

Tanium™ Discover User Guide

Autonomous IT. Unstoppable Business.

2025H2 Semiannual Release

Version 4.15

April 02, 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 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. 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 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 at support@tanium.com, or email accessibility@tanium.com to make further inquiries.

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

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

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

© 2026 Tanium Inc. All Rights Reserved

© 2026 Tanium Inc. All rights reserved.

Table of contents

Discover overview **11**

Scan types 11

Distributed scans 11

Satellite scans 12

Centralized scans 13

Profiles for unmanaged interface discovery 14

Discovery method impact 14

Profile configuration 15

Interface management 15

Locations 16

Labels 16

Notifications 16

Interoperability with other Tanium products 16

Tanium™ Client Management 16

Tanium™ Trends 16

Discover - Interfaces 17

Discover - Labels 17

Discover - Module Health 17

Gaining organizational effectiveness with Discover **18**

Change management 18

RACI chart 18

Organizational alignment 21

Develop a deployment plan 21

Operational metrics 22

Discover maturity 22

Benchmark metrics 22

Discover requirements **26**

© 2026 Tanium Inc. All Rights Reserved

Core platform dependencies ... 26
Computer group dependencies ... 26
Solution dependencies ... 26
Tanium recommended installation ... 26
Import specific solutions ... 27
Required dependencies ... 27
Feature-specific dependencies ... 27
Client extensions and endpoint tools ... 27
Tanium™ Module Server ... 28
Endpoints ... 28
Supported internet protocols ... 28
Supported operating systems ... 28
Host and network security requirements ... 29
Communication ports and destinations ... 30
Scan ports and destinations ... 30
Security exclusions ... 36
Third-party internet URLs ... 52
User role requirements ... 52
Installing Discover ... 58
Before you begin ... 58
Import Discover with default settings ... 58
Import Discover with custom settings ... 59
Manage solution dependencies ... 59
Upgrade Discover ... 59
Verify Discover version ... 59
Configuring Discover ... 60
Prepare endpoints ... 60
Manage solution configurations with Tanium Endpoint Configuration ... 60
Configure import frequency ... 60
Toggle IPv6 compatibility ... 61

© 2026 Tanium Inc. All Rights Reserved

Enable IPv6 compatibility ... 61
Disable IPv6 compatibility ... 62
Purge IPv6 data ... 62
Set up Discover users ... 62
Running distributed scans ... 65
Profile configuration ... 65
Level 1 (ARP/NDP cache and interface connections) ... 65
IPv4 discovery ... 65
IPv6 discovery ... 66
Level 2 (ping) ... 66
Level 3 (Nmap scan with host discovery) ... 67
Level 4 (Nmap scan with host discovery and OS fingerprinting) ... 68
Scan range calculation ... 69
Scenario: Endpoint has forward and backward peers ... 69
Scenario: Endpoint has forward peer but no backward peer ... 69
Configure profile for distributed scan ... 69
Before you begin ... 70
Create profile ... 70
Discovery process ... 76
Scan results ... 76
Force import of scan results ... 76
What to do next ... 77
Running satellite scans ... 78
Scan unmanaged subnets with a satellite scan ... 78
Configure profile for satellite scan ... 78
Before you begin ... 79
Discovery process ... 83
Satellite scan results ... 83
Scan results ... 83
Force import of scan results ... 84

© 2026 Tanium Inc. All Rights Reserved

What to do next ... 84
Running centralized scans ... **85**
Scan unmanaged subnets with a centralized Nmap scan ... 85
Configure profile for centralized Nmap scan ... 85
Before you begin ... 86
Discovery process ... 89
Scan Amazon EC2 environments ... 89
Before you begin ... 89
Configure API user ... 90
Configure profile for Amazon EC2 centralized scan ... 90
Discovery process ... 91
Centralized scan results ... 92
Scan results ... 92
Force import of scan results ... 92
What to do next ... 93
Managing Discover profiles ... **94**
View profiles ... 94
Disable a profile ... 95
Managing interfaces ... **96**
View interface data ... 96
View charts ... 96
Determine data source that found an interface ... 97
Add columns to data grid ... 98
Export data ... 98
Mark interfaces as manageable or unmanageable ... 98
Ignore interfaces ... 99
Locations ... 99
Create location spreadsheet ... 100
CSV header ... 100
CSV values ... 100

© 2026 Tanium Inc. All Rights Reserved

CSV example 100
Import locations 101
Assign location permissions 101
Location results 102
Labels 103
Types of labels 103
Built-in labels 103
Discover Label Gallery labels 103
User-defined labels 103
Import labels 104
Export labels 104
View data in Tanium Trends 104
Automatically label interfaces 105
Activities 105
Label conditions 105
Condition operators 105
Condition wildcards 106
Create an automatic label 106
Manually label interfaces 107
Create a manual label 107
Remove a manual label 107
Best practices for labels 107
Labels for common use cases 107
Create a Connect job for lost interfaces 108
Apply labels by location 108
Endpoint onboarding 109
Exporting Discover data 110
Export to a CSV file 110
Export interface data to a Connect destination 110
Connections to create 111

© 2026 Tanium Inc. All Rights Reserved

Create connection to export interfaces ... 111
Create connection for event notifications ... 112
Prerequisites ... 113
Configure notifications in Connect ... 113
Maintaining Discover ... 117
Review and remediate Discover resource usage on the Module Server ... 117
Review and update discovery methods ... 117
Monitor and troubleshoot endpoints managed ... 118
Monitor and troubleshoot mean time to manage ... 118
Troubleshooting Discover ... 121
Collect logs ... 121
Collect troubleshooting information from endpoints ... 121
Verify endpoint tools ... 122
Identify and resolve issues with Client Extensions ... 122
Review the Extensions log for an endpoint ... 125
View Discover scan ranges ... 125
Problem: No results from running a scan ... 125
Problem: Some endpoints are not scanning ... 125
Problem: Satellite profile appears in ERRORED state ... 126
Symptom ... 126
Cause ... 126
Solution ... 126
Problem: Error with locations CSV file ... 127
Problem: Needs deployment profile status ... 128
FAQ: Why is the number of managed interfaces higher than the client status? ... 128
Remove Npcap from endpoints ... 128
Remove Discover tools from endpoints ... 129
Uninstall Discover ... 130
Contact Tanium Support ... 131
Reference: Discover endpoint tools ... 132

© 2026 Tanium Inc. All Rights Reserved

Reference: Data returned by profile type **133**

Reference: Discover columns for Connect exports **139**

Reference: Gateway examples for Discover **142**

Discover query filter syntax 142

Single column 142

Multiple columns 143

Discover examples 144

Add labels to interfaces (mutation.discoverInterfaceAddLabel) 144

Add Discover labels to Discover interfaces 144

Create a label (mutation.discoverLabelCreate) 146

Create a Discover label 146

Delete a label by name (mutation.discoverLabelDelete) 147

Delete a Discover label by name 148

Get interface by ID (query.discoverInterface) 148

Get a Discover interface by ID 149

Get multiple interfaces (query.discoverInterfaces) 152

Get multiple Discover interfaces 152

Get label by name (query.discoverLabel) 158

Get a Discover label by name 158

Get multiple labels (query.discoverLabels) 159

Get multiple Discover labels 159

Remove labels from interfaces (mutation.discoverInterfaceRemoveLabel) 161

Remove Discover labels from Discover interfaces 161

© 2026 Tanium Inc. All Rights Reserved

Discover overview

With Discover, you can find and maintain an inventory of interfaces. When you install the Tanium™ Client on your endpoints, you can actively scan and monitor the local subnet or other defined network segments to detect unmanaged interfaces.

Interfaces are unique media access control (MAC) addresses. An endpoint with multiple network interface controllers (NICs) displays as multiple interfaces in Discover.

Managed interfaces are on endpoints that have the Tanium Client running and are managed by Tanium. *Unmanaged interfaces* are on the network but do not have the Tanium Client running.

Discover provides real-time information about unmanaged interfaces on your network.

Scan types

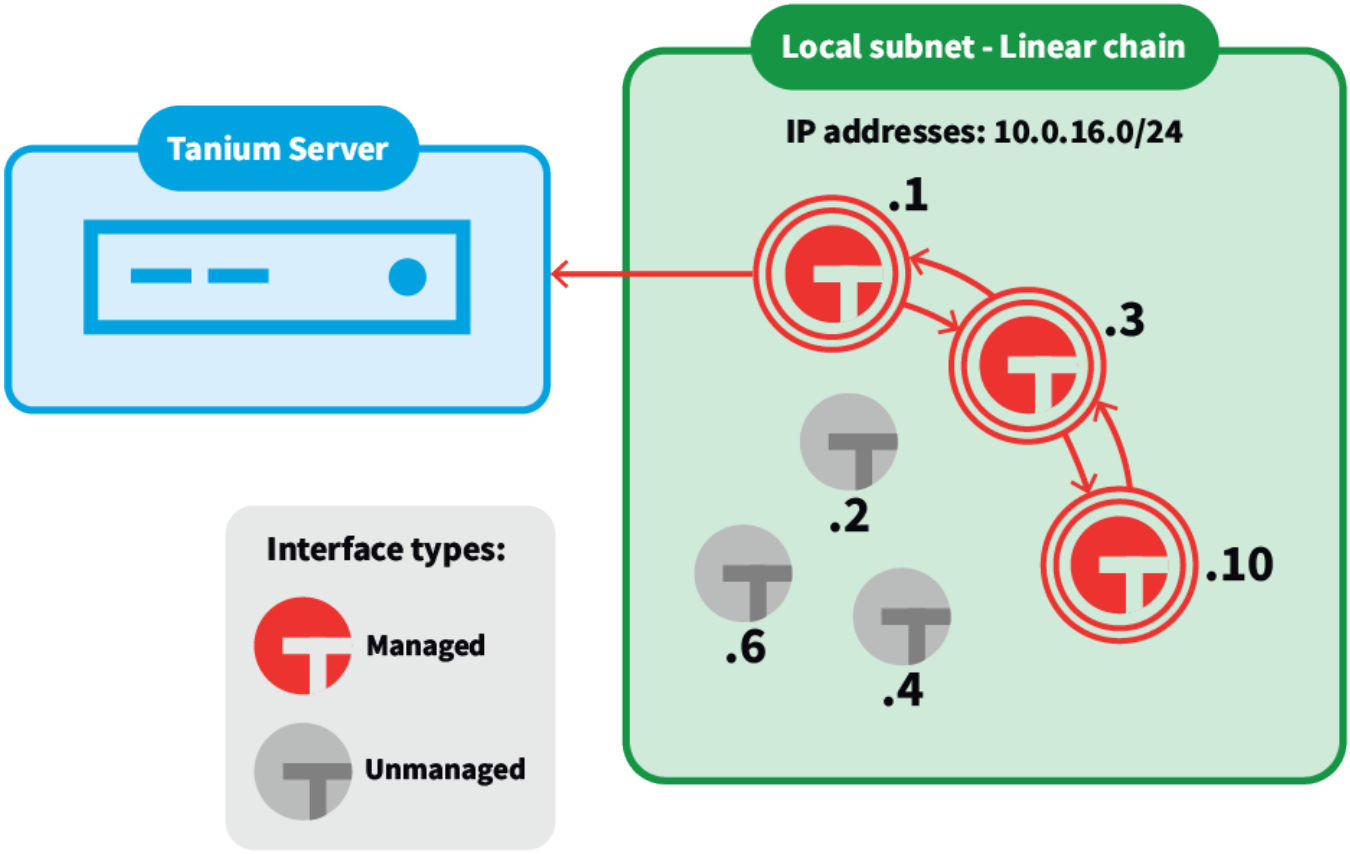
Scan types define which endpoints run Discover scans. For the most complete view of all unmanaged interfaces, use a combination of distributed, satellite, and centralized scans.

