

Mimecast for IBM Resilient

Integrate security tools and processes, automate routine tasks and work smarter: Outpace and outmaneuver cyber-attacks and strengthen cyber resilience.

In an ever evolving, fast moving threat landscape, every organization is under threat. It's a landscape that has pitted security teams against cyber criminals in an escalating technology arms race. But the race to keep up with emerging threats has driven a proliferation of security solutions, which has left often under-resourced security teams struggling with a growing array of point products and independent static security controls with no orchestration between them.

The IBM Resilient Security Orchestration, Automation and Response (SOAR) platform helps organizations to accelerate incident response and remediation. They can quickly and easily integrate existing security and IT investments to ensure that security alerts are instantly actionable, gather valuable intelligence and incident context, and draw on Dynamic Playbooks to streamline responses to complex cyber threats.

But email remains the primary attack vector and the front line of incident detection, response and remediation – so integration is vital. Without it, organizations remain unable to realize the full benefit of SOAR investments, for instance, by efficiently updating protection at the gateway based on Indicators of Compromise (IoCs) identified elsewhere in the infrastructure.

Integrating Mimecast email security data and controls with IBM Resilient addresses this clear need. A simple click from the IBM Resilient platform gets you up and running in minutes via the pre-built API-based Add-On. It gives our joint customers the power to work smarter, respond faster and strengthen cyber resilience to improve ROI and make more efficient use of limited security resources.

Unlock the Value and Power of Your Security Tools. Integrate Them Into a Single Response Hub.

The Mimecast – IBM Resilient integration delivers a more complete SOAR platform. The Mimecast Actions Add-On offers 22 actions to help customers enrich SOC automation and broaden the scope of playbook-driven incident response and remediation. The Add-On enables organizations to complete key email security actions – from blocking a sender or URL and searching for specific messages – from a single interface, in minutes.

Key Benefits

- Easy integration adds Mimecast controls to the IBM Resilient platform in minutes
- Drive resource efficiency by ensuring security automation includes routine email security tasks.
- Work smarter by including email security controls and actions within Dynamic Playbooks.
- Reduce risk by making it easy to apply Mimecast email security actions across email, directory, journal, audit and Targeted Threat Protection.
- Increase Mimecast and IBM Resilient ROI by giving security teams access to a more complete SOAR platform.

Deep Integration: Available Actions

Run Tracked Messages Query: Rapidly search email tracking data according to specified parameters

Get Tracked Email: Get details about tracked email

Get Archived Messages List: 7-second email archive search to identify all emails with specified parameters

Get Archived Message Details: Get details about archived email

Block Sender: Prevent email delivery from known or specified malicious senders or domains

Permit Sender: Allow email receipt from trusted senders or domains

Create Blocked Sender Policy: Creates blocked sender policy

Get Blocked Sender Policy: Get details about specified policy or get a list of all policies

List URLs: Retrieve a list of all the currently managed URLs in the system

Block URL: Block user access to known or specified malicious URLs

Permit URL: Permit user access to trusted URLs

Delete URL: Remove URL from white/black listing

Decode URL: View an original URL where it has previously been listed as a masked URL

