Mimecast - Email Security Cloud Gateway - Data Centers & URLs

Considerations

- When a user enters their email address into Mimecast's Administration Console or an API client, a global resource determines the user's parent account location. This resource provides a 302 redirect to the correct location, ensuring uninterrupted service. These endpoints are available at all Mimecast data centers.
- Outbound HTTPS traffic from your network may be observed to an IP address outside your Mimecast region. To avoid disruption, allow outbound HTTPS connections to these locations. No email is transmitted using this method.
- Your region may be somewhere other than where you are physically located. It is where your data is located. For example, a company with European offices may host its data in North America.
- You must ensure that all connections are allowed access to the ports for the networks listed and mapped to the correct destination on your network.
- To prevent disruption to your service, it's important to ensure that:
  - You allow connections to the appropriate ports from your region's entire Mimecast IP Ranges.
  - They are mapped through to the correct destination on your network.

Global Application Resources

Global Application URL

Application	URL
Administration Console	https://login.mimecast.com
Mimecast Personal Portal	https://webmail.mimecast.com
Mimecast API	https://api.mimecast.com
Service Monitor	https://monitor.mimecast.com/Account/Login

Application	URL
Mimecast E2E, Customer Managed Migration	https://*.mimecast.com

Protocol Connection Ports

The following list shows the most common connection types and the general ports used for each protocol. Also included are the standard connection ports for Mimecast Applications:

Protocol	Default Port	Usage
Simple Mail Transfer Protocol (SMTP)	25	Send Connectors, SMTP Journaling, user application SMTP Services.
Post Office Protocol (POP3)	110	POP Journaling, user application POP Services.
Post Office Protocol Secure (POP3S)	995	
Lightweight Directory Access Protocol (LDAP)	389	Directory Synchronization
Lightweight Directory Access Protocol Secure (LDAPS)	636	
HyperText Transfer Protocol (HTTP)	80	Downloading Strip and Link attachments, Mimecast Synchronization Engine (MSE) with Office 365 hybrid environments. Mimecast for Outlook also authenticates using this port.
HyperText Transfer Protocol (HTTPS)	443	Access to the Administration Console, Mimecast Personal Portal, Mimecast Mobile, Mimecast for Outlook, and Mimecast Synchronization Engine, Mimecast E2E, Customer Managed Migration.

Mimecast Website

To ensure that your users can always log in to the Mimecast website, it is recommended to permit traffic to the Mimecast website IP ranges:

Location	IP Address	CIDR	Netmask
Data Center 1	146.101.202.134	/32	255.255.255.255
	146.101.202.135	/32	255.255.255.255
Data Center 2	81.145.134.178	/32	255.255.255.255

Location	IP Address	CIDR	Netmask
81.145.134.173	/32	255.255.255.255	

Regional IP Addresses, Network Ranges, and Application URLs

Europe (Excluding Germany)

IP Addresses and Network Ranges

Note:	When entering IP ranges, it is essential to note that Microsoft 365 limits the CIDR you can use on the Connection Filter (e.g., 205.139.110.0/23 or 185.58.84.0/22). We recommend breaking up the ranges so they end in/24 as a workaround.

Network	IP Address Range			Netmask
193.7.204.0/24	193.7.204.1	to	193.7.204.254	255.255.255.0
193.7.205.0/24	193.7.205.1	to	193.7.205.254	255.255.255.0
195.130.217.0/24	195.130.217.1	to	195.130.217.254	255.255.255.0
91.220.42.0/24	91.220.42.1	to	91.220.42.254	255.255.255.0
185.58.84.0/24	185.58.84.1	to	185.58.84.254	255.255.255.0
185.58.85.0/24	185.58.85.1	to	185.58.85.254	255.255.255.0
185.58.86.0/24	185.58.86.1	to	185.58.86.254	255.255.255.0
185.58.87.0/24	185.58.87.1	to	185.58.87.254	255.255.255.0
207.82.80.0/24	207.82.80.1	to	207.82.80.254	255.255.255.0

