Create Incident

https://campus.barracuda.com/doc/95258427/

This functionality is available only with Barracuda Email Protection Premium and Premium Plus plans. To upgrade to one of these plans, contact your Barracuda Networks Sales Representative.

Creates an incident for a Microsoft 365 tenant.

Endpoint

POST /beta/accounts/{accountId}/forensics/{tenantId}/incident

Parameters

Name	Type	Required	Description
Path Parameters			
accountId	string	*	The Barracuda Cloud Control account ID obtained from the Get Accounts API.
tenantId	string	*	The Microsoft 365 tenant ID obtained from the Get Tenants API.

Request Body

Content type: *application/json*

Name	Description	Type

<table>
<tr><td>remediationActions</td><td>The remediation actions for an incident.
<table>
<tr><th>Entry</th><th>Description</th><th>Type</th></tr>
<tr><td>enableContinuousRemediation</td><td>Whether continuous remediation is enabled for this incident. Message action must be set to DELETE or NONE.</td><td>boolean</td></tr>
<tr><td>messageAction</td><td>The action taken on emails that match the incident search criteria. <i>Possible values</i> : NONE, DELETE, QUARANTINE</td><td>string</td></tr>
<tr><td>notify</td><td>Whether a warning email alert is sent to the affected users.</td><td>boolean</td></tr>
<tr><td>sendSummary</td><td>Whether an incident summary is sent to your security team for tracking purposes.</td><td>boolean</td></tr>
</table></td></tr>
<tr><td>searchCriteria</td><td>The email search criteria used to find emails that will become the basis of a new incident.
<table>
<tr><th>Entry</th><th>Description</th><th>Type</th></tr>
<tr><td>attachmentName</td><td>The email attachment name search query.</td><td>string</td></tr>
<tr><td>emailSubject</td><td>The email subject search query.</td><td>string</td></tr>
<tr><td>includeQuarantined</td><td>Whether the search should include quarantined emails.</td><td>boolean</td></tr>
<tr><td>includeSent</td><td>Whether the search should include sent emails.</td><td>boolean</td></tr>
<tr><td>sender</td><td colspan="2">The email sender search query.
<table>
<tr><th>Entry</th><th>Description</th><th>Type</th></tr>
<tr><td>displayName</td><td>The sender name search query.</td><td>string</td></tr>
<tr><td>email</td><td>The email address or domain name search query.</td><td>string</td></tr>
</table></td></tr>
<tr><td>timeframe</td><td>How far back the incident email search extends, in hours.
minimum: 1
maximum: 720</td><td>integer</td></tr>
</table></td></tr>
</table>

Response Codes

Code	Description
200	OK
401	Unauthorized: There is a missing or incorrect API token in header or the client did not have permission to access the requested resource.

Response

<table>
<tr><th>Entry</th><th>Description</th><th>Type</th></tr>
<tr><td>attachmentName</td><td>The email attachment name search query.</td><td>string</td></tr>
<tr><td>continuousRemediationCount</td><td>The number of emails for which remediation actions were taken via continuous remediation.</td><td>integer</td></tr>
<tr><td>continuousRemediationUntil</td><td>The date at which continuous remediation stops.</td><td>string</td></tr>
<tr><td>created</td><td>The date the incident was created.</td><td>string</td></tr>
<tr><td>createdBy</td><td>The email address of the administrator who created the incident.</td><td>string</td></tr>
<tr><td>createdByName</td><td>The name of the administrator who created the incident.</td><td>string</td></tr>
<tr><td>distinctRecipientCount</td><td>The number of users involved in this incident.</td><td>integer</td></tr>
<tr><td>domains</td><td>A list of affected domains.</td><td>Array</td></tr>
<tr><td>id</td><td>The incident ID.</td><td>string</td></tr>
<tr><td>incidentDetails</td><td colspan="2">Details about the origins of an incident.
<table>
<tr><th>Entry</th><th>Description</th><th>Type</th></tr>
<tr><td>source</td><td>The method by which the incident was created:
• Incident: Created by an administrator via the Incidents page.
• Potential-Incidents: Created by an administrator via the Potential Incidents Insights page.
• Insights-Automated: Created automatically via Automatic Remediation.
• Region: Created by an administrator via the Emails by Region Insights page.
• User-Reported: Created by an administrator via the User-Reported Emails page.
• ESS: Created via Barracuda Email Security Service.
• Sentinel: Created via Barracuda Sentinel.
• Public-Api: Created by an administrator via the public API.

