Platform Security & Architecture

Coupa Software

Architecture

Coupa's AI-driven source-to-pay platform is delivered using a hosted, software-as-a-service (SaaS) model. It operates on a cloud-native platform that is primarily built on Amazon Web Services (AWS)[1]. Under the AWS "shared responsibility model," AWS provides physical and network security, but it is up to Coupa to build and run a secure and highly-available application.

The Coupa Platform runs across several individual data centers, called Availability Zones (AZs), that are grouped into an AWS Region. Each Availability Zone has its own operations staff, redundant power, climate controls, and physical security. This is to avoid sharing common infrastructure as a single point of failure.

We offer a number of "Coupa Regions" that consist of one or more AWS Regions. Each AWS Region contains multiple AZs. Customer data remains hosted in the Coupa Region that customers select when their instance is provisioned, but note that your users can access your Coupa instance from anywhere in the world.

Table 1: Coupa hosting configurations

Coupa Region	AWS Region 1	AWS Region 2
APAC	Singapore	*N/A*
AU	Sydney, Australia	*N/A*
EU	Germany	Ireland
UAE	United Arab Emirates	*N/A*
USA	US East	US West

In each AWS Region, we operate across multiple AZs; this means your data is synchronized across the AWS Region and we can continue operating even if one or more AZs goes down.

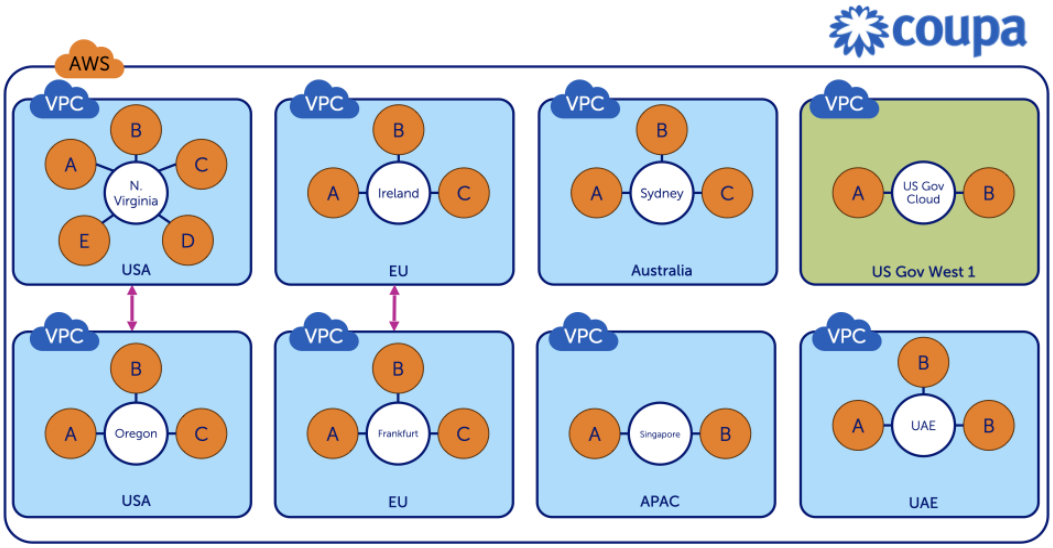
In the US Coupa Region, we use five AZs in the US East AWS Region, and three AZs in the US West AWS Region. Backup snapshots are replicated between the US East and US West Regions.

[1] AWS is our default hosting provider, and this is where your instance will be provisioned. The InvoiceSmash product and OpenAI supported capabilities (Coupa-specific tenant) are hosted in Microsoft Azure for *all* customers in the same Coupa Region you select. Coupa implements the same security controls in AWS and Azure using their respective constructs, and both providers are in-scope where applicable for Coupa's SOC 1 and SOC 2 audits.

In the EU Coupa Region, we use three AZs in the Ireland AWS Region and three in the Germany AWS Region. Backup snapshots are replicated between the two AWS Regions.

We offer additional Coupa Regions in Australia, Singapore, and the United Arab Emirates. In order to accommodate data sovereignty restrictions, these three Coupa Regions are not paired with a separate region. All Coupa Regions use a multi-AZ architecture to provide seamless high availability and disaster recovery capabilities, but only the EU and US Coupa Regions have cross-region pairings.

