

# ThreatQuotient



## Jamf CDF User Guide

Version 1.0.1

February 05, 2024

### ThreatQuotient

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 ThreatQ Supported

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

- Warning and Disclaimer ..... 3
- Support ..... 4
- Integration Details..... 5
- Introduction ..... 6
- Prerequisites ..... 7
  - Asset Custom Object ..... 7
- Installation..... 10
- Configuration ..... 11
- ThreatQ Mapping..... 13
  - Jamf Mobile Devices ..... 13
  - Jamf Computers ..... 18
    - Jamf Computers Supplemental Feed..... 21
- Average Feed Run..... 30
  - Jamf Mobile Devices ..... 30
  - Jamf Computers ..... 30
- Change Log ..... 31

# Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2024 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

# Support

This integration is designated as **ThreatQ Supported**.

**Support Email:** [support@threatq.com](mailto:support@threatq.com)

**Support Web:** <https://support.threatq.com>

**Support Phone:** 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

# Integration Details

ThreatQuotient provides the following details for this integration:

|                                  |                   |
|----------------------------------|-------------------|
| Current Integration Version      | 1.0.1             |
| Compatible with ThreatQ Versions | >= 5.6.0          |
| Support Tier                     | ThreatQ Supported |

# Introduction

The Jamf CDF utilizes Jamf's enterprise mobility management (EMM) tool to ingest information on your organization's Apple devices.

The integration provides the following feeds:

- **Jamf Mobile Devices** - ingests information on your apple mobile devices such as ID, Last Reported IP Address, and Enrollment date.
- **Jamf Computers** - ingests information on your macOS devices such as operating system, hardware model, and MAC Address.

The integration ingests Asset and Asset Attributes object types into your ThreatQ instance.

# Prerequisites

The following is required to install and run the integration:

- A Jamf Pro Client ID and Secret. This can be located in the Jamf portal under **Settings > System > API Roles and Clients**.
- The Asset custom object if you are on ThreatQ version 5.9.0 or earlier.

## Asset Custom Object

The integration requires the Asset object. The Asset installation files are included with the integration download on the ThreatQ Marketplace. The Asset object must be installed prior to installing the integration.

 You do not have to install the Asset object if you are running ThreatQ version 5.10.0 or greater as the object has been seeded as a default system object.

Use the steps provided to install the Asset custom object.

 When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

```
cd /tmp/
```

4. Create a new directory:

```
mkdir jamf_cdf
```

5. Upload the **asset.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the **jamf\_cdf** directory.

```
mkdir images
```

7. Upload the **asset.svg**.
8. Navigate to the **/tmp/jamf\_cdf**.

The directory should resemble the following:

- tmp
  - jamf\_cdf
    - asset.json
    - install.sh
    - images

- `asset.svg`

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
chmod +x install.sh
```

10. Run the following command:

```
sudo ./install.sh
```



You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

```
Installing Custom Objects - Step 1 of 5 (Entering Maintenance Mode)
```

```
Application is now in maintenance mode.
```

```
Installing Custom Objects - Step 2 of 5 (Installing the Asset Custom Object)
```

```
Installing Custom Objects - Step 3 of 5 (Configuring image for Asset Custom Object)
```

```
Installing Custom Objects - Step 4 of 5 (Updating Permissions in ThreatQ)
```

```
Installing Custom Objects - Step 5 of 5 (Exiting Maintenance Mode)
```

```
Application is now live.
```

```
-
```

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf jamf_cdf
```

# Installation

 The CDF requires the installation of a custom object before installing the actual CDF if you are on ThreatQ version 5.9.0 or earlier. See the [Asset Custom Object](#) heading under the Prerequisites chapter for more details. The custom object must be installed prior to installing the CDF. Attempting to install the CDF without the custom object will cause the CDF install process to fail.

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration zip file.
3. Extract the contents of the zip file and, if you are on ThreatQ version 5.9 or earlier, install the required [Asset custom object](#).
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the yaml file using one of the following methods:
  - Drag and drop the file into the dialog box
  - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

7. When prompted, select the individual feeds to install and click **Install**. The feed(s) will be added to the integrations page. You will still need to configure and then enable the feed.

# Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

| PARAMETER     | DESCRIPTION                                      |
|---------------|--------------------------------------------------|
| Client ID     | Your Jamf Pro Client ID used for authentication. |
| Client Secret | Your Jamf Pro Client Secret.                     |
| Server URL    | Your Jamf Pro server URL.                        |

< **Jamf Computers**



Disabled
☐
Enabled

Run Integration

Uninstall

**Additional Information**

Integration Type: Feed

Version:

Configuration

Activity Log

Client ID

Jamf Pro Client ID used to authenticate

Client Secret

Jamf Pro Client Secret used to authenticate

Server URL

Jamf Pro server URL

Set indicator status to...

Active

Run Frequency

Every 24 Hours
▼

Next scheduled run:

2024-01-13 08:42am (-05:00)

☒ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

# ThreatQ Mapping

## Jamf Mobile Devices

The JamF Mobile Devices feed ingests information on your organization's mobile devices (iphone, Ipad, AppleTV). Information ingested includes device display name, ID, device type, IP Address, iOS version, IP Address, and MAC address.

GET {{base\_url}}/api/v2/mobile-devices/detail

### Sample Response:

```
{
  "totalCount": 2,
  "results": [
    {
      "mobileDeviceId": "1",
      "deviceType": "iOS",
      "hardware": {
        "capacityMb": 100,
        "availableSpaceMb": 30,
        "usedSpacePercentage": 70,
        "batteryLevel": 60,
        "serialNumber": "5c28fdae",
        "wifiMacAddress": "ee:00:7c:f0:e5:ff",
        "bluetoothMacAddress": "ee:00:7c:f0:e5:aa",
        "modemFirmwareVersion": "iPad7,11",
        "model": "iPad 7th Generation (Wi-Fi)",
        "modelIdentifier": "iPad7,11",
        "modelName": "MW742LL",
        "bluetoothLowEnergyCapable": false,
        "deviceId": "c6a49c6d-8c09-4d71-a37d-2f6a9dfbb69b",
        "extensionAttributes": [
          {
            "id": "1",
            "name": "Example EA",
            "type": "STRING",
            "value": [
              "EA Value"
            ],
            "extensionAttributeCollectionAllowed": false,
            "inventoryDisplay": "General"
          }
        ]
      },
      "userAndLocation": {
        "username": "admin",
        "realName": "IT Bob",

```

```

"emailAddress": "ITBob@jamf.com",
"position": "IT Team Lead",
"phoneNumber": "555-555-5555",
"departmentId": "1",
"buildingId": "1",
"room": "room",
"building": "Building 1",
"department": "Department 1",
"extensionAttributes": [
  {
    "id": "1",
    "name": "Example EA",
    "type": "STRING",
    "value": [
      "EA Value"
    ],
    "extensionAttributeCollectionAllowed": false,
    "inventoryDisplay": "General"
  }
],
},
"purchasing": {
  "purchased": true,
  "leased": false,
  "poNumber": "8675309",
  "vendor": "Apple",
  "appleCareId": "9546567.0",
  "purchasePrice": "$399",
  "purchasingAccount": "IT Budget",
  "poDate": "2019-02-04T21:09:31.661Z",
  "warrantyExpiresDate": "2019-02-04T21:09:31.661Z",
  "leaseExpiresDate": "2019-02-04T21:09:31.661Z",
  "lifeExpectancy": 7,
  "purchasingContact": "Nick in IT",
  "extensionAttributes": [
    {
      "id": "1",
      "name": "Example EA",
      "type": "STRING",
      "value": [
        "EA Value"
      ],
      "extensionAttributeCollectionAllowed": false,
      "inventoryDisplay": "General"
    }
  ]
},
"applications": [
  {
    "identifier": "com.apple.airport.mobileairportutility",

