ExchangeDefender

ExchangeDefender™
Encryption

v 1.0

May 16,2011

Audience: Staff

For the latest version of this document please go to:
http://www.exchangedefender.com/docs

Table of Contents

ExchangeDefender Overview

ExchangeDefender features a built-in encryption solution that can satisfy many government and regulatory compliance requirements for data security. Compliant with such standards as FINRA, SOX, SEC and HIPAA, ExchangeDefender Encryption meets or exceeds business encryption needs with the unparalleled ease of use.

ExchangeDefender is a cloud-based productivity suite that delivers security, business continuity, regulatory compliance and business information management tools. ExchangeDefender technology provides the following benefits: SPAM filtering, virus filtering, malware protection, DDoS protection, business continuity, Outlook integration, email SPAM quarantine reports, transparent and regulatory encryption, web filtering, desktop alerts, SMTP service monitoring and managed services, Exchange 2010 archive access, long term compliance archiving, HTML5 mobile application and much more. The wide range of solutions in our portfolio is tightly integrated to give users seamless experience across different tasks and be flexible enough for the unique way in which each company implements ExchangeDefender.

ExchangeDefender guides are intended to introduce basic service concepts and offer productivity tips that our customers have shared with us. If you have any suggestions or questions please don't hesitate to contact us.

ExchangeDefender Encryption

Encryption, in it's simplest form takes data in it's original plain text format and uses mathematical algorithms and encryption keys to transform it into unreadable text that cannot be easily interpreted or processed by hackers and packet sniffers.

ExchangeDefender Encryption takes email messages sent from you and encrypts their contents so that the messages cannot be read by anyone other than the intended recipient. Instead of getting plain text messages that could be intercepted by management, packet sniffers or IT administrators, recipients get a link to retrieve their message in a safe and secure ExchangeDefender Encryption environment.

ExchangeDefender Encryption provides a secure and audited trail for messages and assures corporate policies are established and honored, on-demand encryption is enforced when necessary and that the contents of the message are protected from third parties according to the level that meets the business requirements.

Sending an Encrypted Email

Sending encrypted messages with ExchangeDefender is simple and convenient. There is no software to install or configure, just put [ENCRYPT] or [CLEARENCRYPT] in the subject of the message and it will be encrypted all the way to the recipient of the message. Be cautious how you use the encryption:

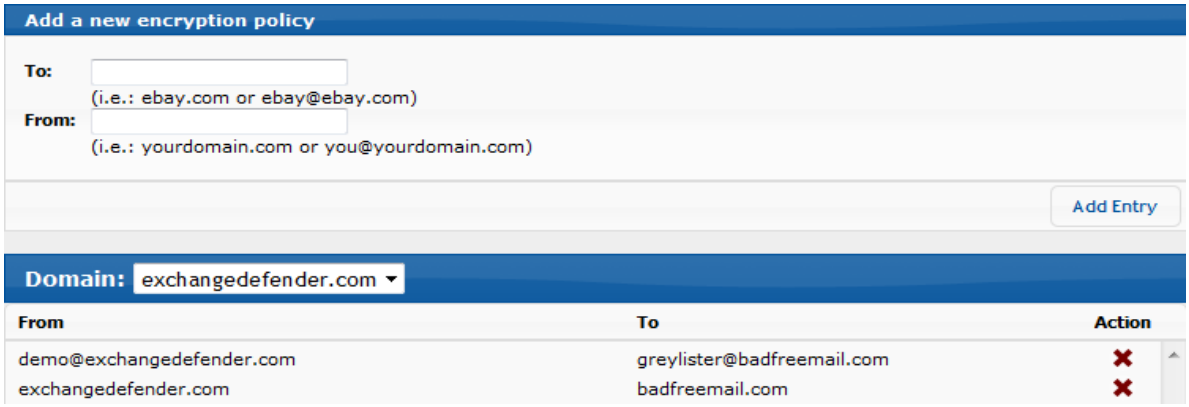
[ENCRYPT] – Strong encryption that requires the recipient to enroll in the free ExchangeDefender Encryption Site to password protect any future messages.

[CLEARENCRYPT] – Strong encryption without password protection.

It's as simple as that.

