

Security Statement

Revision date: 07 October 2025

Table of Contents

- Introduction4
- About Us.....4
- Security by Design.....5
 - Glossary5
 - Session Establishment & Security6
 - AES 256-Bit End-to-End Encryption6
 - Server Connection7
 - Peer-to-Peer Connection.....7
- Secure Initiation of Support Sessions 11
 - Client ID Generation and Lifecycle 11
 - Brute-Force Attack Mitigation..... 12
- Code Signing 12
- Brute Force Intrusion Protection..... 12
- Blank Screen..... 13
- Transparency and Auditability of Support Sessions 13
 - No Stealth Mode 13
 - Session Recording 13
- Two-Factor Authentication (2FA) 14
- Access Control and Identity..... 14
 - Expert Authentication 14
 - Protection Against Account Compromise 15
 - Expert Authorization 15
 - Credential Protection 15
- Detailed Reporting and Audit 15
- Incident management system..... 16
- Infrastructure Security 17

Data-at-Rest Protection and Privacy Policy..... 17

Introduction

This document describes SetMe's comprehensive approach to securing data and communication sessions in its remote access system. Security is the cornerstone of SetMe's architecture, ensuring protection for both your clients (end users receiving support) and your Experts (support engineers providing assistance).

Key takeaways for decision-makers:

- **End-to-end encryption.** All support sessions employ end-to-end encryption (applied to all data connections). Session keys are negotiated via ECDH (ephemeral Elliptic Curve Diffie–Hellman), and data is encrypted with AES-256, regardless of the transmission path. This ensures our servers cannot access session data – eliminating the possibility of interception or tampering, even by SetMe's own servers.
- **Data privacy and control.** SetMe deliberately limits data collection and retention to only what is necessary for the service to function. Billing data (payment card details) is processed directly by payment processors; SetMe has no access to it. End users who receive support via SetMe are always notified about important Expert actions through UI messages and visual indicators (No Stealth Mode) .
- **Protection against unauthorized access.** SetMe implements multi-factor authentication (2FA), a strict lockout policy for password-guessing attempts, and protection against session ID brute-force protection.
- **High availability and resilience.** The server infrastructure is deployed on Amazon Web Services (AWS) in accordance with AWS Well-Architected best practices. Multi-AZ deployment provides availability of up to 99.99%.
- **Transparency and standards alignment.** Binary applications are signed with digital certificates to guarantee code integrity and authenticity.

Conclusion. SetMe delivers enterprise-grade security, built into every component of the system. This enables your organization to provide technical support while minimizing the risks of data leakage and unauthorized access – and building complete trust with your customers.

About Us

Techinline is a dedicated team of professionals passionate about developing innovative software. Since our inception, we have focused on achieving technical excellence, creating products that seamlessly blend reliability, intuitive design, and top-notch security.

Our solutions empower both individuals and businesses to overcome everyday challenges by resolving issues and simplifying complex processes. We are firm believers that technology should make the world a better place, which is why every product we build is a step toward a more efficient and secure digital future.

Techinline is more than just software. It embodies technology designed with the user in mind.

We focus on a highly intricate task: creating software systems for remote computer access. Our application must work under any circumstances, even if the remote machine's operating system is corrupted. It is precisely during these critical moments that users require a reliable troubleshooting tool the most.

Since 2006, we have accumulated extensive experience in this domain while creating and enhancing FixMe.IT – one of the best remote access solutions on the market. Thousands of individuals and businesses worldwide continue to rely on it, sharing their positive feedback with us.

However, we didn't stop there. A few years ago, we set out on an ambitious journey to create SetMe, a system intended to outshine all existing alternatives. It was a formidable technical challenge, but we succeeded. Today, SetMe stands as the most advanced and reliable remote access solution, built on years of our expertise and the latest technology.

We take pride in building solutions that just work – especially when it matters the most.