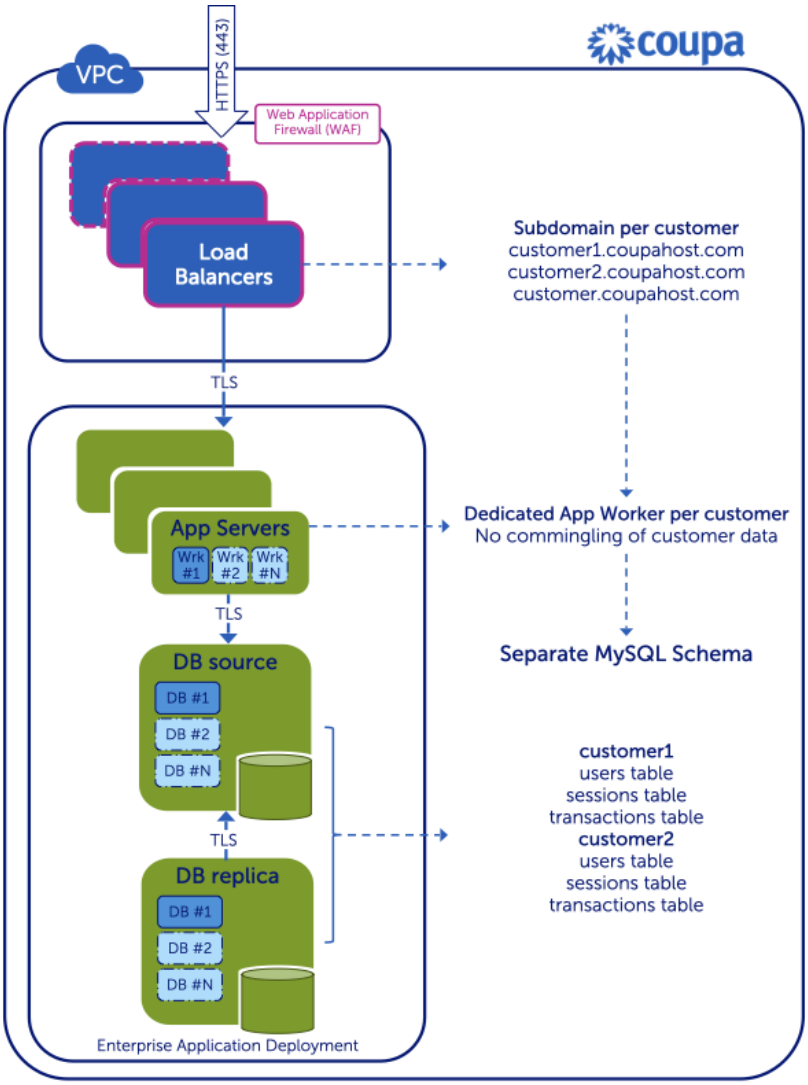
Figure 1: Coupa hosting regions



The Coupa application is fronted by a web application firewall (WAF). Coupa manages the specific firewall rules and AWS provides the underlying service. This cloud-based WAF protects the application from common layer 7 attacks such as SQL injection and cross-site scripting. The WAF and AWS's Shield service work in conjunction to protect the Coupa Platform from application- and network-layer distributed denial of service (DDoS) attacks and ensure high availability.

Behind the WAF is a virtual load balancer that distributes traffic to a pool of application servers deployed across multiple AZs within the AWS Region.

Figure 2: Application architecture overview



The Coupa application is deployed in an AWS Virtual Private Cloud (VPC). The VPC is a logically isolated section of AWS where Coupa has control over the virtual networking environment, including IP address ranges, subnets, route tables, and gateways. Coupa ensures strict network segregation by isolating each tier – web, application server, and database – using a combination of security groups and network access control lists (NACLs). NACLs are applied to subnets and provide stateless allow/deny rules at the network-level. Security groups are applied to specific instances and AWS resources and act as a virtual stateful firewall to further control access with a "default deny" approach; that is, all inbound and outbound traffic must be specifically reviewed and authorized. This combination – traffic must be allowed by both the NACLs and SGs – provides a layered approach to controlling traffic in the environment.

We operate under a “default deny” posture where resources cannot communicate with each other unless permitted by specific security group rules. Database servers are completely segregated from both the application servers and the internet using security groups and private subnets. Authentication between the application server and the database uses a secret that is unique to each customer. All secrets are securely stored and managed using a secrets management platform that provides auditing, monitoring, and fine-grained access control.

