



SPLASHTOP ENTERPRISE — CLOUD EDITION

# Splashtop Enterprise Security Kit

How Splashtop Enterprise keeps your remote  
sessions secure

# Contents

Select a section to jump straight to it. Each one covers what a control does, why it matters, and how it's applied.

## Introduction

PAGE 3



## At a glance

PAGE 3



01

## Encryption and connection security

PAGE 4



02

## Identity: authenticating your users

PAGE 4



03

## Access origin: controlling where and what

PAGE 5



04

## Entitlement: what each user can reach

PAGE 6



05

## Session control: what happens once connected

PAGE 7



06

## Assurance: logging, recording, and audit

PAGE 8



07

## Data protection and hosting

PAGE 9



08

## Compliance and certification

PAGE 11



## Frequently asked questions

PAGE 11



## Introduction

---

When you connect to a computer remotely, that connection has to be trustworthy in three ways: the channel itself has to be private, the people using it have to be who they say they are, and there has to be a record of what happened. Splashtop Enterprise is built around all three, and gives you direct control over each one.

This document walks through the security capabilities available in Splashtop Enterprise (cloud edition) — what each one does, why it matters, and how it fits together. It's organized as a practical reference you can use to answer the question "how does Splashtop keep our sessions secure?", whether that question is coming from your own team, a customer, or an auditor.

For full technical and architectural detail beyond what's summarized here, see the [Splashtop Cloud Products Security Overview](#). For current certification status, see [splashtop.com/compliance](https://splashtop.com/compliance).

## At a glance

---

Splashtop secures a session through independent layers of control. Because they're independent, no single weak point exposes a session — each layer asks a different question.

| Layer                                | Question it answers                               | Key capabilities                                                                                                                  |
|--------------------------------------|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Encryption &amp; architecture</b> | Is the connection itself private?                 | End-to-end TLS 1.2 + AES-256, no inbound ports, signed software                                                                   |
| <b>Identity</b>                      | Who is logging in?                                | SSO (SAML 2.0 / OIDC), two-step verification, device authentication, password policy and expiration, account lockout              |
| <b>Access origin</b>                 | From where, and from what device?                 | IP address allow list, MAC address allow list                                                                                     |
| <b>Entitlement</b>                   | What are they allowed to reach, and for how long? | Role-based access, group permissions, scheduled access, account expiration                                                        |
| <b>Session control</b>               | What can they do once connected?                  | Granular feature controls, request permission to connect, privacy protections, enforced endpoint configuration, automatic updates |
| <b>Assurance</b>                     | Can we prove what happened?                       | Full activity logging, enforced cloud session recording, SIEM export                                                              |
| <b>Data protection</b>               | Where does our data live?                         | Regional data residency, encrypted storage, multi-tenant logical separation                                                       |

# 1. Encryption and connection security

---

Every Splashtop connection is encrypted end-to-end. Web and API traffic uses HTTPS over TLS 1.2; the session itself is carried over a relay-brokered tunnel using TLS 1.2 and AES-256, where the two connecting devices negotiate their encryption key **directly with each other**. The relay server passes the encrypted traffic through — it never holds the key and cannot decrypt the session.

This has a practical benefit beyond confidentiality: because both the endpoint and the client only ever make *outbound* connections, there's nothing to expose. No inbound firewall rules, no listening ports, no service published to the internet for an attacker to find. If you're replacing an exposed RDP setup or a VPN-plus-remote-desktop arrangement, this removes both the open port and the broad network access a VPN typically grants as a side effect.

A few additional details:

- Every API, relay, and web server presents a CA-signed certificate to prevent man-in-the-middle attacks.
- Passwords are never stored in plain text. They're hashed with SHA-512 using a unique salt per password, and the database itself is encrypted with AES-256, including backups.
- Splashtop client and Streamer software is distributed over HTTPS and is code-signed — Windows binaries with extended-validation certificates, macOS binaries per Apple's developer requirements — so the software's authenticity can be verified before it's installed or allow-listed.