IP Addresses/Network Ranges for Non-SPF Email Traffic

Where messages are being sent from accounts with envelope addresses not registered as internal domains, Mimecast routes through separate ranges:

Region	IP Address Range 1	IP Address Range 2

Europe (excluding Germany)	185.58.87.40	to	185.58.87.49	185.58.84.40	to	185.58.84.49

Application URLs

Application	URL
Administration Console	https://login-uk.mimecast.com/u/login?gta=administration
Mimecast Personal Portal	https://webmail-uk.mimecast.com/m/portal/login/#/login
Mimecast API	https://eu-api.mimecast.com
Mimecast Secure Messaging Portal ***	https://login-uk.mimecast.com/m/secure

Note:	*** The Mimecast Secure Messaging Portal URL should only be used by Mimecast customers. Non-Mimecast customers can access the portal by clicking the link in the notification message.

Targeted Threat Protection (TTP)

Suppose you have integrations parsing messages for Mimecast-rewritten URLs or decoding Mimecast-rewritten URLs. In that case, these integrations must know Mimecast's Targeted Threat Protection URL patterns. Relevant integration types include SOAR, XDR, and custom scripts using the Get Message Part or Decode URL API endpoints.

Region	Destination Domain
Europe (excluding Germany)	url.uk.m.mimecastprotect.com

Germany

IP Addresses and Network Ranges

Note:	When entering IP ranges, it is essential to note that Microsoft 365 limits the CIDR you can use on the Connection Filter (e.g., 205.139.110.0/23 or 185.58.84.0/22). We recommend breaking up the ranges so they end in/24 as a workaround.

Network	IP Address Range			Netmask
194.104.108.0/24	194.104.108.1	to	194.104.108.254	255.255.255.0
194.104.109.0/24	194.104.109.1	to	194.104.109.254	255.255.255.0
194.104.110.0/24	194.104.110.1	to	194.104.110.254	255.255.255.0
194.104.111.0/24	194.104.111.1	to	194.104.111.254	255.255.255.0
147.28.34.0/24	147.28.34.1	to	147.28.34.254	255.255.255.0
147.28.35.0/24	147.28.35.1	to	147.28.35.254	255.255.255.0
51.163.158.0/24	51.163.158.1	to	51.163.158.254	255.255.255.0
51.163.159.0/24	51.163.159.1	to	51.163.159.254	255.255.255.0
62.140.7.0/24	62.140.7.1	to	62.140.7.254	255.255.255.0
62.140.10.0/24	62.140.10.1	to	62.140.10.254	255.255.255.0

IP Addresses/Network Ranges for Non-SPF Email Traffic

Where messages are being sent from accounts with envelope addresses not registered as internal domains, Mimecast routes through separate ranges:

Region	IP Address Range 1			IP Address Range 2		
Germany (DE-Grid)	51.163.159.40	to	51.163.159.49	62.140.10.40	to	62.140.10.49

Application URLs

Application	URL
Administration Console	https://login-de.mimecast.com/u/login?gta=administration
Mimecast Personal Portal	https://webmail-de.mimecast.com/m/portal/login/#/login
Mimecast API	https://de-api.mimecast.com
Mimecast Secure Messaging Portal ***	https://login-de.mimecast.com/m/secure

Note:	*** The Mimecast Secure Messaging Portal URL should only be used by Mimecast customers. Non-Mimecast customers can access the portal by clicking the link in the notification message.

Targeted Threat Protection (TTP)

Suppose you have integrations parsing messages for Mimecast-rewritten URLs or decoding Mimecast-rewritten URLs. In that case, these integrations must know Mimecast's Targeted Threat Protection URL patterns. Relevant integration types include SOAR, XDR, and custom scripts using the Get Message Part or Decode URL API endpoints.

Region	Destination Domain
Germany	url.de.m.mimecastprotect.com

United States of America

IP Addresses and Network Ranges

Note:	When entering IP ranges, it is essential to note that Microsoft 365 limits the CIDR you can use on the Connection Filter (e.g., 205.139.110.0/23 or 185.58.84.0/22). We recommend breaking up the ranges so they end in/24 as a workaround.

