

# Account Tour

## Mimecast Training

---

Student Workbook

V 1.2



Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express prior written permission of Mimecast Limited.

A reference to Mimecast shall be deemed to include Mimecast Limited, Mimecast Services Limited, Mimecast South Africa (Pty) Limited, Mimecast Offshore Limited, Mimecast North America Inc. and Mimecast Middle East.

Copyright © 2013 Mimecast Limited. All rights reserved.

Mimecast® is a registered trademark.

Unified Email Management, Secure Messaging Gateway, Message Archive, Stor5, Mimecast Storage Grid, Enhanced Stationery, ARMed SMTP, Always On, UEM Express, UEM Enterprise, UEM Advanced, Mimecast Email Protect, Mimecast Multi, Mimecast 180, Mimecast Small Business Edition, Mimecast Services for Outlook, Mimecast Synchronization Engine, Mimecast Services for BlackBerry®, Unified Email Management for Domino, Unified Email Management for Groupwise, Mimecast Services for Sharepoint, Mimecast Personal Portal, ZHARA and Where business banks its data are trademarks of Mimecast Limited. All other names are trademarks or registered trademarks of their respective owners. Any omission or misuse (of any kind) of service marks or trademarks should not be regarded as intent to infringe on the property of others.

Mimecast disclaims all warranties, either expressed or implied, including, but not limited to, implied warranties of merchantability and fitness for particular purpose, with respect to the instructions contained within this guide.

In no event shall Mimecast be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss), even if Mimecast has been advised of the possibility of such damages. As some US states do not allow the exclusion or limitation of liability for consequential damages, the above limitation may not apply to you.

Requests, amendments and suggestions to [documentation@mimecast.com](mailto:documentation@mimecast.com)



**Table of Contents**

Chapter 1: Mimecast----- 2

    What is Mimecast? -----2

    Software-as-a-Service (SaaS) -----2

    Mimecast Services -----3

    Account Integration Options -----3

Chapter 2: Navigation----- 4

    Logging In -----4

    General Navigation -----5

    Icons and Buttons -----5

    Folder Control -----6

    Groups-----6

    Building Groups-----6

    AD Groups -----7

    Exercise: Administration Console Navigation -----7

Chapter 3: Administrator Roles ----- 8

    Roles Editor -----8

    Security Permissions -----8

    Application Roles -----9

    Exercise: Administrator Roles -----9

Chapter 4: Account Settings ----- 10

    Account Settings ----- 10

    Global Permissions ----- 10

    Contact Information ----- 11

    Password Complexity and Expiration ----- 11

    Exercise: Account Settings ----- 11

Chapter 5: Application Settings----- 12

    Application Settings ----- 12

Chapter 6: Directories ----- 13

    Internal Domains----- 13

    User Permissions ----- 13

    Attributes ----- 13

    External Domains ----- 14

    Exercise: Managing User Directories ----- 14

Chapter 7: Account Connections----- 15

    Authorized Outbounds ----- 15



Delivery Routes -----	15
Directory Connections-----	16
Journaling -----	16
Gateway -----	16
Exercise: Review Configured Connectors -----	17
Chapter 8: Policies -----	18
Policy Lists -----	18
Policy Editor -----	18
Specificity-----	19
Validity -----	19
Policy Order -----	19
Exercise: Restriction Policies -----	20
Chapter 9: Logs -----	21
Event Logs -----	21
Archive Logs -----	21
Exercise: Administration Logs -----	21
Chapter 10: Reports -----	22
Reports -----	22
Exercise: Administrator Reports-----	22
Appendix: Knowledge Base and Resources -----	23
Knowledge Base-----	23
Training Courses-----	23
Other useful links:-----	23
Available Online Course Titles: -----	23



# Chapter 1: Mimecast

KBID10140

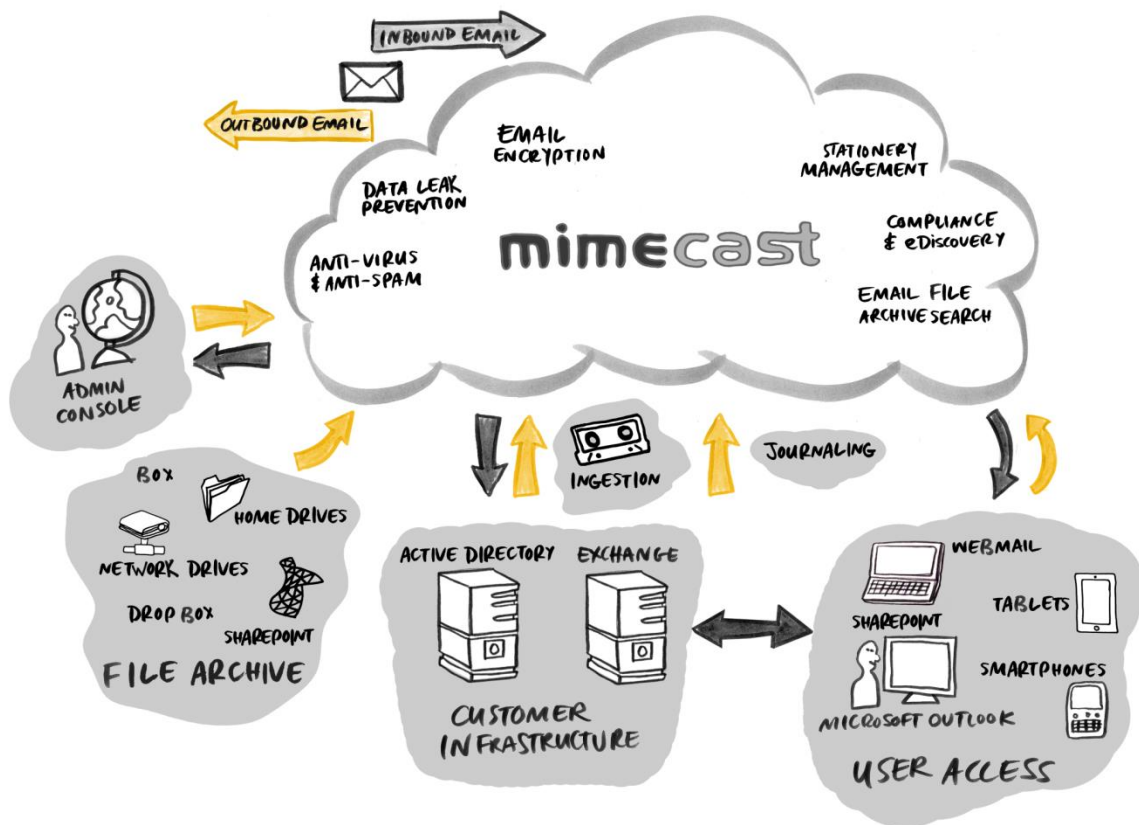
## What is Mimecast?

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.

## 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.

Service	Security	Continuity	Archiving
Mimecast UEM Enterprise	✓	✓	✓
Mimecast UEM Express	✓	✓	
Mimecast Email Security	✓		
Mimecast Email Continuity		✓	
Mimecast Email Archive			✓
Mimecast File Archive			Add-On

## 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**:

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

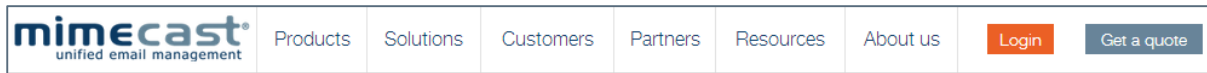
**Note:** These account services are explored in detail later in this module.

## Chapter 2: Navigation

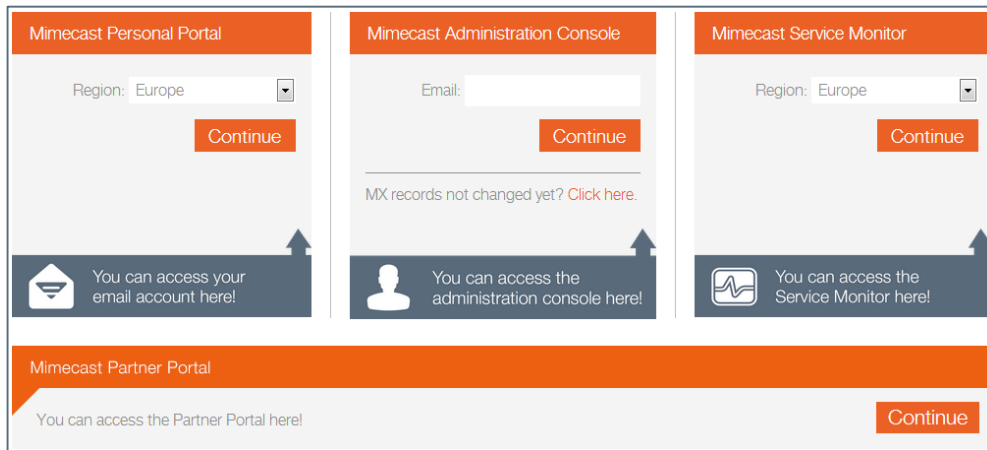
KBID10150

### Logging In

To access the Mimecast Administrator Console, visit our website: <http://www.mimecast.com>. Click on the *Log In* link on the top right side of the screen.



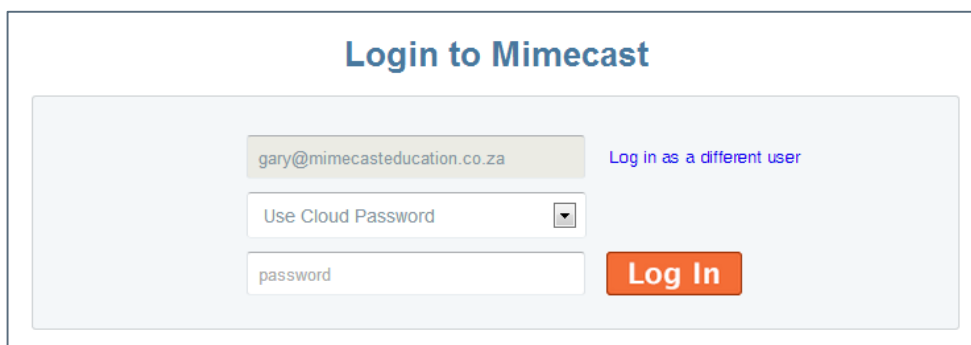
Within the Mimecast Administration Console widget, enter your email address in the available field. Click the *Continue* button.



Select whether you are using a Cloud or Domain password.

**Note:** Your password could be your network password (this is dependent on Directory Sync configuration), or it could be your local Mimecast password (cloud password).

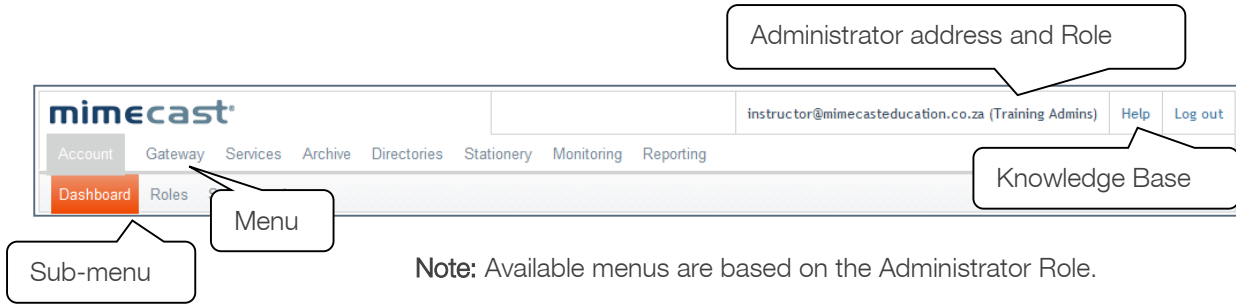
Complete your password, and click the *Log In* button.



## General Navigation

KBID10491

The Administrator Console is based on a number of Application menus, which are displayed at the top of the screen. Top-level menus can be selected directly, or hover over the top menu to display sub-menus. The selected menu is highlighted in orange.



**Note:** Available menus are based on the Administrator Role.

## Icons and Buttons

Icon	Function
	The Refresh button will reload current page information
	The Back button displays the previously viewed page. The back button in the browser window should not be used.
	Selection menus are displayed for some screens in the grey toolbar, and are used for context options items listed in that screen.
	The Close button will close a menu, or delete search parameters
	The Search field is displayed at the top of list screens for context searches.
	The Depth Selector controls the number of records, or rows, displayed in a list.
	Page Selector buttons navigate between pages of displayed list items.
	Calendar Controls are used to set date parameters as a filter.
	Context menus are accessed by right-clicking list items, and display available options for the item that was clicked on.



## Folder Control

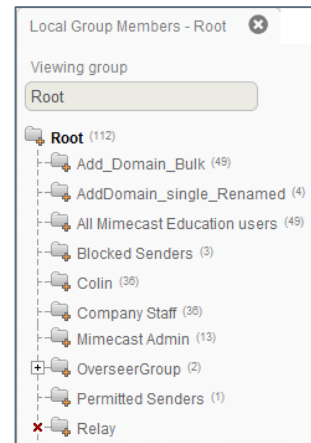
Folders are used to keep your Mimecast account organized, so items can be stored in logical folders for easy reference. Folders will display to the left side of the screen for specific menus only, and are created from a Root folder.

Folders can be used to contain Policy Definitions, and can also be used to store user/domain addresses. Folders that store addresses are called Groups.

**Note:** The folder content depends on the area in which the folder is created.

Use the icons and buttons below to modify folders:

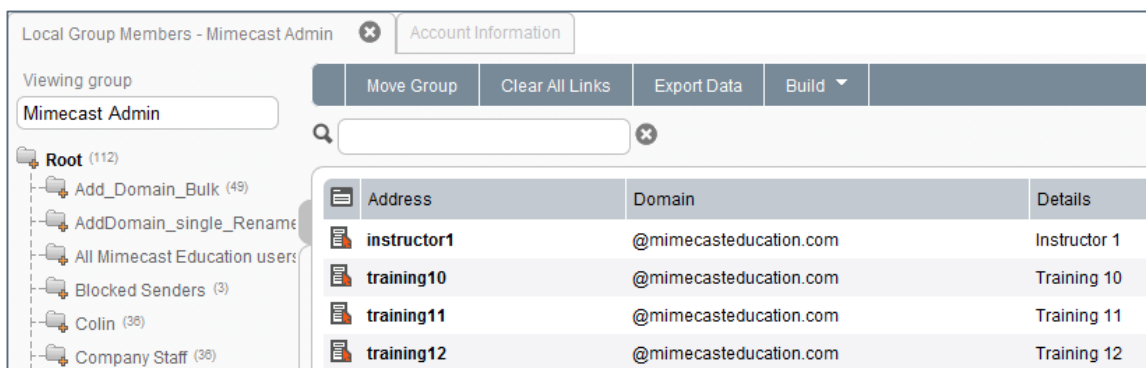
Icon/Button	Description
	Create a new folder or sub-folder
	Expand a folder to display sub-folders
	Delete an empty folder
	Rename a highlighted folder
	Move an existing folder to a different location



The number of items within the folder is displayed to the right of the folder name.

## Groups

Groups, located within the Directories menu, are folders that contain user email addresses or domain names. These lists of users can be referenced by Mimecast Policies, which makes the management and upkeep of Policies very simple.



## Building Groups

Addresses can be added to Groups by using the Build button in the toolbar. Individual addresses or domain names can be added, and a spreadsheet can be used for bulk imports. A Group Builder is also available to populate Groups based on several types of rules.

## AD Groups




KBID10315

Mimecast can synchronize Directory Groups from the network Directory, such as Microsoft Active Directory. These AD Groups can also be referenced by Mimecast Policies, just like the local Groups.

Note: AD Groups are synchronized only if a Directory Sync connector has been configured. More information is provided later in this guide with regards to Directory Sync.

## Exercise: Administration Console Navigation

KBID10600

- Log in to Mimecast
  - Visit the Mimecast website: <http://www.mimecast.com>
  - Click on the Log In link
  - Under Mimecast Administration Console, enter your email address
  - Click the Continue link
  - Select Domain or Cloud Password
  - Complete your password
  - Click the Log In button
- Navigate to different Application menus
  - Click on the Archive menu
  - Use the Back icon  to return to the Dashboard
- Work with Groups
  - Navigate to the Domains menu
  - Select Groups
  - Click on the Add Folder icon  to the left of the Root folder
  - Select the New Folder created in the list
  - Use the Viewing Group field at the top of the folder list to rename the folder
- Populate the Group
  - With the folder selected, click on the Build button
  - Click the Add Email Addresses option
  - Type your email address into the available field, and click the Save and Exit button
  - Your email address is displayed within the Group
  - Right-click your address, and select the Unlink Item from the list
  - Delete the empty folder using the Delete icon 

# Chapter 3: Administrator Roles

KBID10575

## Roles Editor

Administrator access to Mimecast is controlled by Security Permissions that are allocated to a Role. The Administrator email address is added to the Role, which enables that Administrator to log in to the Console and access specific Application menus and perform certain tasks. Only those Administrators that have the necessary Security Permissions can access available Roles from the Accounts menu. By default, Mimecast creates 6 Roles, as seen in the screenshot below.

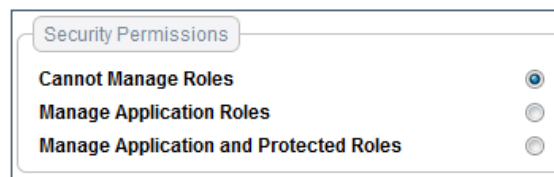
	Action	Role Name	Members	Description
	View Role	Super Administrator	8	Full privileges to all account options including content view of email and the
	View Role	Full Administrator	0	High level administrator with privileges including content view of all email, n
	View Role	Basic Administrator	3	Full administrator account without access to any protected permissions.
	View Role	Help Desk Admin	1	Account with access to common help desk tasks such as track and trace, a
	View Role	Gateway Administrator	1	Access to common gateway functionality such as policy management, track
	View Role	Litigation Administrator	1	Access to common e-Discovery features such as archive search with conte
	Edit Role	<i>Training Admins</i>	21	<i>Training Admins</i>

Note: The default Roles cannot be modified or removed, and one Administrator cannot belong to more than one role. Use the New Role button to create a new Role, or right-click an existing Role, and use the contextual menu to duplicate the Role. New or duplicated Roles are listed in Italic text within the Roles list, and an Edit Role button is available to modify the Role.

## Security Permissions

Each Role has Security Permissions, which determines if the Role can access or modify other user's Roles:

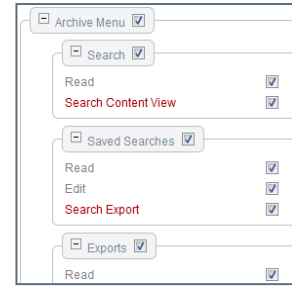
- **Cannot Manage Roles:** If an Administrator that belongs to this Role logs in, they will not see the Roles menu at all
- **Manage Application Roles:** The Administrator can access the Roles menu, and can modify the Application Menus that the Role will have access to. However, they will not be able to modify access to protected areas of Mimecast, where email contents can be accessed.
- **Manage Application and Protected Roles:** The Administrator can access the Roles menu, and can modify Roles completely. This includes access to Application menus as well as access to protected areas of Mimecast, where the contents of emails are available.



## Application Roles

Application menus are displayed at the top of the Administrator console. These menus can be made available to the Role using checkboxes for each menu. It is also possible to manage read/edit permissions, where applicable, to sub-menus.

Protected areas of Mimecast, where email contents can be accessed, are highlighted in red text.



Note: If the Roles menu is not accessible, contact our support team: [support@mimecast.com](mailto:support@mimecast.com)

## Exercise: Administrator Roles

KBID10601

- Navigate to Roles (if available)
  - Select the Account menu
  - Select the Roles menu
- Review existing Roles
  - Click the View Role button for the Basic Administrator Role
  - Review the Security Permissions for the Role
  - Review the Application menus available to the Role members
- Manage Role Administrators
  - Return to the Roles page
  - Click on the Basic Administrator Role text to open the Role
  - Click on the Add User to Role button
  - Select an address from the list
  - Click on the Basic Administrator Role
  - Right-click the address entry added earlier, and select Remove User from the list

# Chapter 4: Account Settings

KBID10012

Your Mimecast Account Settings define the parameters of your Mimecast account. It is important to review this information to ensure that the correct information has been implemented, based on your selected product.

## Account Settings

Navigate to the Account menu, and select the Settings menu. The Knowledge Base article will detail each available field. In this module, we will cover the key elements:

Field Name	Description
Maximum Retention (Days)	The maximum number of days that your emails are retained in the Archive
Number of Users	The number of licensed users for your account. This is based on users, and not on email addresses (e.g. aliases)
Pause Inbound Deliveries	Keeps inbound emails queued within Mimecast during extended mail server outages
Automatically link Aliases	Assigns alias addresses to primary mailbox addresses using the information from the Directory Sync

The screenshot shows the 'Account Settings' configuration page. Fields include: Account Name (A2 - Mimecast Education), Account Code (CCSA1A174), Account Status (Enabled), Maximum Retention (Days) (3653), Number of Users (50), Mobile Continuity Poll Interval (5), Pause Inbound Deliveries (checkbox), Warning Message After (Attempts) (0), Bounce Message After (Attempts) (0), and Automatically Link Aliases (checkbox).

Your Account Retention period is configured by Mimecast Support, based on your contracted services

## Global Permissions

Account-wide user permissions can be assigned using the available options, as detailed in the manual below:

Field Name	Description
Administration Console Timeout	Enables user logon to Mimecast Personal Portal (MPP)
Send BCC to Mail Server	Enables users to compose emails from MPP

The screenshot shows the 'User Access and Permissions' configuration page. Fields include: Administration Console Timeout (12 hour(s)), Send BCC to Mail Server (checkbox), SMTP Submission Override (checkbox), POP Services Override (checkbox), CCM Archive Search Limit (Days) (0), Outlook Services (MSO 3.x) Override (checkbox), Admin IP Ranges (CIDR n.n.n.n/x) (text area), and Security Passphrase (text field).



## Contact Information

It is important to ensure that your Account Contact information is updated regularly. If events occur that affect your Mimecast service, we will utilize the information in this section to contact your organization to inform you of the event, and to keep you updated during the event.

Account Contact	
Contact Name	Gary Bezuidenhout ?
Telephone	0727219426
Email Address	gary@mimecasteducation
CC Email Addresses (,)	gbezuidenhout@mimecast.com

## Password Complexity and Expiration

In order for the validity of the cloud password to be maintained, numerous options have been placed in the IT Administrator's hands to ensure that their cloud passwords are correct and secure.

Password Complexity and Expiration	
<b>Password Complexity</b>	
Minimum password length	0
Include at least one lowercase alphabetical character (a-z)	<input type="checkbox"/>
Include at least one uppercase alphabetical character (A-Z)	<input type="checkbox"/>
Include at least one numeric character (0-9)	<input type="checkbox"/>
Include at least one non-alphanumeric (!@#\$.)	<input type="checkbox"/>
<b>Password Expiry and Lock</b>	
Password expiration	Never
Use System Default	<input checked="" type="checkbox"/>
Account lockout threshold	5 attempts
Account lockout duration	1 mins

## Exercise: Account Settings

KBID10602

- Complete your Contact information
  - Navigate to the Account menu
  - Select the Settings menu
  - Scroll to the bottom of the screen, and complete your contact information
  - Click on the Save button at the top of the page to save your Settings

# Chapter 5: Application Settings

KBID10180

## Application Settings

The Application Settings definition includes options for Mimecast user services, which control the app behavior and level of access. A default definition is created for each Mimecast account, and provides access to various Mimecast applications for all internal Mimecast users. This definition also specifies the authentication method, update method and capabilities that users will have access to. The default definition cannot be edited, but Administrators can create a new definition if they wish to customize any of these settings. The settings are specific to the groups configured, which means that different definitions and settings can be created for different groups.

Application Settings enable Administrators to manage user application features common to all Mimecast applications, as well as specific settings for MSO, MPP and mobile devices. This includes authentication, update methods and access to specific functionality.

A Default Application Settings Definition is created for every Mimecast account. This definition enables access for all internal users to use Mimecast applications, and cannot be edited, but Administrators can create a new definition if they wish to customize any of the settings. The settings are specific to the Groups configured, which means that different definitions and settings can be created for different Groups.

Note: Any changes to application settings may take in the region of 15 minutes before changes are seen on the end user side.



# Chapter 6: Directories

KBID10572

## Internal Domains

User addresses and permissions are managed within the Domains, located within the Directories menu. Each address has its own unique permissions and Attributes. Internal Domains displays a list of all the Domain names that the organization controls from their Mimecast account.

Domain Name	Inbound Checks
@journal.mimecasteducation.co.za	Accept Any Address
@mimecasteducation.co.za	Accept Any Address

Once a Domain name is selected, it expands to display all the email address contained within the Domain:

Email Address	Name
allan@mimecasteducation.co.za	
allstudents@mimecasteducation.co.za	All Students
allusers@mimecasteducation.co.za	All Users

Note: Envelope icons to the right of the email address indicate local Mimecast mailboxes, while Directory Tree icons represent Directory Synchronised addresses.

## User Permissions

Although Global Settings can be applied for some permissions, as described earlier in this module, permissions can be configured for address groups too.

Mimecast cloud passwords can be configured in this area. These do not affect the Network password for the user. A local password is extremely useful when the Network Directory is unavailable – if a user needs to log in to Mimecast, the local password will be accepted.

**Permissions**

Password:

Confirm Password:

Force Change at Logon:

Password Never Expires:

Account Locked Out:  Unlock Account

Archive Start Date:  Clear Start Date

Allow Outlook (MSO 3.x) Services:

Allow Mobile Archive Search (Blackberry 1.2 Only):

Allow Mobile Continuity (Blackberry 1.2 Only):

Allow SMTP Email Submission:

Allow POP Access:

## Attributes

KBID10034

User properties, or Attributes, can be created manually in Mimecast or can be synchronized from the network Directory. These details can be reference in Policies or email Stationery.

**General Attributes**

wwwhomepage (LDAP):

cn (LDAP):

title (LDAP):

mobile (LDAP):



## External Domains

Mimecast will automatically log every communication from an internal user to an external user, or in the reverse. The External Domains provides a listing of all the external Domain names that have been communicated with, for either inbound or outbound messages.

### Exercise: Managing User Directories

KBID10603

- Manage User Addresses
  - Navigate to the Directories menu, and select the Internal menu
  - Use the Search field to locate your email address, and click on it to open it
  - Verify the user permissions and Attributes
  - Add a cloud password for your address
  - Click on the Save and Exit button
- Check External Addresses
  - Navigate to the Directories menu, and select the External menu
  - Select one of the external domain names
  - Review the email addresses within the external domain
- Manage Application Settings
  - Navigate to the Services menu and select the Applications sub-menu
  - Select New Application Settings
  - Enter a description for the Application Setting
  - Ensure that the “Allow Domain Authentication” check-box has been activated
  - Select Save and Exit to save your Application Settings



# Chapter 7: Account Connections

KBID10036

## Authorized Outbounds

An Authorized Outbound is required for each Customer account in Mimecast; and is the only IP address/es that Mimecast will accept outbound emails from. Each account can have multiple Authorized Outbounds.

Mimecast will only accept outbound emails from pre-configured public IP addresses. This is a security feature, and prevents mail servers which are not customer owned from using Mimecast as an open relay.

Note: If using Dynamic IP addresses for outbound email, Mimecast will not add any Authorized Outbounds to your account. Instead, you will need to configure SMTP authentication for your SMTP Connector/Send Connector to enforce authentication with Mimecast. Therefore, when sending outbound email, Mimecast will only accept emails based on successful authentication.

Entry Narrative	IP Address
Mimecast Education Server	10.1.1.1

Authorized Outbounds are configured by Mimecast support, and can be monitored within the Gateway menu, under Outbounds.

## Delivery Routes

KBID10081

Delivery routes are used to deliver emails from Mimecast; typically, inbound to your local infrastructure, although they can also be used to override MX records for outbound delivery. Delivery Routes contain the details of the delivery destination, such as the Host Name or IP Address of the email server. Mimecast’s flexible Routing Policies allow emails to be delivered to a specific server based on a domain, group, attribute or individual address.

**Route Properties**

Description:

Hostname:

Port:

---

**Alternate Routes**

Alternate Route:

---

Route Option 1:

Route Option 2:

Delivery routes determine the route to be used for inbound email delivery. By default, outbound emails will be delivered to the recipient using available MX records, however if an outbound delivery route has been configured, this would override the MX record. Delivery routes require the specific route to be configured, and then a policy to determine the flow of traffic. Alternate routes can also be created, which enables a failover option, should a customer’s primary route be unavailable.

Delivery routes are configured in the Gateway menu, under Policies. Use the Definitions button to view the definition for the Delivery Routes. The definitions are referenced within the Policy.

If multiple similar routes (the FROM and TO variables are the same) are configured, this will result in a round robin (random selection) of these routes. This is useful to balance mail server load.

## Directory Connections

KBID10036

A Directory Connection is a link between Mimecast and the customer Domain Controller. The link is created through Lightweight Directory Application Protocol (LDAP). Periodically, Directory Connections are automatically synchronized by Mimecast in order to keep synced data up to date. Alternatively, an Administrator can manually sync their LDAP details if this is required.

There are three uses for the Directory Connection:

- User Authentication
- Distribution Group Synchronization
- User Data Synchronization

Mimecast can be configured to Authenticate user logon to Mimecast using the domain credentials, so that a user does not need a separate username and password to access Mimecast. Directory Passwords are not stored in Mimecast, thus the network security of Mimecast customers using this feature is not compromised.

Distribution Groups and User Data are also synchronized to Mimecast, with specific Attribute information (if configured - view the article on Attributes for further information). This includes any mail-enabled object in the Directory (any object with an SMTP address).

To configure Directory Connections, navigate to the Services menu and select the Directory Sync menu.

## Journaling

KBID10235

Journaling is the process that allows Mimecast to retrieve internal emails from our customer's environment, in order to provide a full archive of both internal and external emails. Mimecast can archive journal messages via either SMTP or POP3. SMTP journaling allows the customer to push the emails from their internal environment to Mimecast.

If one of your email requirements is to archive all emails, both external and internal, journaling should be enabled. By configuring SMTP journaling, all internal emails are captured from your email Server, and then archived by pushing these emails to Mimecast using the SMTP protocol.

For more information on configuring Journaling for your mail server, view our Knowledge Base.

## Gateway

KBID10928

Mimecast is now inviting existing customers to move to our latest mail gateways. In 2010, Mimecast started a major project to develop a new mail gateway which would offer extended features, better performance, and more effective scaling. The resultant gateway has been in production since the start of 2012, and at the time of writing (June 2013), more than 20% of our customers are using this platform for all of their inbound and outbound mail processing. With the new gateway attaining mainstream status, Mimecast has moved the legacy mail gateway into a "sunset phase" to indicate that future enhancements will be available only on the new gateway. Once all customers have successfully migrated, we will retire the legacy mail gateway and from this point on, further changes to the legacy gateway will be limited to essential maintenance.

Note: Upgrading your Gateway does NOT change your Administrator or User service login addresses.



## Exercise: Review Configured Connectors

- Confirm the configuration of the additional services:
  - Authorized Outbounds: Navigate to Gateway | Outbound
  - Delivery Routes: Navigate to Policies | Definitions | Delivery Routes
  - Directory Connections: Navigate to Services | Directory Sync
  - Journaling: Navigate to Services | Journaling



# Chapter 8: Policies

KBID10191

## Policy Lists

Mimecast Policies are a set of rules that affect the flow of email traffic, and are applied to either Inbound or Outbound messages. The available Policies allow an Administrator to apply granular control to the flow of email as they are processed by Mimecast.

Policies can be set to affect emails in many ways - email flow can be halted (Hold for Review, or Block Policies), data leaks can be prevented (Content Examination, or Document Conversion Policies), and Attachment Handling and Spam Policies can also be applied.

All available Policies are consolidated in a dedicated Gateway Policy Editor within the Gateway menu. By selecting any of the Policy types, an Administrator is able to create new policies, and amend or remove existing policies. The Policy Editor should also be used to configure Policy definitions which are used to apply even more granular control to certain policies.

Description	Policies	Definitions
Address Alterations	7	N/A
Attachment Block On Size	8	N/A
Attachment Link On Size	50	N/A
Attachment Management	44	101 <a href="#">Definitions</a>
Auto Allow	2	N/A

## Policy Editor

The Policy Editor is used to create or amend Policies in Mimecast. If the policy is set to Active, as soon as the changes are Saved, the Policy will take effect based on the parameters specified in the Policy.

Navigate to the Gateway menu, and select the Policy that you would like to manage. Click on an existing Policy to edit it, or click on the New Policy button to create a new Policy.

**Options**  
 Policy Narrative: [ ]  
 Select Option: **Take no action**

**Emails From**  
 Addresses Based On: **The Return Address**  
 Applies From: **Everyone**  
 Specifically: **Applies to all Senders**

**Emails To**  
 Applies To: **Everyone**  
 Specifically: **Applies to all Recipients**

**Validity**  
 Set policy as perpetual: **Always On**  
 Date Range: **All Time**  
 Policy Override:   
 Bi Directional:   
 Source IP Ranges (n.n.n.n/x): [ ]

## Specificity

KBID10193

Specificity relates to the order in which Mimecast applies Policies to emails. The more specific a Policy is, the higher the priority. For example, a Policy specifying a single individual email address is very specific and will be applied first, in contrast to a Policy applied to Everyone which is the least specific of all, and will therefore be applied last.

## Validity

KBID10194

Validity parameters control the application of a Policy to an email. An Active Policy is applied to emails, and an Expired Policy is ignored by Mimecast. Validity can be controlled manually, and Policies can also be automatically set to expire on a certain date. By default policies are set to apply Eternally.

Policy Validity also allows certain options to be applied to Policies, e.g. bi-directional Policy application, Policy override, and adding Source IP addresses.

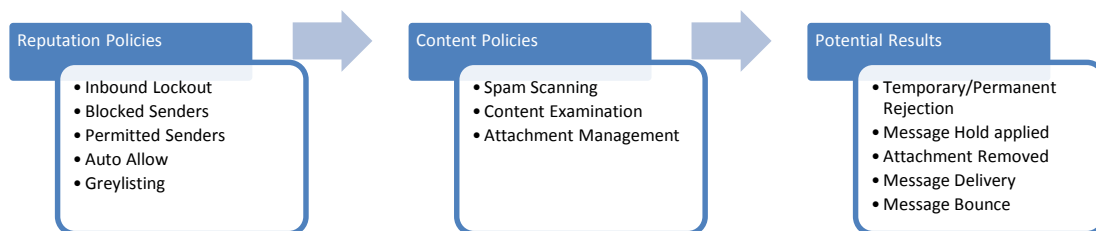
Status Indicators	Description
	Policy is currently active
	Policy starts in the future
	Policy has expired
	Policy Override

An Override changes the order of selection for a list of Policies. When an Administrator needs to force Mimecast to ignore specificity, they can apply the Override option - Mimecast will apply the Policy with the Override before it applies the other Policies.

## Policy Order

KBID10191

Mimecast Policies are applied in a specific order to emails that are processed for delivery. A full Policy Processing flowchart is available from download from our Knowledge Base. The manual below outlines a high-level view of the Policy flow:



## Exercise: Restriction Policies

KBID10605

- Navigate to the Gateway menu, and select the Policies menu
- Select the Blocked Senders Policy, and click on the New Policy button
- Add a description in the Narrative field: Test Block Policy
- Change the Blocked Sender Policy field to Block Sender
- Within the Emails From section, change the Applies From field from the Everyone option to Individual Email Address. The page refreshes to display the Specifically field
- Enter your internal email address within this field (i.e. the email address from where you will send the test email message)
- Within the Emails To section, change the Applies To field from the Everyone option to Individual Email Address. The page refreshes to display the Specifically field
- Enter your external email address within this field (i.e. the email address to which you will send the test email message)
- Use the Date Range calendar control to adjust the Policy Validity so that the Policy applies for today's date only
- Select the Bi Directional checkbox, and click the Save and Exit button to save the Policy
- Using the email address specified in the Emails From section, send a test email to the address specified in the Emails To section. The email should fail in delivery
- Using the email address specified in the Emails To section, send a test email to the address specified in the Emails From section. The email should fail in delivery
- Return to the Policy in the Mimecast Administration console, and right-click it to remove it.



## Chapter 9: Logs







KBID10103

### Event Logs

The Event Log provides a comprehensive list of changes and events that have occurred within your Mimecast Account. The logs are immutable, and will be available for the length of the retention configured for the Mimecast account.

The Event Log acts as an audit of all relevant Administrator, user and automatic activities within your Mimecast Account and provides monitoring and accountability. Below is a list of some of the event types that are captured:

- Users logged on, Login failures
- Account changes
- User Account changes (including password changes)
- New Policies, deleted policies
- Any definition or policy amendments
- Directory Synchronization
- Journal failures
- Folders being created, updated

User	Type	Date Time	Details
 aohare@mimecasteducation.com	User Logged On	2011-12-24 09:51:44	 120.147.118.59; v2
 <->	Completed Directory Sync	2011-12-24 08:00:05	 Processed 2 domain(s), 29 user(s), 60 group(s)
 <->	Completed Directory Sync	2011-12-24 02:05:37	 Processed 2 domain(s), 29 user(s), 60 group(s)

### Archive Logs

KBID10135

The Message 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.

Message View logs provide a full audit trail of all Administrator views of both the metadata and content of emails in the Archive.

### Exercise: Administration Logs

KBID10606

- Event Logs
  - Navigate to the Accounts menu, and select the Logs menu
  - Review the log entries
- Search Logs
  - Navigate to the Archive menu, and select the Search Logs menu
  - Review the log entries
- View Logs
  - Navigate to the Archive menu, and select the View Logs menu
  - Review the log entries

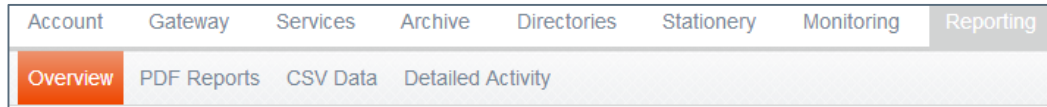


# Chapter 10: Reports

KBID10137

## Reports

The Mimecast Reporting module contains detailed statistics covering emails processed, rejected emails, and communication flows. These reports can assist with infrastructure planning through data load analysis, show spam and virus trends, as well as supply usage reports on a per user basis. The Reporting Overview graph allows an Administrator to review the flows of traffic within their environment; outbound, inbound and internal.



Menu Item	Description
Overview	Shows a graphical representation of inbound, outbound and internal email volumes within the customer environment.
PDF Reports	Schedule weekly or monthly reports to be emailed to specific recipients, or made available for download.
CSV Data	Mimecast Reporting provides graphs to show email volumes and bandwidth usage for your account. Some of this data and other logs are made available through a daily download of the CSV data.
Detailed Activity	This customizable Report can be used to query specific email transmission data between senders and recipients, and provides the Administrator with reports on the email or byte count either between individual email addresses, domains or everyone.

## Exercise: Administrator Reports

KBID10607

- Navigate through the available reports within the Reports, and view available report data

# Appendix: Knowledge Base and Resources

## Knowledge Base

KBIDxxxxx

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:

<http://www.mimecast.com/What-we-offer/email-support-and-education/Upcoming-course-schedule/>

Online Training (1 hour)	Date	Start Time	Remaining Places	
Product Overview	12-Aug	13:00	28	<a href="#">Book now</a>
Account Tour	14-Aug	13:00	33	<a href="#">Book now</a>
Continuity	19-Aug	13:00	35	<a href="#">Book now</a>
Security	17-Jul	13:00	13	<a href="#">Book now</a>
Archiving	18-Jul	13:00	20	<a href="#">Book now</a>
Stationery	22-Jul	13:00	18	<a href="#">Book now</a>
Admin Tasks	29-Jul	13:00	20	<a href="#">Book now</a>
Exchange Tools	24-Jul	13:00	23	<a href="#">Book now</a>
User Services	31-Jul	13:00	23	<a href="#">Book now</a>

## Available Online Course Titles:

- Mimecast Product Overview
- Mimecast Account Tour
- Mimecast Continuity
- Mimecast Security
- Mimecast Archiving
- Mimecast Admin Tasks
- Mimecast Exchange Tasks
- Mimecast Stationery
- Mimecast Admin Tasks

## Available Classroom Course Titles:

- Mimecast Service Management
- Mimecast Power Tools
- Mimecast Stationery Management

## 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>