# 2. Identity: authenticating your users

---

## Single Sign-On (SSO)

Splashtop Enterprise supports SSO via SAML 2.0 and OpenID Connect, with pre-built connectors for common identity providers including Microsoft Entra ID, Okta, ADFS, JumpCloud, and OneLogin. Authentication happens against your own directory rather than a separate Splashtop password, which means your existing password policy, conditional access rules, and — most importantly — your offboarding process apply directly to Splashtop access. When someone leaves the organization, removing their directory access removes their Splashtop access.

SCIM and Just-in-Time (JIT) provisioning extend this further: users and groups can be created, grouped, permissioned, and removed automatically from your identity provider, so access stays current without manual upkeep on the Splashtop side.

## Two-step verification (2FA)

Splashtop supports TOTP-based two-step verification using any standard authenticator app (Google Authenticator, Microsoft Authenticator, Cisco Duo Mobile, and others). Once enabled,

logging in requires a time-based one-time code in addition to the password. It can be required for the entire team, or enforced selectively by user, group, or role.

Trusted devices can be managed centrally: administrators can see every device marked as trusted, revoke any of them, and set how long a device stays trusted before it has to re-authenticate.

## **Device authentication**

Independent of 2FA, every login from an unrecognized device or browser triggers a mandatory verification step that confirms the person genuinely controls the email address behind their account. This is what stops a stolen password alone from producing a session — an attacker would also need access to the account holder's mailbox. Device authentication emails can be routed to administrators instead of end users, giving IT explicit approval rights over every new device.

## **Password requirements**

Splashtop enforces password complexity for all accounts: a minimum of 8 characters (up to 64), at least one uppercase letter, one lowercase letter, and one number, and a check against commonly used passwords.

## **Password expiration**

Splashtop Enterprise can require users to update their password on a set schedule, forcing a reset every defined number of days. This closes the risk window on a credential that may have been quietly compromised without the user's knowledge, and is a common requirement in regulated environments where standing credentials can't be left unchanged indefinitely.

## **Account lockout policy**

Accounts can be configured to lock automatically after a defined number of consecutive failed login attempts, for a defined lockout duration, with lockout behavior shared across the web console and the Business app. Locked accounts can be unlocked automatically after the duration expires, or manually by an authorized admin or owner.

## **Session timeouts**

Idle sessions in the web console and Business app can be configured to log out automatically after a set period of inactivity, closing the window in which an unattended, already-authenticated session could be misused.

# **3. Access origin: controlling where and what**

---

## **IP address allow list**

You can restrict logins to the web console, the Business app, or both, to a defined list of IP addresses. Connections from outside that list are refused. This is commonly used to require

that access only happens from the corporate network or a corporate VPN egress, and the web console and Business app scopes can be configured independently.

### **MAC address allow list**

For a tighter requirement — “only company-issued devices may connect” — Splashtop Enterprise can restrict Business app logins to a defined list of device MAC addresses, with the option to block mobile devices entirely. This is a strong policy-enforcement control and pairs well with device management (MDM) tooling for environments that don’t allow a BYOD path. As with any MAC-based control, it should be understood as one layer among several rather than a standalone barrier, since MAC addresses can in principle be altered by someone with local administrative rights on a device.

## **4. Entitlement: what each user can reach**

---

### **Roles**

Splashtop Enterprise separates administrative capability into distinct roles — Owner, Super Admin, Admin, Group Admin, and Member — so day-to-day administration can be delegated without handing over control of billing or team-wide security settings. Group Admins, in particular, can be scoped to manage only the users and computers in specific groups, rather than the whole team.

### **Group-based access permissions**

Access to each computer is granted explicitly. A newly invited user has access to no computers by default unless they’re placed in a group that carries permissions — entitlement is something you grant, not something you have to remove. Grouping lets permissions scale with your organization rather than being managed one user at a time, and where SCIM is in use, group membership can be driven entirely from your identity provider.