<i>Possible values</i> : ESS, Incident, Insights-Automated, Potential-Incidents, Public-Api, Region, Sentinel, User-Reported</td><td>string</td></tr>
<tr><td>subSource</td><td>Extra information about the source of the incident.</td><td>string</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>labels</td><td>A list of objects representing labels that can be used to filter incidents.<table><tr><th>Entry</th><th>Description</th><th>Type</th></tr><tr><td>id</td><td>The unique ID of the label.</td><td>integer</td></tr><tr><td>name</td><td>The name of the label.</td><td>string</td></tr></table></td><td>Array</td></tr>
<tr><td>notifiedEmailCount</td><td>The number of warning email alerts sent to the affected users.</td><td>integer</td></tr>
<tr><td>remediatedEmailCount</td><td>The number of emails for which remediation actions were taken.</td><td>integer</td></tr>
<tr><td>remediationActions</td><td colspan="2">The remediation actions for an incident.<table><tr><th>Entry</th><th>Description</th><th>Type</th></tr><tr><td>enableContinuousRemediation</td><td>Whether continuous remediation is enabled for this incident. Message action must be set to DELETE or NONE.</td><td>boolean</td></tr><tr><td>messageAction</td><td>The action taken on emails that match the incident search criteria.
<i>Possible values</i> : NONE, DELETE, QUARANTINE</td><td>string</td></tr><tr><td>notify</td><td>Whether a warning email alert is sent to the affected users.</td><td>boolean</td></tr><tr><td>sendSummary</td><td>Whether an incident summary is sent to your security team for tracking purposes.</td><td>boolean</td></tr></table></td></tr>
<tr><td>remediationStatus</td><td>The current remediation status.
<i>Possible values</i> : Completed, In Progress, Not Started</td><td>string</td></tr>
<tr><td>sender</td><td colspan="2">The email sender search query.<table><tr><th>Entry</th><th>Description</th><th>Type</th></tr><tr><td>displayName</td><td>The sender name search query.</td><td>string</td></tr><tr><td>email</td><td>The email address or domain name search query.</td><td>string</td></tr></table></td></tr>
<tr><td>senderPolicies</td><td>A list of global sender policies added to your Barracuda Email Security Service account, if you have an account. The format is "{email|domain}:[quarantine|block]"
example: ["john@email.com:quarantine"]</td><td>Array</td></tr>
</table>

subject	The email subject search query.	string
timeframe	How far back the incident email search extends in hours.	integer

Sample Usage

```
curl -X POST
"https://api.barracudanetworks.com/beta/accounts/{accountId}/forensics/{tenantId}/incident" \
--header "Content-Type: application/json" \
--data-raw '{
    "searchCriteria": {
        "timeframe": 720,
        "emailSubject": "Example Subject",
        "sender": {
            "email": "",
            "displayName": ""
        },
        "attachmentName": "",
        "includeQuarantined": false,
        "includeSent": false
    },
    "remediationActions": {
        "messageAction": "DELETE",
        "notify": false,
        "sendSummary": true,
        "enableContinuousRemediation": false
    }
}' \
--header "Authorization: Bearer {access_token}"
```

Sample Response

```
{
    "id": "2047f505-ea48-4740-a370-a98611ea0c9f",
    "created": "2021-04-05T09:00:00.000000Z",
    "createdBy": "",
    "createdByName": "Public API",
    "sender": {
        "email": "",
        "displayName": ""
    },
    "subject": "Example Subject",
    "attachmentName": "",
    "timeframe": 720,
    "remediatedEmailCount": 0,
    "notifiedEmailCount": 0,
    "continuousRemediationCount": 0,
    "distinctRecipientCount": 0,
    "remediationStatus": "Not Started",
    "remediationActions": {
        "messageAction": "DELETE",
        "notify": false,
        "sendSummary": true,
        "enableContinuousRemediation": false
    },
    "senderPolicies": null,
    "domains": [
        "barracuda.com"
    ],
    "continuousRemediationUntil": null,
    "incidentDetails": {
        "source": "Public-Api",
        "subSource": null
    },
    "labels": []
}
```

Content type: *application/json*