Distributed scans

Configure distributed scans to use managed endpoints to scan for or detect unmanaged interfaces at configurable intervals. Discover queries endpoints for updated detection data periodically. New information is immediately available. The detection process provides continuous scanning without impact to network operations.

© 2026 Tanium Inc. All Rights Reserved

Distributed scan



Satellite scans

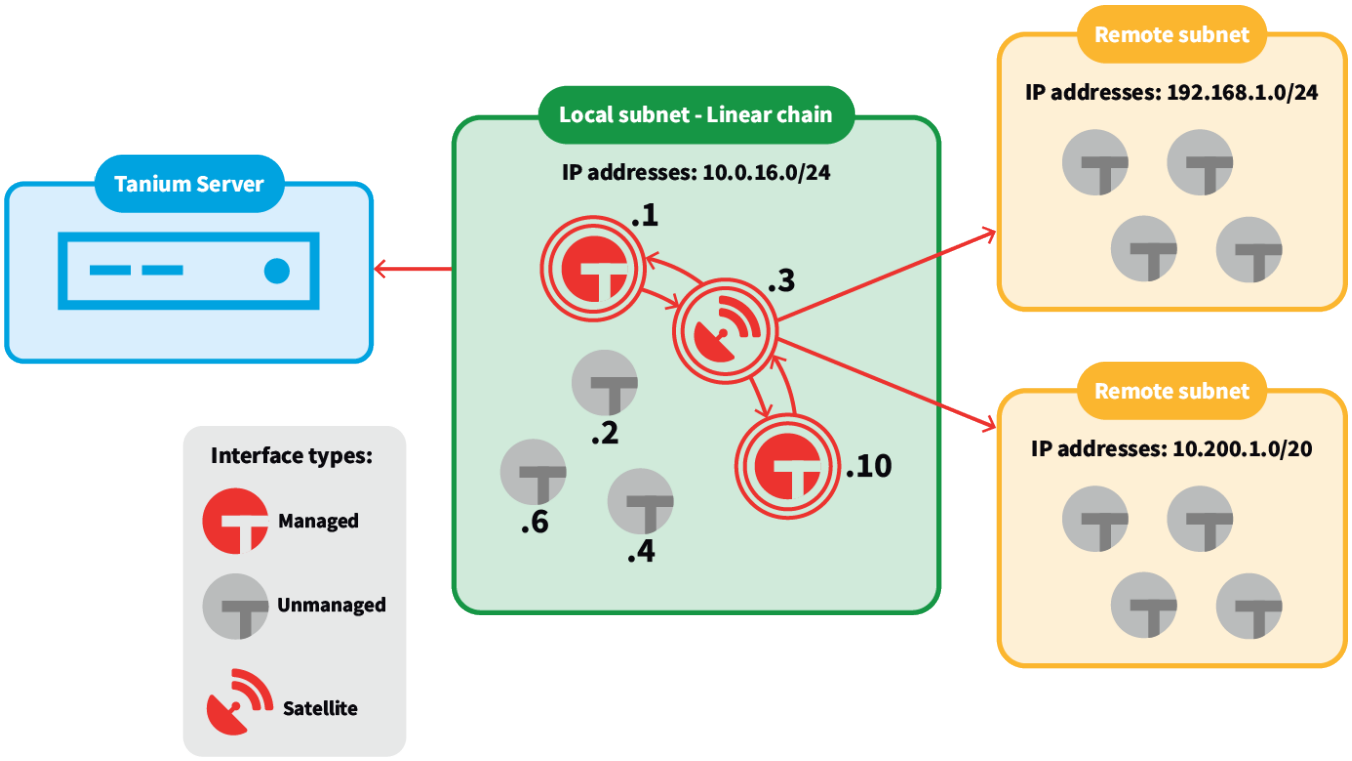
Configure satellite scans to use a satellite endpoint to scan for or detect unmanaged interfaces that cannot be reached directly from Tanium™ Module Server, such as subnets that have only a bridged connection to the main network.

Satellites are specific Tanium Clients that you designate to run certain targeted, secure workloads on behalf of Tanium Module Server. Because sensitive, encrypted data (such as credentials) might need to be sent to a satellite when running a workload, you must verify each endpoint that you designate as a satellite to prevent spoofing attacks. Any such sensitive data is never sent using the linear chain, nor is it stored on disk on the satellite.

For more information about how to manage satellites, see Tanium™ Direct Connect User Guide: Managing satellites.

© 2026 Tanium Inc. All Rights Reserved

Satellite scan

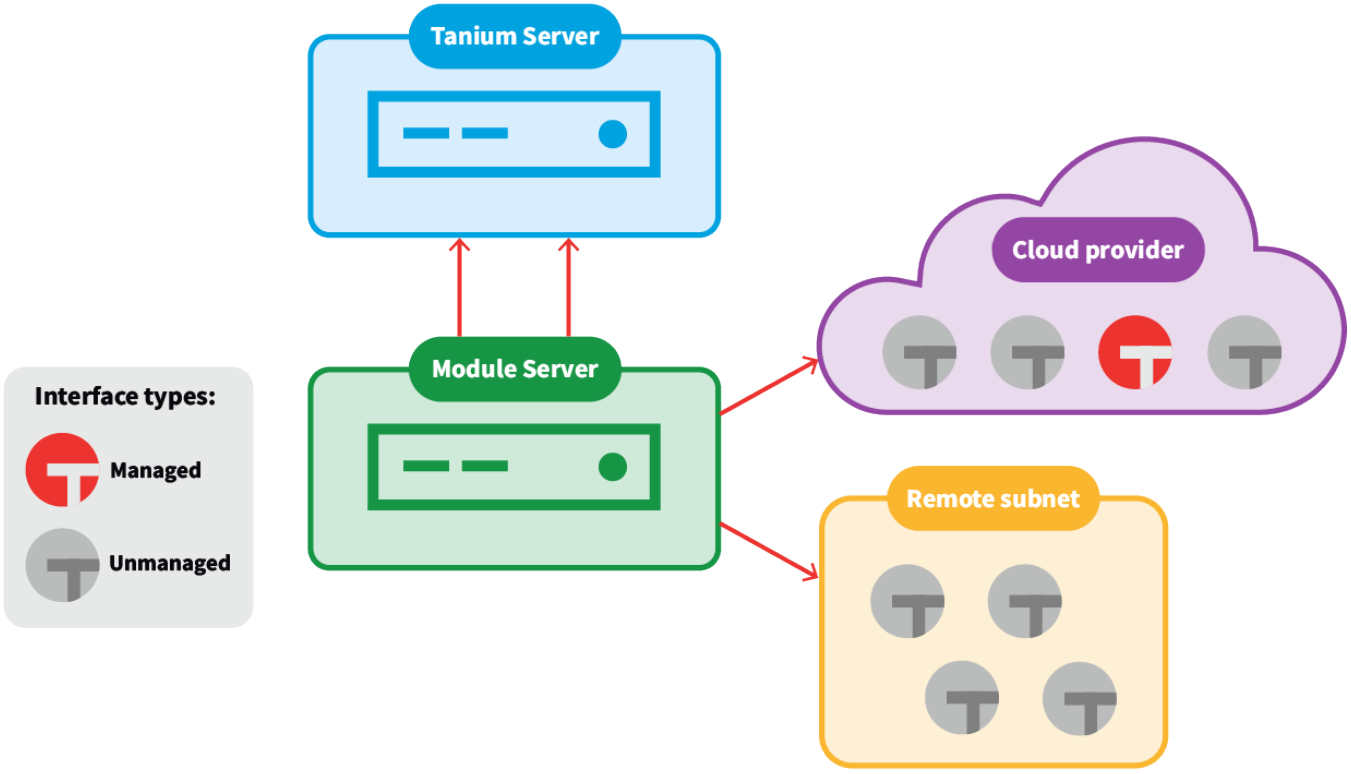


Centralized scans

Configure centralized scans to use the Tanium Module Server to detect unmanaged interfaces beyond your local network, such as in cloud-hosted environments or targeted subnets where no Tanium Clients exist.

© 2026 Tanium Inc. All Rights Reserved

Centralized scan



Profiles for unmanaged interface discovery

Create profiles to detect interfaces that are on the network but not under Tanium management. Each profile consists of a set of network inclusions and exclusions, a discovery method, and schedule information. You can configure multiple profiles to cover different types of scans and to scan different parts of the network. For more information, see Running distributed scans on page 65, Running satellite scans on page 78, and Running centralized scans on page 85.

If you selected the **Automatic configuration with default settings option** during installation, a Level 2 ping distributed profile is created by default. You can use or edit this profile or create a new one. For more information about this type of profile, see Level 2 (ping) on page 66.

Discovery method impact

Before you configure a profile, you must understand the impact of the different discovery methods. Passive discovery methods use existing information on the endpoints to find interfaces, generating no network activity. Active discovery methods perform network scanning.

You can use four levels of distributed discovery. Satellite and centralized Nmap scans are equivalent to level 4 distributed scans. Lower levels of discovery are more passive, have less network impact, but provide a limited set of information. Higher levels perform active scans on the network, but provide more information about unmanaged interfaces, such as host name and operating system.

© 2026 Tanium Inc. All Rights Reserved

Discovery method network impact

Discovery Method	Approximate Bytes per IP Found (DNS Lookup Disabled)	Approximate Bytes per IP Found (DNS Lookup Enabled)
Distributed level 1 (ARP cache and interface connections)	0	512
Distributed level 2 (ping)	74	586
Distributed level 3 (Nmap scan with host discovery)	56	586
Distributed level 4 (Nmap scan with host discovery and OS fingerprinting, 1000 port default)	n/a	122000
Centralized Nmap	n/a	244000
Centralized Amazon EC2 environments	n/a	n/a
Satellite	n/a	244000

All values are estimates and are calculated based on standard network equipment. Actual values can vary widely depending on your network configuration.

Profile configuration

Each profile is scoped by different network inclusions, exclusions, and schedules. With an active discovery method, you might choose to scope the discovery to run on a specific subnet a few times a day. Because passive discovery methods have less network impact, you might choose to scope the discovery to scan a broader part of the network every hour.



Overall, the best data is provided by satellite, centralized Nmap, or distributed level 4 (Nmap scan with host discovery and OS fingerprinting) profiles. These profile types provide data that includes open ports and attempt to identify the OS platform and OS Generation. If Nmap is not allowed in your environment, the level 2 (ping) scan generates some OS Platform information.

Level 3 and level 1 scans provide the least information. Level 3 is a quick scan without port probing but finds all IP addresses using active ARP probing. The level 1 scan is passive and looks at connections or ARP cache to determine what the endpoint knows about without any network probing.

Centralized Amazon EC2 environment profiles provide data only for AWS EC2 instances.

For more information about the data provided by each profile type, see Reference: Data returned by profile type on page 133.

