Get Incidents

https://campus.barracuda.com/doc/95258434/

> 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.

Retrieves a list of created incidents for a Microsoft 365 tenant.

See Get Incident to retrieve a single incident using the incident ID.

Endpoint

GET /beta/accounts/{accountId}/forensics/{tenantId}/incidents

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.
Query Parameters			
labels	array[string]		The labels used to filter results.
page	integer		The current page to return. *Default value* : 0
size	integer		The number of results to return. *Default value* : 10

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>itemsTotal</td><td>The total number of items.</td><td>integer</td></tr>
<tr><td>pageNum</td><td>The current page number.</td><td>integer</td></tr>
<tr><td>pagesTotal</td><td>The total number of pages.</td><td>integer</td></tr>
<tr><td>results*</td><td>
<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>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.
Possible values : 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>
<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>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.
Possible values : 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.
Possible values : Completed, In Progress, Not Started</td><td>string</td></tr>
<tr><td>sender</td><td>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>
<tr><td>subject</td><td>The email subject search query.</td><td>string</td></tr>
<tr><td>timeframe</td><td>How far back the incident email search extends, in hours.</td><td>integer</td></tr>
</table></td></tr>
<tr><td>resultsCount</td><td>The number of items on the current page.</td><td>integer</td></tr>
</table>

Sample Request

```
curl -X GET
"https://api.barracudanetworks.com/beta/accounts/{accountId}/forensics/{tenan
tId}/incidents" \
--header "Authorization: Bearer {access_token}"
```

Sample Response


```
{
    "resultsCount": 1,
    "pageNum": 0,
    "itemsTotal": 1,
    "pagesTotal": 1,
    "results": [
        {
            "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": 1,
            "notifiedEmailCount": 0,
            "continuousRemediationCount": 0,
            "distinctRecipientCount": 1,
            "remediationStatus": "Completed",
            "remediationActions": {
                "messageAction": "DELETE",
                "notify": false,
                "sendSummary": true,
                "enableContinuousRemediation": false
            },
            "senderPolicies": [],
            "domains": [
                "barracuda.com"
            ],
```

```
            "continuousRemediationUntil": null,
            "incidentDetails": {
                "source": "Public-Api",
                "subSource": null
            },
            "labels": []
        }
    ]
}
```