The Coupa Platform architecture offers single-tenant isolation along with multi-tenant efficiency. Coupa’s virtual private cloud security infrastructure ensures data never co-mingles across tenants and customers. Each customer has a separate database schema, instance of the code, object storage, and Ruby on Rails framework. Furthermore, the Rails application uses customer-specific credentials to connect to a backend database instance that is used only for that customer. This framework is fast and scalable for integrations, allowing us to drive more innovation for our customers, and maximize code quality.

AI Architecture

Coupa’s GenAI platform and language models are private to Coupa and part of our overall architecture. The GenAI platform is hosted in a logically isolated network managed by Coupa. Additional segmentation is provided by security groups to ensure only authorized Coupa services in the appropriate region can access the GenAI platform.

Coupa’s GenAI platform is deployed regionally. We ensure that customers use the GenAI platform in their Coupa Region (Table 1). For example, a customer hosted in the EU Coupa Region will use Coupa’s GenAI platform hosted in the EU.

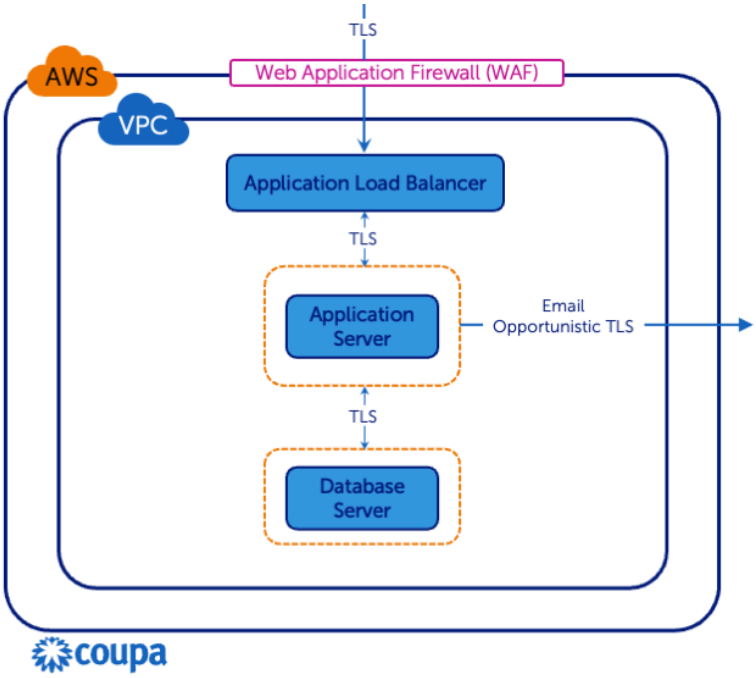
Please visit the AI Trust Center for more information on how we ethically use AI and our AI governance program.

Data Encryption

Data In Transit

Customer data is encrypted in transit and at rest in the Coupa Platform. All connections to and from the Coupa Platform use TLS 1.2 or greater with support for strong ciphers. We use opportunistic TLS for email; HIPAA instances enforce TLS for email.

Figure 3: Data encryption in transit



Data At Rest

Coupa uses AWS Key Management Service (KMS) to manage encryption keys for data at rest. KMS provides a highly-available key generation, storage, management, and auditing solution. The keys used for data encryption are Data Encryption Keys (DEK). The DEK is further encrypted by a process known as Envelope Key Encryption. The top of the key hierarchy is an AWS KMS key that does not leave KMS.

Transactional data is stored on databases backed by EBS (Elastic Block Store) volumes for persistent storage. These EBS volumes are encrypted using the 256-bit Advanced Encryption Standard algorithm (AES-256) in Galois/Counter Mode (GCM). All EBS volumes, including backup snapshots, are encrypted at rest with AES-256-GCM. EBS encryption uses AWS-managed keys in each AWS region that are rotated annually.

Files uploaded via the web, mobile app, APIs, and SFTP are stored in AWS Simple Storage Service (S3) with AES-256 encryption. Prior to storing in S3, the Coupa application encrypts each file using a key that is unique per customer.

Each customer instance has its own unique DEK that encrypts sensitive columns in the database using AES-256. Coupa's DEKs are rotated every 180 days. Please visit the Compass portal for a list of encrypted fields for customers on HIPAA instances.

Backups and Disaster Recovery

Coupa's backup schedule and disaster recovery program are designed to meet our recovery point and recovery time objectives of 1 hour and 24 hours, respectively.