Interface management

Organize interfaces by applying locations or labels. View statistics about interfaces over time.

© 2026 Tanium Inc. All Rights Reserved

Locations

Assign interfaces to geographic, physical, or logical locations. Define a hierarchy of network addresses, network address translation (NAT) addresses, and locations. Addresses can consist of an IP, IP range, or classless inter-domain routing (CIDR) address. The location hierarchy goes from a larger to smaller location, such as `country, state, city` or `Site, building, floor`. After the hierarchy is defined, locations are matched with the interfaces during the import process of a discovery scan. For more information, see Locations on page 99.

Labels

Labels include descriptive information or metadata that you can use to identify and group interfaces. Then, you can classify or search for interfaces based on the labels. You can also automatically apply labels or ignore interfaces based on a specifically defined set of conditions. To get started with labels, a gallery of commonly-defined labels is available. For more information, see Labels on page 103.

Notifications

Discover records the following events:

- Found an unmanaged interface
- Found a new managed endpoint
- Lost an interface

With a connection in Tanium™ Connect, Discover can send these events to a destination, such as security information and event management (SIEM) system, email, or file. For example, use the **Found an unmanaged interface** event as an alert to the operations team, so they install Tanium on unmanaged interfaces.

For more information about how to configure the Discover notifications connection, see Create connection for event notifications on page 112.

Interoperability with other Tanium products

Discover integrates with other Tanium products to provide additional features and reporting.

Tanium™ Client Management

You can apply labels to unmanaged interfaces to target endpoints in Client Management deployments.

Tanium™ Trends

Discover features Trends boards that provide data visualization of Discover concepts.

© 2026 Tanium Inc. All Rights Reserved

DISCOVER - INTERFACES

Contains information about the interfaces that Discover has found in the environment. The following panels are in the **Discover - Interfaces** board:

- Interfaces managed
- Mean time to managed
- Lost interfaces
- All interfaces
- Managed interfaces
- Unmanaged interfaces
- Unmanageable interfaces

DISCOVER - LABELS

Contains information about the labels that have been applied to interfaces. The following panels are in the **Discover - Labels** board:

- Discover label counts - latest
- Discover labels over time

DISCOVER - MODULE HEALTH

Contains information about the resource usage of the Discover service on the Module Server. The following panels are in the **Discover - Module Health** board:

- Discover module average CPU usage
- Discover module average heap memory used

For more information about how to import the Trends boards that are provided by Discover, see Tanium Trends User Guide: Importing the initial gallery.

© 2026 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Discover

The five key organizational governance steps to maximizing the value that is delivered by Discover are as follows:

- Develop a dedicated change management process. For more information, see Change management on page 18.
- Define distinct roles and responsibilities. For more information, see RACI chart on page 18.
- Validate cross-functional alignment. For more information, see Organizational alignment on page 21.
- Develop a deployment plan. For more information, see Develop a deployment plan on page 21.
- Track operational maturity. For more information, see Operational metrics on page 22.

Change management

Develop a tailored, dedicated change management process for asset discovery, taking into account the new capabilities provided by Tanium.

- Update SLAs and align activities to key resources for Tanium Discover activities across IT Security, IT Operations, and IT Risk / Compliance.
- Designate change or maintenance windows for various asset discovery scenarios. Scanning activities, such as ARP, Ping, or Nmap scanning of the network, require planning and testing.
- Identify internal and external dependencies to your asset discovery process, such as required network controls.
- Create a Tanium Steering Group (TSG) for discovery activities to expedite reviews, and approvals of processes that align with SLAs.

RACI chart

A RACI chart identifies the team or resource who is **R**esponsible, **A**ccountable, **C**onsulted, and **I**nformed, and serves as a guideline to describe the key activities across the security, risk/compliance, and operations teams. Every organization has specific business processes and IT organization demands. The following table represents Tanium's point of view for how organizations should align functional resources against finding unmanaged interfaces. Use the following table as a baseline example.

© 2026 Tanium Inc. All Rights Reserved

RACI chart for Tanium Discover

Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Determine Discover scanning types	C	R/A	-	-	When you configure scanning activity, use careful planning, change control, and testing to measure the potential network impact.
Analyze unmanaged interfaces	C	R/A	-	-	After a scan runs, all interfaces across the network are reported as managed (Tanium Client installed) or unmanaged interfaces. This list is a baseline to review and start the labeling process.

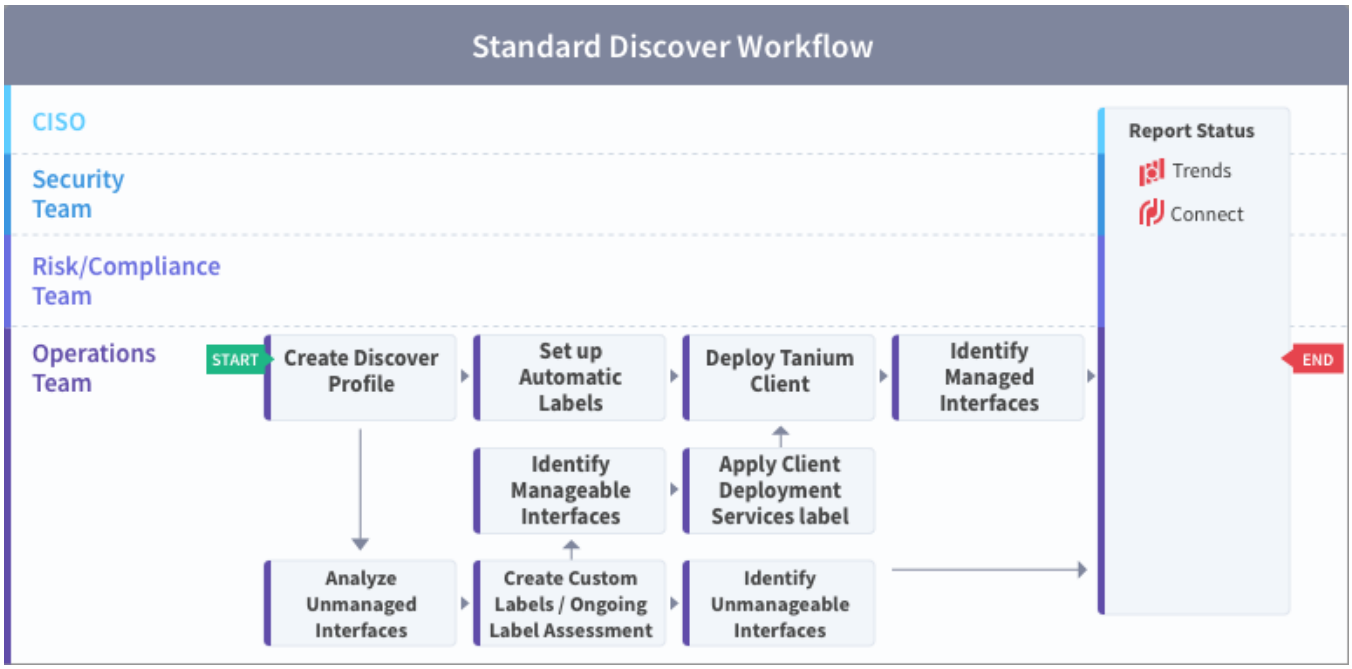
© 2026 Tanium Inc. All Rights Reserved

RACI chart for Tanium Discover (continued)

Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Identify manageable interfaces or create custom labels / ongoing label assessment	C	R/A	-	-	The Discover Label Gallery contains pre-defined labels that you can import to apply to discovered interfaces. You can also create custom labels and apply to discovered interfaces.
Apply Client Deployment Services label / Identify unmanageable interfaces	C	R/A	-	-	Use Discover labels to target installation of the Tanium Client by Tanium Client Management. Labels can be applied automatically or manually by the administrator as needed.
Report status	C	R/A	C/I	C/I	Automate reporting with Trends boards, or integrate with other tools such as a SIEM or CMDB. Share reports that require action or remediation with executives or other owners.

© 2026 Tanium Inc. All Rights Reserved

Standard Discover workflow



Organizational alignment

Successful organizations use Tanium across functional silos as a common platform for high-fidelity endpoint data and unified endpoint management. Tanium provides a common data schema that enables security, operations, and risk/compliance teams to assure that they are acting on a common set of facts that are delivered by a unified platform.

In the absence of cross-functional alignment, functional silos often spend time and effort in litigating data quality instead of making decisions to improve discovery of unmanaged interfaces.

Develop a deployment plan

Because Discover introduces some minimal network traffic, it is important to work with the correct stakeholders to understand how Discover is used in the environment.

- Evaluate discovery method options. For more information about discovery method options and the data that gets returned by each discovery method, see Running distributed scans on page 65, Running satellite scans on page 78, Running centralized scans on page 85, and Reference: Data returned by profile type on page 133.
- Define network exceptions and exclusions. Determine sensitive ports that should not be scanned and VPN networks to exclude. The list of VPN networks is often the same list as isolated subnets.
- Gather a list of subnets in the environment. This list is required to create a rollout plan and configure satellite and centralized scanning. You also must have this list to define locations in Discover.

© 2026 Tanium Inc. All Rights Reserved

- Create a network rollout plan. The simplest option is to select **All Networks** when you create a profile, and scan all networks at the same time. You can also scan by subnet. Get a listing of all client subnets in the environment and build a deployment plan for each subnet.
- Create an Amazon Web Services (AWS) rollout plan. Collect or create credentials in AWS to query the Discover API.
- Determine any networks that have no Tanium Clients installed, for satellite and centralized Nmap scanning.
- Determine the schedule for scanning and network tolerance.
- Determine if any servers require specific scan windows.

Operational metrics

Discover maturity

Managing an asset discovery program successfully includes operationalization of the technology and measuring success through key benchmarking metrics. The four key processes to measure and guide operational maturity of your Tanium Discover program are as follows:

Processes to measure Tanium Discover maturity

Process	Description
Usage	How and when Tanium Discover is used in your organization (example: is Discover supplemental for another legacy tool)
Automation	How Tanium Discover is automated across endpoints
Functional Integration	How Tanium Discover is integrated across IT security, IT operations, and IT risk/compliance teams (examples: automated client deployments, data sent to external destinations)
Reporting	How Tanium Discover is automated, and the audience of Discover reporting

Benchmark metrics

The key benchmark metrics that align to the operational maturity of the Tanium Discover program to achieve maximum value and success follow:

Benchmark metrics for Tanium Discover maturity

Executive Metrics	Interfaces Managed	Mean Time to Managed
Description	Percentage of interfaces that are currently being managed by the Tanium platform, divided by the total number of discovered interfaces (not counting ignored interfaces).	Average number of days or hours to bring an endpoint under management, or to mark the interface as unmanaged or unmanageable.

© 2026 Tanium Inc. All Rights Reserved

Benchmark metrics for Tanium Discover maturity (continued)

Executive Metrics	Interfaces Managed	Mean Time to Managed
Instrumentation	Managed / (Unmanaged + Managed)	For a managed client, calculate the time elapsed between when an endpoint was **First Seen** until it was **First Managed**.
Why this metric matters	If a given device is not managed by Tanium, the device cannot be secured and managed.	If a new device takes a long time to become managed, efficacy of Tanium tooling is limited and potential exposure to bad actors increases.

Use the following table to determine the maturity level for Tanium Discover in your organization.

