Mimecast

Reference Guide

Contents

Overview 4

Dashboard 4

Service Monitor 5

Configure Alerts 6

Account settings 7

Account roles 9

Archive 12

Creating an Archive Search 12

Creating a saved Archive Search 15

Adding an eDiscovery Case 17

Search logs 18

Litigation Holds 19

Directories 20

Using Directory Groups 21

Add user to Mimecast Using a Spreadsheet Import 22

Adding an Internal Domain 22

Managing Profile Groups 23

Add to Whitelist/Blacklist 24

Gateway 24

Accepted Email 25

Managed senders 25

Policies 26

Anti-Spoofing Policy 27

Track and trace 29

Monitoring 30

Attachments 31

Reporting Overview 31

Guidelines for working with Graphs 33

Services 34

Enabling Mimecast for Outlook for end users 34

Managing Continuity Events 35
Stationary 37
Branding 38
Micro Sites 39

Overview

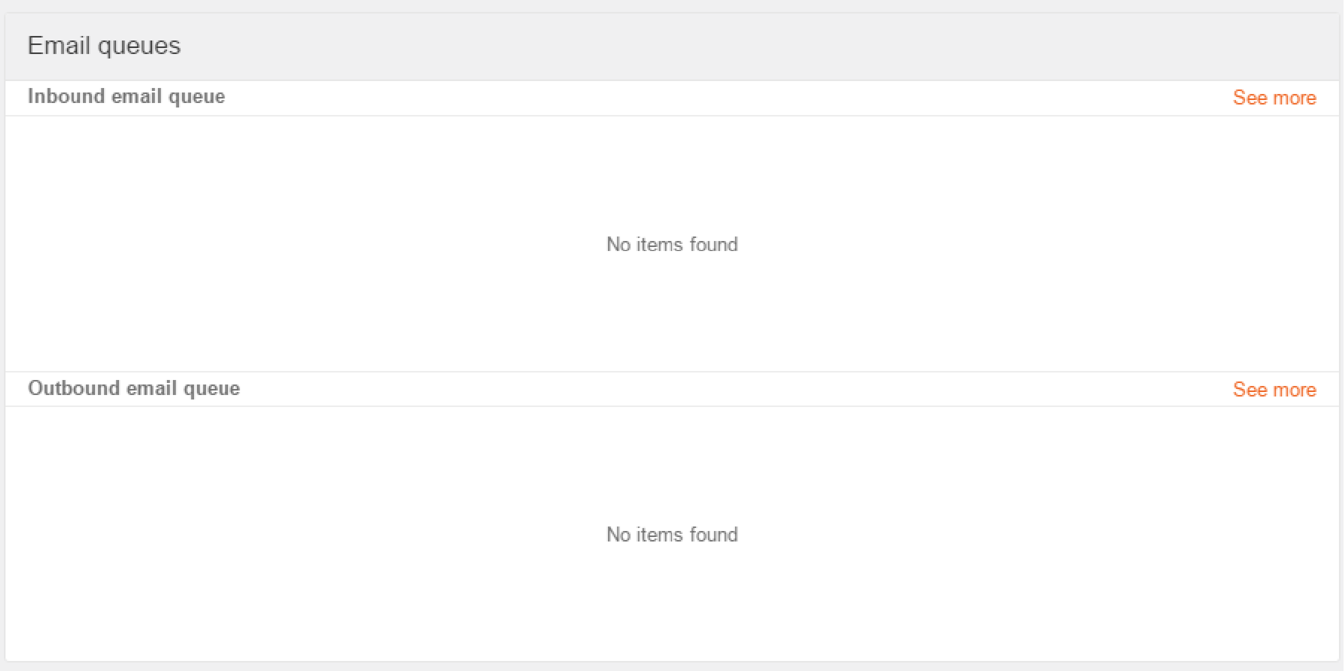
Email continues to be one of the most effective attack vectors for cryptolocker and other viruses. Infections can have dramatic negative impact on any organization, for example two full weeks of downtime. Through Evolve IP's partnership with Mimecast, customers can build a wall of protection around their organization as well as purchase very effective and useful add-on's. Deployed from the cloud, Evolve IP enables customers to focus on implementing the security measures needed without any onsite equipment or mail filtering appliances. And in the case of a planned or unplanned outage, this service provides easy to implement options for continuous web-based email access, management, and use.

The following reference guide has been developed for Evolve IP customers to quickly and effectively navigate the most common functions and interfaces in the mimecast portal.   Please use this guide as a reference during both the onboarding phase of your project as well as for ongoing support as needed. The Evolve IP support staff will be happy to engage with you should there be a request not covered in this guide or in-app support.

Dashboard

When you login you will be immediately taken to your dashboard. From here you will see:

- Hourly email flow of inbound and outbound mail
- Notifications of services (Mimecast updates)
- Directory connectors – journal connectors – exchange services status's
- Email activity (held, rejected, bounced, attachments, policies)
- Rejections



Email queues

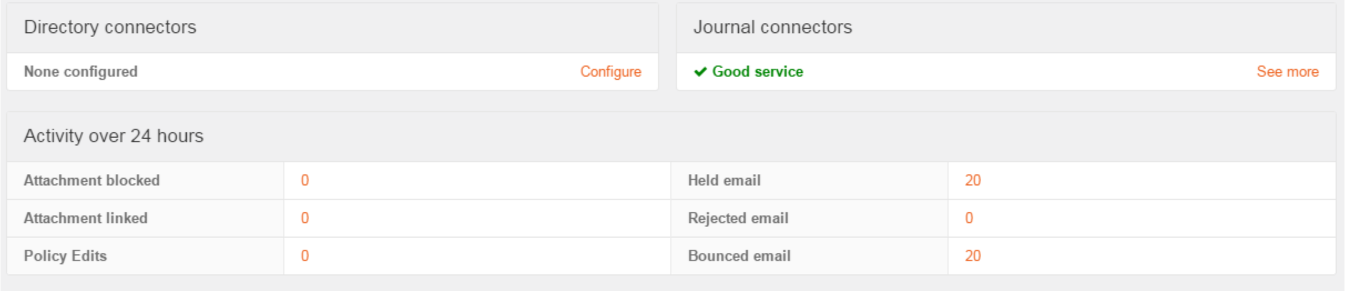
Inbound email queue — See more

No items found

Outbound email queue — See more

No items found

Through these tables you are able to click orange highlighted areas to view more, fix issues, or change settings.



Directory connectors

None configured — Configure

Journal connectors

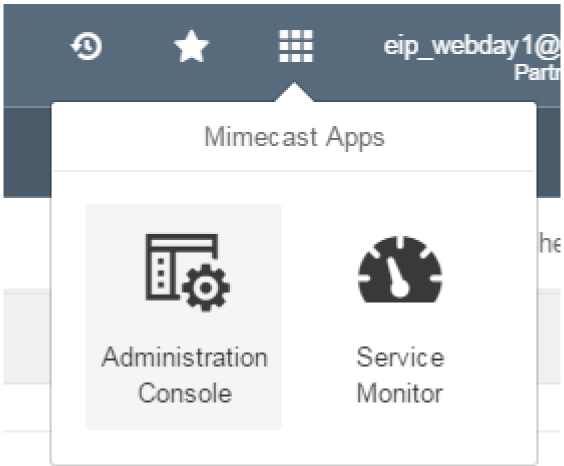
✓ Good service — See more

Activity over 24 hours

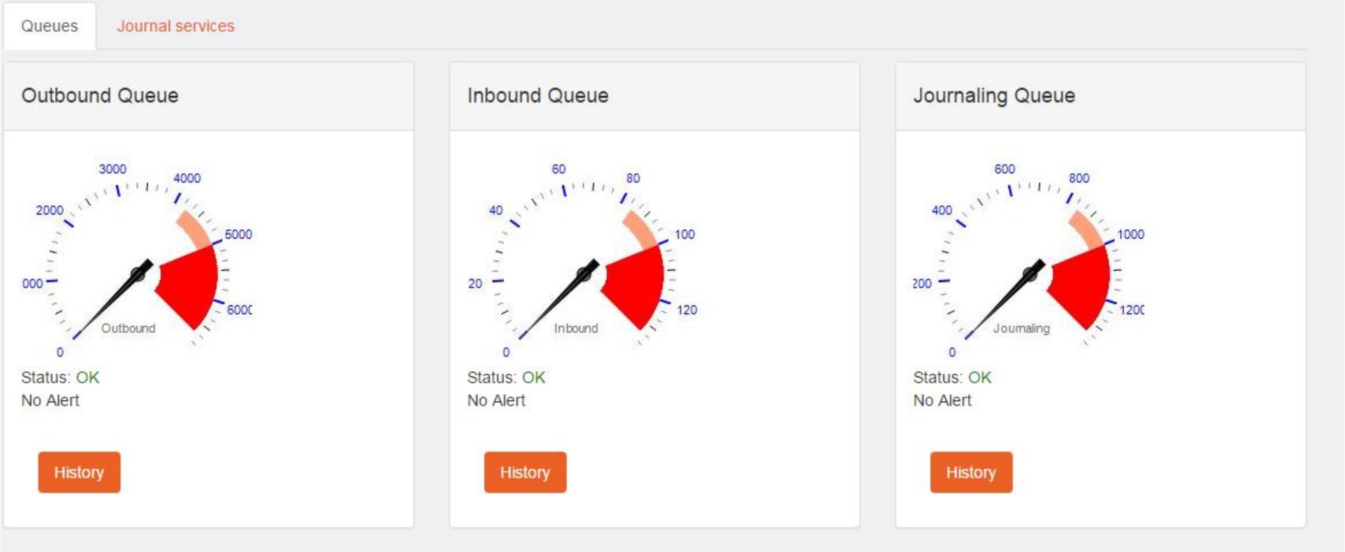
Attachment blocked	0	Held email	20
Attachment linked	0	Rejected email	0
Policy Edits	0	Bounced email	20

Service Monitor

From the top right panel, selecting service monitor will open up another browser.



From there you can view your queues from a 15 minute, hourly or daily flow and monitor your data.



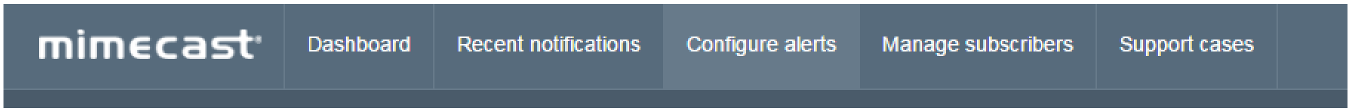
Outbound Queue: Status: OK, No Alert

Inbound Queue: Status: OK, No Alert

Journaling Queue: Status: OK, No Alert

Configure Alerts

From the top of the service monitor page, select configure alerts.



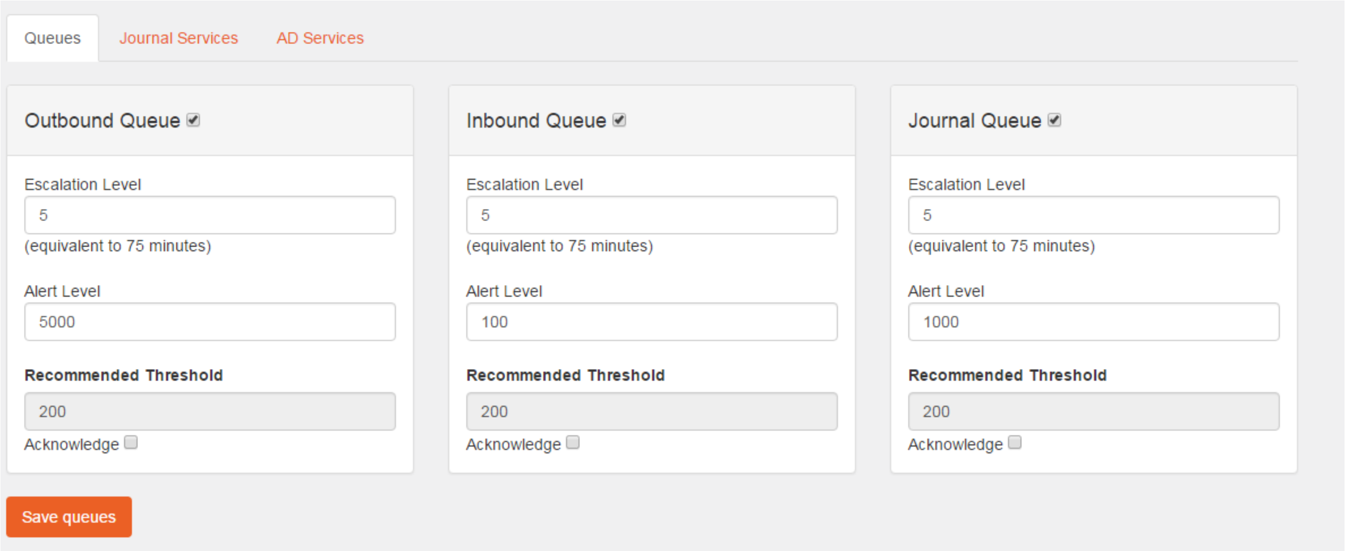
Enable and set the thresholds for all alert types. Additionally subscribers should be configured with notification options in order to start receiving the alerts.

Escalation Level – The number of alerts that are sent out, before the escalation point is notified (default is set to 5).

Alert Level – Once the number of items in a queue goes beyond this threshold an alert is generated.

Recommended Threshold - This is an auto generated threshold based on the recent history of your account queues.

Acknowledge the alerts – Once this option is checked, no further notifications for this particular alert are sent. Once the queue is no longer in alert this flag is re-set.



Outbound Queue ☑

Escalation Level: 5
(equivalent to 75 minutes)

Alert Level: 5000

Recommended Threshold: 200

Acknowledge □

Inbound Queue ☑

Escalation Level: 5
(equivalent to 75 minutes)

Alert Level: 100

Recommended Threshold: 200

Acknowledge □

Journal Queue ☑

Escalation Level: 5
(equivalent to 75 minutes)

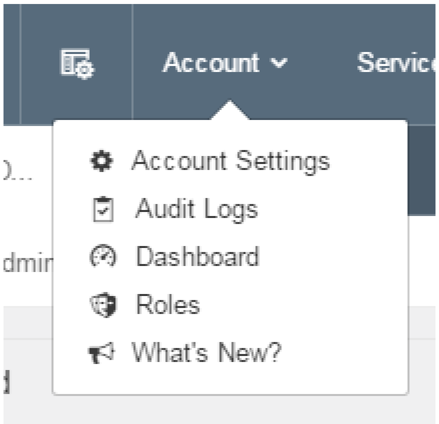
Alert Level: 1000

Recommended Threshold: 200

Acknowledge □

Account settings

To manage account settings, from the administration console go to account then account settings



Below you will be able to change settings for:

Account settings: license and retention details regarding your Mimecast account

> **NOTE**: The pause inbound deliveries option is a great tool to note. By enabling this option it allows you to globally halt Mimecast from sending emails to your mail server(s). You may need this if you mail server(s) is temporarily unable to accept emails due to an unplanned outage, software updates, geographical event, or server relocation. Emails would still be accessible through Mimecast User Services while they are paused.

Directory Options: Determines is LDAP integration is enabled

User Access and Permissions: Configure global access for users and timeout for Administration Console sessions

Mimecast provides several ways to assign user permissions:

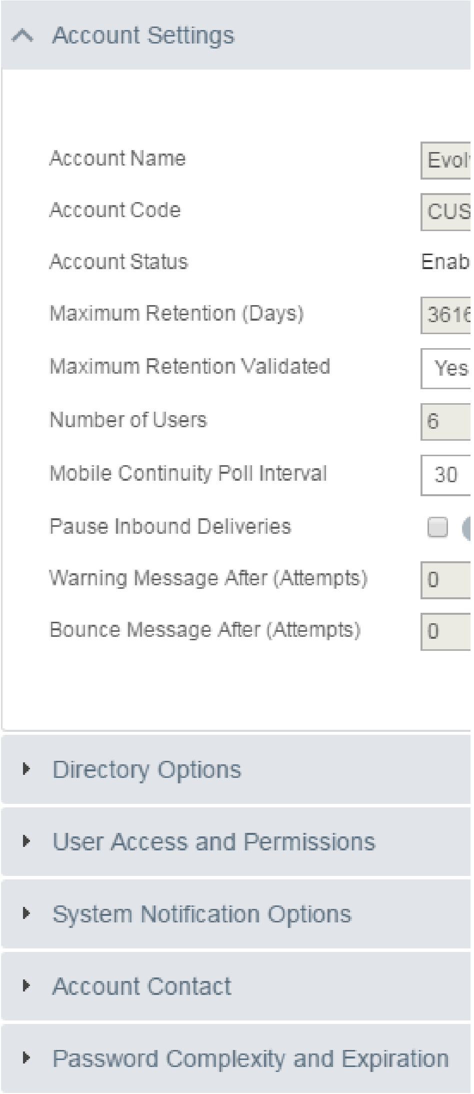
- Configured for the entire organization using Application Setting definition
- Configured manually at the individual email level
- Imported in bulk using a spreadsheet import

System Notification Options: Specify certain notification addresses

Account Contact: Account contact details

Password Complexity and Expiration: Control password complexity, expiration and account lockout for Mimecast Cloud Passwords

NOTE: These settings apply to Mimecast user account, and therefore only affect cloud passwords, not Active Directory accounts and passwords



Account Settings

Account Name	Evol
Account Code	CUS
Account Status	Enab
Maximum Retention (Days)	3616
Maximum Retention Validated	Yes
Number of Users	6
Mobile Continuity Poll Interval	30
Pause Inbound Deliveries	☐
Warning Message After (Attempts)	0
Bounce Message After (Attempts)	0

Directory Options

User Access and Permissions

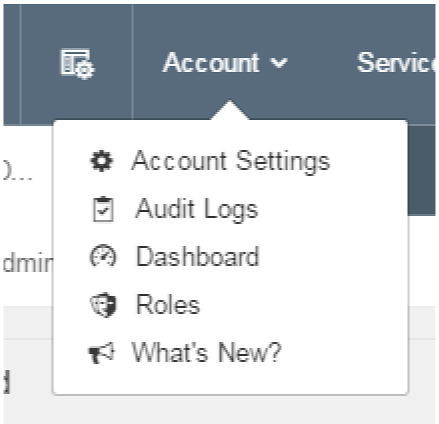
System Notification Options

Account Contact

Password Complexity and Expiration

Account roles

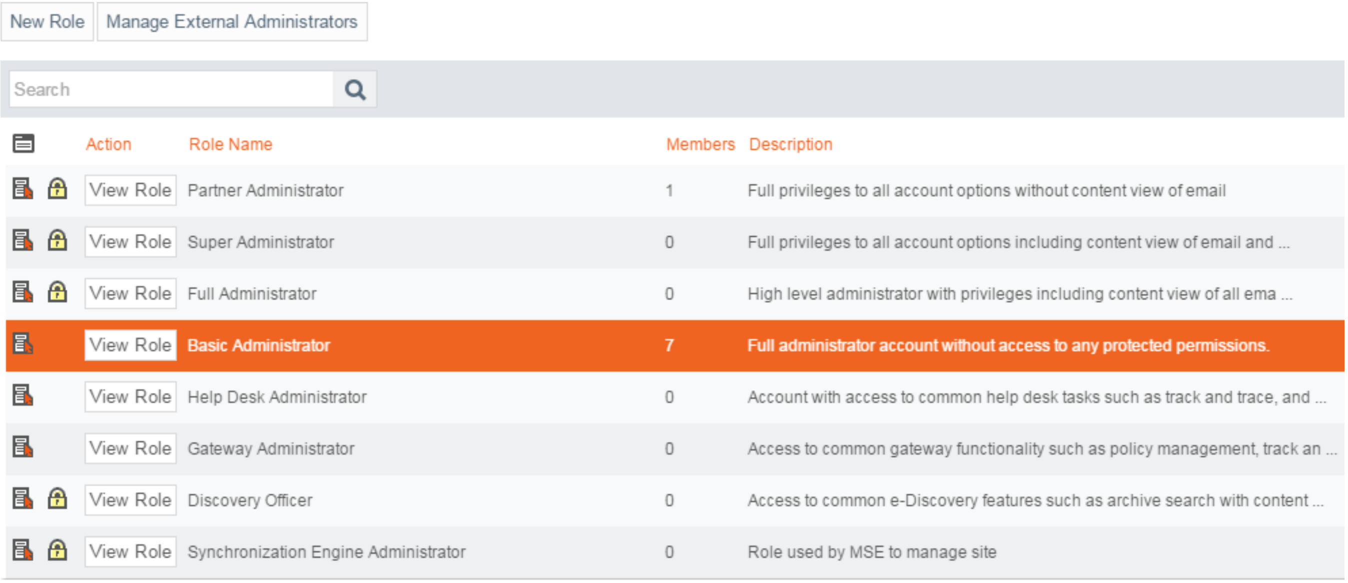
Access account roles by going to the account tab and selecting “roles”



Roles are used to provide access rights for those who need to use the Administration Console. Each role determines the depth of access, and can be used to control the tasks that can be performed by an administrator.

