SauceLabs

WHITE PAPER

An Overview of Sauce Labs Security Processes

LEARN MORE AT SAUCELABS.COM

UPDATED AUGUST 2023

Introduction

Enterprises large and small trust Sauce Labs to provide a secure platform for testing their web and mobile applications. Helping to protect our customers' data is of the utmost importance to us, as is maintaining customer trust and confidence. This document is an overview of the technology, processes and security operations that govern the Sauce Labs Continuous Testing Platform.

Table of Contents

SauceLabs

Executive Summary

This document provides an overview of the technology, software development, and service management practices used to deliver the Sauce Labs Continuous Testing Cloud. Sauce Labs provides a secure and scalable cloud computing platform for testing web and mobile apps using both virtual and real devices.

This paper is intended for prospective customers and technology professionals focused on cloud security looking to leverage Sauce Labs as a hosted digital lab. Sauce Labs provides both a real device cloud (RDC) and a virtual device cloud (VDC) for testing digital applications. Both the RDC and VDC are multi-tenant public clouds deployed across multiple data centers globally. Global support is provided by a 24x7 operations and customer support team.

Compliance Statement

Sauce Labs is a cloud-based testing lab that does not require the use of personal data, PII, PHI, or other sensitive data. The use of sanitized or synthetic data for testing is, in fact, considered a best practice. With the passing of the 2018 EU General Data Protection Law (GDPR), Sauce Labs classifies itself as a data processor with respect to its customers' test data and as a data controller with respect to account information (as such terms are discussed in Section 1 below). Sauce Labs maintains SOC 2 Type 2, ISO 27001, and ISO 27701 certifications through an annual audit and recertification process.

Data Privacy

In providing its continuous testing cloud service, Sauce Labs receives two categories of data from its customers. The first category consists of data about our customers' access to and use of our service, and may include information about the specific customer employees or contractors that use our service. We refer to this data as "account information". The second category consists of the data that our customers upload to our service or that is otherwise accessed by our service in the course of testing customer applications, and the reports, logs, and other artifacts of such testing that are generated by our service. Our service operates by processing what a user's computer or device would process when accessing and using a web or native mobile application, which typically includes the customer's compiled web application rendered in a browser or executable native mobile application installed in a real or virtual device, and the test script or commands and data inputs to manipulate the browser or application that is being tested, to mimic user behavior. Our service also generates artifacts from tests that are run, including images and videos of the application as the test is conducted, and reports, logs and analysis of the test results, We refer to this data as "test data" or "customer data". In general, test data need not and should not include any sensitive or personal data regarding customer personnel, customers, end users, or other third parties.

The Sauce Labs service is a test execution environment and is not intended as a production environment or "system of record" for any customer data (beyond data related to the tests themselves). All test logs, images and videos of applications being tested, and related reports and analysis, are automatically deleted from our service as soon as 30 days after they are generated by default, and our customers have access to and the ability to manually delete any or all such data at any time.

Sauce Labs has implemented and maintains a data privacy compliance program intended to comply with applicable requirements of the GDPR. Among other things, we:

- Maintain policies, procedures and protocols to ensure that we only process personal data lawfully, fairly, transparently, and in accordance with other privacy standards set forth in the GDPR;

- Select vendors that have implemented robust data protection measures and execute data processing and sub-processing agreements with them as appropriate;
- Offer assistance to customers to give effect to data subject rights and comply with relevant requirements under the GDPR as appropriate;
- Design our services and internal systems with data privacy principles in mind; and,
- Implement and maintain reasonable and appropriate technical, physical and organizational security measures to protect the data that we process.

We can provide additional information about our data privacy practices on request.

E.U. GDPR / Data Residency
Adhering to the GDPR, Sauce Labs works with customers to ensure, to the extent applicable, that an appropriate mechanism is implemented to legitimate transfers of personal data outside of the European Union. Sauce Labs offers EU customers service from data centers and storage infrastructure located in Europe, which avoids the need to transfer customers' raw test data (including any personal data therein) outside of the EU.

All deployments are supported by a global support team based in the U.S., and account information is also generally transferred to the U.S.

Data Controls

For data in flight, customers may choose to access Sauce Labs via Sauce Connect (SSL Proxy) or IPSec VPN. Both options support secure connectivity using TLS 1.2 or above.

For data at rest, all data is encrypted using AES 256.

3rd Party Access to Data
Sauce Labs does not share customer data or provide 3rd parties access to production systems. Contractual agreements are in place with specific vendors/partners who provide support services to Sauce Labs (e.g., hosting and code repositories).