Encryption Policies & Management

ExchangeDefender Encryption service can be used on-demand (by typing [ENCRYPT] or [CLEARENCRYPT] in the subject) or can be established through company policies. Your IT Solution Provider or IT administrator can create policies that always encrypt messages going from a specific sender to a specific recipient.



For example, a policy can be put in place so that messages going from the in-house book keeper to the payroll company are always encrypted because they contain account number data.

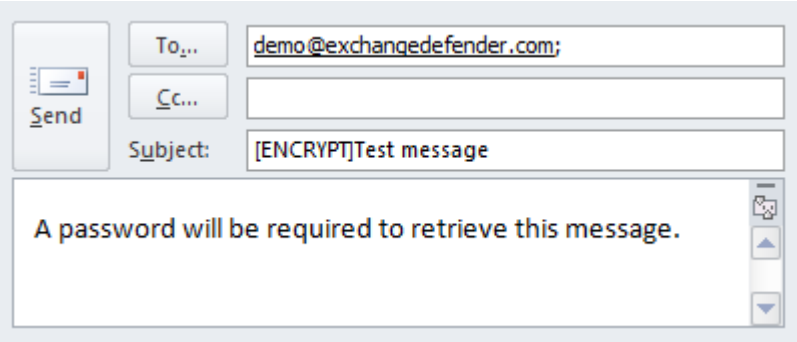
To manage policies please contact your IT Solution Provider and ask them to setup a policy in the ExchangeDefender Administrative Portal under the Configuration tab → Encryption.

Note: If this service is not enabled in your ExchangeDefender Administrative Portal, please contact your IT Service Provider.

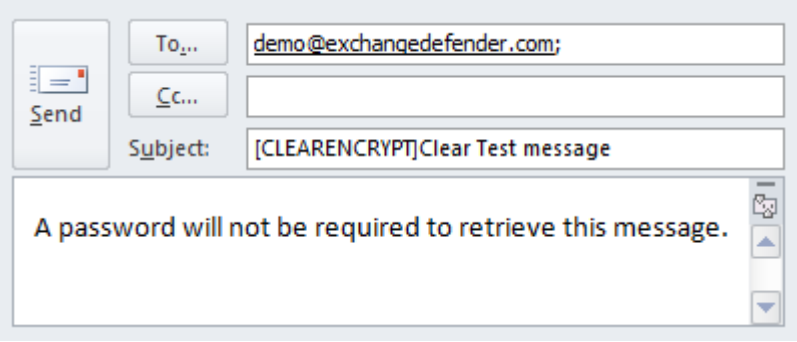
Business Considerations

While the act of sending an encrypted message through ExchangeDefender is simple, the business considerations behind encryption can be quite complex. Let's first discuss the difference between [ENCRYPT] and [CLEARENCRYPT] behavior:

[ENCRYPT] – Message will be encrypted and the recipient will receive an email notification of where they can access the message. If this is their first time receiving an encrypted message they will be prompted to enroll in the ExchangeDefender Encryption service which is completely free and only requires the recipient to provide their email address, physical address, choose a password and a PIN. By using this strong encryption, the user will have to authenticate to the ExchangeDefender Encryption site to retrieve the message. This level of security assures you that only the recipient of the message will be able to access the message and it won't be intercepted by packet sniffers, hackers, IT staff or company management.



[CLEARENCRYPT] – Message will be encrypted and the recipient will receive an email notification with the link to their encrypted message. No information is requested from the recipient, they just see the encrypted message.



Using [ENCRYPT] gives you the most assurance that the message will be received by your client and only your client. Sniffing, packet logging even mail logging are not effective ways to compromise this level of encryption because it requires the user to actually establish an account and provide data. While that gives you the most security and assurance, your recipient may not want or be allowed to follow these steps.

Major companies and many Fortune 500 organizations prohibit their employees from issuing personally identifiable information such as their email address, company name or phone number to third parties. As such, your encrypted message may be ignored.

Likewise, by sending a [CLEARENCRYPT] message you run a small risk that their network is being monitored, that their email is being read by their management or that they have a compromised system that is controlled by hackers. In those cases, they may be screenscrapping or automatically downloading all the content sent to the recipient.

Security is a compromise and arrangement between the two organizations that are exchanging information. While the ExchangeDefender technology makes this easy, take the extra step to assure people you work with that you are sending them confidential information and what steps they need to take.

