Tenable.io API Best Practices Guide

Last Revised: January 30, 2019

Table of Contents

Welcome to Tenable.io API Best Practices

The REST API for Tenable.io allows you to integrate Tenable.io with other standalone or web applications by scripting interactions with the Tenable.io server.

This document describes recommended approaches to common tasks using the Tenable.io API. For descriptions of all available endpoints for the Tenable.io API, see the Tenable.io API reference guide.

This documentation describes tasks you can perform in the following areas:

- Assets
- Vulnerabilities

> **Note:** This documentation provides examples in JavaScript Object Notation (JSON). For examples in Python, Tenable recommends the pyTenable library or the Tenable.io SDK.

Authorization

Tenable.io generates a unique set of API keys for each user account. These keys allow your application to authenticate to the Tenable.io API without creating a session.

To authorize your application to use the Tenable.io API, you must include the **X-ApiKeys** header element in your HTTP request messages.

X-ApiKeys Header Element

The **X-ApiKeys** header element has the following format:

```
X-ApiKeys: accessKey={accessKey}; secretKey={secretKey};
```

The *accessKey* and *secretKey* parameters correspond to the API keys that Tenable.io generates for each system user. For more information, see Generate an API Key in the *Tenable.io Vulnerability Management User Guide*.

Example

```
curl -H "X-ApiKeys:
accessKey=2c935f507d0686382bb383e4daf92eef8b4a349b9b9de2bf85343c0f7e7265d-
b;
secretKey=0553ac5757e8e741d6ef034dc06618106e7855887428e662adcde8862d017cf-
9" https://cloud.tenable.com/scans
```

Permissions

Tenable.io uses the following permissions types:

- User
- Scan
- Policy
- Scanner
- Agent
- Target Group (System)
- Target Group (User)

User Roles

Tip: To determine user permissions for the current user, see Determine Current User Permissions.

Name	Value	Description
Basic	16	Users with this role can view and configure scan results.
Standard	32	Users with this role can create scans, policies, and user target groups.
Administrator	64	Users with this role have the same privileges as the standard user but can also manage users, groups, agents, exclusions, system target groups, user target groups, access groups, and scanners.

Scan Roles

Name	Value	Description
No Access	0	Users assigned this permission for a scan cannot view, control, or configure the scan. As a result, the scan does not appear for the user in the Tenable.io user interface, and the user cannot access the scan using the scans API.
Can View	16	Users assigned this permission can view the results of the scan. As a result,

		the scan appears for the user in the Tenable.io user interface, and the user can access the scan using the scans API.
Can Control	32	Users assigned this permission can launch, pause, and stop a scan, in addition to performing any tasks allowed by Can View.
Can Configure	64	Users assigned this permission can modify any setting for the scan except scan ownership, in addition to performing any tasks allowed by Can Control.
Owner	128	The user assigned this permission owns the scan. The owner can modify any setting for the scan, including scan ownership.

Policy Roles

Name	Value	Description
No Access	0	Users assigned this permission cannot view or use the policy. As a result, this policy does not appear for the user in the Tenable.io user interface, and the user cannot access the policy using the policies API.
Can Use	16	Users assigned this permission can view the policy and use it to create scans.
Can Edit	32	Users assigned this permission can modify any setting for the policy except permissions, in addition to performing any tasks allowed by Can Use.
Can Configure	64	Users assigned this permission can modify any setting for the policy except policy ownership, in addition to performing any tasks allowed by Can Edit.

Scanner Roles

Name	Value	Description
No Access	0	Users assigned this permission cannot use the scanner. As a result, this scanner does not appear for the user in the Tenable.io user interface, and the user cannot access the scanner using the scanners API.
Can Use	16	Users assigned this permission can use the scanner.
Can	64	Users assigned this permission can manage the scanner.

Manage		

Agent Roles

Name	Value	Description
No Access	0	Users assigned this permission cannot use the agent group in agent scans. As a result, this agent group does not appear for the user in the Tenable.io user interface, and the user cannot access the agent group using the agent-groups API.
Can Use	16	Users assigned this permission can use the agent group in agent scans.

Target Group (System Roles)

Note: System target groups allow you to control which hosts a user can scan. By default, all users can scan all hosts. You can restrict this by removing scan permissions on the default target group and creating additional target groups with more granular permissions.

Name	Value	Description
No Access	0	Users assigned this permission cannot scan hosts in the system target group or use hosts in the system target group to filter dashboards.
Can Use	32	Users assigned this permission can use hosts in the system target group to filter dashboards.
Can Scan	64	Users assigned this permission can scan hosts in the system target group.

Target Group (User Roles)

Note: User target groups do not grant scan permissions. Instead, user target groups provide more granular filtering on the hosts permitted to you in system target groups. You can use these lists when filtering dashboards or configuring scans.

Name	Value	Description
No	0	Users assigned this permission cannot configure scans for hosts in the user

Access		target group or use hosts in the user target group to filter dashboards.
Can Use	32	Users assigned this permission can use hosts in the user target groups to filter dashboards and configure scans.
Can Change	64	Users assigned this permission can modify the user target group.

Determine Current User Permissions

User Permissions: Basic (16)

To determine the permissions for your user account, use the API endpoint described below.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/session
```

Request Path Parameters

None.

Request Path Example

See "Request Path Syntax."

Request Body Syntax

None.

HTTP Response

Response Codes

Status	Description
200	Returns data for the current session. For more information, see "Response Body Syntax."
403	Returned if you do not have permission to view the session data.

429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "id": {integer},
  "uuid": {string},
  "uuid_id": {string},
  "username": {string},
  "user_name": {string},
  "email": {string},
  "name": {string},
  "type": {string},
  "permissions": {integer},
  "enabled": {boolean},
  "last_login_attempt": {integer},
  "login_fail_count": {integer},
  "login_fail_total": {integer},
  "container_id": {integer},
  "container_uuid": {string},
  "container_name": {string},
  "features": [
    {feature_name}: {boolean}
  ],
  "apps":{array},
  "group_uuids":{array},
  "groups":{array},
  "lastlogin": {integer}
}
```

Response Body Attributes

Attribute	Type	Description
id	integer	The ID of the user account.
uuid	string	The UUID of the user account.
uuid_id	string	The UUID of the user account.
username	string	The username.
user_name	string	The username.
email	string	The email account of the user.
name	string	The name of the user.
type	string	The authentication type for the user account. For example, `local` indicates that the user account authenticates directly in Tenable.io.
permissions	integer	The user permissions assigned to this user account.
enabled	boolean	A value indicating whether the user account is enabled or disabled.
last_login_attempt	integer	The date and time in Unix format when the user account credentials were last used in a failed login attempt.
login_fail_count	integer	The number of failed login attempts for this user account in the last 24 hours.
login_fail_total	integer	The total number of failed login attempts for this user account.
container_id	integer	The ID of the Tenable.io instance where the user has been granted access.
container_uuid	string	The UUID of the Tenable.io instance where the user has been granted access.
container_name	string	The human readable name of the Tenable.io instance where the user has been granted access.
features	array	An array of boolean values representing specific features enabled for the Tenable.io instance.
apps	array	The applications licensed for the Tenable.io instance where the user has been granted access.

group_uuids	array	An array of UUIDs of the user groups to which the user belongs. The items in this array are strings.
groups	array	An array of human readable names of the user groups to which the user belongs. The items in this array are strings.
lastlogin	integer	The date and time in Unix format when the user account credentials were last used to successfully log in.

Response Body Example


```
{
  "id":2,
  "uuid":"fb76f456-9a6f-4f63-8553-1cee234eb777",
  "uuid_id":"fa76e456-9a6f-4f63-8553-1ced233eb777",
  "username":"user2@example.com",
  "user_name":"user2@example.com",
  "email":"user2@example.org",
  "name":"Sample User",
  "type":"local",
  "permissions":64,
  "enabled":true,
  "last_login_attempt":1540942030719,
  "login_fail_count":0,
  "login_fail_total":14,
  "container_id":766315,
  "container_uuid":"3bc442f4-0cd1-4de0-95a3-3d8e587931ff",
  "container_name":"demo",
  "features":{
    "access_groups":true,
    "access_groups_migration":true,
    "advanced_search_v2":true,
    "agent_triage_m2":true,
    "agent_updates":true,
```

```
    "analytics":true,
    "analytics_v2":true,
    "asset_deleting_ui":true,
    "asset_management":true,
    "audits_workbench":false,
    "aws_connector_v1":true,
    "cfl_core_ssor":true,
    "connectors_gen2":false,
    "container_security":true,
    "container_security_gen2":true,
    "container_security_gen2_runtime":true,
    "credentials_mgmt":true,
    "credentials_mgmt_v2":true,
    "dashboards_gen2":false,
    "dashboards_gen2_blank_canvas":false,
    "dashboards_gen2_export":false,
    "dashboards_gen2_export_png":false,
    "dashboards_gen2_lumin_enabled":false,
    "dashboards_gen2_schedule":false,
    "dashboards_gen2_tag_filter":false,
    "dashboards_gen2_widget_filters":false,
    "dashboards_gen2_widget_library":false,
    "dynamic_tagging":true,
    "environment_management":true,
    "export_dashboard":true,
    "export_dashboard_pdf":true,
    "general_data_protection_compliance":true,
    "import_data":false,
    "indexing_v2":true,
    "lumin_beta_allowed":true,
    "lumin_beta_enabled":true,
    "modify_vulnerability":false,
    "pci_multiscan":true,
```

```
    "qualys_connector":true,
    "qualys_vuln_connector":true,
    "rbac":true,
    "recast_rules":true,
    "reporting":true,
    "scan_service":true,
    "scans_gen2":true,
    "state":true,
    "suggest_feature":true,
    "system":false,
    "tagging":true,
    "vm_service_query":true,
    "vulnerability_management_gen2":true,
    "was_discovery":true,
    "was_multi_scanning":true,
    "was_plugin_selection":true,
    "was_scan_progress":true,
    "webapp_scanning":true,
    "webapp_scanning_gen2":true
  },
  "apps":{
    "consec": "standard",
    "was": "standard"
  },
  "group_uuids": [
    "f764340b-0165-45d2-a574-36af488cbdd2"
  ],
  "groups": [
    {
      "uuid": "f764340b-0165-45d2-a574-36af488cbee5",
      "name": "Columbia office",
      "permissions": 0,
      "container_uuid": "8f9d0b84-ede2-4954-a0c9-0bde292ac36f",
```

```
      "id": 1
    }
  ],
  "lastlogin":1543864186682
}
```

Reference Guide

https://cloud.tenable.com/api#/resources/session/get

Date Formats

Time and date formats in Tenable.io API messages can be in the following formats:

- Abbreviated Timestamp
- Standard Timestamp
- Unix Timestamp

Abbreviated Timestamp

The abbreviated timestamp is formatted as follows:

```
YYYYMMDDTHHMMSS
```

This format consists of the following elements:

Element	Description	# of Digits	Example
YYYY	Year	4	2018
MM	Month	2	05
DD	Day	2	09
T	Placeholder between date and time	--	T
HH	Hour in military time	2	16
MM	Minute	2	00
SS	Second	2	00

Example

```
20181017T130000
```

Standard Timestamp

The standard timestamp follows the ISO-8601 standard.

The standard timestamp contains all the elements of the abbreviated timestamp, but contains additional punctuation for human readability and includes a timezone element, as follows:

```
YYYY-MM-DDTHH:MM:SS.mssZ
```

This format consists of the following elements:

Element	Description	# of Digits	Example
YYYY	Year	4	2018
MM	Month	2	05
DD	Day	2	09
T	Placeholder between date and time	--	T
HH	Hour in military time	2	16
MM	Minute	2	00
SS	Second	2	00
mss	Milliseconds	3	535
Z	Code indicating that the timestamp uses Coordinated Universal Time (UTC), also known as Zulu time	1	Z

Example

```
2017-12-14T20:40:44.535Z
```

Unix Timestamp

The single signed number that represents the date and time in Unix time.

Example

```
1540944000
```

Rate Limiting

Tenable.io performs rate limiting on API requests to ensure that all customers experience the same level of service. Based on current processing load, Tenable.io calculates the number of API requests it can accept from a single user per minute. Individual users are identified by the API key used in each API request. An individual user can have only one valid API key at a time.

If you submit an API request after the processing limit is reached, Tenable.io returns an HTTP response message with a `429 (Too Many Requests)` status code. The response also includes a `retry-after` header element that specifies the number of seconds to wait before retrying.

Example Response Header

```
connection:keep-alive
content-length:580
content-type:text/html
date:Wed, 24 Oct 2018 17:13:43 GMT
retry-after:30
server:tenable.io
strict-transport-security:max-age=63072000; includeSubDomains
x-content-type-options:nosniff
x-gateway-site-id:nginx-router-b-eng-us-east-1.dcld
x-path-handler:tenable-io-plugins-plugin
```

Examples

- Handling 429 messages with pyTenable module
- Handling 429 messages without pyTenable module
- Retry logic (does not use `retry-after` header element)

Recommendations to Avoid Rate Limits

- Use the exports endpoints to retrieve data from Tenable.io. While Tenable.io supports the

workbenches export endpoints, Tenable recommends using the optimized exports endpoints instead.

- Do not multi-thread your requests. As long as you are using the appropriate APIs, you should be able to export data from Tenable.io without reaching rate limits.
- If your process regularly reaches the API request rate limit, review your code to ensure that you are not co-processing requests.
- *Always* use a unique user account for each API integration you enable or create. This approach ensures proper tracking of who is accessing which data and allows Tenable.io to enforce rate limits for each API user.

Test API Requests in the Tenable.io Reference Guide

The *Tenable.io API Reference Guide* allows you to test API requests against your organization's Tenable.io instance.

To test API requests in the API reference guide:

1. In your browser, log in to Tenable.io.

   > **Tip:** Make sure to log in using an account with permissions appropriate to the endpoints you want to test.

2. In the same browser, view the page for an endpoint you want to test in the API Reference Guide.

   For example, you might want to test the API request that allows you to view the list of Tenable.io users associated with your organization.

   > **Note:** This interactive testing requires that you open the reference guide in the same browser as you opened Tenable.io.

3. Scroll down to the **Test** section at the bottom of the reference page.

   If the request for the endpoint supports parameters, the **Test** section contains text boxes or drop-down boxes for each parameter as appropriate.

4. As needed, enter or select parameters for the request.

5. Click **Send**.

   The response message for the request appears.

6. (Optional) Click **Reset** to clear the parameters you entered and any response messages received.

Assets

You can use the Tenable.io API to perform the following tasks:

- Add Asset Data to Tenable.io
- List Assets
- View Asset Details
- Retrieve Asset Data from Tenable.io
- Generate the Asset Export File
- Query for Asset Export Status and Chunk ID Information
- Download Asset Export Chunks
- Retrieve Agent Data for an Asset
- Manage Asset Tags

Add Asset Data to Tenable.io

User Permissions: Standard (32)

Scan Permissions: Can Configure (64)

You can use the Tenable.io API to import a list of assets in JSON format.

To add asset data to Tenable.io, use the API endpoint described below.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Caution: The request size cannot exceed 5 MB. For example, if the average asset record you want to import is about 2 KB, you can import approximately 2,500 assets in a single request.

Request Path Syntax

```
POST https://cloud.tenable.com/import/assets
```

Request Path Parameters

None.

Request Path Example

See "Request Path Syntax."

