



SecureLine Datasheet

Effortless End-to-End Email Encryption

Secure Emails to Anyone with an Email Address
Receive Secure Emails from Anyone with an Email Address
Automatic Gateway Makes Encryption/Decryption Transparent to Users

Imagine being able to easily send secure messages to any user with an email address—even users with no security systems and no knowledge of email security. Imagine that those same users are able to easily send secure messages to you. Fully integrate it with transparent encryption and decryption, and you have LuxSci's premium secure email service: SecureLine.

How does SecureLine work?

SecureLine seamlessly integrates two distinct modes of secure email communications, SecureLine Escrow and SecureLine PKI, to meet the combined goals of ease of use, maximum security, and communications with anyone, anywhere.

SecureLine Escrow: Secure communications with anyone, anywhere. When composing an email for escrow, the SecureLine-enabled sender provides an authorization question and answer; something that is confidential and known only to the sender, recipient, and other authorized people. When sent, the secure email message is encrypted and stored in a special “escrow” database at LuxSci. The recipient is sent an email notification with the password to the secure message. The recipient then follows a provided link to the “Escrow Portal” to pick up the secure message and to optionally reply back securely to the sender. In order to access the escrowed message, the recipient needs both the password from the notification email and the answer to the sender-provided authorization question (which can be saved for easy repeated use). Thus, SecureLine Escrow allows simple secure communication with anyone who has an email address.

SecureLine PKI: For secure communications with other users of SecureLine and with other people on the Internet who have compatible secure email services, LuxSci's SecureLine also supports a Public Key Infrastructure (PKI) compatible with the S/MIME (Secure MIME) and PGP (Pretty Good Privacy) Public Key technologies. In a public key system, the encrypted message content is sent within the email message to the recipient, instead of being placed in escrow for later retrieval; the recipient can easily decrypt and read these secure messages from within his/her usual email client program or on the server using WebMail. This mode of operation is a more flexible and familiar use of email than the “Escrow” system. However it requires that the recipient be another SecureLine user or someone who utilizes PGP or S/MIME email encryption technologies.

SecureLine empowers users to send and view secure messages in LuxSci's WebMail interface. It also permits licensed users to send and view secure messages in any email client program using SecureLine's optional features of automated outbound and inbound email encryption. SecureLine can function as an “encryption gateway” and a “decryption gateway.”



SecureLine SecureSend Portal: To complement the ability of a SecureLine user being able to send a secure email message to anyone with an email address, the “SecureSend Portal” allows anyone with an email address to send a new secure email message to any SecureLine user. The sender just has to go to <http://securesend.luxsci.com> (or your own private labeled SecureSend domain name), register their email address, and then enter your email address to send you a message with attachments up to 20Mb in size. This service is free and open to anyone. As a SecureLine user, it is easy to both send and receive secure messages to and from anyone.

What security features does SecureLine provide?

Combined with the use of LuxSci’s SSL-based secure information transmission services for WebMail, POP, IMAP, and SMTP, use of SecureLine provides comprehensive email security features which include:

- **End-to-end email content encryption:** Your message content can be encrypted from the time it is sent, to the time it is viewed by the recipient. This includes:
 - Secure transport – no one can eavesdrop on the message content during any stage of transport or delivery.
 - Secure storage – messages are stored encrypted on disk so that they are secure in backups and against administrative disk access.
 - Access by anyone who has an email address – no matter what email service provider they have or email software they use.
 - Integrity of message content is guaranteed.
 - Only the intended recipients of your messages can access them.
- **Digital signatures:** Verify that messages were actually sent by the claimed sender and that messages have not been tampered with or altered.
- **Protection** of your username and password when logging into our services.
- **Tracking and Auditing:** SecureLine Escrow allows you to track the receipt and viewing of messages by your recipients.
- **Retraction:** SecureLine Escrow allows you to retract a message, effectively stopping a recipient from gaining any further access to the message content.
- **Content-Driven Automatic Encryption:** SecureLine allows you to set up rules to automatically encrypt only certain messages based on keywords, phrases, and regular expressions that appear within the text.



What makes SecureLine easy to use?

SecureLine is designed to make it so easy to send and receive secure messages, that complexity, usability, and software compatibility are no longer obstacles to effectively securing your communications.

