Tanium Endpoint Management for Operational Technology User Guide

2026H2 Semiannual Release

Version 1.0

November 19, 2026



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://help.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 servicesprovided 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. We certify against the WCAG 2.2 / VPAT 2.5 standards for all major product modules. Tanium performs ongoing reassessments as appropriate, given the scope and type of changes to the UI and product features from release to release. In the most recent testing, the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.2 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 commercially reasonable efforts to address any gaps as quickly as is feasible, given the severity of the issue and scope of the changes. Tanium factors these objectives 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

©2026 Tanium Inc. All Rights Reserved

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, Tanium Support atsupport@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 the irrespective owners.

Kubernetes®, K8s®, and the Kubernetes logo are registered trademarks of The Linux Foundation®.

Android, ChromeOS, and Google are trademarks of Google LLC.

iOS, iPad, iPadOS, iPhone, Mac, and macOS are trademarks of Apple Inc., and registered in the U.S. and other countries and regions.

Patents: https://www.tanium.com/patents

Tanium Open Source Disclosure : https://tanium.github.io/opensource/

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview 7
- Entity providers 7
- Architecture 8
- Interoperability with other Tanium products 12

Getting started with Tanium Endpoint Management for Operational Technology 14

Requirements 15
- Core platform dependencies 15
- Solution dependencies 15
  - Tanium recommended installation 16
  - Import specific solutions 16
  - Required dependencies 16
  - Feature-specific dependencies 17
- Client extensions and endpoint tools 17
- Tanium™ Module Server 17
- Endpoints 18
  - Supported Internet protocols 18
  - Supported communication protocols 18
  - Supported operating systems 18
- Host and network security requirements 18
  - Ports 19
  - Security exclusions 20
- User role requirements 21

Installing 25
- Before you begin 25
- Import Endpoint Management for Operational Technology with default settings 26
- Import Endpoint Management for Operational Technology with custom settings 26
- Upgrade Endpoint Management for Operational Technology 26

©2026 Tanium Inc. All Rights Reserved

Verify Endpoint Management for Operational Technology version 26
Troubleshoot issues 27

Configuring 28
Install and configure Tanium Endpoint Configuration 28
Manage solution configurations with Tanium Endpoint Configuration 28
Approve configuration changes 30
Configure Tanium Endpoint Management for Operational Technology 30
Configure a satellite 30
(Optional) Restrict communication protocols from discovery 31
Example communication protocol restriction 32
Configure restricted communication protocols 34
Set up Tanium Endpoint Management for Operational Technology users 35

Upgrading 37
Before you begin 37
Upgrade Endpoint Management for Operational Technology 37

Ingesting operational technology devices 38
Plan and update network infrastructure to support Tanium Endpoint Management for Operational Technology 38
Create an OT satellite configuration 40
View the list of satellites 42
Filter satellite configurations list 42
View details of a single satellite 43
Edit a satellite configuration 43
Disable a satellite configuration 43
Enable a disabled satellite configuration 44
Delete a satellite configuration 44

Monitoring operational technology devices 45
Issue questions to target OT devices 45
Include OT devices in a report 47
Export OT device data using Tanium Connect 48

Using Tanium Exposure Management for Operational Technology 49
Create an operational technology scan assessment 49
Create an OT scan assessment 49

©2026 Tanium Inc. All Rights Reserved

View vulnerability findings for OT devices 50
View vulnerability findings for OT devices 51

Troubleshooting **52**
Collect logs 52
Collect troubleshooting information from the satellite 52
View and export the audit log 53
Cannot select a satellite running macOS for configuration 54
Cannot establish communications between satellite and OT devices 54
Cannot discover OT devices 55
EtherNet/IP devices not discovered on Linux satellite 55
An OT device appears more than once in Tanium 56
Contact Tanium Support 57

Reference: Endpoint Management for Operational Technology endpoint tools **58**

©2026 Tanium Inc. All Rights Reserved

Tanium Endpoint Management for Operational Technology overview

The Tanium Endpoint Management for Operational Technology entity provider uses a satellite endpoint to ingest operational technology (OT) device data into the Tanium environment. Ingesting OT device data alongside other endpoints in your network allows you to better manage all endpoints in Tanium™ Console, instead of using multiple endpoint management methods. You can view OT devices managed using Tanium Endpoint Management for Operational Technology in Tanium™ Console alongside devices managed using Tanium™ Client. If you also configure Tanium™ Exposure Management for Operational Technology, you can view vulnerability findings associated with OT device data in Tanium™ Comply.

Entity providers

All entities managed by Endpoint Management for Operational Technology are endpoints. You can ingest data from endpoints managed using Tanium Client and endpoints managed using other entity providers into the same Tanium instance to gain broader visibility into your entire network.

An *entity provider* is an adapter that ingests entity data into the Tanium environment. The Tanium environment uses this data to manage the entity. Entity providers collect entity data without installing Tanium Client on the endpoint. For example, you cannot install Tanium Client on mobile devices that run Android or iOS. You can configure the Tanium Connector for Microsoft Intune to integrate with a Microsoft Intune instance to ingest mobile device data.

- Management using Tanium Client: Tanium Client runs on endpoints that run a compatible operating system (OS), such as computers or virtual machines that run Linux, macOS, or Windows. These endpoints are generally part of the linear chain. Tanium Client reports information back to Tanium Core Platform through the linear chain.

- Management using entity providers: Entity providers collect device information through an integration, such as the Tanium Connector for Microsoft Intune that ingests Microsoft Intune mobile device data, or directly from an entity, such as OT devices (used to monitor industrial or operational machinery that uses OT protocols like Profinet or ControlBus). Management of these devices does not rely on Tanium Client being installed directly on an entity, but it might

©2026 Tanium Inc. All Rights Reserved

leverage a satellite endpoint with the Tanium Client installed to facilitate communication with the entity provider service. The entity provider might report endpoint information that is different from the information that a Tanium Client reports, due to the difference in entity type. For example, mobile devices are assigned an International Mobile Equipment Identity (IMEI) serial number, which are not assigned to other types of devices, such as an endpoint that runs Windows Server.

Each entity is associated with a **Provider Type**, **Provider Name**, and **Entity Type**, which identify how Tanium Core Platform manages the entity.

Entity providers and related sensor values

Entity Provider	Provider Type value	Provider Name value	Entity Type value
Tanium Client	Tanium Client	Tanium	Computer
Tanium Endpoint Management for Operational Technology	Operational Technology	*<configured-entity-provider-name>*	Operational Technology Device

Architecture

Tanium Endpoint Management for Operational Technology uses an endpoint configured as a satellite to ingest OT device data into the Tanium environment. If Tanium Exposure Management for Operational Technology is configured, this OT device data is associated with vulnerability findings using Tanium™ Comply.

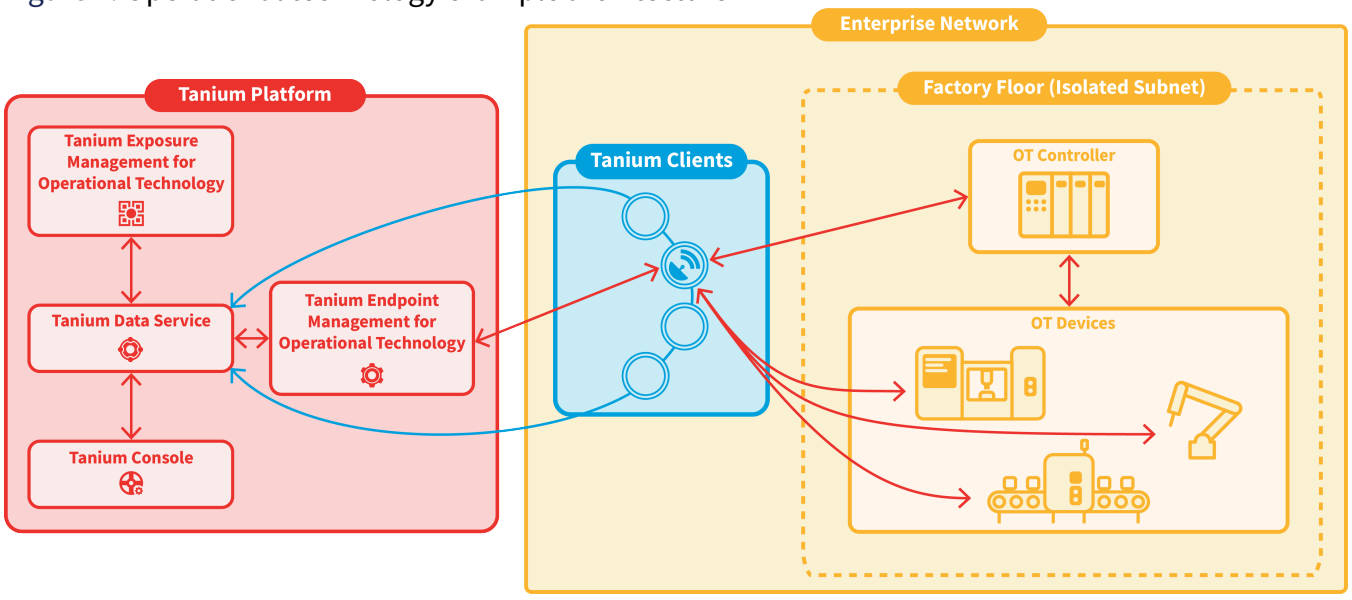
The Tanium™ Operational Technology shared service uses an endpoint configured as a satellite to communicate with OT devices. The satellite sends messages to devices that run supported communication protocols at a regular. The satellite receives a response and then sends the message to the Tanium environment, which caches the data in Tanium Data Service. If you configure Tanium™ Exposure Management for Operational Technology, vulnerability findings are associated with OT device data.

