Tanium™ Endpoint Identity User Guide

Version 1.1.3

September 08, 2021

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 for our products. To date, Tanium has focused on compliance with U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years and has most recently completed certification against the WCAG 2.1 / VPAT 2.3 standards for all major product modules in summer 2021. In the recent testing the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.1 criteria. 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.

Table of contents

Endpoint Identity overview **5**

Integration overview scenario 5

Configuration overview 6

Identity provider integration 6

Integration with other Tanium products 6

Comply 6

Patch 6

Endpoint Identity requirements **7**

Tanium dependencies 7

Endpoints 7

Supported operating systems 7

Third-party software 7

Host and network security requirements 8

Ports 8

Security exclusions 8

Installing Endpoint Identity **9**

Before you begin 9

Import Endpoint Identity 9

Configure Endpoint Identity on endpoints **10**

Distribute tools packages 10

Generate key pairs 10

Generate Tanium RSA key pair with OpenSSL 11

Validate server key pair 11

Update configuration packages 11

Distribute configuration packages 12

Check Endpoint Identity tools installation 13

What to do next 13

Troubleshooting Endpoint Identity **14**

Troubleshooting Cloudflare integration issues 14

Remove Endpoint Identity tools from endpoints 16

Contact Tanium Support 17

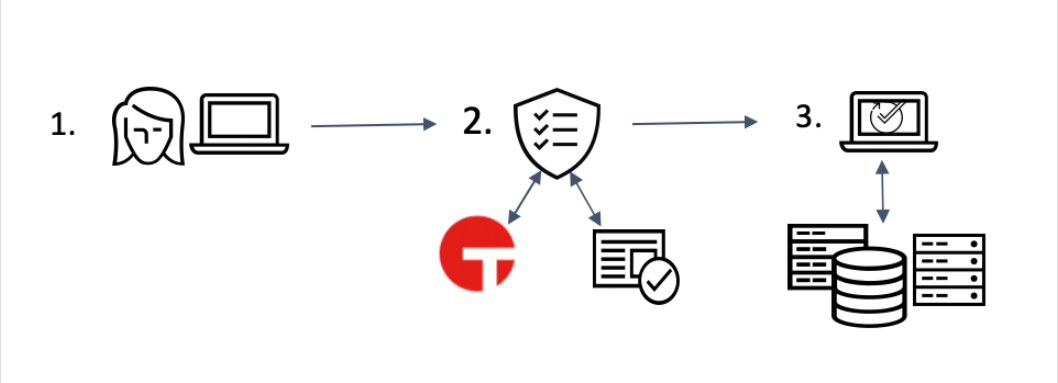
Endpoint Identity overview

With Endpoint Identity, you can integrate Tanium with Cloud Access Security Brokers and Zero Trust Network Access providers, such as Cloudflare and Google BeyondCorp, to verify that devices connecting to your cloud applications and zero trust networks are managed and secure.

Integration overview scenario

When Endpoint Identity is configured on Tanium endpoints, an authentication or authorization provider can query the endpoint for information. This information helps the authentication or authorization provider decide whether to allow that endpoint and user to access a privileged application.

The following image illustrates how this works.



1. An employee requests access to an application. For example, the employee might be requesting access from an updated company-provided computer, an outdated company-provided computer, or a home computer.
2. The authentication or authorization provider receives the request and does the following:
    1. Verifies endpoint security with Endpoint Identity. Endpoint Identity returns information to the authentication or authorization provider that includes if the endpoint has a Tanium Client installed, the last time an operating system update was applied, and vulnerability scores.
    2. Verifies user identity.
3. Based on the verification results and company policies, the authentication or authorization provider grants or denies the employee access to the application.

    For example, the employee might be able to access a critical application from an updated Tanium-managed computer but cannot access that same application on a non-Tanium managed computer. The employee might be able to access a non-critical application on a non-Tanium managed computer.

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 you configure the endpoints, the Endpoint Identity API returns platform, Patch status, and Comply vulnerability information about Tanium-managed endpoints to the authentication or authorization provider. Tanium calculates the values each time that an API request is received. The authentication or authorization 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 scans are returned for each endpoint. For more information, see Tanium Comply User Guide.

