Secure E-mail

This document describes how secure e-mail applies to TeamHealth's corporate security infrastructure, and how to manage secure messages from TeamHealth associates. If you have any questions, please contact TeamHealth via telephone at 865.693.1000.

E-mail has become a key communication tool in the health-care industry and many others, providing a simple method to quickly share information across the office and around the world. However, e-mail traffic between organizations suffers from a wide variety of security vulnerabilities. Consider the following scenarios:

- You send an e-mail message to a colleague who works at a client hospital. How do you really know the message reached its intended recipient? What if it was read or modified before it reached its destination?
- You receive a message from a colleague at a commercial insurance payer. How can you verify the identity of the sender? How do you know it hasn't been altered en route?
- Your colleague's e-mail system was hacked, and all of the messages in her inbox were compromised. Were any of those messages sent by you? Who now has access to that sensitive information?

Encrypting your e-mail messages will keep even the most dedicated hackers from intercepting and reading your private communications. Using encryption, the contents of the message are scrambled and locked in such a way that only the intended recipient can supply the key and read the message. Additionally, the recipient can verify the sender's digital signature to ensure the message's authenticity. This combination creates a powerful end-to-end security solution for communications.

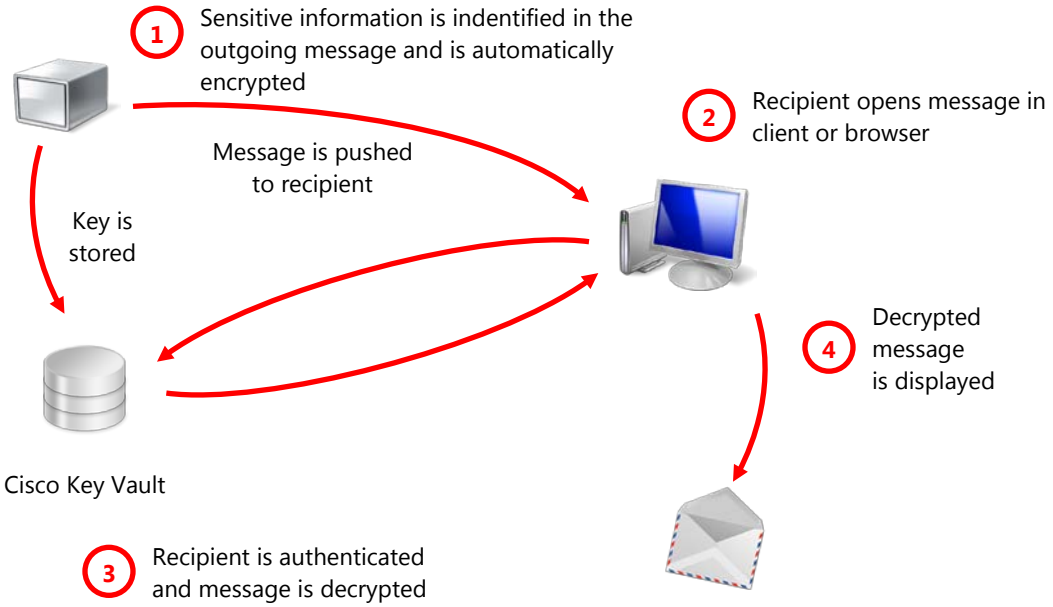
Does it make sense to encrypt *every* outgoing message? No, but those containing sensitive data should be encrypted, particularly if they are transmitted outside of the TeamHealth corporate network. According to corporate policy, "sensitive, confidential, or proprietary information including Protected Health Information (PHI), must never be sent over the Internet unless it has first been encrypted by approved methods."

Within our corporate network, encryption is readily available and widely used, but what about e-mail messages sent to recipients outside our organization? When you mail a confidential parcel, you trust a delivery service to transport the parcel securely and verify the recipient's identity. Our trusted "delivery service" for external e-mail is the Cisco Registered Envelope Service (CRES).

