Security

Mimecast Training

Student Workbook

V 1.2
Table of Contents

Chapter 1: Mimecast

- What is Mimecast? .................................................. 2
- Data Center architecture .......................................... 2

Chapter 2: Mimecast Infrastructure

- Software-as-a-Service (SaaS) .................................... 3
- Mimecast Services ................................................. 4
- Account Integration Options ..................................... 4

Chapter 3: Mimecast Secure Email Gateway

- ARMed SMTP .......................................................... 5

Chapter 4: Email Processing Steps

- Exercise: Confirm Active Security Policies .................... 7

Chapter 4: Security Policies

- Exercise: Manage Security Policies ............................ 9

Chapter 5: Reputation Checks

- Reputation Definitions ............................................ 10
- Exercise: Work with Reputation Checks ...................... 11

Chapter 6: Recipient Validation

- Exercise: Confirm Recipient Validation Settings ............ 13

Chapter 7: Content Spam Scanning

- Spam Scanning ....................................................... 14
- Held Queue .......................................................... 16
- Digest ...................................................................... 16
- Exercise: Manage Content Checking .......................... 17

Chapter 8: Attachment Handling

- Exercise: Implement Attachment Management ............. 19

Appendix: Knowledge Base and Resources

- Knowledge Base ...................................................... 20
- Training Courses .................................................... 20
- Available Online Course Titles: ................................. 20
- Other useful links: .................................................. 20
Chapter 1: Mimecast

What is Mimecast?

Mimecast delivers cloud-based email management services, including Security, Archiving and Continuity. By unifying disparate and fragmented email environments into one holistic solution that is always available from the cloud, Mimecast minimizes risk and reduces cost and complexity, while providing total end-to-end control of email. Founded in the United Kingdom in 2003, Mimecast serves thousands of customers worldwide and has offices in Europe, North America, Africa, and the Channel Islands.

Data Center architecture

Mimecast infrastructure consists of two geographically dispersed data centers in each physical location. This provides not only load balancing of all email processing and archiving, but also provides DR coverage in the event of a natural disaster.

The Mimecast architecture is made up of layers of servers based on functionality: Processing Layer, Scanning Layer and the Archiving Layer. For this session, we are going to concentrate on the Archiving layer.

The Processing layer is the layer which makes up our customer front-end clusters. So for example, your account may reside on service37-us and 38-us; which together make up a front end cluster. The processing layer is responsible for the security and reputation checks, which are coupled with the Mimecast Mail Transfer Agent (MTA). Other activities performed at this layer include email Policy application.

Once reputation checks and the relevant policies have been applied, the processing layer hands the email over to the scanning engines. The scanning servers run multiple technologies concerned with the scanning of emails and attachments looking for spam, viruses and malware. If the email passes the scanning process and no virus is detected, the message will be moved to the Storage or Archiving Layer. It is at this stage that the email is archived and indexed for searching capabilities.

Storage infrastructure is a key element of the Mimecast Grid. As outlined above, this is supported by triple redundancy - data is continuously replicated to primary, secondary and tertiary storage nodes at one location and then again at multiple geographic locations. This process protects data to such a degree that the Mimecast Grid is able to automatically heal and protect itself against data loss and corruption. The process is entirely proprietary and remains confidential to Mimecast. The use of continuous replication sets us apart from our competitors, most of whom only use a low level of mirroring or warm standby infrastructure - and that is a recipe for data loss in the event of an outage.
Software-as-a-Service (SaaS)

Mimecast provides email services from the internet, also referred to as the cloud, delivered through a SaaS model. In simple terms, this means that Mimecast will handle your email data in a secure way, and deliver it to your existing infrastructure. The benefit of this SaaS model is that it is always accessible, 100% of the time, and all you need is an internet connection to access your emails.

The SaaS solution is made available through two physically separate data centers. In the event of infrastructure outage, emails will continue to flow to the alternative data center. This event is completely seamless, and ensures 100% email Continuity.
Mimecast Services

The available service features will depend on your specific Mimecast service subscription. Mimecast’s current service portfolio is outlined in the manual below, and shows which areas of email management are included in each service.

