Email Encryption FAQs

Which messages are encrypted?

Currently encryption occurs on outgoing messages that are manually tagged with ENCRYPT or [SEND SECURE] in the subject line. To encrypt messages **manually** use the **SEND SECURE** button.

What kind of encryption does IronPort provide? Will emails between OA's environment and the agencies be encrypted? Is internal email encrypted?

IronPort provides outbound email encryption to external recipients only. All of the Exchange servers reside at the Enterprise Data Center. All internal email traffic between the Exchange servers is encrypted using TLS encryption protocol, however Email between the Exchange servers and the Outlook clients will be encrypted only if the Outlook client is Outlook 2007 and above.

How will the "Send Secure" button get to users' Outlook clients?

Two different .msi files need to be pushed out to clients using SCCM. The .msi file is different for Outlook 2000-2002(XP) and Outlook 2003/2007/2010, so there are two different packages. The Enterprise SCCM team has created SCCM packages that are available at the following links:

Outlook 2000/2002(XP) - OutlookDesktopFlag_6.3.0_011.msi

Outlook 2003/2007/2010 - OutlookDesktopFlag_6.5.0_003.msi

Do the passwords for external users registered in the email encryption system expire after a certain amount of time?

Yes, unused registrations will expire after **14 days** and used registrations are set to expire after **60 days**. Password expiration in the email encryption will comply with the ITB

How can people manually encrypt messages?

1 - Type [SEND SECURE] or ENCRYPT in the subject line of the email

2- Click on the Send Secure button in Outlook, rather than the normal Send button

What happens if the recipient's organization strips HTML attachments?

Most organizations don't, but if they do and this becomes a problem, there are "fallback" mechanisms we can set up in IronPort to ensure that these people can receive encrypted emails sent to them from the Commonwealth. Please contact the Enterprise Messaging team if you encounter this problem.

What happens if a registered user forgets his/her password?

There is a "forgot your password" link, in the messages sent to recipients of encrypted emails. They can click on that link, if they forget their passwords. Users are sent a temporary password that allows them to log into the system, reset their password, and access the encrypted email.

Can encrypted emails be sent and received via Blackberry?

Users with commonwealth issued Blackberry devices are able to send encrypted emails manually by including [SEND SECURE] or ENCRYPT in the subject line of the emails they send from those devices.

Incoming encrypted reply emails will be decrypted before the messages reach the user's inbox, so they will look like normal email messages.

External users accessing encrypted emails using a Blackberry or other mobile devices will be able to do so as long as their device supports HTML well enough to open the attachment.

Can encrypted emails be sent via Outlook Webmail?

Yes, by using the subject line and encryption methods outlined above.

How much load volume can the IronPort system handle?

The IronPort appliances in the cloud can handle extremely high volumes of outgoing encrypted emails. However, the size of each message can affect the time it takes to be delivered to the recipient and the time it takes the recipient to open and decrypt on the receiving end. Users opening large encrypted emails may experience some latency.

Will Outlook read receipts be affected?

Commonwealth users who request 'read receipts' for encrypted emails will receive them when the recipient opens the initial email that contains the link to the actual content of the email. Outlook 'read receipts' confirm that the email itself was received, but not that the encrypted content was read.

Is a notification sent to the sender if the recipient doesn't receive a message?

Not by default; if there is a need, we can configure the system to notify senders if encrypted emails are not opened within a certain amount of time.

How can recipients of encrypted emails save these messages?

They can be saved in their native format.

How will recipients know that encrypted emails are legitimate?

Initially, users will have to either rely on the fact that they were expecting a message from the person who sent the email to them, or they call the sender to verify the legitimacy of the email.

Once the recipient has registered in the IronPort system for the first time, subsequent encrypted emails received will contain their "personal security phrase" to prove legitimacy.

Can anyone register in the IronPort system?

Anyone who receives a secure email in their inbox can register. In cases where an email is mistakenly sent to an incorrect user, the agency should let the Enterprise Exchange team know so they can "expire" the message to keep the unintended recipient from opening the

encrypted email. This should help mitigate the risk of incorrect users opening secure emails.

If there's a security breech, can agencies gain access to emails that were sent encrypted for e-discovery?

Yes, they will need to contact the Enterprise Exchange Team to do this, but it is possible.

Can we monitor who is sending encrypted emails?

Yes.

Is there a cost to agencies to use email encryption?

No, the IronPort solution was paid for in full by OA/OIT and agencies will not be asked to pay for its use. If agencies have specific requirements they would like to implement in future phases, then there is a possibility that they would incur some cost, if Cisco IronPort professional services would be required to implement the changes.

Can agencies send bulk "no reply" encrypted emails?

Yes.

Are there any plans to use IronPort to encrypt internal email traffic?

No, IronPort is the standard for encrypting emails going from the Commonwealth email system to external recipients. The standard for internal email encryption is Outlook 2007 and above. Once users have the Outlook client, emails they send to other internal users with the Outlook will be encrypted by default.

Do IronPort password requirements meet commonwealth minimum password standards?

Yes, IronPort security requirements are set to match the commonwealth's policy.

I sent an encrypted email to wrong email address. What do I do now?

Contact the Exchange Team immediately to have the message locked.

Will TLS connections to existing email domains remain in place or will they be decommissioned?

Current TLS connections will remain in place. Emails encrypted by IronPort will use a TLS tunnel to connect to the domains to which we have TLS connections.

If LMS training is to be provided, will it be made available to people outside the commonwealth?

No, external users will not have access to the LMS training; however, we will be putting together a short user information sheet that they can link to from the encrypted emails they

receive. Information on how to register in the system and how to access encrypted emails they receive from the commonwealth is provided.

When will a finished user guide be available for distribution to our customers and employees?

The EMT IronPort Email Encryption User Guide is available on the Enterprise Exchange Team's portal site is available and can be distributed to customers and employees.

We use ZIX encryption, how can we make use of the [SEND SECURE] button?

In order to use both ZIX and the [SEND SECURE] button you will need to uninstall the ZIX component, install the [SEND SECURE] button, then reinstall the ZIX component.

How large an attachment can I send?

You can send an attachment of up to 10 Megs. The use of encryption, can possibly double the size of the message; as a result, the recipients email system may reject the message as too large.

How will I know if a message I sent got encrypted?

You will receive a notification for each encrypted message, confirming the encryption.

Is there a way to encrypt meeting requests with sensitive documents attached?

Meeting requests will encrypt by any of the standard methods.

I had Outlook XP installed and added the Send Secure button, then I upgraded to later version of Outlook and the button is not there. How do I get the button back?

You will need to uninstall the Outlook XP add-in through Add/ Remove Programs in the Control Panel, and then install the add-in for the version of Outlook that is installed.

How can I open the link on my BlackBerry mobile device?

If the link doesn't open, you may need to change the TLS option:

Click Options > Security Options > TLS

Change default TLS from proxy to handheld.

How do I encrypt attachments?

Attachments are encrypted along with the email.

What category should I use when submitting an incident for encryption?

Agency: Global
Category: Enterprise Exchange Support
Type: Exchange
Item: Email Encryption

When I try to open a message, I enter my password but I don't see the "open" button?

Security settings may prevent the download of the "Open" graphic. You should see a red "**X**" indicating where the graphic should be, you can click the red "x" and the message will open.

I would like to take E-LMS training and I have not been notified that I'm registered. Will I receive a notification?

Everyone has been registered in the commonwealth but only certain users identified by the agencies have been notified. Agencies can contact LMS admin to identify who has taken the training so far.

Is there support for the Send Secure button in Windows 7?

Yes.