Tanium operators that issue questions in Tanium Console can target all types of managed entities, including endpoints managed using Tanium Endpoint Management for Operational Technology and those managed using Tanium Client. Tanium operators can also include endpoints managed using Tanium Endpoint Management for Operational Technology in Tanium Reporting reports and dashboards, view vulnerability finding data associated with OT devices in Tanium Comply, or export

©2026 Tanium Inc. All Rights Reserved

the data using Tanium Connect.

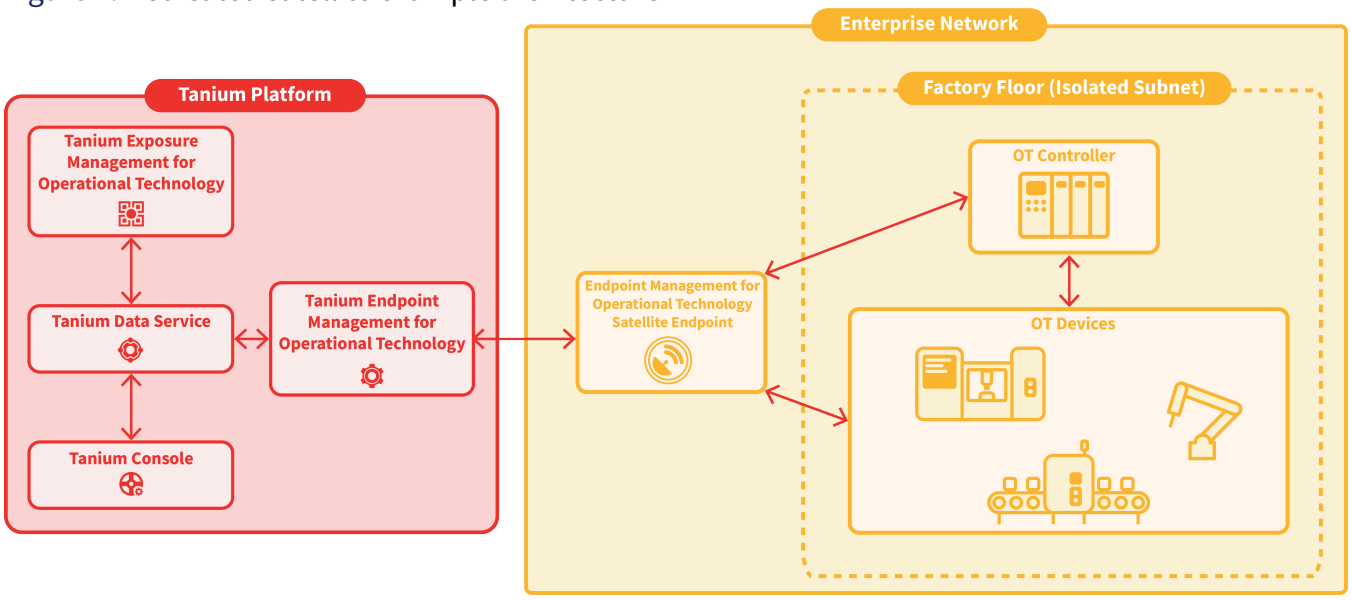
Figure 1. Operational technology example architecture



Satellite deployment

Based on your network architecture, the satellite endpoint can be a dedicated device that functions only as a satellite to communicate with the OT devices.

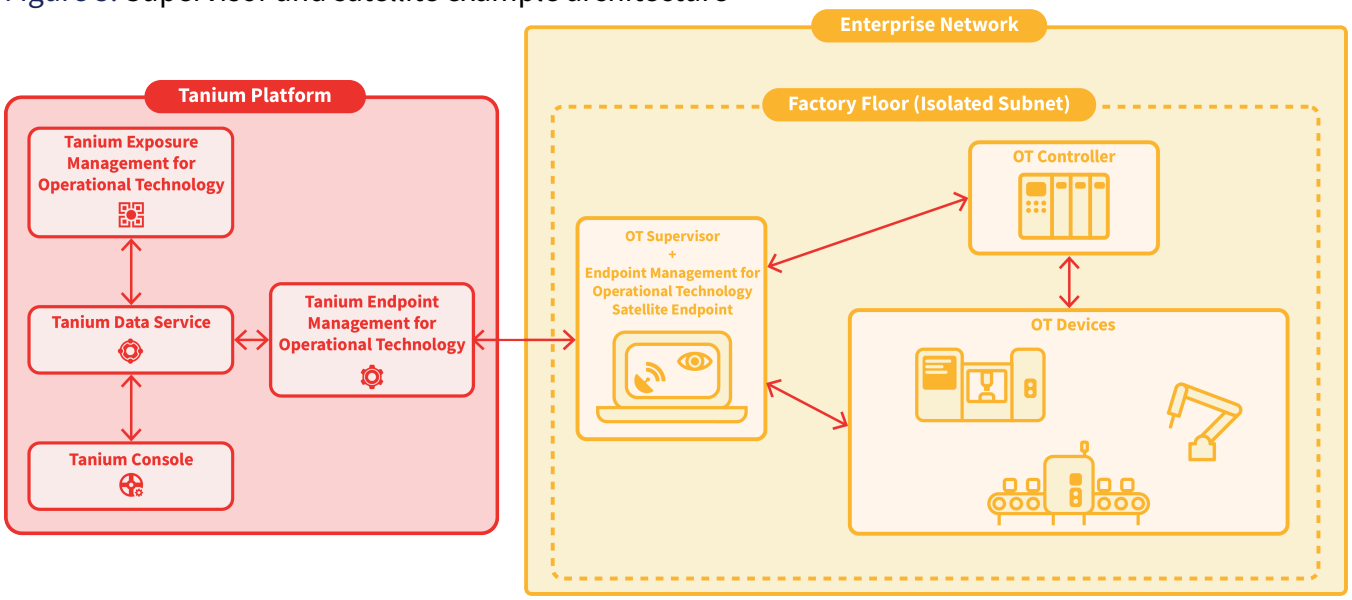
Figure 2. Dedicated satellite example architecture



If you deployed a Windows or Linux endpoint in an isolated subnet, such as an OT supervisor, you can also configure that endpoint as a satellite endpoint to communicate with the OT devices.

©2026 Tanium Inc. All Rights Reserved

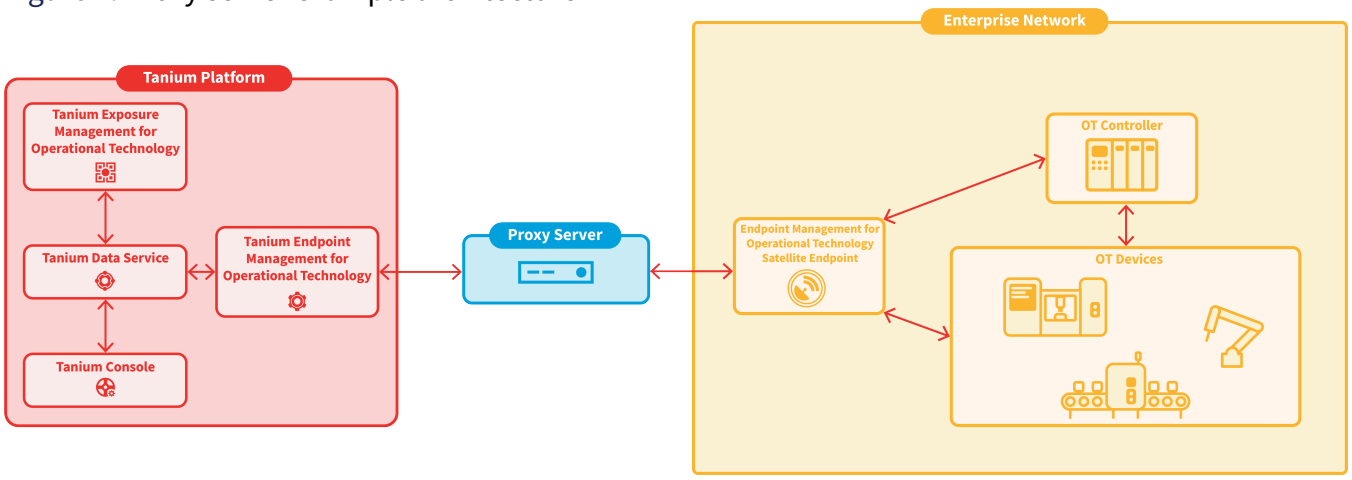
Figure 3. Supervisor and satellite example architecture



Routing traffic

Depending on your network architecture, if you cannot directly establish a connection between the satellite endpoint and Tanium Platform, you might need to deploy a proxy server to properly route traffic.

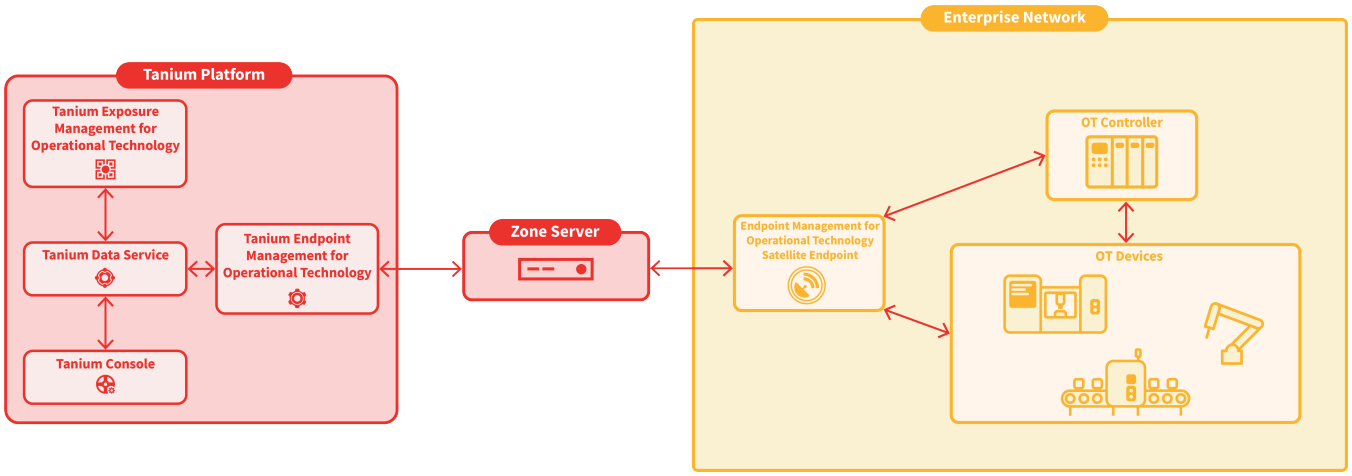
Figure 4. Proxy server example architecture



You can also deploy a Tanium™ Zone Server to route traffic. For more information, see Tanium Appliance User Guide: Installing individual Zone Servers.