Imprint:

SetMe Headquarters

Canada	18 King Street East Suite 1210 Toronto, Ontario M5C 1C4	Email info@techinline.com +1 437 253 7514
United Kingdom	4th Floor 1 Aldermanbury Square London EC2V 7HR	Email info@techinline.com +44 203 769-9927
Ireland	Riverside 4 Third Floor Central Quay Sir John Rogerson's Quay Dublin D02 RR77	Email info@techinline.com
Estonia	Hobujaama 4 Tallinn 10151	Email info@techinline.com

You can find a list of Authorized Partners worldwide at: <https://www.setme.net/Contact-U>

Security by Design

At SetMe we take security very seriously. At SetMe, security isn't a feature we add at the end – it's the foundation we build upon from day one. Every architectural decision, every design choice, every line of code is guided by security-first principles. We apply industry-standard security technologies to protect your data and comply with the strictest security standards.

Glossary

SetMe uses the following terminology when describing remote control session establishment:

- **Client** – a person that requests a connection to their computer for the purpose of getting remote technical assistance.
- **Expert** – a person providing technical support to remote users.

- **SetMe Client** – the application, which is running on the Client side.
- **SetMe Expert Console** – the application used to manage remote clients.
- **Server Connection** – the initial **TLS 1.2+** connection SetMe establishes with an SetMe server.
- **Direct Connection** – an end-to-end encrypted direct connection between SetMe endpoints **DTLS** (Datagram Transport Layer Security) connection, which uses AES-256 encryption in GCM mode.
- **Turn Connection** – an end-to-end encrypted connection (**TLS 1.2**) between a SetMe endpoint and a SetMe TURN server.
- **Control Channel** – the signaling channel responsible for setting up and keeping the connection active between two endpoints. The Remote Desktop Data Stream is only possible as long as the Control Channel is active.
- **Remote Desktop Data Stream** refers to the encrypted data path within a Direct Connection or a TURN relay that transports screen images, file transfers, and audio/video between the SetMe Expert Console and the SetMe Client. This stream accounts for the majority of bandwidth usage and is offloaded to a Direct Connection whenever feasible.
- **Client ID** – a unique identifier used to locate and connect SetMe Client to SetMe Expert Console. Security in a Support Session.

Session Establishment & Security

The session begins when the **SetMe Client** application on the remote computer initiates a **Server Connection**, authenticating the SetMe server using encryption. Upon successful connection, the Client is issued a unique, time-limited **Client ID**.

Concurrently, the **SetMe Expert Console** establishes its own authenticated **Server Connection**. After the connection is up and the Expert is authenticated and authorized, the SetMe system links the **SetMe Client** and **SetMe Expert Console** using the **Client ID**.

The endpoints (**SetMe Expert Console** and **SetMe Client**) then negotiate either a **Direct Connection** or a **TURN Connection**, depending on the network configuration. In both cases, they establish a channel secured with AES-256 symmetric encryption.

The original **Server Connection** stays active only as a **Control Channel** – handling session management and carries no **Remote Desktop data**.

AES 256-Bit End-to-End Encryption

Core Principle

All SetMe support sessions are protected by true end-to-end encryption (E2EE). This means the keys for encrypting the data stream are generated and used exclusively on the Client and Expert devices. SetMe servers cannot access these keys and therefore cannot decrypt the transmitted session traffic.

Cryptographic Standards

All session data is protected using the **AES-256** symmetric encryption algorithm. The AES-256 session keys are securely negotiated between endpoints using the **Diffie–Hellman** key-exchange algorithm. For a **Direct Connection**, peers use **ephemeral Elliptic Curve Diffie–Hellman (ECDHE)**.

Application and Scope

This encryption is used for all data transmitted during a support session, regardless of the transmission path:

- For data relayed via the SetMe server (e.g., commands).
- For data transmitted via a peer-to-peer connection (e.g., remote desktop stream, file transfer), whether established directly or relayed through a TURN server. In the latter case, the TURN server also acts as a blind relay with no access to the data.

Server Connection

A Server Connection is used only for the Control Channel, is relayed via an SetMe server. All information used or transferred during the session (including chat) is temporarily stored in the server's operating memory without anyone having access to this information. Once the data is processed by one session participant, it is entirely removed from the operating memory. Once the session is terminated, all data is entirely removed.