<table>
<thead>
<tr>
<th>Service</th>
<th>Security</th>
<th>Continuity</th>
<th>Archiving</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mimecast UEM Enterprise</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Mimecast UEM Express</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Mimecast Email Security</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mimecast Email Continuity</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Mimecast Email Archive</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Mimecast File Archive</td>
<td></td>
<td></td>
<td>Add-On</td>
</tr>
</tbody>
</table>

Account Integration Options

A number of connections are available for use when Mimecast is implemented. These features may be enabled, if the organization requires the functionality, but not all elements are required in order to benefit from Mimecast services:

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Outbounds</td>
<td>IP address origination points from which Mimecast accepts the organization’s outbound emails.</td>
</tr>
<tr>
<td>KBID10036</td>
<td></td>
</tr>
<tr>
<td>Delivery Routes</td>
<td>The mail server that Mimecast should deliver inbound emails to.</td>
</tr>
<tr>
<td>KBID10081</td>
<td></td>
</tr>
<tr>
<td>Directory Connections</td>
<td>Synchronisation services to network directories, such as Microsoft Active Directory, using LDAP/LDAPS.</td>
</tr>
<tr>
<td>KBID10092</td>
<td></td>
</tr>
<tr>
<td>Journaling</td>
<td>Journal connectors are used to import internal email communications from the email server to the Mimecast archive.</td>
</tr>
<tr>
<td>KBID10235</td>
<td></td>
</tr>
</tbody>
</table>

Note: These account services are explored in detail later in this module.
Chapter 3: Mimecast Secure Email Gateway

Email as a means to conduct business is becoming more and more the norm, and provides the backbone to most organisations’ activity. As such, the importance of email security becomes more significant.

There are many functions of the secure email gateway. This includes securing the customer environment by protecting them from the ever increasing number of email threats, as well as providing methods to deliver email securely, and also protecting from data leaks.

This session is going to concentrate on the core email security functions, Mimecast’s proprietary ARMed SMTP, as well as the reputation, content, security checks and Policies used to process inbound emails.

ARMed SMTP

Mimecast uses a combination of Policies, reputation checks, anti-spam and anti-virus systems to detect, and if necessary, reject any spam emails. ARMed SMTP, or Advanced Reputation Management, is a proprietary Mail Transfer Agent (MTA) that has been purpose built to make email processing more efficient and effective. This is achieved by looking at the reputation of the sending IP address and email address.

Mimecast ARMed SMTP which consists of a combination of policies and reputation checks, takes place during the communication between the sending email server, and the receiving Mimecast MTA. Emails are analysed in protocol, or on-the-wire, before they are accepted or rejected in protocol. This prevents the unnecessary transfer of unwanted email content to the customer infrastructure.

Note: ARMed SMTP Blocks 98.5% of all dark SMTP traffic (unwanted inbound SMTP traffic including spam, DoS attacks, directory harvest attacks and malformed SMTP packets).

Emails are analysed against multiple engines as follows:

1. Inbound Lockout – to prevent spoofed emails
2. Blocked Sender Policies (Company or Individual) – to prevent unwanted emails
3. Permitted Sender Policies (Company or Individual) – to bypass all content and reputation Spam checks
4. Auto Allow – to bypass all content and reputation Spam checks
5. Greylisting, RBL and Realtime Reputation Checks – Reputation checks used to prevent emails from known or potential spammers

Following this, the content of emails are also scanned for viruses and malware, and if configured for spam signatures.

There are many types of malware that could target your environment, and cause theft of data, irritation, loss of productivity, and other immeasurable losses. Mimecast provides a series of checks for all inbound email to prevent spam and malware.
Chapter 4: Email Processing Steps

All inbound emails will go through a series of checks to ensure that any email threats are detected and prevented. These checks are dependent on the configuration of the customer’s Mimecast account. There are, however, some checks that will always be applied, specifically the malware and virus scanning. Depending on the outcome of these checks, the email will either be rejected in protocol (i.e. the content is not saved), or accepted and delivered to the organization’s mail server. The exception is for any emails that have triggered a Hold action, and have been held on the Mimecast platform in the Held queue.