```

```

    "name": "AirPort Utility",
    "version": "135.24",
    "shortVersion": "7.0",
    "managementStatus": "Managed",
    "validationStatus": true,
    "bundleSize": "1024",
    "dynamicSize": "1423"
  }
],
"certificates": [
  {
    "commonName": "3B259E4B-FAD5-4860-B1DD-336ADA786EBA",
    "identity": false,
    "expirationDate": "2019-02-04T21:09:31.661Z"
  }
],
"profiles": [
  {
    "displayName": "Test WiFi",
    "version": "1",
    "uuid": "D29DD9FB-0D5B-422F-A3A2-ABBC5848E949",
    "identifier": "ac2-server4.D0EFAC2D-326C-4BB6-87E6-2BCB88490AAA",
    "removable": true,
    "lastInstalled": "2019-02-04T21:09:31.661Z"
  }
],
"userProfiles": [
  {
    "displayName": "Test WiFi",
    "version": "1",
    "uuid": "D29DD9FB-0D5B-422F-A3A2-ABBC5848E949",
    "identifier": "ac2-server4.D0EFAC2D-326C-4BB6-87E6-2BCB88490AAA",
    "removable": true,
    "lastInstalled": "2019-02-04T21:09:31.661Z",
    "username": "admin"
  }
],
"extensionAttributes": [
  {
    "id": "1",
    "name": "Example EA",
    "type": "STRING",
    "value": [
      "EA Value"
    ],
    "extensionAttributeCollectionAllowed": false,
    "inventoryDisplay": "General"
  }
],
"general": {

```

```

    "udid": "0dad565fb40b010a9e490440188063a378721069",
    "displayName": "Banezicron",
    "assetTag": "8675309",
    "siteId": "-1",
    "lastInventoryUpdateDate": "2022-10-17T11:48:56.307Z",
    "osVersion": "11.4",
    "osRapidSecurityResponse": "(a)",
    "osBuild": "15F79",
    "osSupplementalBuildVersion": "22A103310o",
    "softwareUpdateDeviceId": "J132AP",
    "ipAddress": "10.0.0.1",
    "managed": true,
    "supervised": true,
    "deviceOwnershipType": "Institutional",
    "enrollmentMethodPrestage": {
      "mobileDevicePrestageId": "5",
      "profileName": "All Mobiles"
    },
    "enrollmentSessionTokenValid": false,
    "lastEnrolledDate": "2022-10-17T11:48:56.307Z",
    "mdmProfileExpirationDate": "2022-10-17T11:48:56.307Z",
    "timeZone": "Europe/Warsaw",
    "declarativeDeviceManagementEnabled": true,
    "extensionAttributes": [
      {
        "id": "1",
        "name": "Example EA",
        "type": "STRING",
        "value": [
          "EA Value"
        ],
        "extensionAttributeCollectionAllowed": false,
        "inventoryDisplay": "General"
      }
    ],
    "airPlayPassword": "1234",
    "locales": "null",
    "languages": "english"
  }
}

```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH                      | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES                 | NOTES                                                       |
|-------------------------------------|-----------------|--------------------------------------|----------------|--------------------------|-------------------------------------------------------------|
| .results[].general.displayName      | Asset.Value     | N/A                                  | N/A            | Banezicron               | N/A                                                         |
| .results[].mobileDeviceId           | Asset.Attribute | ID                                   | N/A            | 1                        | N/A                                                         |
| .results[].deviceType               | Asset.Attribute | Device Type                          | N/A            | iOS / tvOS               | N/A                                                         |
| .results[].hardware.wifiMacAddress  | Asset.Attribute | WIFI Mac Address                     | N/A            | ee:00:7c:f0:e5:ff        | N/A                                                         |
| .results[].general.ipAddress        | Asset.Attribute | IP Address                           | N/A            | 10.0.0.1                 | If the attribute already exists, the value will be updated  |
| .results[].general.lastEnrolledDate | Asset.Attribute | Last Enrolled Date                   | N/A            | 2022-10-17T11:48:56.307Z | If the attribute already exists, the value will be updated. |
| .results[].hardware.osVersion       | Asset.Attribute | Operating System Version             | N/A            | 11.4                     | If the attribute already exists, the value will be updated. |
| .results[].hardware.osBuild         | Asset.Attribute | Operating System Build               | N/A            | 15F79                    | If the attribute already exists, the value will be updated. |

## Jamf Computers

High-level summary of what info the feed ingests information on your Apple computers such as ID, enrollment date, and last reported IP Address.