Request Body Syntax

```
{
  "assets": [
    {asset object},
    {asset object},
```

```
    {asset object}
  ],
  "source": {string}
}
```

Request Body Attributes

Attribute	Type	Description	Required?
assets	array	An array of asset objects to import.	yes
source	string	A user-defined name for the source of the asset records you want to import.	yes

Request Body Example

```
{
  "assets": [
    {
      "ipv4": [
        {
          "172.204.81.57",
          "172.82.157.177"
        }
      ],
      "operating_system": [
        {
          "Linux Kernel 2.6.32-71.el6.i686 on Red Hat Enterprise Linux
Server release 6.0 (Santiago)"
        }
      ],
      "ssh_fingerprint": "423fa07b4a12f386149e09ea10021a89",
      "bios_uuid": "423ee0f1-0032-700c-afd7-a686d88da63e"
  ],
```

```
  "source": local_scan
}
```

HTTP Response

Response Codes

Status	Description
200	Returns the import job UUID. For more information, see "Response Body Syntax."
400	Returned if you submitted a bad request.
403	Returned if you do not have permission to import assets.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "asset_import_job_uuid": {string}
}
```

Response Body Attributes

Attribute	Type	Description
asset_import_job_uuid	string	The unique identifier for the import job. Use this value to query the status of the asset import job.

Response Body Example

```
{
  "asset_import_job_uuid": "c25af9c0-8327-4af6-b9e5-d39b7f190e9b"
}
```

Reference Guide

https://cloud.tenable.com/api#/resources/assets/import

Examples

- asset import (library)
- asset import (SDK)

List Asset Import Jobs

User Permissions: Standard (32)

Scan Permissions: Can Configure (64)

To list asset import jobs, use the API endpoint described below.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/import/asset-jobs
```

Request Path Parameters

None.

Request Path Example

See "Request Path Syntax."

HTTP Response

Response Codes

Status	Description
200	Returns a list of asset import jobs. For more information, see "Response Body Syntax."
403	Returned if the user does not have permission to list asset import jobs.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "asset_import_job_uuid": {string}
}
```

Response Body Attributes

Attribute	Type	Description
asset_import_job_uuid	string	The unique identifier for the import job.

Response Body Example

```
{
  "asset_import_job_uuid": "c25af9c0-8327-4af6-b9e5-d39b7f190e9b"
}
```

Reference Guide

https://cloud.tenable.com/api#/resources/assets/import

Examples

- asset import (library)
- asset import (SDK)

Retrieve Asset Data from Tenable.io

User Permissions: Administrator (64)

The asset export APIs provide the ability to retrieve all assets and related metadata from Tenable.io for integration into third-party systems. With these APIs, you can perform a large initial synchronization of Tenable.io with a third-party system. You can then retrieve differentials to update on a regular basis. For example, you can use the asset export APIs to retrieve all known assets, then use the data to create and regularly update your configuration management database (CMDB).

The Tenable.io API exports asset data in data chunks. You can configure chunk size to maximize network performance and satisfy data ingestion requirements for third-party applications.

To retrieve asset data using the Tenable.io API, Tenable recommends the following approach:

1. Generate the export file.
2. Query for the export generation status and chunk identification information.
3. Download completed export chunks.
4. Retrieve agent data related to the assets.

   Note: Asset data is only relevant if the **has_agent** parameter is set to `true` for assets in the export chunk.

Generate the Asset Export File

User Permissions: Administrator (64)

To generate the export file, use the API endpoint described below.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
POST https://cloud.tenable.com/assets/export
```

Request Path Parameters

None.

Request Path Example

See "Request Path Syntax."

Request Body Syntax

```
{
  "chunk_size": {integer},
  "filters": {
    "created_at": {long},
    "updated_at": {long},
    "terminated_at": {long},
    "deleted_at": {long},
    "first_scan_time": {long},
    "last_authenticated_scan_time": {long},
    "last_assessed": {long},
```

```
    "servicenow_sysid": {boolean},
    "sources": {array},
    "has_plugin_results": {boolean}
    "tag.category": {array}
  }
}
```

Request Body Attributes

Note: To return all assets, omit the `filters` parameter. For most deployments, Tenable does not recommend that you omit the `filters` parameter.

Note: If your request specifies multiple filters, the system combines the filters using the AND search operator.

Parameter	Child Parameter	Type	Value	Required?
chunk_size	--	integer	Specifies the number of assets per exported chunk. Range is 100-10000. If you specify a value outside of that range, a 400 error is returned.	required
filters	created_at	long	Returns all assets created later than the date specified. The specified date must be in the Unix timestamp format.	optional
	updated_at	long	Returns all assets updated later than the date specified. The specified date must be in the Unix timestamp format.	optional
	terminated_at	long	Returns all assets terminated later than the date specified. The specified date must be in the Unix timestamp format.	optional
	deleted_at	long	Returns all assets deleted later than the date specified. The specified date must in the Unix timestamp format.	optional

	first_scan_time	long	Returns all assets with a first scan time later than the date specified. The specified date must be in the Unix timestamp format.	optional
	last_authenticated_scan_time	long	Returns all assets with a last credentialed scan time later than the date specified. The specified date must be in the Unix timestamp format.	optional
	last_assessed	long	Returns all assets with a last assessed time later than the date specified. An asset is considered assessed if it has been scanned by a credentialed or non-credentialed scan. The specified date must be in the Unix timestamp format.	optional
	servicenow_sysid	boolean	If `true`, returns all assets that have a ServiceNow Sys ID, regardless of value. If `false`, returns all assets that do not have a ServiceNow Sys ID.	optional
	sources	array	Returns assets that have the specified source. An asset source is the entity that reported the asset details. Sources can include sensors, connectors, and API imports. If your request specifies multiple sources, this request returns all assets that have been seen by any of the specified sources. The items in the sources array must be strings and must correspond to the names of the sources as defined in your organization's implementation of Tenable.io. Commonly used names include:	optional

			• AWS—You obtained the asset data from an Amazon Web Services connector. • NESSUS_AGENT—You obtained the asset data obtained from a Nessus agent scan. • PVS—You obtained the asset data from a Nessus Network Monitor (NNM) scan. • NESSUS_SCAN—You obtained the asset data from a Nessus scan. • WAS—You obtained the asset data from a Tenable.io Web Application Scanning scan. If your request specifies multiple sources, this request returns all assets that have been seen by any of the specified sources.	
	has_plugin_results	boolean	If `true`, returns all assets that have plugin results. If 'false', returns all assets that do not have plugin results. An asset may not have plugin results if the asset details originated from a connector, an API import, or a discovery scan, rather than a vulnerabilities scan.	optional
	tag.*category*	array	Returns all assets with the specified tags. The filter is defined as the word "tag", a period ("."), and the tag category name. The value of the filter is an array of tag values. For more information about tags, see Manage Asset Tags.	optional

Request Body Example

```
{
  "chunk_size": 100,
  "filters": {
    "servicenow_sysid": false,
    "created_at": 1525781704,
    "sources": [
      "NESSUS_SCAN"
    ],
    "tag.Location": [
      "Chicago",
      "Austin"
       ]
  }
}
```

HTTP Response

Response Codes

Status	Description
200	Returned if Tenable.io successfully queues the export request. For more information, see "Response Body Syntax."
400	Returned if any of the filters in the request is invalid.
403	Returned if you do not have permission to export asset data.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "export_uuid": {string}
}
```

Response Body Attributes

Attribute	Type	Description
export_uuid	string	The unique identifier of the export request.

Response Body Example

```
{
  "export_uuid": "a483adf8-24e3-4c7f-818a-6867b02310dd"
}
```

Reference Guide

https://cloud.tenable.com/api#/resources/exports/assets-request-export

Examples

- exports (library)
- exports (SDK)

Query for Asset Export Status and Chunk ID Information

User Permissions: Administrator (64)

Note: When generating the asset export, Tenable.io processes the chunks in parallel, so the chunks may not complete in order.

To query for the status of the export and chunk identification information, use the API endpoint described below.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/assets/export/{export_uuid}/status
```

Request Path Parameters

Attribute	Type	Description	Required?
export_uuid	string	The unique identifier of an export request. This value corresponds to the value returned in the assets export response message.	required

Request Path Example

```
GET https://cloud.tenable.com/assets/export/a483adf8-24e3-4c7f-818a-6867b02310dd/status
```

Request Body Syntax

None.

HTTP Response

Response Codes

Status	Description
200	Returned if Tenable.io successfully retrieves the export status. For more information, see "Response Body Syntax."
403	Returned if you do not have permission to view the export status.
404	Returned if Tenable.io cannot identify an export with the UUID specified in the request.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "status": {string},
  "chunks_available": [
    {integer},
    {integer}...]
}
```

Response Body Attributes

Attribute	Type	Description
status	string	The status of the export request. Possible values include: • QUEUED— Tenable.io has queued the export request until it completes other requests currently in process. • PROCESSING—Tenable.io has started processing the export request. • FINISHED—Tenable.io has completed processing the export request. The list of chunks is complete.

		• ERROR—Tenable.io encountered an error while processing the export request. **Tip:** If you encounter an ERROR status, Tenable recommends that you retry the request. If the status persists on retry, contact Support.
chunks_available	array	A comma-separated list of completed chunks available for download.

Response Body Example

```
{
  "status": "FINISHED",
  "chunks_available": [
    1,
    2
    ]
}
```

Reference Guide

https://cloud.tenable.com/api#/resources/exports/assets-export-status

Examples

- exports (library)
- exports (SDK)

Download Asset Export Chunks

User Permissions: Administrator (64)

To download available asset export chunks, use the API endpoint described below.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/assets/export/{export_uuid}/chunks/{chunk_id}
```

Request Path Parameters

Parameter	Type	Description	Required
export_uuid	string	The UUID of the export request.	required
chunk_id	integer	The ID of the asset chunk you want to export.	required

Request Path Example

```
GET https://cloud.tenable.com/assets/export/a483adf8-24e3-4c7f-818a-6867b02310dd/chunks/1
```

Request Body Syntax

None.

HTTP Response

Response Codes

Status	Description
200	Returned if file is downloaded successfully. For more information, see "Response Body Syntax."
400	Returned if the chunk ID is invalid or the chunk is not ready for download.
403	Returned if you do not have permission to export asset data.
404	Returned if a chunk with the specified export chunk is not found.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

Note: The response attributes listed below represent all available attributes. The API response body excludes an attribute if the attribute is empty in the vulnerability record. For a description of the attributes, see Asset Export Attributes.

```
[
  {
    "id": {string},
    "has_agent": {boolean},
    "has_plugin_results": {boolean},
    "created_at": {string},
    "terminated_at": {string},
    "terminated_by": {string},
    "updated_at": {string},
    "deleted_at": {string},
    "deleted_by": {string},
    "first_seen": {string},
    "last_seen": {string},
    "first_scan_time": {string},
    "last_scan_time": {string},
    "last_authenticated_scan_date": {string},
    "last_licensed_scan_date": {string},
```

```
    "azure_vm_id": {string},
    "azure_resource_id": {string},
    "aws_ec2_instance_ami_id": {string},
    "aws_ec2_instance_id": {string},
    "agent_uuid": {string},
    "bios_uuid": {string},
    "environment_id": {string},
    "aws_owner_id": {string},
    "aws_availability_zone": {string},
    "aws_region": {string},
    "aws_vpc_id": {string},
    "aws_ec2_instance_group_name": {string},
    "aws_ec2_instance_state_name": {string},
    "aws_ec2_instance_type": {string},
    "aws_subnet_id": {string},
    "aws_ec2_product_code": {string},
    "aws_ec2_name": {string},
    "mcafee_epo_guid": {string},
    "mcafee_epo_agent_guid": {string},
    "servicenow_sysid": {string},
    "agent_names": {array},
    "ipv4s": {array},
    "ipv6s": {array},
    "fqdns": {array},
    "mac_addresses": {array},
    "netbios_names": {array},
    "operating_systems": {array},
    "system_types": {array},
    "hostnames": {array},
    "ssh_fingerprints": {array},
    "qualys_asset_ids": {array},
    "qualys_host_ids": {array},
    "manufacturer_tpm_ids": {array},
```

```
    "symantec_ep_hardware_keys": {array},
    "sources": {array},
    "tags": {array},
    "network_interfaces": {array},
  }
]
```

Response Body Attributes

See Asset Export Attributes.

Response Body Example

```
[
  {
    "id": "60d5a1e7-aec0-45d3-b196-c2356b1567b9",
    "has_agent": false,
    "has_plugin_results": true,
    "created_at": "2017-12-14T20:40:44.535Z",
    "terminated_at": null,
    "terminated_by": null,
    "updated_at": "2018-02-23T22:27:58.599Z",
    "deleted_at": null,
    "deleted_by": null,
    "first_seen": "2017-12-14T20:40:23.447Z",
    "last_seen": "2018-02-23T22:27:52.869Z",
    "first_scan_time": "2017-12-14T20:40:23.447Z",
    "last_scan_time": "2018-02-23T22:27:52.869Z",
    "last_authenticated_scan_date": null,
    "last_licensed_scan_date": "2018-02-23T22:27:52.869Z",
    "azure_vm_id": null,
    "azure_resource_id": null,
    "aws_ec2_instance_ami_id": null,
    "aws_ec2_instance_id": null,
```

```
  "agent_uuid": null,
  "bios_uuid": null,
  "environment_id": "00000000-0000-0000-0000-000000000000",
  "aws_owner_id": null,
  "aws_availability_zone": null,
  "aws_region": null,
  "aws_vpc_id": null,
  "aws_ec2_instance_group_name": null,
  "aws_ec2_instance_state_name": null,
  "aws_ec2_instance_type": null,
  "aws_subnet_id": null,
  "aws_ec2_product_code": null,
  "aws_ec2_name": null,
  "mcafee_epo_guid": null,
  "mcafee_epo_agent_guid": null,
  "servicenow_sysid": null,
  "agent_names": [],
  "ipv4s": [
    "172.1.2.57"
  ],
  "ipv6s": [],
  "fqdns": [
    "172-1-2-57.lightspeed.hstntx.sbcglobal.net"
  ],
  "mac_addresses": [],
  "netbios_names": [],
  "operating_systems": [],
  "system_types": [],
  "hostnames": [],
  "ssh_fingerprints": [],
  "qualys_asset_ids": [],
  "qualys_host_ids": [],
  "manufacturer_tpm_ids": [],
```

```
    "symantec_ep_hardware_keys": [],
    "sources": [
      {
        "name": "NESSUS_SCAN",
        "first_seen": "2017-12-14T20:40:23.447Z",
        "last_seen": "2018-02-23T22:27:52.869Z"
      }
    ],
    "tags": [
      {
        "uuid": "6ee5761f-5c99-434b-aecb-e09b755921b7",
        "key": "Geographic Area",
        "value": "APAC",
        "added_by": "e7ecb50b-1330-4a8c-b8e5-ee00ec8c46f8",
        "added_at": "2018-02-13T14:53:13.817Z"
      }
    ],
    "network_interfaces": []
  }
]
```


Reference Guide

https://cloud.tenable.com/api#/resources/exports/assets-download-chunk

Examples

- exports (library)
- exports (SDK)

Asset Export Attributes

The table below defines all available attributes of an asset export data chunk. Export chunks do not include an attribute if that attribute is empty in the asset record.

Note: Dates and times in the response message use the standard timestamp format.

