SSH Secure Messaging Cookie and Privacy Policy

SSH Secure Messaging Privacy policy

1. Introduction

'**SSH Secure Messaging**, **SSH Secure Messaging Matrix Services**', '**the SSH Secure Messaging app store**' or '**customer.sshcollabx.net' (or similar domain name)** refers to all services made available at https://ssh.sshcollabx.net or SSH Secure Messaging application and services hosted on customers own instance or on-premises for:

- The **SSH Secure Messaging** app, a closed source Matrix client which you can use to connect to SSH Synapse server that implements the Matrix protocol;
- The purchase, provisioning, configuration, monitoring and management of hosted homeservers and associated services via the **SSH Secure Messaging app store and other channels.**

Where you read '**homeserver**', '**homeservers**' or '**the Homeserver**', it refers to the services configured within **SSH Secure Messaging** which store the user account and personal conversation history, provide additional functionality such as bots and bridges, and (where enabled by the Customer) communicate via the open Matrix decentralised communication protocol with the federated Matrix Network.

Where you read '**the Service**' in this document, it refers to the SSH Secure chat app instances exposed on https://ssh.sshcollabx.net (or subdomains) or "SSH Secure chat application and services hosted on customers own instance or on premise" by SSH Communication Security (trading as SSH).

Where you read 'SSH' or '**we**' or '**us**' below, it refers to **SSH Secure Messaging**, a trading name of SSH Communication Security.

SSH is the Data Controller for your data. We can be contacted as per the details below:

Email: security@ssh.com

Postal address:
Global and EMEA headquarters
SSH Communications Security Oyj
Karvaamokuja 2B, Suite 600
00380 Helsinki

Finland
Tel. +358 20 500 7000

Should you have other questions or concerns about this document, please send us an email at security@ssh.com or contact us from https://www.ssh.com/products/support/report-vulnerability

1.1. Scope of This Document

This document explains how we process personal data, as it relates to:

- **SSH Secure Messaging app users: SSH Secure Messaging** app users use **SSH Secure Messaging** to connect to SSH's synapse server that implements the Matrix Protocol.
- **SSH Secure Messaging Customers: SSH Secure Messaging** Customers use Element Matrix Services (EMS) and SSH software to provision and manage hosted homeservers. Apart from where otherwise noted, this document does not address data protection issues relating to the messaging and file data submitted by Users to the hosted homeserver instances, as this is the legal responsibility of the Customer. For general Terms of Use for Homeserver users, please see: Standard Terms for SSH Secure Collaboration Products.

This document does not cover:

- **Your relationship with identity servers:** you might choose to use an identity server, to allow other Matrix users to discover you via the **SSH Secure Chat** app. This is optional and requires your explicit consent to discover users from your personal contacts. For the identity server made available by us, please see the Identity Server Privacy Notice.

1.2. The Customer and the User

This document is designed to explain Data Protections issues relating to SSH Secure Messaging and Users. Put simply, you're a Customer if you're paying (or otherwise compensating) SSH Secure Messaging to provide a dedicated hosted messaging service. If you have an account registered on a homeserver that you use to send and receive messages, or use the SSH Secure Messaging app to connect any server within the Matrix Protocol, you are a User.

It is possible to be both a Customer and a User, but we encourage you to consider these roles separately when thinking about Data Protection concerns.

1.3. Changes to This Document

Over time we may make changes to this document. If we make a material change we will provide the Customer with reasonable notice prior to the change. We will set forth the date upon which the changes will become effective; any use of SSH Secure Messaging by the Customer, or any use of a hosted homeserver from SSH Secure Messaging by a User will constitute the Customer's acceptance of these changes.

Your access and use of SSH Secure Messaging is always subject to the most current version of this document.

2. Access to Your Data

2.1. What is the legal basis for processing my data and how does this affect my rights under GDP (General Data Protection Regulation)?

2.1.1 Legal Basis for Processing

SSH Secure Messaging has different legal basis for processing, based on which product you are using:

- SSH Secure Messaging **app users:** we collect your IP address when you request access to the SSH Secure Messaging client from our web server. This data is collected on grounds of legitimate interest, as defined in the EU GDPR, to support operational maintenance and to protect against malicious actions against our infrastructure.
- SSH Secure Messaging **customers:** your data is processed as necessary for the performance of the contract as defined in the EU GDPR. This means that we process your data only as necessary to meet our contractual obligations to you, or to engage with you to do something before entering into a contract (such as providing a quote);

2.1.2. Data Ownership - Messaging and File data within hosted homeservers

The Customer can use SSH Secure Messaging Services to provision and manage hosted Matrix homeservers. The Customer owns and controls all messages and files submitted to their homeserver by User accounts registered natively on their homeserver. This ownership does not extend to messages and files submitted over federation or bridging.

This means that, in addition to the usual data access controls defined by the Matrix protocol, all unencrypted messages and files can be accessed by the Customer, and that access is retained even if no User account within the system retains access to the data.