Figure 5. Zone server example architecture

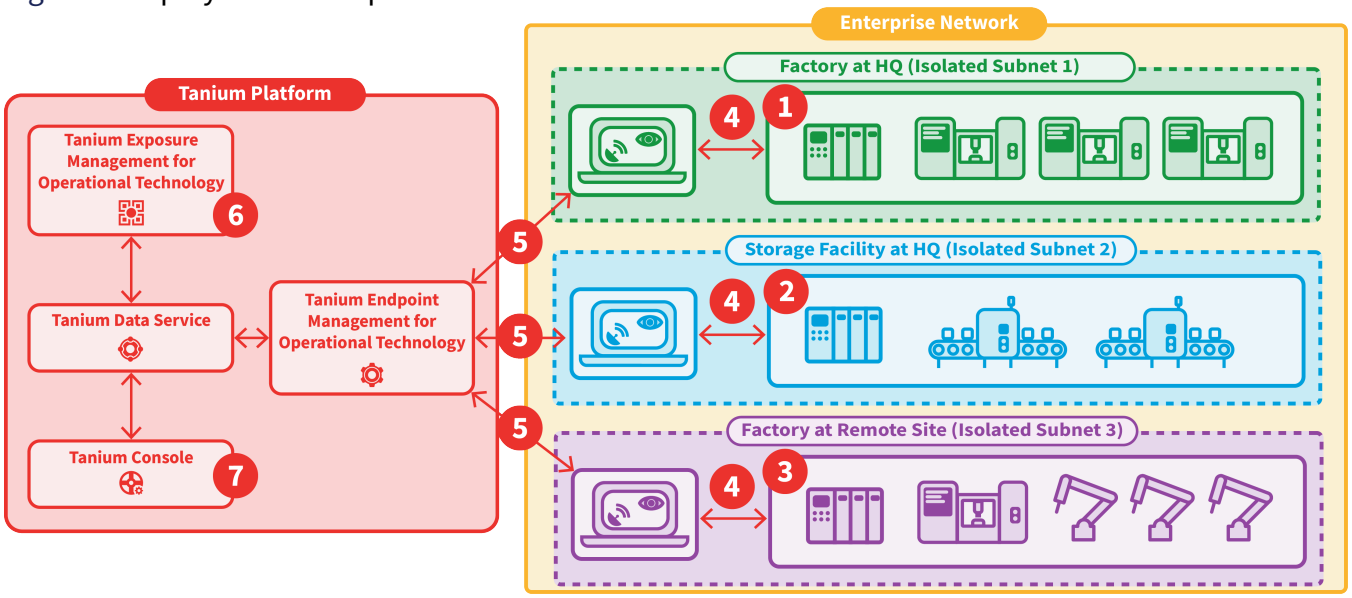
©2026 Tanium Inc. All Rights Reserved



Deployment example

The figure Figure 6. Deployment example architecture on page 11 shows an example enterprise architecture containing multiple isolated subnets and OT devices.

Figure 6. Deployment example architecture



1	The factory, located at headquarters, has an isolated subnet containing Profinet A and Profinet B devices, and a supervisor that runs Linux and is configured as a satellite.
2	The storage facility, located at headquarters, has an isolated subnet containing EtherNet/IP devices, and a supervisor that runs Windows and is configured as a satellite.
3	The factory, located remote to headquarters, has an isolated subnet containing EtherNet/IP, Profinet A, and Profinet B devices, and a supervisor that runs Windows and is configured as a satellite.

©2026 Tanium Inc. All Rights Reserved

4	Each configured satellite ingests OT device data from the isolated subnet.
5	OT device data is ingested into the Tanium environment, using Tanium Endpoint Management for Operational Technology .
6	Tanium Exposure Management for Operational Technology associates OT device data with vulnerability information
7	Tanium operators can view OT device information in Tanium Console.

Interoperability with other Tanium products

Interact

Endpoint Management for Operational Technology ingests OT device information, which you can target with Interact questions. For more information, see Tanium Interact User Guide: Asking questions and searching endpoints in Interact.

Connect

Endpoint Management for Operational Technology ingests OT device information, which can be exported to a destination using a Connect connection. For more information, see Tanium Connect User Guide: Managing connections.

Exposure Management for Operational Technology

Use Tanium™ Exposure Management for Operational Technology to configure Tanium™ Comply vulnerability assessments for OT endpoints and view vulnerability findings for those endpoints.

For more information, see Using Tanium Exposure Management for Operational Technology on page 49 and Tanium Comply User Guide: Creating vulnerability assessments.

Reporting

Endpoint Management for Operational Technology ingests OT device information, which can be included in Tanium™ Reporting dashboards and reports, and can be viewed in the **Endpoint Details**

©2026 Tanium Inc. All Rights Reserved

page. For more information, see Tanium Reporting User Guide: Working with dashboards, Tanium Reporting User Guide: Working with reports, and Tanium Reporting User Guide: Working with a single endpoint.

©2026 Tanium Inc. All Rights Reserved

Getting started with Tanium Endpoint Management for Operational Technology

Follow these steps to configure and use Tanium Endpoint Management for Operational Technology.

Step 1: Plan and implement network infrastructure updates to facilitate communication with OT devices

Identify a Windows or Linux endpoint that can establish bidirectional connections with OT devices using a physical wired connection. For more information, see Plan and update network infrastructure to support Tanium Endpoint Management for Operational Technology on page 38.

Step 2: Configure a satellite endpoint

Configure the Windows or Linux endpoint as a satellite. For more information, see Tanium Direct Connect User Guide: Managing satellites.

Step 3: Create a satellite configuration to ingest OT devices

Create a satellite endpoint configuration for the Operational Technology shared service, using the satellite to ingest OT device information. For more information, see Create an OT satellite configuration on page 40

Step 4: (Optional) Configure a vulnerability assessment scan method in Comply

If you want to use Tanium Exposure Management for Operational Technology to view vulnerability findings associated with an OT device, configure a vulnerability assessment scan method. For more information, see Using Tanium Exposure Management for Operational Technology on page 49.

©2026 Tanium Inc. All Rights Reserved

Tanium Endpoint Management for Operational Technology requirements

Review the requirements before you install and use Tanium Endpoint Management for Operational Technology.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Tanium Endpoint Management for Operational Technology. For more information about how to get Tanium Endpoint Management for Operational Technology, see Tanium Solutions & Bundles.

  > **Note:** OT devices ingested using Tanium Endpoint Management for Operational Technology do not count against endpoint licensing totals.

- Tanium license that includes Exposure Management for Operational Technology, if you want to view limited vulnerability information related to OT devices in Comply. For more information about how to get Exposure Management for Operational Technology, see Tanium Solutions & Bundles.
- **Tanium™ Core Platform** servers 7.8.2.1111
- Tanium Client 7.8.2.1111 or later

  > **Note:** Tanium Client is required to configure a satellite endpoint. Tanium Client is not installed on OT devices.

- **Tanium™ Console**

Solution dependencies

©2026 Tanium Inc. All Rights Reserved

Other Tanium solutions are required for Endpoint Management for Operational Technology to function (required dependencies) or for specific Endpoint Management for Operational Technology features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.

Note: Some Endpoint Management for Operational Technology dependencies have their own dependencies, which you can see in the lists of required and feature-specific dependencies below. Where a dependency links to its own user guide, that link opens the guide for the latest version of the solution, not necessarily the minimum version that Endpoint Management for Operational Technology requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Endpoint Management for Operational Technology, the Tanium Server automatically imports all your licensed solutions at the same time. For more information, see Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Tanium Endpoint Management for Operational Technology to import and are using Tanium Core Platform 7.8.2.3531 or later with Tanium Console 3.21 or later, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Tanium Endpoint Management for Operational Technology, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Tanium Endpoint Management for Operational Technology has the following required dependencies:

- Tanium™ Direct Connect
- Tanium™ Endpoint Configuration
- Tanium™ Operational Technology service
- Tanium™ RDB service

©2026 Tanium Inc. All Rights Reserved

Feature-specific dependencies

If you select only Tanium Endpoint Management for Operational Technology to import, you must manually import or update its feature-specific dependencies regardless of Tanium Console or Tanium Core Platform versions. Tanium Endpoint Management for Operational Technology has the following feature-specific dependencies:

- Tanium™ Interact to ask questions and retrieve OT device data
- Tanium™ Comply to view vulnerability information for an OT device
- Tanium™ Connect to export OT device data to a destination
- Tanium™ Reporting to include OT device data in reports and dashboards

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for endpoints. Client extensions perform tasks that are common to certain Tanium solutions. Each Client Extension and tool might have recommended security exclusions to allow them to run without interference. For a list of all Client Extensions and tools, see Reference: Client extensions used for Tanium solutions.

For more information, see Security exclusions on page 20.