Attribute	Value	Description
id	string	The UUID of the asset in Tenable.io.
has_agent	boolean	Specifies whether a Nessus agent scan identified the asset.
has_plugin_results	boolean	Specifies whether the asset has plugin results associated with it.
created_at	string	The time and date when Tenable.io created the asset record.
terminated_at	string	The time and date when a user terminated the Amazon Web Service (AWS) virtual machine instance of the asset.
terminated_by	string	The user who terminated the AWS instance of the asset.
updated_at	string	The time and date when the asset record was last updated.
deleted_at	string	The time and date when a user deleted the asset record. When a user deletes an asset record, Tenable.io retains the record until the asset ages out of the license count.
deleted_by	string	The user who deleted the asset record.
first_seen	string	The time and date when a scan first identified the asset.
last_seen	string	The time and date of the scan that most recently identified the asset.
first_scan_time	string	The time and date of the first scan run against the asset.
last_scan_time	string	The time and date of the last scan run against the asset.
last_authen-	string	The time and date of the last credentialed scan run on the asset.

ticated_scan_date		
last_licensed_scan_date	string	The time and date of the last scan that identified the asset as licensed. Tenable.io categorizes an asset as licensed if a scan of that asset has returned results from a non-discovery plugin within the last 90 days.
azure_vm_id	string	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see Accessing and Using Azure VM Unique ID in the Microsoft Azure documentation.
azure_resource_id	string	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
aws_ec2_instance_ami_id	string	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.
aws_ec2_instance_id	string	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.
agent_uuid	string	The unique identifier of the Nessus agent that identified the asset.
bios_uuid	string	The BIOS UUID of the asset.
environment_id	string	The environment your organization assigned to the asset in Tenable.io. Tenable is enabling scan environments for customers in a rolling fashion. This attribute is empty if scan environments have not yet been enabled for your organization.
aws_owner_id	string	The canonical user identifier for the AWS account associated with the virtual machine instance. For example, "79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be". For more information, see AWS Account Identifiers in the AWS documentation.
aws_availability_zone	string	The availability zone where Amazon Web Services hosts the virtual machine instance, for example, "us-east-1a". Availability zones are

		subdivisions of AWS regions. For more information, see Regions and Availability Zones in the AWS documentation.
aws_region	string	The region where AWS hosts the virtual machine instance, for example, "us-east-1". For more information, see Regions and Availability Zones in the AWS documentation.
aws_vpc_id	string	The unique identifier for the virtual public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.
aws_ec2_instance_group_name	string	The virtual machine instance's group in AWS.
aws_ec2_instance_state_name	string	The state of the virtual machine instance in AWS at the time of the scan.
aws_ec2_instance_type	string	The type of instance in AWS EC2.
aws_subnet_id	string	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.
aws_ec2_product_code	string	The product code associated with the AMI used to launch the virtual machine instance in AWS EC2.
aws_ec2_name	string	The name of the virtual machine instance in AWS EC2.
mcafee_epo_guid	string	The unique identifier of the asset in McAfee ePolicy Orchestrator (ePO) . For more information, see the McAfee documentation.
mcafee_epo_agent_guid	string	The unique identifier of the McAfee ePO agent that identified the asset. For more information, see the McAfee documentation.
servicenow_sysid	string	The unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.
agent_names	array	The names of any Nessus agents that scanned and identified the

		asset.
ipv4s	array	The IPv4 addresses that scans have associated with the asset record.
ipv6s	array	The IPv6 addresses that scans have associated with the asset record.
fqdns	array	The fully-qualified domain names that scans have associated with the asset record.
mac_ addresses	array	The MAC addresses that scans have associated with the asset record.
netbios_ names	array	The NetBIOS names that scans have associated with the asset record.
operating_ systems	array	The operating systems that scans have associated with the asset record.
system_types	array	The system types as reported by Plugin ID 54615. Possible values include "router," "general-purpose," "scan-host," and "embedded."
hostnames	array	The hostnames that scans have associated with the asset record.
ssh_fin- gerprints	array	The SSH key fingerprints that scans have associated with the asset record.
qualys_ asset_ids	array	The Asset ID of the asset in Qualys. For more information, see the Qualys documentation. **Note:** Tenable is enabling Qualys asset import for customers in a rolling fashion. For more information, contact your Tenable rep- resentative.
qualys_host_ ids	array	The Host ID of the asset in Qualys. For more information, see the Qualys documentation. **Note:** Tenable is enabling Qualys asset import for customers in a rolling fashion. For more information, contact your Tenable rep- resentative.
man- ufacturer_ tpm_ids	array	The manufacturer's unique identifier of the Trusted Platform Module (TPM) associated with the asset.

symantec_ep_hardware_keys	array	The hardware keys for the asset in Symantec Endpoint Protection.
sources	array	The sources of the scans that identified the asset. For more information, see Source Objects.
tags	array	Category tags assigned to the asset in Tenable.io. For more information, see Tag Objects.
network_interfaces	array	The network interfaces that scans identified on the asset. For more information, see Network Interface Objects.

Retrieve Agent Data for an Asset

User Permissions: Administrator (64)

An asset export response message does not include information related to Nessus agents installed on the exported assets.

Basic agent information you might find useful includes the following attributes of the agent list response: `distro`, `core_version`, `last_connect`, `status`, and `groups`.

To retrieve agent data for an asset:

1. Retrieve agent data.
2. Match the agent data to the asset data using the common identifier:

Response Message	Attribute
List Agents	uuid
Download Asset Export Chunks	id

List Agents

User Permissions: Administrator (64)

To retrieve information about Nessus agents installed on your assets, use the API endpoint described below.

Before You Begin

Determine the ID of the scanner associated with the agents.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/scanners/{scanner_id}/agents
```

Request Path Parameters

Attribute	Type	Description	Required?
Path Parameters			
scanner_id	integer	The ID of the scanner to query for agents.	required
Query Parameters			
offset	integer	The starting record to retrieve. If this parameter is not supplied, the default value is 0.	optional
limit	integer	The number of records to retrieve. If you omit this parameter, Tenable.io uses a default of 50 records. The minimum supported limit is 1, and the maximum supported limit is 5000.	optional

sort	string	The sort order of the returned records. Sort can only be applied to the `sortable_fields` specified by the filter capabilities. There may be no more than `max_sort_fields` number of columns used in the sort, as specified by the filter capabilities. Sort is applied, in order, in the following format: "*field1*:[asc|desc],*field2*:[asc|desc]". For example, "sort=*field1*:asc,*field2*:desc" would first sort by *field1*, ascending, then sort by *field2*, descending.	optional
f	string	Apply a filter in the format "*field*:*operator*:*value*". For example, *`field1`*`:match:`*`sometext`* would match any records where the value of *field1* contains "*sometext*". You can use multiple query filters.	optional
ft	string	Filter type. If the filter type is `and`, the record is only returned if all filters match. If the filter type is `or`, the record is returned if any of the filters match.	optional
w	string	Wildcard filter text. Wildcard search is a mechanism where multiple fields of a record are filtered against one given filter string. If any one of the wildcard fields' values matches against the filter string, the record matches the wildcard filter. For a record to be returned, the record must pass the wildcard filter (if there is one) AND the set of standard filters. For example, if you submit the filter, `w=wild&f=field1:match:one&f=field2:match:two&ft=or`, the record would match if the value of any supported wildcard fields contained the text `wild`, AND either `field1`'s value contained `one` or `field2`'s value contained `two`.	optional
wf	string	A comma-delimited subset of wildcard fields to search when applying the wildcard filter, for example `field1,field2`. If you provide a `w`parameter, but do not provide a `wf` parameter, all wildcard fields' values are searched against the wildcard filter text.	optional

Request Path Example

```
GET https://cloud.tenable.com/scanners/18788321/agents
```

HTTP Response

Response Codes

Status	Description
200	Returns the agent list. For more information, see "Response Body Syntax."
403	Returned if the user does not have permission to view the list.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "agents": [
    {
      "id": {integer},
      "uuid": {string},
      "name": {string},
      "platform": {string},
      "distro": {string},
      "ip": {string},
      "last_scanned": {integer},
      "plugin_feed_id": {string},
      "core_build": {string},
      "core_version": {string},
      "linked_on": {integer},
      "last_connect": {integer},
      "status": {string},
      "groups": [
        {
```

```
          "name": {string},
          "id": {integer}
        }
      ]
    }
  ],
  "pagination": {
    "total": {integer},
    "offset": {integer},
    "limit": {integer},
    "sort": [
      {
        "name": {string},
        "order": {string}
      }
    ]
  }
}
```

Response Body Attributes

Attribute	Object Attribute	Type	Description
agents			
id	–	integer	The unique ID of the agent.
uuid	–	string	The UUID of the agent. **Note:** This value corresponds to the ID of the asset where the agent is installed. You can use this attribute to match agent data to asset data.
name	–	string	The name of the agent.
platform	–	string	The platform of the agent.

distro	–	string	The agent software distribution.
ip	–	string	The IP address of the agent.
last_ scanned	–	integer	The last scanned date for the agent (in the Unix timestamp format).
plugin_ feed_id	–	string	The currently loaded plugin set of the agent (null if the agent has no plugin set loaded).
core_ build	–	string	Build number for the agent.
core_ver- sion	–	string	Build version for the agent.
linked_ on	–	integer	The time the agent was linked (in the Unix timestamp format).
last_con- nect	–	integer	The last time the agent communicated with the server (in the Unix timestamp format).
status	–	string	A status value indicating whether the agent has connected to the manager recently. Possible values include: • on—The agent has connected to the manager recently and is, therefore, likely ready to scan. • off—The agent has not connected to the manager recently and should be considered offline. • init—The agent is online, but is still processing plugin updates and is not ready to scan.
groups	name	string	The name of the agent group to which the agent belongs.
	id	integer	The ID of the agent group to which the agent belongs.
pagination			
total	–	integer	The total number of records which match any applied filters. This number may be approximate.
limit	–	integer	The number of records returned with this response.

offset	–	integer	The index of the first record retrieved.
sort	name	string	The name of the field by which Tenable.io sorts the records in the response. Sort fields are listed in order of application.
	order	string	The direction by which Tenable.io sorted the records. Possible values include: • asc—Sorted in ascending order (for example, a-z). • desc—Sorted in descending order (for example, z-a).

Response Body Example


```
{
  "agents": [
    {
      "id": 156,
      "uuid": "07e496f5-d2dc-4232-9733-12e5f7d05ae3",
      "name": "usersmacbook.local",
      "platform": "DARWIN",
      "distro": "macosx",
      "ip": "172.204.81.57",
      "last_scanned": 1539206978,
      "plugin_feed_id": "201810122051",
      "core_build": "17",
      "core_version": "7.1.1",
      "linked_on": 1456774734,
      "last_connect": 1539480598,
      "status": "off",
      "groups": [
        {
          "name": "Headquarters Agents",
          "id": 8
        },
        {
          "name": "Macbook Users",
```

```
          "id": 3315
        }
      ]
    }
  ],
  "pagination": {
    "total": 11,
    "limit": 50,
    "offset": 0,
    "sort": [
      {
        "name": "name",
        "order": "asc"
      }
    ]
  }
}
```


Reference Guide

https://cloud.tenable.com/api#/resources/agents/list

Examples

- agents (library)
- agents (SDK)

Manage Asset Tags

In Tenable.io, asset tags are composed of custom categories and associated values. For example, if you want to group your assets by location, create a *Location* category with the value *Headquarters*. Note that this definition of tag is more specific than the more general usage of "tag."

You can assign these tags to assets to categorize or group the assets. Tenable does *not* support using asset tags to define custom attributes for individual assets.

> **Note:** Tenable.io supports a maximum of 100 tag categories per organization. By default, the maximum number of total tags for your organization is 100,000. If your organization wants to change the total tag maximum, contact your Tenable representative.

In the Tenable.io user interface, you can create dynamic tags, that is, asset tags that the system automatically applies to assets based on asset attribute rules. The Tenable.io API does not support creating dynamic tags, but you can view information about dynamic tags created in the user interface.

To manage asset tags:

1. Create asset tags that reflect your business context.
2. Assign tags to your assets.
3. Maintain the tags you've assigned:
    - Correct asset tag assignments.
    - Update an existing tag.
    - Delete a single asset tag.
    - Delete multiple asset tags.
    - Delete an asset tag category and associated tags.
    - List all asset tags, assets for a specific tag, or tags for a specific asset.

Create an Asset Tag

User Permissions: Basic (16)

To create a asset tag, use the API endpoint described below.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
POST https://cloud.tenable.com/tags/values
```

Request Path Parameters

None.

Request Path Example

See "Request Path Syntax."

Request Body Syntax

```
{
  "category_name": {string},
  "category_uuid": {string},
  "category_description": {string},
  "value": {string},
  "description": {string}
}
```

Request Body Attributes

Attribute	Type	Description	Required?
category_name	string	The name of the tag category to associate with the new value. Specify the name of a *new* category if you want to add both a new category and tag value. Specify the name of an *existing* category if you want to add the tag value to the existing category. **Caution:** This value is case-sensitive. For example, Tenable.io considers "location" and "Location" to be separate categories. The category_name can result in the following responses: • If the `category_name` you specify exists, and the tag value you specify already exists for that category, Tenable.io returns a 400 response code, instead of adding the tag. • If the `category_name` you specify exists, but the tag value you specify does not yet exist for that category, Tenable.io adds the tag value to the existing category. • If the `category_name` you specify does not exist, Tenable.io creates a new tag category and adds the new tag value to that category.	required if category_uuid is not present
category_uuid	string	The UUID of the tag category to associate with the new value. Use this parameter only if you want to add the tag value to an existing category. If the UUID you specify does not exist, Tenable.io does not create a new catgory. Instead, it returns a 400 (Bad Request) response code.	required if category_name is not present
category_description	string	The description for the new tag category that Tenable.io creates if the category specified by name by name does not exist. Otherwise Tenable.io ignores the description.	optional
value	string	The new tag value.	required

		Caution: This value is case-sensitive. For example, Tenable.io considers "headquarters" and "Headquarters" to be separate tag values.	
description	string	The new tag value description.	optional

Request Body Example

```
{
  "category_name": "Location",
  "category_description": "Geographical location.",
  "value": "Headquarters",
  "description": "Devices installed at the Columbia, MD office."
}
```

HTTP Response

Response Codes

Status	Description
200	Returned if Tenable.io successfully creates a value. For more information, see "Response Body Syntax."
400	Returned if Tenable.io encountered any of the following error conditions: • `not_found`—The category you specified does not exist. • `max_entries`—Your request exceeded a tag limit for your organization. These limits can be either the maximum number of categories (100) or the maximum number of tag values (100,000 per category, or as configured for your organization). • `duplicate`—The combination of category and value you specified already exists.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "uuid": {string},
  "created_at": {string},
  "created_by": {string},
  "updated_at": {string},
  "updated_by": {string},
  "category_uuid": {string},
  "value": {string},
  "description": {string},
  "type": {string},
  "category_name": {string},
  "category_description": {string}
}
```

Response Body Attributes

Attribute	Type	Description
uuid	string	The UUID of the tag value. Use this value to assign the tag to assets.
created_at	string	A timestamp in standard format indicating when the tag was created.
created_by	string	The user who created the tag
updated_at	string	A timestamp in standard format indicating when the tag was last updated. At this stage, this date matches the `created_at` date.
updated_by	string	The user who last updated the tag. At this stage, this date matches the `created_by` value.
category_uuid	string	The UUID of the category. Use this value to create future tags in the same category.
value	string	The tag value (the second half of the category:value pair).
description	string	The description of the tag value.
type	string	The tag type: • `static`—A user must manually apply the tag to an asset. You can

		use the Tenable.io API to create and assign static tags to assets. • dynamic—Tenable.io automatically applies the tag based on asset attribute rules. You can use the Tenable.io user interface to create dynamic asset tags. For more information, see the *Tenable.io Vulnerability Management User Guide*.
category_name	string	The tag category name (the first half of the category:value pair).
category_description	string	The description of the tag category.

Response Body Example

```
{
  "uuid":"86499fa2-1206-46f6-a6b8-532383d066c2",
  "created_at":"2018-11-29T22:55:35.246Z",
  "created_by":"api@api.demo",
  "updated_at":"2018-11-29T22:55:35.246Z",
  "updated_by":"api@api.demo",
  "category_uuid":"db36f7c6-0f5d-4868-9fc4-765edc4ad0b4",
  "value":"Headquarters",
  "description":"Devices installed at the Columbia, MD office.",
  "type":"static",
  "category_name":"Location",
  "category_description":"Geographical location."
}
```

Reference Guide

https://cloud.tenable.com/api#/resources/tags/create-tag-value

Update an Asset Tag

User Permissions: Basic (16)

To update an asset tag, use the API endpoint described below.

