Sertifi | Security Settings Overview

General Security Features

- TLS 1.2 + encryption protects all information flows and communication.
- Fully redundant and replicated in real-time, our solutions operate from secure AT 101 SOC 2 Type 2 and ISO 27001 Compliant Data Facilities. 90 day automatic deactivation for inactive users
- All data and documents are stored using encryption
- Complete audit trail for tasks, including each time a document is accessed and signed, along with the date, IP address, email address, hash record, and signing method.
- Advanced Fraud Tools that automatically assess authorizations for any signs of risk before the authorization is processed.
- 90 day mandatory password reset
- Strong password requirements
- Unmasked card data is only viewable for a maximum of 60 seconds
- 2FA duration for unmasking card information is capped at 24 hours
- Admin cascading roles; different levels of admins have different permissions, so not every admin necessarily has universal control over the portal
- Auto-expiration for documents, uploads, and payment visibility
- IP Address Restrictions, so that only users from particular IPs can access a particular Sertifi portal.

PCI DSS Level 1 Compliance Certified

Sertifi is a validated PCI Compliance Level 1 service provider. Our solution has been independently verified for PCI Level 1 compliance by a PCI Security Standards Council Qualified Security Assessor.

You can view our *PCI DSS Attestation of Compliance on our website*.

PCI DSS Level 1 Compliance is required for all merchants who process more than 6 million transactions per year. This level of compliance also requires strict controls on who can access credit card information, as well as minimizing the amount of information needed for processing transactions.

GDPR/PSD2

Sertifi operates in full compliance with Article 28 of the European Union's General Data Protection Regulation (GDPR). Our products can also use 3D Secure verification technology in order to satisfy regulatory requirements as laid out in the Payment Service Provider Directive.

Security Groups

Within a Sertifi portal, security groups offer admins the ability to precisely control which users are allowed to perform certain functions.

By default, no user accounts can perform security-sensitive actions like unmasking card data. The ability to access confidential information **must be specifically granted by an admin** through adding a user to the security group with the permission to view card-holder data.

Furthermore, admins can allow or prohibit users in a security group from performing the following tasks:

- Inviting participants
- Viewing documents
- Viewing unmasked documents
- Editing uploads
- Adding payments
- Editing payments
- Viewing last 4/payment method
- Sending page defaults
- Viewing GatewayTokenId
- Clone/refund payments
- Viewing payment information (unmasked card info)
- Viewing eConf payment
- Viewing eConf records
- Limiting payment clone amount
- Limiting refund amount