Note: Endpoint Management for Operational Technology requires Client extensions and endpoint tools only on the configured satellite endpoint, not OT devices.

Note: The change management feature of Endpoint Configuration might affect the version of each endpoint tool installed on endpoints.

For more information, see Configure Tanium Endpoint Configuration on page 28.

Tanium™ Module Server

Tanium Endpoint Management for Operational Technology is installed and runs as a service on the

©2026 Tanium Inc. All Rights Reserved

Module Server host computer. The impact on the Module Server is minimal and depends on usage.

For more information about Module Server sizing in a Windows deployment, see Tanium Core Platform User Guide for Windows Deployments: Host system sizing guidelines.

Endpoints

Supported Internet protocols

Tanium Endpoint Management for Operational Technology supports IPv4 addresses.

Supported communication protocols

The following endpoint communication protocols are supported with Tanium Endpoint Management for Operational Technology.

- EtherNet/IP
- DeviceNet
- PROFINET A and B

Supported operating systems

The following endpoint operating systems are supported with Tanium Endpoint Management for Operational Technology satellites.

- Windows 8.1 or later
- Windows Server 2012 R2 or later
- Linux

Tanium Endpoint Management for Operational Technology does not deploy packages to endpoints. For more information about Tanium Client operating system support, see Tanium Client Management User Guide: Client version and operating system requirements.

Host and network security requirements

©2026 Tanium Inc. All Rights Reserved

Specific ports and processes are needed to run Endpoint Management for Operational Technology.

Ports

The following ports are required for Tanium Endpoint Management for Operational Technology communication.

> **Note:** If the satellite endpoint runs Linux, opening the required ports is not sufficient — configure the OS firewall (firewalld) to allow EtherNet/IP discovery responses. For more information, see EtherNet/IP devices not discovered on Linux satellite on page 55.

Source	Destination	Port	Protocol	Purpose
Satellite endpoint	EtherNet/IP device	44818	TCP	Establish connections between the satellite and EtherNet/IP devices
Satellite endpoint	EtherNet/IP device	44818	UDP	Allow communication between the satellite and EtherNet/IP devices
EtherNet/IP device	Satellite endpoint	1024–65535	UDP	EtherNet/IP discovery response from EtherNet/IP device to satellite
Satellite endpoint	PROFINET A or B device	34962	UDP	Establish connections for unicast communications between the satellite and PROFINET A or B devices
Satellite endpoint	PROFINET A or B device	34963	UDP	Establish connections for multicast communications between the satellite and PROFINET A or B devices
Satellite endpoint	PROFINET B device	161	UDP	Establish SNMP connections between the satellite and PROFINET B devices
Satellite endpoint	PROFINET B device	162	UDP	Establish SNMP connections between the satellite and PROFINET B devices

©2026 Tanium Inc. All Rights Reserved

Best Practice: Configure firewall policies to open ports for Tanium traffic with TCP-based rules instead of application identity-based rules. For example, on a Palo Alto Networks firewall, configure the rules with service objects or service groups instead of application objects or application groups.

Security exclusions

If antivirus (AV) or other security software is in use in the environment to monitor and block unknown host system processes, Tanium requires that a security administrator create exclusions to allow the Tanium processes to run without interference. This software can include security applications that are included with an endpoint operating system, such as fapolicyd on some Linux distributions, or Microsoft Defender on Windows. The configuration of these exclusions varies depending on the security software.

For more information about security exclusions to define across Tanium, see Tanium Client Management Guide: Reference: Endpoint security exclusions.

Note: If the required exclusions are not configured, or if Tanium suspects interference from AV or security software, Tanium might require you to remove or disable the AV or security software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.

Endpoint Management for Operational Technology security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	*<Tanium Client>* \TaniumCX.exe
		File	*<Tanium Client>* \TaniumEntity.dll
		File	*<Tanium Client>* \TaniumEntity.dll.sig
	for discovering OT devices that run EtherNet/IP	Process	*<Tanium Client>* \extensions\entity\providers\TaniumEthernetIpEntityProvider.exe
	for discovering OT devices that run Profinet	Process	*<Tanium Client>* \extensions\entity\providers\TaniumProfinetEntityProvider.exe
Linux		Process	*<Tanium Client>* /TaniumCX

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /TaniumEntity.so
		File	*<Tanium Client>* /TaniumEntity.so.sig
	for discovering OT devices that run EtherNet/IP	Process	*<Tanium Client>* /extensions/entity/providers/TaniumEthernetIpEntityProvider
	for discovering OT devices that run Profinet	Process	*<Tanium Client>* /extensions/entity/providers/TaniumProfinetEntityProvider

User role requirements

The following tables list the role permissions required to use Tanium Endpoint Management for Operational Technology. For more information about predefined roles, see Set up Tanium Endpoint Management for Operational Technology users on page 35.

Predefined roles grant the following permissions, which are required to use Endpoint Management for Operational Technology functionality:

- solution permissions on page 22
- administration and platform content permissions on page 23: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Endpoint Management for Operational Technology users on page 35.



Note: Do not assign the **Operational Technology Service Account** and **Operational Technology Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Some Endpoint Management for Operational Technology solution permissions provide permissions that are associated with other solutions. Furthermore, all the platform content permissions and some solution permissions apply to content sets that might contain content for other solutions in addition to Endpoint Management for Operational Technology. If you create custom roles for

©2026 Tanium Inc. All Rights Reserved

Endpoint Management for Operational Technology users, be sure to assign all the solution permissions and content set permissions that are required for Endpoint Management for Operational Technology functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined roles. For more information, see the following sections of the Tanium Console User Guide:

- RBAC overview (provides an overview of roles, permissions, and content sets)
- Provided role permissions
- View effective role permissions
- Configure a custom role

Tanium Endpoint Management for Operational Technology solution permissions

Permission	Operational Technology Administrator [1]	Operational Technology Read-Only User [1]
Operational Technology View the Operational Technology workbench	✓ READ SHOW WRITE	✓ READ SHOW
Operational Technology Administrator Read sensors and packages in Operational Technology, write actions in Operational Technology	✓ SPECIAL	✗
Operational Technology Api User Operational Technology service APIs	✓ EXECUTE	✓ EXECUTE
Operational Technology Audit View Operational Technology audit logging	✓ READ	✗
Operational Technology Protocol Restriction Access communication protocol restrictions in the Operational Technology service	✓ READ WRITE	✓ READ
Operational Technology Read Only Read sensors, packages, and actions in Operational	✗	✓ READ

©2026 Tanium Inc. All Rights Reserved

Permission	Operational Technology Administrator [1]	Operational Technology Read-Only User [1]
Technology		
Operational Technology Support Bundle Download a support bundle for Operational Technology	✓ READ	✗

[1] The permissions for this role provide solution permissions for other solutions. To view the provided permissions, see View effective role permissions .

Tanium Endpoint Management for Operational Technology administration and platform content permissions

Permission	Permission Type	Operational Technology Administrator	Operational Technology Read-Only User
Action Group	Administration	✓ READ	✗
Action	Platform Content	✓ READ WRITE	✓ READ
Own Action	Platform Content	✓ READ	✗
Package	Platform Content	✓ READ	✓ READ
Plugin	Platform Content	✓ EXECUTE READ	✓ EXECUTE READ
Sensor	Platform Content	✓ READ	✓ READ

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Operational Technology Administrator	Operational Technology Read-Only User
To view the content sets to which the platform content permissions apply, see View effective role permissions .			

©2026 Tanium Inc. All Rights Reserved

Installing Tanium Endpoint Management for Operational Technology

About this task

Use Tanium Console **Solutions** page to install Endpoint Management for Operational Technology and choose either automatic or manual configuration:

- Automatic configuration with default settings: Endpoint Management for Operational Technology is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Endpoint Management for Operational Technology, see Import Endpoint Management for Operational Technology with default settings on page 26.

- Manual configuration with custom settings: After installing Endpoint Management for Operational Technology, you must manually configure required settings. Select this option only if Endpoint Management for Operational Technology requires settings that differ from the recommended default settings. For more information, see Import Endpoint Management for Operational Technology with custom settings on page 26.

Before you begin

- Read the release notes.

- Review the Tanium Endpoint Management for Operational Technology requirements on page 15.

- Assign the correct roles to users for Endpoint Management for Operational Technology. Review the User role requirements on page 21.

    - To create a satellite, you must be assigned the Administrator reserved role, the Operational Technology Administrator system role, or a role that has the **Direct**

©2026 Tanium Inc. All Rights Reserved

Connect Satellite write permission.

- To configure a satellite to ingest OT device data, you must be assigned the Administrator reserved role or the Operational Technology Administrator system role.

Import Endpoint Management for Operational Technology with default settings

About this task

No default settings are configured for Tanium Endpoint Management for Operational Technology.

To import Endpoint Management for Operational Technology and configure default settings, see Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed: see Verify Endpoint Management for Operational Technology version on page 26.

Import Endpoint Management for Operational Technology with custom settings

About this task

To import Endpoint Management for Operational Technology without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** option while performing the steps in Tanium Console User Guide: Import or update specific solutions. After the import, verify that the correct version is installed: see Verify Endpoint Management for Operational Technology version on page 26.

Other Tanium solutions are required for Endpoint Management for Operational Technology to function (required dependencies) or for specific Endpoint Management for Operational Technology features to work (feature-specific dependencies).

Upgrade Endpoint Management for Operational Technology

Verify Endpoint Management for Operational Technology version

©2026 Tanium Inc. All Rights Reserved

About this task

After you import or upgrade Endpoint Management for Operational Technology, verify that the correct version is installed:

1. Refresh your browser.
2. From the Main menu, go to **Shared Services** > **Operational Technology**.
3. To display version information, click Info .

Troubleshoot issues

About this task

If you experience issues with installing Endpoint Management for Operational Technology, see Troubleshooting Tanium Endpoint Management for Operational Technology on page 52.