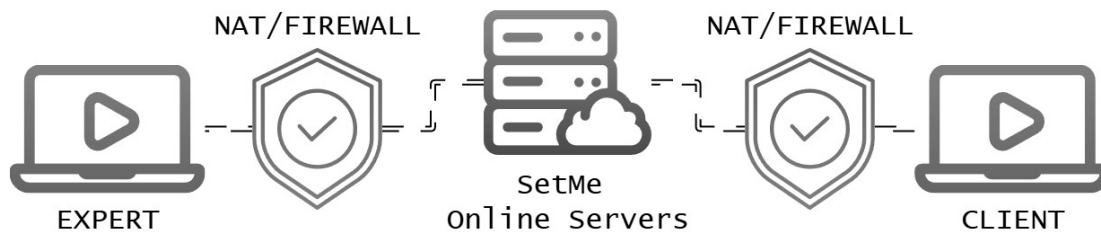


Diagram of Server Connection

Peer-to-Peer Connection

In certain scenarios, a Direct Connection can be established, allowing the data stream to bypass the SetMe TURN server and connect the SetMe Expert Console directly with the SetMe Client. The Control Channel continues to be handled via the Server Connection.

When both Direct and TURN Connections are available, SetMe evaluates session speed and quality and selects the superior option. Following Control Channel setup, SetMe initiates ICE (Interactive Connectivity Establishment) candidate checks to determine Direct availability.

ICE candidates represent potential network addresses that facilitate path discovery across NATs and firewalls. While metadata remains on the SetMe Server (Control Channel over MUX transport), the Remote Desktop Data Stream is offloaded to a **Direct Connection** when feasible. Otherwise, a **TURN connection** is used.

Throughout the ICE process, peers exchange candidates and perform connectivity checks to identify the optimal route. SetMe compares MUX and ICE transports – considering latency (ping) in particular – and chooses the path with the lower latency to ensure optimal performance.

The main types of ICE candidates are:

- Host Candidates
- Server-Reflexive Candidates
- Relay Candidates

Host Candidates

These correspond to the device’s local IP addresses. Host candidates reflect its physical or virtual network interfaces and are used to establish direct connectivity when both endpoints reside on the same LAN.

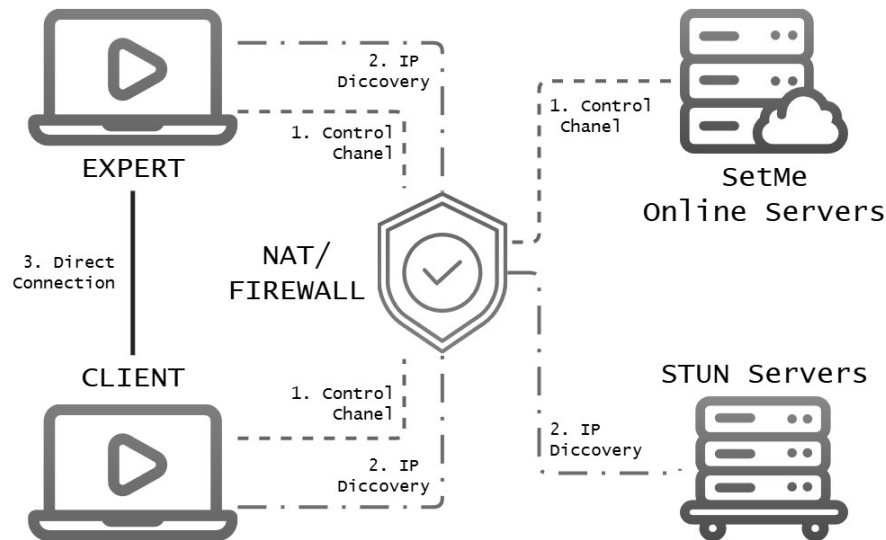


Diagram of Direct Connection via Host Candidates in a Local Area Network (LAN).