Cisco Registered Envelope Service (CRES)

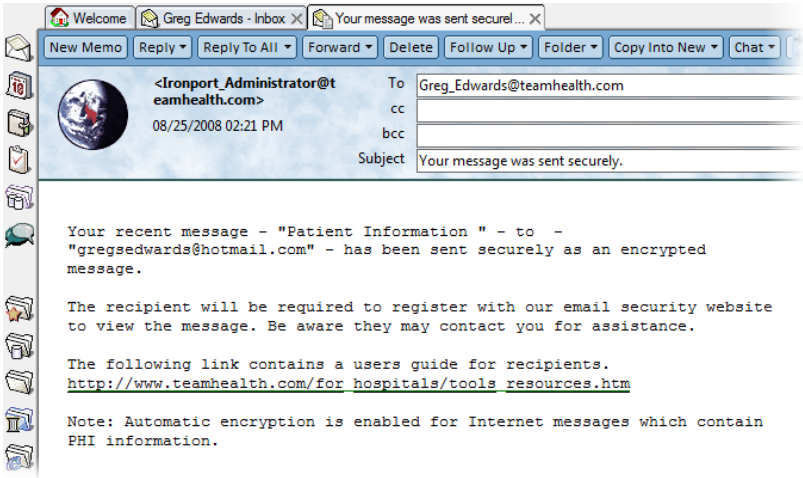
TeamHealth employs CRES to effectively provide seamless message encryption outside our organization. CRES combines a sophisticated scanning engine that can automatically identify and encrypt a message that includes sensitive information, and an online key vault that verifies the recipient's identity and decrypts the message.

Here's how it works:

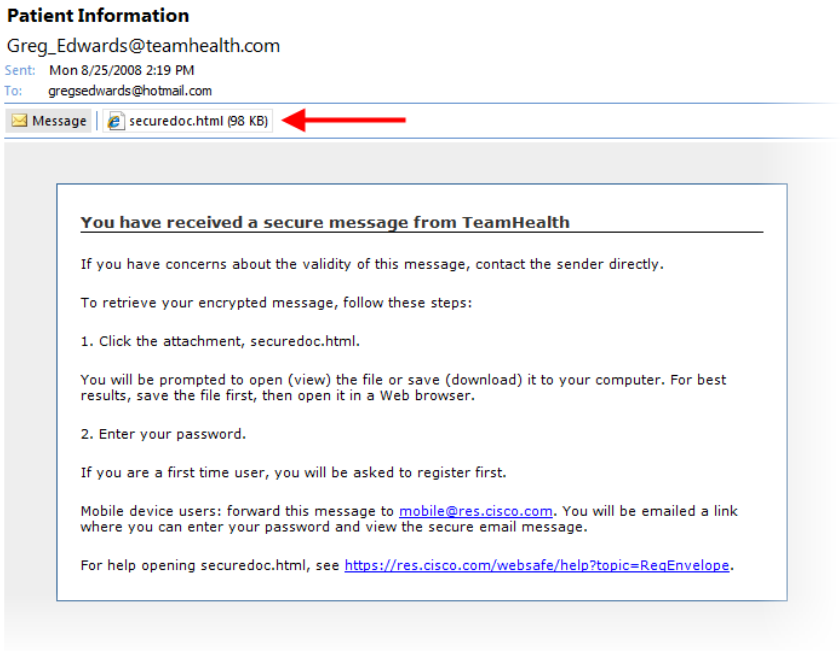


It may seem complicated at first glance, but the process is streamlined for both senders and recipients.

1. When a TeamHealth associate sends a message that contains sensitive information, IronPort automatically encrypts the message and notifies the sender.



2. As the recipient, you receive the secure message. Access to encrypted messages is managed using CRES.

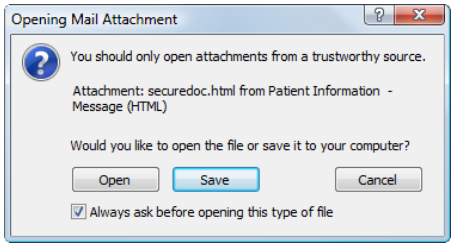


Note: CRES delivers the security notification and attaches an encrypted version of the original message, so sensitive information is never stored by a third-party hosting service. Only the recipient has access to the message content.