- All SecureLine features are integrated with LuxSci WebMail, so users can send and view secure messages from anywhere they have access to the Internet, using the same familiar tools for composing and viewing email messages.
- Users can send encrypted messages from any email client connected to LuxSci via our secure SMTP services.
- SecureLine can auto-encrypt messages to your recipients if they are SecureLine users or if information on how to encrypt their mail is stored in the sender's address book(s).
- Use of shared address books makes it easier to have a central location of recipient information (PGP or S/MIME keys, or Escrow questions and answers) accessible to all users.
- Use of personal, domain-wide, and global default Escrow questions and answers makes it a snap to send secure email messages anyone you like using a pre-defined question. This minimizes the setup needed to send secure messages.
- If automatic outbound encryption is enabled, one can determine what happens to messages that cannot be encrypted; these messages can be sent normally, or refused with notifications going back to the sender.
- Users can choose to have SecureLine auto-decrypt PGP and S/MIME messages as they arrive so that messages can be filtered and stored in an unencrypted format in their email folders. Using secure POP or IMAP, the recipient can then access the message securely in any email client.
- Users can easily send a single message securely to multiple recipients who require different modes of email security – i.e. Escrow, PGP, and/or S/MIME. SecureLine automatically picks the best secure communications mode for each recipient, based on the information on file, and manages all of the transmission details for you.
- Our SecureSend portal enables non-users to send secure email messages to SecureLine users.
- Administrators can have all users' PGP or S/MIME keys created automatically. They can enforce the automatic use of encrypted outbound email for all users, standardizing the use of secure email painlessly and automatically.
- Users can manage PGP and S/MIME keys – both personal and external. LuxSci supports simple key generation, as well as import and sharing of external users' keys through shared address books.
- The SecureLine Escrow authorization questions and answers can be memorized in users' personal or shared address books to make it easy to send Escrow messages to the same recipients using the same questions and answers every time.
- SecureLine provides an optional password Escrow service whereby users can have the password to their PGP and/or S/MIME security certificates securely saved in case they are lost. In such a case, LuxSci has a procedure in place to authenticate the user so the password can be retrieved.
- Account administrators can enforce a requirement that their users connect to LuxSci POP, IMAP, SMTP, and WebMail services only over secure connections. This can be configured on a per-user, per-domain, or entire account basis.
- Users can import and export SecureLine Escrow information in the address books to and from CSV files. This makes it easy to edit your user security data offline and then import it into LuxSci for general use.



Feature Details

SecureLine is a feature-rich email encryption system. Below is a detailed list of most of the features included with this service.

Sending Secure Email Messages

- Supported currently only from LuxSci WebMail and LuxSci SMTP
- Supports S/MIME, PGP/MIME, PGP/Inline, and PGP/Inline encrypted attachments.
- Supports sending via SecureLine Escrow
- Complex messages with attachments can be sent securely.
- Send one message to multiple recipients who require any combination of encryption mechanisms
- Adds digital signatures to messages if the sender and recipient have compatible certificates.
- LuxSci's email archival/capturing services, outbound email content monitoring services, and global message tagline service all are compatible with SecureLine.
- Forward and reply to secure messages.
- Disk space used to store messages sent via SecureLine Escrow counts toward the disk usage of the message sender.
- Sender can determine when messages sent via Escrow "expire." At that time the disk space is released and the recipients can no longer access them. This can be specified on a per-recipient basis.



Feature Details (continued)

Viewing Secure Email Messages in WebMail

- Supports viewing of messages that are encoded using S/MIME, PGP/MIME, and PGP/Inline
- Supports Signed-only messages, Encrypted-only messages, and Signed+Encrypted Messages
- Supports PGP/Inline encrypted file attachments
- Does not support nested encryption ... i.e. encrypted messages that are encrypted again

Viewing SecureLine Escrowed Messages

- Escrow portal, where you pickup escrowed messages, is secured via SSL
- Recipient can view messages and download attachments
- Recipient can view a history of message accesses
- Recipient can reply securely back to the message sender. This message can include attachments and can be composed using a rich text editor
- Recipient can securely download the message to his/her computer in a [.eml] file format that is easily readable in programs like Microsoft Outlook Express, Microsoft Outlook, and Mozilla Thunderbird
- Replies to the sender will use the best available or preferred encryption mechanism: S/MIME, PGP, or Escrow — based on the original sender's settings
- Times and dates are shown in time zone of the sender