The Expert’s PC (host candidate) starts a Control Channel inside the LAN, which traverses NAT to the SetMe Server. The client follows the same pattern, with its connection also crossing NAT to reach the SetMe Server. From there, both the Expert and Client establish paths (IP Discovery) through NAT to a STUN server. After successful discovery, a direct peer-to-peer session (Direct Connection) – the Remote Desktop data stream – is created between the SetMe Expert Console and the SetMe Client.

Server-Reflexive Candidates

Using STUN (Session Traversal Utilities for NAT), a device sends a UDP probe and receives it back “reflected,” which exposes the NAT-mapped external IP and port. Those server-reflexive candidates are then used to negotiate connectivity with remote peers beyond the local network.

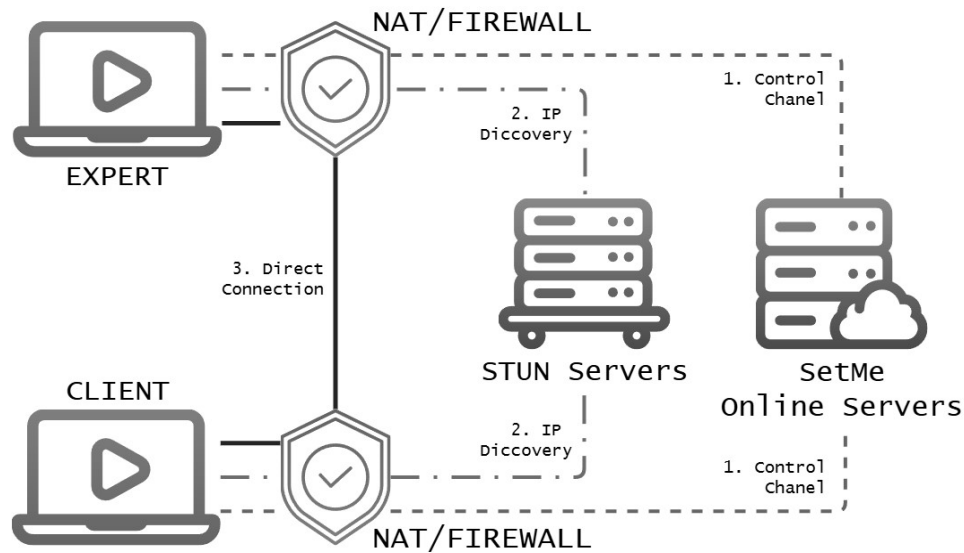


Diagram of Direct Connection via Server-Reflexive Candidates (STUN Server(s)).

For a server-reflexive candidate, the Expert’s Control Channel traverses NAT to the SetMe Server; the client does the same. From both endpoints, a follow-up path (IP Discovery) crosses NAT to a STUN server. After successful discovery, a Direct Connection – the Remote Desktop data stream – is formed between the SetMe Expert Console and the SetMe Client.

Relay Candidates

TURN (Traversal Using Relays around NAT) provides relayed candidates by forwarding media/data through a third-party server. This is used when direct connectivity fails – e.g., under symmetric NAT or restrictive firewall policies – to ensure a functioning connection.