3. To decrypt the message, open the **securedoc.html** attachment.

Note: Outlook users may need to right-click the attachment and click **Open**.

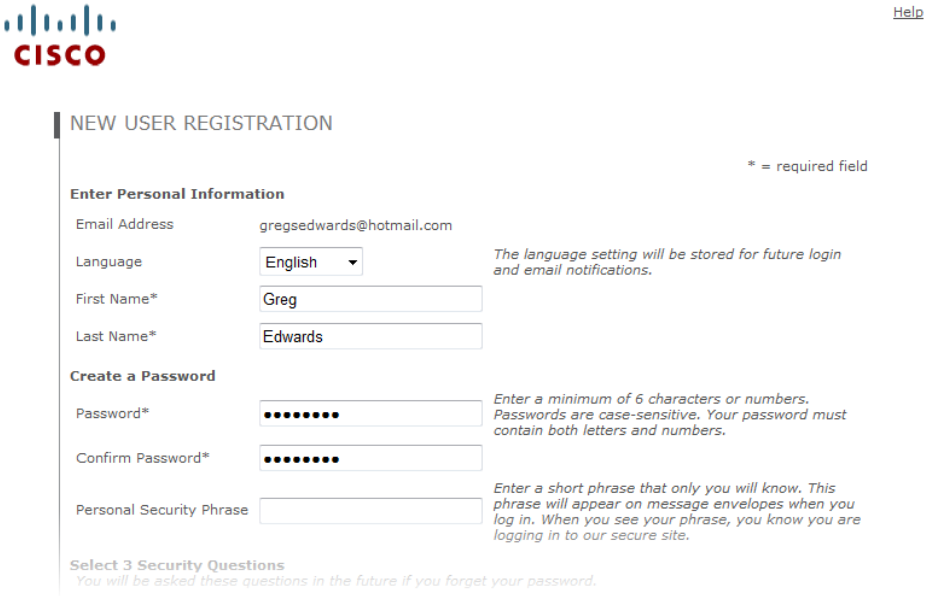
A confirmation window may be displayed.



4. Click **Open**. The Secure Registered Envelope page is displayed in your default browser.

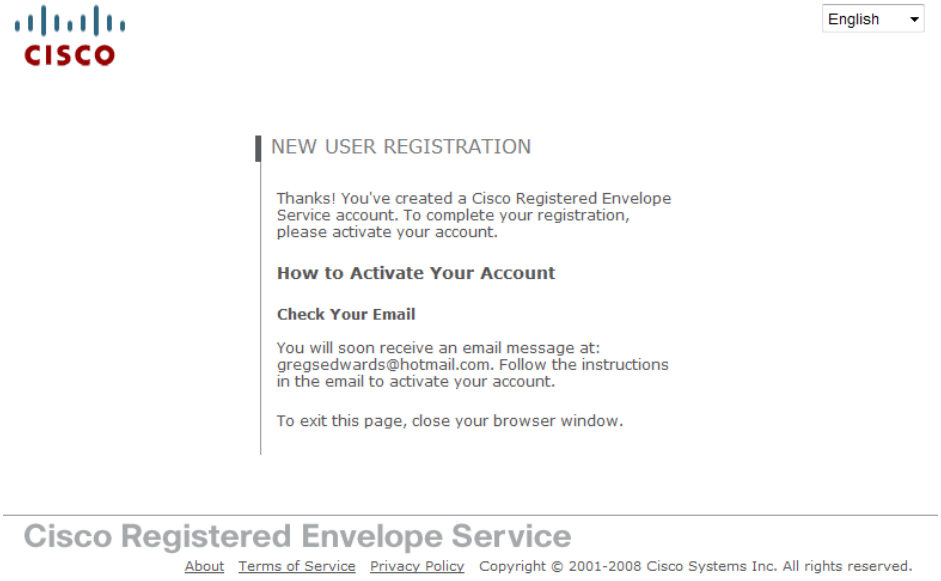
Note: If your e-mail address has already been registered, skip to step 10.

