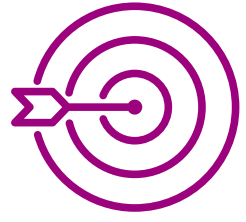




Implementation Overview Phases & Status

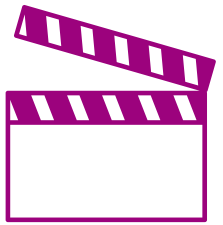
Phase 1 – Account Setup & Initial Configuration (Completed)



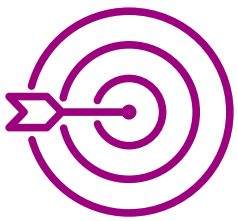
Goal: Establish Mimecast account, validate domains, and configure routing and security basics.

Actions Taken:

- Configured mail infrastructure.
- Validated domains and configured routing via Mimecast Onboarding Assistant
- Set up emergency contact details
- Added Mimecast IPs to allowlist to prevent mail being marked as spam
- Configured delivery routes (Outbound mail routing)
- Directory sync setup (AD/Azure)
- Verified SPF, configured journaling, and reviewed mail forwarding



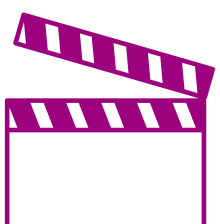
Phase 2 – Inbound Routing & Go-Live Cutover (Complete)



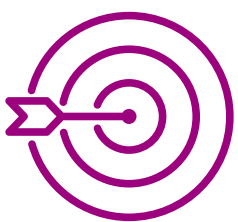
Goal: Complete the live mail flow transfer into Mimecast.

Actions Taken:

- Covered anti spoofing bypass for trusted third party senders (We need to confirm this has been completed and can cover it again in phase 3)
- Updated MX records to route inbound mail through Mimecast
- Checked domains are validated.



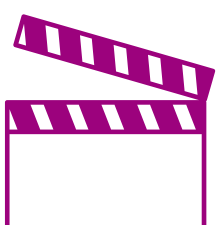
Phase 3 – Final Configuration & Admin Enablement (Remaining)



Goal: Confirm full operation and finalise settings.

Actions Taken:

- Cover Anti Spoofing bypass (Need to confirm if this includes Hostnames/IPs that require SMTP authentication with password).
- Revisit mail forwarding (If required)
- DKIM Policy configuration
- Admin Console overview and walkthrough
- Review of policies (DLP, content/attachment controls)
- SSO configuration
- Final troubleshooting and validation





Customer Responsibilities:

- Review and confirm policy settings
- Have access to Entra/Enterprise Apps for SSO configuration
- Confirm readiness for full operational use

Timeframes

Phases 1 & 2: Complete

Phase 3: To be scheduled (I will confirm the date once I've checked availability with our lead implementation engineer)

Please note that this timeframe is not final additional sessions can be scheduled if required to complete configuration or address any outstanding items.

Important Notes

- This is not a POC. This is a live deployment for an active, paid Mimecast licence.
- The scope is the live transfer and configuration of mail flow into Mimecast.
- Once the service is live, any additional domain configuration beyond the agreed scope is the customer's responsibility.

Sync & Recover	https://mimecastsupport.zendesk.com/hc/en-us/articles/34000705748115-Sync-Recover-Getting-Started
Archive	https://mimecastsupport.zendesk.com/hc/en-us/articles/34000702488723-Archiving-Guides
Awareness Training	https://mimecastsupport.zendesk.com/hc/en-us/articles/34000407848723-Engage-Rapid-Deployment-for-Email-Security-Cloud-Gateway#h_01J9RBEQEMNVSAHNCAT2VTAIS
Large File Send	https://mimecastsupport.zendesk.com/hc/en-us/articles/34000491473171-Large-File-Send-Configuration-and-Use
Secure Messaging	https://mimecastsupport.zendesk.com/hc/en-us/articles/34000464071315-Secure-Messaging-Definitions-Policies
Privacy Pack	https://mimecastsupport.zendesk.com/hc/en-us/articles/34000809117459-Content-Examination-Configuring
ABEC	https://mimecastsupport.zendesk.com/hc/en-us/articles/34000865961747-Advanced-BEC-Overview#h_01K6DA6ZHYJ7DQ9AXDGXFYQHE5
Collaboration Tools	https://mimecastsupport.zendesk.com/hc/en-us/articles/34000494659347-Collaboration-Security-Protection-for-Microsoft-Teams