The order that these checks are applied is important to understand and troubleshoot email delivery.
The checks applied to emails can be classified into the groups below:

<table>
<thead>
<tr>
<th>Viewer / Queue</th>
<th>Description</th>
<th>Knowledge Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Policies</td>
<td>Policies applied to inbound emails typically looking at the sender’s email address or domain</td>
<td>KBID10219</td>
</tr>
<tr>
<td>Reputation Checks</td>
<td>Analyses the IP and email address of the sender, Confirms the sending mail server is RFC compliant, does not have a poor reputation and is configured to retry the email connection</td>
<td>KBID10184</td>
</tr>
<tr>
<td>Recipient Validation</td>
<td>Ensures that only emails destined to valid internal email addresses are accepted</td>
<td>KBID10176</td>
</tr>
<tr>
<td>Content and Attachment Scanning</td>
<td>Emails and attachments are scanned for spam, viruses and malware. The structure of emails is also analysed to ensure it is compliant and contain all the necessary parts e.g. header and body.</td>
<td>KBID10297</td>
</tr>
</tbody>
</table>

Exercise: Confirm Active Security Policies

- Review Default Security Policies
  - Navigate to Gateway | Policies
  - Select each of the following Policies in turn, and review the settings:
    - Inbound Lockout Policy - Do you have any bypass policy configured?
    - Blocked Senders Policy
    - Permitted Senders Policy
    - Auto Allow Policy
    - Greylisting Policy - Do you have any bypass policy configured?

Note: All these policies are configured by default when your Mimecast account is created.

- Review Groups assigned to Policies
  - Navigate to Directories | Groups
  - Review the contents of the following Groups:
    - Blocked Senders
    - Permitted Senders

When a user sends an email to an external recipient, the external address is automatically added to the Auto Allow list. Future inbound emails from the external sender will bypass Reputation and Content-based spam checks. This exercise assumes you have sent an outbound email from your work email address to an external personal email address.

- Log into the Mimecast Administration Console
- Navigate to Gateway | Managed Senders
- Search for your external email address. This entry should be marked as Auto for your work email address
- Right-click on the entry and select Delete. This will remove the entry from the Managed Senders list.
- Send an outbound email from your work address to your external email address
- Click refresh on the Managed Senders page and once again search for your external email address.
Chapter 4: Security Policies

Security Policies are the first set of checks applied to inbound emails. Typically these Policies verify if the email address or domain of the sender, matches a pre-configured Policy in the customer’s Mimecast account. These Policies are configured to block spoofing, block or permit trusted/unwanted emails or domains, or to allow inbound emails from those users who are known to be trusted (Auto Allow).

Note: These Security policies do not include any content scanning checks.

<table>
<thead>
<tr>
<th>Viewer / Queue</th>
<th>Description</th>
<th>Knowledge Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound Lockout</td>
<td>Blocks unwanted spoofed emails, i.e. an inbound email originating from the internet, but displaying the internal domain name, and directed to the internal end users.</td>
<td>KBID10219</td>
</tr>
<tr>
<td>Permitted Senders</td>
<td>Allows inbound emails to bypass security checks (reputation and spam checks) but does not override virus checks. Used to ensure emails are delivered directly to the internal recipients.</td>
<td>KBID10184</td>
</tr>
<tr>
<td>Blocked Senders</td>
<td>Used to restrict messages from or to certain email addresses or domains. This can apply to inbound or outbound emails, although typically it is used to block inbound senders that a company does not want to receive email from.</td>
<td>KBID10176</td>
</tr>
<tr>
<td>Managed Senders</td>
<td>Contains a list for each end user, of those email addresses and domains which have been manually added to their personal Block and Permit lists, or automatically added to their Auto-allow list.</td>
<td>KBID10297</td>
</tr>
<tr>
<td>Auto Allow</td>
<td>For every email sent outbound (excluding auto responders), Mimecast will add the recipient to the Auto Allow (or trusted sender database). As a result, any inbound email coming from a sender listed in the Auto Allow database will only be scanned for viruses.</td>
<td>KBID10323</td>
</tr>
</tbody>
</table>
All emails that are explicitly permitted based on the above Policies will be passed through to the internal recipient without undergoing the reputation or spam based content checks. These emails will only be scanned for malware or viruses.

