McAfee® SaaS Email Encryption FAQ

GENERAL INFO

What is McAfee® SaaS Email Encryption?
McAfee SaaS Email Encryption is a cloud-based email security solution that protects organizations from the loss of confidential data, and helps to ensure compliance with privacy and security regulations. The McAfee® SaaS Email Protection service feature offers easy administration through the SaaS Control Console, and a host of convenient and intuitive ways to send, receive and view encrypted email.

How are the primary benefits of SaaS Email Encryption?
SaaS Email Encryption will help customers to:

- Enforce email encryption without disrupting the day-to-day workflow
- Protect the organization from liabilities associated with privacy regulations
- Ensure ease of use and keeps the underlying encryption complexities hidden for the end user
- Monitor all messages via outbound content filtering to ensure compliance
- Extend encryption services internationally via a recipient pick-up portal that supports 14 languages including: English; German; Spanish; French; French (Canadian); Italian; Dutch; Japanese; Korean; Portuguese (Brazilian); Portuguese (Portugal); Russian; Chinese (Traditional); Chinese (Taiwanese)

When will the new feature available?
SaaS Email Encryption will be available for sale on Monday, June 21, by all partners within the McAfee SaaS PartnerFocus program and by the former MX Logic direct sales team.

What is the price for the new feature?
The MSRP for SaaS Email Encryption is $1.75 per month/$18.96 per year for SaaS PartnerFocus and MXL direct sales. Partner-group specific pricing sheets and order forms can be found on the McAfee SaaS PartnerFocus in **Sales & Marketing > Sales Tools**.

Can SaaS Email Encryption be sold as a stand-alone service?
No, it is an optional feature in the following SaaS Email Protection Service packages and SaaS Service Suites:

- McAfee SaaS Email Protection & Continuity
- McAfee SaaS Email Protection
- MX Enterprise Defense (Also requires Outbound Filtering)
- McAfee SaaS Web & Email Security with Archiving
- McAfee SaaS Email Security & Archiving Suite
- McAfee SaaS Web & Email Protection Suite

Customers on legacy MX Logic packages, such as MX Defense I, II or III, will need to upgrade to one of the packages or Service Suites listed above in order to purchase SaaS Email Encryption.

Are there any seat limitations or conditions?
There are no seat minimums for SaaS PartnerFocus and MXL direct sales. Generally, seats for SaaS Email Encryption should equal those for the customer's SaaS Email Protection service. Contact your

PartnerFocus Channel Manager if a particular deal requires selling SaaS Email Encryption to a subset of SaaS Email Protection service seats.

TECHNOLOGY

Who is providing the underlying encryption technology?
The McAfee SaaS-branded solution is provided by Echoworx, the leading provider of cloud-based encryption services for complete enterprise email and data protection.

Will Echoworx be referenced in sales materials?
No, but while the service will not be co-branded as "powered by Echoworx", you can reference the relationship in conversations with customers and prospects.

What kind of encryption is used in the service?
The encryption portal utilizes standards-based encryption technology including:

- Public Key Infrastructure (PKI)
- Secure / Multipurpose Internet Mail Extensions (S/MIME)
- X.509 certificates
- Triple Data Encryption Standard (3DES)
- Support for standard algorithms, including AES-256 and the use of RSA-1024 bit keys

The Encrypted Message Pick-up Portal utilizes 128-bit Secure Sockets Layer (SSL).

What is PKI (Public Key Infrastructure)?
Public Key Infrastructure or PKI is the industry-trusted and proven encryption technology that allows email users to digitally encrypt email message ensuring that only the intended recipient can read the message. Messages are decrypted using two keys (small files); one is public and is used by the sender to encrypt the message, and the other is private and is used by the recipient to decrypt the message.

USING SaaS EMAIL ENCRYPTION

How does McAfee SaaS Email Encryption work for service administrators and users?

Administrator*:* Through the SaaS Control Console, a Customer Administrator can set, review and customize their organization's privacy policies so confidential content is automatically encrypted.

The administrator can add a new action – Encrypt Message – to any of the existing Outbound Policies>Content content groups, or to custom content groups that they create. Any outbound emails with content that triggers the policy will be sent from the McAfee SaaS system to the encryption portal. For example, an administrator can create a content policy for emails that include the word "confidential," and set the action on the content group to Encrypt Message. Any message containing the word "confidential" would then be automatically processed for encryption.

In addition, via a new checkbox, an administrator can set a policy whereby any message that contains "[encrypt]" (bracket-encrypt-close bracket] in the subject line or message body will automatically be sent to the encryption portal.

Sender: If a user sends a message that includes content which triggers the Encrypt Message action within a content group, the message will be automatically sent to the encryption portal. If the user's administrator has also enabled encryption per inclusion of [encrypt] (see above), the user can insert [encrypt] in either the subject line or message body to force encryption of the message.

How does the recipient read the encrypted message?
The recipient can view the message either directly from their inbox using the Secure Message Reader, or more commonly, after login on the Encrypted Message Pick-up Portal.