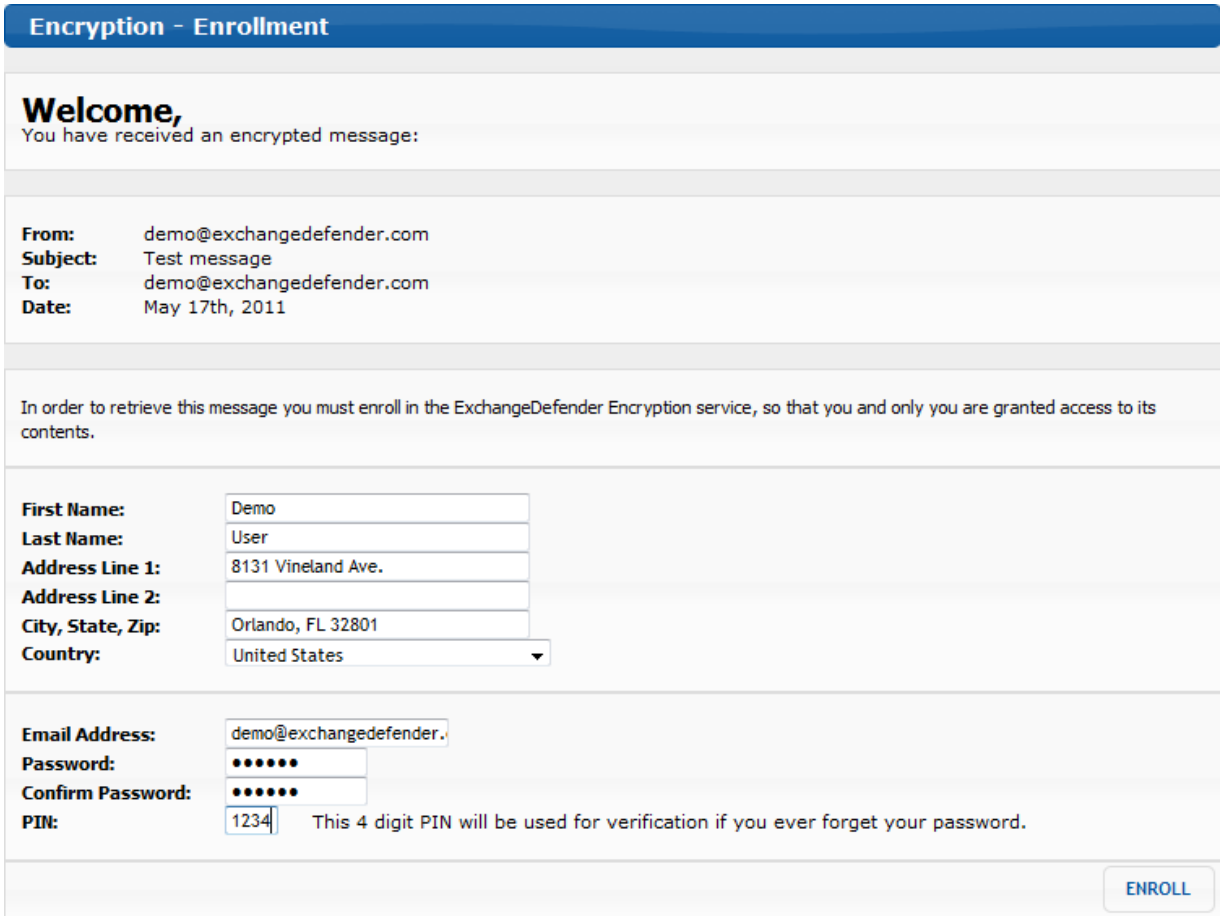
Retrieving Encrypted Messages

ExchangeDefender makes it simple to retrieve encrypted messages but the solution is also flexible enough to meet a more complex encryption requirement.