1. To access the Role Editor, navigate to Account | Roles.
2. Default roles cannot be edited or deleted, and are shown in plain text with the option to view the Role (by selecting the View Role button)
3. Customized Roles are shown in italics, and can be edited (by selecting the Edit Role button)
4. To create a new Role, select the Create Role button
5. To copy an existing Role, right-click the Role and select Copy Role
6. To view a list of Administrators assigned to a Role, click on the Role
7. To add members to a Role, select the Role, and click the Add Users to Role button. Use the search field, then select the individuals email address
8. Roles with a padlock icon on the left indicate that the role has protected permissions assigned
9. A specific user can only belong to one Role at any given time. If the user’s email address is added to a second Role, the address entry in the original Role is automatically removed.

To view the role assigned to a user, navigate to Directory | Internal, open the relevant domain, and select the users email address. The role will be displayed, as well as the ability to edit the role by clicking on the Role Edit button:



		Action	Role Name	Members	Description
	🔒	View Role	Partner Administrator	1	Full privileges to all account options without content view of email
	🔒	View Role	Super Administrator	0	Full privileges to all account options including content view of email and ...
	🔒	View Role	Full Administrator	0	High level administrator with privileges including content view of all ema ...
		View Role	Basic Administrator	7	Full administrator account without access to any protected permissions.
		View Role	Help Desk Administrator	0	Account with access to common help desk tasks such as track and trace, and ...
		View Role	Gateway Administrator	0	Access to common gateway functionality such as policy management, track an ...
	🔒	View Role	Discovery Officer	0	Access to common e-Discovery features such as archive search with content ...
	🔒	View Role	Synchronization Engine Administrator	0	Role used by MSE to manage site

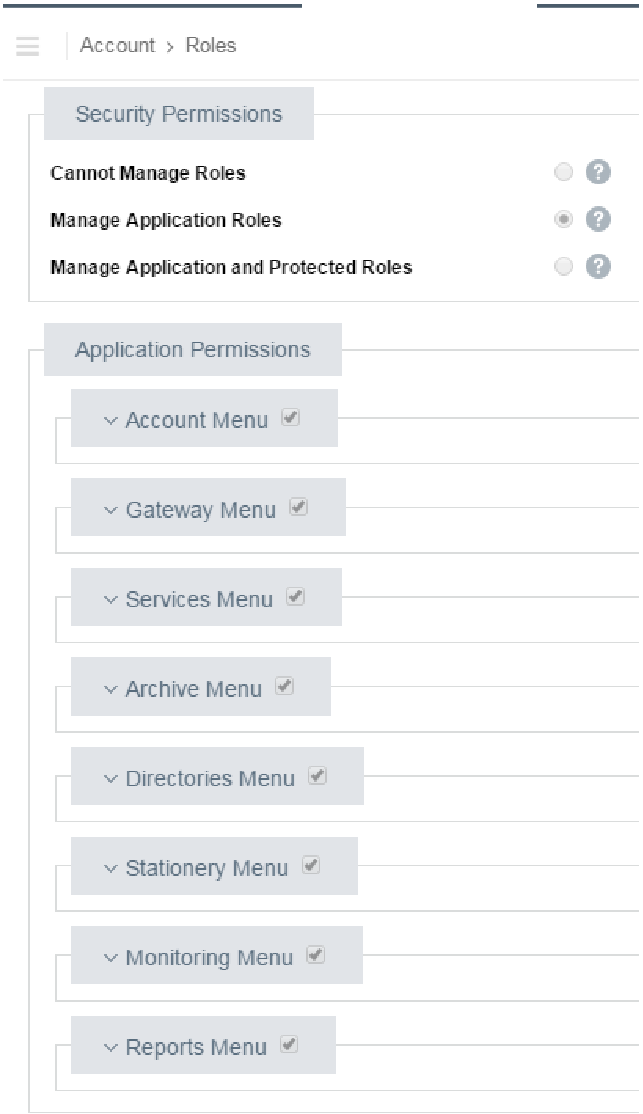
Roll permissions are broken down as follows:

Application: Access to menu options in the admin console. Typically read or write access is enabled

Protected: Ability to perform protected tasks (e.g. viewing the content of email, exporting emails, or assigning permissions to view Smart Tags)

Security: Additional access to the Role Editor, to control the management of roles and administrators, options are:

- Cannot manage roles - Do not see roles tab displayed
- Manage Application roles – Able to modify access to admin console tabs
- Protected roles – able to modify admin access to protected application areas



Account › Roles

Security Permissions

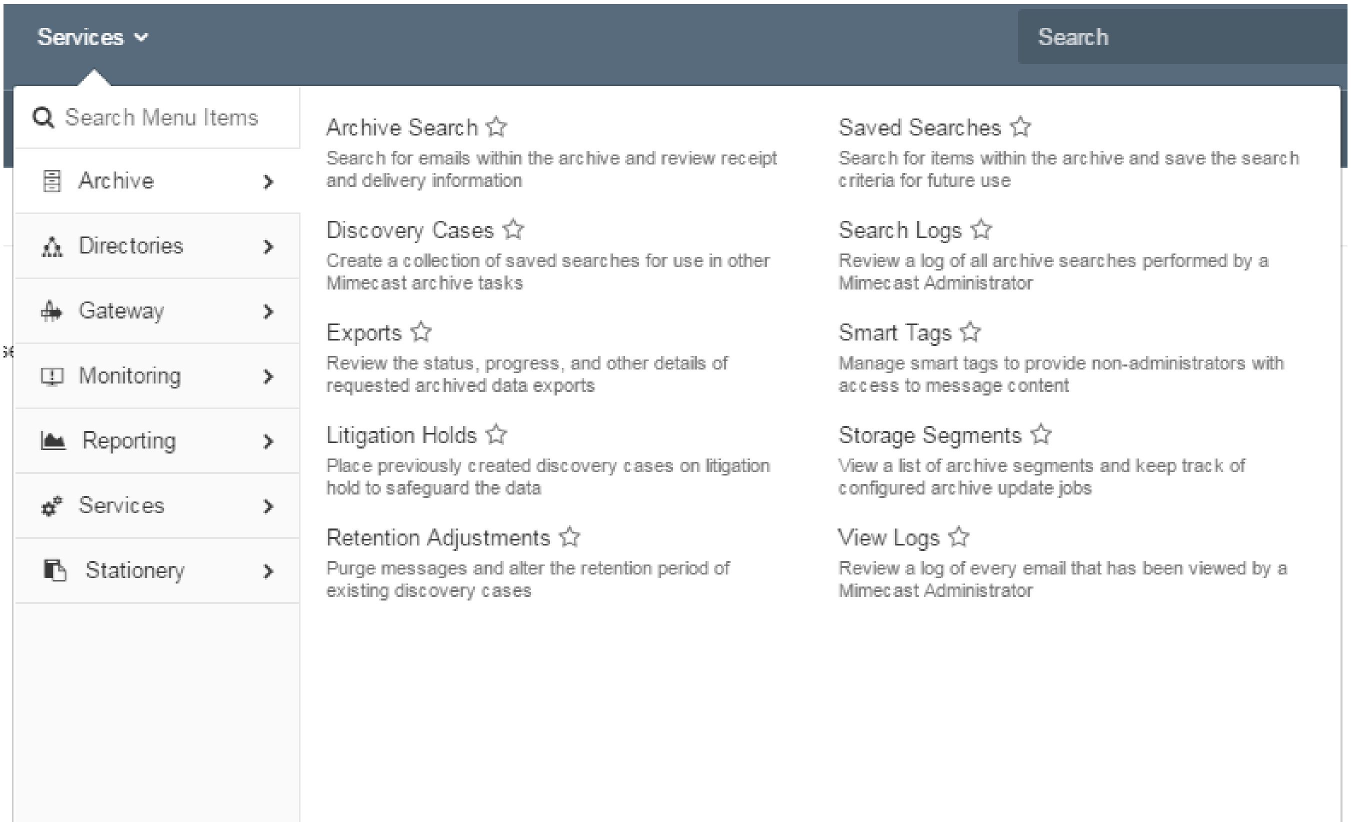
- ○ Cannot Manage Roles
- ● Manage Application Roles
- ○ Manage Application and Protected Roles

Application Permissions

- Account Menu ☑
- Gateway Menu ☑
- Services Menu ☑
- Archive Menu ☑
- Directories Menu ☑
- Stationery Menu ☑
- Monitoring Menu ☑
- Reports Menu ☑

Archive

To access your archive, click “services” tab and select archive. Here you will see your options for managing your archive with a brief description.



Archive Search ☆
Search for emails within the archive and review receipt and delivery information

Saved Searches ☆
Search for items within the archive and save the search criteria for future use

Discovery Cases ☆
Create a collection of saved searches for use in other Mimecast archive tasks

Search Logs ☆
Review a log of all archive searches performed by a Mimecast Administrator

Exports ☆
Review the status, progress, and other details of requested archived data exports

Smart Tags ☆
Manage smart tags to provide non-administrators with access to message content

Litigation Holds ☆
Place previously created discovery cases on litigation hold to safeguard the data

Storage Segments ☆
View a list of archive segments and keep track of configured archive update jobs

Retention Adjustments ☆
Purge messages and alter the retention period of existing discovery cases

View Logs ☆
Review a log of every email that has been viewed by a Mimecast Administrator

Creating an Archive Search

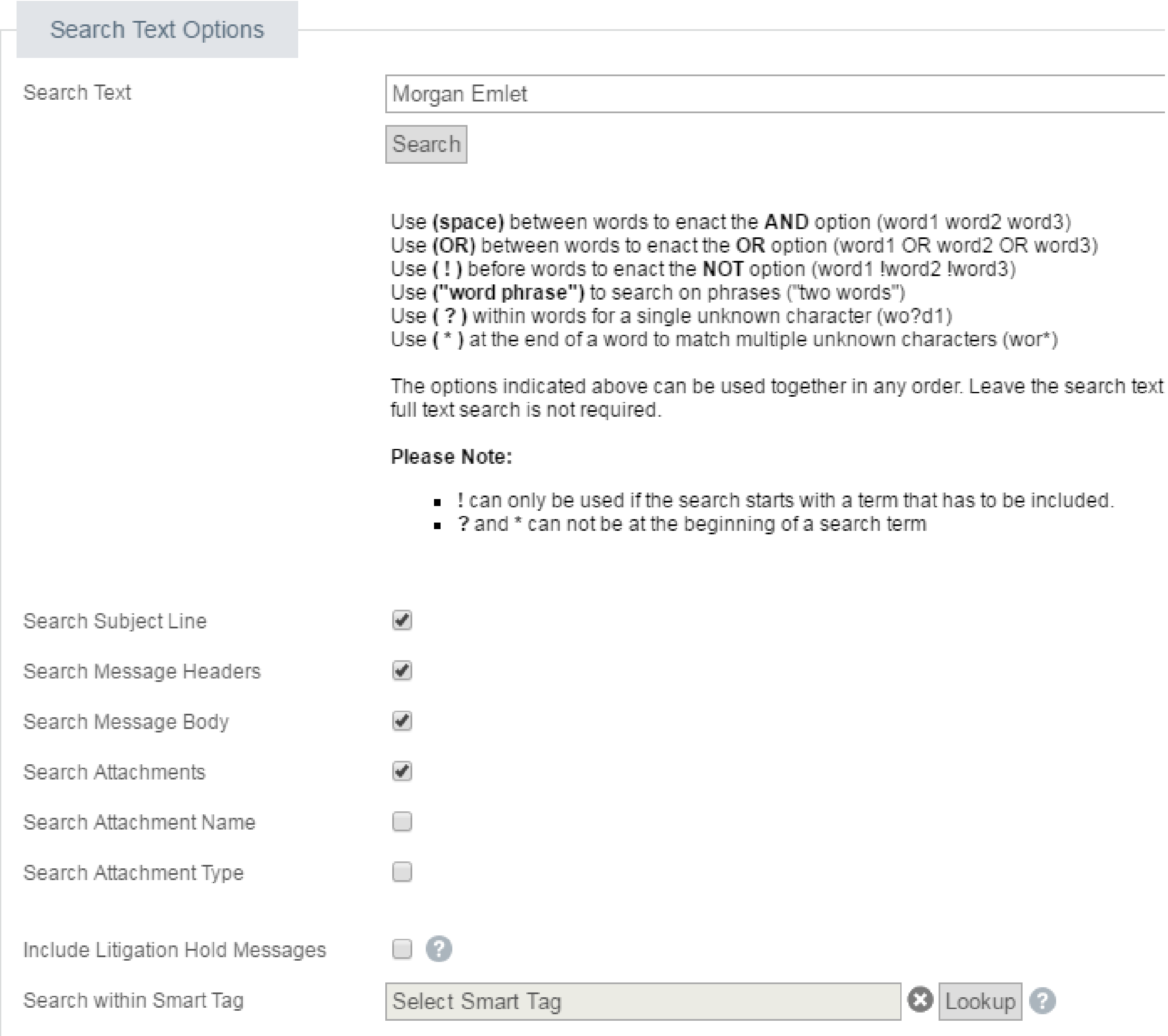
Go to services > archive > archive search

The archive search allows administrators to perform a full search across all emails in the archive, including ingested historical email data. The ability to search the Mimecast archive instantly for email data, provides the administrator with access to email delivery information. This aids in troubleshooting email delivery queries. Administrators with appropriate permissions are also able to read the contents of emails in the archive, forward emails to internal users, or export emails from the Mimecast platform. Archive searches can also be saved with their search parameters for repeated use.

Search Text Options:

Search Text: This field is used to specify the text to search for and allows searches to be performed using Boolean search parameters. When entering the text, it can be entered exactly, or if you’re not sure, you have the ability to use some wild card characters.

Search within smart tag: If a Smart Tag is selected using the **Lookup** button, the search results will be filtered to only return the results from that Smart Tag. Use the X to clear a selected Smart Tag.



Search Text Options

Search Text: Morgan Emlet

Use **(space)** between words to enact the **AND** option (word1 word2 word3)
Use **(OR)** between words to enact the **OR** option (word1 OR word2 OR word3)
Use **(!)** before words to enact the **NOT** option (word1 !word2 !word3)
Use **("word phrase")** to search on phrases ("two words")
Use **(?)** within words for a single unknown character (wo?d1)
Use **(*)** at the end of a word to match multiple unknown characters (wor*)

The options indicated above can be used together in any order. Leave the search text
full text search is not required.