© 2026 Tanium Inc. All Rights Reserved

Maturity levels for Tanium Discover

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Discover is configured, initial unmanaged interfaces visible	Baseline visibility of unmanaged interfaces with Tanium Client	Discover used to audit and target installation of Tanium Client on unmanaged interfaces	Discover used to audit and take action on unmanaged interfaces	Discover used to audit and take action on unmanaged interfaces
	Automation	One or more profiles configured: • Level 1 passive scan: Address Resolution Protocol (ARP) • Level 2 scan: Ping	Define and configure customized Level 3 or 4 Nmap profile	Base labels configured, Discover label gallery imported Set up satellite or centralized Nmap scanning profiles for any gaps in network	Custom locations configured for tracking and visual representation for responsible teams	Custom labels built based on an understanding of the network and client environment for tracking devices and interfaces in the environment that are unauthorized, built alerting workflow with Tanium Connect
	Functional integration	N/A	Verification of settings to not cause false security alerts, tune settings for Nmap configuration	Trends boards imported, scanning gaps conducted of subnets	Automated installation of Tanium Client on unmanaged interfaces or previously managed interfaces based on labels	Real-time alerting configured to ticketing system, SIEM for data correlation and intelligence
	Reporting	Manual; Discover workbench dashboard for operators only	Manual; Discover workbench dashboard for operators and peer group only	Automated; Trends boards for operators and peer group only	Automated; Trends boards tailored to stakeholders ranging from operator to executive	Automated; Trends boards tailored to stakeholders ranging from operator to executive

© 2026 Tanium Inc. All Rights Reserved

Maturity levels for Tanium Discover (continued)

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Metrics	Endpoints Managed	0-49%	50-64%	65-84%	85-94%	95-100%
	Mean Time to Manage	> 30 days	8-30 days	1-7 days	1-24 hours	0-3 hours

© 2026 Tanium Inc. All Rights Reserved

Discover requirements

Review the requirements before you use Discover.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Discover. For more information about how to get Discover, see Tanium Solutions & Bundles.
- Tanium™ Core Platform servers
- Tanium Client: Any supported version of Tanium Client. For more information, see Tanium Client Management User Guide: Client version and host system requirements.
  If you use a Client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.

Computer group dependencies

When you first sign in to Tanium™ Console after a fresh installation of Tanium Server, the server automatically imports the computer groups that Discover requires: `All Computers`.

For earlier versions of the Tanium Server, or after upgrading from an earlier version, you must manually create the computer groups. For more information, see Tanium Console User Guide: Create a computer group.

Solution dependencies

Other Tanium solutions are required for Discover to function (required dependencies) or for specific Discover 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.



Some Discover dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 27 and Feature-specific dependencies on page 27. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Discover requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Discover, 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.

© 2026 Tanium Inc. All Rights Reserved

Import specific solutions

If you select only Discover to import, 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 Discover, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Discover has the following required dependencies:

- Tanium Client Management
- Tanium™ Core Content
- Tanium™ Data Service (TDS)
- Tanium™ Default Content
- Tanium™ Endpoint Configuration
- Tanium™ Interact
- Tanium™ RDB Service
- Tanium™ Secrets Service
- Tanium™ System User Service
- Tanium Trends

Feature-specific dependencies

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

- Tanium™ Direct Connect is required to run satellite scans
- Tanium™ Connect is required to export Discover data

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for Discover on 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 more information, see Security exclusions. For a list of Discover tools, see Reference: Discover endpoint tools on page 132.For a list of Discover tools, see Reference: Endpoint Management for Operational Technology endpoint tools. For a list of all Client Extensions and tools, see Tanium Client Management User Guide: Reference: Client extensions used for Tanium solutions.

© 2026 Tanium Inc. All Rights Reserved

Tanium™ Module Server

Discover is installed and runs as a service on the Module Server host computer. The impact on Module Server host computer sizing is minimal and depends on usage.

For more information, see Tanium Core Platform Installation Guide: Host system resource guidelines.

Endpoints

Supported internet protocols

Discover scans for IPv4 addresses and, optionally, IPv6 addresses. You can use any distributed or satellite scan to find endpoints by IPv4 address. For IPv6, you can use level 1 distributed scans to find endpoints. For more information about distributed scans, see Running distributed scans on page 65. For more information about enabling IPv6 compatibility, see Toggle IPv6 compatibility on page 61.

Supported operating systems

For more information about Tanium Client operating system support, see Tanium™ Client Management User Guide: Client version and operating system requirements. Managed endpoints perform discovery scans.

Supported operating systems for Tanium Discover

Operating System	Version	Notes
Windows	Windows 7 SP1 or later and Windows Server 2008 R2 SP1 or later If the endpoints are not up-to-date and Python content does not run, it might generate an error about `nt._add_dll_directory` with `The specified procedure could not be found`. For more information, see Microsoft Security Advisory.	• Windows 7 SP1 requires Microsoft KB2758857. • Windows Server 2008 R2 SP1 requires Microsoft KB2758857.
macOS	Same as Tanium Client support	Discover automatically filters out interfaces with MAC addresses of `ac:de:48:00:11:22` and `ac:de:48:33:44:55`. These addresses are commonly used for communication between a macOS machine and the BridgeOS in the Touch Bar.
Linux	Same as Tanium Client support	
Solaris	Same as Tanium Client support	NOTE Solaris endpoints cannot be designated as satellites.

© 2026 Tanium Inc. All Rights Reserved

Supported operating systems for Tanium Discover (continued)

Operating System	Version	Notes
AIX	7.1.4 or later	The IBM XL C++ runtime libraries file set (`xlC.rte`), version 16.1.0.0 or later, and the IBM LLVM runtime libraries file set (`libc++.rte`) must be installed. For more information, see Tanium Client Management User Guide: Deploy the Tanium Client to AIX endpoints using a package file. NOTE Discover does not support AIX endpoints for IPv6 distributed scans. NOTE AIX endpoints cannot be designated as satellites.

Supported platforms for each discovery method

	Level 1 (ARP cache)	Level 1 (Interface Connections)	Level 2 (Ping)	Level 3/4 (Nmap) and Satellite
Windows	✓	✓	✓	✓[3]
Linux	✓	✓	✓	✓
macOS	✓	✓	✓	✓
Solaris	✓	✓	✓[2]	✗[1]
AIX	✓	✓	✓	✗[1]

[1] For level 3 and 4 discovery on Solaris and AIX, level 2 discovery is used because Nmap is not supported on these platforms.

[2] Solaris endpoints do not perform OS detection.

[3] Windows 11 Arm is not supported for Level 3 and 4 scans that use Nmap. An endpoint running Windows 11 Arm cannot be used as a satellite.

Host and network security requirements

Specific ports and processes are needed to run Discover.

© 2026 Tanium Inc. All Rights Reserved

Communication ports and destinations

The following ports and protocols are required for Discover communication.

Ports for Tanium Discover communication

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17446	TCP and UDP	Internal purposes for Discover; not externally accessible
	Module Server (loopback)	17447	TCP and UDP	Internal purposes for Discover; not externally accessible
	content.tanium.com	443	TCP and UDP	Module Server (TaniumModuleServer.exe) communication with content.tanium.com to import updates
Tanium Server	content.tanium.com	443	TCP and UDP	Tanium Server (TaniumReceiver.exe) communication with content.tanium.com to import updates

Scan ports and destinations

The following ports and protocols are required for Discover scanning.

© 2026 Tanium Inc. All Rights Reserved

Ports for Tanium Discover scanning

Source	Destination	Scan Type	Port	Protocol	Purpose
Tanium Client	Configured DNS servers for the client	Level 1 or level 2 distributed scans for which **Use host name lookup to resolve host names** is selected	53	UDP	Level 1 or level 2 distributed scans configured to use host name lookup for resolving host names use DNS for host name resolution.

© 2026 Tanium Inc. All Rights Reserved

Ports for Tanium Discover scanning (continued)

Source	Destination	Scan Type	Port	Protocol	Purpose
	Devices with an IP address in the same subnet as the Tanium Client	Level 1 or level 2 distributed scans for which **Use host name lookup to resolve host names** is selected	• 137 (Windows only) • 5355 (Windows only)	• netbios-ns • LLMNR	On Windows endpoints, level 1 or level 2 distributed scans configured to use host name lookup for resolving host names might use netbios or LLMNR for name resolution if enabled in the operating system on the Tanium Client.

© 2026 Tanium Inc. All Rights Reserved

Ports for Tanium Discover scanning (continued)

Source	Destination	Scan Type	Port	Protocol	Purpose
		Level 2 distributed	N/A	ICMP	Level 2 distributed scans require ICMP echo-request and echo-response traffic from all managed endpoints to all other devices on the Tanium Client subnet.
		Level 3 distributed	N/A	ARP	Level 3 distributed scans require ARP-request traffic from the managed endpoint on the Tanium Client subnet.
		Level 4 distributed	1000 most common TCP ports (default setting)	• ARP • TCP	Level 4 distributed scans require ARP-request traffic from the managed endpoint on the Tanium Client subnet. Additionally, by default, Discover scans the 1000 most commonly used TCP ports on the Tanium Client subnet to calculate the **OS Generation** field. You can change this setting in the scan profile. For more information, see Running distributed scans on page 65.

© 2026 Tanium Inc. All Rights Reserved

Ports for Tanium Discover scanning (continued)

Source	Destination	Scan Type	Port	Protocol	Purpose
Module Server	Customer-defined subnets	Centralized Nmap	N/A	ICMP	Centralized Nmap scans require ICMP traffic to all IP addresses specified in the scan.
			1000 most common open TCP ports (default setting)	TCP	For centralized Nmap scans, by default, Discover scans the 1000 most commonly used TCP ports on the Tanium Client subnet to calculate the **OS Generation** field. You can change this setting in the scan profile. For more information, see Running centralized scans on page 85.
	ec2.*.amazonaws.com sts.*.amazonaws.com ssm.*.amazonaws.com	Centralized Amazon EC2 environment	443	TCP	Centralized Amazon EC2 environment scans require access to Amazon Web Services.

© 2026 Tanium Inc. All Rights Reserved

Ports for Tanium Discover scanning (continued)

Source	Destination	Scan Type	Port	Protocol	Purpose
Satellite	Local network	Satellite	N/A	ARP	Satellite scans on a local network require ARP-request traffic from the managed endpoint on the Tanium Client subnet.
			1000 most common open TCP ports (default setting)	TCP	Additionally, by default, Discover scans the 1000 most commonly used TCP ports on the Tanium Client subnet to calculate the **OS Generation** field. You can change this setting in the scan profile. For more information, see Running satellite scans on page 78.
	Remote subnets	Satellite	N/A	ICMP	Remote network satellite scans require ICMP traffic to all IP addresses specified in the scan
			1000 most common open TCP ports (default setting)	TCP	By default, Discover scans the 1000 most commonly used TCP ports on the Tanium Client subnet to calculate the **OS Generation** field. You can change this setting in the scan profile. For more information, see Running satellite scans on page 78.

© 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 and for Windows-based Tanium Core Platform deployments, see Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server 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.