Network	IP Address Range			Netmask
170.10.132.0/24	170.10.132.1	to	170.10.132.254	255.255.255.0
170.10.133.0/24	170.10.133.1	to	170.10.133.254	255.255.255.0
170.10.128.0/24	170.10.128.1	to	170.10.128.254	255.255.255.0
170.10.129.0/24	170.10.129.1	to	170.10.129.254	255.255.255.0
170.10.130.0/24	170.10.130.1	to	170.10.130.254	255.255.255.0
170.10.131.0/24	170.10.131.1	to	170.10.131.254	255.255.255.0
207.211.31.0/25	207.211.31.1	to	207.211.31.127	255.255.255.128
207.211.30.0/24	207.211.30.1	to	207.211.30.254	255.255.255.0
205.139.110.0/24	205.139.110.1	to	205.139.110.254	255.255.255.0
205.139.111.0/24	205.139.111.1	to	205.139.111.254	255.255.255.0
216.205.24.0/24	216.205.24.1	to	216.205.24.254	255.255.255.0
63.128.21.0/24	63.128.21.1	to	63.128.21.254	255.255.255.0

IP Addresses / Network Ranges for Non-SPF Email Traffic

Where messages are being sent from accounts with envelope addresses not registered as internal domains, Mimecast routes through separate ranges.

Region						
United States of America (US-Grid)	207.211.30.40	to	207.211.30.49	205.139.111.40	to	205.139.111.49

Application URLs

Application	URL
Administration Console	https://login-us.mimecast.com/u/login?gta=administration
Mimecast Personal Portal	https://webmail-us.mimecast.com/m/portal/login/#/login
Mimecast API	https://us-api.mimecast.com
Mimecast Secure Messaging Portal ***	https://login-us.mimecast.com/m/secure

Note:	*** The Mimecast Secure Messaging Portal URL should only be used by Mimecast customers. Non-Mimecast customers can access the portal by clicking the link in the notification message.

Targeted Threat Protection (TTP)

Suppose you have integrations parsing messages for Mimecast-rewritten URLs or decoding Mimecast-rewritten URLs. In that case, these integrations must know Mimecast's Targeted Threat Protection URL patterns. Relevant integration types include SOAR, XDR, and custom scripts using the Get Message Part or Decode URL API endpoints.

Region	Destination Domain
United States of America (US-Grid)	url.us.m.mimecastprotect.com

United States of America (USB)

IP Addresses and Network Ranges

Note:	When entering IP ranges, it is essential to note that Microsoft 365 limits the CIDR you can use on the Connection Filter (e.g., 205.139.110.0/23 or 185.58.84.0/22). We recommend breaking up the ranges so they end in/24 as a workaround.

Network	IP Address Range			Netmask
170.10.150.0/24	170.10.150.1	to	170.10.150.254	255.255.255.0
170.10.151.0/24	170.10.151.1	to	170.10.151.254	255.255.255.0
170.10.152.0/24	170.10.152.1	to	170.10.152.254	255.255.255.0
170.10.153.0/24	170.10.153.1	to	170.10.153.254	255.255.255.0
170.10.154.0/24	170.10.154.1	to	170.10.154.254	255.255.255.0
170.10.155.0/24	170.10.155.1	to	170.10.155.254	255.255.255.0
170.10.156.0/24	170.10.156.1	to	170.10.156.254	255.255.255.0
170.10.157.0/24	170.10.157.1	to	170.10.157.254	255.255.255.0

IP Addresses / Network Ranges for Non-SPF Email Traffic

Where messages are being sent from accounts with envelope addresses not registered as internal domains, Mimecast routes through separate ranges.

Region	IP Address Range 1			IP Address Range 2		
United States of America (USB-Grid)	170.10.150.40	to	170.10.150.49	170.10.152.40	to	170.10.152.49

Application URLs

Field / Option	Description
Administration Console	https://login-usb.mimecast.com/u/login/?gta=apps#/login
Mimecast Personal Portal	https://webmail-usb.mimecast.com/m/portal/login/#/login
Mimecast API	https://usb-api.mimecast.com
Mimecast Secure Messaging Portal ***	https://login-usb.mimecast.com/m/secure

Note:	*** The Mimecast Secure Messaging Portal URL should only be used by Mimecast customers. Non-Mimecast customers can access the portal by clicking the link in the notification message.

