Tanium™ Endpoint Identity User Guide

Version 1.0.0

December 14, 2020

The information in this document is subject to change without notice. Further, the information provided in this document is provided "as is" and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium's customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://docs.tanium.com for the most current Tanium product documentation.

This documentation may provide access to or information about content, products (including hardware and software), and services provided by third parties ("Third Party Items"). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium.

Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.

Tanium is committed to the highest accessibility standards to make interaction with Tanium software more intuitive and to accelerate the time to success. To ensure high accessibility standards, Tanium complies with the U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. We have conducted third-party accessibility assessments over the course of product development for many years, and most recently a comprehensive audit against the WCAG 2.1 / VPAT 2.3 standards for all major product modules was completed in September 2019. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making best efforts to address any gaps quickly, as is feasible, given the severity of the issue and scope of the changes. These objectives are factored into the ongoing delivery schedule of features and releases with our existing resources.

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, email Tanium Support at support@tanium.com, or email accessibility@tanium.com to make further inquiries.

Tanium is a trademark of Tanium, Inc. in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners.

Table of contents

Endpoint Identity overview

With Endpoint Identity, you can integrate Tanium with Identity and Access Management (IAM) vendors, such as Cloudflare, to verify that devices connecting to your cloud applications and zero trust networks are managed and secure.

Device verification scenario

While employees typically access cloud applications from their company-provided computer, sometimes an employee might find a need to use another computer to log into cloud applications. For example, an employee has left their company-provided computer at home while visiting a relative, but an urgent work request comes up. They use their relative's unmanaged computer to try to log into the cloud application.

When the employee attempts this login, the endpoint is checked against the known managed endpoints in Tanium. Because the employee is attempting to log in with an unmanaged computer, they are not allowed to log into the cloud application.

Configuration overview

To configure Tanium endpoints to provide Endpoint Identity data, deploy configurations and packages to the endpoints. For more information, see Configure Endpoint Identity on endpoints on page 10.

Identity provider integration

After endpoints are configured, the Endpoint Identity API returns platform, status, and vulnerability information about Tanium-managed endpoints to the identity provider. The identity provider can then manage access to cloud applications or zero trust networks based on this endpoint information.

Integration with other Tanium products

Comply

If you have Tanium™ Comply running vulnerability scans, the latest results from the scan are returned for each endpoint.

Endpoint Identity requirements

Review the requirements before you install and use Endpoint Identity.

Tanium dependencies

In addition to a license for Endpoint Identity, make sure that your environment meets the following requirements.

Component	Requirement
Tanium™ Core Platform	7.2 or later
Tanium products	(Optional) Tanium Comply 2.6 or later

Endpoints

Supported operating systems

The following endpoint operating systems are supported with Endpoint Identity.

- Windows
- macOS
- Linux

For Tanium Client operating system support, see Tanium Client User Guide: Host system requirements.

Third-party software

Endpoint identity enables integration with third-party vendors:

- CloudFlare

Host and network security requirements

Specific ports and processes are needed to run Endpoint Identity.

Ports

The following ports are required for Endpoint Identity communication.

Component	Port	Direction	Purpose
Endpoints	17472	Inbound / Outbound	Client / server communication

Security exclusions

If security software is in use in the environment to monitor and block unknown host system processes, your security administrator must create exclusions to allow the Tanium processes to run without interference.

Table 1: Endpoint Identity security exclusions

Target Device	Process
Endpoints (Windows)	`<Tanium Client>\TaniumCX.exe`
Endpoints (macOS, Linux)	`<Tanium Client>/TaniumCX`

Installing Endpoint Identity

Use the **Tanium Solutions** page to install Endpoint Identity.

Before you begin

- Read the release notes.
- Review the Endpoint Identity requirements on page 7.

Import and configure Endpoint Identity with custom settings

Perform the steps in Tanium Console User Guide: Manage Tanium modules.

Configure Endpoint Identity on endpoints

When Endpoint Identity is configured on Tanium endpoints, an identity provider can query the endpoint for information. This information helps the identity provider decide whether to allow that endpoint and user to access a privileged app. To configure Endpoint Identity, you must distribute tools and configuration packages to the endpoints.

Distribute tools packages

Distribute the Endpoint Identity tools packages to the endpoints. Create questions that target a specific operating system, then deploy an action to the endpoints. For more information about deploying actions, see Tanium Interact User guide: Deploying Actions.

1. Target a set of endpoints by operating system by asking a question:
   - All Windows endpoints question example: `Get Is Windows from all machines`
   - All Linux endpoints question example: `Get Is Linux from all machines`
   - All Mac endpoints example: `Get Is Mac from all machines`
2. Deploy an action to the targeted set of endpoints. Click **Deploy Action**. Deploy the package that is appropriate for the operating system:
   - `Endpoint Identity - Tools [Windows]`
   - `Endpoint Identity - Tools [Linux]`
   - `Endpoint Identity - Tools [Mac]`

Generate key pairs

Generate RSA key pairs:

- One RSA key pair for the client/integration partner. The public key is used as the client public key in the configuration packages. Check with the third-party integration vendor on this item. They might provide the file to you, or provide instructions on how to generate and export these key pairs. This file must be named `client-public.key`.
- One RSA key pair for the Tanium Endpoint Identity solution. Put the `server-private.key` file in the configuration packages. Provide the `server-public.key` file to the integration vendor.