Discover security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\discover-service\node.exe`
		Process	`<Module Server>\plugins\content\discover-proxy\proxyplugin.exe`
		Process	`<Module Server>\services\twsm-v1\twsm.exe`
		Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	`<Tanium Client>\TaniumCX.exe`

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	<*Tanium Client*>\Tools\Discover\nmap\vcredist_x86.exe

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\TaniumClientExtensions.dll`

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<*Tanium Client*>\TaniumClientExtensions.dll.sig

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<*Tanium Client*>\extensions\SupportCX.dll

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<*Tanium Client*>\extensions\SupportCX.dll.sig
		File	<*Tanium Client*>\extensions\TaniumConfig.dll
		File	<*Tanium Client*>\extensions\TaniumConfig.dll.sig
		File	<*Tanium Client*>\extensions\discover\data\discover.db
		File	<*Tanium Client*>\extensions\discover\data\discover.db-wal
		File	<*Tanium Client*>\extensions\discover\data\discover.db-shm
	(Distributed level 3, distributed level 4, and satellite profiles only)	Folder	C:\Program Files\Npcap
	(Distributed level 3, distributed level 4, and satellite profiles only)	Process	<*Tanium Client*>\Tools\Discover\nmap\nmap.exe
	(When Direct Connect is installed; satellite profiles only)	File	<*Tanium Client*>\extensions\TaniumDEC.dll
	(When Direct Connect is installed; satellite profiles only)	File	<*Tanium Client*>\extensions\TaniumDEC.dll.sig
	(Satellite profiles only)	File	<*Tanium Client*>\extensions\TaniumDiscover.dll
	(Satellite profiles only)	File	<*Tanium Client*>\extensions\TaniumDiscover.dll.sig
	(Satellite profiles only)	File	<*Tanium Client*>\extensions\TaniumExtras.dll
	(Satellite profiles only)	File	<*Tanium Client*>\extensions\TaniumExtras.dll.sig

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux		Process	`<Tanium Client>/TaniumCX`

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/libTaniumClientExtensions.so`

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/libTaniumClientExtensions.so.sig`

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libSupportCX.so`
		File	`<Tanium Client>/extensions/libSupportCX.so.sig`
		File	`<Tanium Client>/extensions/libTaniumConfig.so`
		File	`<Tanium Client>/extensions/libTaniumConfig.so.sig`
		File	`<Tanium Client>/extensions/discover/data/discover.db`
		File	`<Tanium Client>/extensions/discover/data/discover.db-wal`
		File	`<Tanium Client>/extensions/discover/data/discover.db-shm`
	(Distributed level 3, distributed level 4, and satellite profiles only)	Process	`<Tanium Client>/Tools/Discover/nmap/nmap`
	(When Direct Connect is installed; satellite profiles only)	File	`<Tanium Client>/extensions/libTaniumDEC.so`
	(When Direct Connect is installed; satellite profiles only)	File	`<Tanium Client>/extensions/libTaniumDEC.so.sig`
	(Satellite profiles only)	File	`<Tanium Client>/extensions/libTaniumDiscover.so`
	(Satellite profiles only)	File	`<Tanium Client>/extensions/libTaniumDiscover.so.sig`
	(Satellite profiles only)	File	`<Tanium Client>/extensions/libTaniumExtras.so`
	(Satellite profiles only)	File	`<Tanium Client>/extensions/libTaniumExtras.so.sig`

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
macOS		Process	`<Tanium Client>/TaniumCX`

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/libTaniumClientExtensions.dylib`

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>*/libTaniumClientExtensions.dylib.sig

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libSupportCX.dylib`

© 2026 Tanium Inc. All Rights Reserved

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<*Tanium Client*>/extensions/libSupportCX.dylib.sig
		File	<*Tanium Client*>/extensions/libTaniumConfig.dylib
		File	<*Tanium Client*>/extensions/libTaniumConfig.dylib.sig
		File	<*Tanium Client*>/extensions/discover/data/discover.db
		File	<*Tanium Client*>/extensions/discover/data/discover.db-wal
		File	<*Tanium Client*>/extensions/discover/data/discover.db-shm
	(Distributed level 3, distributed level 4, and satellite profiles only)	Process	<*Tanium Client*>/Tools/Discover/nmap/nmap
	(When Direct Connect is installed; satellite profiles only)	File	<*Tanium Client*>/extensions/libTaniumDEC.dylib
	(When Direct Connect is installed; satellite profiles only)	File	<*Tanium Client*>/extensions/libTaniumDEC.dylib.sig
	(Satellite profiles only)	File	<*Tanium Client*>/extensions/libTaniumDiscover.dylib
	(Satellite profiles only)	File	<*Tanium Client*>/extensions/libTaniumDiscover.dylib.sig
	(Satellite profiles only)	File	<*Tanium Client*>/extensions/libTaniumExtras.dylib
	(Satellite profiles only)	File	<*Tanium Client*>/extensions/libTaniumExtras.dylib.sig

© 2026 Tanium Inc. All Rights Reserved

Third-party internet URLs

If security software is deployed in the environment to monitor and block unknown URLs, your security administrator must allow the following URLs:

Third-party internet URLs

Source	Destination	Port	Protocol	Purpose
Module Server	ec2.*.amazonaws.com	443	TCP and UDP	For centralized scans of Amazon EC2 environments
	sts.*.amazonaws.com	443	TCP and UDP	
	ssm.*.amazonaws.com	443	TCP and UDP	

User role requirements

Predefined roles grant the following permissions, which are required to use Discover functionality:

- Discover solution permissions on page 53
- Discover administration and platform content permissions on page 56: The solution permissions automatically provide some of these permissions.

For more information about predefined roles, see Set up Discover users.

Optional roles for Discover on page 57 are required to enable optional Discover functionality.

Some Discover 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 Discover. If you create custom roles for Discover users, be sure to assign all the solution permissions and content set permissions that are required for Discover 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



Do not assign the **Discover Service Account** role to users. This role is for internal purposes only.

© 2026 Tanium Inc. All Rights Reserved

Discover solution permissions

Permission	Discover Administrator[1]	Discover Operator[1]	Discover User[1,2]	Discover Read Only User[1]	Discover Endpoint Configuration Approver[1,2,3]	Discover Optional Feature Administrator
Discover View managed and unmanaged interfaces	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✗	✗
Discover API Use the Discover API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✗
Discover Asset View lists of managed and unmanaged interfaces; export data from interface tables; apply or remove label on an interface	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✗
Discover Components Manage backend components, including Discover action groups and computer groups	✗	✗	✗	✗	✗	✗
Discover Connect Integration Service Account Enable the Discover service account to interface with Connect	✗	✗	✗	✗	✗	✗

© 2026 Tanium Inc. All Rights Reserved

Discover solution permissions (continued)

Permission	Discover Administrator[1]	Discover Operator[1]	Discover User[1,2]	Discover Read Only User[1]	Discover Endpoint Configuration Approver[1,2,3]	Discover Optional Feature Administrator
Discover Endpoint Configuration Approve Discover configuration changes in the Endpoint Configuration service	✗	✗	✗	✗	✓ APPROVE	✗
Discover Keys Rotate keys used to encrypt sensitive data	✓ ROTATE	✗	✗	✗	✗	✗
Discover Location Permissions Define locations and corresponding permissions for user groups	✓ WRITE	✓ WRITE	✗	✗	✗	✗
Discover Locations Define locations by importing CSV file	✓ WRITE	✓ WRITE	✗	✗	✗	✗
Discover Manual Import Import interfaces manually with the **Discover Unmanaged Interfaces** button	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✗	✗	✗

© 2026 Tanium Inc. All Rights Reserved

Discover solution permissions (continued)

Permission	Discover Administrator[1]	Discover Operator[1]	Discover User[1,2]	Discover Read Only User[1]	Discover Endpoint Configuration Approver[1,2,3]	Discover Optional Feature Administrator
Discover Optional Feature Access to module settings for Discover	✓ WRITE	✓ WRITE	✗	✗	✗	✓ WRITE
Discover Profile View, create, edit, and delete Discover profiles	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✓ READ	✗
Discover Settings Edit Discover settings	✓ WRITE	✗	✗	✗	✗	✗
Discover Tag Create or remove labels	✓ WRITE	✓ WRITE	✓ WRITE[6]	✗	✗	✗
Discover TDS Integration Service Account Provide access to promote Discover data to Tanium™ Data Service (TDS)	✗	✗	✗	✗	✗	✗
Discover Trends Manipulate Discover data in Trends	✓ WRITE	✓ WRITE	✓ READ	✓ READ	✗	✗

© 2026 Tanium Inc. All Rights Reserved

Discover solution permissions (continued)

Permission	Discover Administrator[1]	Discover Operator[1]	Discover User[1,2]	Discover Read Only User[1]	Discover Endpoint Configuration Approver[1,2,3]	Discover Optional Feature Administrator
Discover Trends Integration Service Account Provide access for module service accounts to read and write data, and to define sources and boards	✗	✗	✗	✗	✗	✗

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

[2]If location permissions are defined, **Discover User** role cannot create labels.

[3]By default, configuration changes that the solution service account initiates (such as tool deployment) require approval if you enabled configuration approvals in Endpoint Configuration. To bypass approval for solution-generated configuration changes, apply the **Endpoint Configuration Bypass Approval** permission to the relevant content sets in the **Discover Service Account** role. For more information, see Tanium Endpoint Configuration User Guide: User role requirements and Tanium Endpoint Configuration User Guide: Managing approvals.

Discover administration and platform content permissions

Permission	Permission type	Discover Administrator	Discover Operator	Discover User	Discover Read Only User	Discover Endpoint Configuration Approver	Discover Optional Feature Administrator
Action Group	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✗	✗
Computer Group	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✗
Server Status	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✗
User	Administration	✓ READ	✗	✗	✗	✗	✗
User Group	Administration	✗	✗	✗	✗	✗	✗

© 2026 Tanium Inc. All Rights Reserved

Discover administration and platform content permissions (continued)

Permission	Permission type	Discover Administrator	Discover Operator	Discover User	Discover Read Only User	Discover Endpoint Configuration Approver	Discover Optional Feature Administrator
Action	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✓ READ	✗
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✗
Own Action	Platform Content	✓ READ	✓ READ	✗	✗	✗	✗
Package	Platform Content	✓ READ	✓ READ	✗	✗	✗	✗
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✗
Sensor	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✗

To view the content sets to which the platform content permissions apply, see Tanium Console User Guide: View effective role permissions.

Optional roles for Discover

Role	Enables
Connect User	For signed in user: • Configure connections for Discover notifications • Configure connections for exporting interface reports
Administrator	Create Trends boards from Discover sources

© 2026 Tanium Inc. All Rights Reserved

Installing Discover

Use Tanium Console **Solutions** page to install Discover and choose either automatic or manual configuration:

- **Automatic configuration with default settings**: Discover 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 Discover, see Import Discover with default settings on page 58.
- **Manual configuration with custom settings**: After installing Discover, you must manually configure required settings. Select this option only if Discover requires settings that differ from the recommended default settings. For more information, see Import Discover with custom settings on page 59.

Before you begin

- Read the release notes.
- Review the Discover requirements on page 26.
- For more information about how to upgrade from a previous version of Discover, see Upgrade Discover on page 59.
  Review the User role requirements and assign the correct roles to Discover users. For more information, see Tanium Console User Guide: Managing roles.
  - To import Discover, you must be assigned the Administrator reserved role.
  - To configure the Discover action group, you must be assigned the Content Administrator reserved role or a role that has the **Action Group write** permission.