GET `{{base_url}}/api/v1/computers-inventory`

### Sample Response:

```
{
  "totalCount": 2,
  "results": [
    {
      "id": "1",
      "udid": "152835A5-AEA3-55C4-90E0-2B7DB38009B6",
      "general": {
        "name": "Bigâ€™s MacBook Pro",
        "lastIpAddress": "71.187.71.19",
        "lastReportedIp": "192.168.86.211",
        "jamfBinaryVersion": "11.1.1-t1701704198",
        "platform": "Mac",
        "barcode1": null,
        "barcode2": null,
        "assetTag": null,
        "remoteManagement": {
          "managed": true,
          "managementUsername": null
        },
        "supervised": true,
        "mdmCapable": {
          "capable": true,
          "capableUsers": [
            "bigsurtest"
          ]
        },
        "reportDate": "2023-12-19T15:18:15.178Z",
        "lastContactTime": "2023-12-19T15:17:55.86Z",
        "lastCloudBackupDate": null,
        "lastEnrolledDate": "2023-11-15T22:31:48.607Z",
        "mdmProfileExpiration": "2025-11-15T22:31:33Z",
        "initialEntryDate": "2023-11-15",
        "distributionPoint": null,
        "site": {
          "id": "-1",
          "name": "None"
        },
        "itunesStoreAccountActive": false,
        "enrolledViaAutomatedDeviceEnrollment": false,
        "userApprovedMdm": true,
        "enrollmentMethod": {
```

```

        "id": "1",
        "objectName": null,
        "objectType": "User-initiated - no invitation"
    },
    "declarativeDeviceManagementEnabled": false,
    "managementId": "c98948ba-f921-462e-939f-799091c5627c",
    "extensionAttributes": []
},
"diskEncryption": null,
"localUserAccounts": null,
"purchasing": null,
"printers": null,
"storage": null,
"applications": null,
"userAndLocation": null,
"configurationProfiles": null,
"services": null,
"plugins": null,
"hardware": null,
"certificates": null,
"attachments": null,
"packageReceipts": null,
"fonts": null,
"security": null,
"operatingSystem": null,
"licensedSoftware": null,
"softwareUpdates": null,
"groupMemberships": null,
"extensionAttributes": null,
"contentCaching": null,
"ibeacons": null
}
]
}

```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH                      | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES                 | NOTES                                                       |
|-------------------------------------|-----------------|--------------------------------------|----------------|--------------------------|-------------------------------------------------------------|
| .results[].general.name             | Asset.Value     | N/A                                  | N/A            | Bigâ€™s MacBook Pro      | N/A                                                         |
| .results[].id                       | Asset.Attribute | ID                                   | N/A            | 1                        | N/A                                                         |
| .results[].general.lastEnrolledDate | Asset.Attribute | Last Enrolled Date                   | N/A            | 2023-11-15T22:31:48.607Z | If the attribute already exists, the value will be updated. |
| .results[].general.lastIpAddress    | Asset.Attribute | Last IP Address                      | N/A            | 71.187.71.19             | If the attribute already exists, the value will be updated. |
| .results[].general.lastReportedIp   | Asset.Attribute | Last Reported IP Address             | N/A            | 192.168.86.211           | If the attribute already exists, the                        |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES                  |
|----------------|----------------|--------------------------------------|----------------|----------|------------------------|
|                |                |                                      |                |          | value will be updated. |

## Jamf Computers Supplemental Feed

The Jamf Computers Supplemental feed ingests further details on your apple computers such as hardware models, network adapter types, and serial numbers.

GET {{base\_url}}/JSSResource/computers/id/{{id}}

```
{
  "computer": {
    "general": {
      "id": 1,
      "name": "Bigâ€™s MacBook Pro",
      "network_adapter_type": "IEEE80211",
      "mac_address": "8C:85:90:78:D1:DA",
      "alt_network_adapter_type": "Ethernet",
      "alt_mac_address": "82:DC:72:62:B4:01",
      "ip_address": "71.187.71.19",
      "last_reported_ip": "192.168.86.211",
      "serial_number": "C02VN0XJHTD6",
      "udid": "152835A5-AEA3-55C4-90E0-2B7DB38009B6",
      "jamf_version": "11.1.1-t1701704198",
      "platform": "Mac",
      "barcode_1": "",
      "barcode_2": "",
      "asset_tag": "",
      "remote_management": {
        "managed": true,
        "management_username": "deprecated",
        "management_password_sha256": "deprecated"
      },
      "supervised": true,
      "mdm_capable": true,
      "mdm_capable_users": {
        "mdm_capable_user": "bigsurtest"
      },
      "management_status": {
        "enrolled_via_dep": false,
        "user_approved_enrollment": true,
        "user_approved_mdm": true
      },
      "report_date": "2023-12-19 15:18:15",
      "report_date_epoch": 1702999095178,
      "report_date_utc": "2023-12-19T15:18:15.178+0000",
      "last_contact_time": "2023-12-19 15:17:55",
      "last_contact_time_epoch": 1702999075860,
      "last_contact_time_utc": "2023-12-19T15:17:55.860+0000",
      "initial_entry_date": "2023-11-15",
      "initial_entry_date_epoch": 1700087472868,
      "initial_entry_date_utc": "2023-11-15T22:31:12.868+0000",
      "last_cloud_backup_date_epoch": 0,