5. If you have not yet registered for the service, click **Register**. The Cisco New User Registration page is displayed.

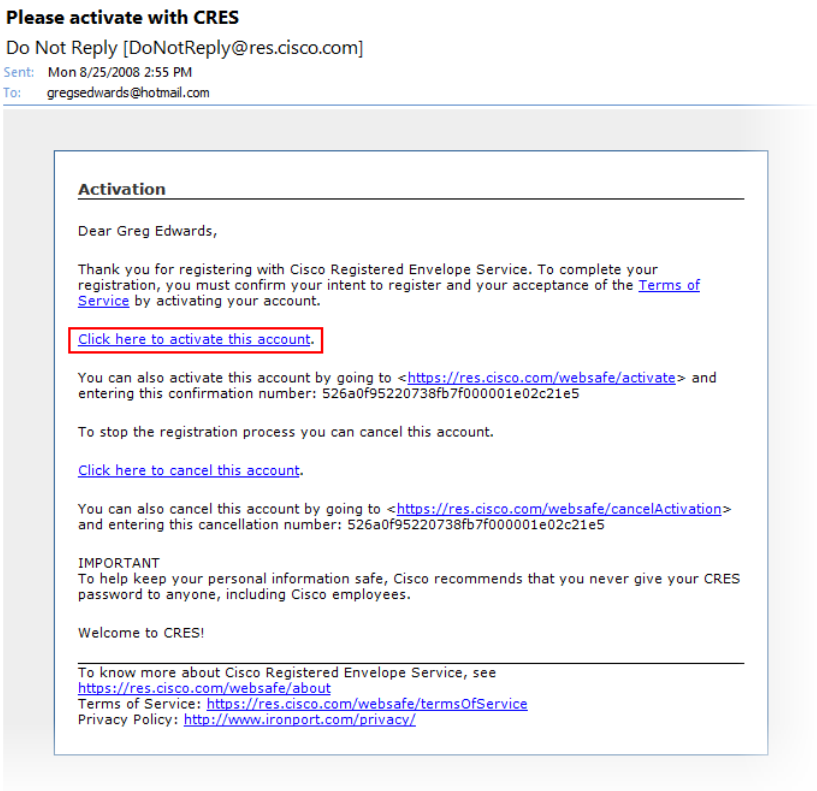


Note: For added security, the e-mail address field is automatically populated with address of the original message recipient. This prevents the encrypted message from being redirected to another e-mail address.

6. Enter the required fields, and click **Register** at the bottom of the page. A confirmation page is displayed, which indicates that a confirmation message will be sent to your e-mail address to verify your identity.

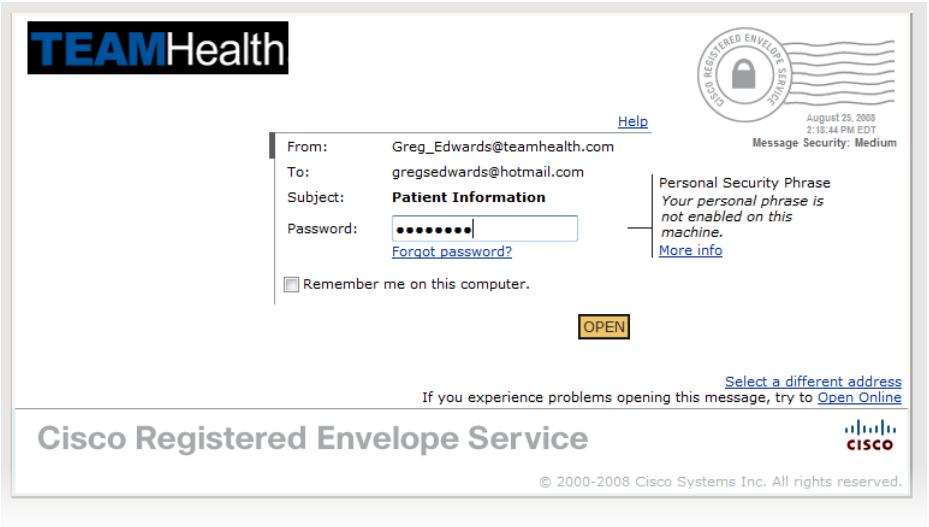


7. Navigate to your e-mail program, and open the message entitled "Please activate with CRES". The message contains a link to activate your account.