Targeted Threat Protection (TTP)

Suppose you have integrations parsing messages for Mimecast-rewritten URLs or decoding Mimecast-rewritten URLs. In that case, these integrations must know Mimecast's Targeted Threat Protection URL patterns. Relevant integration types include SOAR, XDR, and custom scripts using the Get Message Part or Decode URL API endpoints.

Region	Destination Domain
United States of America (USB-Grid)	url.usb.m.mimecastprotect.com

Canada

IP Addresses and Network Ranges

Note:	When entering IP ranges, it is essential to note that Microsoft 365 limits the CIDR you can use on the Connection Filter (e.g., 205.139.110.0/23 or 185.58.84.0/22). We recommend breaking up the ranges so they end in/24 as a workaround.

Network	IP Address Range			Netmask
170.10.144.0/24	170.10.144.1	to	170.10.144.254	255.255.255.0
170.10.145.0/24	170.10.145.1	to	170.10.145.254	255.255.255.0
170.10.146.0/24	170.10.146.1	to	170.10.146.254	255.255.255.0
170.10.147.0/24	170.10.147.1	to	170.10.147.254	255.255.255.0
170.10.148.0/24	170.10.148.1	to	170.10.148.254	255.255.255.0
170.10.149.0/24	170.10.149.1	to	170.10.149.254	255.255.255.0
216.145.216.0/24	216.145.216.1	to	216.145.216.254	255.255.255.0

Application URLs

Application	URL
Administration Console	https://login-ca.mimecast.com/u/login?gta=administration
Mimecast Personal Portal	https://webmail-ca.mimecast.com/m/portal/login/#/login
Mimecast API	https://ca-api.mimecast.com
Mimecast Secure Messaging Portal ***	https://login-ca.mimecast.com/m/secure

Note:	*** The Mimecast Secure Messaging Portal URL should only be used by Mimecast customers. Non-Mimecast customers can access the portal by clicking the link in the notification message.

Targeted Threat Protection (TTP)

Suppose you have integrations parsing messages for Mimecast-rewritten URLs or decoding Mimecast-rewritten URLs. In that case, these integrations must know Mimecast's Targeted Threat Protection URL patterns. Relevant integration types include SOAR, XDR, and custom scripts using the Get Message Part or Decode URL API endpoints.

Region	Destination Domain
Canada (CA-Grid)	url.ca.m.mimecastprotect.com

South Africa

IP Addresses and Network Ranges

Network	IP Address Range			Netmask
41.74.192.0/24	41.74.192.1	to	41.74.192.254	255.255.255.0
41.74.193.0/24	41.74.193.1	to	41.74.193.254	255.255.255.0
41.74.194.0/24	41.74.194.1	to	41.74.194.254	255.255.255.0
41.74.195.0/24	41.74.195.1	to	41.74.195.254	255.255.255.0
41.74.196.0/24	41.74.196.1	to	41.74.196.254	255.255.255.0
41.74.197.0/24	41.74.197.1	to	41.74.197.254	255.255.255.0
41.74.198.0/24	41.74.198.1	to	41.74.198.254	255.255.255.0
41.74.199.0/24	41.74.199.1	to	41.74.199.254	255.255.255.0

Network	IP Address Range			Netmask
41.74.200.0/24	41.74.200.1	to	41.74.200.254	255.255.255.0
41.74.201.0/24	41.74.201.1	to	41.74.201.254	255.255.255.0
41.74.202.0/24	41.74.202.1	to	41.74.202.254	255.255.255.0
41.74.203.0/24	41.74.203.1	to	41.74.203.254	255.255.255.0
41.74.204.0/24	41.74.204.1	to	41.74.204.254	255.255.255.0
41.74.205.0/24	41.74.205.1	to	41.74.205.254	255.255.255.0
41.74.206.0/24	41.74.206.1	to	41.74.206.254	255.255.255.0
41.74.207.0/24	41.74.207.1	to	41.74.207.254	255.255.255.0

IP Addresses / Network Ranges for Non-SPF Email Traffic

Where messages are being sent from accounts with envelope addresses not registered as internal domains, Mimecast routes through separate ranges.