Before You Begin

Determine the UUID of the tag you want to update.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
PUT https://cloud.tenable.com/tags/values/{value_uuid}
```

Request Path Parameters

Attribute	Type	Description	Required?
value_uuid	string	The UUID of the tag value you want to update.	required

Request Path Example

```
PUT https://cloud.tenable.com/tags/values/ce8e96b5-4e4a-4469-99a6-
425479153dea
```

Request Body Syntax

```
{
  "value": {string},
```

```
  "description": {string}
}
```

Request Body Attributes

Attribute	Type	Description	Required?
value	string	The new tag value.	optional
description	string	The new tag value description.	optional

Request Body Example

```
{
  "value": "Seattle",
  "description": "Devices installed at the Seattle, WA office"
}
```

HTTP Response

Response Codes

Status	Description
200	Returned if Tenable.io has successfully updated the tag value. For more information, see "Response Body Syntax."
400	Returned if the new tag value already exists in the category.
404	Returned if Tenable.io could not find the specified tag value.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "uuid": {string},
  "created_at": {string},
  "created_by": {string},
  "updated_at": {string},
  "updated_by": {string},
  "category_uuid": {string},
  "value": {string},
  "description": {string},
  "type": {string},
  "category_name": {string},
  "category_description": {string}
}
```

Response Body Attributes

See Detailed Tag Object.

Response Body Example

```
{
  "uuid": "0a6c1176-4c03-4776-a60a-048021a48799",
  "created_at": "2018-10-30T15:39:16.687Z",
  "created_by": "user3@example.com",
  "updated_at": "2018-10-30T15:39:16.687Z",
  "updated_by": "user3@example.com",
  "category_uuid": "8981f2d8-a043-4a74-ad78-e6a73b13ccaf",
  "value": "Seattle",
  "description": "Devices installed at the Seattle, WA office",
  "type": "static",
  "category_name": "location",
  "category_description": "Asset location",
}
```

Reference Guide

https://cloud.tenable.com/api#/resources/tags/update-tag-value

Delete a Single Asset Tag

User Permissions: Basic (16)

To delete a single asset tag, use the API endpoint described below.

If you delete an asset tag, Tenable.io also removes that tag from any assets where the tag was assigned.

Note: If you delete all asset tags associated with a category. Tenable.io retains the category. You must delete the category separately.

Before You Begin

Determine the UUID of the tag you want to delete.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
DELETE https://cloud.tenable.com/tags/values/{value_uuid}
```

Request Path Parameters

Attribute	Type	Description	Required?
value_uuid	string	The UUID of the tag you want to delete. **Note:** A tag UUID is technically assigned to the tag value only (the second half of the category:value pair), but the API commands use this value to represent the whole category:value pair.	required

Request Path Example

```
DELETE https://cloud.tenable.com/tags/values/18179e00-b0e0-4fd7-be91-e9e854fe66b9
```

Request Body Syntax

None.

HTTP Response

Response Codes

Status	Description
200	Returned if Tenable.io successfully deletes the specified tag value.
404	Returned if Tenable.io cannot find the specified tag value.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

None.

Reference Guide

https://cloud.tenable.com/api#/resources/tags/delete-tag-value

Delete Multiple Asset Tags

User Permissions: Basic (16)

To delete multiple asset tags, use the API endpoint described below.

If you delete an asset tag, Tenable.io also removes that tag from any assets where the tag was assigned.

Note: If you delete all asset tags associated with a category. Tenable.io retains the category. You must delete the category separately.

Before You Begin

Determine the UUIDs of the tags you want to delete.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
POST https://cloud.tenable.com/tags/values/delete-requests
```

Request Path Parameters

None.

Request Path Example

See "Request Path Syntax."

Request Body Syntax

```
{
  "values": [
    {string},
    {string},
    {string}
  ]
}
```

Request Body Attributes

Attribute	Object Attribute	Type	Description	Required?
values	value_uuid	string	The UUID of a tag you want to delete. **Note:** A tag UUID is technically assigned to the tag value only (the second half of the category:value pair), but the API commands use this value to represent the whole category:value pair.	required

Request Body Example

```
{
  "values": [
    "18179e00-b0e0-4fd7-be91-e9e854fe66b9",
    "f45a48b4-50e7-41c3-afb9-2e01f5423698",
    "fb7fae7d-8acb-48e4-928c-d93103e9e73f"
  ]
}
```

HTTP Response

Response Codes

Status	Description
200	Returned if Tenable.io successfully deletes the specified tag values.
400	Returned if you specify invalid UUIDs.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

None.

Reference Guide

https://cloud.tenable.com/api#/resources/tags/delete-tag-values-bulk

Delete an Asset Tag Category

User Permissions: Basic (16)

To delete an asset tag category, use the API endpoint described below.

Caution: Deleting an asset tag category automatically deletes all tag values associated with that category.

Before You Begin

Determine the `category_uuid` of the category you want to delete.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
DELETE https://cloud.tenable.com/tags/categories/{category_uuid}
```

Request Path Parameters

Attribute	Type	Description	Required?
category_uuid	string	The UUID of the category you want to delete.	required

Request Path Example

```
DELETE https://cloud.tenable.com/tags/categories/7138cd5a-76c1-433e-b62a-c60ec2d14611
```

Request Body Syntax

None.

HTTP Response

Response Codes

Status	Description
204	Returned if Tenable.io successfully deleted the specified tag category.
404	Returned if Tenable.io could not find the specified tag category.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

None.

Reference Guide

https://cloud.tenable.com/api#/resources/tags/delete-tag-category

Determine Tag Identifiers

Certain Tenable.io API requests require one or more of the following tag identifiers:

- Category name (the first half of the category:value pair)
- Tag value (the second half of the category:value pair)
- Tag UUID

> **Note:** A tag UUID is technically assigned to the tag value only (the second half of the category:value pair), but the API commands use this value to represent the whole category:value pair.

To determine these tag identifiers, you can use any of the following approaches:

- List Asset Tags
- List Assets for a Specific Tag
- List Tags for a Specific Asset

List Asset Tags

User Permissions: Basic (16)

To list asset tags, use the API endpoint described below.

Tip: This list also includes tag categories where no tag values have been added. Use this command to determine the UUIDs of those categories.

Before You Begin

If you want to filter the returned asset tag list, determine your filter terms. For example, if you want to list tags for a specific category, determine the name of the category you want to use.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/tags/values?{query parameter}
```

Request Path Parameters

Attribute	Type	Description	Required?
Query Parameters			
f	string	A filter condition in the `field:operator:value` format. For example, your request might specify `f=value:match:-:rhel`. Filter conditions can include: • `value:eq:<value>`	optional

		• value:match:<value> • category_name:match:<partial_value> • category_name:eq:<category_name> • category_name:match:<partial_category_name> • description:eq:<description> • description:match:<partial_description> • updated_at:date-eq:<timestamp_as_int> • updated_at:date-gt:<timestamp_as_int> • updated_at:date-lt:<timestamp_as_int> • updated_by:eq:<user_uuid>	
ft	string	If multiple f parameters are present, specifies whether Tenable.io applies 'AND' or 'OR' to conditions. Supported values are and and or. If you omit this parameter when using multiple f parameters, Tenable.io applies 'AND' by default.	optional
wf	string	A comma-separated list of fields to include in the wildcard search. Provides the same functionality as a match condition in the f parameter. For example, f=value:match:Chi returns the same results as wf=value&w=Chi. Wildcard fields include: • category_name • value • description Use the w parameter to specify the search value.	optional

w	string	A single search value for the wildcard fields specified in the `wf` parameter.	optional
limit	integer	Maximum number of records requested. Must be in the int32 format.	optional
offset	integer	The number of records to skip in the returned result set. Must be in the int32 format.	optional
sort	array	The fields to sort on, for example, `sort=updated_at`. If you specify multiple fields, fields must be separated by commas. Sortable fields include: • `category_name` • `value` • `description`	optional

Request Path Example 1: List All Asset Tags for Your Organization

```
GET https://cloud.tenable.com/tags/values
```

Request Path Example 2: List Asset Tags for a Specific Category

```
GET https://cloud.tenable.com/tags/values?f=category_name:eq:Location
```

Request Body Syntax

None.

HTTP Response

Response Codes

Status	Description

200	Returns a list of tags with pagination information. For more information, see "Response Body Syntax."
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "values": [
    {
      {object},
      {object},
      {object}
    }
  ]
}
```

Response Body Attributes

See Detailed Tag Object.

Response Body Example

```
{
  "values": [
    {
      "uuid": "0a6c1176-4c03-4776-a60a-048021a48799",
      "created_at": "2018-10-30T15:39:16.687Z",
      "created_by": "user3@example.com",
      "updated_at": "2018-10-30T15:39:16.687Z",
      "updated_by": "user3@example.com",
      "category_uuid": "8981f2d8-a043-4a74-ad78-e6a73b13ccaf",
      "value": "Seattle",
      "description": "",
```

```
      "type": "static",
      "category_name": "location",
      "category_description": "Asset location",
    }
  ]
}
```

Reference Guide

https://cloud.tenable.com/api#/resources/tags/list-tag-values

List Assets for a Specific Tag

> **User Permissions:** Administrator (64)

To list assets that you have assigned a specific tag, use the API endpoint described below.

Before You Begin

Determine the category name and tag value for the tag you want to use to filter assets.

HTTP Request

> **Note:** To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/workbenches/assets
```

Request Path Parameters

None.

Request Path Example

See "Request Path Syntax."

Request Body Syntax

```
{
  filters: [
    {
      "filter": {string},
      "quality": {string},
      "value": {string}
```

```
    }
  ]
}
```

Request Body Attributes

Attribute	Object Attribute	Type	Description	Required?
filters	filter	string	Identifier. The asset attribute on which you want to filter. For asset tags, this attribute must be in the following format: `tag.category_name`	required to filter on tag
	quality	string	Operator. For asset tags, `eq` is the only supported operator.	required to filter on tag
	value	string	The value you want to filter on. For asset tags, this is the tag value.	required to filter on tag

Request Body Example

```
{
  filters: [
    {
      "filter": "tag.Location",
      "quality": "eq",
      "value": "Chicago"
    }
  ]
}
```

HTTP Response

Response Codes

Status	Description
200	Returns an array of asset objects. For more information, see "Response Body Syntax."
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax


```
{
  assets: [
    {
      "id": "ebe455fa-0558-4cd4-8b07-7164e27bcb80",
      "has_agent": false,
      "last_seen": "2018-08-30T13:46:31.449Z",
      "sources": [
        {
          "name": "connector",
          "first_seen": "2018-08-30T13:39:51.176Z",
          "last_seen": "2018-08-30T13:46:31.449Z"
        }
      ],
      "ipv4": [
        "100.66.33.136",
        "54.193.84.63"
      ],
      "ipv6": [],
      "fqdn": [],
      "netbios_name": [],
      "operating_system": [
        "windows"
      ],
      "agent_name": [],
```

```
      "aws_ec2_name": [],
      "mac_address": []
    },
  ],
  "total": {integer}
}
```

Response Body Attributes

Attribute	Object Attribute	Type	Description

assets	id	string	The UUID of the asset in Tenable.io.
	has_agent	boolean	Specifies whether a Nessus agent scan identified the asset.
	last_seen	string	The time and date of the scan that most recently identified the asset.
	sources	array	The sources of the scans that identified the asset. For more information, see Source Objects.
	ipv4	array	The IPv4 addresses that scans have associated with the asset record.
	ipv6	array	The IPv6 addresses that scans have associated with the asset record.
	fqdn	array	The fully-qualified domain names that scans have associated with the asset record.
	netbios_name	array	The NetBIOS names that scans have associated with the asset record.
	operating_system	array	The operating systems that scans have associated with the asset record.
	agent_name	array	The names of any Nessus agents that scanned and identified the asset.
	aws_ec2_name	array	The names of the AWS EC2 virtual machine instances associated with the asset record.
	mac_address	array	The MAC addresses that scans have associated with the asset record.
total	–	integer	The total number of asset objects returned.

Response Body Example

```
{
  "assets": [
    {
      "id": "d691bd93-5483-42ee-ae2b-7f25d2f8075a",
```

```
    "has_agent": false,
    "last_seen": "2018-10-17T15:30:41.411Z",
    "sources": [
      {
        "name": "NESSUS_SCAN",
        "first_seen": "2018-10-17T15:30:41.411Z",
        "last_seen": "2018-10-17T15:30:41.411Z"
      }
    ],
    "ipv4": [
      "172.204.81.57"
    ],
    "ipv6": [],
    "fqdn": [
      "accc5365.ipt.aol.com"
    ],
    "netbios_name": [],
    "operating_system": [],
    "agent_name": [],
    "aws_ec2_name": [],
    "mac_address": []
  },
  {
    "id": "538d2d84-32b7-4d1d-ae6c-8dfa2f50ed0d",
    "has_agent": false,
    "last_seen": "2015-05-06T17:48:46.000Z",
    "sources": [
      {
        "name": "NESSUS_SCAN",
        "first_seen": "2015-05-06T17:48:46.000Z",
        "last_seen": "2015-05-06T17:48:46.000Z"
      }
    ],
```

```
      "ipv4": [
        "172.82.157.177"
      ],
      "ipv6": [],
      "fqdn": [],
      "netbios_name": [],
      "operating_system": [
        "Linux Kernel 2.6.18-278.el5PAE on CentOS release 5.7 (Final)"
      ],
      "agent_name": [],
      "aws_ec2_name": [],
      "mac_address": []
    }
  ],
  "total": 2
}
```


Reference Guide

https://cloud.tenable.com/api#/resources/workbenches/assets

List Tags for a Specific Asset

> **User Permissions:** Basic (16)

To list tags assigned to a specific asset, use the API endpoint described below.

Before You Begin

Determine the UUID of the asset for which you want to view the assigned tags.

HTTP Request

> **Note:** To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/tags/assets/{asset_uuid}/assignments
```

Request Path Parameters

Attribute	Type	Description	Required?
asset_uuid	string	The UUID of the asset.	required

Request Path Example

```
GET
https://cloud.tenable.com/tags/assets/6edeee7cf86e47adb4f6f61cb9184eaa/ass-
ignments
```

Request Body Syntax

None.

HTTP Response

Response Codes

Status	Description
200	Returns a list of tags assigned to the specified asset. For more information, see "Response Body Syntax." **Note:** • If no tags are assigned to the asset, Tenable.io returns an empty list. • The service does not validate the asset UUID.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "tags": [
    {
      "value_uuid": {string},
      "category_name": {string},
      "asset_uuid": {string},
      "created_at": {string},
      "source": {string};
      "value": {string};
      "created_by": {string};
      "category_uuid": {string};
    }
  ]
}
```

Response Body Attributes

Attribute	Type	Description
value_uuid	string	The UUID of the tag value. Use this value to assign the tag to assets. **Note:** A tag UUID is technically assigned to the tag value only (the second half of the category:value pair), but the API commands use this value to represent the whole category:value pair.
category_name	sting	The tag category name (the first half of the category:value pair).
asset_uuid	string	The UUID of the asset where the tag is assigned.
created_at	string	A timestamp in standard format indicating when the tag was created.
source	string	The tag type: • `static`—A user must manually apply the tag to an asset. You can use the Tenable.io API to create and assign static tags to assets. • `dynamic`—Tenable.io automatically applies the tag based on asset attribute rules. You can use the Tenable.io user interface to create dynamic asset tags. For more information, see the *Tenable.io Vulnerability Management User Guide*.
value	string	The tag value (the second half of the category:value pair).
created_by	string	The user who created the tag value.
category_uuid	string	The UUID of the category. Use this value to create future tags in the same category.