Import Discover with default settings

You can set the Discover action group to target the **No Computers** filter group by enabling restricted targeting before importing Discover. This option enables you to control tools deployment through scheduled actions that are created during the import and that target the Tanium Discover action group. For example, you might want to test tools on a subset of endpoints before deploying the tools to all endpoints. In this case, you can manually deploy the tools to an action group that you configured to target only the subset. To configure an action group, see Tanium Console User Guide: Managing action groups. To enable or disable restricted targeting, see Tanium Console User Guide: Tools deployment and restricted targeting.

When you import Discover with the **Tanium Recommended Installation** workflow, the following default settings are configured:

Default settings for Tanium Discover

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group

© 2026 Tanium Inc. All Rights Reserved

Default settings for Tanium Discover (continued)

Setting	Default value
Level 2 ping distributed profile	This profile is created and deployed to all Tanium Clients. For more information about this type of profile, see Level 2 (ping) on page 66.

For more information about how to import Discover and configure default settings, see Tanium Console User Guide: Import all modules and services. For more information about how to verify that the correct version is installed after the import, see Verify Discover version on page 59.

Import Discover with custom settings

To import Discover without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Import or update specific solutions. For more information about how to verify that the correct version is installed after the import, see Verify Discover version on page 59.

For more information about how to configure the Discover action group, see Configuring Discover on page 60.

For more information about how to configure the import frequency, see Configure import frequency on page 60.

Manage solution dependencies

Other Tanium solutions are required for Discover to function (required dependencies) or for specific Discover features to work (feature-specific dependencies). For more information, see Solution dependencies on page 26.

Upgrade Discover

For more information about how to upgrade Discover, see Tanium Console User Guide: Managing Tanium solutions. For more information about how to verify the version, see Verify Discover version on page 59.

Verify Discover version

After you import or upgrade Discover, verify that the correct version is installed:

1. Refresh your browser.
2. From the Main menu, go to **Modules > Discover** to open the Discover **Overview** page.
3. To show version information, click Info .

© 2026 Tanium Inc. All Rights Reserved

Configuring Discover

If you did not install Discover with the **Apply All Tanium recommended configurations** option, you must enable and configure certain features.

Prepare endpoints

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.



For information about how to install Endpoint Configuration, see Tanium Endpoint Configuration User Guide: 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 Discover, see User role requirements on page 52. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.



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 Tanium Console User Guide: Managing action locks.

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

Configure import frequency

(Optional) Configure the import frequency. This setting determines how often the results from running discovery methods are imported to the **Interfaces** pages.

From the Main menu, go to **Modules> Discover > Overview**. Click Settings and go to the **Global Settings** tab. Edit the **Import Frequency** setting.

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

Leave the **Import Frequency** setting at the default value (every 30 minutes), unless you are directed to change the value by Tanium Support.

Toggle IPv6 compatibility

By default, IPv6 compatibility is disabled in Discover. To find IPv6 interfaces in your environment, you must enable IPv6 compatibility.

IMPORTANT

Consumer devices, particularly macOS devices, can randomize and cycle IPv6 MAC addresses frequently. As a result, you might see excess managed interface data when IPv6 compatibility is enabled.

NOTE

You must have a role with the **Discover Optional Feature write** permission to enable and disable IPv6 compatibility. Users assigned the Discover Administrator, Discover Operator, and Discover Optional Feature Administrator roles have this permission.

Enable IPv6 compatibility

1. From the Main menu, go to **Modules > Discover > Overview** and click Settings.
2. Navigate to the **Global Settings** tab.
3. Toggle **IPv6 Compatibility** to **Enabled**, and then click **Confirm**.
4. Create scan profiles to scan for IPv6 interfaces. For more information, see Running distributed scans on page 65 or Running satellite scans on page 78.

NOTE

Interfaces can have both IPv4 and IPv6 addresses. Discover does not promote IPv6-only interfaces to Tanium Data Service.

After you enable IPv6 compatibility, Discover automatically purges IPv6 interfaces that match the following criteria:

- Interfaces hosted on cloud providers that have not been seen in the last 24 hours.
- Interfaces not hosted on cloud providers that have not been seen in the last 7 days.

© 2026 Tanium Inc. All Rights Reserved

Disable IPv6 compatibility

NOTE

Notes on disabling IPv6 compatibility:

- If you disable IPv6 compatibility, Discover disables all IPv6 profiles and no longer imports IPv6 managed interfaces. If you re-enable IPv6 compatibility, you must manually re-enable any IPv6 profiles.
- You cannot edit or create IPv6 profiles when IPv6 compatibility is disabled.
- The option to manually purge IPv6 data is available only when IPv6 compatibility is disabled. You can choose to purge IPv6 data when you disable IPv6 compatibility, or you can also manually purge IPv6 interfaces at a later time. For more information, see Purge IPv6 data on page 62.

1. From the Main menu, go to **Modules > Discover > Overview** and click Settings.
2. Navigate to the **Global Settings** tab.
3. Toggle **IPv6 Compatibility** to **Disabled**.
   The **Disabled IPv6 Compatibility** dialog appears.
4. (Optional) To purge existing IPv6 data from Discover, select **Purge all existing IPv6 interface**.
5. Click **Confirm**.

Purge IPv6 data

When IPv6 compatibility is disabled, you can purge IPv6 data from Discover.

NOTE

You must have a role with the **Discover Optional Feature write** permission to purge IPv6 data. Users assigned the Discover Administrator, Discover Operator, and Discover Optional Feature Administrator roles have this permission.

1. From the Main menu, go to **Modules > Discover > Overview** and click Settings.
2. Navigate to the **Global Settings** tab and ensure **IPv6 Compatibility** is set to **Disabled**.
3. Click **Purge IPv6 Data** and then click **Confirm**.

After you purge IPv6 data, the option to purge no longer appears on the **Settings** page.

Set up Discover users

You can use the following set of predefined user roles to set up Discover users. For more information about how to review specific permissions for each role, see User role requirements on page 52.

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

© 2026 Tanium Inc. All Rights Reserved

Discover Administrator

Assign the **Discover Administrator** role to users who manage all configuration and deployment of Discover functionality to endpoints.
This role can perform the following tasks:

- Configure Discover settings
- Create, edit, and delete profiles
- View managed and unmanaged interfaces; manually import interfaces; export interface data
- Create and apply labels to interfaces; remove labels from interfaces
- Define and import locations; apply corresponding location permissions to user groups
- Manipulate Discover data in Trends

Discover Operator

Assign the **Discover Operator** role to users who manage most of the configuration and deployment of Discover functionality to endpoints, usually in Tanium Cloud environments.
This role can perform the following tasks:

- Configure Discover settings
- Create, edit, and delete profiles
- View managed and unmanaged interfaces; manually import interfaces; export interface data
- Create and apply labels to interfaces; remove labels from interfaces
- Define and import locations; apply corresponding location permissions to user groups
- Manipulate Discover data in Trends

Discover Optional Feature Administrator

Assign the **Discover Optional Feature Administrator** role to users who need to manage Discover settings but do not require full **Discover Administrator** or **Discover Operator** permissions.

Discover User

Assign the **Discover User** role to users who analyze and organize results of Discover scans.
This role can perform the following tasks:

- View managed and unmanaged interfaces; manually import interfaces; export interface data
- Create and apply labels to interfaces; remove labels from interfaces (only if location permissions are not defined)

Discover Read Only User

© 2026 Tanium Inc. All Rights Reserved

Assign the **Discover Read Only User** role to users who analyze Discover scan results.
This role can perform the following tasks:

- View managed and unmanaged interfaces
- View labels applied to interfaces

Discover Endpoint Configuration Approver

Assign the **Discover Endpoint Configuration Approver** role to a user who approves or rejects Discover configuration items in Tanium Endpoint Configuration.
This role can perform the following tasks:

- Approve, reject, or dismiss changes that target endpoints where Discover is installed
- View Discover profiles



Do not assign the **Discover Service Account** role to users. This role is for internal purposes only.

© 2026 Tanium Inc. All Rights Reserved

Running distributed scans

Distributed scans are performed by endpoints that are running the Tanium Client and have Discover tools installed. After identifying unmanaged interfaces, you can apply Discover labels to them. These labels can be used as deployment targets in Tanium Client Management for installation of the Tanium Client, bringing the interfaces under management by the Tanium Server. For more information about how to deploy the Tanium Client, see Tanium Client Management User Guide: Deploying the Tanium Client using Client Management.

Profile configuration

There are four levels of distributed scanning. You can create multiple profiles that include passive and active discovery methods. Each profile is scoped by different network inclusions, exclusions, and schedules. With an active discovery method, you might choose to scope the discovery to run on a specific subnet a few times a day. Because passive discovery methods have less network impact, you might choose to scope the discovery to scan a broader part of the network every hour.



For distributed scanning, the best data is provided by a level 4 (Nmap scan with host discovery and OS fingerprinting) profile. This profile type provides data that includes open ports, attempts to identify the OS platform and OS Generation.

If Nmap is not allowed in your environment, the level 2 (ping) scan generates some OS Platform information.

Level 3 and level 1 scans provide the least information. Level 3 is a quick scan without port probing, but finds all IP addresses using active ARP probing. The level 1 scan is passive and looks at connections or ARP cache to determine what the endpoint knows about without any network probing.

For more information about the data provided by each profile type, see Reference: Data returned by profile type on page 133.

Level 1 (ARP/NDP cache and interface connections)



Level 1 discovery scans support either IPv4 or IPv6 addresses. For IPv4, Discover uses Address Resolution Protocol (ARP) to scan for interfaces. For IPv6, Discover uses Neighbor Discovery Protocol (NDP) to scan for interfaces.

IPv4 discovery

Level 1 discovery for IPv4 addresses is a passive discovery method that combines ARP cache and interface connections discovery. No endpoints are scanned with level 1 discovery because the results are returned from the local ARP cache on each endpoint.

© 2026 Tanium Inc. All Rights Reserved

On Windows, macOS, and Linux endpoints, Discover filters the ARP cache based on the computed scan range, as if it is doing an active forward (and possibly backward) scan. For more information, see Scan range calculation on page 69. On Solaris and AIX endpoints, Discover filters the ARP cache based on the profile network inclusions and exclusions, returning a maximum of 1000 results.

The interface connections method sends actions to the endpoints to trigger the collection of all current IP connections that are on each managed endpoint. Then, the related MAC address is resolved by looking up the interfaces in the local ARP cache.

Value on Interfaces pages: arp, connected

IPv6 discovery

Level 1 discovery for IPv6 addresses is a passive discovery method that combines NDP cache and interface connections discovery. No endpoints are scanned with level 1 discovery because the results are returned from the local NDP cache on each endpoint.

On each endpoint, Discover filters the NDP cache for `ff00::/8` multicast addresses, adhering to any profile network inclusions and exclusions, and returns a maximum of 4096 results.



Discover does not support AIX endpoints for IPv6 distributed scans.

The interface connections method sends actions to the endpoints to trigger the collection of all current IP connections that are on each managed endpoint. Then, the related MAC address is resolved by looking up the interfaces in the local NDP cache.

Value on Interfaces pages: ndp, connected

Level 2 (ping)



Level 2 discovery scans support only IPv4 addresses.

The level 2 discovery method uses a ping discovery method to find unmanaged interfaces.

When level 2 discovery is initiated on a managed endpoint, the scan range is calculated based on its peers in the linear chain. For more information, see Scan range calculation on page 69.