Security of Data in Testing
Sauce Labs encourages customers to test using only non-sensitive or sanitized datasets. Sauce Labs considers all data as sensitive and therefore encrypts data at rest (AES256) and in motion (TLS 1.2) using Sauce Connect Proxy or IPSec VPN.

Production Access Security
Production access is limited to dedicated VLANs, systems, and admin privileges using multi-factor authentication. In addition, least privilege is supported and required where applicable.

Device Security
Devices in the real device cloud (RDC) are deployed in a multitenant environment. "Public" devices are shared and assigned on a per use basis to users. Public pool devices are reset after test sessions using automated scripts. See Real Devices and Security

Virtual device cloud (VDC) is also deployed in a multitenant environment. Browser/OS combinations or emulator/simulator devices are provisioned on demand in virtual machines and destroyed at the end of every test execution.

Data Retention
Sauce Labs collects test data assets from individual tests that are being run on our platform. These assets include Selenium/Appium logs, screenshots, a video of the test, and metadata.

All test execution reports are available from the Sauce Labs user interface. Test execution reports and other test data assets are stored for 30 days and then automatically deleted. Customers who require longer data retention periods are encouraged to download their data directly.

Sauce Labs Architecture

Sauce Labs ensures that customer websites and mobile apps work flawlessly on every browser, OS and device. The company's Continuous Testing Cloud helps organizations accelerate software development cycles, improve application quality, and deploy with confidence across hundreds of browser / OS platforms, including Windows, Linux, iOS, Android & Mac OS X. Optimized for Continuous Integration (CI), Continuous Delivery (CD), and DevOps, the Sauce Labs platform is designed to ensure the highest level of security. Figure 1 below illustrates the data flow across the Sauce Labs solution in relation to a customer application.

Cross Browser Web Testing

Sauce Labs gives users the ability to run manual and automated functional tests written with Selenium and Appium across more than 800 browser and OS combinations. The platform eliminates the need to build and maintain an on-premise test grid, and provides the ability to run cross-browser tests in parallel, significantly reducing the time it takes to execute these tests. Results can be analyzed using videos, screenshots, log files and Test Analytics to quickly identify test patterns and resolve defects, enabling faster release cycles.

Mobile App Testing

Sauce Labs users can test mobile native, hybrid and web apps across real devices as well as hundreds of iOS simulators and Android emulators. Mobile app tests can be conducted manually ("live" testing) to spot check issues, or automated using the Appium, Espresso or XCUITest test frameworks. Mobile tests can be run on a public real device cloud across thousands of devices, or on a private cloud, with unique devices dedicated to individual customers.

All database access is managed through an object relational and service application model. Users are assigned a unique ID and access key. Data access is limited to data associated with a specific account.