Response Body Example

```
{
  "tags": [
    {
      "value_uuid": "18179e00-b0e0-4fd7-be91-e9e854fe66b9",
```

```
      "category_name": "location",
      "asset_uuid": "842fa017-0141-4fdd-a53b-bcdd971ed1da",
      "created_at": "2018-11-01T16:29:40.606Z",
      "source": "static",
      "value": "Chicago",
      "created_by": "fa76f456-9a6f-4f63-8553-1cee233eb965",
      "category_uuid": "8981f2d8-a043-4a74-ad78-e6a73b13ccaf"
    },
    {
      "value_uuid": "f45a48b4-50e7-41c3-afb9-2e01f5423698",
      "category_name": "threat",
      "asset_uuid": "842fa017-0141-4fdd-a53b-bcdd971ed1da",
      "created_at": "2018-11-01T16:29:40.606Z",
      "source": "static",
      "value": "wannacry",
      "created_by": "fa76f456-9a6f-4f63-8553-1cee233eb965",
      "category_uuid": "a43054ec-87d7-4290-951f-2c489e848463"
    }
  ]
}
```


Reference Guide

https://cloud.tenable.com/api#/resources/tags/list-asset-tags

Assign Tags to Assets

User Permissions: Basic (16)

To assign tags to assets, or remove tags from assets, use the API endpoint described below.

Before You Begin

- Determine the UUID of any tag you want to use in this procedure.
- Determine the UUID of any asset you want to use in this procedure.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
POST https://cloud.tenable.com/tags/assets/assignments
```

Request Path Parameters

None.

Request Path Example

See "Request Path Syntax."

Request Body Syntax

```
{
  "action": {string},
  "assets": [
    {string},
    {string},
```

```
    {string}
  ],
  "tags": [
    {string},
    {string},
    {string},
  ]
}
```

Request Body Attributes

Attribute	Type	Description	Required?
action	string	Specifies the action you want to take: • add—Assign a tag to an asset. • remove—Remove a tag from an asset	required
assets	array	An array of asset UUIDs.	required
tags	array	An array of tag UUIDs.	required

Request Body Example 1: Add One Tag to Multiple Assets

```
{
  "action": "add",
  "assets": [
    "208d8f5f-73a9-47cd-8b04-4aa99f38af79",
    "c2332afe-5bfd-41fe-9e2e-5462dd3df455",
    "9166eea2-d4aa-4a99-99eb-fee1c36d6457",
    "5fc79177-e820-4ff7-ac28-6a5a995fea8b",
    "fc0a57cb-66fc-43a5-a628-13ef10664fe8"
  ],
  "tags": [
    "18179e00-b0e0-4fd7-be91-e9e854fe66b9"
```

```
  ]
}
```

Request Body Example 2: Add Multiple Tags to One Asset

```
{
  "action": "add",
  "assets": [
    "208d8f5f-73a9-47cd-8b04-4aa99f38af79"
  ],
  "tags": [
    "18179e00-b0e0-4fd7-be91-e9e854fe66b9",
    "f45a48b4-50e7-41c3-afb9-2e01f5423698",
    "fb7fae7d-8acb-48e4-928c-d93103e9e73f"
  ]
}
```

Request Body Example 3: Add Multiple Tags to Multiple Assets

```
{
  "action": "add",
  "assets": [
    "208d8f5f-73a9-47cd-8b04-4aa99f38af79",
    "c2332afe-5bfd-41fe-9e2e-5462dd3df455",
    "9166eea2-d4aa-4a99-99eb-fee1c36d6457",
    "5fc79177-e820-4ff7-ac28-6a5a995fea8b",
    "fc0a57cb-66fc-43a5-a628-13ef10664fe8"
  ],
  "tags": [
    "18179e00-b0e0-4fd7-be91-e9e854fe66b9",
    "f45a48b4-50e7-41c3-afb9-2e01f5423698",
    "fb7fae7d-8acb-48e4-928c-d93103e9e73f"
```

```
  ]
}
```

HTTP Response

Response Codes

Status	Description
200	Returns the UUID of the asynchronous asset update job. For more information, see "Response Body Syntax."
400	Returned if Tenable.io could not find the specified assets.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "job_uuid": {string}
}
```

Response Body Attributes

Attribute	Type	Description
job_uuid	string	The UUID of the asynchronous asset update job.

Response Body Example

```
{
  "job_uuid": "62210d02a7056d0297f50a8ddfbd549e:aef1d0bc94e1ea3fad09"
}
```

Reference Guide

https://cloud.tenable.com/api#/resources/tags/assign-asset-tags

Correct Assigned Asset Tags

If you assign an incorrect tag to multiple assets, Tenable recommends that you take the following approach to correct the tags:

1. Create the new, correct tag.
2. Identify assets with the incorrect tag.
3. Assign the new, correct tag to the assets identified in the previous step.
4. Delete old, incorrect tag.

List Assets

User Permissions: Administrator (64)

To list assets, use the API endpoint described below.

Note: Tenable.io lists only assets from access groups to which you belong. For more information, see access-groups in the Tenable.io API reference guide.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/assets
```

Request Path Parameters

None.

Request Path Example

See "Request Path Syntax."

HTTP Response

Response Codes

Status	Description
200	Returns a list of assets. For more information, see "Response Body Syntax."
403	Returned if you do not have permission to list assets.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "assets": [
    {
      "id": {string},
      "has_agent": {boolean},
      "last_seen": {string},
      "sources": [
          {
            "name": {string},
            "first_seen": {string},
            "last_seen": {string}
          }
      ],
      "ipv4": [
        {string},
        {string}
      ],
      "ipv6": [
        {string},
        {string}
      ],
      "fqdn": [
        {string},
        {string}
      ],
      "netbios_name": [
        {string},
        {string}
      ],
      "operating_system": [
        {string},
        {string}
```

```
      ],
      "agent_name": [
        {string},
        {string}
      ],
      "aws_ec2_name": [
        {string},
        {string}
      ],
      "mac_address": [
        {string},
        {string}
      ]
    },
  ],
  "total": {integer}
  }
}
```

Response Body Attributes

Attribute	Object Attribute	Type	Description

assets	id	string	The UUID of the asset.
	has_agent	boolean	Specifies whether a Nessus agent scan identified the asset.
	last_seen	string	The time and date of the scan that most recently identified the asset.
	sources	array	The sources of the scans that identified the asset. For more information, see Source Objects.
	ipv4	array	A list of IPv4 addresses for the asset.
	ipv6	array	A list of IPv6 addresses for the asset.
	fqdn	array	A list of FQDNs for the asset.
	netbios_name	string	The NetBIOS name for the asset.
	operating_system	string	The operating system installed on the asset.
	agent_name	array	The names of any Nessus agents that scanned and identified the asset.
	aws_ec2_name	string	The name of the virtual machine instance in AWS EC2.
	mac_address	array	A list of MAC addresses for the asset.
totals	–	integer	The total number of assets in the list.

Response Body Example

```
{
  "assets": [
    {
      "id": "ebe455fa-0558-4cd4-8b07-7164e27bcb81",
      "has_agent": false,
      "last_seen": "2018-08-30T13:46:31.449Z",
      "sources": [
```

```
          {
            "name": "connector",
            "first_seen": "2018-08-30T13:39:51.176Z",
            "last_seen": "2018-08-30T13:46:31.449Z"
          }
      ],
      "ipv4": [
        "172.204.81.57",
        "172.82.157.177"
      ],
      "ipv6": [],
      "fqdn": [],
      "netbios_name": [],
      "operating_system": [
        "windows"
      ],
      "agent_name": [],
        "aws_ec2_name": [],
        "mac_address": []
      },
    ],
    "total": 102
  }
}
```


Reference Guide

https://cloud.tenable.com/api#/resources/assets/list-assets

View Asset Details

User Permissions: Administrator (64)

To view asset details, use the API endpoint described below.

Before You Begin

Determine the UUID of the asset for which you want to view details.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/assets/{asset_uuid}
```

Request Path Parameters

Attribute	Type	Description	Required?
asset_uuid	string	The UUID of the asset.	required

Request Path Example

```
https://cloud.tenable.com/assets/538d2d84-32b7-4d1d-ae6c-8dfa2f50ed0d
```

Request Body Syntax

None.

HTTP Response

Response Codes

Status	Description
200	Returns a list of assets. For more information, see "Response Body Syntax."
403	Returned if you do not have permission to view information about an asset.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "id": {string},
  "has_agent": {boolean],
  "created_at": {string},
  "updated_at": {string},
  "first_seen": {string},
  "last_seen": {string},
  "last_authenticated_scan_date": {string},
  "last_licensed_scan_date": {string},
  "sources": [
    {
      "name": {string},
      "first_seen": {string},
      "last_seen": {string}
    }
  ],
  "tags": [
    {
      "tag_uuid": {string},
      "tag_key": {string},
      "tag_value": {string},
      "added_by": {string},
      "added_at": {string}
```

```
    }
  ],
  "ipv4": [
    {string}
  ],
  "ipv6": [
    {string}
  ],
  "fqdn": [
    {string}
  ],
  "mac_address": [
    {string}
  ],
  "netbios_name": [
    {string}
  ],
  "operating_system": [
    {string}
  ],
  "system_type": [
    {string}
  ],
  "hostname": [
    {string}
  ],
  "agent_name": [
    {string}
  ],
  "bios_uuid": [
    {string}
  ],
  "aws_ec2_instance_id": [
```

```
    {string}
  ],
  "aws_ec2_instance_ami_id": [
    {string}
  ],
  "aws_owner_id": [
    {string}
  ],
  "aws_availability_zone": [
    {string}
  ],
  "aws_region": [
    {string}
  ],
  "aws_vpc_id": [
    {string}
  ],
  "aws_ec2_instance_group_name": [
    {string}
  ],
  "aws_ec2_instance_state_name": [
    {string}
  ],
  "aws_ec2_instance_type": [
    {string}
  ],
  "aws_subnet_id": [
    {string}
  ],
  "aws_ec2_product_code": [
    {string}
  ],
  "aws_ec2_name": [
```

```
    {string}
  ],
  "azure_vm_id": [
    {string}
  ],
  "azure_resource_id": [
    {string}
  ],
  "gcp_project_id": [
    {string}
  ],
  "gcp_zone": [
    {string}
  ],
  "gcp_instance_id": [
    {string}
  ],
  "ssh_fingerprint": [
    {string}
  ],
  "mcafee_epo_guid": [
    {string}
  ],
  "mcafee_epo_agent_guid": [
    {string}
  ],
  "qualys_asset_id": [
    {string}
  ],
  "qualys_host_id": [
    {string}
  ],
  "servicenow_sysid": [
```

```
    {string}
  ]
}
```

Response Body Attributes

Attribute	Type	Description
id	string	The UUID of the asset.
has_agent	boolean	Specifies whether a Nessus agent scan identified the asset.
created_at	string	The time and date when Tenable.io created the asset record.
updated_at	string	The time and date when the asset record was last updated.
first_seen	string	The time and date when a scan first identified the asset.
last_seen	string	The time and date of the scan that most recently identified the asset.
last_authenticated_scan_date	string	The time and date of the last credentialed scan run on the asset.
last_licensed_scan_date	string	The time and date of the last scan that identified the asset as licensed. Tenable.io categorizes an asset as licensed if a scan of that asset has returned results from a non-discovery plugin within the last 90 days.
sources	array	The sources of the scans that identified the asset. For more information, see Source Objects.
tags	array	Category tags assigned to the asset in Tenable.io. For more information, see Tag Objects.
ipv4	array	The IPv4 addresses that scans have associated with the asset record.
ipv6	array	The IPv6 addresses that scans have associated with the asset record.
fqdn	array	The fully-qualified domain names that scans have associated with the asset record.
mac_address	array	The MAC addresses that scans have associated with the asset record.

netbios_name	array	The NetBIOS names that scans have associated with the asset record.
operating_system	array	The operating systems that scans have associated with the asset record.
system_type	array	The system types as reported by Plugin ID 54615. Possible values include "router," "general-purpose," "scan-host," and "embedded."
hostname	array	The hostnames that scans have associated with the asset record.
agent_name	array	The names of any Nessus agents that scanned and identified the asset.
bios_uuid	array	The BIOS UUID that scans have associated with the asset.
aws_ec2_instance_id	array	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.
aws_ec2_instance_ami_id	array	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.
aws_owner_id	array	The canonical user identifier for the AWS account associated with the virtual machine instance. For example, "79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be". For more information, see AWS Account Identifiers in the AWS documentation.
aws_availability_zone	array	The availability zone where Amazon Web Services hosts the virtual machine instance, for example, "us-east-1a". Availability zones are subdivisions of AWS regions. For more information, see Regions and Availability Zones in the AWS documentation.
aws_region	array	The region where AWS hosts the virtual machine instance, for example, "us-east-1". For more information, see Regions and Availability Zones in the AWS documentation.
aws_vpc_id	array	The unique identifier for the virtual public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.

aws_ec2_instance_group_name	array	The virtual machine instance's group in AWS.
aws_ec2_instance_state_name	array	The state of the virtual machine instance in AWS at the time of the scan.
aws_ec2_instance_type	array	The type of instance in AWS EC2.
aws_subnet_id	array	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.
aws_ec2_product_code	array	The product code associated with the AMI used to launch the virtual machine instance in AWS EC2.
aws_ec2_name	array	The name of the virtual machine instance in AWS EC2.
azure_vm_id	array	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see Accessing and Using Azure VM Unique ID in the Microsoft Azure documentation.
azure_resource_id	array	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
gcp_project_id	array	The customized name of the project to which the virtual machine instance belongs in Google Cloud Platform (GCP). For more information, see Creating and Managing Projects in the GCP documentation.
gcp_zone	array	The zone where the virtual machine instance runs in GCP. For more information, see Regions and Zones in the GCP documentation.
gcp_instance_id	array	The unique identifier of the virtual machine instance in GCP.
ssh_fingerprint	array	The SSH key fingerprints that scans have associated with the asset record.

mcafee_epo_guid	array	The unique identifier of the asset in McAfee ePolicy Orchestrator (ePO) . For more information, see the McAfee documentation.
mcafee_epo_agent_guid	array	The unique identifier of the McAfee ePO agent that identified the asset. For more information, see the McAfee documentation.
qualys_asset_id	array	The Asset ID of the asset in Qualys. For more information, see the Qualys documentation.
qualys_host_id	array	The Host ID of the asset in Qualys. For more information, see the Qualys documentation.
servicenow_sysid	array	The unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.

Response Body Example


```
{
  "id": "60d5a1e7-aec0-45d3-b196-c2356b1567b9",
  "has_agent": false,
  "created_at": "2017-12-14T20:40:44.535Z",
  "updated_at": "2018-02-23T22:27:58.599Z",
  "first_seen": "2017-12-14T20:40:23.447Z",
  "last_seen": "2018-02-23T22:27:52.869Z",
  "last_authenticated_scan_date": null,
  "last_licensed_scan_date": null,
  "sources": [
    {
      "name": "NESSUS_SCAN",
      "first_seen": "2017-12-14T20:40:23.447Z",
      "last_seen": "2018-02-23T22:27:52.869Z"
    }
  ],
  "tags": [
    {
      "tag_uuid": "6ee5761f-5c99-434b-aecb-e09b755921b7",
```

```
      "tag_key": "Geographic Area",
      "tag_value": "APAC",
      "added_by": "e7ecb50b-1330-4a8c-b8e5-ee00ec8c46f8",
      "added_at": "2018-02-13T14:53:13.817Z"
    }
  ],
  "ipv4": [
    "172.1.2.57"
  ],
  "ipv6": [],
  "fqdn": [
    "172-1-2-57.lightspeed.hstntx.sbcglobal.net"
  ],
  "mac_address": [],
  "netbios_name": [],
  "operating_system": [],
  "system_type": [],
  "hostname": [],
  "agent_name": [],
  "bios_uuid": [],
  "aws_ec2_instance_id": [],
  "aws_ec2_instance_ami_id": [],
  "aws_owner_id": [],
  "aws_availability_zone": [],
  "aws_region": [],
  "aws_vpc_id": [],
  "aws_ec2_instance_group_name": [],
  "aws_ec2_instance_state_name": [],
  "aws_ec2_instance_type": [],
  "aws_subnet_id": [],
  "aws_ec2_product_code": [],
  "aws_ec2_name": [],
  "azure_vm_id": [],
```

```
  "azure_resource_id": [],
  "gcp_project_id": [],
  "gcp_zone": [],
  "gcp_instance_id": [],
  "ssh_fingerprint": [],
  "mcafee_epo_guid": [],
  "mcafee_epo_agent_guid": [],
  "qualys_asset_id": [],
  "qualys_host_id": [],
  "servicenow_sysid": []
}
```


Reference Guide

https://cloud.tenable.com/api#/resources/assets/asset-info

Asset Objects

You can specify the attributes listed below in asset objects when adding asset data to Tenable.io.