Add Ons or Standalone Products

DMARC Analyzer	https://mimecastsupport.zendesk.com/hc/en-us/articles/34000795481107-DMARC-Analyzer-Configuring-DMARC
DMARC Managed Service	This will be managed by Mimecast, for any queries please reach out to your account manager
Brand Exploit Protect	This will be managed by Mimecast, for any queries please reach out to your account manager
Aware	This will be managed by Mimecast, for any queries please reach out to your account manager
Incydr	This will be managed by Mimecast, for any queries please reach out to your account manager
Engage	https://mimecastsupport.zendesk.com/hc/en-us/articles/37445617009299-Configure-Engage
Awareness Training	https://mimecastsupport.zendesk.com/hc/en-us/articles/37352102706835-Configure-Awareness-Training

Best Practice Resources

To maximise value and ensure your configuration is solid from the start, here are some helpful resources:



<https://www.mimecast.com/content/email-security-tips/>

<https://mimecastsupport.zendesk.com/hc/en-us>



Mimecast Resources

Mimecast Support Centre	https://mimecastsupport.zendesk.com/hc/en-us
Mimecast Community Page	https://community.mimecast.com/

Want to further your Mimecast Knowledge? – Mimecast University for training and certification pathways

Mimecast Partner One Professional Services Certification

<https://mupartner.mimecast.com/pages/210/mimecast-university-partner-reseller>



Mimecast Technical Pre Sales Certification

https://mupartner.mimecast.com/learn/courses/2398/partner-technical-pre-sales-certification?hash=a05ddf5f5705a6573bfe1732e048c077f39f1c04&generated_by=47369

Mimecast Reseller Sales Certification

https://mupartner.mimecast.com/learn/courses/2397/partner-sales-certification?hash=30f3f90b2c333c3232a7e6656455172aca93c7e9&generated_by=47369

Need More support?

Here at Exclusive Networks, we've got the team of experts to support you, who are available to carry out implementation.

We have a variety of packages across the Mimecast product portfolio:

Set up Email Security – Cloud Gateway

Core P-SP021-1P-MC-0001 / Guided P-SP021-1P-MC-0002 / Managed P-SP021-1P-MC-0004

Set up Email Security – Cloud Integrated

Cloud Integrated / P-SP021-1P-MC-0008

Add on or Standalone products

Archiving / P-SP021-1P-MC-0006

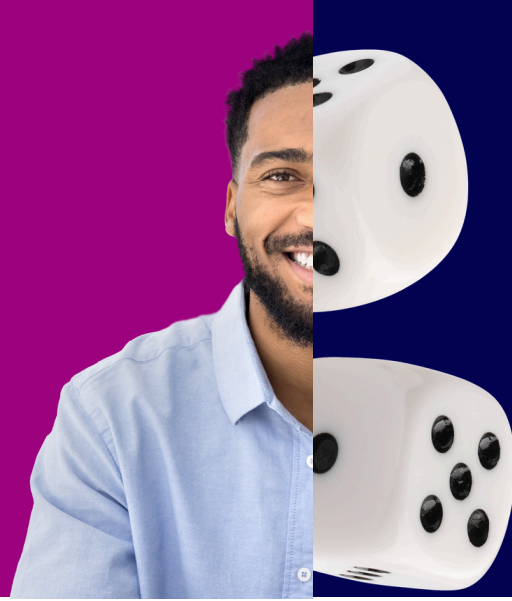
Engage & Awareness Training / P-SP021-1P-MC-0005

DMARC / P-SP021-1P-MC-0007

Need help with New Package upgrades and the setup of new features?

New Feature Secure Start / P-SP021-1P-MC-0010

Contact the team at Mimecast_UK@exclusive-networks.com for further information and support.