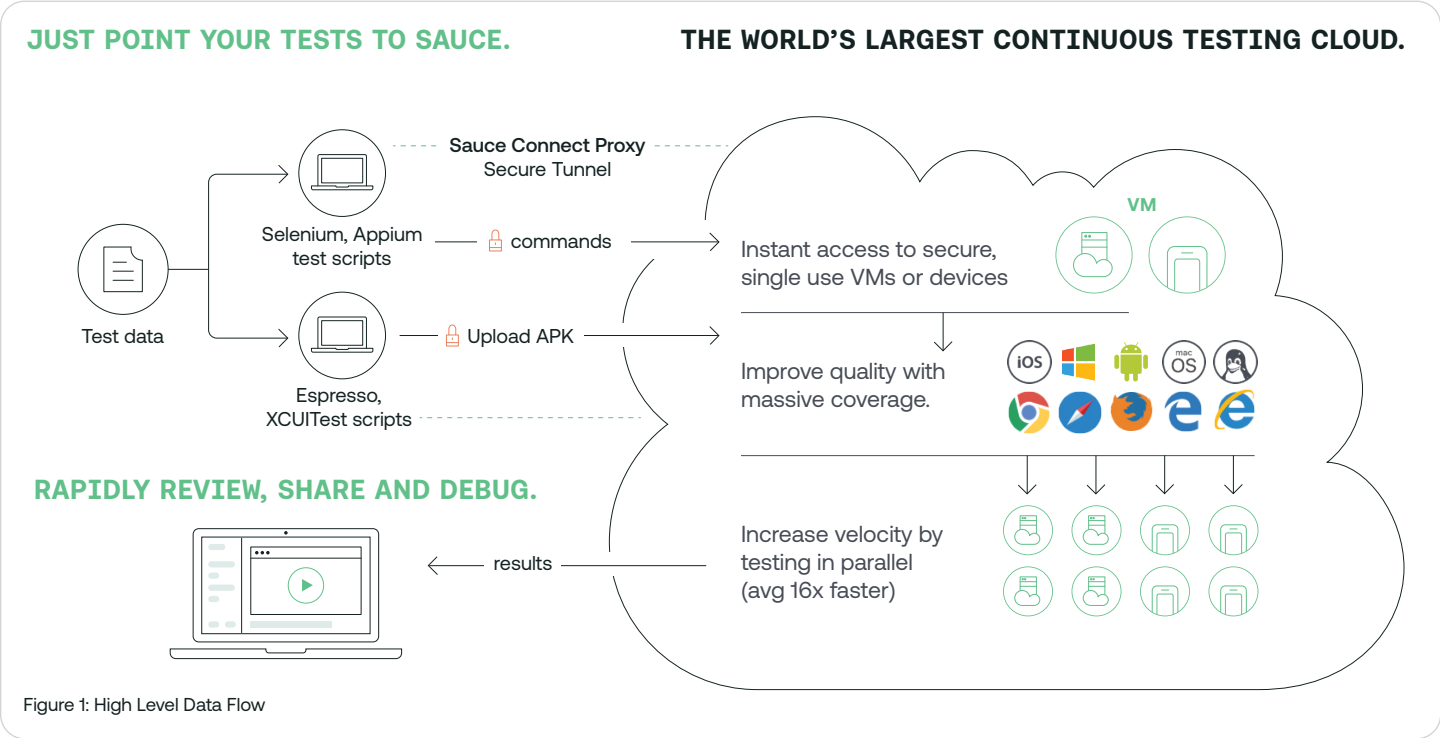


Figure 1: High Level Data Flow

Connectivity Options

Sauce Labs supports two connection options - IPSec VPN or TLS-protected proxy connections using Sauce Connect local client. The following sections provide a brief overview.

Sauce Connect Proxy and IPSec VPN solve the same problem, which is to establish a secure connection between applications hosted on an internal server and the Sauce Labs virtual machines or real devices that are used for testing. The difference is that IPSec VPN is based on an industry standard, while Sauce Connect Proxy is based on a proprietary protocol that runs over TLS. Sauce Connect Proxy is available for use by any Sauce Labs account, while IPSec VPN is a feature that requires an additional fee.

Sauce Connect Proxy

Sauce Connect Proxy™ is a proxy server that opens a secure connection between a Sauce Labs virtual machine, emulator, simulator or real device running your browser or native app tests, and an application or website you want to test that is on your local machine or behind a corporate firewall. Figure 2 illustrates the high-level architecture of the solution (please note that this diagram is for high level illustrative purposes only). Sauce Connect is not required to run tests with Sauce Labs, except for websites or applications that are not publicly accessible, where it is required. Because network architectures can be complex, it is imperative that a network administrator or engineer be involved in the implementation process as soon as possible. In addition to providing a means for Sauce Labs to access your application or website, Sauce Connect has some other uses in your testing network architecture:

- As a means of monitoring upstream traffic through a proxy like BrowserMob;
- As a way to stabilize network connections (for instance, detecting/re-sending dropped packets).
- As a superior alternative to allowlisting ("whitelisting").