All emails that are blocked will be rejected in protocol by Mimecast, which means that the connection is dropped prior to any data being streamed. As a result, the email cannot be retrieved in Mimecast, however details regarding the rejection can be found in the Rejection Viewer.

Exercise: Manage Security Policies

These exercises assume that you have an personal external email address that you can access to send emails from.

- **Block a Sender using a Policy**
  - Log into the Mimecast Administration Console
  - Navigate to Gateway | Policies
  - Open and view the Blocked Senders Policy
  - Click the New Policy button
  - Complete the Policy fields as follows:
    - Narrative: Test Block Policy
    - Policy Option: Block Sender
    - Emails From: Change the Everyone option to Individual Email Address
    - The screen refreshes to display the Specifically field. Add your personal external address in this field
    - Emails To: Change the Everyone option to Individual Email Address
    - The screen refreshes to display the Specifically field. Add your personal internal address in this field
  - Click the Save and Exit button
  - Send a test email from your external address to your internal address, which should be Blocked by Mimecast
  - Right-click your Block Policy, and select Remove Policy.

- **Confirm the Email Rejections**
  - Navigate to Monitoring | Rejections
  - Search for your external email address
  - View the entry for the blocked email, with the rejection reason: Envelope Blocked

- **Bypass Spam Checks using a Permitted Sender Policy**
  - The Permitted Senders Policy is created by default using the Permitted Senders Group. If you add an entry to the group, it will automatically have the policy applied.
  - Navigate to Directories | Groups
  - Select the Permitted Senders Group
  - In the right-hand pane, click on the Build menu
  - Select Add Email Address option, and add your external email address to Permit Senders group
  - Click on the Save and Exit button
  - Send a test email from your external address to your internal address, which should be allowed by Mimecast without applying reputation or spam checks
  - Right-click on your email address in the group, and click on the Unlink Item option. This removes the entry from the group.
Chapter 5: Reputation Checks

For inbound emails from senders that have not explicitly been permitted, Mimecast applies additional reputation checks. These reputation checks analyse the IP address and email address of the sender. Using reputation checks increases the efficiency of processing inbound emails as potential spam and viruses can be detected and blocked before the content of the email is scanned.

Reputation checks are applied by default, unless the sender has its email address, domain or IP address permitted in a policy. Administrators are also able to configure a Reputation definition to control which checks and specific RBL’s are applied (discussed below).

### Reputation Check Description

<table>
<thead>
<tr>
<th>Reputation Check</th>
<th>Description</th>
<th>Knowledge Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greylisting</td>
<td>Greylisting is a default compliance check that is applied to all inbound email for connections not previously seen by Mimecast. Mimecast looks at the sender’s IP address, email address and recipient’s email address and subjects the connection to a temporary busy signal (for 60 seconds). The mail server must retry within 12 hours to be successful.</td>
<td>KBID10219</td>
</tr>
<tr>
<td>Real-time Black hole Lists (RBLs)</td>
<td>Inbound emails are checked to see if the sending IP address is listed in a RBL, or block list. Mimecast uses its own RBL, along with other commercial DNS RBLs. If a match is found, the email is rejected.</td>
<td>KBID10184</td>
</tr>
<tr>
<td>Real-time Reputation Lists</td>
<td>Functions as a global network outbreak detection system, which allows Mimecast to be the first responder to many malware threats, both known and unknown. Mimecast utilises a real-time reputation service which temporarily defers connections if they are suspected to have a poor reputation. If the reputation continues to hold a poor reputation, the email is rejected.</td>
<td>KBID10176</td>
</tr>
</tbody>
</table>

**Reputation Definitions**

Although not recommended, Administrators are able to control which reputation checks are applied to emails. Reputation Definitions provide Administrators with granular control over the reputation based spam detection technologies that Mimecast utilizes as part of the default security stack. By default, all Mimecast RBLs and Reputation checks are applied to Inbound emails, but using Reputation Definitions, these can be adjusted to exclude some of these checks, or to decrease their sensitivity.