### **Scheduled access**

Access can be granted only within defined time windows rather than standing access at all times — useful for contractors, third-party vendors, and shift-based support. Scheduled access is additive to any standing permission a user already has, so for a fully time-bounded user, set their standing permission to “no computers” and grant the schedule alone.

### **Account expiration for temporary access**

User accounts can be given an expiration date, after which the account is automatically disabled — no manual cleanup required. This is designed for contractors, seasonal staff, and external vendors who need access for a defined period. The account isn’t deleted and can be re-enabled at any time by an admin. (This applies to Member-role accounts; Admin accounts are excluded.)

## Authentication at the endpoint

Reaching a computer in the Splashtop console doesn't have to mean being able to use it immediately. A second authentication step can be required at the target machine itself: entering its Windows/Mac login credentials, or entering a security code specific to that computer.

## Request permission to connect

One of the most frequently requested controls: the person physically at the target device can be required to explicitly approve a connection before it's allowed to proceed. When a technician attempts to connect, an on-screen prompt appears at the Streamer (the target device) with a countdown, and the session only opens if the local user accepts it. This puts a human checkpoint in front of every connection to that machine, which matters most for personal or sensitive workstations where the person sitting at the computer should always have the final say over whether someone connects to it.

Behavior when the prompt times out — whether the connection is automatically rejected, automatically allowed, or something in between — is configurable, as is how the prompt behaves when the machine is sitting at a locked login screen with no one there to respond.

# 5. Session control: what happens once connected

---

## Granular controls

Individual session capabilities — remote control, file transfer, copy and paste, remote printing, remote command execution, system tools, and more — can be turned on or off per user, per group, or per role, rather than as a single team-wide switch. This lets you apply different policies to different populations: for example, disabling file transfer and clipboard access broadly, while enabling it for a small, named group that genuinely needs it.

Settings resolve in layers — team default, then group, then individual user override — so policy can be as broad or as specific as you need.

## Session privacy protections

A set of controls protect the physical environment around an endpoint during a session:

- **Mandatory session notification** — a notification always appears on the target computer whenever it's being accessed, which cannot be suppressed. This is a built-in anti-surveillance guarantee.
- **Blank screen** — the target computer's physical display is blanked during the session.
- **Lock keyboard and mouse** — local input is disabled while a session is active.
- **Lock screen on connect / disconnect** — the machine can be locked automatically at the start of a session and returned to the OS lock screen when the session ends.
- **Automatic log-off and idle timeout** — sessions that disconnect unexpectedly or sit idle are handled automatically rather than left open.
- **Watermarking** — customizable text can be overlaid on the session, deterring and helping attribute out-of-band capture such as screen photography.

## Enforced endpoint configuration

Settings that a local user could otherwise change are locked down centrally:

- **Deployment packages** apply your intended configuration — security settings, grouping, naming — at install time, and can be rolled out through your existing tools (Group Policy, Microsoft Intune, Jamf Pro, PDQ, etc.).
- **Streamer setting lock** ensures settings can only be changed by a Splashtop team administrator, not by anyone with local machine administrator rights.
- **Endpoint Policy** lets you configure and update Streamer settings across all deployed endpoints centrally from the web console, without touching the machine directly. Settings governed by policy are greyed out locally until removed from the policy.
- **Automatic updates** keep the Streamer current without manual intervention — new versions roll out silently and progressively across your fleet, so endpoints stay patched against known vulnerabilities without waiting on individual users to update.
- **Version control** lets you cap the version that Streamers and Business Apps are allowed to auto-update to, per platform (Windows, Mac, Linux, Android). Rather than always jumping to the latest release, you can pin your fleet to a specific validated version — useful for testing a new release on a small group before approving it more broadly, or for holding a known-good version in place until a compatibility concern is resolved.