Object Syntax

```
{
  "tenable_uuid": {string},
  "mac_address": [
    {string}
  ],
  "netbios_name": {string},
  "fqdn": [
    {string}
  ],
  "ip_address": [
    {string}
  ],
  "ipv4": [
    {string}
  ],
  "ipv6": [
    {string}
  ],
  "hostname": [
    {string}
  ],
  "operating_system": [
    {string}
  ],
  "ssh_fingerprint": {string},
  "bios_uuid": {string},
  "manufacturer_tpm_id": {string},
```

```
  "mcafee_epo_guid": {string},
  "mcafee_epo_agent_guid": {string},
  "symantec_ep_hardware_key": {string},
  "qualys_asset_id": {string},
  "qualys_host_id": {string},
  "servicenow_sys_id": {string},
  "gcp_project_id": {string},
  "gcp_zone": {string},
  "gcp_instance_id": {string},
  "azure_vm_id": {string},
  "azure_resource_id": {string},
  "aws_availability_zone": {string},
  "aws_ec2_instance_id": {string},
  "aws_ec2_instance_ami_id": {string},
  "aws_ec2_instance_group_name": [
    {string}
  ],
  "aws_ec2_instance_state_name": {string},
  "aws_ec2_instance_type": {string},
  "aws_ec2_name": {string},
  "aws_ec2_product_code": [
    {string}
  ],
  "aws_owner_id": {string},
  "aws_region": {string},
  "aws_subnet_id": {string},
  "aws_vpc_id": {string}
}
```

Object Attributes

The table below defines the attributes of an asset object.

Note: To add an asset object to Tenable.io, the asset object in the request must contain a value for at least one identifier attribute. The **Required** column in the table below indicates which attributes are required identifiers.

Attribute	Type	Description	Required?
tenable_uuid	string	The UUID of the asset.	excluded from add requests (system-generated)
mac_address	array	A list of MAC addresses for the asset.	required identifier
netbios_name	string	The NetBIOS name for the asset.	required identifier
fqdn	array	A list of FQDNs for the asset.	required identifier
ip_address	array	A list of IPv4 addresses for the asset. Tenable.io supports this legacy field for backwards compatibility, but for new requests, this field should be replaced by the **ipv4** field.	required identifier (legacy)
ipv4	array	A list of IPv4 addresses for the asset.	required identifier
ipv6	array	A list of IPv6 addresses for the asset.	optional
hostname	array	A list of hostnames for the asset.	optional

operating_system	string	The operating system installed on the asset.	optional
ssh_fingerprint	string	The SSH key fingerprints that scans have associated with the asset record.	optional
bios_uuid	string	The BIOS UUID of the asset.	optional
manufacturer_tpm_id	string	The manufacturer's unique identifier of the Trusted Platform Module (TPM) associated with the asset.	optional
mcafee_epo_guid	string	The unique identifier of the asset in McAfee ePolicy Orchestrator (ePO) . For more information, see the McAfee documentation.	optional
mcafee_epo_agent_guid	string	The unique identifier of the McAfee ePO agent that identified the asset. For more information, see the McAfee documentation.	optional
symantec_ep_hardware_key	string	The hardware key for the asset in Symantec Endpoint Protection.	optional
qualys_asset_id	string	The Asset ID of the asset in Qualys. For more information, see the Qualys documentation. **Note:** Tenable is enabling Qualys asset import for customers in a rolling fashion. For more information, contact your Tenable representative.	optional
qualys_host_id	string	The Host ID of the asset in Qualys. For more information, see the Qualys documentation. **Note:** Tenable is enabling Qualys asset import for customers in a rolling fashion. For more information, contact your Tenable representative.	optional
servicenow_sys_id	string	The unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.	optional

gcp_project_id	string	The customized name of the project to which the virtual machine instance belongs in Google Cloud Platform (GCP). For more information, see Creating and Managing Projects in the GCP documentation.	optional
gcp_zone	string	The zone where the virtual machine instance runs in GCP. For more information, see Regions and Zones in the GCP documentation.	optional
gcp_instance_id	string	The unique identifier of the virtual machine instance in GCP.	optional
azure_vm_id	string	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see Accessing and Using Azure VM Unique ID in the Microsoft Azure documentation.	optional
azure_resource_id	string	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.	optional
aws_availability_zone	string	The availability zone where Amazon Web Services hosts the virtual machine instance, for example, "us-east-1a". Availability zones are subdivisions of AWS regions. For more information, see Regions and Availability Zones in the AWS documentation.	optional
aws_ec2_instance_id	string	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.	optional
aws_ec2_instance_ami_id	string	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.	optional
aws_ec2_instance_group_name	array	The virtual machine instance's group in AWS.	optional
aws_ec2_instance_	string	The state of the virtual machine instance in AWS at the time of the scan.	optional

state_name			
aws_ec2_instance_type	string	The type of instance in AWS EC2.	optional
aws_ec2_name	string	The name of the virtual machine instance in AWS EC2.	optional
aws_ec2_product_code	array	The product code associated with the AMI used to launch the virtual machine instance in AWS EC2.	optional
aws_owner_id	string	The canonical user identifier for the AWS account associated with the asset, for example, "79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be". For more information, see AWS Account Identifiers in the AWS documentation.	optional
aws_region	string	The region where AWS hosts the virtual machine instance, for example, "us-east-1". For more information, see Regions and Availability Zones in the AWS documentation.	optional
aws_subnet_id	string	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.	optional
aws_vpc_id	string	The unique identifier for the virtual public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.	optional

Object Example

```
{
  "tenable_uuid": "6edeee7cf86e47adb4f6f61cb9184eaa",
  "mac_address": [
    {
      "00-00-5E-00-53-00",
      "00-00-5E-00-53-FF"
```

```
    }
  ],
  "netbios_name": "COMPUTERNAME1",
  "fqdn": [
    {
      "example.com"
    }
  ],
  "ip_address": [],
  "ipv4": [
    {
      "172.204.81.57",
      "172.82.157.177"
    }
  ],
  "ipv6": [
    {
      "2001:DB8:1234:1234/32"
    }
  ],
  "hostname": [
    {
      "rhel6x86.target.example.com"
    }
  ],
  "operating_system": [
    {
          "Linux Kernel 2.6.32-71.el6.i686 on Red Hat Enterprise Linux Server
release 6.0 (Santiago)"
       }
  ],
  "ssh_fingerprint": "423fa07b4a12f386149e09ea10021a89",
  "bios_uuid": "423ee0f1-0032-700c-afd7-a686d88da63e",
```

```
  "manufacturer_tpm_id": null,
  "mcafee_epo_guid": null,
  "mcafee_epo_agent_guid": null,
  "symantec_ep_hardware_key": null,
  "qualys_asset_id": null,
  "qualys_host_id": null,
  "servicenow_sys_id": null,
  "gcp_project_id": null,
  "gcp_zone": null,
  "gcp_instance_id": null,
  "azure_vm_id": null,
  "azure_resource_id": null,
  "aws_availability_zone": null,
  "aws_ec2_instance_id": null,
  "aws_ec2_instance_ami_id": null,
  "aws_ec2_instance_group_name": [],
  "aws_ec2_instance_state_name": null,
  "aws_ec2_instance_type": null,
  "aws_ec2_name": null,
  "aws_ec2_product_code": [],
  "aws_owner_id": null,
  "aws_region": null,
  "aws_subnet_id": null,
  "aws_vpc_id": null
}
```

Network Interface Objects

Tenable.io returns network interface objects when you retrieve asset data from Tenable.io. For the complete list of attributes included in an asset export chunk, see Asset Export Attributes.

Object Syntax

```
{
  "name": {string},
  "mac_address": {array},
  "ipv4": {array},
  "ipv6": {array},
  "fqdn": {array}
}
```

Object Attributes

The table below defines the attributes of a network interface object.

Attribute	Type	Description
name	string	The name of the interface.
mac_address	array	The MAC addresses of the interface.
ipv4	array	One or more IPv4 addresses belonging to the interface.
ipv6	array	One or more IPv6 addresses belonging to the interface.
fqdn	array	One or more FQDN belonging to the interface.

Object Example

```
{
  "name": "enccw0.0.1234"
  "mac_address": [
```

```
    {
      "00-00-5E-00-53-00",
      "00-00-5E-00-53-FF"
    }
  ],
  "ipv4": [
    {
      "172.204.81.57",
      "172.82.157.177"
    }
  ],
  "ipv6": [
    {
      "2001:DB8:1234:1234/32"
       }
  ],
  "fqdn": [
    {
      "example.com"
    }
  ]
}
```

Source Objects

Tenable.io returns source objects when you list asset details in Tenable.io.

Object Syntax

```
{
  "name": {string},
  "first_seen": {string},
  "last_seen": {string}
}
```

Object Attributes

The table below defines the attributes of a source object.

Attribute	Type	Description
name	string	The name of the entity that reported the asset details. Sources can include sensors, connectors, and API imports. Source names can be customized by your organization (for example, you specify a name when you import asset records). If your organization does not customize source names, system-generated names include: • AWS—You obtained the asset data from an Amazon Web Services connector. • NESSUS_AGENT—You obtained the asset data obtained from a Nessus agent scan. • PVS—You obtained the asset data from a Nessus Network Monitor (NNM) scan. • NESSUS_SCAN—You obtained the asset data from a Nessus scan. • WAS—You obtained the asset data from a Tenable.io Web Application Scanning scan.
first_	string	The ISO timestamp when the source first reported the asset.

seen		
last_seen	array	The ISO timestamp when the source last reported the asset.

Object Example

```
{
  "name": "NESSUS_SCAN",
  "first_seen": "2015-05-06T17:48:46.000Z",
  "last_seen": "2015-05-06T17:48:46.000Z"
}
```

Tag Objects

Tenable.io API responses can include detailed or brief tag objects.

Detailed Tag Object

Tenable.io returns this object in response messages from the /tags endpoints.

Detailed Tag Object Syntax

```
{
  "uuid": {string},
  "created_at": {string},
  "created_by": {string},
  "updated_at": {string},
  "updated_by": {string},
  "category_uuid": {string},
  "value": {string},
  "description": {string},
  "type": {string},
  "category_name": {string},
  "category_description": {string}
}
```

Detailed Tag Object Attributes

Attribute	Type	Description
uuid	string	The UUID of the tag. Use this UUID when you want to query on the category:tag pair.
created_at	string	An ISO timestamp indicating the date and time on which the tag value was created, for example, `2018-08-09T13:51:17.243Z`.
created_by	string	The name of the user who created the tag value.
updated_	string	An ISO timestamp indicating the date and time on which the tag value was

at		last updated, for example, `2018-08-09T13:51:17.243Z`.
updated_by	string	The name of the user who last updated the tag value.
category_uuid	string	The UUID of the tag category associated with the tag value.
description	string	The description of the tag value.
value	string	The tag value. Must be unique within the category.
type	string	The tag type: • `static`—A user must manually apply the tag to an asset. You can use the Tenable.io API to create and assign static tags to assets. • `dynamic`—Tenable.io automatically applies the tag based on asset attribute rules. You can use the Tenable.io user interface to create dynamic asset tags. For more information, see the *Tenable.io Vulnerability Management User Guide*.
category_name	string	The name of the category associated with the tag value.
category_description	string	The description of the category associated with the tag value.

Detailed Tag Object Example

```
{
  "uuid": "0a6c1176-4c03-4776-a60a-048021a48799",
  "created_at": "2018-10-30T15:39:16.687Z",
  "created_by": "user3@example.com",
  "updated_at": "2018-10-30T15:39:16.687Z",
  "updated_by": "user3@example.com",
  "category_uuid": "8981f2d8-a043-4a74-ad78-e6a73b13ccaf",
  "value": "Seattle",
  "description": "",
  "type": "static",
```

```
  "category_name": "location",
  "category_description": "Asset location",
}
```

Brief Tag Object

Tenable.io returns this object in asset chunk downloads when you retrieve asset data.

Brief Tag Object Syntax

```
{
  "uuid": {string},
  "key": {string},
  "value": {string},
  "added_by": {string},
  "added_at": {string}
}
```

Brief Tag Object Attributes

The table below defines the attributes of a brief asset tag object.

Attribute	Type	Description
uuid	string	The UUID of the tag.
key	string	The tag category (the first half of the category:value pair).
value	string	The tag value (the second half of the category:value pair).
added_by	string	The UUID of the user who assigned the tag to the asset.
added_at	string	The ISO timestamp when the tag was assigned to the asset.

Brief Tag Object Example

```
{
  "uuid": "6ee5761f-5c99-434b-aecb-e09b755921b7",
  "key": "Geographic Area",
  "value": "APAC",
  "added_by": "e7ecb50b-1330-4a8c-b8e5-ee00ec8c46f8",
  "added_at": "2018-02-13T14:53:13.817Z"
}
```

Vulnerabilities

You can use the Tenable.io API to perform the following tasks:

- Retrieve Vulnerability Data from Tenable.io
- Generate the Vulnerability Export File
- Query for Vulnerability Export Status and Chunk ID Information
- Download Vulnerability Export Chunks

Retrieve Vulnerability Data from Tenable.io

User Permissions: Administrator (64)

The vulnerability export APIs provide the ability to retrieve all vulnerabilities on each asset, including the vulnerability state, for integration into third-party tools. With these APIs, you can perform a large initial synchronization of Tenable.io with a third-party tool. You can then retrieve differentials to update on a regular basis. For example, you can use the vulnerability export APIs to retrieve all vulnerabilities that are currently active in your environment and integrate them with a ticketing system. You can then leverage the differential functionality to:

- Retrieve newly discovered vulnerabilities and create new tickets.
- Retrieve fixed vulnerabilities to automatically close open tickets.

The Tenable.io API exports vulnerability data in data chunks. You can configure chunk size to maximize network performance and satisfy data ingestion requirements for third-party applications.

To retrieve vulnerability data using the Tenable.io API, Tenable recommends the following approach:

1. Generate the export file.
2. Query for the export generation status and chunk identification information.
3. Download completed export chunks.

Generate the Vulnerability Export File

User Permissions: Administrator (64)

To generate the export file, use the API endpoint described below.