The Reputation Definition Policy can be located by navigating to Gateway | Policies.
Exercise: Work with Reputation Checks

- **Bypass Reputation Checks using a Greylisting Bypass Policy**
  - Log into the Mimecast Administration Console
  - Navigate to Gateway | Policies
  - Select Greylisting from the available Policy list
  - Complete the Policy fields as follows:
    - **Narrative**: Test Greylist Bypass Policy
    - **Policy Option**: Take No Action
    - **Emails From**: Change the Everyone option to Domain
      - The screen refreshes to display the Specifically field. Add an external domain address in this field that should bypass Reputation checks
    - **Emails To**: Change the Everyone option to Individual Email Address
      - The screen refreshes to display the Specifically field. Add your personal internal address in this field
    - Click the Save and Exit button.

- **View the Rejection Graph for Inbound Email**
  - Log into the Mimecast Administration Console
  - Navigate to Reporting | Overview
  - Click on the Rejection Overview graph in the Summary Graph section
  - View the rejections based on reputation checks:
    - IP in RBL: The originating IP address was blacklisted in a RBL
    - Sender Failed to Retry: The sender was Greylisted, and did not retry

- **Review Greylisted Emails**
  - Navigate to Monitoring | Connections
  - Review the items that have been deferred due to Reputation checks
    - Attempt Greylisted - triplet has attempted to connect to Mimecast
Chapter 6: Recipient Validation

Recipient validation is one of the security checks performed by Mimecast for all inbound email, to ensure that only emails destined to valid internal email addresses are accepted. Email addresses are verified against the internal domain addresses within Mimecast, and emails that fail recipient validation will be rejected in protocol.

Many spammers will send messages to any email address in a domain in the hope that they may be accepted. For example, they will try addresses like abc@domain.com or jane@domain.com. When Mimecast processes an inbound email, the address is verified against your account based on the configure recipient validation method. The email is then either rejected in protocol or accepted as a valid email. This shifts the recipient validation from your internal mail environment to Mimecast, so that by the time email is delivered to your mail server, it is only for legitimate email addresses.

Only Mimecast Support Administrators can configure the recipient validation method to be used. Each internal domain requires initial configuration. There are four available options:

<table>
<thead>
<tr>
<th>Reputation Check</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept inbounds for valid LDAP users only</td>
<td>Only addresses that have been synced with your LDAP environment will be accepted</td>
</tr>
<tr>
<td>Accept emails for Known recipients only</td>
<td>Those addresses that are either synced or known to Mimecast (based on emails traversing Mimecast from internal domains, including journaling) will be accepted</td>
</tr>
<tr>
<td>Use SMTP call forwarding to check recipient addresses</td>
<td>A request is made to your mail server, which then validates if the address is legitimate or not (requires recipient filtering configured on your mail server)</td>
</tr>
<tr>
<td>Accept all inbounds for this domain</td>
<td>All emails for the internal domain are accepted (not recommended)</td>
</tr>
</tbody>
</table>

Note: Using “LDAP users only” is the most secure method as Mimecast will then only accept emails for current valid LDAP users. However, ensure that you do not have other email addresses in your environment (e.g. Unix based or Fax machine addresses) that also require inbound emails from the internet.

Any address that is not accepted will be rejected in protocol, and logged in the Rejection Viewer.
Exercise: Confirm Recipient Validation Settings

- Confirm the Recipient Validation Method
  - Log into the Mimecast Administration Console
  - Navigate to Directories | Internal
  - Review the Inbound Checks column for each internal domain. What have you inbound recipient checks been set to?

- View Rejections for Inbound Email
  - Log into the Mimecast Administration Console
  - Navigate to Reporting | Overview
  - Click on the Rejection Overview graph in the Summary Graph section
  - Review the number of emails that have been rejected based on Invalid Recipient Address.
Chapter 7: Content Spam Scanning

Following the security, reputation checks and recipient validation conducted at the Processing server level, emails are directed to the scanning engines. At this point, emails and attachments are scanned for spam, viruses and malware. The structure of emails are also analysed to ensure they are compliant and contain all the necessary parts, e.g. header and body.