Please Note:

- ! can only be used if the search starts with a term that has to be included.
- ? and * can not be at the beginning of a search term

Search Subject Line ☑

Search Message Headers ☑

Search Message Body ☑

Search Attachments ☑

Search Attachment Name □

Search Attachment Type □

Include Litigation Hold Messages □

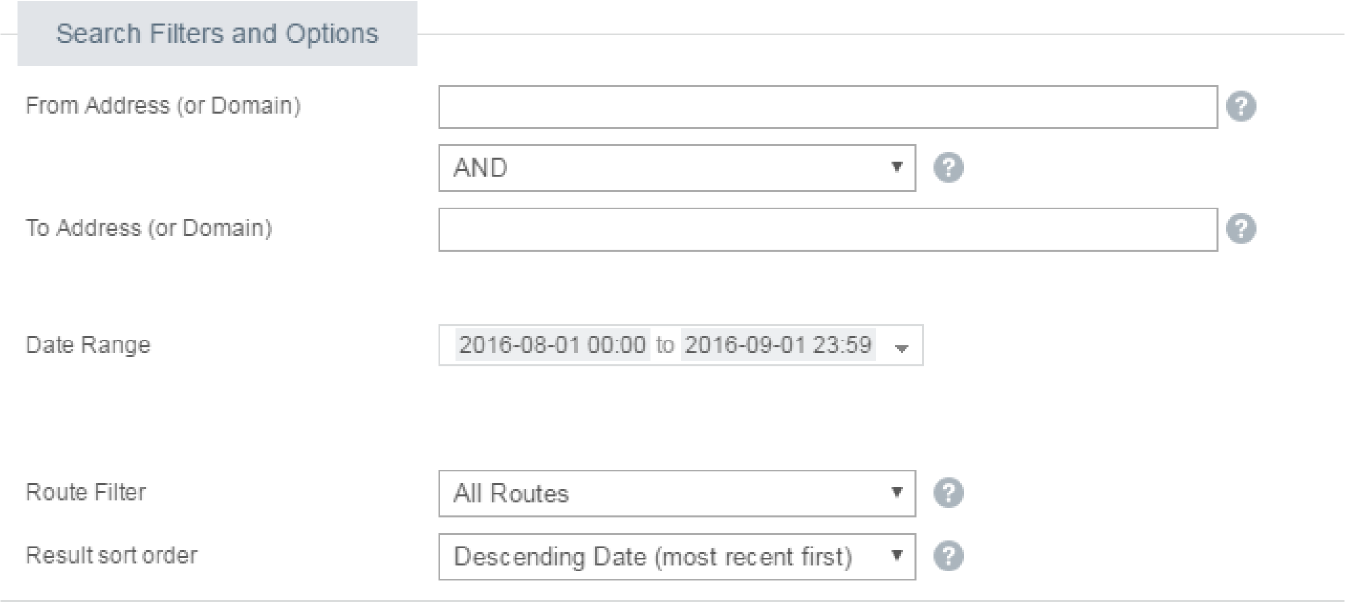
Search within Smart Tag: Select Smart Tag

Additional Search parameters can be specified within the **Search Filters and Options** section. To ensure that only relevant search data is returned, it is important to specify as many filters as possible

To and From fields:

- You cannot use a wildcard at the beginning of the entry
- If you are looking for multiple addresses, list them by separating them with a space
- If you are not sure of the full email address, enter the name part and then add a wildcard (*) for the domain portion
- You can use the term NOT to specify an email address or domain to exclude from the results

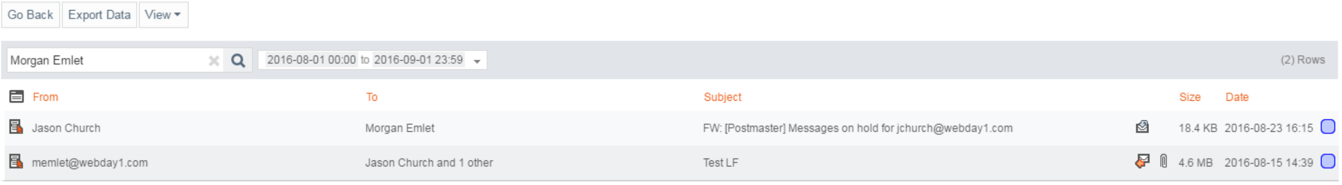
Then, fill in the rest of the fields to fit your criteria



Search Filters and Options

From Address (or Domain)	
	AND ▾
To Address (or Domain)	
Date Range	2016-08-01 00:00 to 2016-09-01 23:59
Route Filter	All Routes ▾
Result sort order	Descending Date (most recent first) ▾

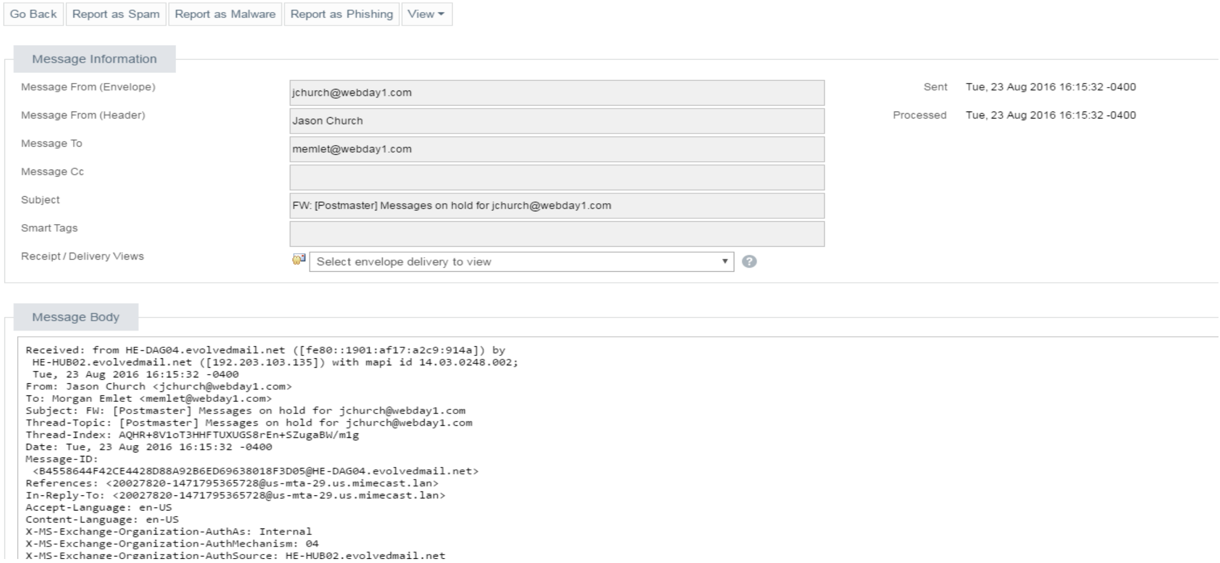
Click the "search" button to initiate the search. With correct permissions, administrators are able to *Forward Selected Items* or *Export* email messages from the Archive.



Morgan Emlet — 2016-08-01 00:00 to 2016-09-01 23:59 — (2) Rows

From	To	Subject	Size	Date
Jason Church	Morgan Emlet	FW: [Postmaster] Messages on hold for jchurch@webday1.com	18.4 KB	2016-08-23 16:15
memlet@webday1.com	Jason Church and 1 other	Test LF	4.6 MB	2016-08-15 14:39

Depending on your permissions you are able to click into each email to see the message, from here you can report emails for spam, phishing and malware if need be



Message Information

Message From (Envelope)	jchurch@webday1.com	Sent	Tue, 23 Aug 2016 16:15:32 -0400
Message From (Header)	Jason Church	Processed	Tue, 23 Aug 2016 16:15:32 -0400
Message To	memlet@webday1.com		
Message Cc			
Subject	FW: [Postmaster] Messages on hold for jchurch@webday1.com		
Smart Tags			
Receipt / Delivery Views	Select envelope delivery to view ▾		

Message Body

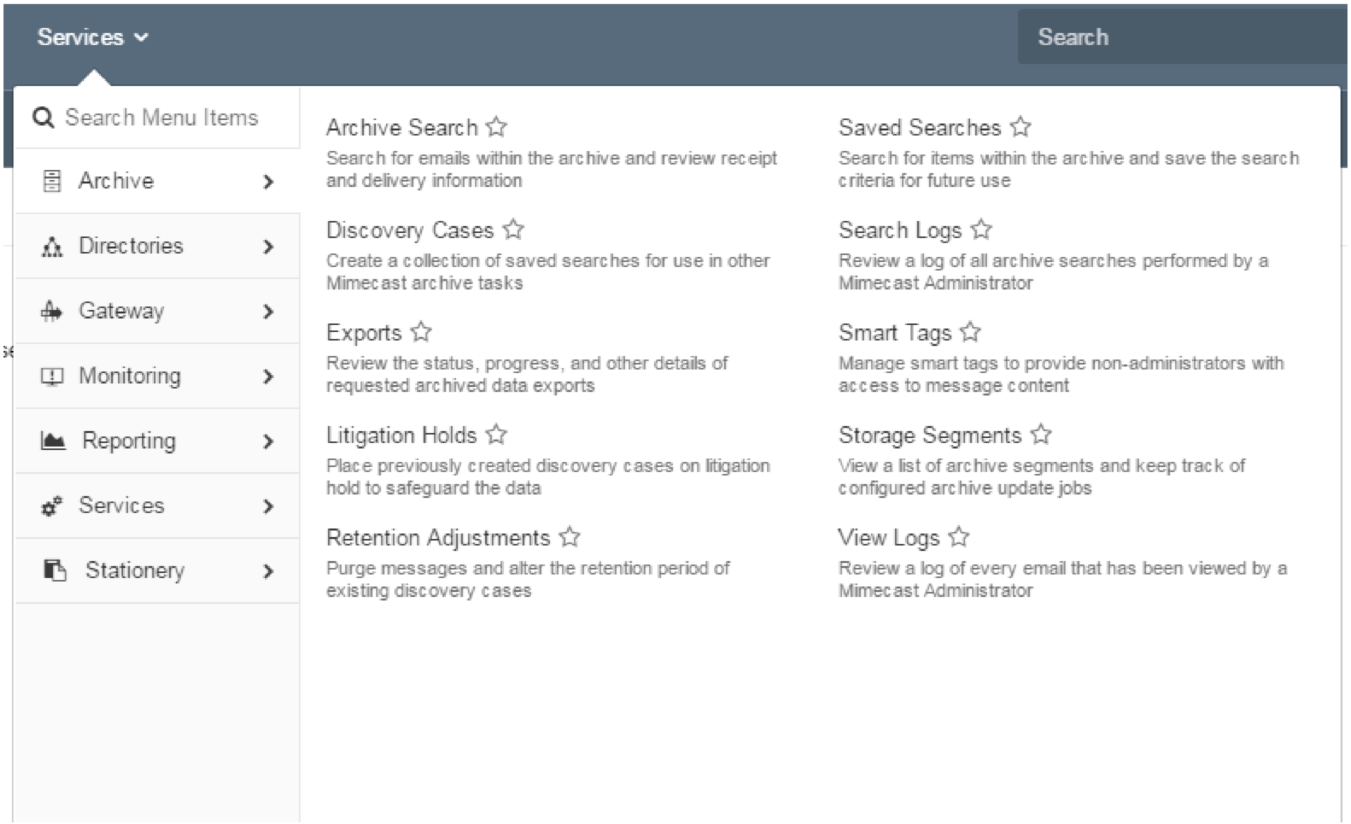
```
Received: from HE-DAG04.evolvedmail.net ([fe80::1901:af17:a2c9:914a]) by
 HE-HUB02.evolvedmail.net ([192.203.103.135]) with mapi id 14.03.0248.002;
 Tue, 23 Aug 2016 16:15:32 -0400
From: Jason Church <jchurch@webday1.com>
To: Morgan Emlet <memlet@webday1.com>
Subject: FW: [Postmaster] Messages on hold for jchurch@webday1.com
Thread-Topic: [Postmaster] Messages on hold for jchurch@webday1.com
Thread-Index: AQHR+8V1oT3HHFTUXUGS8rEn+SZugaBW/m1g
Date: Tue, 23 Aug 2016 16:15:32 -0400
Message-ID:
 <B4558644F42CE4428D88A92B6ED69638018F3D05@HE-DAG04.evolvedmail.net>
References: <20027820-1471795365728@us-mta-29.us.mimecast.lan>
In-Reply-To: <20027820-1471795365728@us-mta-29.us.mimecast.lan>
Accept-Language: en-US
Content-Language: en-US
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-MS-Exchange-Organization-AuthSource: HE-HUB02.evolvedmail.net
```

Creating a saved Archive Search

An Archive Search allows a Mimecast Administrator or end user to filter messages in the Mimecast Archive. The criteria used in the search can be retained for ease of use in future searches using a Saved Search.

Saves searches have multiple uses:

- To save frequently used search parameters
- As part of a message export
- For eDiscovery cases



Archive Search ☆
Search for emails within the archive and review receipt and delivery information

Discovery Cases ☆
Create a collection of saved searches for use in other Mimecast archive tasks

Exports ☆
Review the status, progress, and other details of requested archived data exports

Litigation Holds ☆
Place previously created discovery cases on litigation hold to safeguard the data

Retention Adjustments ☆
Purge messages and alter the retention period of existing discovery cases

Saved Searches ☆
Search for items within the archive and save the search criteria for future use

Search Logs ☆
Review a log of all archive searches performed by a Mimecast Administrator

Smart Tags ☆
Manage smart tags to provide non-administrators with access to message content

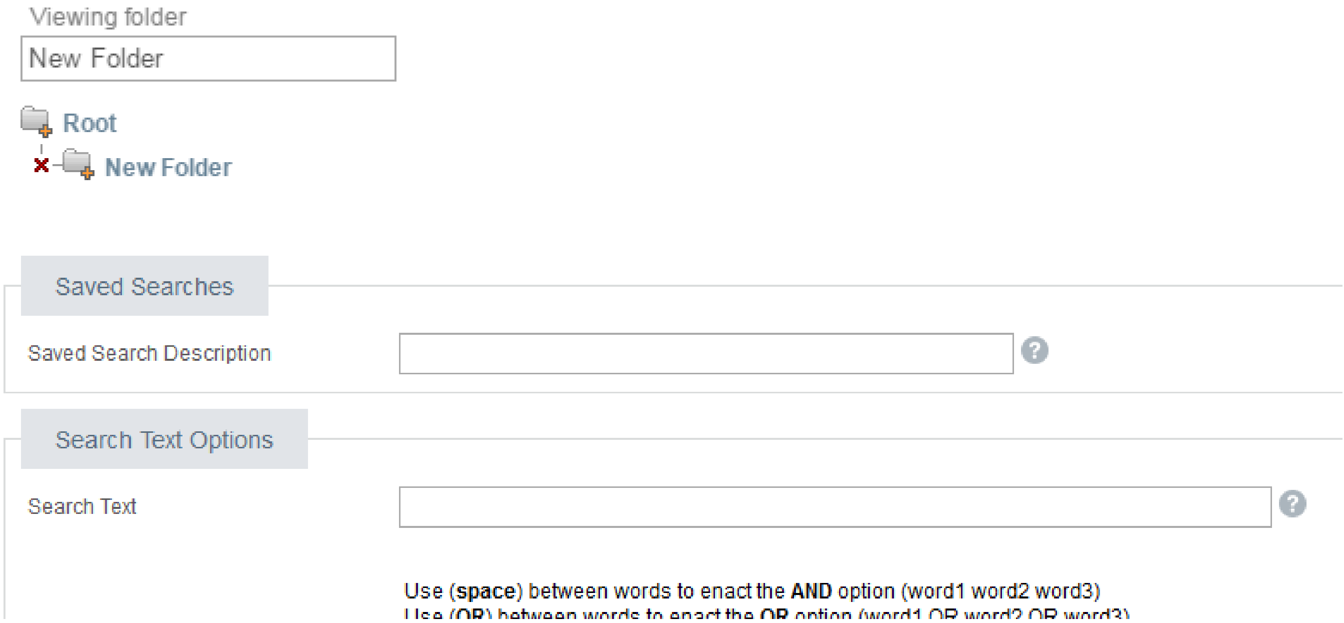
Storage Segments ☆
View a list of archive segments and keep track of configured archive update jobs

View Logs ☆
Review a log of every email that has been viewed by a Mimecast Administrator

To create a saved search:

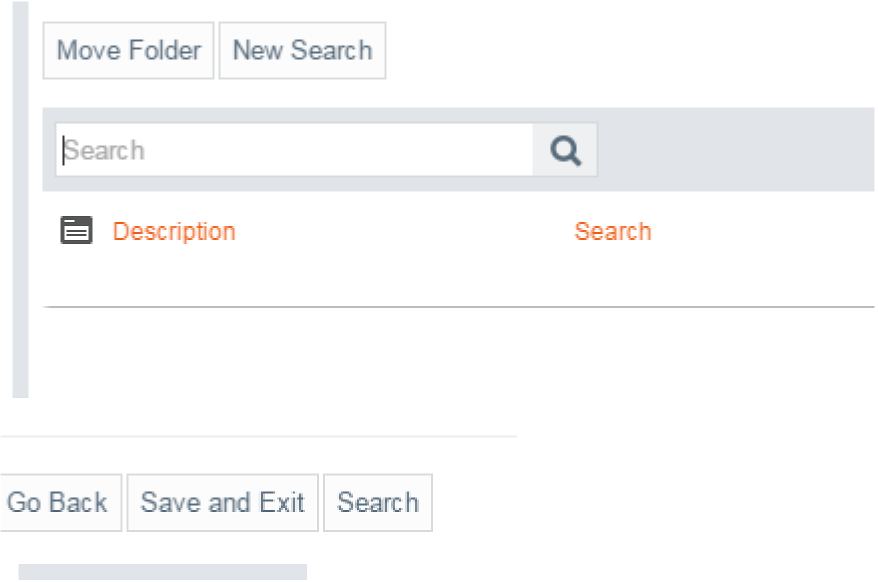
1. Log in to the Administration Console.
2. Click on the Services toolbar button. A menu drop down is displayed.
3. Click on the Archive | Saved Searches menu item. A list of your saved searches is displayed.
4. Select the New Search button.

5. Click the “+” sign on the Root folder to create a subfolder, and click inside the subfolder. You cannot save a search in the Root folder.
6. A page similar to the Archive Search page is now displayed. The only difference is that a Saved Search Description field is available. This allows you to provide a description for the search:



Use (**space**) between words to enact the **AND** option (word1 word2 word3)
Use (**OR**) between words to enact the **OR** option (word1 OR word2 OR word3)

7. Select the Search button to view the results. Once the search results are displayed, the View menu can be used to re-sort the results.
8. Select the Go Back button when you've confirmed the results and search criteria.
9. Select the Save and Exit button to save the search criteria. You are returned to the list of all saved searches (if any). To view the search results, find the saved search in the list and select it.



Adding an eDiscovery Case

eDiscovery Cases allow administrators to group multiple Archive Searches together in a single case. They can be used in a number of ways:

Export: Messages can be exported from the administration console in zip files containing messages in eml format

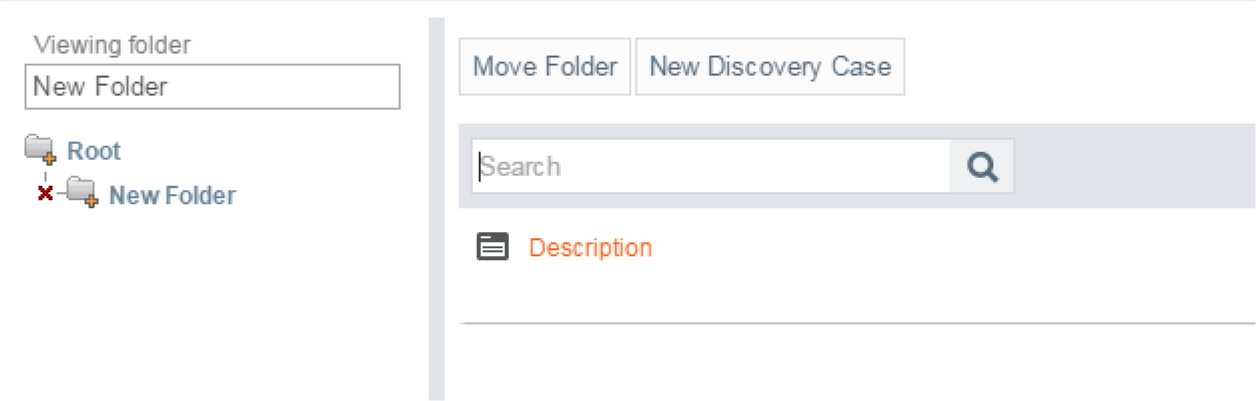
Retention Adjustment: Messages can be made subject to a retention adjustment, to increase or decrease the length of time that they are stored in the Mimecast archive

Litigation hold: Messages can be placed in litigation hold, where they will not be expired from the Mimecast archive for a period of time defined by an Administrator. This is regardless of the messages actual expiry date

Link to Smart Tag: Messages can be linked to a Smart Tag. This allows individual users or groups or users to view archived messages, where they are not the sender or recipient

To create an eDiscovery case:

1. Log in to the Administration Console.
2. Click on the Services toolbar button. A menu drop down is displayed.
3. Click on the Archive | Discovery Cases menu item.
4. Click on the New discovery Case button

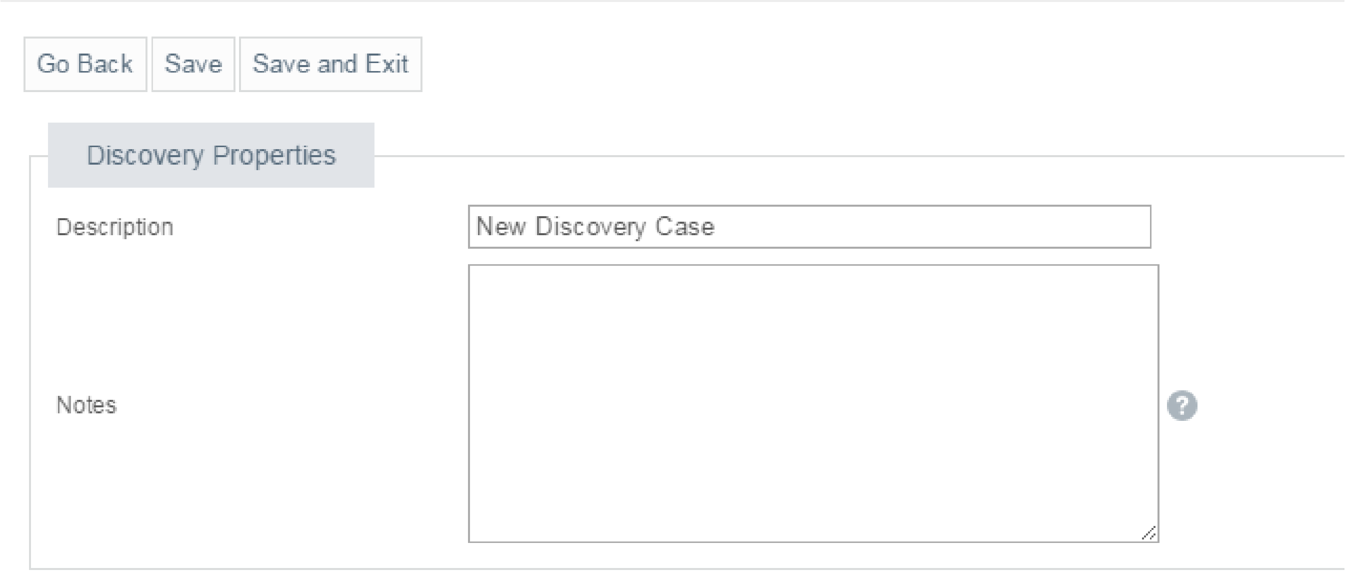


5. Complete the Discovery Properties dialog as follows

   Description – enter in a description for your case. This will be displayed in the Discovery Case Definitions list

   Notes – Enter the case details. This helps you and other Admins identify the case at a later date

   Click save and exit



Description: New Discovery Case

Notes

Search logs

The Archive contains the email communications for your organization within Mimecast. It is important, therefore, that a full log be kept of individuals with Administrative permissions that have performed searches in the Archive. The **Search Logs** lists all searches performed by Administrators, including those that have not been saved.

To display a search log file:

1. Log in to the Administration Console.
2. Click on the Services toolbar button. A menu drop down is displayed.
3. Click on the Archive | Search Logs menu item. A list of log files is displayed.
4. Click on a log file to display the following details:

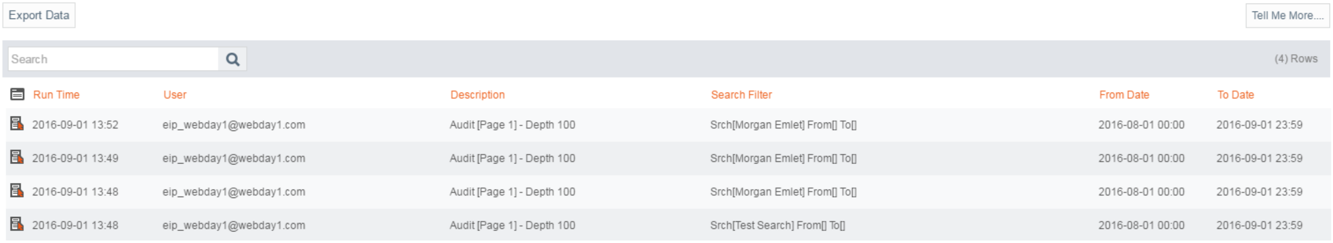
Run time: Time and date stamp of when the search was run

User: The admin that performed the search

Description: The name of the saves search

Search filter: details the parameters of the search

To and From date: indicates starting and end date filter applied to the search



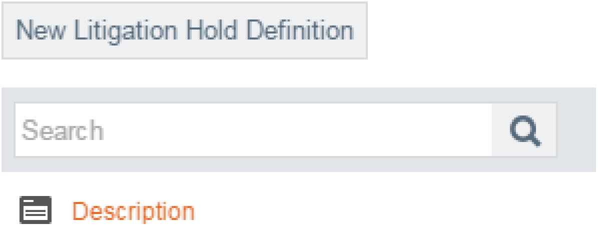
Run Time	User	Description	Search Filter	From Date	To Date
2016-09-01 13:52	eip_webday1@webday1.com	Audit [Page 1] - Depth 100	Srch[Morgan Emlet] From[] To[]	2016-08-01 00:00	2016-09-01 23:59
2016-09-01 13:49	eip_webday1@webday1.com	Audit [Page 1] - Depth 100	Srch[Morgan Emlet] From[] To[]	2016-08-01 00:00	2016-09-01 23:59
2016-09-01 13:48	eip_webday1@webday1.com	Audit [Page 1] - Depth 100	Srch[Morgan Emlet] From[] To[]	2016-08-01 00:00	2016-09-01 23:59
2016-09-01 13:48	eip_webday1@webday1.com	Audit [Page 1] - Depth 100	Srch[Test Search] From[] To[]	2016-08-01 00:00	2016-09-01 23:59

Litigation Holds

Litigation Holds allow Administrators to preserve emails in the archive, ensuring that their retention periods aren't adjusted either via a Retention Adjustment, a Folder Based Retention (FBR) task or a retention preservation policy. Messages are identified using an eDiscovery Case and placed into a Litigation Hold. The date selected for the hold will mean that all emails included will not be purged from Mimecast until the Litigation Hold expires.

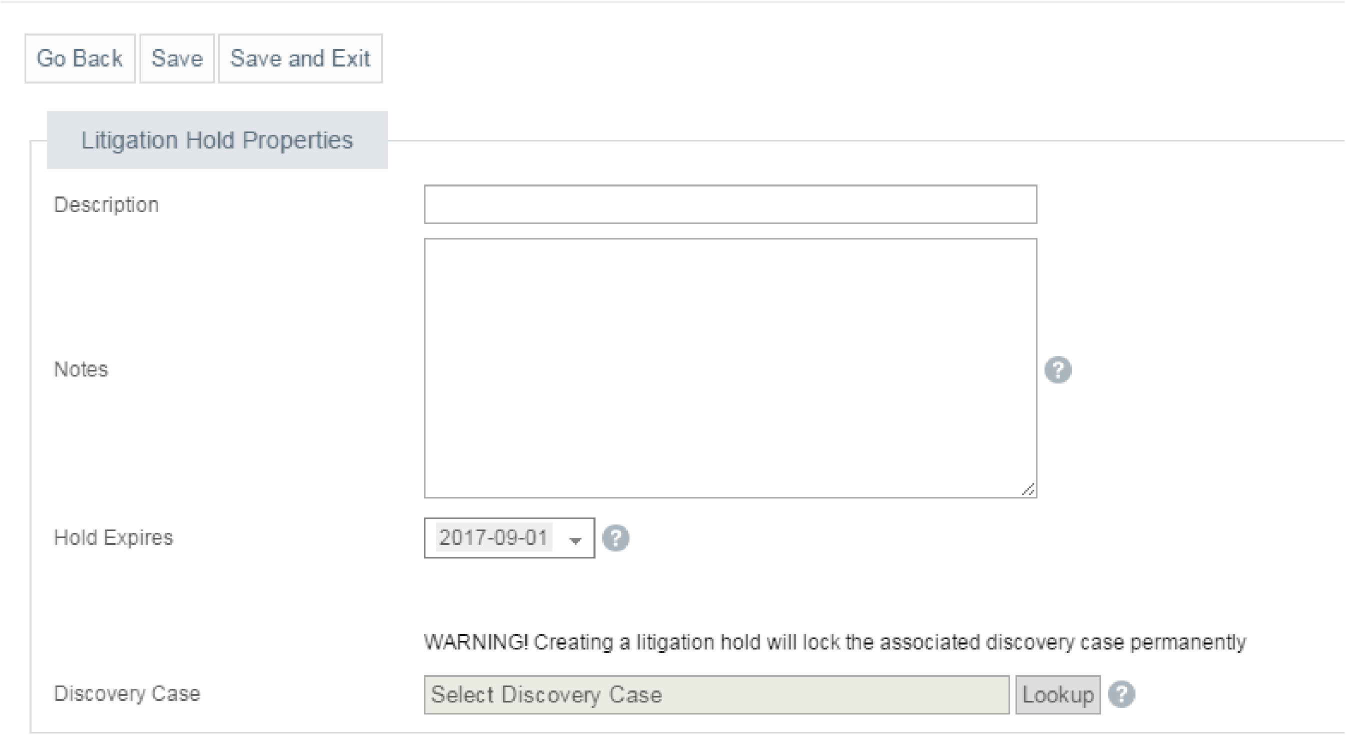
Creating a Hold is a two-step process.

1. An eDiscovery Case must be created (unless implementing a hold on all company emails), which contains the search criteria for emails that are to be held. This ensures that future emails matching these search terms will also be included in the case.
2. A Litigation Hold must be created.



To create a litigation hold:

1. Log in to the Administration Console.
2. Click on the Services toolbar button. A menu drop down is displayed.
3. Click on the Archive | Litigation Holds menu item.
4. Click on the New Litigation Hold Definition button. The Litigation Hold Properties dialog is displayed.



Description

Notes

Hold Expires 2017-09-01

WARNING! Creating a litigation hold will lock the associated discovery case permanently

Discovery Case Select Discovery Case

Complete the dialog above as follows:

Description: Specify a description for your litigation hold

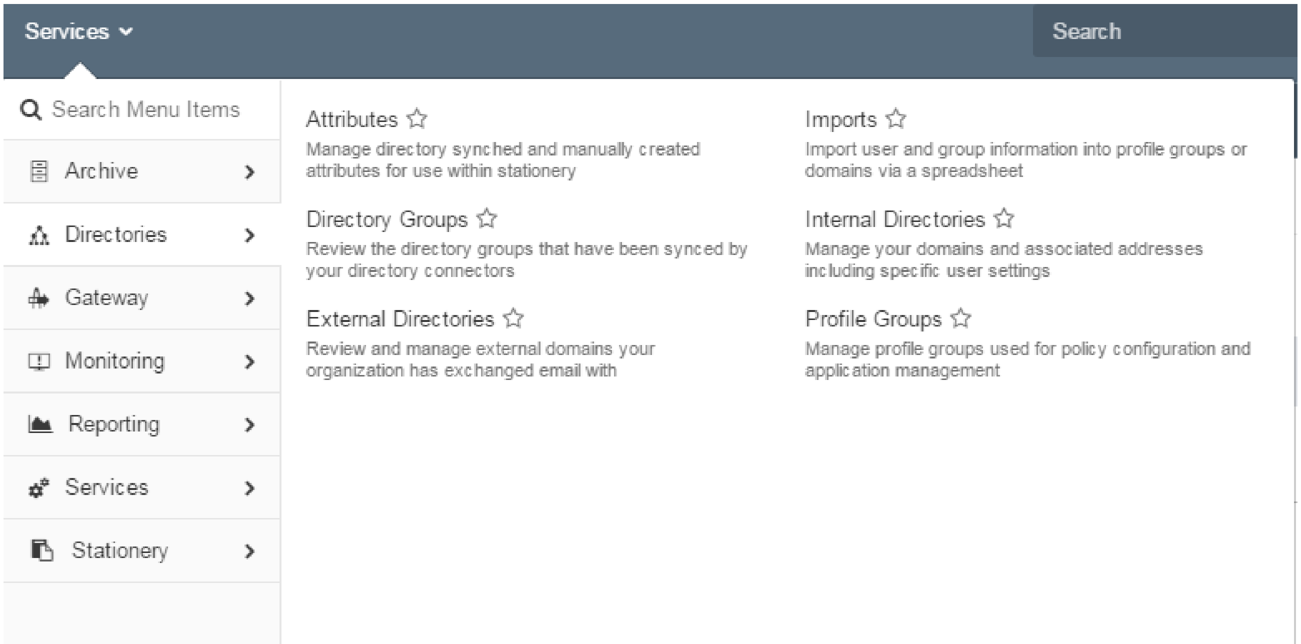
Notes: Any details or reason for hold for other administrators to reference

Hold Expires: Specify a date when the hold expires. Once a Litigation Hold expires, any messages covered by the eDicovery case are subjected to any applicable retention alterations (purge requests)

Then click on **Save and Exit**

Directories

To access directories, go to the “service” tab and click “directories” from here you can view your options and manage your users and groups



Attributes ☆
Manage directory synched and manually created attributes for use within stationery

Directory Groups ☆
Review the directory groups that have been synced by your directory connectors

External Directories ☆
Review and manage external domains your organization has exchanged email with

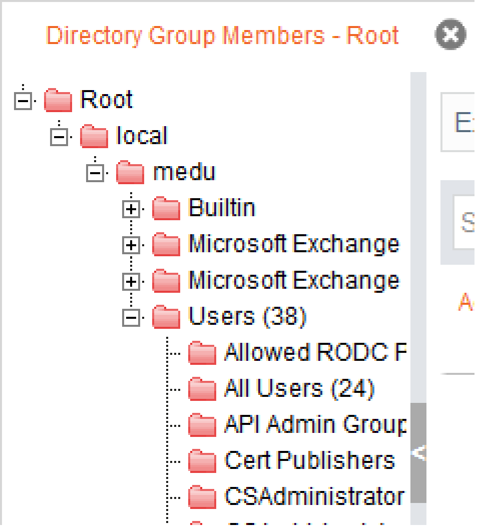
Imports ☆
Import user and group information into profile groups or domains via a spreadsheet

Internal Directories ☆
Manage your domains and associated addresses including specific user settings

Profile Groups ☆
Manage profile groups used for policy configuration and application management

Using Directory Groups

A Directory Group is a listing of synchronized Distribution Lists from the network Directory (such as Active Directory, or AD), using an Directory connector. As with Groups, the Directory Groups contain email addresses, but are synchronized from the network Directory, and cannot be modified in Mimecast.



To access your directory groups:

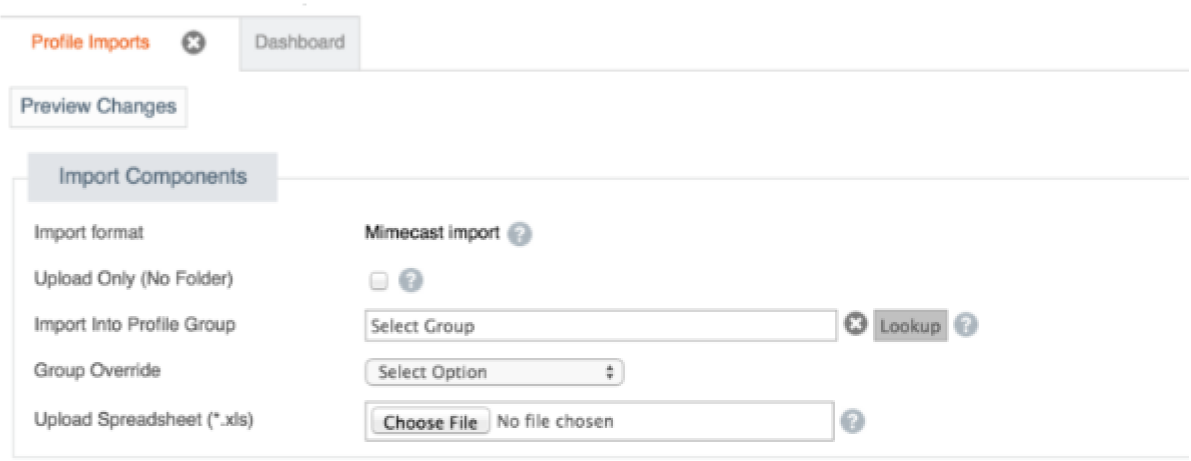
1. Log in to the Administration Console.
2. Click on the Services toolbar button. A menu drop down is displayed.
3. Click on the Directories | Directory Groups menu item.

Add user to Mimecast Using a Spreadsheet Import

To enable your users to receive emails and sign in to Mimecast applications, they will need a user account. You can add multiple user accounts at a time using a spreadsheet import function

After creating your spreadsheet you can import it by:

1. Sign-in to the Administration Console.
2. Select the Directories | Import menu item.



Import format	Mimecast import
Upload Only (No Folder)	□
Import Into Profile Group	Select Group
Group Override	Select Option
Upload Spreadsheet (*.xls)	Choose File No file chosen

3. Select the Upload Only (No Folder) check box.
4. Use the Choose File button in the Upload Spreadsheet (*.XLS) field to browse your local file system and upload the spreadsheet of users you wish to import.
5. Click the Preview Changes button to start the import process.
6. Once the spreadsheet has been processed you will be presented with a preview summary of the users found.
7. Click Save to commit these changes to Mimecast.

Adding an Internal Domain

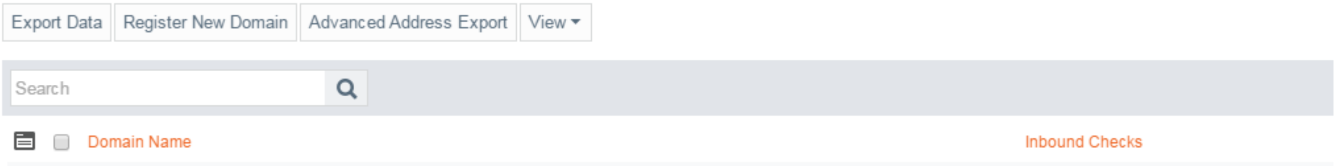
An internal domain, is a domain owned or controlled by your organization. What you will need to register more domains:

- A Mimecast administrator account with edit permissions to the Directories | Internal menu of the Administration Console.
- Access to the control panel for the DNS zone of the domain you want to register.

To add an internal domain:

1. Login to the Administration Console.

2. Click the Directories | Internal menu item.
3. Click the Register New Domain button.
4. Follow the guidance on screen to enter your domain name. A Verification Code is issued to you.
   Domain names will only be accepted if they are not already registered in your or any other Mimecast customer's account.
5. Copy the verification code to your clipboard.
6. Add the verification code as a TXT record in the DNS zone for the domain you are adding. Click here for guidance for some of the most common domain registrars.
   Typically this is an instant process. However Mimecast has observed delays of up to 2 hours for a new DNS record to be available. While you wait for the TXT record to be added you can click Go Back to continue working in the Administration Console. Click the View filter on the Directories | Internalpage to see your Pending Domains (domains that are pending confirmation of ownership via TXT record verification). These have an expiry date. You need to verify the domain before this date to successfully register the domain. If the expiry date passes, you will need to restart the verification process. A Pending Domain can be removed by right-clicking the domain in the list and selecting Remove Register Domain.
7. Once the TXT record has been successfully added to your domain, click Retry Domain Verification.
8. Select the option to automatically create an anti-spoofing policy for the domain. This prevents the domain from being spoofed from outside sources.
9. Specify the type of Recipient Validation you would like applied for emails received by Mimecast, to this domain.



Managing Profile Groups

A profile group is a local Mimecast folder containing email addresses or domain names. Once created, address information can be added to them either:

- Manually. Individual entries can be added, or a spreadsheet import can import multiple entries.
- Automatically using group builder rules (see the Group Builder section below).
- Mimecast can also synchronize distribution lists and security groups from your organization's domain controller using LDAP Synchronization. Synchronized groups are called Directory Groups.

To create a profile group:

1. Log in to the Administration Console.
2. Click on the Services toolbar button. A menu drop down is displayed.

3. Click on the Directories | Profile Groups menu item.
4. Click the + icon in the bottom right hand corner of the folder where the group is to be placed. A sub-group called "New Folder" is created in the group's hierarchy in a collapsed format.
5. Rename the group:

a. Expand the group's hierarchy.

b. Click on the new group.

c. Enter the group name in the Edit Group field at the top of the hierarchy.

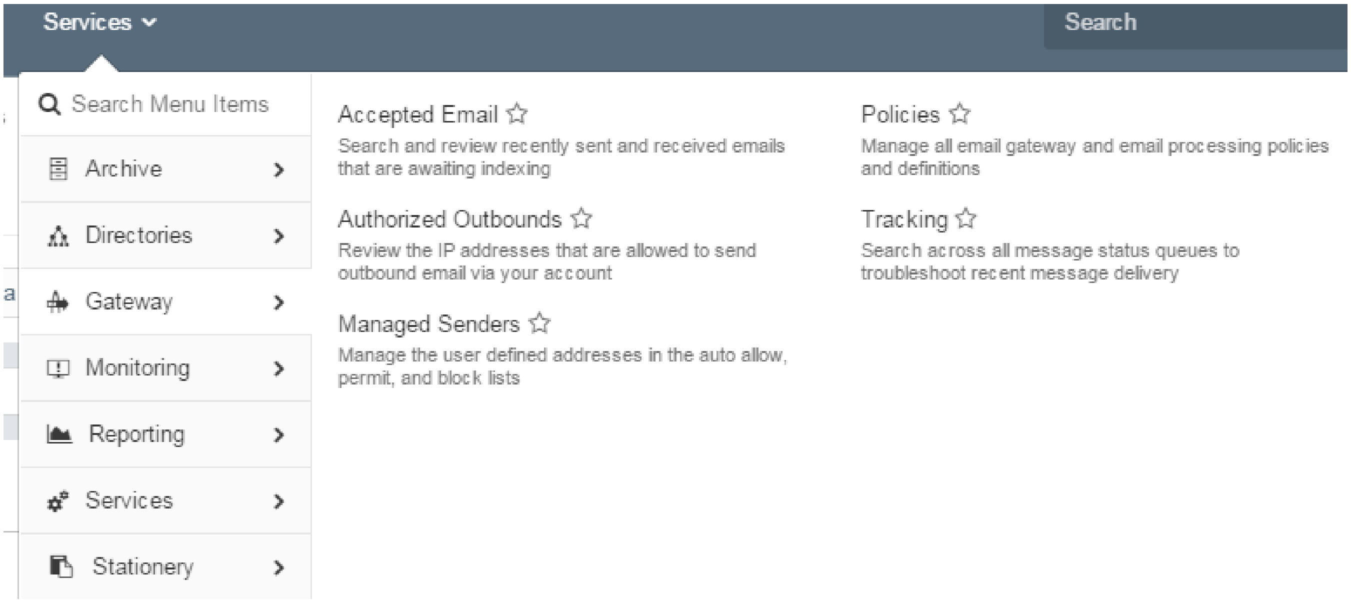
d. Press the Enter key.

Add to Whitelist/Blacklist

1. Select Services -> Directories -> Profile Groups
2. To add to a blacklist, select Blocked Senders. To add to a whitelist, select Permitted Senders.
3. Select Build and then select either Add Email Addresses or Add Email Domains depending on what needs whitelisted or blacklisted.
4. Add in your addresses & domains (One per line) and then select Save and Exit.

Gateway

To access and manage your gateway go to the “services” and then “gateway” – each option will provide you a short description, you can manage each option by clicking on it



Accepted Email ☆
Search and review recently sent and received emails that are awaiting indexing

Authorized Outbounds ☆
Review the IP addresses that are allowed to send outbound email via your account

Managed Senders ☆
Manage the user defined addresses in the auto allow, permit, and block lists

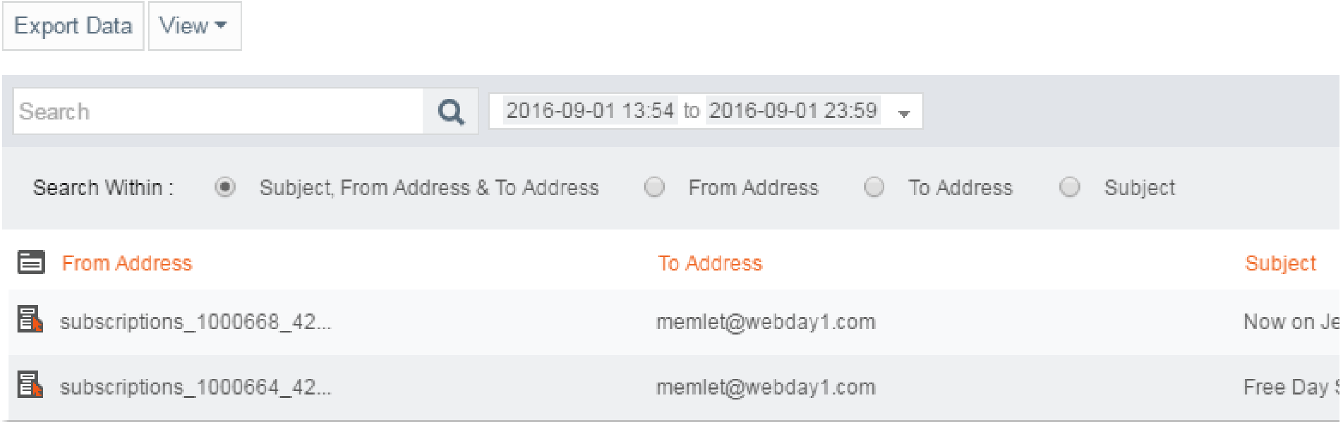
Policies ☆
Manage all email gateway and email processing policies and definitions

Tracking ☆
Search across all message status queues to troubleshoot recent message delivery

Accepted Email

To view accepted email go to Gateways | Accepted email for current emails – or go through your archive for old emails

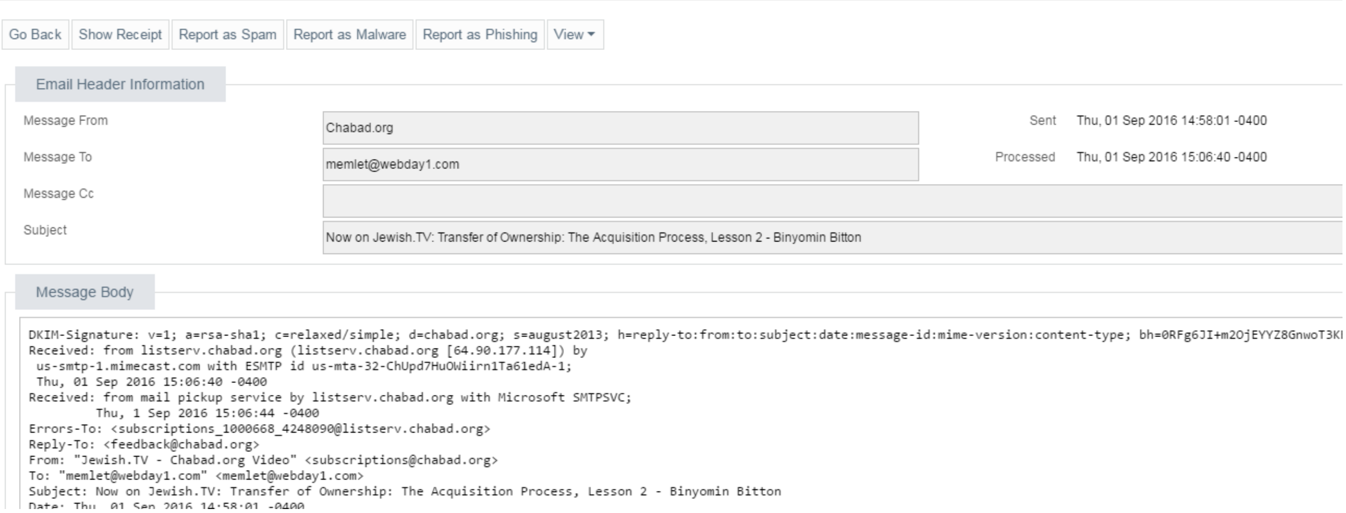
When the email has been opened, the default view displayed is the **Delivery View**. At the top of the message viewer, the title bar indicates whether you are looking at the Receipt or Delivery view for that email.



Search Within : ● Subject, From Address & To Address ○ From Address ○ To Address ○ Subject

From Address	To Address	Subject
subscriptions_1000668_42...	memlet@webday1.com	Now on Je
subscriptions_1000664_42...	memlet@webday1.com	Free Day S

Depending on your permissions, clicking on an email will provide you access to the message content and receipt information



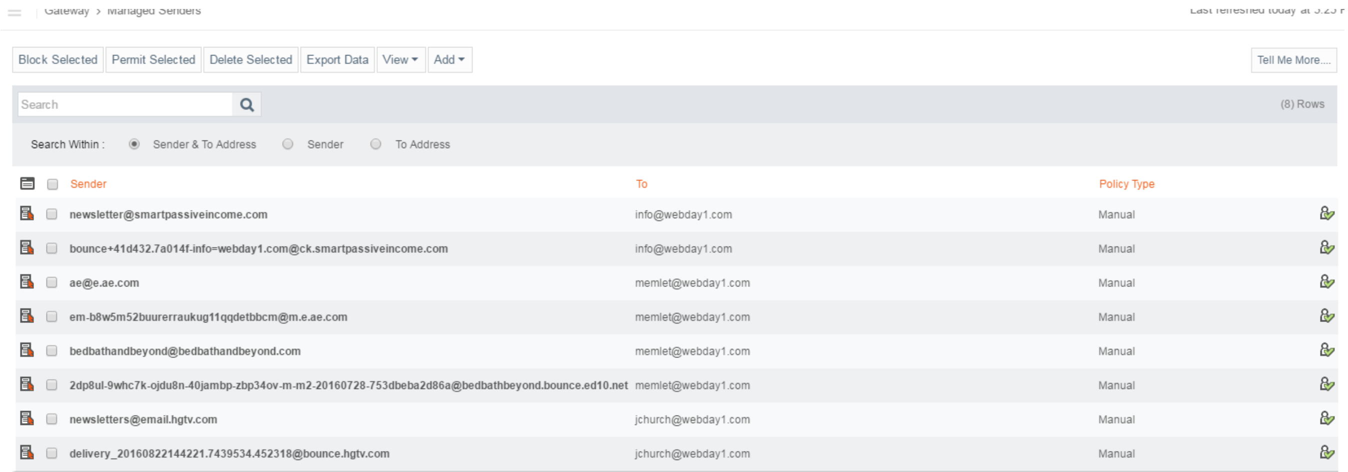
Message From: Chabad.org
Message To: memlet@webday1.com
Message Cc:
Subject: Now on Jewish.TV: Transfer of Ownership: The Acquisition Process, Lesson 2 - Binyomin Bitton
Sent: Thu, 01 Sep 2016 14:58:01 -0400
Processed: Thu, 01 Sep 2016 15:06:40 -0400

```
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/simple; d=chabad.org; s=august2013; h=reply-to:from:to:subject:date:message-id:mime-version:content-type; bh=0RFg6JI+m2OjEYYZ8GnwoT3K
Received: from listserv.chabad.org (listserv.chabad.org [64.90.177.114]) by
 us-smtp-1.mimecast.com with ESMTP id us-mta-32-ChUpd7HuOWiirn1Ta61edA-1;
 Thu, 01 Sep 2016 15:06:40 -0400
Received: from mail pickup service by listserv.chabad.org with Microsoft SMTPSVC;
         Thu, 1 Sep 2016 15:06:44 -0400
Errors-To: <subscriptions_1000668_4248090@listserv.chabad.org>
Reply-To: <feedback@chabad.org>
From: "Jewish.TV - Chabad.org Video" <subscriptions@chabad.org>
To: "memlet@webday1.com" <memlet@webday1.com>
Subject: Now on Jewish.TV: Transfer of Ownership: The Acquisition Process, Lesson 2 - Binyomin Bitton
Date: Thu, 01 Sep 2016 14:58:01 -0400
```

Managed senders

Managed Senders 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. An administrator can view, add, modify or even remove these personal entries by using the Managed Senders menu option in the Administration console. It is also possible to import a spreadsheet of existing personal entries from third-party systems when migrating to Mimecast.

Administrators can view, modify, remove or add policies from the **Gateway | Managed Senders** view. The default view displays a list of existing entries, with action buttons in the grey toolbar and a **Search** field to easily locate items in the list:


Gateway > Managed Senders
Last refreshed today at 3:25 P
Block Selected
Permit Selected
Delete Selected
Export Data
View ▾
Add ▾
Tell Me More....
Search
(8) Rows
Search Within : ● Sender & To Address ○ Sender ○ To Address

Sender	To	Policy Type
newsletter@smartpassiveincome.com	info@webday1.com	Manual
bounce+41d432.7a014f-info=webday1.com@ck.smartpassiveincome.com	info@webday1.com	Manual
ae@e.ae.com	memlet@webday1.com	Manual
em-b8w5m52buurerraukug11qqdetbbcm@m.e.ae.com	memlet@webday1.com	Manual
bedbathandbeyond@bedbathandbeyond.com	memlet@webday1.com	Manual
2dp8ul-9whc7k-ojdu8n-40jambp-zbp34ov-m-m2-20160728-753dbeba2d86a@bedbathbeyond.bounce.ed10.net	memlet@webday1.com	Manual
newsletters@email.hgtv.com	jchurch@webday1.com	Manual
delivery_20160822144221.7439534.452318@bounce.hgtv.com	jchurch@webday1.com	Manual

Policies

Mimecast Gateway Policies are a set of rules, applied to either Inbound or Outbound messages, that affect the email traffic flow. They allow Administrators to apply granular control to email messages processed by Mimecast. For example they can:

- Stop email flow (e.g. Hold for Review, Block Policies)
- Prevent data leaks (e.g. Content Examination, Document Services Policies)
- Handle attachments
- Handle spam

A number of default policies are provided with each Mimecast installation, with the available policies being dependent on the Mimecast products purchased. As there are policies for specific pieces of Mimecast functionality, each policy is listed by it's Policy Type

To access the gateway policy editor:

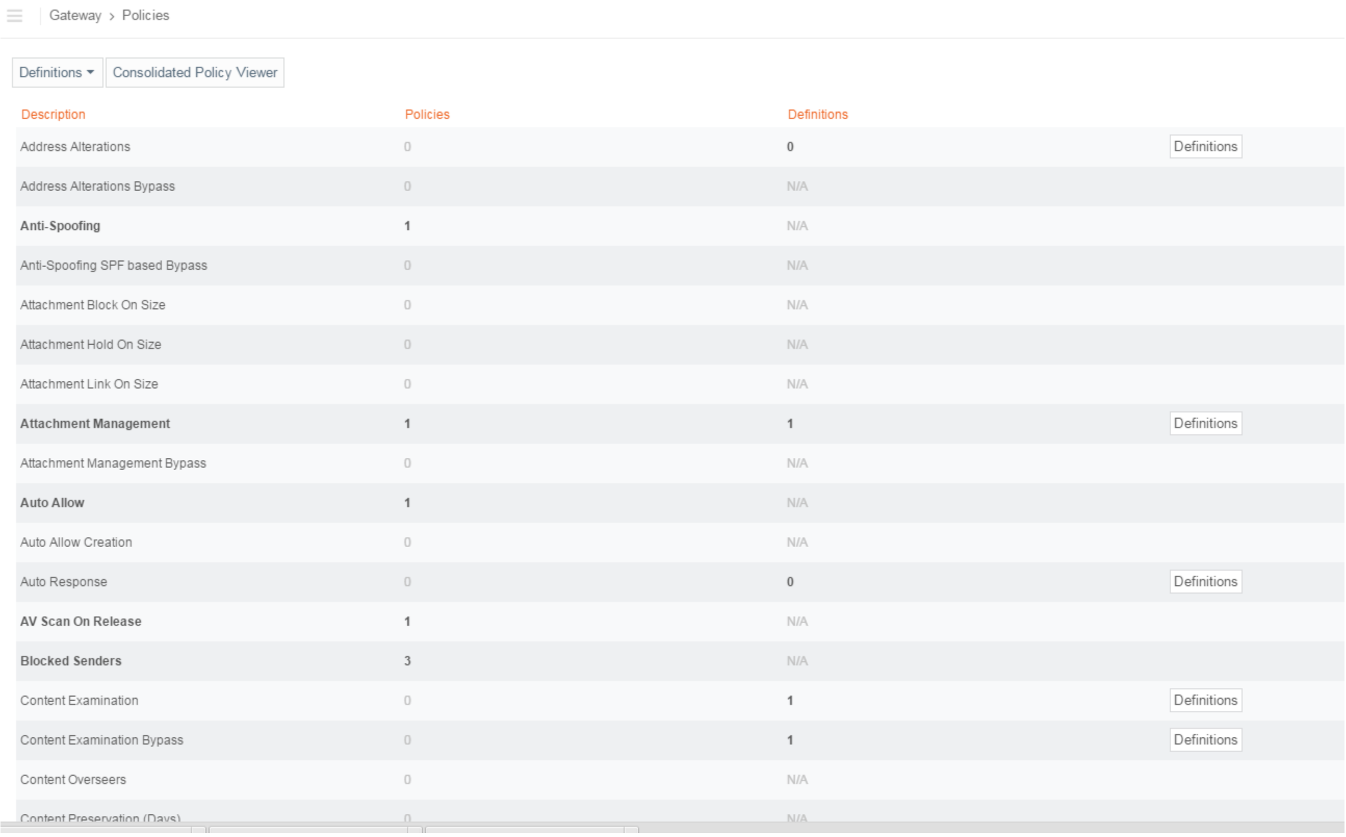
Go to the services tab > gateway > policies

The following information will be displayed in the policy editor:

Description: Displays the policy name

Policies: Displays the number of policies configured with that policy type

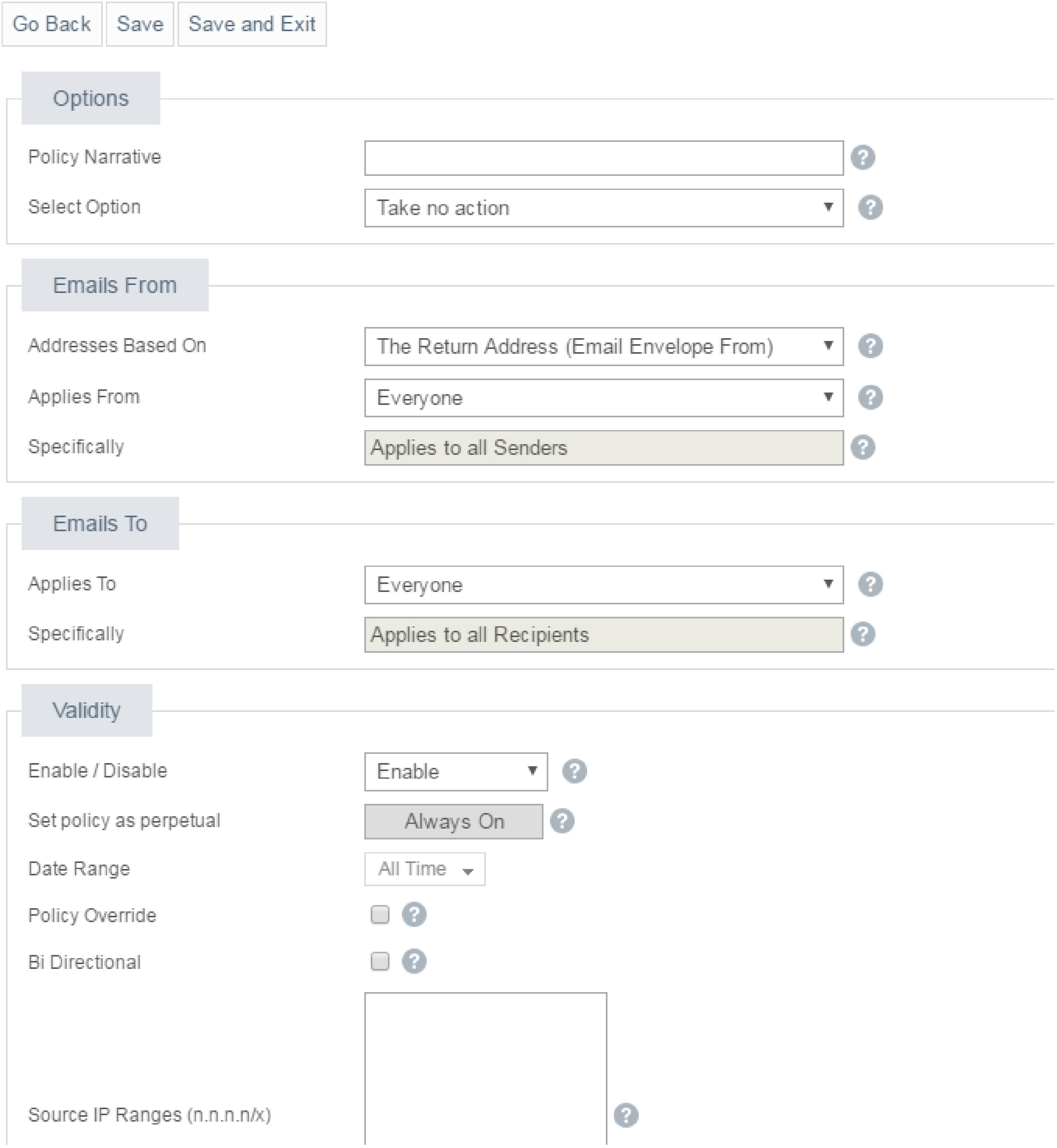
Definitions: Indicates whether a definition is required for the policy type. If a number is displayed, that number of definitions have been configured. You can display these definition, or create on using the definitions button



Description	Policies	Definitions	
Address Alterations	0	0	Definitions
Address Alterations Bypass	0	N/A	
Anti-Spoofing	1	N/A	
Anti-Spoofing SPF based Bypass	0	N/A	
Attachment Block On Size	0	N/A	
Attachment Hold On Size	0	N/A	
Attachment Link On Size	0	N/A	
Attachment Management	1	1	Definitions
Attachment Management Bypass	0	N/A	
Auto Allow	1	N/A	
Auto Allow Creation	0	N/A	
Auto Response	0	0	Definitions
AV Scan On Release	1	N/A	
Blocked Senders	3	N/A	
Content Examination	0	1	Definitions
Content Examination Bypass	0	1	Definitions
Content Overseers	0	N/A	
Content Preservation (Days)	0	N/A	

Anti-Spoofing Policy

1. Log in to the Mimecast Admin portal
2. Select Gateway -> Policies
3. Select Anti Spoofing
4. Select New Policy
5. Fill out the policy as follows:



Options

Policy Narrative:
Select Option: Take no action ▾

Emails From

Addresses Based On: The Return Address (Email Envelope From) ▾
Applies From: Everyone ▾
Specifically: Applies to all Senders

Emails To

Applies To: Everyone ▾
Specifically: Applies to all Recipients

Validity

Enable / Disable: Enable ▾
Set policy as perpetual: Always On
Date Range: All Time ▾
Policy Override: □
Bi Directional: □
Source IP Ranges (n.n.n.n/x):

a. Policy Narrative: Anti-Spoofing Bypass
b. Select Option: Take No Action
c. Email From:
i. Address Based On: Both
ii. Applies From: Everyone

d. Email To: Everyone
e. Enable
f. Set Policy As Perpetual: Always On
g. Policy Override: Checked
h. Bi Directional: Unchecked
i. Add IP Addresses / Host names as needed

6. Select Save and Exit.

Track and trace

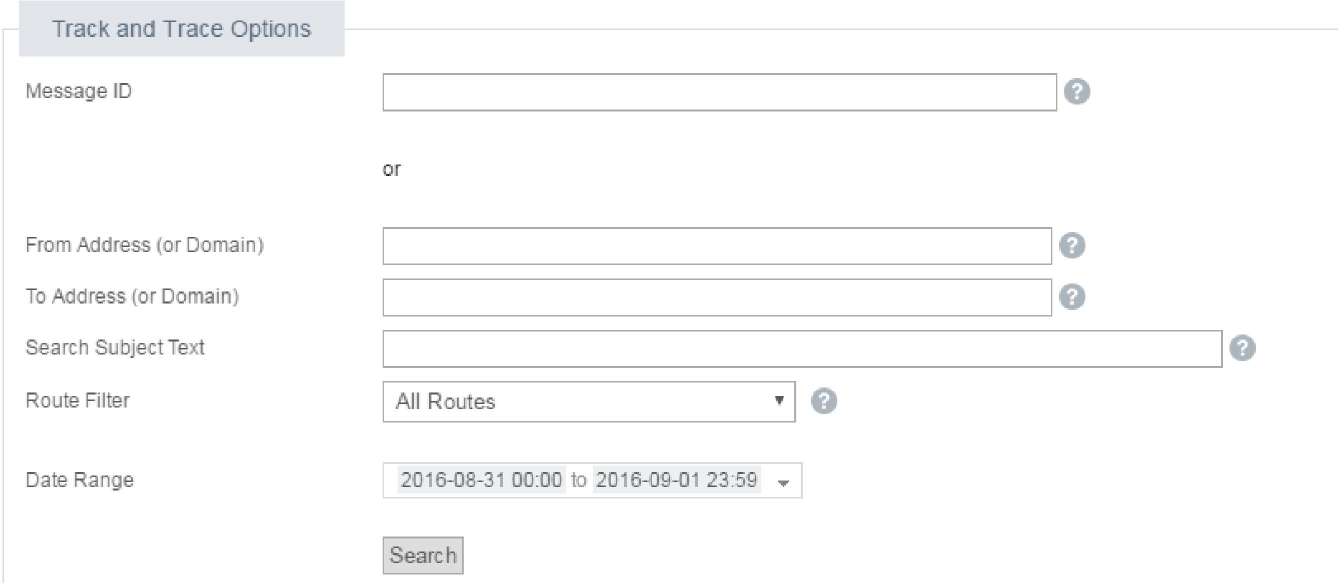
Using the Track and Trace functionality in the Administration Console, administrators can search across multiple viewers and queues from a single place using specific message information. The results provide information regarding the processing of the email, as well as its current state.

The following viewers and queues are included in the search process:

- Connection Attempts
- Bounce Viewer
- Rejection Viewer
- Delivery Queue
- Hold Review Queue
- Active Messages
- Email Archive

To search for a message:

1. Log in to the Administration Console.
2. Click on the Services toolbar button. A menu drop down is displayed.
3. Click on the Gateway | Tracking menu item. The Track and Trace Options dialog is displayed. Fill out appropriate options for your search:



Track and Trace Options

Message ID:

or

From Address (or Domain):

To Address (or Domain):

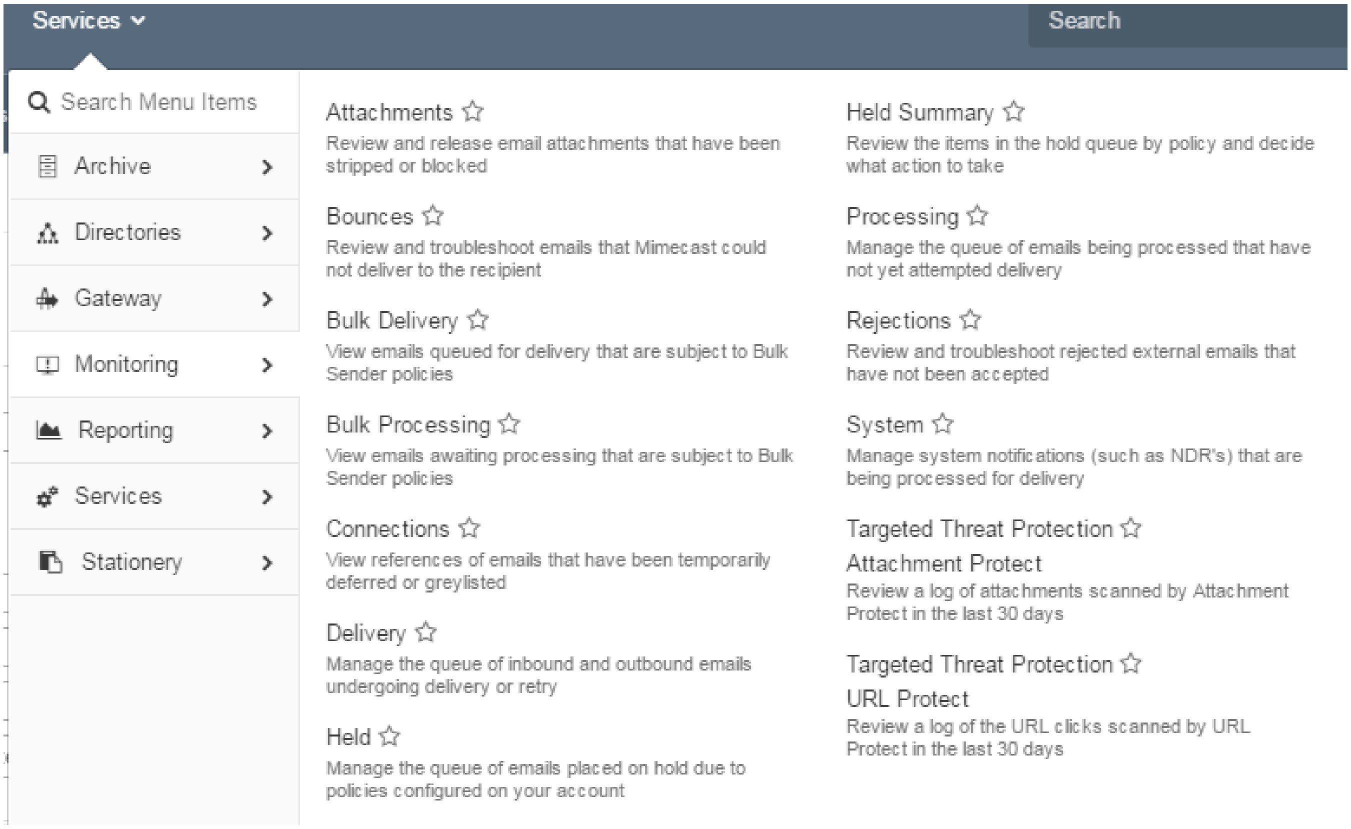
Search Subject Text:

Route Filter: All Routes

Date Range: 2016-08-31 00:00 to 2016-09-01 23:59

Monitoring

Access by going to “services” and then “monitoring”



Attachments ☆
Review and release email attachments that have been stripped or blocked

Bounces ☆
Review and troubleshoot emails that Mimecast could not deliver to the recipient

Bulk Delivery ☆
View emails queued for delivery that are subject to Bulk Sender policies

Bulk Processing ☆
View emails awaiting processing that are subject to Bulk Sender policies

Connections ☆
View references of emails that have been temporarily deferred or greylisted

Delivery ☆
Manage the queue of inbound and outbound emails undergoing delivery or retry

Held ☆
Manage the queue of emails placed on hold due to policies configured on your account

Held Summary ☆
Review the items in the hold queue by policy and decide what action to take

Processing ☆
Manage the queue of emails being processed that have not yet attempted delivery

Rejections ☆
Review and troubleshoot rejected external emails that have not been accepted

System ☆
Manage system notifications (such as NDR's) that are being processed for delivery

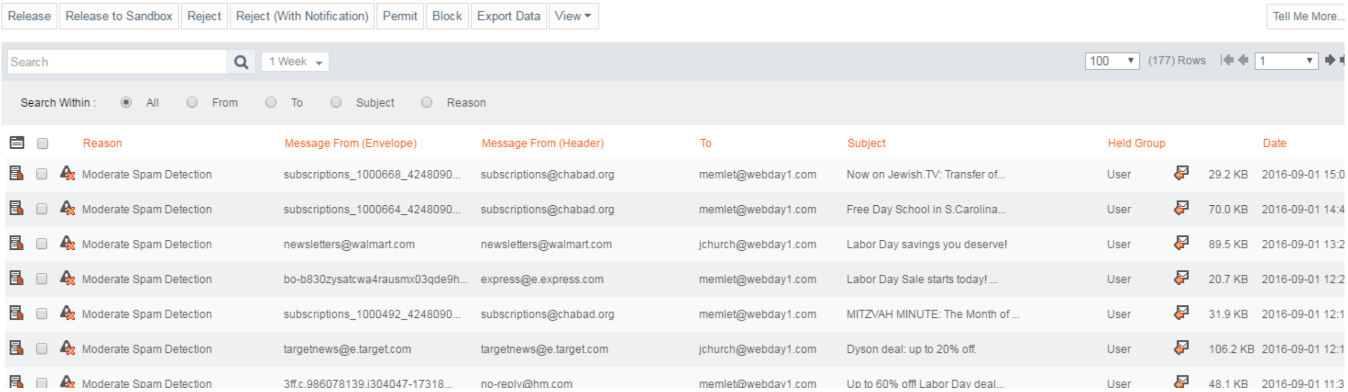
Targeted Threat Protection ☆
Attachment Protect
Review a log of attachments scanned by Attachment Protect in the last 30 days

Targeted Threat Protection ☆
URL Protect
Review a log of the URL clicks scanned by URL Protect in the last 30 days

Attachments

Any attachment that is blocked or stripped and linked from a message based on an attachment policy, is logged and available for release by an administrator using stripped attachments.

Here you can **release, reject, permit, block, view and export data** by selecting the messages and selecting one of the options above those messages.



Search Within : ● All ○ From ○ To ○ Subject ○ Reason

□	Reason	Message From (Envelope)	Message From (Header)	To	Subject	Held Group		Date
□	Moderate Spam Detection	subscriptions_1000668_4248090...	subscriptions@chabad.org	memlet@webday1.com	Now on Jewish.TV: Transfer of...	User	29.2 KB	2016-09-01 15:0
□	Moderate Spam Detection	subscriptions_1000664_4248090...	subscriptions@chabad.org	memlet@webday1.com	Free Day School in S.Carolina...	User	70.0 KB	2016-09-01 14:4
□	Moderate Spam Detection	newsletters@walmart.com	newsletters@walmart.com	jchurch@webday1.com	Labor Day savings you deserve!	User	89.5 KB	2016-09-01 13:2
□	Moderate Spam Detection	bo-b830zysatcwa4rausmx03qde9h...	express@e.express.com	memlet@webday1.com	Labor Day Sale starts today! ...	User	20.7 KB	2016-09-01 12:2
□	Moderate Spam Detection	subscriptions_1000492_4248090...	subscriptions@chabad.org	memlet@webday1.com	MITZVAH MINUTE: The Month of ...	User	31.9 KB	2016-09-01 12:1
□	Moderate Spam Detection	targetnews@e.target.com	targetnews@e.target.com	jchurch@webday1.com	Dyson deal: up to 20% off.	User	106.2 KB	2016-09-01 12:1
□	Moderate Spam Detection	3ff.c.986078139.i304047-17318...	no-reply@hm.com	memlet@webday1.com	Up to 60% off! Labor Day deal...	User	48.1 KB	2016-09-01 11:3

It is important to note that there are four policies that can be used to handle attachments. All are located in the **Gateway | Policies** section:

Attachment management: Allows individual attachment types to be blocked, linked or held using an Attachment Set

Attachment Block on Size: Removes attachments based on the cumulative size of the attachments

Attachment Hold on Size: Holds the emails based on the cumulative size of the attachments

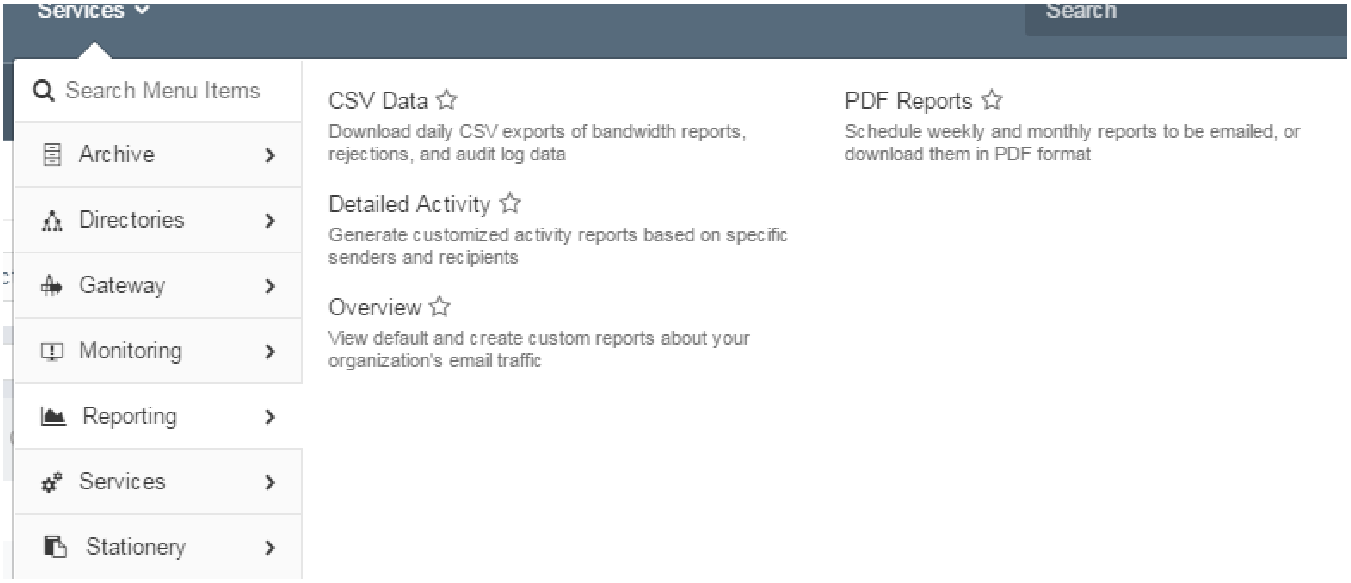
Attachment Link on Size: Strips and Links all attachments based on the cumulative size of the attachments

Reporting Overview

Reports can assist with infrastructure planning through data load analysis, gauge user efficiency, as well as provide graphical representation of email volumes and flows. Reporting Overview shows groups of graphs which aim to provide granular information about your organization's email volumes and traffic:

- **Summary Graphs** - display the volumes of email split into Outbound, Inbound and Internal messages, as well as Rejected volumes

- **Outbound Email** - displays email communication from internal users to external users and domains
- **Inbound Email** - displays email communication from external users to internal users and domains
- **Internal Email** - displays email communication between internal users
- **Custom Reports** - displays any Custom Report Definitions that have been configured



CSV Data ☆
Download daily CSV exports of bandwidth reports, rejections, and audit log data

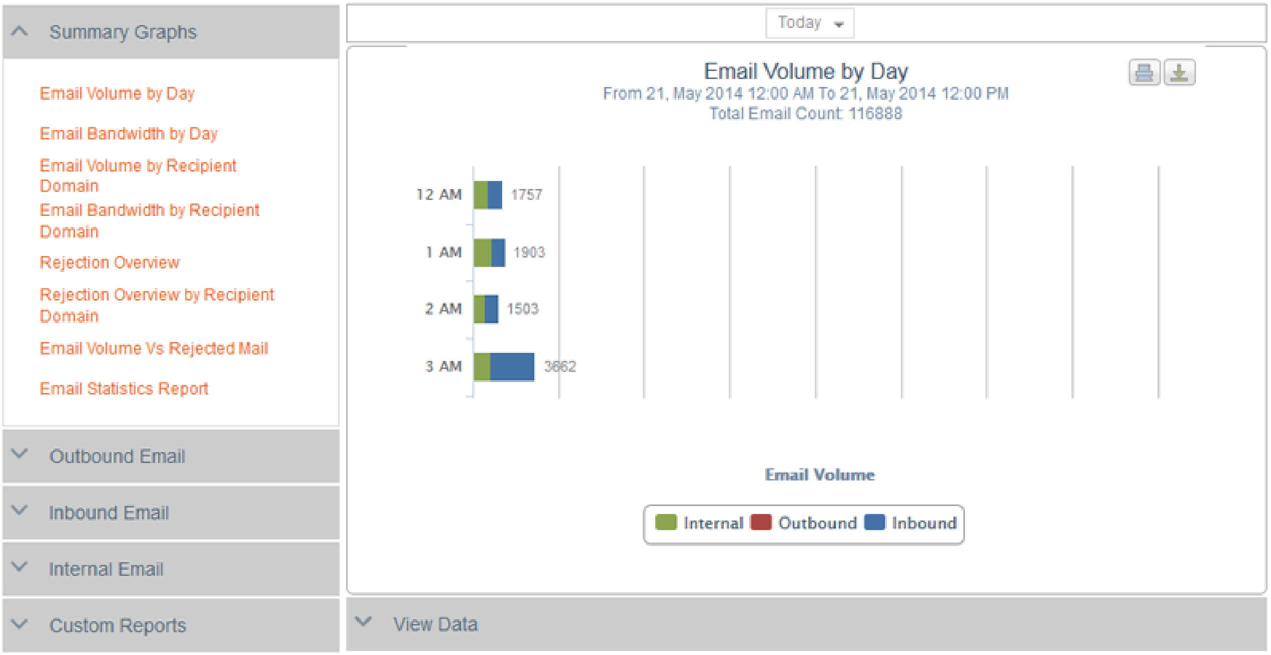
Detailed Activity ☆
Generate customized activity reports based on specific senders and recipients

Overview ☆
View default and create custom reports about your organization's email traffic

PDF Reports ☆
Schedule weekly and monthly reports to be emailed, or download them in PDF format

To access the graphs, navigate to Reporting | Overview.

This page displays an accordion menu on the left, which is split into various groups of reports. The page on the right displays a graph based on your menu selection:


Summary Graphs
Email Volume by Day
Email Bandwidth by Day
Email Volume by Recipient Domain
Email Bandwidth by Recipient Domain
Rejection Overview
Rejection Overview by Recipient Domain
Email Volume Vs Rejected Mail
Email Statistics Report
Outbound Email
Inbound Email
Internal Email
Custom Reports
Today
Email Volume by Day
From 21, May 2014 12:00 AM To 21, May 2014 12:00 PM
Total Email Count: 116888
12 AM
1757
1 AM
1903
2 AM
1503
3 AM
3662
Email Volume
🟩 Internal 🟥 Outbound 🟦 Inbound
View Data

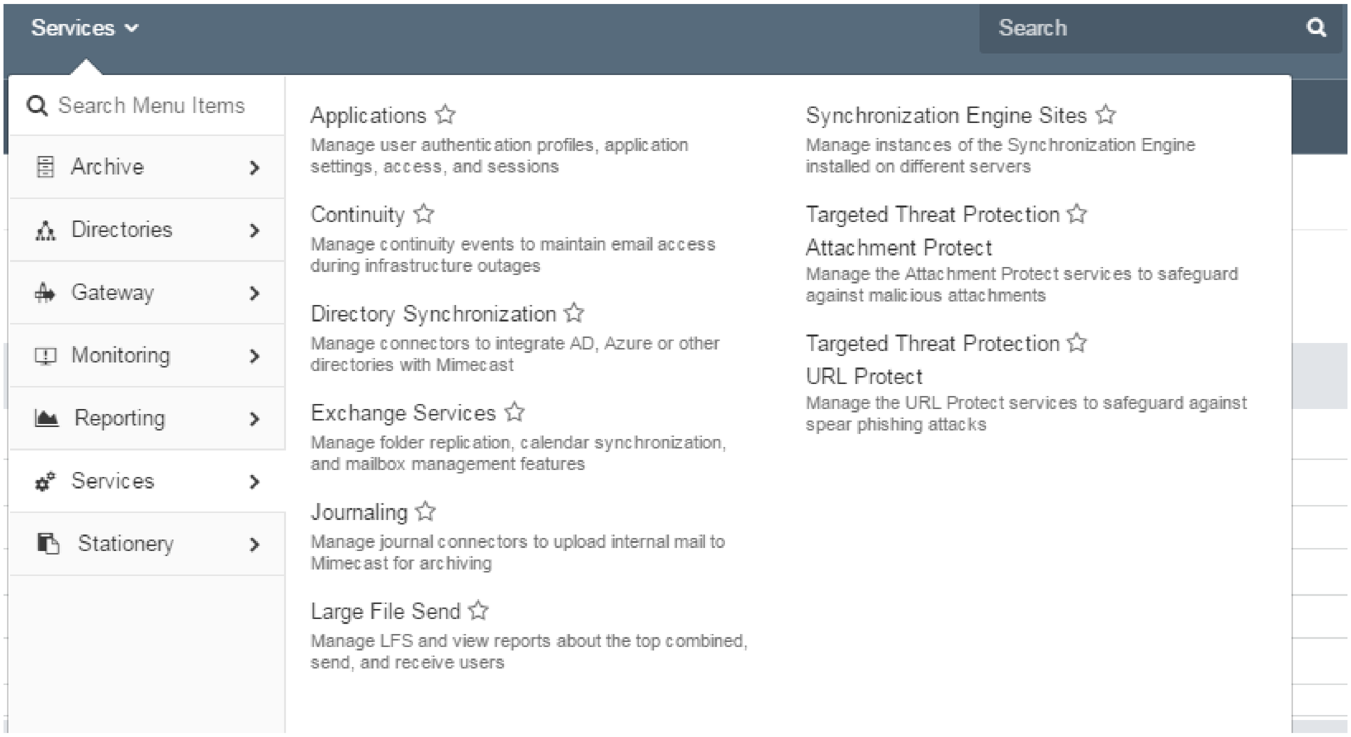
Guidelines for working with Graphs

There are certain guidelines to be aware of when working with graphs:

- By default, the graphs will display Today's results. Use the calendar control to select the time period you wish to view. Note that the calendar control is not included in the Email Statistics Report as the information displayed relates to a rolling 12 month period
- For most graphs, the X axis shows the email volume, while the Y axis shows the date, email address or domain. If the graph is based on a single day i.e. Yesterday, hourly results are shown; otherwise the total for each day is displayed
- Graphs can be downloaded by clicking on the download Reporting - Download.png icon. The following file types are available: PNG, JPEG, PDF, SVG Vector image
- Graphs can be printed by clicking on the print Reporting - Print.png icon, and then confirming the printer and settings
- For graphs displaying email volumes, the total volumes are shown as well as the split of traffic. i.e. the email route is shown in different colors:
  - Green - Internal
  - Red - Outbound
  - Blue - Inbound
- If you hover over the graph columns, the totals are displayed. Administrators are also able to toggle the results by clicking on the graph legend.

Services

– Journaling – directory sync – applications(Mimecast for outlook) – continuity –



Applications ☆
Manage user authentication profiles, application settings, access, and sessions

Continuity ☆
Manage continuity events to maintain email access during infrastructure outages

Directory Synchronization ☆
Manage connectors to integrate AD, Azure or other directories with Mimecast

Exchange Services ☆
Manage folder replication, calendar synchronization, and mailbox management features

Journaling ☆
Manage journal connectors to upload internal mail to Mimecast for archiving

Large File Send ☆
Manage LFS and view reports about the top combined, send, and receive users

Synchronization Engine Sites ☆
Manage instances of the Synchronization Engine installed on different servers

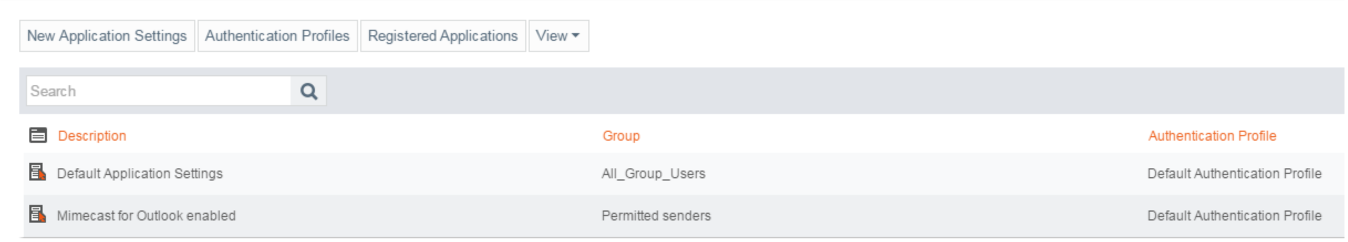
Targeted Threat Protection ☆ Attachment Protect
Manage the Attachment Protect services to safeguard against malicious attachments

Targeted Threat Protection ☆ URL Protect
Manage the URL Protect services to safeguard against spear phishing attacks

Enabling Mimecast for Outlook for end users

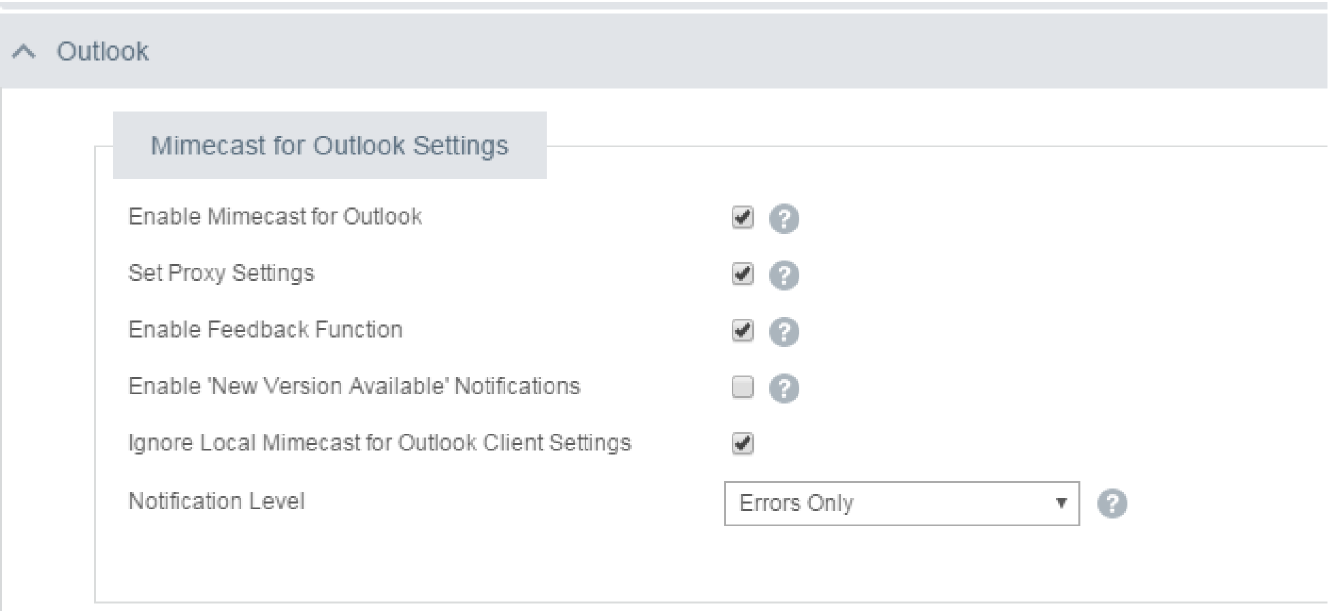
In order for your end users to use the Mimecast plugin for Outlook you must enable it from the administration console.

Go to Services, then services. You can then edit your current default policy by clicking into it OR you can create a new one if you choose to only specify certain users and groups



Description	Group	Authentication Profile
Default Application Settings	All_Group_Users	Default Authentication Profile
Mimecast for Outlook enabled	Permitted senders	Default Authentication Profile

Click on new application settings from the applications page, and scroll to the “Outlook” tab



Outlook

Mimecast for Outlook Settings

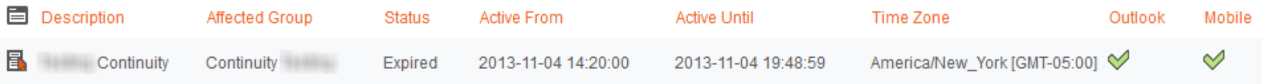
Enable Mimecast for Outlook	☑
Set Proxy Settings	☑
Enable Feedback Function	☑
Enable 'New Version Available' Notifications	□
Ignore Local Mimecast for Outlook Client Settings	☑
Notification Level	Errors Only ▾

Make sure that the “Enable Mimecast for Outlook” option is selected. By default it will not be.

Managing Continuity Events

Continuity events allow you to control the start and end time of an outage. Once scheduled, it communicates with the registered continuity devices or applications in the associated group, and if configured, forces them into disaster recovery mode. This results in all outbound and inbound emails being sent directly via your Mimecast service.

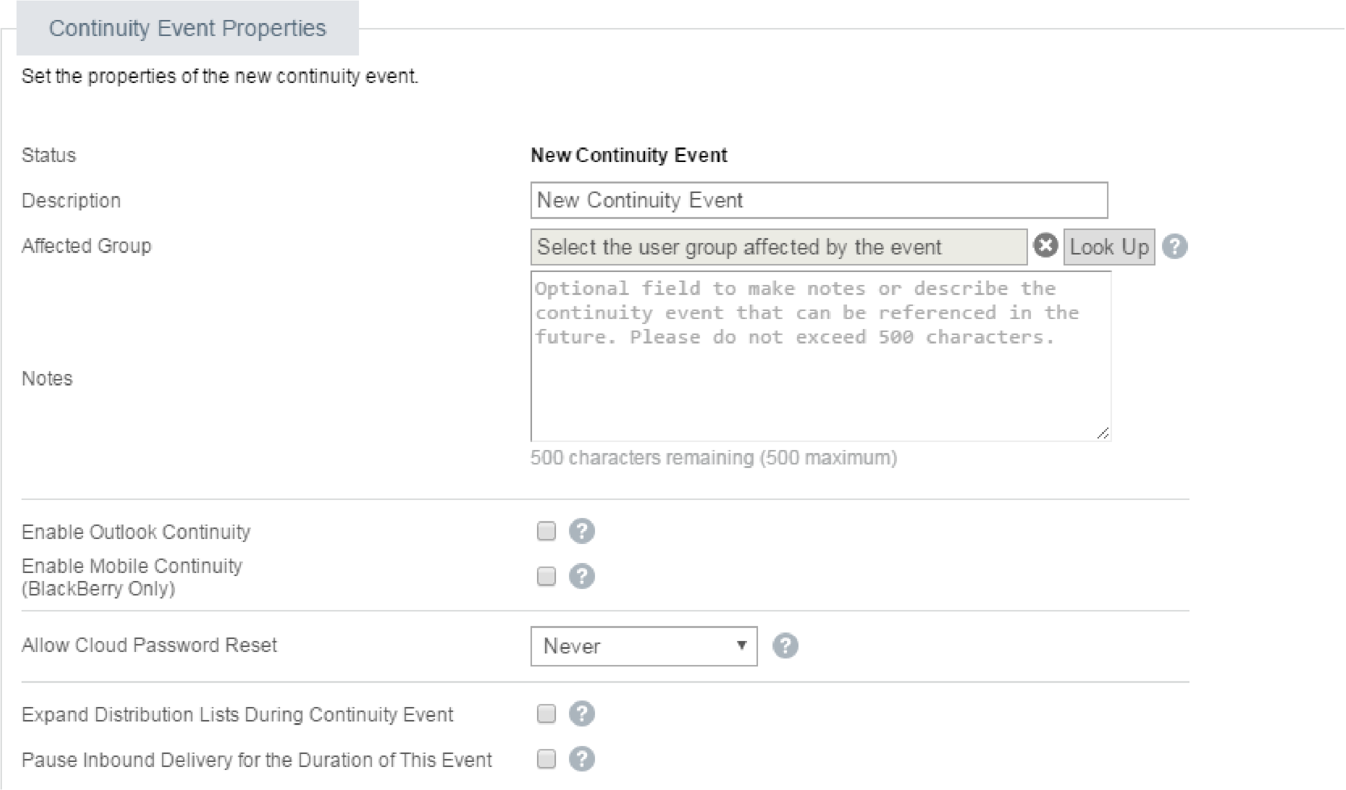
You can create a continuity event by creating a record from the default blank template, or by cloning an existing continuity event. Once created, all continuity events are listed including details about the affected group, event status, active dates / times, time zone, and whether it is set for Outlook or Mobile devices.



Description	Affected Group	Status	Active From	Active Until	Time Zone	Outlook	Mobile
[redacted] Continuity	Continuity [redacted]	Expired	2013-11-04 14:20:00	2013-11-04 19:48:59	America/New_York [GMT-05:00]	✓	✓

To create a continuity event from the default blank template:

1. Log in to the Administration Console.
2. Click on the Services toolbar button. A menu drop down is displayed.
3. Click on the Services | Continuity menu item. A list of all future, current, and expired continuity events is displayed.
4. Click on the New Continuity Event button. The Continuity Event Properties dialog is displayed.
5. Complete the Continuity Event Properties section as required.

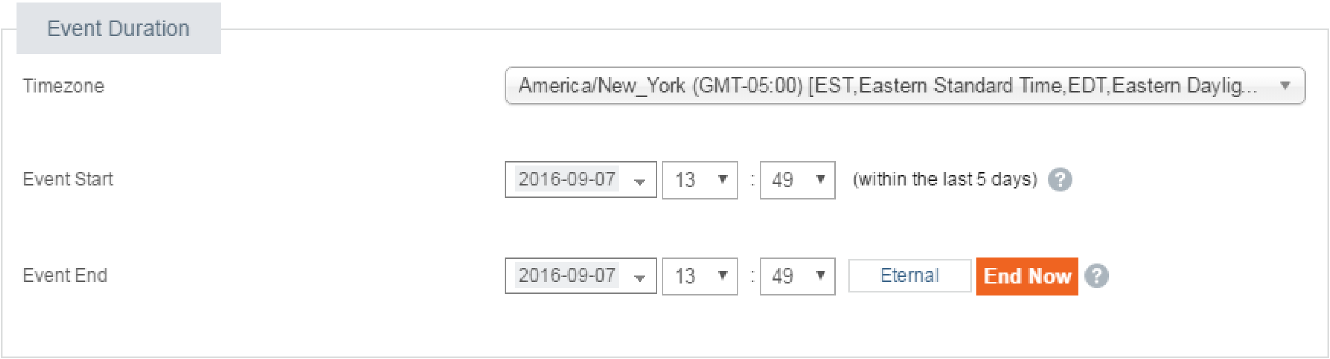


Continuity Event Properties

Set the properties of the new continuity event.

Status	**New Continuity Event**
Description	New Continuity Event
Affected Group	Select the user group affected by the event
Notes	Optional field to make notes or describe the continuity event that can be referenced in the future. Please do not exceed 500 characters. 500 characters remaining (500 maximum)
Enable Outlook Continuity	□
Enable Mobile Continuity (BlackBerry Only)	□
Allow Cloud Password Reset	Never
Expand Distribution Lists During Continuity Event	□
Pause Inbound Delivery for the Duration of This Event	□

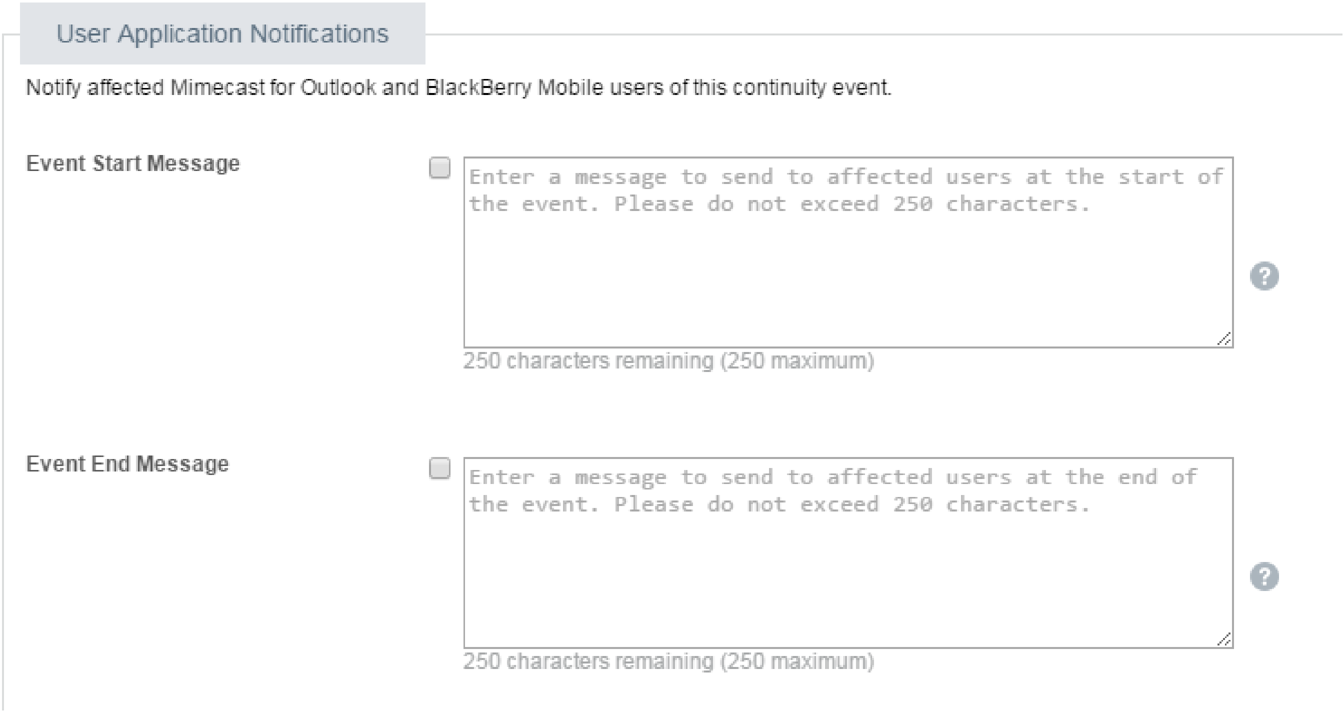
6. Complete the Event Duration section as required.



Event Duration

Timezone	America/New_York (GMT-05:00) [EST,Eastern Standard Time,EDT,Eastern Daylig...
Event Start	2016-09-07 13 : 49 (within the last 5 days)
Event End	2016-09-07 13 : 49

7. Complete the Notification Messages section as required.



User Application Notifications

Notify affected Mimecast for Outlook and BlackBerry Mobile users of this continuity event.

Event Start Message □ Enter a message to send to affected users at the start of the event. Please do not exceed 250 characters.

250 characters remaining (250 maximum)

Event End Message □ Enter a message to send to affected users at the end of the event. Please do not exceed 250 characters.

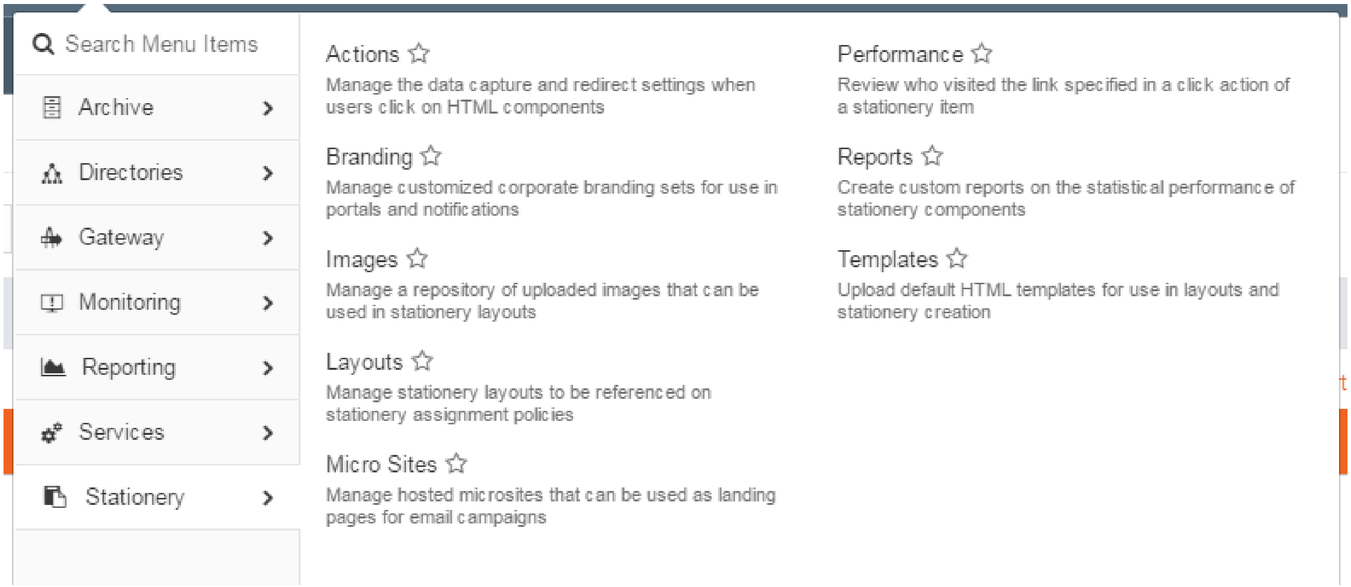
250 characters remaining (250 maximum)

8. Click on the Save and Exit button.

Stationary

You can access your stationary settings by going to “Services” and then “Stationary”

Here you can manage your branding and click rates, even create a micro site



Actions ☆
Manage the data capture and redirect settings when users click on HTML components

Branding ☆
Manage customized corporate branding sets for use in portals and notifications

Images ☆
Manage a repository of uploaded images that can be used in stationery layouts

Layouts ☆
Manage stationery layouts to be referenced on stationery assignment policies

Micro Sites ☆
Manage hosted microsites that can be used as landing pages for email campaigns

Performance ☆
Review who visited the link specified in a click action of a stationery item

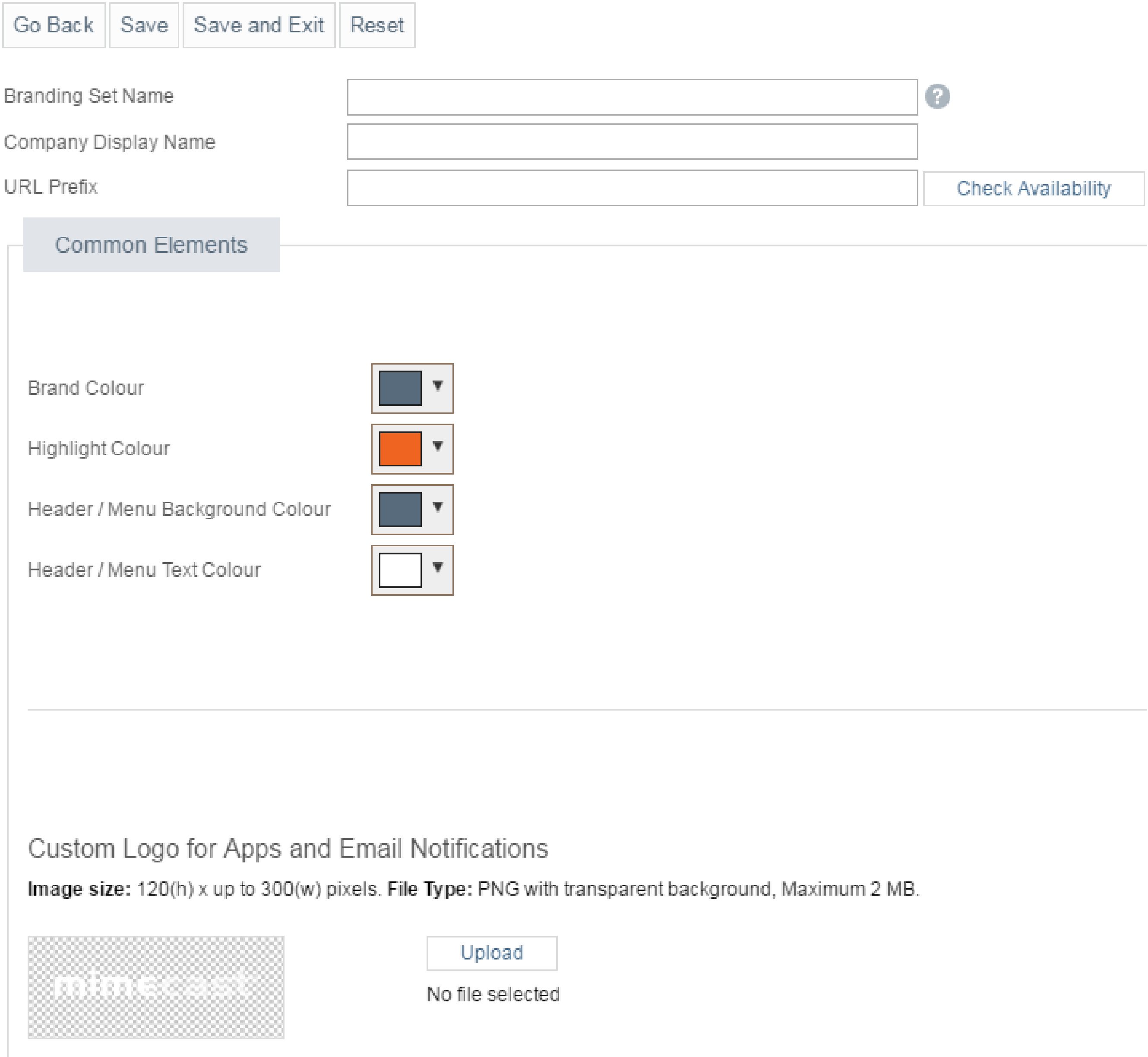
Reports ☆
Create custom reports on the statistical performance of stationery components

Templates ☆
Upload default HTML templates for use in layouts and stationery creation

Branding

Branding enables Administrators to apply custom brand elements to external facing portals and notifications, giving your customers clear indication that the Portals and messages are provided by you. This helps with marketing your brand, and giving the user the reassurance that this is your service.

To access branding go to "services" > "stationary" > "branding" > and then select "new branding set"



Branding Set Name

Company Display Name

URL Prefix

Brand Colour

Highlight Colour

Header / Menu Background Colour

Header / Menu Text Colour

Custom Logo for Apps and Email Notifications

Image size: 120(h) x up to 300(w) pixels. **File Type:** PNG with transparent background, Maximum 2 MB.

No file selected

The Mimecast services that support branding are:

- Secure Messaging (SM)
- Large File Send (LFS)

- Mimecast Personal Portal (MPP)
- Targeted Threat Protection(TTP)

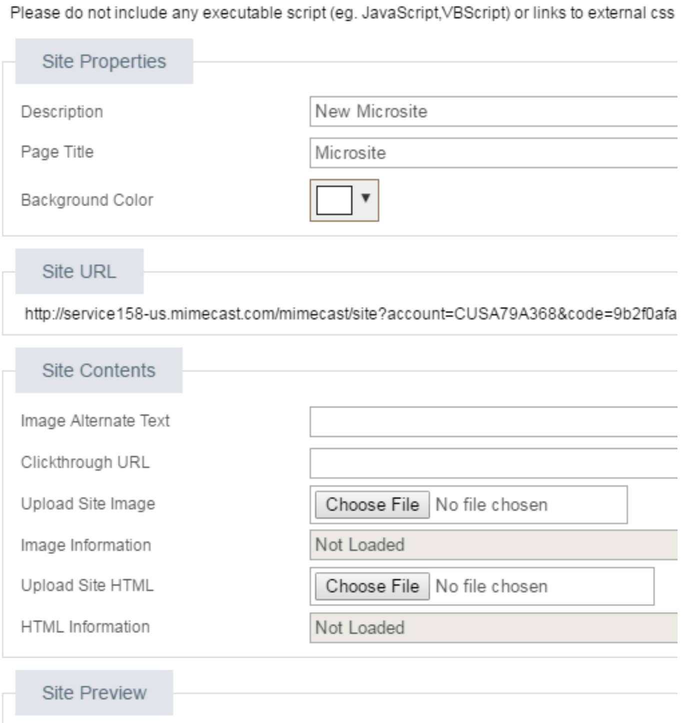
As part of the configuration of these brand elements, a subdomain URL is created to personalize the portal for the organization. It is also possible to have multiple custom URLs if required.

Micro Sites

Micro Sites are essentially temporary websites with limited content. They are typically used for confirmation purposes during a marketing campaign. For example, a landing page launched from a stationery click image with campaign specific marketing information and perhaps user registration.

To upload a Micro Site:

1. Log in to the Administration Console.
2. Click on the Services toolbar button. A menu drop down is displayed.
3. Click on the Stationery | Micro Sites menu item.
4. Select the New Micro Site button. The Micro Site Administration page is displayed.
5. Complete the page as required:



Please do not include any executable script (eg. JavaScript,VBScript) or links to external css

Site Properties

Description: New Microsite

Page Title: Microsite

Background Color: □ ▼

Site URL

http://service158-us.mimecast.com/mimecast/site?account=CUSA79A368&code=9b2f0afa

Site Contents

Image Alternate Text:

Clickthrough URL:

Upload Site Image: Choose File No file chosen

Image Information: Not Loaded

Upload Site HTML: Choose File No file chosen

HTML Information: Not Loaded

Site Preview

End of Document