Table 2: Backup schedule and retention

Backup Schedule	Retention Period
Hourly	24 hours
Daily	14 days
Weekly	6 weeks
Monthly	12 months

Snapshots of EBS volumes are taken per the backup schedule in **Table 2**. These snapshots are encrypted using AES-256 and replicated across AZs and to the paired AWS Region where available (see **Figure 2**). In the APAC, AU, and UAE Coupa Regions, customer data is replicated across multiple AZs within those regions for data residency purposes. In the event we have to switch over to the secondary AWS Region, a customer's database can be relaunched from the most recent EBS snapshot. Application servers, containers, and supporting infrastructure are deployed as code to scale in the secondary region.

Since Coupa's Platform is deployed across multiple AZs in each AWS Region, we can continue operating in the event a single AZ goes down. Should that occur, we automatically scale resources in the still-operating AZs, and monitor overall regional capacity and utilization to determine if and when a regional failover is needed (for the USA and EU Coupa Regions).

Coupa performs an annual disaster recovery test to validate that we can successfully meet our recovery time and recovery point objectives. During the testing period, the operations team runs technical failover exercises in all Coupa Regions and for each product. Additionally, we organize a tabletop exercise involving senior management and test call trees and other communication procedures for effectiveness. These tests and tabletop exercises provide invaluable "lessons learned" that we use to strengthen and improve our processes.

A summary report and attestation of these exercises are available to customers on the Compass portal.

Infrastructure Security and Operations

Coupa's Security Operations Center (SOC) is staffed 24/7 to monitor the platform and investigate any security alerts.

Logs from application servers and containers, database servers, and cloud infrastructure are collected and analyzed in our security information and event management (SIEM) system. This allows us to detect any potential security threats and promptly respond to them.

Containers and servers in the Coupa Platform are protected with host-based agents that scan for vulnerabilities, provide runtime protection against malicious code, and perform real-time file integrity monitoring. Virus and malware definitions are updated daily. Coupa's cloud infrastructure is continuously monitored for any misconfigurations or deviations from our security standards. These tools work together to provide real-time monitoring and protection across the whole stack, including the underlying cloud infrastructure.

We also partner with SecurityScorecard to monitor the configuration and security posture of our external infrastructure, such as DNS, load balancers, and TLS certificates – this is in addition to our "in house" monitoring. If there is a change to Coupa's score, we'll investigate and remediate as appropriate. Coupa's SecurityScorecard covers the infrastructure that hosts our customers' data.

Access to production resources requires phishing-resistant multi factor authentication (MFA) and is limited to authorized Coupa personnel with specific permission grants based on the principle of least privilege and job role. We use a multi-VPC, multi-account architecture to segregate and manage traffic to and from specific tooling and administrative VPCs, which can only be accessed through hardened bastion hosts requiring MFA.

All access requests require multiple layers of approval, and privileged access management is regularly audited by internal teams and our external auditor, for example, as part of the annual SOC 2 Type 2 audits and biannual SOC 1 Type 2 audits.

Secure Software Development

We implement multiple layers of security controls as product features move from design documents to running in production so that we *develop* a secure platform, not simply secure a developed one.

To further support secure software development, Coupa has a dedicated application security ("AppSec") team. This team is responsible for managing security controls in the software

development pipeline and collaborates closely with development teams to build and release secure software.

All product features and infrastructure designs go through a comprehensive review and approval process with a cross-functional team of architecture, DevOps, and security staff. Security and data privacy controls are considered and designed from the start.

Coupa's entire codebase is scanned regularly to identify vulnerable software packages and ensure compliance with commercial and open source licenses. Tickets are automatically created and assigned to development teams to fix any findings resulting from these scans. Additionally, all code changes are scanned to detect secrets, tokens, or private keys in the code. Code cannot progress in the pipeline until all secrets are removed or the security team grants an exception if there's a false-positive.

All code is required to undergo peer review and receive sign-off prior to being released to production. This process is enforced programmatically in the code repository so that multiple individuals review and approve all code changes.

Regular dynamic application security tests (DAST) are conducted by the AppSec team. These tests assess our applications, including APIs, in a runtime environment to identify vulnerabilities and exploitable flaws. Fuzz testing is also performed as part of this process, which helps identify software defects, security vulnerabilities, and unexpected behaviors that may not be detected through other testing methods.

Technical Security Assessments

Coupa uses a combination of internal and external testers to proactively assess the security of the Coupa Platform throughout the year. Coupa's internal security red team has in-depth knowledge of the platform and environment, and performs pen tests prior to each major release, which occur three times per year.