After the range is calculated, the scanning package pings the targeted IP addresses with an Internet Control Message Protocol (ICMP) ping. Pings without a response take 3 seconds. Pings that return a response take much less time.

Isolated endpoints are not scanned by default. Isolated endpoints are endpoints that are on an isolated subnet, or appear to be on an isolated subnet because the endpoint has no peers. For more information about isolated subnets, see Tanium Client Management User Guide: Configure isolated subnets. To enable scanning of isolated endpoints, clear the **Isolated Subnets/Systems** option when you configure the discovery method.

When the results are imported, the Discover service:

© 2026 Tanium Inc. All Rights Reserved

- Resolves host names
- Checks if the interface is managed or unmanaged
- Resolves MAC address and Manufacturer
- Resolves OS Platform based on time to live (TTL) value in the ping response: Windows, Linux/Mac, or Solaris/AIX (Solaris endpoints do not detect OS Platform)

The ping discovery causes a small amount of network traffic over time. You might choose to run it on a smaller part of the network or at a longer schedule interval.

When you configure level 2 discovery on a sparsely populated network, set the schedule **Reissue every** setting to an hour or more to prevent scans from overlapping. If scans overlap, data may never be gathered for the upper end of the scan range.

Value on Interfaces pages: ping

Level 3 (Nmap scan with host discovery)



Level 3 discovery scans support only IPv4 addresses.

The level 3 discovery method uses Network Mapper (Nmap) utility on each endpoint to find information about network interfaces.

When level 3 discovery is initiated on an endpoint, the scan range is calculated based on its peers in the linear chain. For more information, see Scan range calculation on page 69.

Nmap scan host discovery finds unmanaged interfaces by automatically distributing a scanning package to the Tanium managed endpoints. This package consists of drivers (Windows only), libraries, and executable files. Then, an Nmap scan runs with an ARP broadcast scan only. If an ARP reply to the target is found, the endpoint is listed as available. No operating system or open port information is returned about the interfaces. Because level 3 discovery performs an ARP broadcast, you might see a spike in network activity at the beginning of the scan.

Endpoint files: The Nmap discovery method uses Npcap, a device driver, on Windows endpoints. For more information about exclusions that might need to be enabled for Nmap, see Host and network security requirements on page 29.



Tanium installs Npcap on endpoints that do not have Npcap installed. By default, Tanium does not update the Npcap version on endpoints that already have Npcap installed. You can configure the scan profile so that Tanium updates Npcap on endpoints where Npcap was previously installed by Tanium. To force endpoints to use the latest Tanium version of Npcap for scans instead of any version of Npcap that might already be on the endpoints, deploy the **Discover - Install Npcap** package to the endpoints. When you deploy the **Discover - Install Npcap** package, Npcap is installed only on endpoints with valid scan profiles that require Npcap.

Tanium installs the following files:

© 2026 Tanium Inc. All Rights Reserved

- `nmap.exe`: Runs scanning operations from the `<Tanium Client>\Tools\Discover\nmap` directory.
- `npcap-[version]-oem.exe` and `vcredist_x86.exe`: Run on the endpoint and add libraries and drivers that Nmap requires. These executable files run out of the `<Tanium Client>\Downloads\Action_<action_id>` directory. On Windows endpoints, Npcap is loaded on demand and is available to only admin users on the endpoint. Npcap files are installed in the `C:\Program Files\Npcap` directory. For Windows 7 and Windows Server 2008 endpoints, Tanium installs Npcap 1.20 for compatibility reasons. For all other endpoints, Tanium installs Npcap 1.75.

Nmap is not supported on AIX or Solaris. If Nmap scanning is configured for endpoints on these platforms, the endpoints perform level 2 scans instead. Level 2 scans are also performed if the Nmap scan has any problems running on the endpoint.

For more information about how to uninstall Npcap, see Remove Npcap from endpoints on page 128.

Value on Interfaces pages: nmap

Level 4 (Nmap scan with host discovery and OS fingerprinting)



Level 4 discovery scans support only IPv4 addresses.

Like the level 3 discovery method, level 4 also uses Nmap to find unmanaged interfaces. Level 4 discovery also includes OS fingerprinting.

By default, Discover scans 1000 commonly used TCP ports to calculate the **OS Generation** field. For more information, see Top 1,000 TCP and UDP ports (nmap default). In the profile settings you can configure different ports to scan and can change the source port from which the scan originates. The value of the **OS Generation** field is a “best guess” from Nmap, and is not displayed for managed interfaces.

Endpoint files: The Nmap discovery method uses Npcap, a device driver, on Windows endpoints. For more information about exclusions that might need to be enabled for Nmap, see Host and network security requirements on page 29.



Tanium installs Npcap on endpoints that do not have Npcap installed. By default, Tanium does not update the Npcap version on endpoints that already have Npcap installed. You can configure the scan profile so that Tanium updates Npcap on endpoints where Npcap was previously installed by Tanium. To force endpoints to use the latest Tanium version of Npcap for scans instead of any version of Npcap that might already be on the endpoints, deploy the **Discover - Install Npcap** package to the endpoints. When you deploy the **Discover - Install Npcap** package, Npcap is installed only on endpoints with valid scan profiles that require Npcap.

Tanium installs the following files:

- `nmap.exe`: Runs scanning operations from the `<Tanium Client>\Tools\Discover\nmap` directory.
- `npcap-[version]-oem.exe` and `vcredist_x86.exe`: Run on the endpoint and add libraries and drivers that Nmap requires. These executable files run out of the `<Tanium Client>\Downloads\Action_<action_id>` directory. On

© 2026 Tanium Inc. All Rights Reserved

Windows endpoints, Npcap is loaded on demand and is available to only admin users on the endpoint. Npcap files are installed in the `C:\Program Files\Npcap` directory. For Windows 7 and Windows Server 2008 endpoints, Tanium installs Npcap 1.20 for compatibility reasons. For all other endpoints, Tanium installs Npcap 1.75.

Nmap is not supported on AIX or Solaris. If Nmap level 3 scanning is configured for endpoints on these platforms, the endpoints perform level 2 scans instead. Level 2 scans are also performed if the Nmap scan has any problems running on the endpoint.

For more information about how to uninstall Npcap, see Remove Npcap from endpoints on page 128.

Value on Interfaces pages: nmap

Scan range calculation

Discover caps scan ranges at the /22 range (1024 IP addresses). When a scan runs, the Tanium Client calculates scan range automatically.

With level 2-4 discovery methods, scans typically run only in the gaps between the managed interfaces. Scanning only in the gaps eliminates many of the common issues with network scanners that generate significant network traffic and trigger alarms in intrusion prevention systems (IPS) and firewalls.

Most endpoints perform forward scans to avoid overlaps in scanning from other endpoints. Endpoints with no backward peers also scan backwards to avoid any gaps in scans. Review the following scenarios to fully understand how scan ranges are calculated.

Scenario: Endpoint has forward and backward peers

A managed endpoint at address 192.168.1.10 has a forward peer at address 192.168.1.20 and a backward peer at address 192.168.1.5.

A forward scan occurs from 192.168.1.11 to 192.168.1.19. Because the IP address has a backward peer, a backward scan is not performed.

Scenario: Endpoint has forward peer but no backward peer

A managed endpoint at address 192.168.1.10 has a forward peer at address 192.168.1.20, but no backward peer.

A forward scan occurs from 192.168.1.11 to 192.168.1.19. Because the endpoint has no backward peer, a backward scan from 192.168.1.1 to 192.168.1.9 is performed.

A scan occurs from 192.168.1.1 to 192.168.1.19 (excluding the origin endpoint: 192.168.1.10).

Configure profile for distributed scan

Configure a profile for the distributed scan by defining which networks to scan, the discovery method, and a scan schedule.



Create profiles according to your deployment plan. For more information, see Develop a deployment plan on page 21. If you are using a by subnet deployment policy, test and continue to add subnets to the profile until you are comfortable using all subnets.

© 2026 Tanium Inc. All Rights Reserved

Before you begin

- To scan portions of the network, you must know the IP ranges or the networks that you want to scan.
- (Optional) Create a locations file to map physical locations to discovered interfaces. Assign users to specific locations to limit access to interface data to specific user groups. You can configure locations at any time because the locations are evaluated every time a Discover scan completes. For more information, see Locations on page 99.

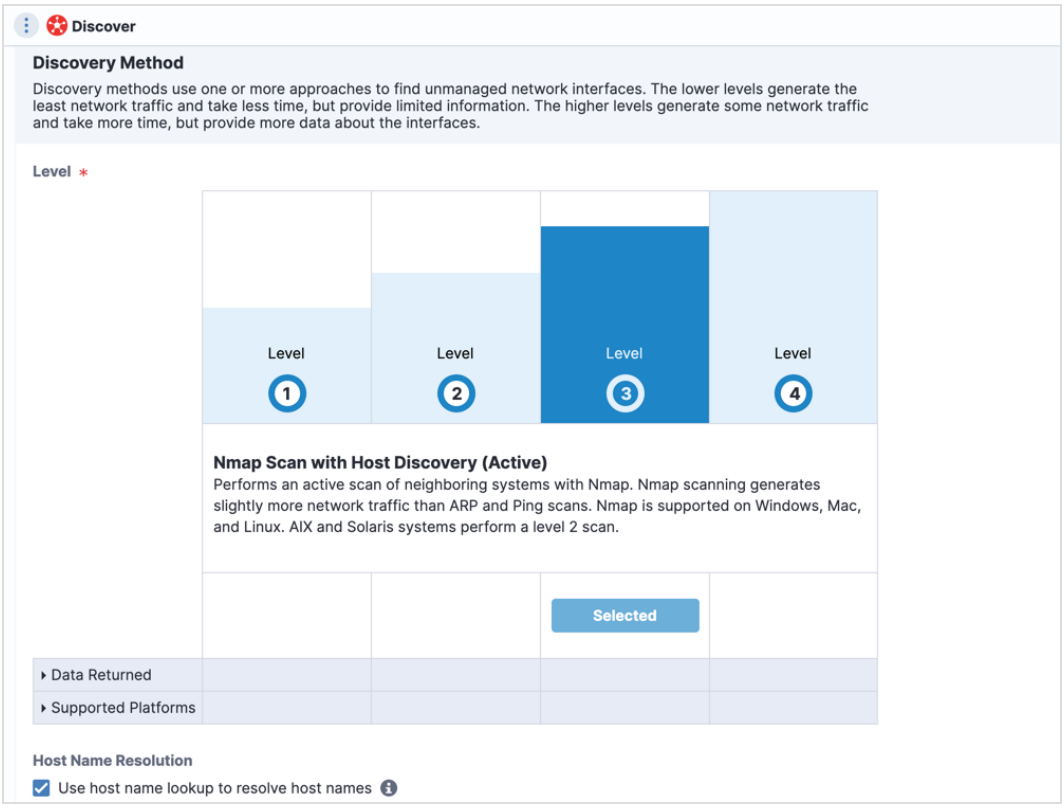
  For the most complete results from the scan, import locations before configuring a profile. You can update locations later as you find more information about your networks.