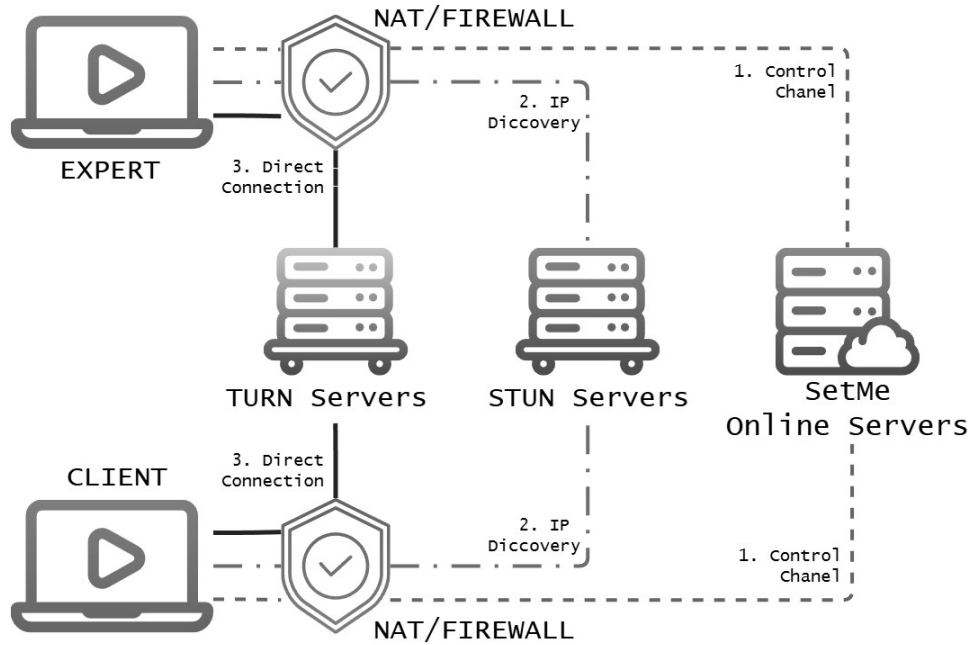


Diagram of Turn Connection via Relay Candidates.

With relay candidates, both the Expert and the Client establish a Control Channel through NAT to the SetMe Server. Each endpoint then performs IP discovery by contacting a STUN server through NAT. In contrast to server-reflexive cases, the Remote Desktop data stream is carried over a **TURN connection**, relayed by a SetMe TURN server between the SetMe Expert Console and the SetMe Client. End-to-end encryption ensures the TURN server functions solely as a packet forwarder and cannot access the content.

Secure Initiation of Support Sessions

The process of establishing a connection between the SetMe Expert Console and the Client is protected by multi-layer mechanisms that ensure a secure, controlled start to each session.

Client ID Generation and Lifecycle

The **Client ID** is a single-use, unique identifier that serves as a secure “token” to start a session.

- The Client ID is generated at random using a cryptographically secure pseudo-random number generator (CSPRNG) and is valid only for a strictly limited period, after which it is automatically invalidated – even if it was never used.
- A Client ID cannot be reused.
- This design prevents interception and unauthorized use of the identifier by an attacker.

As a result, the Client ID provides a secure, one-time, time-bound binding of the connection request to a specific Client device.

Brute-Force Attack Mitigation

SetMe implements a multi-level lockout system in the SetMe Expert Console to protect against SetMe Expert Console ID guessing attacks. The system tracks failed entry attempts per individual account and across the entire subscription. Once the attempt limit is exceeded, connection to the Client is blocked – even if the correct Client ID is entered. This measure effectively neutralizes automated identifier-guessing attacks.

Code Signing

SetMe ensures the integrity and authenticity of its client applications by requiring code signing on all supported platforms. This prevents the execution of modified or substituted versions of the software.

Platform Implementations:

- **macOS:** Applications are signed using a certified Apple Developer ID certificate. The signature is applied to the entire application bundle and to every executable within it, enabling the operating system to perform full integrity verification.
- **Windows:** The following are digitally signed:
 - Installation packages (MSI) and self-extracting archives (SFX)
 - All executables and libraries developed by SetMe

Techinline Ltd protects code-signing private keys using **Hardware Security Modules (HSMs)**. Keys are **non-exportable** and all cryptographic operations occur **inside the HSM**. The HSMs are **tamper-resistant/tamper-evident** and **FIPS 140-3 Level 3 validated** devices, providing hardware-backed key protection consistent with **Zero Trust** principles.

SetMe update mechanism is designed for maximum security by validating the digital signature of every package. This ensures that users always receive and install only authentic, unmodified updates from our official source.

Brute Force Intrusion Protection

Brute-force attacks rely on exhaustive search: automated tools cycle through all feasible password/key combinations. Strong, unique passwords and rate limiting dramatically increase the time required to succeed.

SetMe protects against such intrusion attempts by limiting the number of failed entries within a given time window,

specifically for:

- Expert credentials during sign-in;
- the Client ID during connection to the Client.