An independent external security firm conducts annual pen tests for each Coupa product using a comprehensive methodology based on the Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks. APIs are in-scope for all external pen tests. If the external pen testers identify any vulnerabilities, Coupa will remediate per our vulnerability management process – the external testers will also verify that Coupa has remediated any previously-identified vulnerabilities during their next test. A summary report of the external pen tests is available upon request. Separate annual pen tests are conducted for the PCI and FedRAMP environments as part of those respective programs.

Coupa also has a bug bounty program, inviting external security researchers, commonly known as bug bounty hunters, to search for and report any security flaws, bugs, or vulnerabilities they discover.

We use the HackerOne platform for this program. HackerOne is “always on” and we regularly update our test applications to current versions. We invite bug bounty hunters and researchers to test our applications on HackerOne pursuant to our Vulnerability Reporting Policy. The Policy outlines how you can safely test Coupa’s applications and enroll in the HackerOne bug bounty program, where we validate and reward unique bug discoveries. Note that we do not provide compensation outside of this program for funding and reporting purposes. We recognize the important role independent security researchers play in keeping the internet secure. For any researcher who follows the Vulnerability Reporting Policy, Coupa’s security team will respond to your report in a timely manner, provide an estimated timeframe to address the vulnerability, and notify you when it is remediated.

Coupa customers can report any security concerns or vulnerabilities using the Compass support portal.

Table 3: Summary of Coupa’s security monitoring, assessments, and audits

Regularly		**Major Releases**	**Annual**
Host based anti-malware scans	HackerOne bug bounty campaigns	Pre-release penetration tests by Coupa’s internal red team	Web application security penetration tests by an independent external firm
Scan cloud infrastructure for misconfigurations and security issues	Dynamic application security testing by Coupa’s application security team	Security scan and certification of new infrastructure builds	Audits, including SOC 1, SOC 2, PCI, C5, and ISO 27001, by an independent external auditor
Scan the full codebase for vulnerable packages, and all code changes for secrets and passwords	SecurityScorecard scan of external production infrastructure		

Audit and Compliance Programs

Each year, Coupa undergoes over 30 external audits that evaluate our security policies and operating effectiveness of our security controls. Our security and privacy management systems are certified to ISO:27001 and ISO:27701, respectively. All Coupa products undergo an annual SOC 2 Type 2 audit, with the audit reports available each fall. A subset of Coupa products, including our Procure-to-Pay and Treasury Management suites, undergo SOC 1 Type 2 audits every six months, with reports available in the spring and fall. Audit reports are generally available to customers 4-6 weeks after the conclusion of the audit period.

These independent audit reports are foundational to demonstrating our commitment to protecting our customers' data. We continue to evolve and invest in our security and audit programs; for example we added the Cloud Computing Compliance Controls Catalog (C5) framework to our portfolio to provide additional assurance over our controls.

You can request a copy of our audit reports, monthly bridge letters, and certifications using the self-service portal. Please refer to the audit reports for full descriptions of in-scope products and services.

Table 4: Summary of Coupa's audits and assessments

Framework or Certification	Frequency
Information Security Management System – ISO/IEC 27001:2013	Annual
Privacy Information Management System – ISO/IEC 27701:2019	Annual
SOC 1 Type 2 (*Procure-to-Pay, Coupa Treasury Management, and Coupa Contingent Workforce*)	Every 6 months, spring and fall
SOC 2 Type 2 (*all products*)	Annual
Cloud Computing Compliance Controls Catalog (C5:2020) (*Procure-to-Pay, Coupa Sourcing Optimization, and Contract Lifecycle Management*)	Annual
Asia Pacific Economic Cooperation Privacy Recognition for Processors (APEC PRP)	Annual
Trusted Information Security Assessment Exchange (TISAX)	Annual
Payment Card Industry Data Security Standard (PCI DSS)	Annual

Health Insurance Portability and Accountability Act (HIPAA) *(HIPAA instances only)*	Annual
FedRAMP audit (*FedRAMP Authorized products only)*	Annual
International Traffic in Arms Regulations (ITAR) *(GovCloud only)*	Annual

Audit Trail

Coupa makes audits easier by capturing a digital record of all approvals to identify who approved what purchases, when, and why. Coupa provides several types of reports which allow the company to audit the approval chain setups and approval history. Coupa allows the user to manipulate reports and create end-user specific views as necessary to provide pertinent information, including dates and approver names.