Note:

- *The first time you generate a vulnerabilities export file*, you can omit `filters` parameters to export all current data, or if appropriate use `filters` parameters to limit by date and other attributes.
- *Every time you export after that*, Tenable recommends that you specify parameters for a differential export, with the `filters` parameters set to the time you last exported vulnerability data from Tenable.io.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
POST https://cloud.tenable.com/vulns/export
```

Request Path Parameters

None.

Request Path Example

See "Request Path Syntax."

Request Body Syntax

```
{
  "num_assets": {integer},
```

```
  "filters": {
    "cidr_range": {string},
    "first_found": {long},
    "last_found": {long},
    "last_fixed": {long},
    "plugin_family": [
      {string},
      {string}
    ],
    "severity": [
      {string},
      {string}
    ],
    "since": {long},
    "state": [
      {string},
      {string}
    ],
    "tag.category": [
      {string},
      {string}
    ]
  }
}
```

Request Body Attributes

Parameter	Object Parameter	Type	Value	Required?
num_assets	–	integer	Specifies the maximum number of vulnerabilities per exported chunk. This number does not represent the number of assets per chunk. Instead, it is equal	required

			to the number of assets times the number of vulnerabilities on each asset. The range of supported chunk sizes is a minimum of 50 (the default size) to a maximum of 5,000. If you specify a value outside this range, the system uses the upper- or lower -bound value.	
filters	cidr_range	string	Restricts the export to vulnerabilities on assets assigned an IP address within the specified CIDR range. For example, 0.0.0.0/0 restricts the search to 0.0.0.1 and 255.255.255.254.	optional
	first_found	long	The start date (in Unix time) for the range of vulnerability data you want to export, based on when a scan first found a vulnerability on an asset. When using this filter, make sure the request message also contains the `state` filter set to `open`. If the `state` filter specifies a value other than `open`, the request effectively fails, because Tenable.io cannot find any records that match the conflicting criteria.	optional
	last_found	long	The start date (in Unix time) for the range of vulnerability data you want to export, based on when a scan last found a vulnerability on an asset. When using this filter, make sure the request message also contains the `state` filter set to `reopened`. If the `state` filter specifies a value other than `reopened`, the request effectively fails, because Tenable.io cannot find any records that match the conflicting criteria.	optional

	last_fixed	long	The start date (in Unix time) for the range of vulnerability data you want to export, based on when the vulnerability state was changed to fixed. Tenable.io updates the vulnerability state to fixed when a scan no longer detects a previously detected vulnerability on the asset. When using this filter, make sure your request message also contains the `state` filter set to `fixed`. If the `state` filter specifies a value other than `fixed`, the request effectively fails, because Tenable.io cannot find any records that match the conflicting criteria.	optional
	plugin_family	array	Limits the vulnerabilities you want to include in the export by plugin family. This parameter value is case-sensitive. Use the family names (including capitalization) specified here: Plugins. If your request omits this parameter, the export includes all vulnerabilities, regardless of plugin family.	optional
	severity	array	Specifies the severity of the vulnerabilities to include in the export. Defaults to all severity levels. The severity of a vulnerability is defined using the Common Vulnerability Scoring System (CVSS) base score. Supported array values are: • `info`—The vulnerability has a CVSS score of 0. • `low`—The vulnerability has a CVSS score between 0.1 and 3.9.	optional

			• `medium`—The vulnerability has a CVSS score between 4.0 and 6.9. • `high`—The vulnerability has a CVSS score between 7.0 and 9.9. • `critical`—The vulnerability has a CVSS score of 10.0.	
	since	long	Specifies the start date (in Unix time) for the range of data you want to export. Use this filter in conjunction with the `state` filter as follows: • If the `state` filter is set to `open`, the export includes data for vulnerabilities that were first seen on or after the `since` date you specify. • If the `state` filter is set to `reopened`, the export includes data for vulnerabilities that were last seen on or after the `since` date you specify. • If the `state` filter is set to `fixed`, the export includes data for vulnerabilities that were fixed on or after the `since` date you specify. • If you do not include the `state` filter in your request, the export includes data for `open` vulnerabilities that were first seen on or after the `since` date you specify, **AND** `reopened` vulnerabilities that were last seen on or after the `since` date you specify. **Note:** This filter cannot be used in con-	optional

			junction with the `first_found`, `last_found`, or `last_fixed` filters.	
	state	array	Specifies the state of the vulnerabilities you want the export to include. Supported, case-insensitive values are: • open—The vulnerability is currently present on a host. • `reopened`—The vulnerability was previously marked as fixed on a host, but has returned. • `fixed`—The vulnerability was present on a host, but is no longer detected. If your request omits this parameter, the export includes default states `open` and `reopened` only.	required if filters include `first_found`, `last_found`, or `last_fixed`
	tag.*category*	array	Returns vulnerabilities on assets with the specified asset tags. The filter is defined as "tag", a period ("."), and the tag category name. For example, `tag.Location`. The value of the filter is an array of tag values, for example, `Headquarters`. For more information about tags, see Tenable.io Vulnerability Management User Guide.	optional

Request Body Example 1: Since Only

```
{
  "num_assets": 100,
  "filters": {
```

```
    "severity": [
      "low",
      "medium",
      "high",
      "critical"
      ],
    "since": 1546300800
  }
}
```

In this example, the request message contains a `since` filter specifying Jan 1, 2019, and does not contain a `state` filter.

The export includes vulnerabilities that meet the following criteria:

- The `state` attribute in the vulnerability record is open **AND** the `first_found` attribute in the vulnerability record is 1/1/19 or later.
- The `state` attribute in the vulnerability is `reopened` **AND** the `last_found` attribute in the vulnerability record is 1/1/19 or later.

The export omits any vulnerabilities where the `state` attribute in the vulnerability record is `fixed`.

Request Body Example 2: Since and State

```
{
  "num_assets": 100,
  "filters": {
    "severity": [
      "low",
      "medium",
      "high",
      "critical"
      ],
    "since": 1546300800,
    "state": [
```

```
      "open",
      "reopened",
      "fixed"
    ]
  }
}
```

In this example, the request message includes both the `since` and `state` filters.

The export includes only vulnerabilities where the `state` attribute in the vulnerability record is either `open`, `reopened`, or `fixed`. **AND** the `since` attribute in the vulnerability record is 1/1/19 or later.

Request Body Example 3: Last_fixed and Correct State

```
{
  "num_assets": 100,
  "filters": {
    "severity": [
      "low",
      "medium",
      "high",
      "critical"
      ],
    "last_fixed": 1546300800,
    "state": [
      "fixed"
    ]
  }
}
```

In this example, the request message contains both the `last_fixed` and `state` parameters.

The export includes only vulnerabilities where the `state` attribute in the vulnerability record is `fixed` **AND** the `since` attribute in the vulnerability record is 1/1/19 or later.

Request Body Example 4: Tags

```
{
  "num_assets": 100,
  "filters": {
    "severity": [
      "low",
      "medium",
      "high",
      "critical"
      ],
    "tag.Location": "Headquarters"
  }
}
```

In this example, the export includes only vulnerabilities on assets that you assigned the `Location:Headquarters` tag.

HTTP Response

Response Codes

Status	Description
200	Returned if Tenable.io successfully queues the export request. For more information, see "Response Body Syntax."
400	Returned if any of the filters in the request is invalid.
403	Returned if you do not have permission to export vulnerabilities.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "export_uuid": {string}
}
```

Response Body Attributes

Attribute	Type	Description
export_uuid	string	The unique identifier of the export request.

Response Body Example

```
{
  "export_uuid": "a483adf8-24e3-4c7f-818a-6867b02310dd"
}
```

Reference Guide

https://cloud.tenable.com/api#/resources/exports/vulns-request-export

Examples

- exports (library)
- exports (SDK)

Query for Vulnerability Export Status and Chunk ID Information

User Permissions: Administrator (64)

Note: When generating the vulnerabilities export, Tenable.io processes the chunks in parallel, so the chunks may not complete in order.

To query for the status of the export and chunk identification information, use the API endpoint described below.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/vulns/export/{export_uuid}/status
```

Request Path Parameters

Attribute	Type	Description	Required?
export_uuid	string	The unique identifier of an export request. This value corresponds to the value returned in the /vulns/export response message.	required

Request Path Example

```
GET https://cloud.tenable.com/vulns/export/a483adf8-24e3-4c7f-818a-6867b02310dd/status
```

Request Body Syntax

None.

HTTP Response

Response Codes

Status	Description
200	Returned if Tenable.io successfully retrieves the export status. For more information, see "Response Body Syntax."
403	Returned if you do not have permission to view the export status.
404	Returned if an export with the specified UUID is not found.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

```
{
  "status": {string},
  "chunks_available": [{integer},{integer}...],
  "chunks_failed": [{integer},{integer}...],
  "chunks_cancelled": [{integer},{integer}...]
}
```

Response Body Attributes

Attribute	Type	Description
status	string	The status of the export request. Possible values include: • QUEUED— Tenable.io has queued the export request until it completes other requests currently in process. • PROCESSING—Tenable.io has started processing the export request. • FINISHED—Tenable.io has completed processing the export request. The list of chunks is complete.

		• ERROR—Tenable.io encountered an error while processing the export request. **Tip:** If you encounter an ERROR status, Tenable recommends that you retry the request. If the status persists on retry, contact Support.
chunks_available	array	A comma-separated list of completed chunks available for download.
chunks_failed	array	A comma-separated list of chunks for which the export process failed. If a chunk fails processing, submit the export request again. If the chunk continues to fail, contact Support.
chunks_cancelled	array	A comma-separated list of chunks for which the export process was cancelled. If a chunk fails processing, Tenable.io automatically cancels all subsequent chunks queued for export in the same request.

Response Body Example

```
{
  "status": "FINISHED",
  "chunks_available": [
    1,
    2
    ],
  "chunks_failed": [],
  "chunks_cancelled": []
}
```

Reference Guide

https://cloud.tenable.com/api#/resources/exports/vulns-export-status

Examples

- exports (library)
- exports (SDK)

Download Vulnerability Export Chunks

User Permissions: Administrator (64)

To download available export chunks, use the API endpoint described below.

HTTP Request

Note: To authenticate your request, be sure to include API keys in the HTTP header of the request. For more information, see Authorization.

Request Path Syntax

```
GET https://cloud.tenable.com/vulns/export/{export_uuid}/chunks/{chunk_id}
```

Request Path Parameters

Parameter	Type	Description	Required
export_uuid	string	The UUID of the export request.	required
chunk_id	integer	The ID of the asset chunk you want to export.	required

Request Path Example

```
GET https://cloud.tenable.com/vulns/export/a483adf8-24e3-4c7f-818a-6867b02310dd/chunks/1
```

Request Body Syntax

None.

HTTP Response

Response Codes

Status	Description
200	Returned if the file is downloaded successfully. For more information, see "Response Body Syntax."
400	Returned if the chunk ID is invalid or the chunk is not ready for download.
403	Returned if you do not have permission to export vulnerabilities.
404	Returned if a chunk with the specified export chunk is not found.
429	Returned if you attempt to send too many requests in a specific period of time. For more information, see Rate Limiting.

Response Body Syntax

Note: The response attributes listed below represent all available attributes. The API response body excludes an attribute if the attribute is empty in the vulnerability record. For a description of the attributes, see Vulnerability Export Attributes.

```
{
  "asset": [
    "agent_uuid": {string},
    "bios_uuid": {string},
    "device_type": {string},
    "fqdn": {string},
    "hostname": {string},
    "uuid": {string},
    "ipv4": {string},
    "ipv6":  {string},
    "last_authenticated_results":  {string},
    "last_unauthenticated_results":  {string},
    "mac_address": {string},
    "netbios_name":  {string},
    "netbios_workgroup": {string},
    "operating_system":  {string},
    "tracked":  {string},
```

```
    ],
  "output": {string},
  "plugin": [
    "bid":  {string},
    "canvas_package": {string},
    "checks_for_default_account": {string},
    "checks_for_malware": {string},
    "cpe": {string},
    "cve": {string},
    "cvss3_base_score": {string},
    "cvss3_temporal_score": {string},
    "cvss3_temporal_vector": {
      "Exploitability":  {string},
      "RemediationLevel": {string},
      "ReportConfidence": {string},
      },
    "cvss3_vector": {
      "AccessComplexity": {string},
      "AccessVector": {string},
      "Authentication": {string},
      "Availability-Impact": {string},
      "Confidentiality-Impact": {string},
      "Integrity-Impact": {string},
      },
    "cvss_base_score": {string},
    "cvss_temporal_score": {string},
    "cvss_temporal_vector": {
      "Exploitability": {string},
      "RemediationLevel": {string},
      "ReportConfidence": {string},
      },
    "cvss_vector": {
      "AccessComplexity": {string},
```

```
    "AccessVector": {string},
    "Authentication": {string},
    "Availability-Impact": {string},
    "Confidentiality-Impact": {string},
    "Integrity-Impact": {string},
    },
  "d2_elliot_name": {string},
  "description": {string},
  "exploit_available": {string},
  "exploit_framework_canvas": {string},
  "exploit_framework_core": {string},
  "exploit_framework_d2_elliot": {string},
  "exploit_framework_exploithub": {string},
  "exploit_framework_metasploit": {string},
  "exploitability_ease": {string},
  "exploited_by_malware": {string},
  "exploited_by_nessus": {string},
  "exploithub_sku": {string},
  "family": {string},
  "family_id": {string},
  "has_patch": {string},
  "id": {string},
  "in_the_news": {string},
  "metasploit_name": {string},
  "ms_bulletin": {string},
  "name": {string},
  "patch_publication_date": {string},
  "modification_date": {string},
  "publication_date": {string},
  "risk_factor": {string},
  "see_also": {string},
  "solution": {string},
  "stig_severity": {string},
```

```
    "synopsis": {string},
    "type": {string},
    "unsupported_by_vendor": {string},
    "usn": {string},
    "version": {string},
    "vuln_publication_date": {string},
    "xrefs": {string},
    ],
  "port": [
    "port": {string},
    "protocol": {string},
    "service": {string},
    ],
  "recast_reason": {string},
  "recast_rule_uuid": {string},
  "scan": [
    "completed_at": {string},
    "schedule_uuid": {string},
    "started_at": {string},
    "uuid": {string},
    ],
  "severity": {string},
  "severity_id": {string},
  "severity_default_id": {string},
  "severity_modification_type": {string},
  "first_found": {string},
  "last_fixed": {string},
  "last_found": {string},
  "state": {string},
}
```

Response Body Attributes

See Vulnerability Export Attributes.

Response Body Example


```
[
  {
    "asset": {
      "fqdn":"example.com",
      "hostname":"172.106.217.225",
      "uuid":"150dee8f-6090-4a9c-907c-54a1c39ddab0",
      "ipv4":"172.156.65.8",
      "operating_system":["Apple Mac OS X 10.5.8"],
      "tracked":true
      },
    "output":"The observed version of Google Chrome is : \n
Chrome/21.0.1180.90",
    "plugin":{
      "cve":[
        "CVE-2016-1620",
        "CVE-2016-1614",
        "CVE-2016-1613",
        "CVE-2016-1612",
        "CVE-2016-1618",
        "CVE-2016-1617",
        "CVE-2016-1616",
        "CVE-2016-1615",
        "CVE-2016-1619"
        ],
      "cvss_base_score":9.3,
      "cvss_temporal_score":6.9,
      "cvss_temporal_vector":{
      "exploitability": "Unproven",
      "remediation_level":"Official-fix",
      "report_confidence":"Confirmed",
      "raw":"E:U/RL:OF/RC:C"
      },
```