Patch

If you have Tanium™ Patch automating patch delivery, the latest results from the scans are returned for each endpoint. For more information, see Tanium Patch User Guide.

Endpoint Identity requirements

Review the requirements before you install and use Endpoint Identity.

Tanium dependencies

Component	Requirement
Tanium™ Core Platform	7.2 or later
Tanium solutions	(Optional) • Tanium Comply 2.6 or later • Tanium Patch 3.0 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 Management User Guide: Client version and host system requirements.

Third-party software

Endpoint Identity enables integration with the following third-party vendors:

- Cloudflare
- Google BeyondCorp

The following table identifies the integration functionality offered by each vendor.

Identity Provider	Platform Integration	Patch Integration	Comply Integration
Cloudflare	✅	❌	❌
Google BeyondCorp	✅	✅	✅

Host and network security requirements

Endpoint Identity requires specific ports and processes to run.

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.

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 Endpoint Identity

1. From the Main menu, go to **Administration > Configuration > Solutions** and scroll to the **Content** section.
2. Select **Endpoint Identity**, click **Import Selected**, and complete the import.
   For more information, see Tanium Console User Guide: Manage Tanium shared services and content.

Configure Endpoint Identity on endpoints

When you configure Endpoint Identity 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 application. To configure Endpoint Identity, you must distribute tools and configuration packages to the endpoints.

The following instructions use actions to distribute configuration packages to endpoints. For an enterprise-wide deployment, use scheduled actions to simplify distribution. For details, see Managing scheduled actions and action history.

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:
    1. All Windows endpoints question example: `Get Is Windows from all machines`
    2. All Linux endpoints question example: `Get Is Linux from all machines`
    3. 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:
    1. `Endpoint Identity - Tools [Windows]`
    2. `Endpoint Identity - Tools [Linux]`
    3. `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. Note that the commands may vary depending on the keys supported by the library you are using.

```
openssl genpkey -out <<client-private.key>> -algorithm RSA -pkeyopt rsa_keygen_
bits:2048
```

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

```
openssl genpkey -out <<server-private.key>> -algorithm RSA -pkeyopt rsa_keygen_
bits:2048
```

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

Validate server key pair

Validate that the MD5 hashes on the `server-private.key` and `server-public.key` match. If you have OpenSSL installed, you can run the following commands:

```
openssl rsa -noout -modulus -in <<server-private.key>> | openssl md5
```

```
openssl rsa -noout -modulus -pubin -in <<server-public.key>> | openssl md5
```

Update configuration packages

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

1. From the Main menu, click **Administration > Content > Packages**.
2. In the filter, type `Endpoint Identity` to display the list of configuration packages:
    1. `Endpoint Identity - Configure Endpoint Identity [Windows]`
    2. `Endpoint Identity - Configure Endpoint Identity [Linux]`
    3. `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 allowed list.

    1. The `httpPort` property is the port on which the endpoint listens for calls from the authentication or authorization provider. The value is `8181` by default.
    2. 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.
    3. The `originAllowed` 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": "",
    "originAllowed": "provider.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:
    1. All Windows endpoints question example: `Get Is Windows from all machines`
    2. All Linux endpoints question example: `Get Is Linux from all machines`
    3. 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:
    1. `Endpoint Identity - Configure Endpoint Identity [Windows]`
    2. `Endpoint Identity - Configure Endpoint Identity [Linux]`
    3. `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 provides the following information:

- If the endpoint has the Tanium Client installed, the platform of the endpoint and the last time that the endpoint connected to the Tanium Server.
- If Tanium Patch scans are being run on the Windows endpoint, the last time that a Windows update was successfully applied on the endpoint.
- If Tanium Comply vulnerability scans are being run on the endpoint, the API provides the following:
    - Number of vulnerabilities with low, medium, and high severities
    - Highest, mean, median, and lowest vulnerability scores
    - Total number of vulnerabilities
    - Total number of reports
      Endpoint Identity leverages all available Comply reports.