Generate Tanium RSA key pair with OpenSSL

If you have OpenSSL installed, you can run the following commands:

```
openssl genrsa -out <<private-key-filename>> 2048
```

```
openssl rsa -in <<private-key-filename>> -outform PEM -pubout -out
<<public-key-filename>>
```

Update configuration packages

Update the Endpoint Identity configuration packages to include port and key pair settings.

1. From the Main menu, click **Content > Packages**.
2. In the filter, type `Endpoint Identity` to display the list of configuration packages:
   - `Endpoint Identity - Configure Endpoint Identity [Windows]`
   - `Endpoint Identity - Configure Endpoint Identity [Linux]`
   - `Endpoint Identity - Configure Endpoint Identity [Mac]`
3. Select the configuration package you want to update and click **Edit**.
4. Edit the packages to set the keys and port to use. In the **Files** section of the package, download the `config.json` file. Update the port and origin whitelist.
   - The `httpPort` property is the port on which the endpoint listens for calls from the identity provider. The value is `8181` by default.
   - The `serverPrivateKey` and `clientPublicKey` properties are ignored if you upload these files into the package. If you define these properties in the `config.json` file, the values must be a single line, inserting `\n` for any breaks.
   - The `originWhitelist` property is a comma-separated list of domains that are allowed to make requests. Get this list from the integration vendor. This list should not contain any white space. You can use a leading asterisk `*` to indicate that any subdomain is allowed. You cannot use an asterisk by itself as a value.

   Verify that the `config.json` is valid after updating. An example follows:

   ```
   { "httpPort": 8181,
   "serverPrivateKey": "",
   "clientPublicKey": "",
   "originWhitelist": "mydomain.com,*.onlysubdomains.com"
    }
   ```
5. Upload the configured `config.json` file in the package. Delete the existing `config.json` file, then click **Add > Local File**.

6. Add the client public key provided by the integration vendor to the package. Click **Add > Local File**. This file must be named `client-public.key`. Uploading this file overrides the `clientPublicKey` value in the `config.json` file.
7. Add the server private key that you generated for Tanium Endpoint Identity. Click **Add > Local File**. This file must be named `server-private.key`. Uploading this file overrides the `serverPrivateKey` value in the `config.json` file.
8. Save the package and repeat for each configuration package.

Distribute configuration packages

Distribute the Endpoint Identity configuration packages to the endpoints. Create questions that target a specific operating system, then deploy an action to the endpoints. For more information about deploying actions, see Tanium Interact User guide: Deploying Actions.

1. Target a set of endpoints by operating system by asking a question:
   - All Windows endpoints question example: `Get Is Windows from all machines`
   - All Linux endpoints question example: `Get Is Linux from all machines`
   - All Mac endpoints example: `Get Is Mac from all machines`
2. Deploy an action to the targeted set of endpoints. Click **Deploy Action**. Deploy the package that is appropriate for the operating system:
   - `Endpoint Identity - Configure Endpoint Identity [Windows]`
   - `Endpoint Identity - Configure Endpoint Identity [Linux]`
   - `Endpoint Identity - Configure Endpoint Identity [Mac]`

Check Endpoint Identity tools installation

To check the status of tools installation on your endpoints, ask the question: `Get Endpoint Identity - Tools Version from all machines`.

What to do next

The third-party identity provider can now use the Endpoint Identity API to get information about the Tanium-managed endpoints. The API returns the following JSON for your endpoints:

```
{
        "nonce" : "peanut-butter",
        "patchStatus" :
        {
                "lastSystemUpdateTime8601" : "2020-03-17T16:20:17Z"
        },
        "platform" :
        {
                "platformType" : "MacOS"
        },
        "taniumStatus" :
        {
                "lastConnectionTime8601" : "2020-03-30T12:20:17Z"
        },
        "vulnerabilities" :
        {
                "countHigh" : 54,
                "countLow" : 30,
                "countMedium" : 63,
                "maxScore" : 9.3000000000000007,
                "meanScore" : 5.7400000000000002,
                "medianScore" : 5,
                "minScore" : 0,
                "totalCount" : 147,
                "totalReports" : 19
        }
}
```

The Endpoint Identity API returns the following objects and key/values. The values are calculated by Tanium each time that an API request is received.

nonce object

Echos a unique identifier of the API call, if a nonce was defined in the request.

patchStatus object

- lastSystemUpdateTime8601
  (Windows only) Reports the last time that a Windows update was successfully applied on the endpoint. For non-Windows platforms, an empty string `""` returned.

platform object

- platformType
  Specifies the platform of the endpoint, if the endpoint has the Tanium Client installed. Valid values: MacOS, Windows, Linux

taniumStatus object

- lastConnectionTime8601
  Reports the last time that the endpoint connected to the Tanium Server. If the Tanium Client is not installed on the endpoint, an empty string `""` is returned.

vulnerabilities object

If Tanium Comply vulnerability scans are being run on the endpoint, the following attributes are returned. If Comply is not available on the endpoint, a `0` value is returned for all the attributes.

- countHigh
  Number of vulnerabilities with high severity
- countLow
  Number of vulnerabilities with low severity
- countMedium
  Number of vulnerabilities with medium severity
- maxScore
  Highest vulnerability score
- meanScore
  Mean vulnerability score
- medianScore
  Median vulnerability score
- minScore
  Lowest vulnerability score
- totalCount
  Total number of vulnerabilities
- totalReports
  Total number of reports