©2026 Tanium Inc. All Rights Reserved

Configuring Tanium Endpoint Management for Operational Technology

If you did not install Endpoint Management for Operational Technology with the **Apply All Tanium recommended configurations** option, you must enable and configure certain features.

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

Tanium Endpoint Configuration delivers configuration information and required tools for Tanium Solutions to endpoints. Endpoint Configuration consolidates the configuration actions that traditionally accompany additional Tanium functionality and eliminates the potential for timing errors that occur between when a solution configuration is made and the time that configuration reaches an endpoint. Managing configuration in this way greatly reduces the time to install, configure, and use Tanium functionality, and improves the flexibility to target specific configurations to groups of endpoints.

Endpoint tools are bundled together in a versioned toolset. Each toolset contains a specific version of each tool. The Endpoint Configuration Toolset Solution provides upgrades to the toolset, and it imports upgraded versions of the entire toolset as needed by upgraded or newly installed solutions.

©2026 Tanium Inc. All Rights Reserved

Important:

When you upgrade Endpoint Management for Operational Technology, the change management feature enables you to perform a staged rollout of the endpoint tools associated with the new version of Endpoint Management for Operational Technology. Endpoint Management for Operational Technology remains compatible with earlier versions of the endpoint tools and so continues to function with endpoints in rings that have not yet received the latest tools. However, any functionality added in the upgrade of Endpoint Management for Operational Technology might not be available on these endpoints until they receive the upgraded tools.

In some cases, multiple solutions install the same endpoint tool, but upgraded endpoint tools remain compatible with all associated solutions. For example, both Tanium™ Threat Response and Tanium™ Reveal install and use index-cx. When you upgrade Threat Response, it might install version x.6.yyyy of index-cx, superseding version x.5.zzzz that Reveal previously installed. The index-cx upgrade from Threat Response does not affect the Index-related functionality of Reveal on the upgraded endpoints. For more information about the change management feature, see Tanium Endpoint Configuration User Guide: Managing endpoint tool upgrade rollouts.

Note: For information about how to install Endpoint Configuration, see Installing Endpoint Configuration.

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Endpoint Management for Operational Technology, see User role requirements. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Managing approvals.

©2026 Tanium Inc. All Rights Reserved

Important: For solutions to perform configuration changes or tool deployment through Endpoint Configuration on endpoints with action locks turned on, you must enable the **Manifest Package Ignore Action Lock** and **Deploy Client Configuration and Support Package Ignore Action Lock** settings. To access these settings, from the Endpoint Configuration **Overview** page, click Settings and select **Global**. For more information about action locks, see Managing action locks.

For more information about Endpoint Configuration, see Tanium Endpoint Configuration User Guide.

Approve configuration changes

If you enabled configuration approvals, the following configuration changes must be approved in Endpoint Configuration before they deploy to endpoints:

- Creating, updating, or deleting patch lists
- Adding or removing enforcements
- Removing all enforcements
- Updating scan configuration priorities
- Creating deployments
- Stopping deployments
- Adding targets to deployments
- User-initiated actions, such as initializing endpoints, uploading custom field files, enabling Linux

Configure Tanium Endpoint Management for Operational Technology

Configure a satellite

To ingest OT device data into the Tanium environment, configure an endpoint that runs Windows 8.1 or later, Windows Server 2012 R2 or later, or a Linux distribution as a satellite that can communicate

©2026 Tanium Inc. All Rights Reserved

with the OT devices. Ensure that the satellite can establish bidirectional connections with OT devices using a physical wired connection. For more information, see Tanium Direct Connect User Guide: Managing satellites.

Note: Configuring a satellite requires the **Direct Connect Satellite write** permission. The **Operational Technology Administrator** and **Direct Connect Satellite Operator** system roles have this permission.

(Optional) Restrict communication protocols from discovery

By default, you can configure a satellite endpoint to discover all supported communication protocols. You can restrict communication protocol discovery based on content set access, or prevent all discovery of a communication protocol. Configure communication protocol restriction when your network does not have any devices running a communication protocol, or if you want to further limit access to configure communication protocol discovery based on the following RBAC permissions.

Permissions required for restricting communication protocols

Permission	Allowed functionality
Operational Technology Protocol Restriction read permission on a content set	View a content set when configuring communication protocol restrictions
Operational Technology Protocol Restriction write	Update a communication protocol restriction
Operational Technology write permission (on at least one content set associated with a restricted protocol)	Add a restricted protocol to a satellite configuration **Note:** If you do not have the **Operational Technology write** permission on at least one content set for a restricted protocol, or the communication protocol is restricted and not allowed at all, you can remove the communication protocol from an existing satellite configuration, but you cannot add the communication protocol to a new or existing satellite configuration.

Note: Updating a protocol restriction applies to all satellite configurations created after the update, but does not update existing satellite configurations.

©2026 Tanium Inc. All Rights Reserved

EXAMPLE COMMUNICATION PROTOCOL RESTRICTION

Consider an example Tanium deployment with two Operational Technology content sets, **Example Operational Technology** and **Example Protocol Restriction**. The following example users have certain Operational Technology permissions.

Example Tanium users and assigned Operational Technology permissions

Tanium user	Assigned Operational Technology roles and permissions
Tanium administrator	• **Operational Technology write** permission • **Operational Technology Protocol Restriction write** permission • **Operational Technology Protocol Restriction read** permission on the **Example Operational Technology** content set • **Operational Technology Protocol Restriction read** permission on the **Example Protocol Restriction** content set
Tanium operator A	• **Operational Technology write** permission on the **Example Operational Technology** content set • **Operational Technology write** permission on the **Example Protocol Restriction** content set
Tanium operator B	• **Operational Technology write** permission on the **Example Operational Technology** content set

If the Tanium administrator configures one of the following protocol restrictions, that restriction has an effect on how Tanium operator A and Tanium operator B create or edit a satellite configuration.

Communication protocol restriction effect on satellite configuration

Protocol restriction	Tanium operator A satellite configuration	Tanium operator B satellite configuration
EtherNet/IP is **Not Allowed**	• Tanium operator A cannot add the EtherNet/IP protocol to new and existing satellite configurations. • Tanium operator A can remove the EtherNet/IP protocol from an existing satellite configuration, but	• Tanium operator B cannot add the EtherNet/IP protocol to new and existing satellite configuration. • Tanium operator B can remove the EtherNet/IP protocol from an existing satellite configuration, but cannot subsequently add the EtherNet/IP protocol to that satellite configuration.

©2026 Tanium Inc. All Rights Reserved

Protocol restriction	Tanium operator A satellite configuration	Tanium operator B satellite configuration
	cannot subsequently add the EtherNet/IP protocol to that satellite configuration.	
EtherNet/IP has **No Restrictions**	Tanium operator A can add the EtherNet/IP protocol to new and existing satellite configurations.	Tanium operator B can add the EtherNet/IP protocol to new and existing satellite configurations.
EtherNet/IP is **Restricted**, requiring the **Operational Technology Protocol Restriction write** permission on the **Example Operational Technology** or **Example Protocol Restriction** content set to configure	Tanium operator A can add the EtherNet/IP protocol to new and existing satellite configurations.	Tanium operator B can add the EtherNet/IP protocol to new and existing satellite configurations.
Profinet B is **Restricted**, requiring the **Operational Technology Protocol Restriction write** permission on the **Example Protocol Restriction** content set to configure	Tanium operator A can add the Profinet B protocol to new and existing satellite configurations.	**Creating a satellite configuration:** The PROFINET B row is not visible. Tanium operator B cannot enable PROFINET B. **Editing an existing satellite configuration:** • If PROFINET B is currently enabled on the satellite configuration, the PROFINET B row is visible. Tanium operator B can keep the protocol enabled or disable it. If Tanium operator B disables PROFINET B and saves, the PROFINET B row is not visible on subsequent edits. • If PROFINET B is not currently enabled on the satellite configuration, the PROFINET B row is not visible. Tanium operator B cannot enable PROFINET B.
DeviceNet Scanner is **Restricted**, requiring the **Operational Technology Protocol Restriction**	Tanium operator A can add the **DeviceNet Scanner** discovery option to new and existing	• Tanium operator B cannot add the **DeviceNet Scanner** discovery option to a satellite configuration.

©2026 Tanium Inc. All Rights Reserved

Protocol restriction	Tanium operator A satellite configuration	Tanium operator B satellite configuration
write permission on the **Example Protocol Restriction** content set to configure	satellite configurations.	Tanium operator B can remove the **DeviceNet Scanner** discovery option from an existing satellite configuration, but cannot subsequently add the **DeviceNet Scanner** discovery option to that satellite configuration.

Note: When a restricted sub-protocol (such as PROFINET B or DeviceNet) is already enabled on a satellite configuration, operators without the required content set access can see the protocol row on the edit form and choose to keep or disable it. If an operator without access disables the protocol and saves, the row is no longer visible to that operator on subsequent edits. If the protocol is not currently enabled on the satellite configuration, the row is not visible and the operator cannot enable it.

Note: If you disable a parent protocol, such as PROFINET or EtherNet/IP, the restricted sub-protocol, such as PROFINET B or DeviceNet, is also disabled on save.

CONFIGURE RESTRICTED COMMUNICATION PROTOCOLS

Configure communication protocol restrictions from the Protocols page.

1. From the Main menu, go to **Shared Services** > **Operational Technology**.
2. Click Settings.
3. Click Edit next to the communication protocol that you want to update.
4. Select a restriction type:
   - Select **No Limitations** to allow Tanium operators to add this communication protocol to a satellite configuration without additional permissions on content sets.
   - Select **Limit to Content Set** and then select one or more content sets. Tanium operators must be assigned the **Operational Technology Protocol Restriction write** permission on at least one selected content set to add the communication protocol

©2026 Tanium Inc. All Rights Reserved

to a satellite configuration.