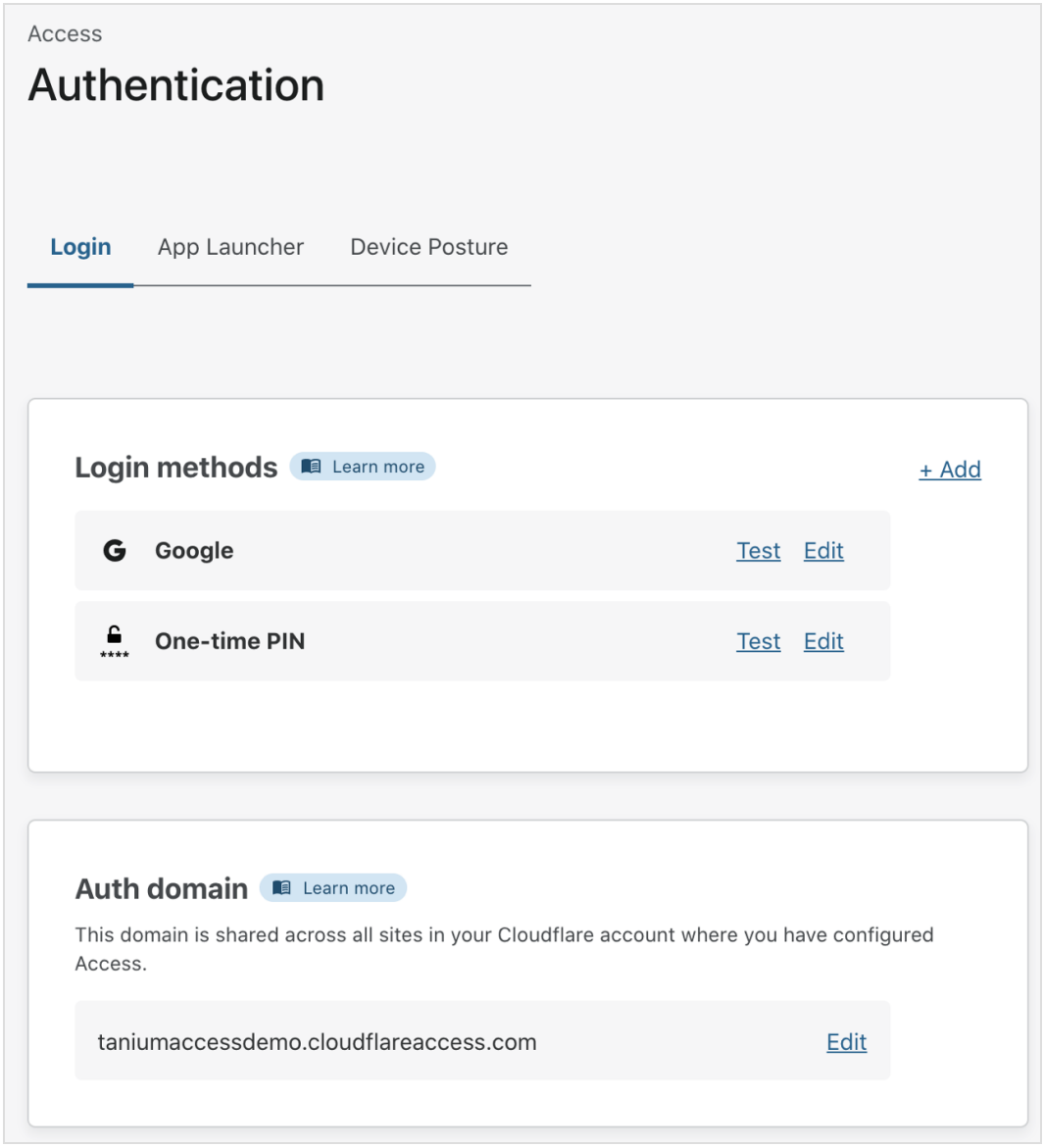
Troubleshooting Endpoint Identity

To collect and send information to Tanium for troubleshooting, collect relevant information.

