Administrator Guide for Encryption

modusCloud

November 2016

Email Encryption and Data Loss Prevention Feature Description

Reduce the risk inherent in individuals making security and disclosure policy decisions by creating custom filters to automate enforcement of data security policies for sensitive data. Emails are identified based on industry relevant smart identifiers and dictionaries and the appropriate action is automatically taken – e.g., allowing the information to be sent, blocked or encrypted if appropriate.

Service Architecture

As the message filtering layer is hosted, actual detection and filtering of suspicious mail occurs not in your email environment, but at our external data center. This is a robust and secure cloud security platform that sits between your users and the Internet, and is managed by our highly specialized personnel.

Once the service is set up, all incoming traffic to users is filtered at the data center according to your configuration—before it reaches your server. Within seconds, heuristics-based anti-spam and virus engines separate spam and viruses from legitimate messages. Legitimate messages are delivered to users without delay, while suspicious mail is diverted to a quarantine area where you or your users can review it.

Configuring Encryption

Email Encryption (Advanced and Professional packages only)

Create custom filters that will encrypt an email when specific conditions are met such as an embedded trigger term (e.g., Confidential, Sensitive, Encrypt, etc.) or sensitive data is found.

To enable or disable features:

1. Click on the Company Settings tab.
2. Click on the Features tab.
3. Enable (check) or Disable (uncheck) features as necessary.
4. Click Save.

Outbound Filter Management (Specifies Encryption Triggers)

Filters can be managed on a page underneath the Company Settings tab. From this location administrators can manage filters that apply to the company, a group of a user or an individual users. In addition, you can access filters when managing a specific group or a specific user.

To view current outbound filters:

1. Click on the Outbound tab

To change the filter view:

1. Click the drop-down and select the appropriate view:
    - *All (Default view): A list of all organization, group and user filters.*
    - *Organization: A list of all organization filters.*
    - *Group: A list of all group filters, grouped by group.*
    - *Users: A list of all user filters, grouped by user.*

To adjust the priority of a filter

You can adjust the priority of a filter only if it applies to the same entity. For example, you can adjust the priority of any company inbound filters but you cannot prioritize a group filter ahead of an end-user filter.

1. Click on the down arrow next to the filter you wish to lower in priority.
2. Click on the up arrow next to the filter you wish to increase the priority.

To add a new filter:

1. Click on the Company Settings tab.
2. Click on the Filters tab.
3. Click New Filter.

   A new window will open.
4. Enter a name
5. Choose the direction the filter should be applied.
   - *Inbound: Email sent to your licensed users.*
   - *Outbound: Email sent from your licensed users.*
6. Click Continue.
7. Choose the scope the filter should be applied.
   - *Company: All licensed users that are associated with the company.*
   - *Group: A specific group of users.*
   - *User: A specific user.*
8. Add condition:
   - *Sender Address: Matches the email address that the message in question originated from.*
   - *Recipient Address: Matches the email address that the message in question is sent to as a final destination, in other words the To address used by the originating sender.*
   - *Email Size (kb):Is greater than can be used to detect an email larger a specified size in order to trigger this rule set. This can be used to block large email or to define which address within a company can receive email over a specified size.*
   - *Client IP Country: Type in the country name and the select the matching selection once it appears. Select more than 1 country by adding multiple values and separating by a comma.*
   - *Email Subject: Used to trigger a rule set defined by any word(s) contained within the emails subject line defined in the pattern field.*
   - *Email Headers: Used to trigger a rule set defined by any word(s) contained within the emails header defined in the pattern field.*
   - *Email Message Content: Used to trigger a rule set defined by any word(s) contained within the email message content defined in the pattern field.*
   - *Raw Email: Used to trigger a rule set defined by a block of words contained within the email body defined in the pattern field.*
   - *Attachment Type: Used to trigger a rule set when an email contains a specified attachment type, including: Windows executable components, installers and other vulnerabilities, Other executable components and installers, Office documents and archives, Audio/Visual, Other including PGP encrypted files.*
   - *Attachment Name: Used to trigger a rule set defined by any word(s) contained within the attachment name defined in the pattern field.*

- *Smart Identifier Scan (Available only to Business and Professional package subscribers): Used to identify emails that contain content patterns such as credit card numbers, bank account numbers, etc.*
- *Dictionary Scan (Available only to Business and Professional package subscribers): Used to identify emails that contain common terms such as protected health information (i.e., NDC terms), personal information (i.e., SSN), and financial information (i.e., ABA terms).*

9. Choose operator.

   The operator options will depend on the filter condition selected.

10. Enter value.
11. If you wish to add another condition, click Add Another Condition

    *The relationship between each condition specified is AND. For example, if sender address is *@domain.com AND attachment is financial report.*

12. Choose action.
    - *Quarantine: Used for filters where you want to ensure email is not delivered to the intended recipient.*
    - *Allow: Used for filters where you want to ensure email to be delivered (i.e. allow list).*
    - *Nothing: Used for filters where you do not want to influence destination (allow, quarantine) but you want to perform a secondary action (i.e., Alert)*
    - *Encrypt: Used to filters where you want to encrypt the email that is caught by the conditions.*

    Encrypt is only available where direction is outbound and scope is the company. Available with Advanced and Professional packages only.

14. If you wish to add another condition, click Add Another Action.

This will add a new action control.

15. Choose action.
    - *Alert Tech Contact: Will send an alert to the tech contact associated with the site. Alert Specified Users: Will send an alert to the SMTP addresses specified.*
    - *Hide Logs: Will hide the log from the all users including administrators.*
    - *Hide Logs from Non-Admin Users: Will hide the log from the users view. The email will still be visible to the administrator.*
    - *Stop Processing Additional Filters: Will stop processing any additional filters that normally would have been applied.*
    - *Require Admin Privileges to Release: Requires an administrator to release.*
    - *Enforce Completely Secure SMTP Delivery: Will force delivery over TLS without an unencrypted fallback. Will check for a valid certificate for the recipient domain.*
    - *Enforce only TLS on SMTP Delivery: Will force delivery over TLS without an unencrypted fallback. Strip Subject Line Encryption Terms: Will strip terms from the email when identified in a Subject Line condition.*

16. Enter a description (Optional).
17. Click Save.

To edit a filter:

1. Click on the Company Settings tab.
2. Click on the Filters tab.
3. Click the Edit icon next to the filter you with to edit.
4. Make appropriate changes.
5. Click Save.

To duplicate an existing filter:

1. Click on the Company Settings tab.
2. Click on the Filters tab.
3. Click the Duplicate icon next to the filter you with to edit.
4. Make appropriate changes.
5. Click Save.

To delete a filter:

1. Click on the Company Settings tab.
2. Click on the Filters tab.
3. Click the Delete icon next to the filter you with to delete.

To disable / enable a filter:

1. Click on the Company Settings tab.
2. Click on the Filters tab.
3. If enabled, click the slider next the filter you wish to disable. If disabled, click the slider next to the filter you wish to enable.

To search for a filter:

1. Click on the Company Settings tab.
2. Click on the Filters tab.
3. Type in a domain, email address or a portion of the name/description of the filter in the search field.

   Results are dynamically returned as you type.