Your account configuration will determine what happens to emails which match a spam based signature. Spam scanning can be configured to check inbound emails for these signatures, and can be set to different levels of sensitivity. Further configuration options allow the Administrator to control what happens to these emails when a match is triggered. Any virus or malware signature will always result in the email to be rejected in protocol, even if the sender is a known trusted or Permitted sender.

<table>
<thead>
<tr>
<th>Content Scanners</th>
<th>Description</th>
<th>Knowledge Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam Scanning</td>
<td>Consists of multiple content based heuristic scanning engines. These engines examine the content of emails and look for key phrases and other identifiers commonly used by spammers. These include content-matching rules, and also DNS-based, checksum-based and statistical filtering definitions.</td>
<td>KBID10219</td>
</tr>
<tr>
<td>Virus and Malware</td>
<td>Mimecast uses multiple anti-virus engines to scan all emails and attachments. This includes its own proprietary software as well as market leading Commercial software. ZHARA is Mimecast proprietary software which provides highly effective zero-day protection against previously unknown threats through deep level anomaly detection; and trending across the entire Mimecast customer base.</td>
<td>KBID10184</td>
</tr>
<tr>
<td>Message Structure</td>
<td>Emails are checked to ensure that all the necessary components exist, e.g. email headers and body. This helps in determining if the email is legitimate or not.</td>
<td>KBID10176</td>
</tr>
</tbody>
</table>
Spam Scanning

The aim of Mimecast’s initial layers of defence is to reject unwanted spam and malware emails in protocol. However, there are occasions where Mimecast cannot determine if an email is wanted by the end user or not, such as promotional notifications, newsletters or advertisements. A spam scanning policy is configured to check the content of all inbound emails.

Note: If an email address, domain name or IP address is added as a Permitted Sender, either on the customer account or as a Mimecast global setting, the inbound email will always bypass these content based spam checks (but virus scanning will still apply).

Note: An email with a high enough spam score will be rejected in protocol, and logged in the Rejection Viewer.

<table>
<thead>
<tr>
<th>Content Scanners</th>
<th>Description</th>
</tr>
</thead>
</table>
| Detection Level  | Relaxed: Sets the triggering threshold of the spam definitions to 7 points. This setting is recommended for users that receive some junk email.  
Moderate: Sets the triggering threshold of the spam definitions to 5 points. This setting is recommended for users that are actively targeted by promotional and junk emails.  
Aggressive: Sets the triggering threshold of the spam definitions to 3 points. This setting is recommended for users who do not want to receive any possible spam or junk emails |
| Detection Action | Tag headers: Does not affect the delivery of the email, but inserts a tag into the headers of the email message. If required, a rule can be configured in Outlook to move any emails with the tag in the header or another folder for review by the end user.  
Hold for review: This is the recommended option, as the email delivery will be halted in the Hold Review Queue. The Digest can be utilized to inform the user of messages on Hold, at which point the email can be released, permitted for future delivery or blocked.  
Reject to sender: The email is rejected in protocol, and the content of the email is not retained by Mimecast. Should the sender be legitimate, the sender will need to resend the email messages, once the Spam checks have been bypassed. |
| Notifications     | A Notification can be sent to the intended Recipient, an Overseer, or to a group of users. However, it is recommended that the Notifications be disabled if the Digest feature |
is utilized for Spam checks, as users might receive duplicate notices of emails Held due to Spam checks

Held Queue

The Held Queue contains emails that have been held by Mimecast based on Policy configuration. Policies that can be configured to hold emails include Content Examination, Message Scanning and Attachment Management Policies. Emails are Held for a maximum of 30 days, after which they are still available in the Archive. Administrators can control which users (and Administrators) have access to Held emails.

The Held Queue allows the Administrator to troubleshoot email delivery by viewing all those emails that have not been delivered to the intended recipients, based on a Policy. This is generally for inbound emails, however can also include outbound emails where a Content Examination Policy has been used to hold all emails containing a particular word or phrase.

