

eService KANA Secure Messaging



KANA Secure Messaging Top 5 Features

- ☑ Standard email and secure personal portals provide a simple, convenient way to conduct secure communications.
- ☑ Secure messaging is fully embedded in the agent desktop so that messages can be treated confidentially with just one click.
- ☑ User-defined rules automatically enforce corporate security policies for email communications.
- ☑ Multiple layers of security for transmission and user access maintain corporate security standards.
- ☑ Zero-footprint deployment eliminates software downloads or the need for encryption/decryption programs.

Secure Communications Made Simple

For companies that want to enhance the quality of their customer service through convenient Web channels, strict privacy laws present a tough challenge. What today's companies need is a solution that makes it easy to communicate with customers, yet ensures the privacy of those interactions.

KANA Secure Messaging makes confidential communication a breeze by combining the simplicity of email management with secure Web portals.

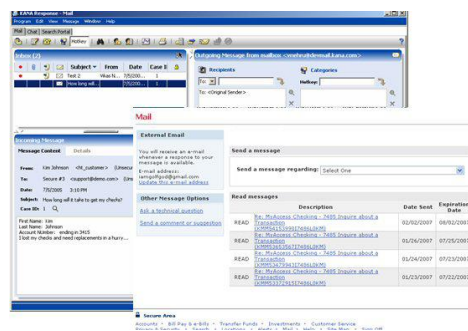
This elegant solution allows your customer service agents to interact securely with customers and partners without using cumbersome, costly encryption/decryption applications.

KANA Secure Messaging does not include any sensitive data in email messages. Instead, the solution uses standard emails that include hyperlinks to a secure, personal portal. The email messages can include links to secured information placed anywhere on your Web site, such as knowledgebase articles.

Multiple layers of security for transmission and user access maintain message privacy including industry-standard HTTPS, authentication, and permissions that manage user actions on the secured Web site. A firewall-friendly architecture prohibits direct client-to-database access.

- Engage in secure communications that do not require customers to install additional software or hardware.
- Automatically enforce corporate communication security policies.
- Exchange confidential messages without any change to current procedures for email processing and management.
- Leverage all of KANA's award-winning email management capabilities to cost-effectively manage rapid growth in secure messaging volume.

KANA Secure Messaging can be used in any combination of confidential and standard email communications. For example, agents can be required to reply to a standard email message using secure messaging. Even auto-replies can be sent confidentially. Customers can also initiate confidential messages using a secure Web form accessible from their personal portals, and they can be prohibited from replying to a secured communication using unsecured email.



KANA Secure Messaging integrates seamlessly into the agent's email desktop, making it simple and quick to treat emails confidentially.

KANA makes secure messaging simple so that you can continue to provide your customers with the convenience of eService while satisfying corporate and government requirements for consumer privacy.

Complete Messaging Security For Compliance with Corporate and Government Regulations

- Secure messaging is automatic. Rules determine which messages should be treated confidentially by scanning incoming message content such as title, text, or alphanumeric pattern.
- A zero-footprint deployment reduces costs. With no software downloads, agents, customers, and partners continue to use their regular email programs and access secure Web portals via standard Web browsers.
- Ease of use is guaranteed. Customers do not have to learn to use new software, nor engage in any actions to encrypt or decrypt messages.
- Agent-training time is non-existent. Secure messaging is built into the agent's desktop so that agents can create confidential messages with just one click.
- Sending and receiving secure emails does not interfere with current operations. As email messages are not encrypted, you can continue to use current best practices for email management, including intercepting messages, analyzing content, applying routing rules, and sending auto-acknowledgments or replies.
- Message security is always maintained. During multi-email communications, KANA Secure Messaging prohibits users from replying to secure messages over unsecured channels.
- Authentication and authorization effectively manage user access. Recipients must authenticate at the portal before they can view protected messages. You can further manage user access to data and resources within the portal via individual and group permissions.
- Corporate security standards for communication are maintained. Messages are delivered to Web portals via standard HTTPS with 64 or 128-bit encryption.
- High-volume message growth is easily accommodated. The flexible Web architecture provides proven scalability and reliability to handle exponential increases in secure message volume with ease.
- Secure emails encourage customer self-service. With confidential information delivered via secure Web portals, KANA Secure Messaging provides an excellent opportunity to promote customer adoption of self-service.

Message Type	May Be Sent Via	
	Standard Email	KANA Secure Messaging
Customer-initiated message	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Agent-initiated message	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Customer reply to standard email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Customer reply to secure message	Can be prohibited	<input checked="" type="checkbox"/>
Agent reply to standard email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Agent reply to secure message	Can be prohibited	<input checked="" type="checkbox"/>

Whether messages are initiated by customers or agents, KANA Secure Messaging treats email interactions confidentially with messages routed through a secure Web portal.

BARCLAYS USES KANA SECURE MESSAGING FOR UP TO 4 MILLION PERSONAL, PREMIER AND LOCAL BUSINESS CUSTOMERS IN THE UK.

KANA Secure Messaging meets the needs of enterprises looking for a solution that:

- Offers transparency to all users and works in heterogeneous client environments to make it easy for consumers to do business with you.
- Is compatible with existing policies and operations for message processing and can co-exist with the current technology infrastructure.
- Provides secure communications that can be easily and cost-effectively scaled to manage growth in message volume.