

mimecast®

Service Levels and Support Description (for Managed Service Providers)

December 2024

Service Levels and Support Description

(for Managed Service Providers)

December 2024

This Service Levels and Support Description applies where a Customer has subscribed to the Services through a Partner managed service provider. All credits shown will apply to the relevant Service only.

A. SERVICE LEVELS

1. Email Delivery:

This Service Level measures the ability to deliver email messages to or from Mimecast’s servers for each individual Customer and for the Messaging Security and Archiving Services *only*.

Service Availability Per Calendar Month	Credit of Fee for the Affected Month
<100% but >=99%	10%
<99% but >=98%	20%
<98% but >=97%	30%
<97% but >=96%	40%
<96%	50% and Partner may terminate the applicable Order and receive a pro-rata refund of any unused pre-paid fees.

2. DNS Resolution:

This Service Level measures the ability to resolve customer DNS requests against Mimecast’s servers for the Web Security Services *only*.

Service Availability Per Calendar Month	Credit of Fee for the Affected Month
<100% but >=99%	10%
<99% but >=98%	20%
<98% but >=97%	30%
<97% but >=96%	40%
<96%	50% and Partner may terminate the applicable Order and receive a pro-rata refund of any unused pre-paid fees.

3. Spam Protection:

This Service Level measures the effectiveness of the protection against receipt of spam for those Messaging Security and Archiving Services that include such functionality. This Service Level is measured in terms of “False Positives” and “False Negatives” (defined below) for each individual Customer. This Service Level applies across all of Customer’s email traffic and SMTP connection attempts (any attempt to connect to a Mimecast SMTP mail gateway to send email).

- (a) **Definitions:** A “**False Positive**” is an e-mail incorrectly classified as spam by the Service. False Positives do not include emails which: (i) do not constitute legitimate business email; (ii) are sent from a compromised machine; (iii) are sent from a machine which is on a third-party block list; or (iv) are sent from a mail server that does not fully comply with the SMTP delivery standards as defined in RFC 2821 & 2822. A “**False Negative**” is a spam email that the Service does not identify as spam.

(b) Service Levels:

False Positive Service Levels:

False Positive Capture Rate per Calendar Month	Credit of Fee for the Affected Month
>.0001% but <= .001%	10%
> .001% but <= .01%	20%
> .01% but <= .1%	30%
> .1%	40%

False Negative Service Levels:

Consecutive days with False Negative Rate Exceeding 2%	Credit of Fee for the Affected Month
2 – 3	10%
4 – 5	20%
6 – 9	30%
10+	40%

4. Anti-Virus Service:

This Service Level measures protection against infection of Customer’s servers by a virus through the Services, for those Messaging Security and Archiving Services that include anti-virus functionality. Upon confirmation by Mimecast that Customer’s systems have been infected by one or more harmful viruses in any calendar month through the Services, Customer will be entitled to a service credit from Mimecast equal to 50% of the fees paid to Mimecast by Partner for the applicable Customer for the affected calendar month.

5. Search Performance:

This Service Level relates to the search time experienced by Permitted Users accessing Mimecast’s email archiving service. This Service Level measures the time elapsed only when using the administrative console, Mimecast Personal Portal, Mimecast for Outlook or any Mimecast Mobile application between the receipt of the Permitted User’s search request by Mimecast’s systems and when the return of the search results is initiated by Mimecast (the “**Query Time**”). This Service Level does not apply to searches conducted using the Case Review or Supervision components of the administration console. This Service Level applies only where Customer has performed at least 250 searches in the given month.

Query Time *	Credit of Fee for the Affected Month
> 7 seconds but <=20	10%
> 20 seconds but <= 25	15%
Greater than 25 seconds	25%

*Query Time calculated via the median search times for all searches conducted by Permitted Users in the given month across all of the applicable applications.

6. Credit Request Process and Service Credits

To receive a credit under Section A, the Partner must submit a credit request by opening a support case within 14 days after the end of the calendar month in which Mimecast failed to meet the standards. Credits are based on Mimecast’s performance for each individual Customer, not on aggregated performance for all Customers contracting through the Partner. A separate credit request must be made for each affected Customer, including details and dates of anomalies and a reference to the specific Customer’s Order. Upon verification, Mimecast will apply the appropriate credit and notify the Partner. The credit amount will be calculated based on the fees paid by the Partner for the affected Customer for the applicable month and the specified percentages. Mimecast’s

maximum liability for any individual Customer in a calendar month is capped at 100% of the fees paid for that Customer for the applicable month.