```

```

    "last_cloud_backup_date_utc": "",
    "last_enrolled_date_epoch": 1700087508607,
    "last_enrolled_date_utc": "2023-11-15T22:31:48.607+0000",
    "mdm_profile_expiration_epoch": 1763245893000,
    "mdm_profile_expiration_utc": "2025-11-15T22:31:33.000+0000",
    "distribution_point": "",
    "sus": "",
    "site": {
        "id": -1,
        "name": "None"
    },
    "itunes_store_account_is_active": false
},
"location": {
    "username": "",
    "realname": "",
    "real_name": "",
    "email_address": "",
    "position": "",
    "phone": "",
    "phone_number": "",
    "department": "",
    "building": "",
    "room": ""
},
"purchasing": {
    "is_purchased": true,
    "is_leased": false,
    "po_number": "",
    "vendor": "",
    "applecare_id": "",
    "purchase_price": "",
    "purchasing_account": "",
    "po_date": "",
    "po_date_epoch": 0,
    "po_date_utc": "",
    "warranty_expires": "",
    "warranty_expires_epoch": 0,
    "warranty_expires_utc": "",
    "lease_expires": "",
    "lease_expires_epoch": 0,
    "lease_expires_utc": "",
    "life_expectancy": 0,
    "purchasing_contact": "",
    "os_applecare_id": "",
    "os_maintenance_expires": "",
    "attachments": []
},
"peripherals": [],
"hardware": {

```

```

"make": "Apple",
"model": "15-inch Retina MacBook Pro with TouchID (Mid 2017)",
"model_identifier": "MacBookPro14,3",
"os_name": "macOS",
"os_version": "11.6.6",
"os_build": "20G624",
"software_update_device_id": "",
"active_directory_status": "Not Bound",
"service_pack": "",
"processor_type": "Quad-Core Intel Core i7",
"is_apple_silicon": false,
"processor_architecture": "x86_64",
"processor_speed": 2900,
"processor_speed_mhz": 2900,
"number_processors": 1,
"number_cores": 4,
"total_ram": 16384,
"total_ram_mb": 16384,
"boot_rom": "451.140.1.0.0",
"bus_speed": 0,
"bus_speed_mhz": 0,
"battery_capacity": 100,
"cache_size": 8192,
"cache_size_kb": 8192,
"available_ram_slots": 0,
"optical_drive": "",
"nic_speed": "n/a",
"smc_version": "2.45f5",
"ble_capable": true,
"supports_ios_app_installs": false,
"sip_status": "Enabled",
"gatekeeper_status": "App Store and identified developers",
"xprotect_version": "2175",
"institutional_recovery_key": "Not Present",
"disk_encryption_configuration": "TQ Testing",
"filevault2_users": [
    "bigsurtest"
],
"storage": [
    {
        "disk": "disk0",
        "model": "APPLE SSD SM0512L",
        "revision": "CXS5EA0Q",
        "serial_number": "C027446018HHRDV1S",
        "size": 500277,
        "drive_capacity_mb": 500277,
        "connection_type": "NO",
        "smart_status": "Verified",
        "partitions": [