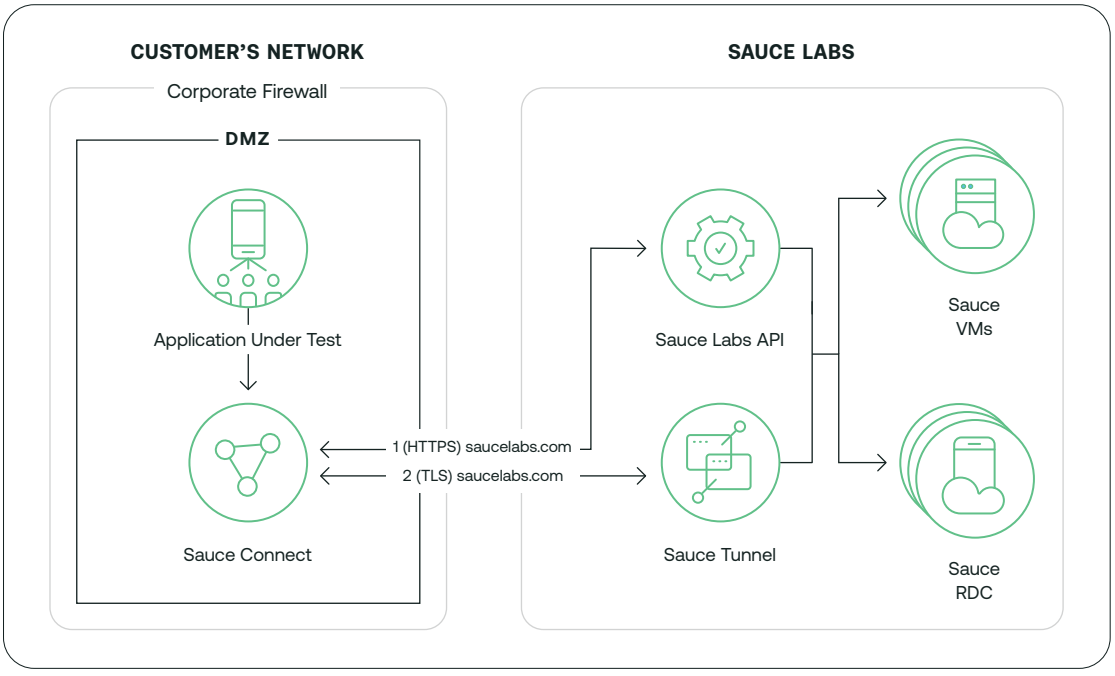


Figure 2: Sauce Connect Proxy, High Level Architecture

Sauce Connect Architecture Overview

From the Sauce Labs side, the Sauce Connect system includes the following components:

- Sauce Connect client
- Sauce Connect server
- Sauce Connect REST API server
- Tunnels Web UI

Here is an overview of how these components interact with a user's environment:

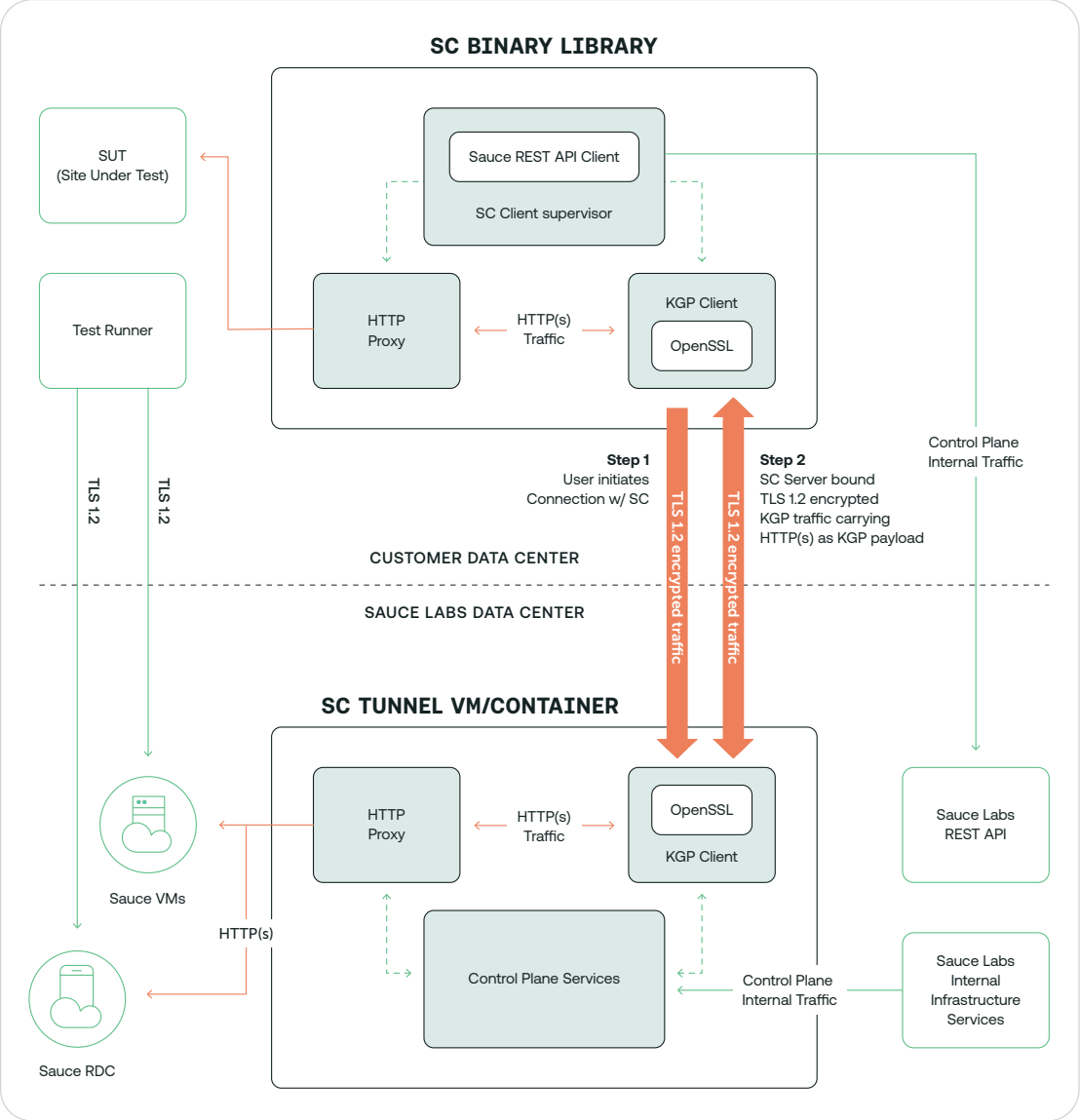


Figure 3: Sauce Connect components interacting with user's environment

DIRECTION	PROTOCOL(S)
Outbound from customer network	HTTPS (TCP/443)
Outbound from customer network	KGP (TCP/443)

Sauce Connect Components Overview

Sauce Connect Client

The Sauce Connect client (also known as SC) is distributed as a single binary that contains several distinct components. These include:

- SC Client controller - this is the “brain” of the SC client. It issues requests to the Sauce Labs REST API, starts all the other included components and ensures that everything is working as expected.
- KGP Client - the client side implementation of KGP, Sauce Labs proprietary protocol.
- HTTP Proxy - this contains a non-caching HTTP proxy that sends HTTP requests coming from tests that run on virtual machines (VMs) or devices on the Sauce Labs infrastructure to the website or application that is hosted inside the user’s firewall (either on an intranet, or a local machine).

All of this is available for download on the Sauce Labs technical documentation website.

Sauce Connect Server

The Sauce Connect Server is a VM (or container) running in Sauce Labs data centers and it includes the following components:

- Tunnel VM Controller - this is the logic that is responsible for configuring the VM, making sure all components are functional, and reporting back to other internal services.
- KGP Server - the server side implementation of KGP, Sauce Labs proprietary protocol. To learn more about this, please reference the Protocol section of this white paper (page 8).
- HTTP Proxy - off the shelf HTTP proxy that is responsible for sending requests from tests running in Sauce Labs VMs or devices to the KGP Server. Note that SSL traffic is “bumped” by default. This can be disabled.