7. Service Level Conditions

Service Levels do not apply under the following circumstances:

- During trial periods, planned maintenance, force majeure events, or service suspensions by Mimecast per the Agreement.
- When the Customer uses the Services contrary to Documentation (including the best practice implementation policies therein) or reasonable usage allowances, defined as three times the typical average user for archiving, journaling, SMS messaging, and DNS resolution.
- Emails with unscannable attachments (e.g., encrypted or password-protected).
- Implementation of excessively complex full text content policies by Customer or Partner.
- Emails sent to large external distribution lists, which may require serialized delivery.
- Denial of service attacks originating from third parties or the Customer.
- Inability to access MX host servers due to Internet failures.
- Viruses introduced by the Customer or Partner.
- Issues caused by non-RFC-822 compliant mail servers.
- Customer's email system operating as an "open relay," allowing unauthorized mail forwarding.

Mimecast reserves the right to contact the Partner to renegotiate terms if a Customer exceeds the reasonable usage allowance.

8. SERVICE MAINTENANCE

Mimecast may from time to time modify and/or enhance the Services, which may require the cessation or interruption of the Services. Mimecast shall use reasonable endeavours to avoid doing so during the hours of 8:00am to 8:00pm on business days in the Applicable Region. Where Mimecast is required to undertake emergency maintenance which is necessary to safeguard the Services and/or any systems on which it operates then it may do so at any time but nonetheless shall endeavour to provide as much advance warning as it reasonably can to Partner.

B. TECHNICAL SUPPORT

Mimecast will offer technical support (“Technical Support”) for the Services, responding to Managed Services Partner (“MSP”) requests within the specified time frames and working to resolve issues promptly. All support requests will be logged, assigned an incident number, and addressed with reasonable efforts to provide a resolution. Temporary solutions may be provided if necessary.

For detailed information on how to raise cases with Mimecast Support, please see the accompanying [Support Guide](#).

1 CONTACTS

In accordance with Mimecast’s Partner One Program, the MSP will ensure that they have sufficient engineers that have successfully completed Mimecast’s Technical Support Certification in order to become a “Certified Technical Contact”. The Certified Technical Contacts will act as the MSP’s Mimecast Subject Matter Experts, serving as internal escalation and enablement points. Mimecast Technical Support will only accept cases from MSP’s Certified Technical Contacts, who are responsible for:

- Ensuring the successful resolution of all cases relating to the Mimecast Platform that are within the MSP’s scope of capability, as detailed in the matrix in Section 2 (below).
- Raising cases to Mimecast Technical Support where the MSP does not have the privileges and/or access needed to resolve the related ticket. Being available to troubleshoot tickets logged.
- Acting as the primary point-of-contact for Customer Critical Cases (as defined in Section 4 below), including ensuring availability of a Certified Technical Contact to work with Mimecast for the duration of the case.

Mimecast will provide and maintain contact information for MSPs to contact the Technical Support team in the applicable region.

2 MSP Support Responsibilities

Support responsibilities are determined by the MSP Program Tier the MSP belongs to, and the responsibilities may vary by tier.

Requirement	MSP Program Tier			
	Authorized	Premium	Elite	Sapphire
Critical Case Support Submission (24/7/365)	<ul style="list-style-type: none"> • Critical requests must be logged by a Certified Technical Contact. • Related logs and completed troubleshooting to be captured on the case. • MSP must have a Certified Technical Contact available for troubleshooting for the duration of the Critical case. • Critical cases must follow Mimecast case priorities as defined in Section 4 (below). 			
Normal Case Support Submission (Business Hours*)	<ul style="list-style-type: none"> • Support requests must be logged by a Certified Technical MSP Contact. • Related logs and completed troubleshooting to be captured on the case. 			
Outside Business Hours* On-Call Availability (weekend)	Critical support requests only.		Support will be provided based on availability of Technical Support Engineers across the globe.	
Service Management Tooling	MSP <i>should</i> use an industry standard Service Management Tool.		MSP <i>must</i> use an industry standard Service Management Tool.	
Language	Regardless of location, all Technical Support related conversations between the MSP and Mimecast will be conducted and documented in the English language.			