Region	IP Address Range 1			IP Address Range 2		
South Africa (ZA-Grid)	41.74.202.40	to	41.74.202.49	41.74.207.40	to	41.74.207.49

Application URLs

Application	URL
Administration Console	https://login-za.mimecast.com/u/login?gta=administration
Mimecast Personal Portal	https://webmail-za.mimecast.com/m/portal/login/#/login
Mimecast API	https://za-api.mimecast.com
Mimecast Secure Messaging Portal ***	https://login-za.mimecast.com/m/secure

Note:	*** The Mimecast Secure Messaging Portal URL should only be used by Mimecast customers. Non-Mimecast customers can access the portal by clicking the link in the notification message.

Targeted Threat Protection (TTP)

Suppose you have integrations parsing messages for Mimecast-rewritten URLs or decoding Mimecast-rewritten URLs. In that case, these integrations must know Mimecast's Targeted Threat Protection URL patterns. Relevant integration types include SOAR, XDR, and custom scripts using the Get Message Part or Decode URL API endpoints.

Region	Destination Domain
South Africa (ZA-Grid)	url.za.m.mimecastprotect.com

Australia

IP Addresses and Network Ranges

Note:	When entering IP ranges, it is essential to note that Microsoft 365 limits the CIDR you can use on the Connection Filter (e.g., 205.139.110.0/23 or 185.58.84.0/22). We recommend breaking up the ranges so they end in/24 as a workaround.

Network	IP Address Range			Netmask
103.96.20.0/24	103.96.20.1	to	103.96.20.254	255.255.255.0
103.96.21.0/24	103.96.21.1	to	103.96.21.254	255.255.255.0
103.96.22.0/24	103.96.22.1	to	103.96.22.254	255.255.255.0
103.96.23.0/24	103.96.23.1	to	103.96.23.254	255.255.255.0
170.10.134.0/24	170.10.134.1	to	170.10.134.254	255.255.255.0
170.10.135.0/24	170.10.135.1	to	170.10.135.254	255.255.255.0
103.13.69.0/24	103.13.69.1	to	103.13.69.254	255.255.255.0
124.47.150.0/24	124.47.150.1	to	124.47.150.254	255.255.255.0
124.47.189.0/24	124.47.189.1	to	124.47.189.254	255.255.255.0
180.189.28.0/24	180.189.28.1	to	180.189.28.254	255.255.255.0
216.145.217.0/24	216.145.217.1	to	216.145.217.254	255.255.255.0

IP Addresses/Network Ranges for Non-SPF Email Traffic

Where messages are being sent from accounts with envelope addresses not registered as internal domains, Mimecast routes through separate ranges.

Region	IP Address Range 1			IP Address Range 2		
Australia (AU-Grid)	103.96.20.40	to	103.96.20.49	103.96.22.40	to	103.96.22.49

Application URLs

Application	URL
Administration Console	https://login-au.mimecast.com/u/login?gta=administration
Mimecast Personal Portal	https://webmail-au.mimecast.com/m/portal/login/#/login
Mimecast API	https://au-api.mimecast.com
Mimecast Secure Messaging Portal ***	https://login-au.mimecast.com/m/secure

Note:	*** The Mimecast Secure Messaging Portal URL should only be used by Mimecast customers. Non-Mimecast customers can access the portal by clicking the link in the notification message.

Targeted Threat Protection (TTP)

Suppose you have integrations parsing messages for Mimecast-rewritten URLs or decoding Mimecast-rewritten URLs. In that case, these integrations must know Mimecast's Targeted Threat Protection URL patterns. Relevant integration types include SOAR, XDR, and custom scripts using the Get Message Part or Decode URL API endpoints.