All Held inbound emails are also accessible by end users in their Personal On Hold queue when logged into Mimecast Personal Portal (MPP) or Mimecast Services for Outlook (MSO 4). Administrator and end users can use the Held Queue to perform various actions on the email:

- Review email, to determine if it should be Held
- Release email: releases the message for delivery, but future emails may be Held again
- Reject email (either with or without a notification): the email expires from the Held queue, but is accessible from the Archive
- Permit the sender: Bypasses spam checks for the sender’s future emails
- Block the sender: Rejects future emails from the sender

Note: If overseer rights have been assigned to a user, they are also able to manage these hold queues using the Moderated On Hold option in MPP, MSO 4 and MSB.

Digest

Email Digests are email notifications that give the end user direct control over their personal Held Queue, by presenting them with a summary of emails that have been held by Mimecast Security Policies. Digests contain basic information regarding the use of the various links within the list of emails on hold, as well as a link to a Knowledge Base article explaining more in depth information on the Digest and Hold Queue.

Digests can be modified in terms of the contents of the notification, the frequency of the delivery, and also the overall design (look and feel) of the notification.
Exercise: Manage Content Checking

- Create a Spam Scanning Definition and Policy
  - Log into the Mimecast Administration Console
  - Navigate to Gateway | Policies
  - Click on the Definition button associated with the Spam Scanning Policy
  - Click on the New Message Scan Definition button
  - Complete the definition fields as follows:
    - Description: Test Moderate Spam Scanning Definition
    - Sensitivity: Moderate
    - Action: Hold for Review
      - Click the Save and Exit button
      - Click on the Go Back button
      - Click on the Spam Scanning Policy
      - Click on the New Policy button
      - Complete the Policy fields as follows:
    - Narrative: Test Spam Scanning Policy
    - Policy Option: Select the Test Moderate Spam Scanning Definition
    - Emails From: Leave this set to Everyone
    - Emails To: Change the Everyone option to Individual Email Address
    - The screen refreshes to display the Specifically field. Add your personal internal address in this field
      - Right-click on the Policy you have just created, and select Remove Policy.

- Review an Email from the Held Queue
  - Log into the Mimecast Administration Console
  - Navigate to Monitoring | Held
  - Use the Search bar to find emails on hold for your email address
  - Right-click on an email to review available options
  - Note: These options will only apply to this particular email.

- Review your Rejected Email Graph
  - Navigate to the Reporting | Overview
  - Select the Rejection Overview graph in the Summary Graphs section
  - Review the chart to determine what is causing most of your rejections. Are there any rejections based on Spam Signature Detection or Virus Signature Detection?
  - Change the date range using the calendar control to view your rejections over a period of time.
Chapter 8: Attachment Handling

Mimecast offers multiple options to assist with managing attachments. This includes managing the type of attachments that are allowed, as well as the sizes of attachments. This can either be done for all attachments, or alternatively configured specifically for different attachment types.

By default, Mimecast creates a standard Attachment Management policy to strip all dangerous attachment types from emails (e.g. exe, bat files) both inbound and outbound. Administrators can extend these capabilities by creating different attachment policies for different groups or individuals, as well as adding to the default list of denied attachment types. Within the Attachment Set definition, you are also able to choose to strip, hold or link individual specific attachment types. As encrypted archives and documents cannot be interrogated, these attachments can be configured to be held in the Administrative hold queue to be reviewed, and if required, released. Additionally Mimecast has pornographic scanning options which can be enabled and set to various levels of probability.