Automated Outbound Encryption

- Will auto-encrypt messages sent via secure SMTP
- Works with any email client with no additional software needed
- Supports sending to multiple recipients in one message
- Configurable on a per-user, per-domain, or per-account basis
- Forces users to only send via secure SMTP
- Auto-encrypts to other SecureLine users or recipients in the sender's subscribed address book(s) that have security information defined
- For recipients to whom messages cannot be encrypted due to a lack of security information on file, it can send normally, send normally and notify the sender, or not send and not notify the sender



Feature Details (continued)

Automated Inbound Decryption

- Will auto-decrypt messages encrypted using PGP or S/MIME
- Requires that the private key needed for decryption be in the recipient's account and that the password to that private key be stored in the "password escrow" mechanism
- Messages that cannot be decrypted will be passed along as-is
- You can choose when messages are decrypted. I.e. you can have some system or custom filters apply before the message is decrypted (i.e. to save a copy to a separate folder) and apply some filters afterwards

User Security Certificate Management

- Import PGP and S/MIME full public/private key pairs
- Export PGP and S/MIME full public/private key pairs
- Export PGP and S/MIME public keys
- Create new PGP public/private key pairs
- Create new S/MIME public/private key pairs using LuxSci as a S/MIME certificate authority
- LuxSci and Thawte are trusted S/MIME Certificate Authorities. Other popular Certificate Authorities may also be trusted
- Change passwords on private keys
- Optionally escrow passwords on private keys. These are encrypted and stored so only authorized LuxSci staff can access them. This provides optional protection against lost passwords to private keys
- If you have multiple PGP or S/MIME keys, you can specify your default or preferred keys for each type

Public Key Management

- All users automatically have access to the public S/MIME and PGP keys for all other SecureLine users across LuxSci — no special configuration or sharing is needed
- Public PGP and S/MIME keys, as well as Escrow questions and answers can be imported into Address Books
- Information stored in address books can be used when composing or viewing email for encrypting messages for these addresses or validating digital signatures from users with these addresses
- If you have Enterprise Web Aide licenses, you can share address books with public key and escrow information with your users so that they can all take advantage of the same information
- For recipients in your address book, you can configure their preferences of PGP vs. S/MIME vs. Escrow and PGP/MIME vs. PGP/Inline



Feature Details (continued)

Administrative Settings

- Optionally force all messages sent from WebMail by your SecureLine-enabled users to be always encrypted
- Optionally have PGP or S/MIME key pairs auto-generated for all of your SecureLine-enabled users who do not have keys yet. Uses their current WebMail password as the private key password and enables password escrow to allow for lost password retrieval
- Account administrators can optionally force all connections by their users to POP, IMAP, SMTP, and WebMail to be made only securely over SSL
- Configure automatic encryption and/or decryption of email for all SecureLine-enabled users
- Configure a global default Escrow question and answer
- Configure allow and deny lists to define who can send your users messages via the SecureSend portal

User Security Certificate Management

- Account administrators can optionally force all connections by users in a domain to POP, IMAP, SMTP, and WebMail to be made only securely over SSL
- Configure automatic encryption and/or decryption of email for all SecureLine-enabled users in the domain
- Configure a domain-wide default Escrow question and answer (users can also create their own personal default questions and answers)

SecureLine Escrow Reporting

- Senders can track messages sent via SecureLine Escrow
- View details on all messages: when sent, when viewed by the recipient, from what IP address, etc.
- Senders can retract messages so that recipients can no longer access their content
- Senders can extend the expiration dates on messages so that recipients have more time to view them
- Message sorting and searching facilities
- This information is available only to the users and not to administrators or support staff

Further Questions?

Please [contact](#) us if you have any technical questions.

Interested in signing up?

Send us an email, call us, or simply [sign up online](#) using one of our Ultra-Secure Email packages or our [Custom Package Wizard](#). Be sure to select choose SecureLine when prompted.