A comprehensive audit trail for each document provides the ability to drill into further detail. Details include evidence regarding approval dates/times and any history behind the document, ranging from changes and comments to status updates. Also, Coupa automatically tracks audit trails on users, user roles and integrations. IT personnel and compliance professionals have the tools that are required to establish and monitor IT controls over critical financial applications and data. Administrators can generate an audit trail report which includes:

- When the user was created
- Who created the user
- When the user was last updated
- Who last updated the user
- User last login date
- User history

An example of the 100 pre-built reports that Coupa provides to ensure complete customer spend visibility includes the Requisition History Report. This report displays a full audit trail for each stage of the requisition, including who acted on it. The fields include:

- created_by – the ID of the user that created the transaction (record)
- created_at – date and time of the record creation
- updated_at – date and time that the record was updated (if necessary)
- requisition_header_id – the requisition number
- status – the status of the requisition when the transaction was recorded

Other key report examples include:

- Approval history data
- List of documents approved using delegates
- Approval chain structure (includes individual approvers and approval groups)
- Requisition and PO data where the requester is an inactive user and PO line is not in
- received status
- View PO, invoice number, invoice date, and receipt date
- Requisitions and orders that bypassed approval
- Rejected requisitions
- All invoices on hold for receipt missing and related PO, invoice, and requestor
- information
- Roles and permissions
- Approved invoices and related history
- Approval override/escalation/delegation audit report
- Invoice status history audit report
- Users with admin roles
- Users with content groups
- Users with missing manager
- Users with non-company email
- Users with a self-approval limit

Administrators can also track and report on user access roles that control access by end users, as well as integrations that control access to Coupa from a third-party system.

Integrations and Interface Security

Coupa offers many different integration options to meet the simplest to the most complex organizational needs when integrating with their in-house systems.

Flat File Integration

Coupa created a set of common flat file formats for common Coupa business objects to manually or automatically export. This allows customers to receive high-quality, quick-running integrations. Coupa's Common Flat File templates are designed to import many records from a single file sent to Coupa, not designed to process a high volume of files containing a single record of each.

- Manual Import/Export – From the administration console for Coupa master data and transactional data.

- Automated Integrations – A common flat file format to exchange multiple records from a single file between Coupa and an in-house system through a batch integration. Common flat file formats use RFC 4180 conventions and support UTF8 text encoding.

Coupa primarily exchanges files with customers via the Secure File Transfer Protocol (SFTP), and an SFTP server as part of the subscription to the service. Coupa supports both username and password, or SSH key authentication.

Coupa requires API keys for users to authenticate and securely send API requests to your Coupa instance. Each API key is unique.API keys now can be configured to have an expiry date. Configuring an API key with an expiry date is optional and if the administrator does not specify an expiry date then the key never expires. If an expiry date is specified, the API key expires at the end of the day (midnight UTC).

API keys can be configured with fine-grained access control, by Coupa object and by action.For integrations where a single record needs to be processed at a time, the Coupa API provides a RESTful interface (Rest API Calls) to facilitate this type of workflow.

OAuth 2.0 Authentication for REST API Calls

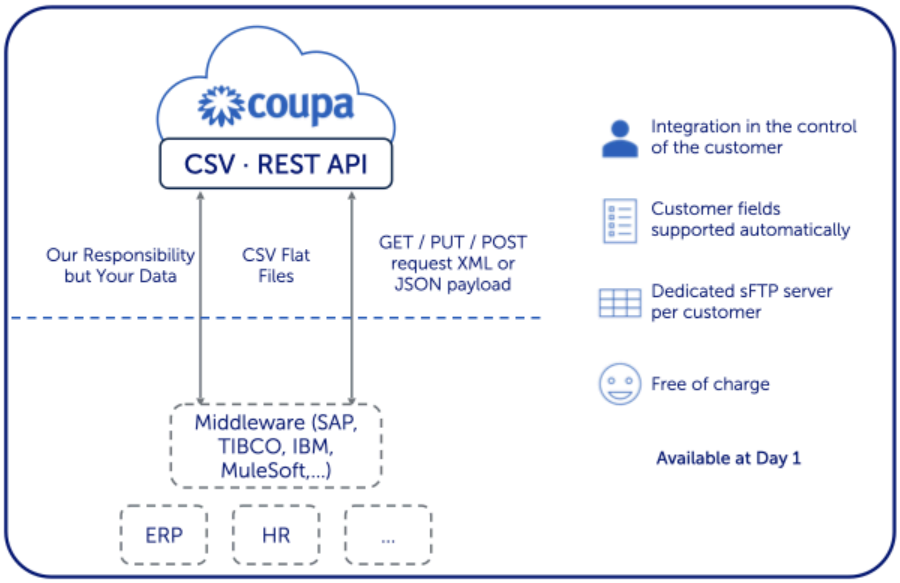
Coupa provides rich, robust access to read, edit, or integrate customer data with a REST API (Representational State Transfer). The API is designed to exchange a limited set of records between Coupa and an in-house system through real-time integration. Requests are authenticated by a unique OAuth token that is generated by Coupa. The OAuth token is bound to a user with an OAuth scope with applied restrictions.