When the maximum number of failed attempts is reached, the operation is blocked, preventing further unauthorized access attempts.

Blank Screen

SetMe's blank-screen mode – available to all Experts – obscures the remote display to reduce exposure of sensitive activity. It's designed for tasks requiring elevated privileges and to deter local snooping on devices used for remote work.

Transparency and Auditability of Support Sessions

It is essential that a remote desktop application is designed so it can never run in the background without the Client's knowledge. SetMe ensures full transparency of the remote-access process for the **SetMe Client** and provides the SetMe Expert Console with tools to document actions, fostering trust and enabling internal audits.

No Stealth Mode

A prominent on-screen border alerts the Client that the Expert is currently viewing or controlling the desktop. When the Client uses multiple monitors, the indicator appears only on the monitor selected by the Expert.

By design, SetMe avoids surveillance use cases. It gives users control to mask sensitive or confidential content on their display throughout a support session.

Session Recording

The Expert can enable video recording of a session for subsequent analysis or reporting.

- **Flexible control:** Recording can be started manually by the Expert after the session begins, or launched automatically based on predefined settings.
- **Recording governance:** The Expert can stop recording at any time. Recording stops automatically when viewing/control of the remote desktop ends.

Use cases:

- **Audit and training:** Analyze Expert actions to improve service quality.
- **Documentation:** Create an evidence trail of the work performed.
- **Incident investigation:** Determine the circumstances of issues that occurred during the session.

Two-Factor Authentication (2FA)

Two-factor authentication (2FA) significantly strengthens the protection of your SetMe account by combining two independent verification factors. When 2FA is enabled, after entering valid credentials the system prompts for a one-time security code generated via the Time-based One-time Password (TOTP) algorithm.

Code delivery methods:

- **Authentication app (recommended):** Generate the security code in a mobile authenticator app (Google Authenticator, Microsoft Authenticator, Authy, etc.).
- **Email:** Receive the security code at the email address configured for the account.

Key capabilities:

- **Enhanced session protection:** Automatically terminates all active sessions when 2FA is enabled or its settings are changed, enforcing new security rules immediately.
- **Change control:** Critical 2FA management actions require confirmation with a valid code.
- **Granular administration:** Experts manage 2FA settings for their own accounts; administrators manage 2FA for all accounts within the subscription.
- **Full transparency:** Email notifications are sent for all changes to 2FA settings.

Access Control and Identity

SetMe implements strict, multi-layer access control based on user authentication and authorization.

Expert Authentication

To access SetMe functionality, the **Expert** must complete authentication. Access is granted **only after** successful authentication.

Authentication Methods:

- **Basic username and password.** The Expert signs in with unique credentials created at registration.
- **Automatic authentication with saved data.** When enabled, the system creates and stores a cryptographically protected **Security Stamp** on the Expert's device. This stamp – a “snapshot” of the account state – allows future authentication without re-entering username and password.

Important: Session security is ensured by invalidating the Security Stamp whenever critical account parameters change (e.g., password reset, permission changes, 2FA enable/disable). A full re-authentication is then required to refresh the stamp.

Protection Against Account Compromise

SetMe enforces a strict policy against brute-force attacks:

- **Automatic lockout on suspicious activity.** If the limit of consecutive failed password attempts is exceeded for an account, authentication for that account is automatically blocked for a defined period.
- **Lockout reset.** Access is restored once the lockout period expires.
- **Scope of lockout.** The lockout applies at the account level and covers all SetMe applications accessible to that Expert.

Expert Authorization

After successful authentication, SetMe performs authorization to ensure the user can access only permitted functions and data.

During authorization – especially when signing in to the SetMe Expert Console – the system verifies:

- **Single active session in the SetMe Expert Console.** For security, simultaneous use of the same account in the Expert App from multiple devices is prohibited. If the account is already active, a new sign-in attempt is blocked.
Note: Authorized users can terminate Expert App sessions of other users within the subscription. This enables immediate blocking of potentially compromised accounts upon suspected data leakage and helps enforce company security policies by stopping unauthorized or suspicious activity.
- **Role-Based Access Control (RBAC).** The Expert’s privileges are defined by their assigned role, implementing the principle of least privilege.