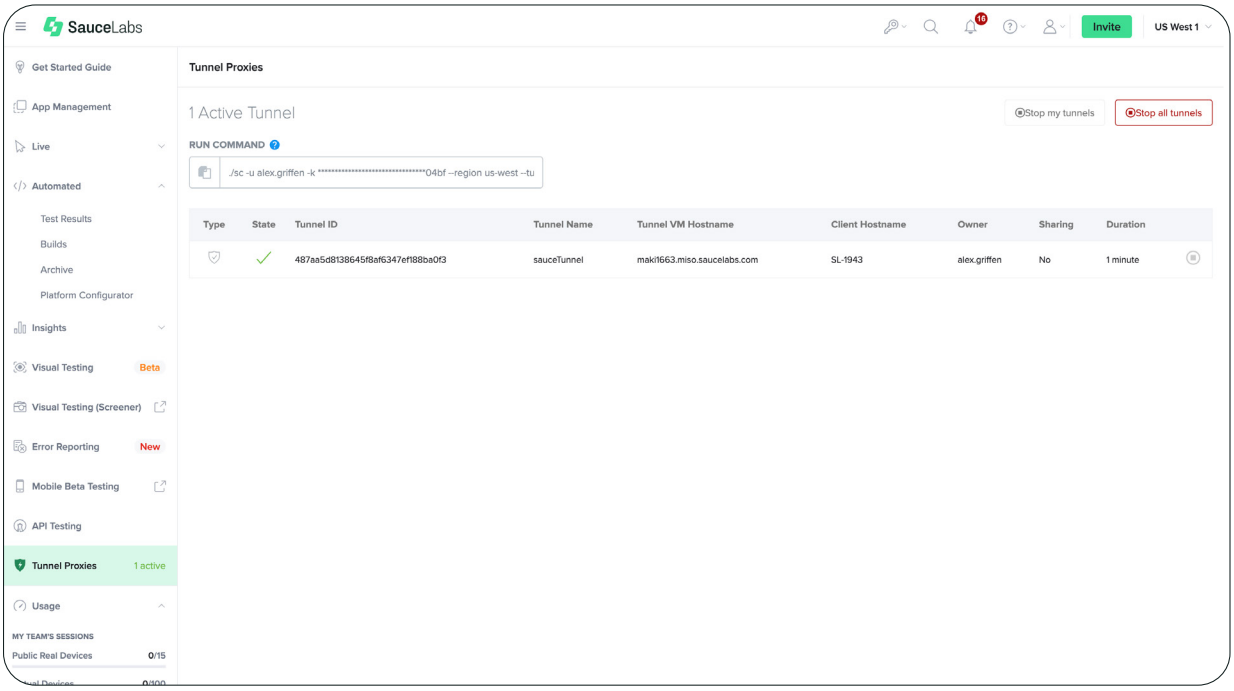
Sauce Labs REST API

The Sauce Labs REST API allows the Sauce Connect client (or any authenticated client) to start and stop tunnels and/or get information about existing tunnels.

To learn more about the Sauce Labs REST API please reference our technical documentation website.

Tunnels Web UI

Users that are executing tests through Sauce Connect can see all information about the tunnels they are running through the web UI. This can be accessed by logging into your Sauce Labs account.



Sauce Connect Security Overview

This section contains more detailed information on the features and procedures that govern Sauce Connect in order to provide the best, most secure experience.

Sauce Labs hosted VMs and real devices

The Sauce Labs infrastructure is configured so that VMs and/or real devices are fully isolated from each other. This means that VMs and/or devices are not able to communicate to any other VMs or devices in our infrastructure. The only exception for this would be tunnel VMs, which are described in the next section. While VMs and devices are allowed to connect to the internet, Sauce Labs also offers a "Lockdown" feature that locks traffic down to that particular user's tunnel only. We only permit allowlist ("whitelist") internal services to communicate to VMs and/or real devices.

Sauce Labs Tunnel VMs security features

When considering the security of Sauce Labs tunnel VMs, it is important to note that while they communicate with the VM or real device running a test, they are fully isolated from each other through traffic filtering. This means that a VM and/or real device being accessed through a tunnel will send HTTPS traffic owned by the customer only, and is not able to communicate with other VMs or real devices in the Sauce Labs cloud. Additionally, Sauce only permits allowlist necessary internal services to communicate with tunnel VMs. Users can customize tunnel VMs from their side, and configure them to direct all traffic through the tunnel, to the internet, or any combination of the two using wildcards. Only user-initiated and authenticated sessions are allowed to utilize that user's tunnel.

Sauce Labs Tunnel communication security features

The Sauce Labs team ensures the security of our tunnels through a number of different methods:

- Certificate status is continually validated by leveraging OCSP
- TLS connections below 1.2 are not permitted
- Sauce tunnels adhere to a minimum standard for allowable cipher suites (at least ECDHE)

Customer Firewall Requirements

In order to successfully run in a customer's environment, the Sauce Connect client requires access to port 443 of the following Sauce Labs domains. This includes control plane requests (HTTPS traffic), as well as the data plane (KGP traffic). It's also important to note that only a user can initiate a tunnel connection from their network to the Sauce Labs cloud, and not the other way around.

DIRECTION	PROTOCOL(S)
Outbound from customer network	HTTPS (TCP/443)
Outbound from customer network	KGP (TCP/443)

To learn more about Sauce Labs public data center endpoints, please reference our technical documentation website.

Sauce Connect Tunneling Protocol - KGP

KGP is an application layer protocol that carries all HTTP(s) traffic as its payload. It is developed and maintained by Sauce Labs, and is used to multiplex established connections for multiple HTTP requests/responses.

KGP packets contain the following components:

- Data packets carrying HTTP(s) traffic
- Control packets, which include:
  - Connection requests
  - Keepalive timers

KGP is preferred over conventional protocols for a number of reasons:

- It's lightweight
- It reconnects when a connection accidentally disconnects
- It ensures that all the data is sent and received, even over an unstable or intermittent connection
- It provides information about the connection state

All KGP packets are encrypted with the industry standard TLS 1.2 protocol. It's also important to note that KGP is not responsible for encryption. Instead, all encryption is processed according to the industry standards defined by the OpenSSL library.

