the application database to a standby system.

Current system status and recent uptime statistics are continuously available at status.workato.com.

Workato has implemented a Business Continuity and Disaster Recovery program. This program includes not just measures to insure the high availability of Workato's IT assets, but also contingency planning for natural disasters, pandemics, and other possible disruptions.

Incident Response

Workato has deployed a variety of security and monitoring tools for its production systems. There is 24x7 monitoring of the security status of its systems and automated alerts are configured for security and performance issues. Current status and historical uptime are available at status.workato.com.

While we don't anticipate there being a breach of our systems, Workato has put in place a Security Incident Response Plan, which details roles, responsibilities and procedures in case of an actual or suspected security incident.

Our Organization

All employees are subject to background checks that cover education, employment and criminal history, to the extent permitted by local law. Employment at Workato requires written acknowledgement by employees of their roles and responsibilities with respect to protecting user data and privacy.

Workato applies to the principle of least privilege for access. All access and authorization rights are reviewed regularly. Access or authorization rights will be withdrawn or modified, as appropriate, promptly upon termination or change of role.

Workato maintains an information security training program that is mandatory for all employees, with additional role-based training for staff with development roles.

Knowledgeable full-time security personnel are on staff.

Vulnerability Disclosure

Workato welcomes reports of vulnerabilities or other security issues

Note that we are primarily interested in issues that may affect authenticated users of our services, rather than something related to our public facing sites, many of which are hosted by 3rd parties unrelated to our services. Note also we do not generally allow automated scanning of our sites and may block it if detected.

Vulnerability reports will be acknowledged and reporters kept apprised of their report's status.

Reports can be submitted to vulnerability@workato.com.