Region	Destination Domain
Australia (AU-Grid)	url.au.m.mimecastprotect.com

Offshore

IP Addresses and Network Ranges

Note:	When entering IP ranges, it is essential to note that Microsoft 365 limits the CIDR you can use on the Connection Filter (e.g., 205.139.110.0/23 or 185.58.84.0/22). We recommend breaking up the ranges so they end in/24 as a workaround.

Network	IP Address Range			Netmask
193.7.206.0/24	193.7.206.1	to	193.7.207.254	255.255.255.0
193.7.207.0/24	193.7.207.1	to	193.7.207.254	255.255.255.0
147.28.32.0/24	147.28.32.1	to	147.28.32.254	255.255.255.0
147.28.33.0/24	147.28.33.1	to	147.28.33.254	255.255.255.0
213.167.75.0/24	213.167.75.1	to	213.167.75.254	255.255.255.0
213.167.81.0/24	213.167.81.1	to	213.167.81.254	255.255.255.0

IP Addresses/Network Ranges for Non-SPF Email Traffic

Where messages are being sent from accounts with envelope addresses not registered as internal domains, Mimecast routes through separate ranges:

Region	IP Address Range 1			IP Address Range 2		
Offshore	213.167.75.240	to	213.167.75.249	213.167.81.240	to	213.167.81.249

Application URLs

Application	URL
Administration Console	https://login-je.mimecast.com/u/login?gta=administration
Mimecast Personal Portal	https://webmail-je.mimecast.com/m/portal/login/#/login
Mimecast API	https://je-api.mimecast.com
Mimecast Secure Messaging Portal ***	https://login-je.mimecast.com/m/secure

Note:	*** The Mimecast Secure Messaging Portal URL should only be used by Mimecast customers. Non-Mimecast customers can access the portal by clicking the link in the notification message.

Targeted Threat Protection (TTP)

Suppose you have integrations parsing messages for Mimecast-rewritten URLs or decoding Mimecast-rewritten URLs. In that case, these integrations must know Mimecast's Targeted Threat Protection URL patterns. Relevant integration types include SOAR, XDR, and custom scripts using

the Get Message Part or Decode URL API endpoints.

Region	Destination Domain
Offshore	url.je.m.mimecastprotect.com

USPCOM

IP Addresses and Network Ranges

Note:	When entering IP ranges, it is essential to note that Microsoft 365 limits the CIDR you can use on the Connection Filter (e.g., 205.139.110.0/23 or 185.58.84.0/22). We recommend breaking up the ranges so they end in/24 as a workaround.

Network	IP Address Range			Netmask
170.10.138.0/24	170.10.138.1	to	170.10.138.254	255.255.255.0
170.10.139.0/24	170.10.139.1	to	170.10.139.254	255.255.255.0
170.10.140.0/24	170.10.140.1	to	170.10.140.254	255.255.255.0
170.10.158.0/24	170.10.158.1	to	170.10.158.254	255.255.255.0

Application URLs

Application	URL
Administration Console	https://login.mimecast-pscom-us.com
Mimecast Personal Portal	https://login.mimecast-pscom-us.com
Mimecast API	https://uspcom-api.mimecast-pscom-us.com
Mimecast Secure Messaging Portal ***	https://login.mimecast-pscom-us.com

Note:	*** The Mimecast Secure Messaging Portal URL should only be used by Mimecast customers. Non-Mimecast customers can access the portal by clicking the link in the notification message.

Mimecast URL Scanning Activity

> When monitoring IP addresses associated with clicked links in your environment, you may observe activity that does not originate from Mimecast-owned IP addresses or IP addresses listed on this page. As part of the Mimecast threat detection stack, the URL scanning layer can utilize various 3rd party vendors whose IP ranges are subject to change and are not tracked or disclosed by Mimecast. Furthermore, Mimecast employs anonymization techniques to prevent threat actors from recognizing and evading our scanners. To protect Mimecast customers, the associated IP addresses will not be disclosed.

Revision #3
Created 2024-11-11 19:01:34 UTC by Ryan
Updated 2025-02-12 01:11:41 UTC by Ryan