- Select **Do Not Allow** to prevent Tanium operators from adding this communication protocol to a satellite configuration.

5. Click **Apply**.

Set up Tanium Endpoint Management for Operational Technology users

You can use the following set of predefined user roles to set up Tanium Endpoint Management for Operational Technology users.

To review specific permissions for each role, see User role requirements on page 21.

Important: On installation, Tanium Endpoint Management for Operational Technology creates a Endpoint Management for Operational Technology user to automatically manage the Endpoint Management for Operational Technology service account. Do not edit or delete the Endpoint Management for Operational Technology user.

For more information about how to assign user roles, see Tanium Console User Guide: Manage role assignments for a user.

Tip: To provide just-in-time access or scalable standing access to Endpoint Management for Operational Technology functionality, you can use SCIM provisioning combined with Tanium user groups. This approach lets you manage user access at scale or ad hoc through your identity provider, without creating users individually in Tanium. For more information, see Provision users into Tanium user groups with SCIM.

Operational Technology Administrator

Assign the **Operational Technology Administrator** role to users who manage the configuration of Operational Technology service functionality, including satellite configuration. This role can perform the following tasks:

- Configure Operational Technology service settings.
- View and modify Operational Technology satellite configurations.

©2026 Tanium Inc. All Rights Reserved

- View the audit log.

Operational Technology Read Only User

Assign the **Operational Technology Read Only User** role to users who need visibility into the Operational Technology service and satellite configuration. This role can view Operational Technology satellite configurations.

> **Note:** Do not assign the **Operational Technology Service Account** and **Operational Technology Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

©2026 Tanium Inc. All Rights Reserved

Upgrading Endpoint Management for Operational Technology

Before you begin

Important: In Endpoint Management for Operational Technology , the steps required to configure the service account are no longer necessary due to the adoption of the System User Service, which performs these tasks automatically. Additionally, the Endpoint Management for Operational Technology database is migrated to RDB in this release. Consequently, after upgrading to Endpoint Management for Operational Technology , it might take time for the database migration to complete and for RBAC privileges and other updates to sync properly. This could lead to issues and error messages when you first query Tanium Console. These issues usually resolve on their own after a few minutes, but could take up to an hour or longer depending on system resources and the amount of data to migrate.

- Read the .
- Review the Tanium Endpoint Management for Operational Technology requirements on page 15.

Upgrade Endpoint Management for Operational Technology

For the steps to upgrade Endpoint Management for Operational Technology, see Tanium Console User Guide: Managing Tanium solutions. After the upgrade, verify that the correct version is installed: see Verify Endpoint Management for Operational Technology version on page 26.

©2026 Tanium Inc. All Rights Reserved

Ingesting operational technology devices

Use an endpoint configured as a satellite to communicate with OT devices and ingest OT device information into the Tanium environment. Ingesting OT device data alongside other endpoints in your network allows you to better manage all endpoints in Tanium Console.

Plan and update network infrastructure to support Tanium Endpoint Management for Operational Technology

Plan updates to your network infrastructure to allow communication between OT devices and a satellite endpoint. Your network infrastructure must comply with the following guidelines.

About this task

- Ensure that OT devices comply with the respective communication protocol requirements.

  #### Port and protocol requirements for operational technology scans

Communication protocol	Communication protocol requirements	Open ports for bidirectional traffic
EtherNet/IP	Ensure that EtherNet/IP devices have a unique device name and IP address.	44818/TCP, 44818/UDP
PROFINET A and B	Ensure that PROFINET A and B devices have a unique MAC address and IP address.	161/UDP (B only), 162/UDP (B only), 34962/UDP, 34963/UDP

- Identify an endpoint that runs Windows 8.1 or later, Windows Server 2012 R2 or later, or a Linux distribution that runs on x86-64 architecture. Ensure that the endpoint has at least one physical network interface. Verify that this endpoint can establish a wired, bidirectional connection with the OT devices, and can be configured as a satellite endpoint. Configure the endpoint as a satellite. For more information, see Configure a satellite on page 30 and Tanium Direct Connect User Guide: Managing satellites.

©2026 Tanium Inc. All Rights Reserved

Note: Tanium Endpoint Management for Operational Technology does not support using a satellite running macOS.

Note: You can configure a satellite to discover one or multiple supported communication protocols.

Do not configure more than one satellite for a communication protocol you want to discover within a subnet. If multiple satellites are configured to discover the same communication protocol in a subnet, an OT device that runs the communication protocol can be ingested by each satellite. This creates multiple devices, which are not deduplicated in Tanium.

- Ensure that your network allow list and block list rules permit the satellite to send broadcast traffic to discover OT devices.
    - Configure network allow list and block list rules to allow broadcast traffic from the satellite to OT devices in the entire ephemeral port range, and to allow UDP broadcast response traffic from the OT devices to the satellite.

      ### Operational technology communication protocol broadcast addresses

Communication protocol	Broadcast address
EtherNet/IP	reserved IP address 255.255.255.255 over UDP
PROFINET A and B	reserved MAC address 01:0E:CD:00:00:00 using PROFINET Discovery and Basic Configuration protocol (PROFINET DCP)

    - Configure network allow list and block list rules to allow traffic between the satellite and OT devices over the open ports for a communication protocol.
    - Configure network allow list and block list rules to block broadcast traffic between the satellite and any devices that you do not want to receive this traffic.

©2026 Tanium Inc. All Rights Reserved

> **Important:** If the satellite endpoint runs Linux, you must also configure the OS-level firewall on the satellite endpoint. Network firewall rules alone are not sufficient for EtherNet/IP discovery. For more information, see EtherNet/IP devices not discovered on Linux satellite on page 55.

- Certain Cisco VLAN-based switches might have issues with forwarding specific PROFINET RT packets. Enable voice VLAN on the switch to prioritize PROFINET RT traffic and ensure that the switch can properly forward packets within the network. For more information, see the Cisco switch documentation.

Create an OT satellite configuration

Create an OT satellite configuration, associated with a satellite endpoint, to communicate with OT devices and ingest OT device data.

> **Note:**
>
> To create an OT satellite configuration, you need the following permissions:
>
> - To create the OT satellite configuration, you require a role with the **Operational Technology write** permission.
> - If a communication protocol is restricted to a content set, you require a role with the **Operational Technology write** permission on the content set.
> - To select a satellite, you require a role with the **Direct Connect Satellite read** permission.
>
> The **Operational Technology Administrator** system role has these permissions.

1. From the Main menu, go to **Shared Services** > **Operational Technology**.
2. Click **Add Satellite Configuration**.
3. Enter a satellite configuration **Name**.
4. Enter an OT device **Location**. Devices ingested by this entity provider are identified with this

©2026 Tanium Inc. All Rights Reserved

descriptive value, and this value does not affect device naming.

5. Select a **Satellite** endpoint. If you do not have a valid satellite endpoint, click **Create Satellite** to create a satellite endpoint, then select it. For more information about how to configure a satellite, see Tanium Direct Connect User Guide: Managing satellites.

6. Select communication **Protocols** associated with OT devices that you want the satellite to ingest.

   Note: If configured, you must have the **Operational Technology write** permission on at least one content set required to add a communication protocol. For more information about restricting communication protocols from a satellite configuration, see (Optional) Restrict communication protocols from discovery on page 31.

   Note: Restricted sub-protocols are only visible to operators who have the required content set access.

   Note:
   Do not configure more than one satellite for a communication protocol you want to discover within a subnet. If multiple satellites are configured to discover the same communication protocol in a subnet, an OT device that runs the communication protocol can be ingested by each satellite. This creates multiple devices, which are not deduplicated in Tanium.

   Note: Selecting **Enable module discovery (DeviceNet)** enables module discovery for EtherNet/IP devices and generates additional network traffic. Select this option only if your network can support the increased traffic volume. If **Enable module discovery (DeviceNet)** is restricted to a content set and you do not have permission for that content set, the configuration saves, but module discovery is disabled.

7. Select a schedule type.
   - Select **Interval** to enter an amount of time that elapses before the satellite discovers OT devices again.
   - Select **Schedule** to use the provided controls to set the schedule of when the satellite discovers OT devices, and the duration of the satellite discovery window.

     The following frequency options are available:

©2026 Tanium Inc. All Rights Reserved

- One run per day
- One run per day, on selected days of the week
- One run per month, on selected day of the month

> **Note:** If you select a day that does not exist in certain months, such as `29`, `30`, or `31`, discovery occurs on the last day of those months.

8. Click **Save**.

View the list of satellites

About this task

To view the status of your satellite configurations:

- From the Main menu, go to **Shared Services** > **Operational Technology** and then go to the **Discovery and Management** section.

A list of your satellite configurations appears with status information.

Filter satellite configurations list

If you have many satellite configurations, you can filter or order the list.

- To filter on a specific satellite configuration, enter the satellite configuration name in the **Filter items** field. The list updates with any satellite configuration names that contain the value you entered. To clear the filter, click **X** in the **Filter items** field.
- To filter on specific columns, click Filters to expand the filters, then enter text in a filter field or select a filter option. To clear the filter, click **X** within the pill that represents the filter value.
- Click a column header to sort the satellites by the data in the column in descending order. Click the column header again to sort the list in ascending order. To clear the sort, click the column header a third time.

©2026 Tanium Inc. All Rights Reserved

View details of a single satellite

Click View Details to view the details of a satellite configuration.

Edit a satellite configuration

If your network architecture changes, such as by needing a different satellite endpoint to discover OT devices or adding OT devices that run a different communication protocol, or you want to change the discovery interval, edit the satellite configuration.

1. From the Main menu, go to **Shared Services** > **Operational Technology**.
2. Select a satellite configuration.
3. Click Edit .
4. Update the **Name**, **Location**, **Satellite**, and communication **Protocols**.