Only after all authorization checks pass is the Expert granted access to the system interface according to their permissions.

Credential Protection

Storage method aligns with contemporary industry security standards and provides robust protection for user accounts.

- Passwords set at registration are processed with the **SHA-256** cryptographic hash function (SHA-2 family).
- A unique cryptographic **salt** (random data string) is added to each password.

Detailed Reporting and Audit

SetMe provides users with a powerful tool for building detailed reports. This capability ensures full operational transparency and supports performance analysis, security auditing, and service quality management.

To generate reports, the system uses **only** the data listed in the section “Data-at-Rest Protection and Privacy Policy,” ensuring adherence to the principle of data minimization.

Report Types:

- **Remote Connections:** Detailed information on all support sessions for a selected period. Enables tracking of connection history, duration, participants, and session parameters.
- **Console Usage:** Statistics on Expert sessions in the SetMe Expert Console. Helps monitor activity and time spent in the system.
- **User Performance:** Analytics of Expert performance, including efficiency metrics over the reporting period.

Data Access Control: the scope of data available in a report varies by the user's functional role.

Flexible Configuration and Export: Reports include additional analysis tools such as filtering, sorting, and configurable data views, as well as export with all applied settings preserved for subsequent in-depth review.

Security and Governance Value: the ability to audit all actions in detail through the reporting system enables organizations to:

- Detect anomalous activity and potential security incidents.
- Conduct internal investigations based on complete session histories.
- Ensure compliance with internal policies and external regulatory requirements.
- Analyze the effectiveness of technical support operations.

Incident management system

Remote desktop software providers must maintain an Incident Management System (IMS) to ensure rapid restoration of service following unplanned interruptions.

SetMe employs a proprietary IMS – developed and operated by the SetMe team – to manage incidents end to end. Each incident record typically includes:

- Timeline (UTC)
- Executive summary
- Root cause
- Resolution and recovery
- Corrective and preventive measures
- Other pertinent information

Our IMS supports continuous service levels, availability measurement, thorough documentation of undesired events, and the

reduction of repeat incidents.

Infrastructure Security

The SetMe backend runs on the global Amazon Web Services (AWS) cloud platform. Security and resiliency are achieved through a multi-layer architecture aligned with AWS Well-Architected Framework best practices.

Key aspects:

- **Access control:** Permissions are managed via AWS IAM with mandatory multi-factor authentication (MFA). All operations are protected with end-to-end encryption (TLS 1.2+).
- **Network isolation:** Resources are hosted in a private cloud network (Amazon VPC) with isolation at the subnet and virtual machine levels.
- **High availability:** The system is deployed across multiple Availability Zones. Critical components use **Multi-AZ** deployment, providing automatic failover and availability up to 99.99%.
- **Server updates:** We regularly apply security patches and update server software, accelerating fixes for critical vulnerabilities.

Data-at-Rest Protection and Privacy Policy

SetMe adheres to the principle of data minimization. We retain only the information that is strictly necessary for service operation, support sessions, and report generation.

SetMe stores the following user data required for the normal functioning of the system:

- Account authentication data for the Expert
- Full name of the Expert
- Expert's public IP address
- Expert platform – operating system used by the Expert
- Expert Console version
- Start and end time of the Expert Console session
- Product/Device ID of the Expert's device
- 2FA-email (stored only while email-based 2FA is enabled)
- Country code specified at the time of subscription purchase



- Start and end time of the support session
- Session type – Attended or Unattended
- Client’s public IP address
- Client platform – operating system used by the Client
- Client app version
- Client (session) name
- Client notes – a comment added to the support session by the Expert
- Product/Device ID of the Client’s device
- Computer name of the Client’s machine

SetMe does not have access to billing data (card details, etc.) provided by the user to pay for the subscription (initial, recurring, or plan-change payments). This information is transmitted directly to a certified payment processor and stored in the provider’s trusted vault.