- **Encrypted Message Pick-up Portal:** The recipient is notified that an encrypted email has arrived for them in the Pick-Up Portal and that they have 14 days to view it. First time users are then required to register and create a password. Once the account has been set up, all subsequent messages to the recipient can be decrypted on the Pick-Up Portal with the user-specific password. Within the portal they can reply to the message, which is sent via TLS back to the original sender. Messages cannot be forwarded from the portal

- **Secure Message Reader:** Using the Secure Message Reader – after initial registration - encrypted messages arrive in the user's inbox as an attachment to a regular email. The user can decrypt the message attachment by inputting a password.

Can an administrator create a number-content rule for numbers other than credit card numbers (Visa, Master Card, Discover, American Express) or U.S. Social Security numbers?
No. That functionality is not part of this deployment

Are there any restrictions to downloading the Secure Message Reader?
It is necessary for the user to have admin rights on their computers in order to download the Reader. For organizations that do not allow users to download executable files, SaaS Email Encryption supports the most common methods for an IT organization to push the Reader out to users. Furthermore, the Reader is only available on Microsoft Windows-based computers and cannot be installed on a portable device.

Which browsers work with SaaS Email Encryption?
SaaS Email Encryption works with all of the most popular browsers including Internet Explorer, Firefox, Safari and Chrome.

Aside from setting up applicable content groups and actions to encrypt, what does a customer need to do to enable SaaS Email Encryption?
McAfee recommends that all customers with SaaS Email Encryption enable TLS on their mail servers to ensure security between the server and the McAfee SaaS system.

Is there a limit to the number of emails an organization can encrypt?
No, there is not a limit.

Can multiple entities within an organization share the same deployment?
Yes, McAfee SaaS Email Encryption allows for multiple domain deployment. This enables multiple domain names (or multiple organizations) to share the same deployment with separate sets of rules.

Will messages sent from Blackberry and other mobile clients be encrypted?

Yes, any message sent from a mobile device that passes through the McAfee SaaS system is subject to your organization's outbound email encryption policies.

Can I encrypt messages using Outlook Web Access (OWA) / other webmail clients?
Yes, messages sent from an Outlook Web Access (OWA) client or any other web-based email client that pass through the SaaS Email Protection system is subject to your organization's outbound email encryption policies.

How long does it take to encrypt an email?
Text messages are encrypted in as little as one to two seconds, depending on size. Messages with attachments, particularly those sized 1 MB or above, are encrypted and delivered within one to two minutes.

Will attachments be scanned for encryption-policy text?
No, only content in the message is scanned per content policy.

Are the actual attachments encrypted?
Yes, every byte within the attachment is encrypted.

Does encryption add to the size of attachments?
Yes, encryption will add to the size of the attachment at a ratio of approximately 1 to 1.8, meaning the size of a 1 MB attachment will increase to roughly 1.8 MB after encryption.

Can I use my smart phone to access messages in the Encrypted Message Pick-up Portal even if I have already downloaded the Secure Message Reader onto my office computer?
Yes, you can always access messages off of the Pick-up Portal, regardless of whether you have installed the Reader on a computer. To change your delivery options, click on the Options tab within the Secure Message Reader or Encrypted Message Pick-up Portal.

Can I forward a message via the Pick-up Portal?
No. That functionality is not part of this deployment.

Can I forward a message that has been delivered to my inbox for viewing via the Reader?
Yes, theoretically you can forward the message as is. However, the recipient would be unable to read the encrypted attachment, even if they have a Reader too, due to different authentication credentials.

Will senders be notified when an encrypted message is read?
Yes, the SaaS Email Encryption system will send a notification email to the sender when the recipient retrieves the encrypted message. The sender will also receive three to five notifications during the 14-day period in which the message is active on the encryption portal if the recipient has not retrieved the message.

Do the Encrypted Message Pick-up Portal and Secure Message Reader support languages other than English?
Yes, both recipient options support 14 languages, listed below, and can be set using the Options tab.

- English
- Spanish
- French (European)

- Chinese (simplified)
- Chinese (Taiwan)
- Dutch
- German
- Italian
- Japanese
- Korean
- Portuguese (European)
- Portuguese (Brazilian)
- Russian

SAAS EMAIL ENCRYPTION AND OTHER FEATURES

How does SaaS Email Encryption work with the McAfee® SaaS Email Archiving service?
SaaS Email Encryption and the McAfee SaaS Email Archiving service work independently of each other. Outbound messages are journaled on the customer mail server, and copies of the journaled messages are ingested into McAfee SaaS Email Archiving, prior to being delivered to the encryption portal. This ensures that an accurate record of all outbound emails is kept to meet compliance needs.

How does SaaS Email Encryption work with SaaS Email Continuity?
Outage-period messages sent from the web-based Email Continuity portal on the SaaS Control Console receive the same content and anti-virus scanning as in normal operations. Any messages that match a content policy or that contain [encrypt] will be automatically encrypted. The user will also be able to use the Email Continuity portal to view notifications sent by the SaaS Email Encryption system.