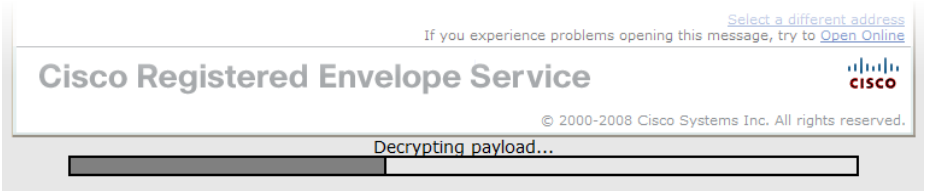
8. Click the link to activate your account. The Cisco New User Registration page is displayed, and your account is activated.

9. Return to the original secure message.



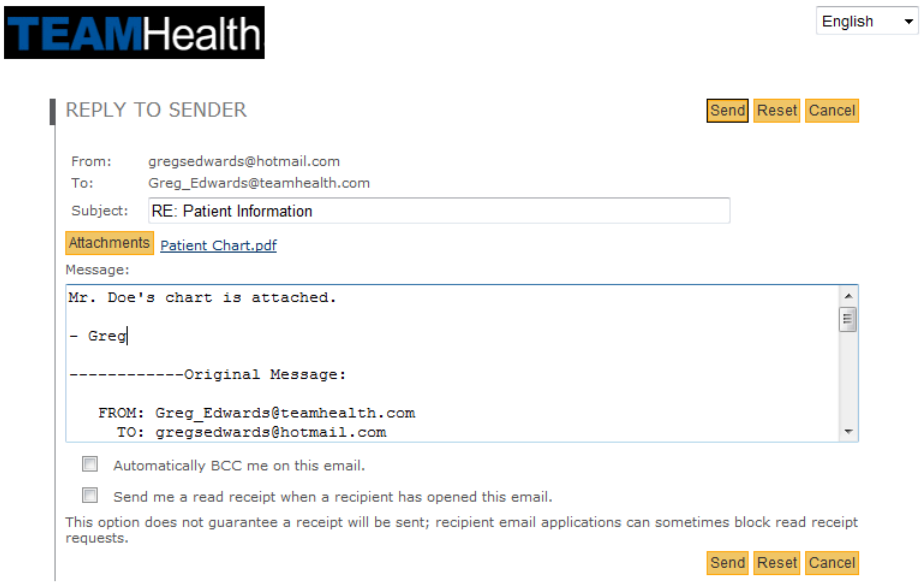
Once registration is complete, the **Register** button is automatically replaced with the **Open** button.

10. Enter your password and click **Open**. The secure message is decrypted.



The decrypted message contents are displayed in the default browser.

11. To send an encrypted response to the sender, click **Reply** in the secure message header. A secure message reply form is displayed.



12. Compose the reply message, attach files as necessary, and click **Send**. The secure reply message is sent and a confirmation window is displayed.

Notices

DISCLAIMER: While TeamHealth Training takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The names used in this manual are fictitious. Any resemblance to current or future companies is purely coincidental. We do not believe we have used anyone's name without consent in creating this material, but if we have, please notify us and we will change the name in the next revision.

Use of screenshots, photographs of another entity's product, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by, nor any affiliation of such entity with TeamHealth Training. This manual may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). We are not responsible for the availability of, or the content located on or through, any External Site. Please contact the Knoxville HelpDesk if you have any concerns regarding such links or External Sites.

TRADEMARK NOTICES: TeamHealth and the TeamHealth logo are registered trademarks of TeamHealth. Cisco and the Cisco logo are registered trademarks of Cisco Systems, Inc.

Copyright © 2008 TeamHealth Training. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. TeamHealth's World Wide Web site is located at www.teamhealth.com.

This manual conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner.