mimecast™

Mimecast Advanced Account Administration

Effectively manage complex, multi-national or multi-divisional messaging environments, with tailored routing, administration and policy controls.

Mimecast Advanced Account Administration provides flexible and effective tools to manage large or complex email infrastructures. These environments are often comprised of groups or divisions with different management or staff requirements.

It allows for individual domains or divisions that require segmentation or separation of administrative duties — but with control retained by top-level administrators. Flexible policy inheritance ensures group or corporate level policies replicate down to regional or divisional business accounts.

How it works

Domain splitting

Mimecast enables administrators to split single domain name email environments across multiple Mimecast customer accounts, as well as multiple accounts across a subset of domains.

Key Features

- Single domain split routing for email across a host of environments and MTAs (Mail Transfer Agent), Example: Microsoft Exchange, Office 365, Domino and Google Apps.

- Policy inheritance and hierarchy gives administrators trickle-down policy control to their sub-organizational units.

- Federated account administration gives top-down administration for sub-organizational accounts within the same structure.

- Segregate account administration for single organizations with multiple accounts.

- Individual account retention and subscription.

This functionality is useful for organizations that have many geographic locations that process email, but maintain a single Internet facing email domain name.

mimecast™

Segregated and Federated Administration

The Advanced Account Administration service enables administrators to link multiple Mimecast accounts to one overall master account, then segregate administrative duties.
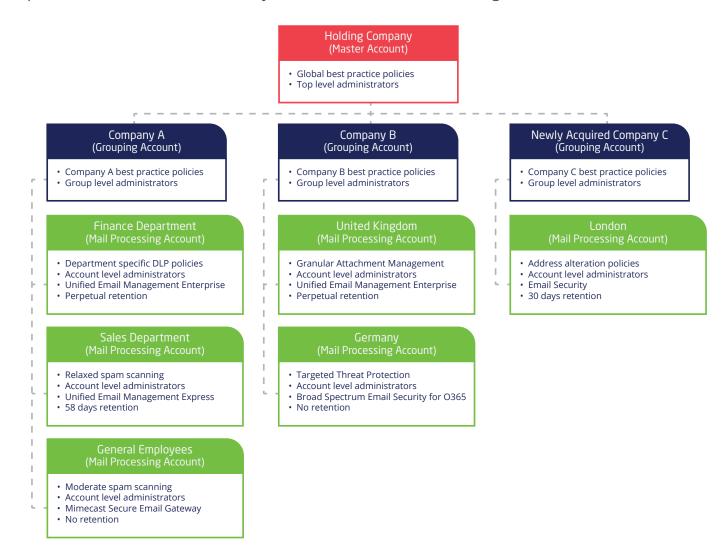
These multiple accounts can be grouped to create a hierarchy. Granular permissions can be given to administrators at lower tiers of the hierarchy. The management permissions granted are reflected in the Mimecast Administration Console.

For example, Company A and Company B merge. Prior to the merger only Company A used Mimecast, now both plan to use Mimecast. However, they want to maintain separation of the two firms' email systems.

A master (top level) administrator controls all aspects of both organizations' Mimecast service. They delegate control of Company A to the Company A (group level) administrator who, in turn, may delegate permissions to separate divisions (mail processing level) within Company A.

The master administrator similarly delegates control of Company B to the Company B (group level) administrator.

Company A and Company B administrators are only able to manage the Mimecast service for their own organizations, while the master administrator can manage and alter policies across both organizations.

Holding Company
(Master Account)
- Global best practice policies
- Top level administrators

Company A
(Grouping Account)
- Company A best practice policies
- Group level administrators

Company B
(Grouping Account)
- Company B best practice policies
- Group level administrators

Newly Acquired Company C
(Grouping Account)
- Company C best practice policies
- Group level administrators

Finance Department
(Mail Processing Account)
- Department specific DLP policies
- Account level administrators
- Unified Email Management Enterprise
- Perpetual retention

United Kingdom
(Mail Processing Account)
- Granular Attachment Management
- Account level administrators
- Unified Email Management Enterprise
- Perpetual retention

London
(Mail Processing Account)
- Address alteration policies
- Account level administrators
- Email Security
- 30 days retention

Sales Department
(Mail Processing Account)
- Relaxed spam scanning
- Account level administrators
- Unified Email Management Express
- 58 days retention

Germany
(Mail Processing Account)
- Targeted Threat Protection
- Account level administrators
- Broad Spectrum Email Security for O365
- No retention

General Employees
(Mail Processing Account)
- Moderate spam scanning
- Account level administrators
- Mimecast Secure Email Gateway
- No retention

Retention and Subscription

For organizations that require multiple archive retention scenarios within different parts of the same business structure, using Advanced Account Administration, retention can be set individually based on users, groups or organizational units.

Policy Inheritance

Policy inheritance optionally ensures that global or group policies are enforced on lower tiers in the organization hierarchy.

This provides the flexibility, for example, to ensure that policies applied at the global level are applied throughout the organization, regardless of any changes made by an administrator of a lower tier.

For example, an organization's master administrator sets a global data leak prevention policy that prevents Excel spreadsheets being sent externally by email and enforces that policy to be inherited by lower hierarchy tiers. The administrator for the United Kingdom division is asked by the sales director to temporarily lift the policy for the United Kingdom sales team. As the master policy is inherited, the United Kingdom administrator cannot change the policy to achieve this, enforcing company best practice globally.