## 6. Assurance: logging, recording, and audit

---

### Activity logging

Every session is logged with start time, end time, duration, the target computer and its IP address, and the user, device, and device IP that connected. Logging covers the full range of session types — remote desktop sessions, file transfer, chat, remote command, system tools,

and support (service desk) sessions — each with its own detailed log. File transfers are logged at the file level — name, size, direction, timestamp — which directly answers the question of what data moved and which way. Team management activity (permission changes, new devices, failed logins) is captured separately, in its own operation log.

| Log type                                                                                                    | Retention                                          |
|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| Session activity logs (remote desktop, file transfer, chat, remote command, system tools, support sessions) | 1 year                                             |
| Operation logs — team management history (web console)                                                      | 3 years                                            |
| SIEM / API export                                                                                           | Continuous — governed by your own retention policy |

## Enforced cloud session recording

By default, session recordings save locally on the technician's own machine — useful, but not an audit control on its own. Splashtop Enterprise offers **centralized cloud recording**, which enforces recording on all sessions, stores the recordings in Splashtop's cloud rather than on a local machine, and makes them available for playback or download from the web console for up to 90 days.

Recordings are treated as highly sensitive. They are encrypted at rest in the same regional database as the rest of your account data (EU, Global, or Oceania — see Section 7), and are not accessible to Splashtop employees. Access is machine-to-machine only, solely to let you play back and download your own recordings from the web console — the sole exception being temporary, monitored troubleshooting access, which requires executive-level approval.

## SIEM integration and open APIs

Session and team logs can be pushed continuously into your SIEM (documented integrations include Splunk, Sumo Logic, Microsoft Sentinel, and Rapid7 InsightIDR), so Splashtop activity is correlated with the rest of your security telemetry rather than reviewed in isolation. RESTful open APIs, including a read-only option, are available for custom reporting and monitoring integrations. Where a supported ticketing platform is in use (ServiceNow, Jira, Zendesk, Freshservice, Freshdesk), session logs can be injected directly into the corresponding ticket.

# 7. Data protection and hosting

## Regional data residency

Splashtop operates separate, independent cloud infrastructure for different regions:

- **Global** infrastructure (serving users outside the EU and Oceania)
- **EU** infrastructure, hosted in Germany, serving European Union users by default
- **Oceania** infrastructure, hosted in Australia, serving select customers in that region

Each region has its own API servers, web servers, and database, with **no data shared between regions**. Data at rest is encrypted in the region of sovereignty, which directly supports data residency requirements common in European and regional procurement processes.

Underlying this regional structure, Splashtop's cloud infrastructure runs across AWS, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI), with cross-provider redundancy built in — so availability doesn't depend on any single cloud provider.

Your account and team data live in the region where your team was originally created — even for a global organization, regardless of where your users and endpoints are actually located. Your account's home region has no effect on connection latency.

Splashtop operates as a multi-tenant environment, with each customer's data logically separated from every other customer's — see Private tenant isolation below for how that separation works in practice.

## Private tenant isolation

Every Splashtop Enterprise account is its own team — a private tenant, by default, for every customer. Endpoints are enrolled and belong to one specific team. Visibility and reachability stop at that boundary: a user can only ever see and connect to the endpoints enrolled in their own team, and reaching an endpoint requires both team membership and an explicit access permission granted by that team's administrators.

This means access is never a property of an endpoint alone — it's always a property of team membership plus an explicit grant, both governed and revocable centrally. There's no shared directory of endpoints across customers and no way to initiate a connection across a tenant boundary.

## Custom FQDN

Splashtop Enterprise supports assigning a custom fully qualified domain name (FQDN) for your team's connection traffic. This lets your network and security teams allow-list a domain specific to your organization in firewall or proxy rules, rather than relying solely on Splashtop's shared domains — useful where policy requires tighter control over what's permitted through outbound filtering.