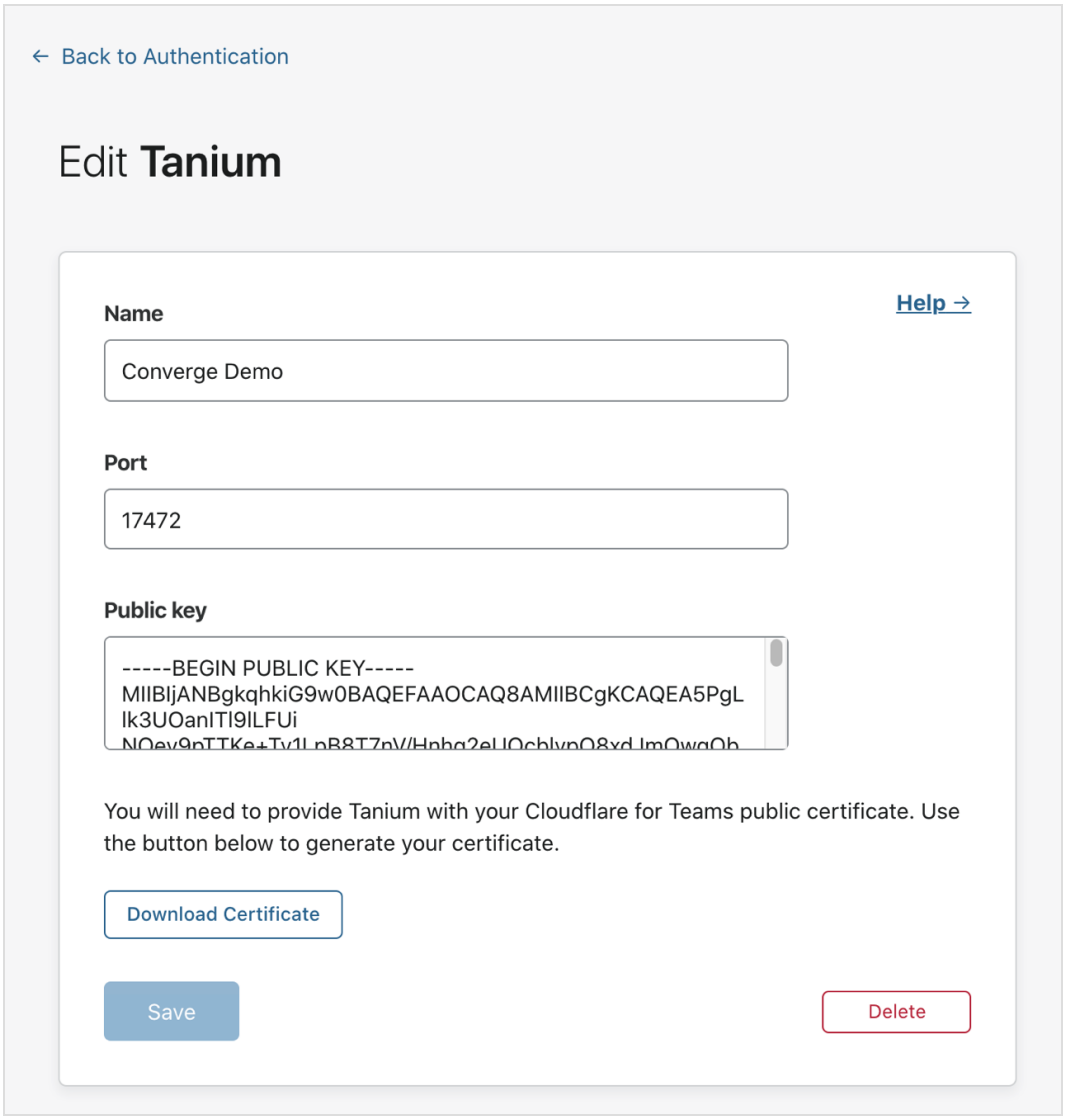
Troubleshooting Cloudflare integration issues

Confirm the following items are properly configured in Cloudflare for Teams.