List Groups: Find and view a list of all groups

List Members: Find and view a list of specified group members

Add Group Member: Add a new member to a group

Remove Group Member: Removes a member from a group

Find Member: Checks does specified member exists in specified group

Create Group: Creates new group

Search File Hash: Searches for specified file hashes over the last year
















Test Connectivity: Checks is connection with Mimecast API enabled

Get Aliases: Lists all account aliases

Mimecast functions

| | | |
|---------------------------------------|---|----|
| Mimecast Add Member | Adds a member to Mimecast group. | 🗑️ |
| Mimecast Block Sender | Blocking a specific sender and recipient on Mimecast. | 🗑️ |
| Mimecast Blacklist URL | Blacklists URL on Mimecast. | 🗑️ |
| Mimecast Create Blocked Sender Policy | Creates blocked sender policy on Mimecast. | 🗑️ |
| Mimecast Create Group | Creates Mimecast group. | 🗑️ |
| Mimecast Create Incident | Create remediation incident. | 🗑️ |
| Mimecast Decode URL | Decodes encoded Mimecast URL. | 🗑️ |
| Mimecast Delete URL | Deletes managed URL on Mimecast. | 🗑️ |
| Mimecast Find Member | Search for a specific member of a Mimecast group. | 🗑️ |
| Mimecast Get Aliases | Returns Aliases of Mimecast account. | 🗑️ |
| Mimecast Get Archived Message Details | Returns message information about archived message. | 🗑️ |
| Mimecast Get Archived Messages List | Search archived Mimecast messages. | 🗑️ |
| Mimecast Get Blocked Sender Policy | Returns blocked sender policy. | 🗑️ |
| Mimecast Get Incident | Returns details about remediation incident. | 🗑️ |
| Mimecast Get Tracked Email | Returns message information about a tracked message. | 🗑️ |
| Mimecast List Groups | Returns list of Mimecast groups. | 🗑️ |
| Mimecast List Members | Returns members of specific Mimecast group. | 🗑️ |
| Mimecast List URLs | Returns a list of all Mimecast managed URLs. | 🗑️ |
| Mimecast Permit URL | Permit URL on Mimecast. | 🗑️ |
| Mimecast Remove Member | Removes a member from Mimecast group. | 🗑️ |
| Mimecast Run Tracked Messages Query | Search tracked Mimecast messages. | 🗑️ |
| Mimecast Search File Hash | Search account for specific file hashes over the last year. | 🗑️ |
| Mimecast Test Connectivity | Test connectivity with Mimecast API endpoints. | 🗑️ |
| Mimecast Permit Sender | Permitting a specific sender and recipient on Mimecast. | 🗑️ |

Mimecast Example Workflows

| | | | | |
|---|---|----------|--|---|
| Example: Mimecast Add Member Workflow | Adds a Note to Incident with message about adding specified member to Mimecast group. | Incident | Example: Mimecast Add Member |  |
| Example: Mimecast Block Sender Workflow | Adds a Note to Incident with message about blacklisting sender on Mimecast. | Incident | Example: Mimecast Blacklist Sender |  |
| Example: Mimecast Block URL Workflow | Adds a Note to Incident with message about blacklisting URL on Mimecast. | Incident | Example: Mimecast Blacklist URL |  |
| Example: Mimecast Create Blocked Sender Policy Workflow | Adds a Note to Incident with message about created Mimecast policy. | Incident | Example: Mimecast Create Blocked Sender Policy |  |
| Example: Mimecast Create Group Workflow | Adds a Note to Incident with message about creation of the Mimecast group. | Incident | Example: Mimecast Create Group |  |
| Example: Mimecast Create Incident Workflow | Adds a Note to Incident with message about created Mimecast incident. | Incident | Example: Mimecast Create Incident |  |
| Example: Mimecast Decode URL Workflow | Adds a Note to Incident with message about decoded URL on Mimecast. | Incident | Example: Mimecast Decode URL |  |
| Example: Mimecast Delete URL Workflow | This workflow adds a Note to incident containing message about deleted URL on Mimecast. | Artifact | Example: Mimecast Delete URL |  |
| Example: Mimecast Find Member Workflow | Adds a Note to Incident with message about existence of a member in specified Mimecast group. | Incident | Example: Mimecast Find Member |  |
| Example: Mimecast Get Aliases Workflow | Adds an Artifact to Incident containing all returned Mimecast aliases. | Incident | Example: Mimecast Get Aliases |  |
| Example: Mimecast Get Archived Message Details Workflow | Adds an Artifact to Incident containing details about specified Mimecast archived message. | Incident | Example: Mimecast Get Archived Message Details |  |
| Example: Mimecast Get Archived Messages List Workflow | Adds an Artifact to Incident containing list of all requested Mimecast archived messages. | Incident | Example: Mimecast Get Archived Messages List |  |
| Example: Mimecast Get Blocked Sender Policy Workflow | Adds an Artifact to Incident containing details about specified Mimecast policy. | Incident | Example: Mimecast Get Blocked Sender Policy |  |
| Example: Mimecast Get Incident Workflow | Adds an Artifact to Incident with details about specified Mimecast incident. | Incident | Example: Mimecast Get Incident |  |
| Example: Mimecast Get Tracked Email Workflow | Adds an Artifact on Incident containing details about specified tracked Mimecast | Incident | Example: Mimecast Get Tracked Email |  |

Complete User Guide Documentation will be provided after the certification process. It will contain screenshots of all functions and workflows together with explanations about input parameters and all other related details.