IPSEC VPN

IPSec VPN allows test virtual machines in the Sauce Labs network to access application servers in customer's private network. However, IPSec VPN doesn't allow application servers to access Sauce test VMs. Figure 4 illustrates the architecture of IPSec VPN solution. The solution consists of two components, a VPN connection between two IPSec gateways, and a tunnel gateway.

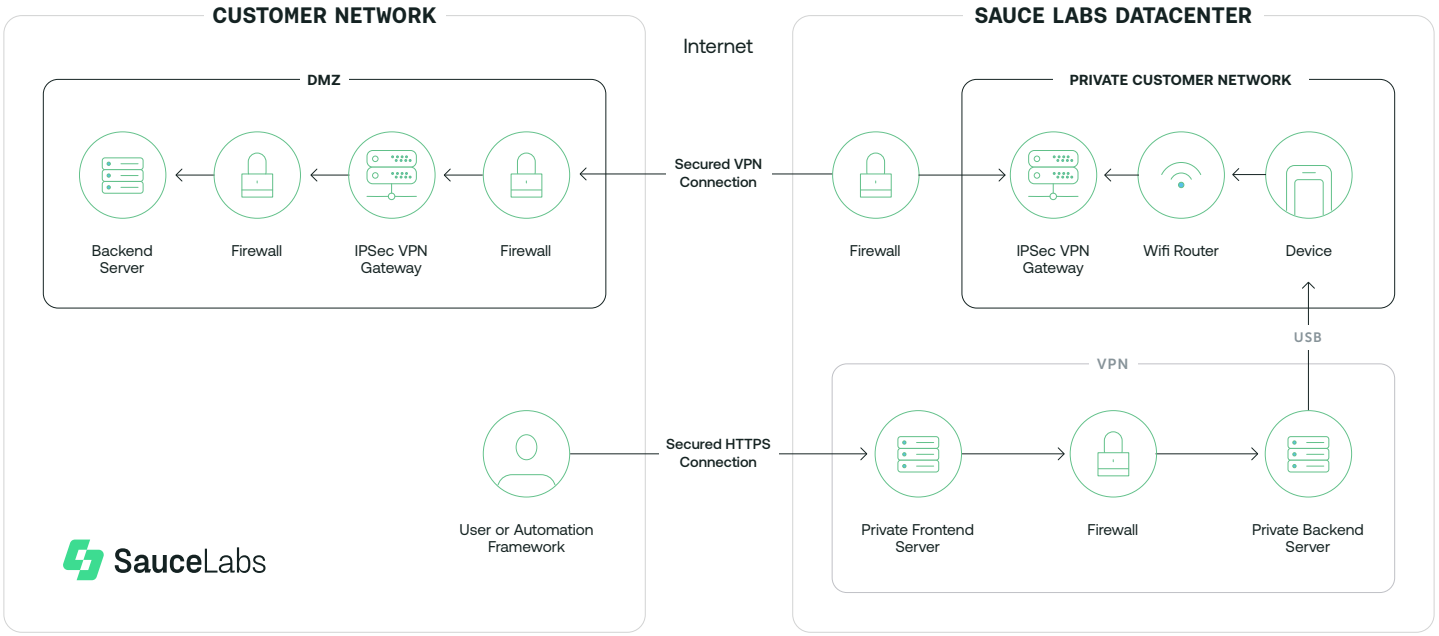


Figure 4: IPSec VPN Data Flow

The tunnel gateway is always on for the lifetime of the IPSec VPN connection, and plays an important role in DNS resolution, routing and security.

The tunnel gateway runs a firewall and only authorized test VMs are allowed to connect through the firewall. Authorized test VMs include:

- Test VMs created by the IPSec VPN tunnel owner
- Test VMs created by accounts with which the tunnel is shared
- All incoming connections from test VMs are blocked

The firewall allows these ports and protocols through the IPSec VPN connection as identified in Figure 5.