*Business hours are 8am – 6pm or as otherwise determined by the hosted region/data center for the end customer

The MSP will provide support to the Customer for all cases within their capability, with Mimecast Technical Support available as expert support for cases where the MSP does not have the privileges and/or access to resolve cases.

MSP is expected to handle customer cases within the scope of the definitions below. Mimecast may choose to review cases raised by MSPs to identify enablement opportunities, and reserves the right (in its sole discretion) to return cases to MSP if requisite pre-work is not completed.

Type	Description
<p>MSP Capabilities</p> <p>(Cases that MSPs should manage)</p>	<ul style="list-style-type: none"> Any matter which can be solved via the information available on Mimecast’s public knowledgebase, Mimecaster Central Policy configurations Platform configurations, such as creating Send Connectors Authentication within the customer’s environment Admin access requests Cases related to Customer environmental issues, including O365 tenant administration Question (How to?) cases Defined and reproducible use case for suspected defects End customer communications and management
<p>Mimecast Technical Support Capabilities</p> <p>(Cases where MSPs do not have the privileges and/or access needed to resolve)</p>	<ul style="list-style-type: none"> Critical Mimecast Platform incidents Mimecast Platform defects (resolution) Cases requiring Mimecast logs Content View Administrator role elevation requests Issues requiring Mimecast Engineering intervention Partner Portal Issues Login issues to the Mimecast Platform Issues unable to be solved due to incorrect Mimecast documentation

3 MIMICAST SUPPORT RESPONSE OBJECTIVES & ENGAGEMENT

The table below describes the options available to MSPs for raising cases and Mimecast’s response commitments. Mimecast will respond to Critical phone support requests by Certified Technical Contacts on a 24x7x365 days a year basis. It is expected that the MSP will have a Certified Technical Contact available for the duration for the Critical case. All Normal cases must be submitted via Customer Support Portal or Support Chat. Please see Section 4 below for Critical and Normal priority descriptions.

All other support requests will be dealt with in accordance with the level of support and within BUSINESS HOURS.

Support Option		Authorized	Premium	Elite	Sapphire
Support Portal		Available			
Critical Phone Support		Case Submissions Available 24/7/365			
Live Chat		Chatbot with auto case logging		Chatbot plus access to Support Engineer**	
Service Level Objectives	Critical (All Hours)	2 hours		2 hours	1 hour
	Normal (Business Hours)	12 hours		6 hours	3 hours
Remote Sessions		N/A		As Required	
# certified contacts able to log cases		5	10	20	Unlimited
N.B. Trials will be supported based on MSP Support level					

**Live chat is based on engineer availability. Availability may vary by product and region.

4 SUPPORT REQUEST PRIORITY

MSPs will investigate and assess the support request and assign a priority categorization as detailed below:

Priority	Description
Critical	<ul style="list-style-type: none"> • Business impacting • Suspected data loss • Critical mail delays / Mail flow outage • Unable to access Administration Console • Impairment of a Service function that lowers the security posture of a customer
Normal	<ul style="list-style-type: none"> • Impairment of a specified function that does NOT lower the security posture of a customer <ul style="list-style-type: none"> ○ E.g. search functionality • Non-business impacting issues <ul style="list-style-type: none"> ○ Low Urgency ○ Low Impact • Questions and Requests • Implementation-related questions

5 EXCLUSIONS

Mimecast shall be under no obligation to provide technical support due to improper installation or operation of the Services or use of the Services not in accordance with the Documentation or the instructions of Mimecast’s support team. In addition, Mimecast shall not be responsible for any performance delays or failure of the Services if the failures or delays are caused by: (a) equipment, software, systems, services, or data not provided by Mimecast, or (b) acts or omissions of MSP or Customer (including Permitted Users) that violate the terms of this document.

Support will not engage in customer setup and configuration of platform and services that requires further maintenance in the future, e.g. Smart host and Send Connectors, API Scripts and HTML Stationary.