Policies which can be used to manage attachments:

<table>
<thead>
<tr>
<th>Viewer / Queue</th>
<th>Description</th>
<th>Knowledge Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment Sets</td>
<td>Attachment Sets can be used to apply granular attachment handling for individual attachment types. Attachments can be limited by size, held for review, or stripped and linked to emails as appropriate</td>
<td>KBID10219</td>
</tr>
<tr>
<td>Attachment Management</td>
<td>In order to implement attachment controls, the Attachment Set Definition must first be created, and then the Attachment Management policy needs to be configured to dictate the route of traffic that the Attachment Set should be applied to.</td>
<td>KBID10489</td>
</tr>
<tr>
<td>Attachment Link on Size</td>
<td>Attachment Link on Size (also known as Strip and Link) allows Administrators to specify an attachment size limit, while still allowing end users to receive attachments over a certain size.</td>
<td>KBID10184</td>
</tr>
<tr>
<td>Attachment Block on Size</td>
<td>The Attachment Block on Size Policy can be used to set restrictions on the maximum attachment size for emails both inbound and outbound</td>
<td>KBID10176</td>
</tr>
<tr>
<td>Stripped Attachments</td>
<td>Any attachment that is blocked or stripped and linked from an email, based on Mimecast Attachment Policies, is logged and available for release by an Administrator using Stripped Attachments.</td>
<td>KBID10297</td>
</tr>
<tr>
<td>Large File Sending</td>
<td>Large File Sending (LFS) enables you to send large files directly through Mimecast when composing emails in MSO4, bypassing the organization's email server. An email sent using LFS is delivered as a notification to the recipient, and includes a link to download the attachment. An additional notification is also delivered to the recipient with the access key to access the location.</td>
<td>KBID10942</td>
</tr>
</tbody>
</table>
Exercise: Implement Attachment Management

- Create an Attachment Management Definition and Policy
- Log into the Mimecast Administration Console
- Navigate to the Gateway Policy Editor (Gateway | Policies)
- Select the Definition button for the Attachment Management Policy
- Click on the New Attachment Definition button
- Complete the Definition fields as follows:
  - Description: Training Attachment Management Definition
  - Notifications: Internal Recipient
  - In the file list, check the Link box and specify the size of 1 Kb for docx extensions
  - Click on the Save and Exit button
- Click on the Go Back button
- Click on the Attachment Management Policy
- Click on the New Policy button
- Complete the Policy fields as follows:
  - Narrative: Test Attachment Management Policy
  - Policy Option: Select the Training Attachment Management Definition
  - Emails From: Change the Everyone option to External Addresses
  - Emails To: Change the Everyone option to Individual Email Address
  - The screen refreshes to display the Specifically field. Add your personal internal address in this field
- Click the Save and Exit button
- Send a docx file to your internal address from an external address as an attachment
- Navigate to the Monitoring menu | select Attachments
- Right-click the attachments that was stripped, and select Release Attachment.
Appendix: Knowledge Base and Resources

Knowledge Base

This manual refers to several Knowledge Base (KB) articles which can be directly accessed by replacing the relevant ID number in the URL:
http://www.mimecast.com/knowledgebase/MimecastKB.htm#KBIDxxxxx.htm
• Where xxxxx represents the ID of the article.

To access the Knowledge Base, use the direct link: http://www.mimecast.com/knowledgebase

Training Courses

Visit our website to view the latest information on our available training courses:

<table>
<thead>
<tr>
<th>Available Online Course Titles:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Mimecast Product Overview</td>
</tr>
<tr>
<td>• Mimecast Account Tour</td>
</tr>
<tr>
<td>• Mimecast Continuity</td>
</tr>
<tr>
<td>• Mimecast Security</td>
</tr>
<tr>
<td>• Mimecast Archiving</td>
</tr>
<tr>
<td>• Mimecast Admin Tasks</td>
</tr>
<tr>
<td>• Mimecast Exchange Tasks</td>
</tr>
<tr>
<td>• Mimecast Stationery</td>
</tr>
<tr>
<td>• Mimecast Admin Tasks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Available Classroom Course Titles:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Mimecast Service Management</td>
</tr>
<tr>
<td>• Mimecast Power Tools</td>
</tr>
<tr>
<td>• Mimecast Stationery Management</td>
</tr>
</tbody>
</table>

Other useful links:

• Mimecast Community:
  https://community.mimecast.com/
• Mimecast TV:
  http://www.youtube.com/user/mimecast
• Mimecast Blog: http://blog.mimecast.com/
• Mimecast Twitter: http://twitter.com/mimecast