DIRECTION	PROTOCOL(S)
Outbound from Sauce	HTTP (TCP/80), HTTPS (TCP/443)
Outbound from Sauce	DNS (UDP/53, TCP/53, TCP/853)
Outbound from Sauce	Web Proxy (TCP/8080, TCP/8443)
Inbound from customer network	BGP (TCP/179)
Inbound from customer network	ICMP

Figure 5: IPSEC VPN Ports

DataCenter Security

Sauce Labs leverages multiple data center locations across the United States and Europe. Sauce Labs also operates within a hybrid-cloud model utilizing multiple cloud providers. Data center partners restrict access to premises, provide surveillance and dedicated, secure cages for Sauce Labs infrastructure.

Datacenter Offerings
We operate in multiple data centers spread across geographic regions. These regions span multiple continents to support Sauce Labs customers' privacy requirements as well as providing high-availability and low-latency response time.

Access Controls

In addition to the physical security, Sauce Labs operations has implemented access control measures restricting access to customers' environments to only those support personnel that have a documented, current business need. Furthermore, all physical and electronic access to data centers is logged and audited routinely.

Application Access
Application access is managed by the customer designated administrator via the Teams function within the Sauce Labs UI. Teams allows for the authorization of individuals, and roles to access the customer's specific instance of Sauce Labs and report data. Additional support for single sign-on (SSO) integration with a customer's existing identity management solution is also available.

Change and Patch Management

Change Control
Sauce Labs change control process is governed by the applicable policy and standard which govern how teams within Sauce Labs assess and deploy required changes to ensure minimal disruption and maximum uptime.

Patch Management
Sauce Labs patch management process is governed by the applicable policy and standard to ensure that all patches, security and otherwise, are deployed in accordance with defined SLAs.

Testing and Scanning

Sauce Labs conducts multiple types of security scans.

Those scans include internal, external, authenticated and unauthenticated scans. These processes are conducted both by Sauce Labs and third-party resources.

Customers are not allowed to conduct their own scans without explicit permission. To request permission customers must work with their Sauce Labs account teams in order to receive the appropriate authorization from the Sauce Labs security team.

Disaster Recovery/Data Backup

Sauce Labs provides backup and redundancy for customer data to ensure full recovery in the event of service disruption or failure.

Our primary data centers are geographically separated co-location facilities with 24x7 physical security, redundant power, HVAC, ISP connections, and fire protection. Primary databases are backed up daily to satisfy our Recovery Point Objective (RPO) of 24 hours maximum. Our Recovery Time Objective (RTO) to restore data in a catastrophic data loss situation is 48 hours.

Business Continuity
Central to the company's business recovery efforts is a requirement that each Sauce Labs business unit develop, test, and maintain recovery plans for each of its core functions. As part of these plans, each business unit identifies critical risks and puts in place the appropriate level of business controls and functionality necessary to mitigate those risks. The resultant plans document the functional requirements needed to re-establish essential business operations. The plans also assess the impact of a business disruption on the company's customers and business partners.

Testing and Validating Disaster Recovery
The Sauce Labs disaster recovery, incident response, contingency planning and recovery procedures are tested and validated annually. Sauce Labs simulates customer disaster declaration scenarios that cover failures and recoveries of each of our critical systems and then analyze the results to continuously improve our operations. Testing is performed periodically, as needed.

Incident Response

Sauce Labs incident response and management includes the Sauce Labs Customer Support, Operations, and Security teams. Team members are on-call 24x7 to respond to customer support requests and incidents.

This team is responsible for managing incident severity, impact, and type classification for effective prioritization of support requests and assignment of qualified experts, with supervised monitoring of support request status and progress.

The Sauce Labs operations team provides contingency and disaster recovery plan activation and escalation, in the event of a major incident affecting multiple customers. In addition, partner and vendor incident response support as needed for triage and resolution. Reporting and analysis of incident response performance metrics are used to achieve SLAs.

Additional Resources

The following wiki links are provided for additional information:

Sauce Labs Documentation

Maintenance Windows for Sauce Labs

Account and Team Management

Setting Up SSO

Sauce Connect Proxy

IPSec VPN

About Sauce Labs

Sauce Labs is the leading provider of continuous test and error reporting solutions that give companies the confidence to develop, deliver and update high quality software at speed. The Sauce DevOps Test Toolchain identifies quality signals in development and production, accelerating the ability to release and update web and mobile applications that look, function and perform exactly as they should on every browser, operating system and device, every single time. Sauce Labs is a privately held company funded by TPG and Riverwood Capital.

For more information, please visit
→ saucelabs.com

saucelabs.com/sign-up

FREE TRIAL

SAUCE LABS INC. - HQ 450 Sansome Street, 9th Floor, San Francisco, Ca Usa 94111

SauceLabs