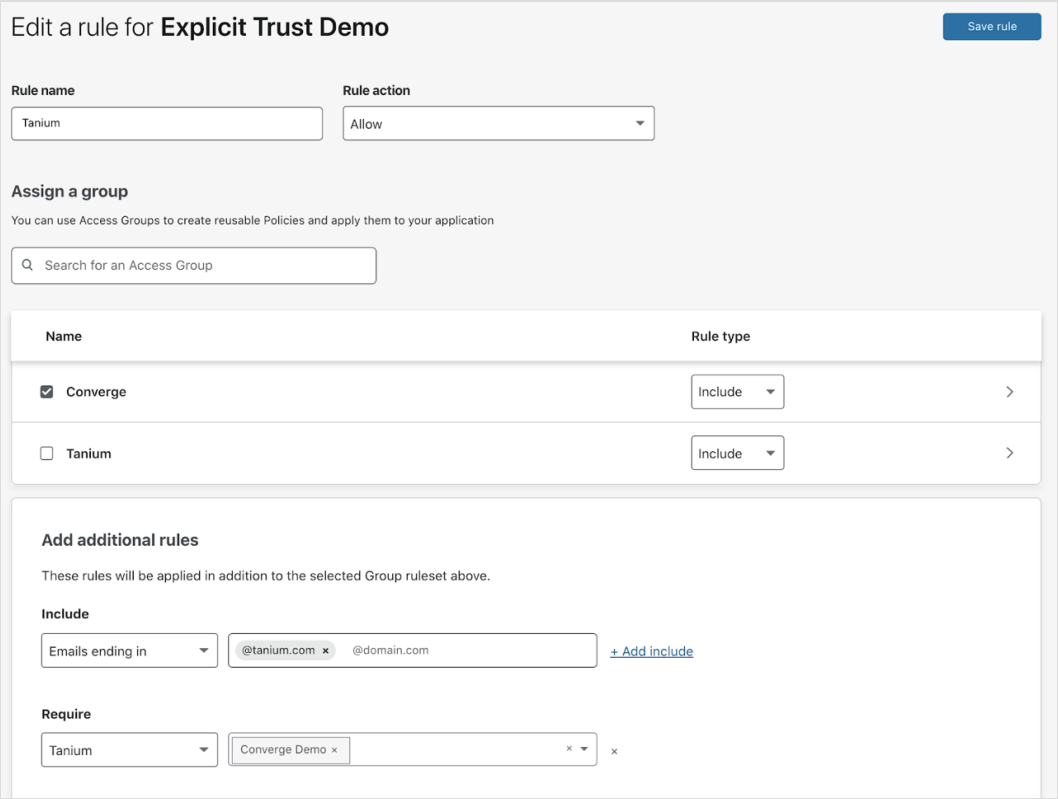
- Authentication domain. In Cloudflare for Teams, click **Access > Authentication > Login**. Verify that the authentication domain matches the domain in `config.json` or that you use `*.cloudflareaccess.com`.



- Device posture. In Cloudflare for Teams, click **Access > Authentication > Device Posture**. Click **Edit** for the Tanium endpoint protection provider. Verify the following:
    - **Port** matches the port number specified in `config.json`.
    - **Public key** is the `server-public.key`.
    - The certificate downloaded by clicking **Download Certificate** is the `client-public.key`.



- Application configuration. In Cloudflare for Teams, click **Access > Applications**. Click **Edit** for the application. Verify the following:
    - **Rule action** is set to **Allow**.
    - The **Include** rule specifies the type of users to include, for example, users with emails ending in @tanium.com.
    - The **Require** rule specifies **Tanium** and the name of the Tanium endpoint protection provider.



Remove Endpoint Identity tools from endpoints

You can deploy an action to remove Endpoint Identity tools from an endpoint.

1. In Interact, ask the question to target a specific operating system. For example, `Get Endpoint Identity - Tools Version from all machines with Is Windows equals True`.
2. Deploy an action to the targeted set of endpoints. Click **Deploy Action**. Deploy the package that is appropriate for the operating system:
    1. `Endpoint Identity - Remove Tools [Windows]`
    2. `Endpoint Identity - Remove Tools [Linux]`
    3. `Endpoint Identity - Remove Tools [Mac]`

3. (Optional) To remove the Endpoint Identity folder from the Tools folder, including the databases and logs, select **Remove saved data**.
4. Click **Show preview to continue**.
5. A results grid at the bottom of the page displays the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

If you have enabled Endpoint Configuration, tool removal must be approved in Endpoint Configuration before tools are removed from endpoints.

Contact Tanium Support

To contact Tanium Support for help, sign in to https://support.tanium.com.