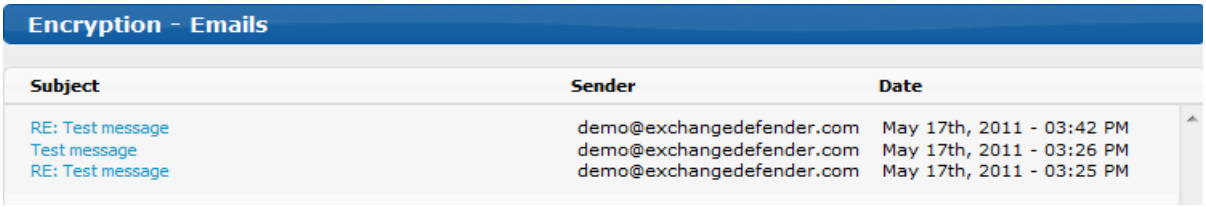
Regardless of whether you use [ENCRYPT] or [CLEARENCRYPT] the recipient will receive the following message indicating that you've sent them an encrypted message and they will be prompted to click on it to retrieve it.

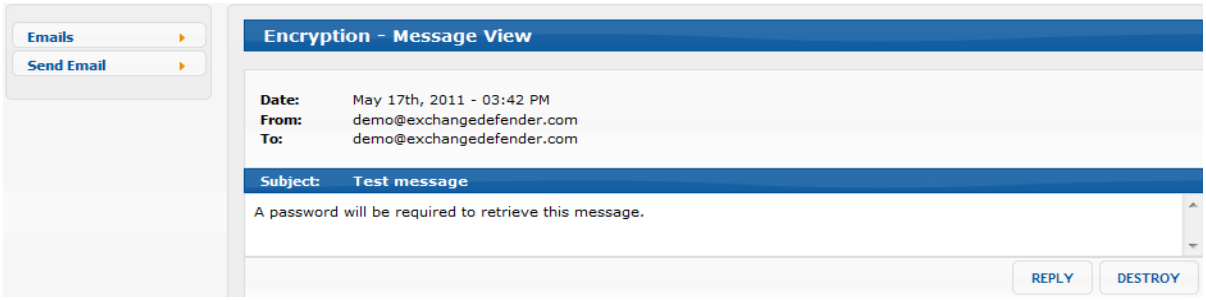
If you used [CLEARENCRYPT], the message will be displayed right away.

If you used [ENCRYPT] the user must verify their identity. If this is the first time they are accessing our system, we will prompt them to choose a password and a PIN so we can be sure that only they have access to their messages.



After enrollment, they will be able to see their ExchangeDefender Encryption Inbox and be able to read, delete or even respond to the encrypted message.





As a best practice, you should always notify someone when you send them an encrypted message for the first time. Because of the general lack of trust and authenticity on the Internet, it helps when you can assure someone that the message is indeed coming from you.

Technical Help & Account Management

Please contact (your local IT Solution Provider) for technical help and account management. Own Web Now Corp is a software developer that builds and manages the ExchangeDefender network and does not have access to your account, your data or your company information.

When contacting (you IT Solution Provider) for assistance please keep in mind that the more information you can provide about the issue the faster and more accurately the answer will be provided. Make sure to provide the following to expedite your request:

ExchangeDefender
8131 Vineland Avenue #102
Orlando, FL 32821 USA

Phone: (877) 546-0316
International: (407) 465-6800

www.exchangedefender.com

ExchangeDefender

ExchangDefender

- **Full description of the problem:** Provide a detailed explanation of the issue that you have experienced, if this is the first time you have experienced a problem or if it's repetitive, and if the issue is only affecting you or multiple users.
- **Relevant tracking data:** Provide any relevant information about where you are experiencing an issue: your computer, website, mobile phone, as well as the basic information that can narrow down the research (when the issue happened), what you were attempting to do, who the message was being sent to or received from).
- **Recent account or configuration changes:** Advise us if you have recently made any configuration changes to either your account or your computer/network so that we can double check if all systems are configured properly.
- **Screenshots:** If the issue is easy to see, such as an error message or prompt, take a screenshot. On Windows computers press ALT + PrintScreen at the same time, on Macintosh press Command+Shift+3 at the same time.

General Security Tips:

- ExchangeDefender will never ask you to provide or verify any billing or financial information.
- ExchangeDefender web sites are always encrypted and always contain ExchangeDefender.com
- Never share your ExchangeDefender password with anyone or use the same password across different services or service providers.
- Never save or store your password on portable or shared devices such as mobile phones, kiosks, or computer labs.
- Always follow your IT department or solution provider's security guidelines and report security concerns or breaches.

Get the latest service alerts: http://www.exchangedefender.com/noc