New Feature: Secure Start

Provides expert guidance on the implementation and configuration of Mimecast Features when added after initial setup. Includes Email Continuity, Sync & Recover, Collaboration Security, Large File Send, Secure Messaging, Internal Email Protection/Targeted Threat Protection, and Advanced BEC. Ensures seamless deployment and optimal performance across all environments, while also assisting with package upgrades to unlock enhanced features and advanced security capabilities.

Base Inclusions

P-SP021-1P-MC-0010

Average Implementation Time (working days)	2 days
Mimecaster Central (KB & Community)	✓
Continuous Knowledge Transfer	✓
Implementation Troubleshooting Support (phone/remote sessions)	✓
Mimecast Adcon familiarization	✓ (limited)
Named Implementation Engineer	✓
Kick-off call	✓
Scheduled calls and remote sessions	✗
Review/Closure call	✓

Advanced BEC

Setup of detection policies and enable "Monitor Mode" to trial BEC protection without immediately blocking emails, allowing you to see how it would affect your environment.	✓
Determine the sensitivity applied to BEC Detections	✓
Select actions triggered by BEC Detections	✓
Choose who will be notified when this policy is applied	✓
Add a rule to apply the policy to different senders and recipients	✓

Internal Email Protect

Create a Connector to establish a connection between Mimecast and your email server.	✓
Create policies for inbound, outbound, and internal email scanning.	✓
Configure URL Protect	✓
Ongoing management of the Admin console	✗
Continuous policy tuning beyond the initial guided session	✗
Continuous monitoring and tuning of detection parameters and review of alerts	✗
Resolution of unrelated email security issues not tied to BEC or IEP	✗
Integration with third-party security tools. Any additional integrations with SIEMs or SOAR platforms	✗
Configuration of any other policies or definitions in the email gateway.	✗
Configuration of any other policies or definitions in the email gateway.	✗

Sync and Recover

Configuration of connectors for Microsoft 365	✓
Creation and scheduling of sync tasks	✓
Target mailbox selection and date filtering setup	✓
Test synchronization to confirm data is properly syncing and recoverable	✓
Ongoing management or monitoring of Sync & Recover post-deployment	✗
Restoration of large volumes of historical email beyond testing or initial validation	✗
Custom automation or scripting outside of native Sync & Recover functionality	✗
Configuration of non-Microsoft 365 environments	✗
Troubleshooting issues unrelated to Sync & Recover setup	✗



New Feature: Secure Start

Collaboration & Messaging

Protection for MS Teams

Configuration of default policies where you can choose monitor or protect mode	✓
Guidance on setting up Policy Management	✓
Guidance on setting up Reports for your Detections data	✓

Protection for Onedrive and SharePoint

Guidance on configuring TTP managed URLs	✓
Guidance on setting up Reports for your Detections data	✓

Large file send

Configuration of Large File Send policies	✓
Setup of user access and permissions	✓
Setup of user access and permissions	✓
Customisation of file size limits and expiration settings	✓

Secure messaging

Configuration of Secure Messaging policies	✓
Setup of content-based triggers or manual sending options	✓
Walkthrough of the admin console	✓
Ongoing policy management or monitoring after go-live	x
End-user training or communications rollout	x
Custom scripting or API integrations beyond standard setup	x
Enablement of unrelated Mimecast services (e.g. Email Gateway, DLP not related to Secure Messaging)	x
Third-party integrations or SIEM logging setup	x
Remediation of existing threats in SharePoint/OneDrive/Teams	x

Continuity

Activation of the Email Continuity service for your environment	✓
Configuration of continuity policies and settings	✓
Ensure mail routing is correctly aligned with continuity failover.	✓
Guidance on Creating a Continuity Monitor or Configuring Continuity Events	✓
Guidance on Creating a Continuity Monitor or Configuring Continuity Events	✓
Guidance to ensure users have access to email via the Mimecast Personal Portal or Outlook add-on	✓
Disaster recovery planning or testing	x
Custom user access configurations. Configuration of user groups, granular permissions, or tiered access for different roles	x
User communication or training plans	x
Integration with third-party backup or DR systems	x
Mobile device setup support	x