```

```

        "name": "Update/mnt1",
        "size": 499963,
        "type": "other",
        "partition_capacity_mb": 499963,
        "percentage_full": 7,
        "available_mb": 345461,
        "filevault_status": "Encrypting",
        "filevault_percent": 43,
        "filevault2_status": "Encrypting",
        "filevault2_percent": 43
    },
    {
        "name": "Data",
        "size": 499963,
        "type": "other",
        "partition_capacity_mb": 499963,
        "percentage_full": 6,
        "available_mb": 345461,
        "filevault_status": "Encrypted",
        "filevault_percent": 100,
        "filevault2_status": "Encrypted",
        "filevault2_percent": 100
    },
    {
        "name": "Update",
        "size": 499963,
        "type": "other",
        "partition_capacity_mb": 499963,
        "percentage_full": 1,
        "available_mb": 345461,
        "filevault_status": "Not Encrypted",
        "filevault_percent": 0,
        "filevault2_status": "Not Encrypted",
        "filevault2_percent": 0
    },
    {
        "name": "Macintosh HD (Boot Partition)",
        "size": 499963,
        "type": "boot",
        "partition_capacity_mb": 499963,
        "percentage_full": 7,
        "available_mb": 345461,
        "filevault_status": "Encrypted",
        "filevault_percent": 100,
        "filevault2_status": "Encrypted",
        "filevault2_percent": 100,
        "boot_drive_available_mb": 345461,
        "lvgUUID": "",
        "lvUUID": "",
        "pvUUID": ""
    }

```

```

    },
    {
      "name": "VM",
      "size": 499963,
      "type": "other",
      "partition_capacity_mb": 499963,
      "percentage_full": 1,
      "available_mb": 345461,
      "filevault_status": "Not Encrypted",
      "filevault_percent": 0,
      "filevault2_status": "Not Encrypted",
      "filevault2_percent": 0
    },
    {
      "name": "Preboot",
      "size": 499963,
      "type": "other",
      "partition_capacity_mb": 499963,
      "percentage_full": 1,
      "available_mb": 345461,
      "filevault_status": "Not Encrypted",
      "filevault_percent": 0,
      "filevault2_status": "Not Encrypted",
      "filevault2_percent": 0
    },
    {
      "name": "Macintosh HD - Data",
      "size": 499963,
      "type": "other",
      "partition_capacity_mb": 499963,
      "percentage_full": 1,
      "available_mb": 345461,
      "filevault_status": "Not Encrypted",
      "filevault_percent": 0,
      "filevault2_status": "Not Encrypted",
      "filevault2_percent": 0
    }
  ]
},
"mapped_printers": [],
},
"certificates": [
  {
    "common_name": "51BBA5AE-4B31-4277-BFC9-1C59C4E7871D",
    "identity": true,
    "expires_utc": "2025-11-15T22:31:33.000+0000",
    "expires_epoch": 1763245893000,
    "name": ""
  }
]

```

```

],
"security": {
  "activation_lock": false,
  "recovery_lock_enabled": false,
  "secure_boot_level": "not supported",
  "external_boot_level": "not supported",
  "firewall_enabled": false
},
"software": {
  "unix_executables": [],
  "licensed_software": [],
  "installed_by_casper": [],
  "installed_by_installer_swu": [
    "com.jamfsoftware.osxenrollment"
  ],
  "cached_by_casper": [],
  "available_software_updates": [],
  "available_updates": [],
  "running_services": [
    "org.cups.cupsd"
  ],
  "applications": [
    {
      "name": "Terminal.app",
      "path": "/System/Applications/Utilities/Terminal.app",
      "version": "2.11",
      "bundle_id": "com.apple.Terminal"
    },
    {
      "name": "TextEdit.app",
      "path": "/System/Applications/TextEdit.app",
      "version": "1.16",
      "bundle_id": "com.apple.TextEdit"
    },
    {
      "name": "Time Machine.app",
      "path": "/System/Applications/Time Machine.app",
      "version": "1.3",
      "bundle_id": "com.apple.backup.launcher"
    },
    {
      "name": "TV.app",
      "path": "/System/Applications/TV.app",
      "version": "1.1.6",
      "bundle_id": "com.apple.TV"
    },
    {
      "name": "VoiceMemos.app",
      "path": "/System/Applications/VoiceMemos.app",
      "version": "2.2",

```

```

        "bundle_id": "com.apple.VoiceMemos"
    },
    {
        "name": "VoiceOver Utility.app",
        "path": "/System/Applications/Utilities/VoiceOver
Utility.app",
        "version": "10",
        "bundle_id": "com.apple.VoiceOverUtility"
    }
],
"fonts": [],
"plugins": []
},
"extension_attributes": [],
"groups_accounts": {
    "computer_group_memberships": [
        "All Managed Clients"
    ],
    "local_accounts": [
        {
            "name": "bigsurtest",
            "realname": "Big Sur Test",
            "uid": "501",
            "home": "/Users/bigsurtest",
            "home_size": "-1MB",
            "home_size_mb": -1,
            "administrator": true,
            "filevault_enabled": true
        },
        {
            "name": "TestUser",
            "realname": "TestUser",
            "uid": "502",
            "home": "/Users/TestUser",
            "home_size": "-1MB",
            "home_size_mb": -1,
            "administrator": true,
            "filevault_enabled": false
        },
        {
            "name": "tq",
            "realname": "TQ Admin",
            "uid": "503",
            "home": "/private/var/tq",
            "home_size": "-1MB",
            "home_size_mb": -1,
            "administrator": true,
            "filevault_enabled": false
        }
    ]
},