Coupa uses OAuth 2.0 to secure call out communications with third-party systems. In most cases, calls to the API originate at the customer to GET, PUT, or POST data. Callouts originate in Coupa in response to an event to POST data to an HTTPS endpoint at the customer, which is often referred to as a webhook. OAuth 2.0 is a specification for secure authentication, authorization, and communication between known systems. When OAuth 2.0 is selected for use, the Call Out UI is updated to allow specification of the Server URL, Client ID, Client Secret, and Verification Token. OAuth2 gives authorization to Coupa without an external application receiving the user's email address or password. Before the OAuth2.0 can be used, the user must receive an access token (a piece of data that authorizes access) to access the client's information. Oauth tokens are only good for 24 hours until they need to be refreshed.

OAuth settings are available within endpoint configuration. Administrators can create, view, and edit Callouts from the Setup > Integrations > Call Outs endpoints, but they can only create new endpoints when creating a new Call Out. When creating a new Call Out, the integration admin can use an endpoint that was previously defined, or create a new link to define a new endpoint.

Note: Customers can use either 100% API integrations, 100% flat file integrations, or a combination of both.

Figure 4: Integrations overview



ERP-Specific Integrations

Coupa offers capabilities to integrate with virtually any ERP vendor. Coupa can connect with the flexibility needed to match with multiple ERP systems, using industry standards with sFTP and REST-based APIs. This open approach to integration has made it possible for Coupa to partner with all the integration technologies in the market to deliver rapid-deployment solutions for existing ERP customers.

For more information on Coupa's Integrations, see the Integration Overview page on Compass.

Bandwidth

The Coupa application is designed for speed and responsiveness, with minimal use of large graphic files. Using the Coupa application requires no more bandwidth than what is required to browse the web. The average page size is 30 kB. The application does not require a large throughput and can be run on low bandwidth networks. Additionally, Coupa is a stateless application, not consuming resources until a page is refreshed or commits a transaction. Coupa also supports compression as defined in the HTTP 1.1 standard to compress the HTML content. The content is compressed before being transmitted as data across the internet to a user. Often, the compression reduces the amount of transmitted data to 10 kB per page. Coupa recommends no less than 40 Kbps per connection, which is achievable for most corporate high-speed connections.

Mobile Security

Coupa uses various mobile security constructs and safeguards to ensure corporate data is only available to securely authenticated and properly authorized users. Coupa Mobile manages risks immagent in giving users access to data across public networks on their personal mobile devices.

iOS and Android

The SQLite database runs within the secure container for the iOS app on the user's device. SQLite is a Relational Database Management System. For SQLite, there is no stand-alone server running in the background. If the user has a passcode set or uses touchID or uses faceID, the SQLite file is encrypted using the built-in iOS encryption from Apple's security framework. Preference data is stored securely within the user's iPhone. For Android, the data that the app caches is encrypted using native Android phone security. The personal device preference data is encoded in an XML file.