## 8. Compliance and certification

| Standard                                           | Status                                                                                                                                                                                                               |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ISO/IEC 27001:2022</b>                          | Annual audits                                                                                                                                                                                                        |
| <b>SOC 2 / SOC 3</b>                               | Annual SOC 2 audits; maintains SOC 2 Type 2 and SOC 3 compliance                                                                                                                                                     |
| <b>Penetration testing</b>                         | Independent third-party penetration testing conducted annually                                                                                                                                                       |
| <b>GDPR</b>                                        | Compliant for EU users as both controller and processor; users can access, correct, and remove personal data                                                                                                         |
| <b>CCPA</b>                                        | Compliant for California residents, with equivalent data rights                                                                                                                                                      |
| <b>HIPAA</b>                                       | Not directly applicable — Splashtop transmits session data end-to-end encrypted and does not store or access the content of sessions. The controls in this document help customers meet their own HIPAA obligations. |
| <b>FERPA</b>                                       | Not directly applicable, on the same basis — Splashtop does not access student educational records. The controls here help institutions meet their own FERPA obligations.                                            |
| <b>PCI DSS</b>                                     | Splashtop does not store or process cardholder data as part of the remote session service, and partners exclusively with PCI DSS-compliant payment providers for its own billing and transaction processing.         |
| <b>NIST</b>                                        | Splashtop's access control, patch management, and policy enforcement capabilities are designed to support customer security programs aligned with NIST frameworks.                                                   |
| <b>NIS2, DORA, ENS, TISA, Cyber Resilience Act</b> | Splashtop's access control, audit logging, vulnerability management, and resilience capabilities support customer compliance efforts under these frameworks.                                                         |
| <b>SOX</b>                                         | The audit trails, encryption, authentication, and access controls described in this document support the remote-access controls organizations need for SOX compliance over financial systems.                        |

Current certification status is always available at [splashtop.com/compliance](https://splashtop.com/compliance).

## Frequently asked questions

**Where is our data stored?** In the region serving your account — separate, independent infrastructure exists for the EU (Germany), Oceania (Australia), and the rest of the world, with no data shared between regions.

**If our account data is hosted in one region, will we see latency connecting to machines in another region?** No. Your account data stays in the region where your team was created, but

that's separate from how a session actually connects. A session is carried over a direct, encrypted path between the two connecting devices, not routed through your account's home region — so a team created on EU infrastructure connecting to a machine in the US doesn't experience added latency because of where the account lives.

**What stops a stolen password from being used to access our systems?** Several things, depending on what you've configured: device authentication (an unrecognized device triggers a verification step), two-step verification, IP or MAC address restrictions, and the requirement that the account belong to a team with an explicit permission to the target computer. Where SSO is in use, the credential itself is governed and can be revoked centrally through your identity provider.

**Do we need to open firewall ports or expose anything to the internet?** No. Both the endpoint and the client make outbound-only connections. There's nothing listening, and nothing to scan or attack from outside.

**Can we stop data from leaving a session?** Yes — file transfer, clipboard copy/paste, and remote printing can each be disabled team-wide or scoped to specific users, groups, or roles.

**Can the person at the target computer control whether someone connects to it?** Yes — Request Permission to Connect requires the local user to explicitly approve each connection attempt from an on-screen prompt before the session is allowed to start.

**Can we prove what happened during a session, after the fact?** Yes. Sessions and file transfers are logged in detail, exportable to your SIEM for longer retention, and — where enforced cloud recording is enabled — every session can be recorded centrally and played back.

**Is our environment isolated from other Splashtop customers?** Yes, by default. Every account is a separate team, and only users belonging to your team, with an explicit permission, can see or reach your enrolled endpoints. There's no cross-tenant visibility.

*This document summarizes security capabilities available in Splashtop Enterprise (cloud edition). Product capabilities evolve over time — please confirm current details with your Splashtop representative before relying on a specific control for a compliance requirement. For full architectural detail, see the Splashtop Cloud Products Security Overview at [splashtop.com](https://splashtop.com); for current certifications, see [splashtop.com/compliance](https://splashtop.com/compliance).*