   > **Note:** If configured, you must have the **Operational Technology write** permission on at least one content set required to add a communication protocol. If a restricted sub-protocol is already enabled on the satellite configuration, the protocol row is visible regardless of your content set access, and you can keep or disable it. If a restricted sub-protocol is not currently enabled, the row is not visible and you cannot enable it without the required content set access.

   > **Note:** Selecting **Enable module discovery (DeviceNet)** enables module discovery for EtherNet/IP devices and generates additional network traffic. Select this option only if your network can support the increased traffic volume. If **Enable module discovery (DeviceNet)** is restricted to a content set and you do not have permission for that content set, the configuration saves, but module discovery is disabled.

5. Click **Save**.

Disable a satellite configuration

Disabling a satellite configuration stops communication between the satellite endpoint and OT devices. Disable a satellite configuration if you want to pause discovery temporarily, such as for maintenance purposes.

©2026 Tanium Inc. All Rights Reserved

About this task

Note: OT device data that this satellite already ingested remains in the Tanium environment. This device data does not update unless you enable the satellite configuration and resume communication protocol discovery.

1. From the Main menu, go to **Shared Services** > **Operational Technology**.
2. Select an enabled satellite configuration.
3. Click **Disable** and then confirm your selection.

Enable a disabled satellite configuration

If you enable a disabled satellite configuration, the satellite resumes communication protocol discovery. Existing OT device data in the Tanium environment is updated with changes since the most recent discovery. New OT device data that matches the satellite configuration is ingested into the Tanium environment.

1. From the Main menu, go to **Shared Services** > **Operational Technology**.
2. Select a disabled satellite configuration.
3. Click **Enable** and then confirm your selection.

Delete a satellite configuration

Deleting a satellite configuration also removes all OT devices ingested using the satellite endpoint from the Tanium environment.

The satellite endpoint itself is not affected, and neither are any configurations other Tanium solutions have for that endpoint.

1. From the Main menu, go to **Shared Services** > **Operational Technology**.
2. Select a satellite configuration.
3. Click Delete and then confirm your selection.

©2026 Tanium Inc. All Rights Reserved

Monitoring operational technology devices

You can target endpoints managed using Tanium Endpoint Management for Operational Technology in Interact questions, include these endpoints in Reporting reports and dashboards, or export the data from these endpoints using Connect. You can include OT device data with other endpoint data, including that of endpoints managed using Tanium Client, to better understand the state of all endpoints in your network.

Issue questions to target OT devices

You can use the **Provider Type**, **Provider Name**, and **Entity Type** sensors to return results from certain types of managed endpoints, such as endpoints managed using Tanium Client or endpoints managed using Tanium Endpoint Management for Operational Technology.

Entity Provider	Provider Type value	Provider Name value	Entity Type value
Tanium Client	Tanium Client	Tanium	Computer
Tanium Endpoint Management for Operational Technology	Operational Technology	*<configured-entity-provider-name>*	Operational Technology Device

Note: If you return results from endpoints managed using Tanium Endpoint Management for Operational Technology, you can also use the **Device Type** sensor to retrieve the device type if available, such as **Controller**, **Device**, or **Programmable Logic Controller**.

The following question returns all OT devices, such as those ingested by the Tanium Endpoint Management for Operational Technology entity provider:

```
Get Computer Name and Provider Name and Provider Type and Entity Type and Device Type from
all entities with Entity Type equals Operational Technology Device
```

The following question returns all OT controller devices, such as those ingested by the Tanium

©2026 Tanium Inc. All Rights Reserved

Endpoint Management for Operational Technology entity provider:

```
Get Computer Name and Provider Name and Provider Type and Entity Type and Device Type from
all entities with OT Device Type equals Controller
```

The following question returns all computers or workstations, such as those managed by Tanium Client:

```
Get Computer Name and Provider Name and Provider Type and Entity Type and Device Type from
all entities with Entity Type equals Computer
```

The following question returns all OT devices ingested by Tanium Endpoint Management for Operational Technology:

```
Get Computer Name and Provider Name and Provider Type and Entity Type and Device Type from
all entities with Provider Type equals Operational Technology
```

The following question returns all programmable logic controllers ingested by Tanium Endpoint Management for Operational Technology:

```
Get Computer Name and Provider Name and Provider Type and Entity Type and Device Type from
all entities with (Provider Type equals Operational Technology and OT Device Type equals
Programmable Logic Controller)
```

The following questions returns all devices managed using Tanium Client:

```
Get Computer Name and Provider Name and Provider Type and Entity Type and Device Type from
all entities with Provider Type equals Tanium Client
```

```
Get Computer Name and Provider Name and Provider Type and Entity Type and Device Type from
all entities with Provider Name equals Tanium
```

The following question returns all OT devices ingested by a Tanium Operational Technology shared service satellite configuration instance named `Example Connector for Operational Technology`:

```
Get Computer Name and Provider Name and Provider Type and Entity Type and Device Type from
all entities with Provider Name equals Example Connector for Operational Technology
```

The following question returns all OT devices with a **Device Type** of **Device**, ingested by a Tanium Operational Technology shared service satellite configuration instance named `Example Connector for Operational Technology`:

```
Get Computer Name and Provider Name and Provider Type and Entity Type and Device Type from
all entities with (Provider Name equals Example Connector for Operational Technology and
OT Device Type equals Device)
```

©2026 Tanium Inc. All Rights Reserved

Include OT devices in a report

When you work in the **Explore Data** page or edit a report, the **Source Data** panel lists all registered sensors, along with certain sources of data that are not present on endpoints, such as entity providers that do not install Tanium Client on endpoints.

About this task

For more information, see Tanium Reporting User Guide: Registered sensors. You use the panel to add data sources as columns to the grid in the page or report. Each column lists the results that endpoints returned for the corresponding sensor or lists the values that Tanium solutions calculated for other data sources. If a single source produces multiple columns of results, the column headings show the source name above the column names.

1. Perform one of the following steps based on whether you plan to edit an existing report or create a new view of endpoint data that you might save as a report.
    - Existing report: Open the report and click **Edit Data**.
    - New view or report: From the Main menu, go to **Data** > **Explore Data**.

    > **Tip:** You can also access the **Explore Data** page through the following options:
    >
    > - An existing report: Click **New Report** or, in a non-editable report, click **Explore Data**.
    > - The **Data** > **Reports** page: Click **Create Report**.

2. Select a **Data Source** to limit the results to endpoints managed using Tanium Client or an entity provider, or select **All Entities** to return results from all endpoints.

    > **Note:** Select **Save as default** to save your current **Data Source** selection for future reports.

3. Configure the report. For more information, see Tanium Reporting User Guide: Explore data and create reports.

    > **Note:** If you select **Operational Technology** or **All Endpoints** as the **Data Source**, you can filter results to show only OT devices.

©2026 Tanium Inc. All Rights Reserved

Export OT device data using Tanium Connect

If the connection source supports OT device data, such as the **Tanium Reporting (Source Data)** source, you can export this data using Tanium Connect.

For more information, see Tanium Connect User Guide: Overview.

Note: If you configure Tanium Exposure Management for Operational Technology, you cannot export OT device vulnerability findings using Tanium Connect. For more information, see Using Tanium Exposure Management for Operational Technology on page 49

©2026 Tanium Inc. All Rights Reserved

Using Tanium Exposure Management for Operational Technology

Use Tanium Exposure Management for Operational Technology to view limited vulnerability finding information related to OT devices in Comply, using an **OT (Operational Technology)** vulnerability assessment scan method.

About this task

Viewing vulnerability findings in Comply allows you to quickly identify possible vulnerabilities on specific OT devices, which you can then mitigate by updating OT device firmware and related software. For more information, see Tanium Comply User Guide: Creating vulnerability assessments.

Create an operational technology scan assessment

OT scans identify vulnerabilities on any OT devices managed using Tanium Endpoint Management for Operational Technology. Use a satellite endpoint to identify OT device manufacturers, communication protocols, firmware versions, and other related information. Tanium Comply reads this data from TDS and converts this information to CPEs. It then compares the CPEs to the vulnerability database and matches them to CVEs to determine which vulnerabilities are associated with an OT device. If it finds associated CVEs, it updates the **Assessment Status** sensor showing that the device has been scanned, and it populates findings with the corresponding data.

OT scans run on a predefined, non-configurable schedule of every 30 minutes, for all devices managed using Tanium Endpoint Management for Operational Technology.

Before you begin

- Configuring an OT scan assessment requires a valid Tanium Endpoint Management for Operational Technology license and a Tanium Exposure Management for Operational Technology license.
- Configure Tanium Endpoint Management for Operational Technology to ingest OT device data.
- An OT scan assessment can target only certain communication protocols. For more

©2026 Tanium Inc. All Rights Reserved

information, see Endpoints.

- An OT scan assessment returns CVEs for both version-agnostic CPEs and firmware-version-specific CPEs. For Detected CPEs, there are two listed for each cell, one with an "o" (operating system) and one with an "h" (hardware).
- You typically need only one Comply OT scan assessment for an environment. The assessment runs on a predefined schedule and targets all devices managed using Tanium Endpoint Management for Operational Technology.
- Air-gapped environments do not support OT scan assessments.

To configure an OT scan assessment in Tanium Comply to identify vulnerabilities on OT devices managed using Tanium Endpoint Management for Operational Technology, complete the following procedure:

1. From the Main menu, go to **Modules** > **Comply** > **Assessments**.
2. Click **Create Assessment** > **Vulnerability**.
3. On the **Create Vulnerability Assessment** page, in the **Summary** section, enter a **Name** for the assessment. You can also provide **Labels**.
4. Select a **Scan Method**:
   - **OT (Operational Technology)**: (requires a Tanium Endpoint Management for Operational Technology license and a Tanium Exposure Management for Operational Technology license) Use an endpoint managed using Tanium Client configured as a satellite to find vulnerabilities on endpoints managed using Tanium Endpoint Management for Operational Technology, based on communication protocol and firmware version.
5. Click **Create & Deploy** and enter your credentials. Results appear on the **Findings** page.