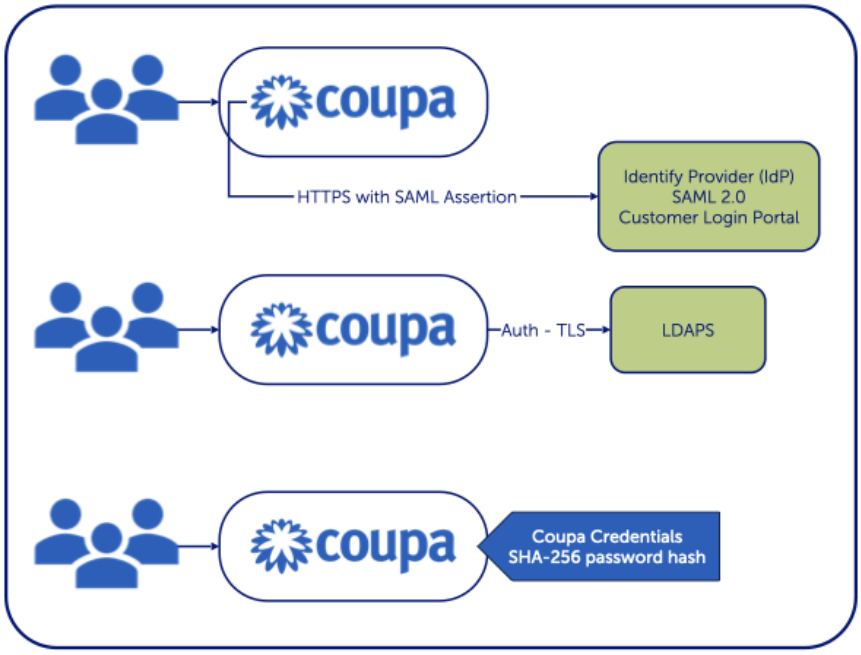
Cached Data

Authenticated Coupa users with an active session have secure access to business data as appropriate for their assigned roles and permissions. It caches minimal user information and transactional data is not stored on the mobile device. When a user logs out, the cache is emptied.

Coupa Support for Single Sign-On (SSO)

Coupa supports Single Sign On (SSO) capability through SAML (Security Assertion Markup Language). SAML permits users to log in with a single username and password to access multiple applications across the Coupa platform, without having to go through the authentication process for each application. The SSO (Single Sign-On) Integration model is described below.

Figure 5: SSO support



For more information, go to *Single Sign on: SAML Made Simple*.

Supported Browsers

Coupa supports the latest versions of these web browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

Note: Supported browser versions are updated for each Coupa release (three times per year) and documented in our release notes. Coupa is an HTML 5 application that does not require special browser plug-ins or extensions.

Release Management

Coupa releases three major software versions per year. These major releases provide new features and enhancements, as part of Coupa's commitment to bring constant innovation to its customers. New features are disabled by default to minimize their impact and allow the

customer to adopt innovations at their own pace, while ensuring they are running the latest and most secure version. Listed below are the three types of software releases.

- Major Release – Three major releases per year contain significant new features and functionalities.
- Maintenance Updates – Biweekly maintenance updates contain minor feature enhancements and stability improvements.
- Daily Updates – Address critical issues before the maintenance update is ready.

Figure 6: Coupa's release schedule

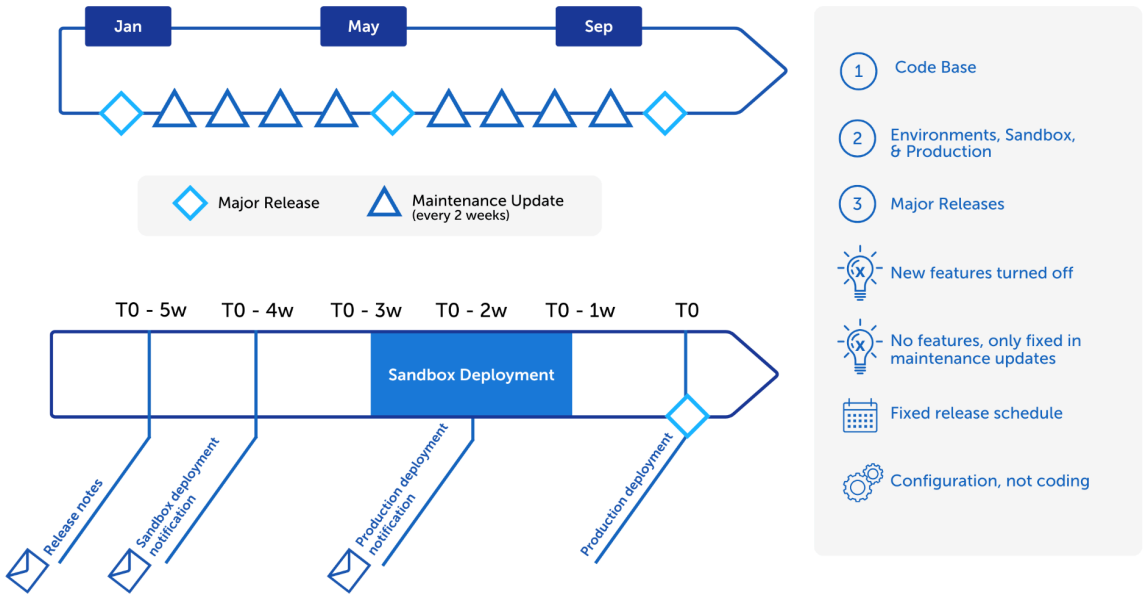


Figure 7: Example release number