```

```

    "user_inventories": {
      "disable_automatic_login": true,
      "user": {
        "username": "tq",
        "password_history_depth": "5",
        "password_min_length": "12",
        "password_max_age": "180",
        "password_min_complex_characters": "",
        "password_require_alphanumeric": "true"
      }
    },
    "iphones": [],
    "configuration_profiles": [
      {
        "id": -1,
        "name": "",
        "uuid": "",
        "is_removable": false
      },
      {
        "id": -27,
        "name": "",
        "uuid": "",
        "is_removable": false
      },
      {
        "id": -1,
        "name": "",
        "uuid": "",
        "is_removable": false
      },
      {
        "id": 1,
        "name": "",
        "uuid": "",
        "is_removable": false
      }
    ]
  }
}

```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH                             | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES                                           | NOTES                                                       |
|--------------------------------------------|-----------------|--------------------------------------|----------------|----------------------------------------------------|-------------------------------------------------------------|
| .computer.general.network_adapter_type     | Asset.Attribute | Network Adapter Type                 | N/A            | IEEE80211                                          | N/A                                                         |
| .computer.general.mac_address              | Asset.Attribute | Mac Address                          | N/A            | 8C:85:90:78:D1:DA                                  | N/A                                                         |
| .computer.general.alt_network_adapter_type | Asset.Attribute | Alternative Network Adapter Type     | N/A            | Ethernet                                           | N/A                                                         |
| .computer.general.alt_mac_address          | Asset.Attribute | Alternative Mac Address              | N/A            | 82:DC:72:62:B4:01                                  | N/A                                                         |
| .computer.general.serial_number            | Asset.Attribute | Serial Number                        | N/A            | C02VN0XJHTD6                                       | N/A                                                         |
| .computer.general.platform                 | Asset.Attribute | Platform                             | N/A            | Mac                                                | N/A                                                         |
| .computer.hardware.make                    | Asset.Attribute | Maker                                | N/A            | Apple                                              | N/A                                                         |
| .computer.hardware.model                   | Asset.Attribute | Model                                | N/A            | 15-inch Retina MacBook Pro with TouchID (Mid 2017) | N/A                                                         |
| .computer.hardware.model_identifier        | Asset.Attribute | Model Identifier                     | N/A            | MacBookPro14,3                                     | N/A                                                         |
| .computer.hardware.os_name                 | Asset.Attribute | Operating System                     | N/A            | macOS                                              | If the attribute already exists, the value will be updated. |
| .computer.hardware.os_version              | Asset.Attribute | Operating System Version             | N/A            | 11.6.6                                             | If the attribute already exists, the value will be updated. |
| .computer.hardware.os_build                | Asset.Attribute | Operating System Build               | N/A            | 20G624                                             | If the attribute already exists, the value will be updated. |
| .computer.hardware.processor_type          | Asset.Attribute | Processor Type                       | N/A            | Quad-Core Intel Core i7                            | N/A                                                         |
| .computer.hardware.processor_architecture  | Asset.Attribute | Processor Architecture               | N/A            | x86_64                                             | N/A                                                         |
| .computer.security.secure_boot_level       | Asset.Attribute | Secure Boot Level                    | N/A            | not supported                                      | N/A                                                         |

# Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

## Jamf Mobile Devices

| METRIC           | RESULT   |
|------------------|----------|
| Run Time         | 1 minute |
| Assets           | 3        |
| Asset Attributes | 12       |

## Jamf Computers

| METRIC           | RESULT   |
|------------------|----------|
| Run Time         | 1 minute |
| Assets           | 3        |
| Asset Attributes | 57       |

# Change Log

- **Version 1.0.1**
  - Updated the authentication method to use API Client ID and Secret.
- **Version 1.0.0**
  - Initial release