2.1.3 Your rights as Data Subject

You have rights in relation to the personal data we hold about you. Some of these only apply in certain circumstances. Some of these rights are explored in more detail elsewhere in this document. For completeness, your rights under GDPR are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

For more information about these rights, please see the guidance provided by the ICO. If you have any questions or are unsure how to exercise your rights, please contact us at security@ssh.com.

2.2 What information do you collect about me and why?

The information we collect is for the purpose of supporting your management of hosted homeservers through SSH Secure Messaging or to support operational maintenance of the SSH Secure Messaging. We do not profile homeserver Users or their data, but we might profile metadata pertaining to the configuration and management of hosted homeservers so that we can improve our products and services.

2.2.1 Information you provide to us:

We collect information about you when you input it to the SSH Secure Messaging apps or otherwise provide it directly to us.

2.2.1 Information we collect automatically as you use the service:

Location Information

We may collect location data on you, if you choose to use the static or live location sharing features within the SSH Secure Messaging app. This includes your longitude, altitude and latitude data in order to accurately calculate your precise location.

Location data is held within the room in which it is shared, so it will be encrypted in encrypted rooms and not encrypted in rooms where encryption is switched off. You will be shown a disclaimer during your first time using this feature, but please apply caution and consideration when sharing your personal data within the app.

The SSH Secure Messaging clients use the third-party service MapTiler to provide the images used to display maps.

2.4. How do you handle passwords?

We never store password data in plain text; instead they are stored hashed (with at least 12 rounds of bcrypt, including both a salt and a server-side pepper secret). Passwords sent to the server are encrypted using SSL.

It is your sole responsibility to keep your username, password and other sensitive information confidential. Actions taken using your credentials shall be deemed to be actions taken by you, with all consequences including service termination, civil and criminal penalties.

If you become aware of any unauthorised use of your account or any other breach of security, you must notify the relevant department of your organization. Users should manage good password hygiene (e.g. using a password manager).

If you forget your password (and you have registered an email address) you can use the password reset facility to reset it.

2.5. Who else has access to my Data?

We host the SSH Secure Messaging SaaS solution on Wapice OY, specifically:

- Our admin server and deployment server are hosted in a Wapice data center in Helsinki;

Wapice employees may have access to some of this data. Here's Wapice’s privacy policy.

We host the SSH Secure Messaging demo environment on AWS data center in Stockholm.

Amazon employees may have access to some of this data. Here's Amazon's privacy policy. Amazon controls physical access to their locations.

Physical access to our offices and locations uses typical physical access restrictions.

Nobody at SSH, or any of our processors, is able to access encrypted data.

If the customer does not want to host their servers in SSH's contracted data centers, they can host them on the server of their choice (SSH Secure Messaging on-premises option).

2.6. How is my Data protected from another user’s Data?

Each Customer tenant has their own instance runtime in a virtualized environment and all of their SSH Secure Messaging user data resides within the same dedicated cluster provided by trusted service providers and. We use industry best practices to guarantee that only the Customer can access it. In other words, we segment User data via software.

2.7. What should I do if I find a security vulnerability in the service?

If you have discovered a security concern, please email us at security@ssh.com. We'll work with you to make sure that we understand the scope of the issue, and that we fully address your concern. Information security is our highest priority, and we work to address any issues that arise as quickly as possible.

Please act in good faith towards our users' privacy and data during your disclosure. White hat security researchers are always appreciated.

SSH Secure Messaging SSHCookie Policy

1. Our approach to analytics and cookies

SSH Secure Messaging uses cookies and other storage techniques to support key application functionality and to improve your experience of the SSH Secure Messaging applications.

1.1. In our apps

SSH Secure Messaging apps (mobile and web) store data on your device to support essential application functionality. Some examples of this functionality are:

- Maintaining a local copy of your chat history;
- Storing an authentication token so you don't have to login each time you open SSH Secure Messaging;
- Caching data locally to reduce the number of network requests, in order to speed up loading time.

This data is not shared with any third parties.
SSH Secure Messaging Web stores data both in cookies and in your browser's Local Storage.

SSH Secure Messaging Android and Element iOS don't use cookies or local storage but store similar data in native app storage.

1. List of Cookies and Identifiers

1.1. Essential cookies and/or identifiers

These are cookies and/or identifiers that are **'strictly necessary'** and don't require your consent, as we need them for the delivery of the services you are using. This means that we need these cookies to be used for the app or website to function properly, or to comply with security requirements.

Cookies with **'session'** retention expire when logging out.

First party cookies are only stored under the domain of the website that you are currently visiting, and can only track your movements in that domain. Third party cookies are created by a domain other than the website you are visiting, and are used to track your movements across different sites.

Domain	**Coofiie/Identifier type**	**Description**	**Retention**	**First Party/Third Party**
"SSH Secure chat application and services hosted on customers own instance or onpremise" or "<customer-instance>.sshcollabx.net"	Local Storage and IndexedDB	Essential application data	Does not expire	First party