Result



Note: It might take up to 30 minutes for results to appear in the **Findings** page.

View vulnerability findings for OT devices

A finding is the result of a check on an endpoint at a specific point in time. When you run an

©2026 Tanium Inc. All Rights Reserved

assessment, the OT results appear on the **Findings** page in the **Vulnerability** tab. OT findings are obtained from the satellite and stored in TDS. Use the provided categories on the Findings page to filter results and save those filtered results as reports.

1. From the Main menu go to **Modules** > **Comply** > **Findings**.
2. Select the **Vulnerability** tab.
3. At the top level, you can filter by Computer Groups. Click within the edit field to add multiple groups to the filter. You can also apply the OR and AND buttons to the selected computer groups.

Result

OT findings include Check ID, Endpoint, Detected CPEs, Scan Method, Operating System, Manufacturer, Model, and Device Type.

Expand Details

Click the **Expand Details** arrow to view more information about the CVE and CVSS scores for the finding.

Note: You can export only OT findings using the **Export** button on the Findings page. You cannot export assessments.

Note: At this time, Operational Technology is not available in the **Scan Method** filter for filtering findings.

Note: OT devices are always marked as not excepted. Vulnerability finding exceptions do not apply to OT devices.

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Tanium Endpoint Management for Operational Technology

If Tanium Endpoint Management for Operational Technology is not performing as expected, you might need to troubleshoot issues or change settings.

Collect logs

The information is saved as a ZIP file that you can download with your browser. The ZIP file is also known as a support bundle.

1. From the Main menu, go to **Shared Services** > **Endpoint Management for Operational Technology**.
2. Click Help ? and then click the **Troubleshooting** tab if needed.
3. Click **Collect**. A tanium-Operational-Technology-support.[timestamp].zip file downloads to the local download directory.
4. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 57.

Collect troubleshooting information from the satellite

You can collect and review endpoint artifacts from the OT satellite to troubleshoot issues. You cannot collect endpoint artifacts from OT devices directly.

You can use Client Management to directly connect to an endpoint and collect a bundle of logs and other artifacts, sometimes referred to as an *Endpoint Must Gather* (EMG).

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Single Endpoint View** search box, enter all or part of an IP address or a computer

©2026 Tanium Inc. All Rights Reserved

name.
Matching results appear after the search completes.

4. From the search results, click the computer name.
   Client Management opens the Endpoint Details page in Single Endpoint View (SEV).

5. Click the **Client Health** tab and, if the endpoint is not yet **Connected**, click **Direct Connect**.

6. In the **Available Steps** grid, select the domains (types of logs and artifacts) for which you want to gather troubleshooting information.
   For Patch information, select the **Core** and **Patch** domains.

   For Comply information, select the **Comply** domain and then select **Comply Database**, **Comply Extension Data**, and **Comply Intel**.

   For Endpoint Management for Operational Technology entity provider information, select the **Core** domain and then select **Tanium Client Logs**. Select the **Entity** domain and then select **Config Data**, **Entity Log**, and **Entity Provider Metadata**.

7. Click **Gather from Endpoint**.
   The selected logs and artifacts are gathered from the endpoint. The package appears in the **Must Gathers** section, and the name of the package corresponds with its time stamp.

8. When **Finished** appears in the **Run State** column, select the package and click **Download** to download a ZIP file that contains the troubleshooting information.
   For more information about collecting troubleshooting information in Single Endpoint View, see Tanium Reporting User Guide: Collect troubleshooting information.

   For more information about how to connect directly to endpoints, see Tanium Direct Connect User Guide.

   For more information about Client health features in Client Management, see Tanium Client Management User Guide: Monitor the Client health overview in Client Management and Tanium Client Management User Guide: Access detailed Client health and troubleshooting information on an endpoint.

View and export the audit log

The Operational Technology **Audit Log** page shows information about OT satellite endpoint configuration changes. Review the audit log to understand when OT satellite endpoint configuration

©2026 Tanium Inc. All Rights Reserved

changes happened, and what changes occurred, such as adding or removing monitored communication protocols. You can either copy audit log entries to the clipboard, or generate a comma-separated value (CSV) file with the audit log entries.

1. From the Main menu, go to **Shared Services** > **Operational Technology** > **Audit Log**.
2. Click **Export** > **Copy to clipboard** to copy the selected data to the clipboard.
3. Click **Export** > **Export to CSV** to export a CSV file containing the list of satellite configuration changes.

Cannot select a satellite running macOS for configuration

Tanium Endpoint Management for Operational Technology does not support using a satellite running macOS. Ensure that your satellite endpoint runs Windows 8.1 or later, Windows Server 2012 R2 or later, or a Linux distribution that runs on x86-64 architecture. For more information, see Tanium Direct Connect User Guide: Managing satellites.

Cannot establish communications between satellite and OT devices

Establishing bidirectional communications between the satellite and OT devices requires a physical wired connection. Verify the following:

- The satellite and OT devices are online.
- The satellite runs Windows 8.1 or later, Windows Server 2012 R2 or later, or a Linux distribution that runs on x86-64 architecture.
- The satellite has a physical wired connection, and satellite traffic can be routed to the OT devices.
- Networking devices that are situated between the satellite and OT devices, such as a router, switch or hub, support the communication protocols that the OT devices are running, and properly route traffic between the satellite and OT devices.
- Each OT device has an IP address and satisfies other requirements needed to establish a connection with the satellite.
- The ports required for the communication protocol are open for the satellite endpoint and

©2026 Tanium Inc. All Rights Reserved

the OT devices.

- The network allow and block list rules allow bidirectional traffic between the satellite and OT devices over the intended ports.
- The network allow and block list rules allow traffic from the satellite to OT devices in the entire ephemeral port range, and UDP broadcast responses from the OT devices to the satellite.
- The OT satellite configuration can discover the communication protocol that the OT devices are running.
- If you deployed a Cisco VLAN-based switch to forward traffic from OT devices running the PROFINET communication protocol, voice VLAN is enabled on the switch.

For more information, see Plan and update network infrastructure to support Tanium Endpoint Management for Operational Technology on page 38.

Cannot discover OT devices

If traffic can be routed between the satellite and OT devices, but you cannot discover OT devices, verify the following:

- In Direct Connect, confirm that the satellite is online. If the satellite is offline, it cannot discover endpoints. For more information, see Tanium Direct Connect User Guide: Managing satellites.
- In Operational Technology, confirm that in a satellite configuration, the satellite is enabled and configured to discover the intended communication protocols. If intended communication protocols are not configured, the satellite cannot discover OT devices running that communication protocol. For more information, see Create an OT satellite configuration on page 40.
- Confirm that the configured schedule interval has elapsed at least once since the initial configuration was created, then wait several minutes to ensure enough time for the satellite to discover OT devices.

EtherNet/IP devices not discovered on Linux satellite

©2026 Tanium Inc. All Rights Reserved

If the satellite endpoint runs Linux with firewalld and EtherNet/IP devices are not discovered, the OS firewall might be rejecting discovery responses.

EtherNet/IP discovery sends UDP broadcasts from an ephemeral source port on the satellite to `255.255.255.255:44818`. Because UDP broadcasts do not create connection tracking entries, unicast responses from EtherNet/IP devices are not associated with the outbound broadcast. When a response arrives at the satellite on an ephemeral destination port, `firewalld` treats it as an unsolicited inbound connection and rejects it.

Opening port 44818/UDP alone is not sufficient. Because responses return to an ephemeral destination port rather than port 44818, a standard port rule does not match the response traffic. Add a rich rule based on the source port of the EtherNet/IP device response. Replace `public` with the firewalld zone assigned to the interface that communicates with OT devices — run `firewall-cmd --get-active-zones` to identify it:

```
firewall-cmd --permanent --zone=public --add-rich-rule='rule source-port port=44818 protocol=udp accept'
```

For tighter security, restrict the rule to the OT device subnet by adding `source address=<subnet>` to the rich rule.

```
firewall-cmd --reload
```

To verify the rule is active, run:

```
firewall-cmd --list-rich-rules
```

After confirming the rule is loaded, re-run OT device discovery to verify that EtherNet/IP devices are now found.



Note: This firewall configuration applies only to the satellite endpoint, not to OT devices.

An OT device appears more than once in Tanium

If an OT device appears more than once, such as in question results or a report, the OT device might have been ingested by more than one satellite. In this case, multiple results for a single OT device are not deduplicated. Verify that only one satellite is configured to discover a communication protocol in a subnet.

©2026 Tanium Inc. All Rights Reserved

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about submitting a support case, see Case Submission Form.

©2026 Tanium Inc. All Rights Reserved

Reference: Endpoint Management for Operational Technology endpoint tools

Note: Each solution includes a tool with the same name as the solution that appears in the Endpoint Configuration Toolset manifest but that does not appear in the following table. This tool is not deployed to the endpoint itself, but it manages the endpoint tooling dependencies for the solution, as listed in the table.

Endpoint tools for Tanium Endpoint Management for Operational Technology

Tool	Description
core-cx	Provides a management framework API for all other Client Extensions and exposes operating system metrics
cx-config	Provides installation and configuration of extensions on an endpoint
entity-cx	Provides management for entity providers and facilitates communication between the entity providers and Tanium Client
extras-cx	Provides a helper library that contains re-usable functions for various client extensions to use
Npcap	Records process and command-line events on supported Windows endpoints to assist with Nmap scans
python312	Provides TPython binary and libraries

Note: Npcap is installed only on satellites configured to discover the Profinet communication protocol.

©2026 Tanium Inc. All Rights Reserved