```
      "cvss_vector":{
        "access_complexity":"Medium",
        "access_vector":"Network",
        "authentication":"None required",
        "availability_impact":"Complete",
        "confidentiality_impact":"Complete",
        "integrity_impact":"Complete","raw":"AV:N/AC:M/Au:N/C:C/I:C/A:C"
        },
      "description":"The version of Google Chrome on the remote host is
prior to 48.0.2564.82 and is affected by the following vulnerabilities
:\n\n - An unspecified vulnerability exists in Google V8 when handling
compatible receiver checks hidden behind receptors.  An attacker can
exploit this to have an unspecified impact.  No other details are
available. (CVE-2016-1612)\n - A use-after-free error exists in 'PDFium'
due to improper invalidation of 'IPWL_FocusHandler' and 'IPWL_Provider'
upon destruction.  An attacker can exploit this to dereference already
freed memory, resulting in the execution of arbitrary code. (CVE-2016-
1613)\n - An unspecified vulnerability exists in 'Blink' that is related
to the handling of bitmaps.  An attacker can exploit this to access
sensitive information.  No other details are available. (CVE-2016-1614)\n
- An unspecified vulnerability exists in 'omnibox' that is related to
origin confusion.  An attacker can exploit this to have an unspecified
impact.  No other details are available. (CVE-2016-1615)\n - An
unspecified vulnerability exists that allows an attacker to spoof a
displayed URL.  No other details are available. (CVE-2016-1616)\n - An
unspecified vulnerability exists that is related to history sniffing with
HSTS and CSP. No other details are available. (CVE-2016-1617)\n - A flaw
exists in 'Blink' due to the weak generation of random numbers by the
ARC4-based random number generator.  An attacker can exploit this to gain
access to sensitive information.  No other details are available. (CVE-
2016-1618)\n - An out-of-bounds read error exists in 'PDFium' in file 'fx_
codec_jpx_opj.cpp' in the 'sycc4{22,44}_to_rgb()' functions. An attacker
can exploit this to cause a denial of service by crashing the application
```

```
linked using the library. (CVE-2016-1619)\n - Multiple vulnerabilities
exist, the most serious of which allow an attacker to execute arbitrary
code via a crafted web page. (CVE-2016-1620)\n - A flaw in 'objects.cc' is
triggered when handling cleared 'WeakCells', which may allow a context-
dependent attacker to have an unspecified impact. No further details have
been provided. (CVE-2016-2051)",
      "family":"Web Clients",
      "family_id":1000020,
      "has_patch":false,
      "id":9062,
      "name":"Google Chrome < 48.0.2564.82 Multiple Vulnerabilities",
      "risk_factor":"HIGH",
      "see_also":
        [
          "http://googlechromereleases.blogspot.com/2016/01/beta-channel-
update_20.html"
        ],
      "solution":"Update the Chrome browser to 48.0.2564.82 or later.",
      "synopsis":"The remote host is utilizing a web browser that is
affected by multiple vulnerabilities."
      },
    "port":{
      "port":0,
      "protocol":"TCP"
      },
  "scan":{
      "completed_at":"2018-05-23T20:59:47Z",
      "schedule_uuid":"413765fb-e941-7eea-ca8b-
0a79182a2806e1b6640fe8a2217b",
      "started_at":"2018-05-23T20:59:47Z",
      "uuid":"e2c070ae-ec37-d9ff-f003-2e89b7e5e1ab8af3a9957a077904"
      },
    "severity":"high",
```

```
    "severity_id":3,
    "severity_default_id":3,
    "severity_modification_type":"NONE",
    "first_found":"2018-05-23T20:59:47Z",
    "last_found":"2018-05-23T20:59:47Z",
    "state":"OPEN"
    },
  {"asset": ...
  }
]
```

Reference Guide

https://cloud.tenable.com/api#/resources/exports/vulns-download-chunk

Examples

- exports (library)
- exports (SDK)

Vulnerability Export Attributes

The table below defines all available attributes of a vulnerability export data chunk. Export chunks do not include an attribute if that attribute is empty in the vulnerability record.

Note: Attribute values that correspond CVSS codes are described fully in the following documents:

- CVSSv2 codes in *A Complete Guide to the Common Vulnerability Scoring System, Version 2.0*
- CVSSv3 codes in the *Common Vulnerability Scoring System v3.0: Specification Document*.

Attribute	Object Attribute	Value	Description
asset			
agent_uuid	–	string	The UUID of the agent that performed the scan where the vulnerability was found.
bios_uuid	–	string	The BIOS UUID of the asset where the vulnerability was found.
device_type	–	string	The type of asset where the vulnerability was found.
fqdn	–	string	The fully-qualified domain name of the asset where a scan found the vulnerability.
hostname	–	string	The host name of the asset where a scan found the vulnerability.
uuid	–	string	The UUID of the asset where a scan found the vulnerability.
ipv6	–	string	The IPv6 address of the asset where a scan found the vulnerability.
last_authenticated_results	–	date	The last date credentials were used successfully to scan the asset.
last_unauthenticated_results	–	date	The last date when the asset was scanned without using credentials
mac_address	–	string	The MAC address of the asset where a scan

			found the vulnerability.
netbios_name	–	string	The NETBIOS name of the asset where a scan found the vulnerability.
netbios_work-group	–	string	The NETBIOS workgroup of the asset where a scan found the vulnerability.
operating_sys-tem	–	string	The operating system of the asset where a scan found the vulnerability.
tracked	–	boolean	A value specifying whether Tenable.io tracks the asset in the asset management system. Tenable.io still assigns untracked assets identifiers in scan results, but these identifiers change with each new scan of the asset. This parameter is relevant to PCI-type scans and in certain cases where there is not enough information in a scan to identify the asset. Untracked assets appear in the scan history, but do not appear in workbenches or reports.
output			
–	–	string	The text output of the Nessus scanner.
plugin			
bid	–	integer	The Bugtraq ID for the plugin.
canvas_package	–	string	The name of the CANVAS exploit pack that includes the vulnerability.
checks_for_ default_account	–	boolean	A value specifying whether the plugin checks for default accounts.
checks_for_mal-ware	–	boolean	A value specifying whether the plugin checks for malware.
cpe	–	string	The Common Platform Enumeration (CPE) number for the plugin.
cve	–	string	The Common Vulnerability and Exposure

			(CVE) ID for the plugin.
cvss3_base_score	–	double	The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
cvss3_temporal_score	–	double	The CVSSv3 temporal score (characteristics of a vulnerability that change over time but not among user environments).
cvss3_temporal_vector	Exploitability	string	The CVSSv2 Exploit Maturity Code (E) for the vulnerability the plugin covers. Possible values are: • `Unproven`—Corresponds to the Unproven (U) value for the E metric. • `Proof-of-concept`—Corresponds to the Proof-of-Concept (POC) value for the E metric. • `Functional`—Corresponds to the Functional (F) value for the E metric. • `High`—Corresponds to the High (H) value for the E metric. • `Not-defined`—Corresponds to the Not Defined (ND) value for the E metric.
	RemediationLevel	string	The CVSSv3 Remediation Level (RL) temporal metric for the vulnerability the plugin covers. The metric value can be (O) Official Fix, (T) Temporary Fix, (W) Workaround, (U) Unavailable, or (X) Not Defined.
	ReportConfidence	string	The CVSSv3 Report Confidence (RC) temporal metric for the vulnerability the plugin covers. The metric value can be (U) Unknown, (R) Reasonable, (C) Confirmed,

			or (X) Not Defined.
cvss3_vector	AccessComplexity	string	The CVSSv3 Access Complexity (AC) metric for the vulnerability the plugin covers. The metric value can be (L) Low, (M) Medium, or (H) High.
	AccessVector	string	The CVSSv2 Attack Vector (AV) metric for the vulnerability the plugin covers. Possible values include: • `Network`—Corresponds to the Network (N) value for the AV metric. • `Adjacent Network`—Corresponds to the Adjacent Network (A) value for the AV metric. • `Local`—Corresponds to the Local (L) value for the AV metric.
	Authentication	string	The CVSSv2 Authentication (Au) metric for the vulnerability the plugin covers. Possible values include: • `None required`—Corresponds to the None (N) value for the Au metric. • `Requires-single-instance`—Corresponds to the Single (S) value for the Au metric. • `Requires-multiple-instances`—Corresponds to the Multiple (M) value for the Au metric.
	Availability-Impact	string	The CVSSv2 availability impact metric for the vulnerability the plugin covers. The metric value can be (N) None, (L) Low, or (H) High.
	Confidentiality-	string	The CVSSv3 confidentiality impact metric of

	Impact		the vulnerability the plugin covers to the vulnerable component. The metric value can be (H) High, (L) Low, or (N) None.
	Integrity-Impact	string	The CVSSv3 integrity impact metric for the vulnerability the plugin covers. The metric value can be (N) None, (L) Low, or (H) High.
cvss_base_score	–	float	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
cvss_temporal_score	–	float	The CVSSv2 temporal score (characteristics of a vulnerability that change over time but not among user environments).
cvss_temporal_vector	Exploitability	string	The CVSSv2 Exploitability (E) temporal metric for the vulnerability the plugin covers. The metric value can be (U) Unproven, (POC) Proof-of-Concept, (F) Functional, (H) High, or (ND) Not Defined.
	RemediationLevel	string	The CVSSv2 Remediation Level (RL) temporal metric for the vulnerability the plugin covers. The metric value can be (OF) Official Fix, (TF) Temporary Fix, (W) Workaround, (U) Unavailable, or (ND) Not Defined.
	ReportConfidence	string	The CVSSv2 Report Confidence (RC) temporal metric for the vulnerability the plugin covers. The metric value can be (UC) Unconfirmed, (UR) Uncorroborated, (C) Confirmed, or (ND) Not Defined.
cvss_vector	AccessComplexity	string	The CVSSv2 Access Complexity (AC) metric for the vulnerability the plugin covers. The metric value can be (L) Low, (M) Medium, or (H) High.
	AccessVector	string	The CVSSv2 Access Vector (AV) metric for

			the vulnerability the plugin covers. The metric value can be (L) Local, (A) Adjacent Network, or (N) Network.
	Authentication	string	The CVSSv2 Authentication (Au) metric for the vulnerability the plugin covers. The metric value can be (N) None, (S) Single, or (M) Multiple.
	Availability-Impact	string	The CVSSv2 availability impact metric for the vulnerability the plugin covers. The metric value can be (N) None, (P) Partial, or (C) Complete.
	Confidentiality-Impact	string	The CVSSv2 confidentiality impact metric for the vulnerability the plugin covers. The metric value can be (N) None, (P) Partial, or (C) Complete.
	Integrity-Impact	string	The CVSSv2 integrity impact metric for the vulnerability the plugin covers. The metric value can be (N) None, (P) Partial, or (C) Complete.
d2_elliot_name	–	string	The name of the exploit in the D2 Elliot Web Exploitation framework.
description	–	string	Full text description of the vulnerability.
exploit_available	–	boolean	A value specifying whether a public exploit exists for the vulnerability.
exploit_framework_canvas	–	boolean	A value specifying whether an exploit exists in the Immunity CANVAS framework.
exploit_framework_core	–	boolean	A value specifying whether an exploit exists in the CORE Impact framework.
exploit_framework_d2_elliot	–	boolean	A value specifying whether an exploit exists in the D2 Elliot Web Exploitation framework.
exploit_frame-	–	boolean	A value specifying whether an exploit exists

work_exploithub			in the ExploitHub framework.
exploit_framework_metasploit	–	boolean	A value specifying whether an exploit exists in the Metasploit framework.
exploitability_ease	–	string	Description of how easy it is to exploit the issue.
exploited_by_malware	–	boolean	The vulnerability discovered by this plugin is known to be exploited by malware.
exploited_by_nessus	–	boolean	A value specifying whether Nessus exploited the vulnerability during the process of identification.
exploithub_sku	–	string	The SKU number of the exploit in the ExploitHub framework.
family	–	string	The family to which plugin belongs.
family_id	–	integer	The ID of the plugin family.
has_patch	–	boolean	A value specifying whether the vendor has published a patch for the vulnerability.
id	–	integer	The ID of the plugin that identified the vulnerability.
in_the_news	–	boolean	This plugin has gotten a lot of media attention (e.g., ShellShock, Meltdown).
metasploit_name	–	string	The name of the related exploit in the Metasploit framework.
ms_bulletin	–	string	The Microsoft security bulletin that the plugin covers.
name	–	string	The name of the plugin that identified the vulnerability.
patch_publication_date	–	date	The date on which the vendor published a patch for the vulnerability.
modification_date	–	date	The date on which the plugin was last modified.

publication_date	–	date	The date on which the plugin was published.
risk_factor	–	string	The risk factor associated with the plugin. Possible values are: `Low`, `Medium`, `High`, or `Critical`.
see_also	–	string	Links to external websites that contain helpful information about the vulnerability.
solution	–	string	Remediation information for the vulnerability.
stig_severity	–	string	Security Technical Implementation Guide (STIG) severity code for the vulnerability.
synopsis	–	string	Brief description of the plugin or vulnerability.
type	–	string	The general type of plugin check (for example, `local` or `remote`).
unsupported_by_vendor	–	boolean	Software found by this plugin is unsupported by the software's vendor (for example, `Windows 95` or `Firefox 3`).
usn	–	string	Ubuntu security notice that the plugin covers.
version	–	string	The version of the plugin used to perform the check.
vuln_publication_date	–	date	The publication date of the plugin.
xrefs	–	string	External references (e.g., `OSVDB`, `Secunia`, or `MS Advisory`).
port			
port	–	string	The port the scanner used to communicate with the asset.
protocol	–	string	The protocol the scanner used to com-

			municate with the asset.
service	–	string	The service the scanner used to communicate with the asset.
recast_reason			
–	–	string	The text that appears in the **Comment** field of the recast rule in the Tenable.io user interface.
recast_rule_uuid			
–	–	string	The UUID of the recast rule that applies to the plugin.
scan			
completed_at	–	date	The date and time in ISO format when the scan completed.
schedule_uuid	–	string	The schedule UUID for the scan that found the vulnerability.
started_at	–	date	The date and time in ISO format when the scan started.
uuid	–	string	The UUID of the scan that found the vulnerability.
severity			
–	–	string	The severity of the vulnerability as defined using the Common Vulnerability Scoring System (CVSS) base score. Possible values are: • `info`—The vulnerability has a CVSS score of 0. • `low`—The vulnerability has a CVSS score between 0.1 and 3.9. • `medium`—The vulnerability has a CVSS

			score between 4.0 and 6.9. • `high`—The vulnerability has a CVSS score between 7.0 and 9.9. • `critical`—The vulnerability has a CVSS score of 10.0.
severity_id			
–	–	string	The code for the severity assigned when a user recast the risk associated with the vulnerability. Possible values are: • 1—The vulnerability has a CVSS score of 0. Corresponds to the "info" severity level. • 2—The vulnerability has a CVSS score between 0.1 and 3.9. Corresponds to the "low" severity level. • 3—The vulnerability has a CVSS score between 4.0 and 6.9. Corresponds to the "medium" severity level. • 4—The vulnerability has a CVSS score between 7.0 and 9.9. Corresponds to the "high" severity level. • 5—The vulnerability has a CVSS score of 10.0. Corresponds to the "critical" severity level.
severity_default_id			
–	–	string	The code for the severity originally assigned to a vulnerability before a user recast the risk associated with the vulnerability. Possible values are the same as for the `severity_id` attribute.

severity_modification_type			
–	–	string	The type of modification a user made to the vulnerability's severity: • none—No modification has been made. • `recasted`— A user in the Tenable.io user interface has recast the risk associated with the vulnerability. • `accepted`—A user in the Tenable.io user interface has accepted the risk associated with the vulnerability. For more information about recast and accept rules, see About Recast Rules in the *Tenable.io Vulnerability Management User Guide*.
first_found			
–	–	date	The date on which the vulnerability was first found on the asset.
last_fixed			
–	–	date	The date on which the vulnerability was last fixed on the asset. Tenable.io updates the vulnerability state to fixed when a scan no longer detects a previously detected vulnerability on the asset.
last_found			
–	–	date	The date on which the vulnerability was last found on the asset.
state			
–	–	string	The state of the vulnerability as determined

			by the Tenable.io state service. Possible values are: • `open`—The vulnerability is currently present on an asset. • `reopened`—The vulnerability was previously marked as fixed on an asset, but has been detected again by a new scan. • `fixed`—The vulnerability was present on an asset, but is no longer detected.