

## Get Incident

<https://campus.barracuda.com/doc/95258436/>

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 single incident using the incident ID.

See [Get Incidents](#) to retrieve a list of incidents for a Microsoft 365 tenant.

### Endpoint

GET /beta/accounts/{accountId}/forensics/{tenantId}/incident/{incidentId}

### Parameters

Name	Type	Required	Description
<b>Path Parameters</b>			
accountId	string	*	The Barracuda Cloud Control account ID obtained from the <a href="#">Get Accounts</a> API.
incidentId	string	*	The incident ID obtained from the <a href="#">Create Incident</a> or <a href="#">Get Incidents</a> APIs.
tenantId	string	*	The Microsoft 365 tenant ID obtained from the <a href="#">Get Tenants</a> API.

### 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

Entry	Description	Type												
attachmentName	The email attachment name search query.	string												
continuousRemediationCount	The number of emails for which remediation actions were taken via continuous remediation.	integer												
continuousRemediationUntil	The date at which continuous remediation stops.	string												
created	The date the incident was created.	string												
createdBy	The email address of the administrator who created the incident.	string												
createdByName	The name of the administrator who created the incident.	string												
distinctRecipientCount	The number of users involved in this incident.	integer												
domains	A list of affected domains.	Array												
id	The incident ID.	string												
incidentDetails	Details about the origins of an incident.													
	<table><tr><th>Entry</th><th>Description</th><th>Type</th></tr><tr><td>source</td><td><div>The method by which the incident was created:<ul style="list-style-type: none"><li>Incident: Created by an administrator via the Incidents page.</li><li>Potential-Incidents: Created by an administrator via the Potential Incidents Insights page.</li><li>Insights-Automated: Created automatically via Automatic Remediation.</li><li>Region: Created by an administrator via the Emails by Region Insights page.</li><li>User-Reported: Created by an administrator via the User-Reported Emails page.</li><li>ESS: Created via Barracuda Email Security Service.</li><li>Sentinel: Created via Barracuda Sentinel.</li><li>Public-API: Created by an administrator via the public API.</li></ul></div><div>Possible values : ESS, Incident, Insights-Automated, Potential-Incidents, Public-API, Region, Sentinel, User-Reported</div></td><td>string</td></tr><tr><td>subSource</td><td>Extra information about the source of the incident.</td><td>string</td></tr><tr><td></td><td></td><td></td></tr></table>	Entry	Description	Type	source	<div>The method by which the incident was created:<ul style="list-style-type: none"><li>Incident: Created by an administrator via the Incidents page.</li><li>Potential-Incidents: Created by an administrator via the Potential Incidents Insights page.</li><li>Insights-Automated: Created automatically via Automatic Remediation.</li><li>Region: Created by an administrator via the Emails by Region Insights page.</li><li>User-Reported: Created by an administrator via the User-Reported Emails page.</li><li>ESS: Created via Barracuda Email Security Service.</li><li>Sentinel: Created via Barracuda Sentinel.</li><li>Public-API: Created by an administrator via the public API.</li></ul></div> <div>Possible values : ESS, Incident, Insights-Automated, Potential-Incidents, Public-API, Region, Sentinel, User-Reported</div>	string	subSource	Extra information about the source of the incident.	string				
	Entry	Description	Type											
	source	<div>The method by which the incident was created:<ul style="list-style-type: none"><li>Incident: Created by an administrator via the Incidents page.</li><li>Potential-Incidents: Created by an administrator via the Potential Incidents Insights page.</li><li>Insights-Automated: Created automatically via Automatic Remediation.</li><li>Region: Created by an administrator via the Emails by Region Insights page.</li><li>User-Reported: Created by an administrator via the User-Reported Emails page.</li><li>ESS: Created via Barracuda Email Security Service.</li><li>Sentinel: Created via Barracuda Sentinel.</li><li>Public-API: Created by an administrator via the public API.</li></ul></div> <div>Possible values : ESS, Incident, Insights-Automated, Potential-Incidents, Public-API, Region, Sentinel, User-Reported</div>	string											
subSource	Extra information about the source of the incident.	string												

labels	<p>A list of objects representing labels that can be used to filter incidents.</p> <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>	Entry	Description	Type	id	The unique ID of the label.	integer	name	The name of the label.	string	Array						
Entry	Description	Type															
id	The unique ID of the label.	integer															
name	The name of the label.	string															
notifiedEmailCount	The number of warning email alerts sent to the affected users.	integer															
remediatedEmailCount	The number of emails for which remediation actions were taken.	integer															
remediationActions	<p>The remediation actions for an incident.</p> <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>	Entry	Description	Type	enableContinuousRemediation	Whether continuous remediation is enabled for this incident. Message action must be set to DELETE or NONE.	boolean	messageAction	The action taken on emails that match the incident search criteria. <i>Possible values</i> : NONE, DELETE, QUARANTINE	string	notify	Whether a warning email alert is sent to the affected users.	boolean	sendSummary	Whether an incident summary is sent to your security team for tracking purposes.	boolean	
Entry	Description	Type															
enableContinuousRemediation	Whether continuous remediation is enabled for this incident. Message action must be set to DELETE or NONE.	boolean															
messageAction	The action taken on emails that match the incident search criteria. <i>Possible values</i> : NONE, DELETE, QUARANTINE	string															
notify	Whether a warning email alert is sent to the affected users.	boolean															
sendSummary	Whether an incident summary is sent to your security team for tracking purposes.	boolean															
remediationStatus	<p>The current remediation status. <i>Possible values</i> : Completed, In Progress, Not Started</p>	string															
sender	<p>The email sender search query.</p> <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>	Entry	Description	Type	displayName	The sender name search query.	string	email	The email address or domain name search query.	string							
Entry	Description	Type															
displayName	The sender name search query.	string															
email	The email address or domain name search query.	string															
senderPolicies	<p>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" ]</p>	Array															

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

## Sample Request

```
curl -X GET
"https://api.barracudanetworks.com/beta/accounts/{accountId}/forensics/{tenantId}/incident/{incidentId}" \
--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": 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": []  
}
```

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.