Create profile

1. Add a profile. From the Discover menu, click **Profiles**, and then click **Create Profile**.
2. Give the profile a name and select the **Distributed** profile type.
3. If IPv6 compatibility is enabled, select a protocol version.
   - If you select **Internet Protocol version 4**, all types of discovery methods are available.
   - If you select **Internet Protocol version 6**, only the level 1 discovery method (NDP) is available.
   - If you specify any IP addresses in the **Scan Inclusions** and **Scan Exclusions** sections, the IP addresses must match the protocol version of the profile (IPv4 or IPv6).
   - For more information about how to enable IPv6 compatibility, see Toggle IPv6 compatibility on page 61.

© 2026 Tanium Inc. All Rights Reserved

4. For IPv4 profiles, select a discovery method (level 1-4) and whether you want to include host name lookup. Host name resolution consumes some network resources, even with lower impact discovery methods.



BEST PRACTICE

To help target installation of the Tanium Client on unmanaged interfaces, configure a scan that returns operating system information about the endpoints. Level 4 Nmap discovery provides the best results, but Level 2 ping scans also provide some operating system information.

5. Select how Tanium manages the Npcap driver on Windows endpoints.

   - To use the existing Npcap version on the endpoint and not update to a newer version, select **Use existing Npcap version**. Tanium installs Npcap on the endpoint if it is not already installed. This is the default setting.

     NOTE

     If you update to Discover 4.1.240 or later from an older version, be aware that the default Npcap management behavior changed to no longer automatically update Npcap. To have Tanium continue to update Npcap on endpoints, select the **Update Tanium version of Npcap** option.

     Select this option if you plan to manually update Npcap versions.

© 2026 Tanium Inc. All Rights Reserved

- To use the Npcap version included with Discover, select **Update Tanium version of Npcap**.
    - Tanium updates Npcap if it is not on the endpoint or if Npcap was previously installed by Tanium. For Windows 7 and Windows Server 2008 endpoints, Tanium installs Npcap 1.20 for compatibility reasons. For all other endpoints, Tanium installs Npcap 1.75.
    - If Npcap was installed outside of Tanium, Tanium does not update Npcap.

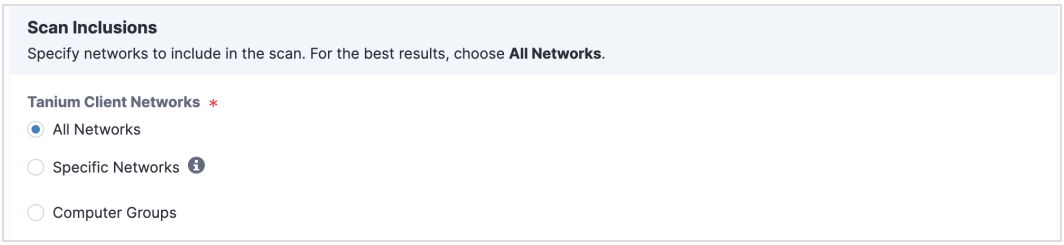


Npcap updates might cause the endpoint to automatically reboot or to restart the network. If you want to manage when endpoints reboot, do not select the **Update Tanium version of Npcap** option.

6. If you selected discovery method level 4, specify the ports to scan.
7. Configure targeting. Targeting specifies the networks to include and exclude from the scan.
    a. **Scan Inclusions**: Specify networks that you want to scan.

    Typically, choose **All Networks** to include the broadest results. The **All Networks** option scans all networks that are accessible to the endpoints that are configured for the Discover action group. For the best results, configure the Discover action group to include all computers. For more information, see Installing Discover on page 58.

    To run scans on endpoints that are only in certain networks, select **Specific Networks**, then click .



    With this selection, results outside the scope of the selected networks are not included in the final report.

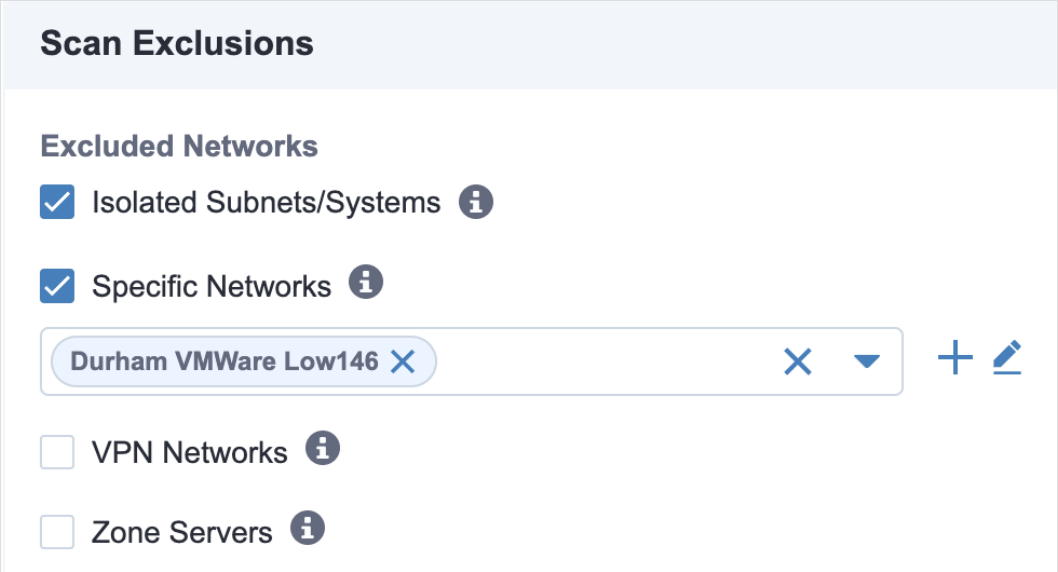


Any IP addresses that you specify must match the protocol version of the profile (IPv4 or IPv6).

    To run scans on endpoints that are only in a certain computer group, select **Computer Groups**, then select the groups. With this selection, results outside the scope of the selected groups do not perform the selected scan.

© 2026 Tanium Inc. All Rights Reserved

b. **Scan Exclusions**: Specify networks that you want to exclude from scans. Endpoints on these networks do not perform scans, and no results are returned from endpoints on these networks. Consider defining the following exclusions:



- **Isolated Endpoints**: Prevent isolated endpoints from performing scans. To enable these endpoints to perform scans, clear the checkbox.
- **Specific Networks**: List critical devices with fragile networking. These IPs are not contacted during the scan process. If any endpoints in this network are running the Tanium Client, these endpoints do not perform scans.
- **VPN Networks:** List VPN subnets to avoid, including interfaces outside your corporate networks. If you do not define VPN networks as an exclusion, devices such as gaming systems and streaming devices from home networks might be discovered. If a managed endpoint is used on a public network, such as in a restaurant or airport, devices on those networks might be discovered if the VPN exclusion is not defined.
- **Zone Servers**: Define internet zone servers to exclude endpoints connecting from internet locations. List the internet-accessible host names or IP addresses of the zone servers to be excluded. As a safety mechanism, if an endpoint that connects through a zone server cannot resolve a host name in a zone server exclusion, the scan is not performed on that endpoint. Configure either all IP addresses or all host names for your zone server exclusions and zone server name definitions. Mixing IP addresses and host names in the configuration and exclusions can have unexpected results.

BEST PRACTICE

At a minimum, configure exclusions for VPN, zone servers, and critical endpoints with fragile network configurations.

NOTE

Any IP addresses that you specify must match the protocol version of the profile (IPv4 or IPv6).

© 2026 Tanium Inc. All Rights Reserved

8. Configure the scan schedule and scan window.

   a. **Schedule**: The schedule defines how often to run the scan.

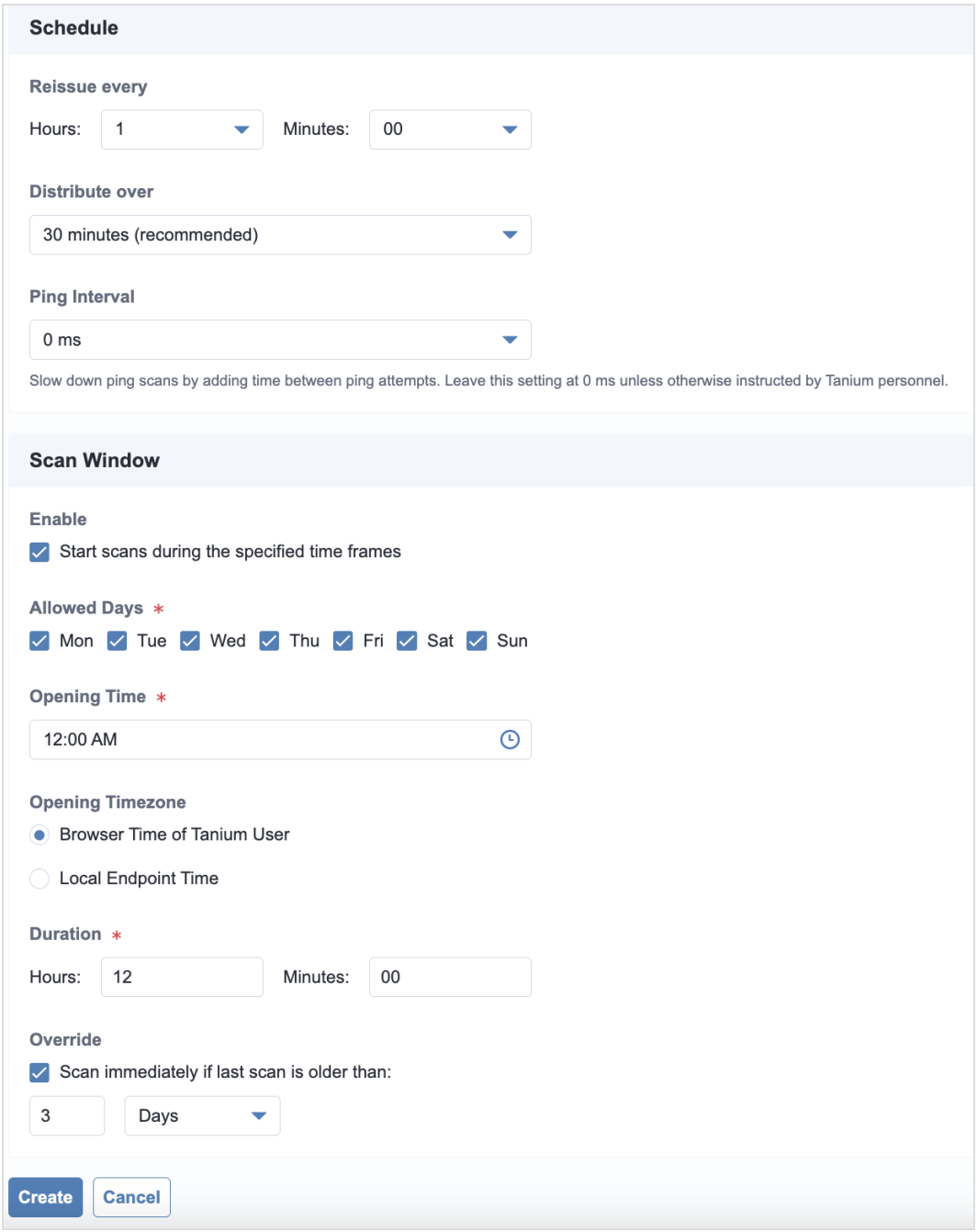
   

   Recommended scanning frequency is once an hour in most environments. If you are using level 2 discovery, set the **Reissue every** interval to an hour or more to ensure that the next scan does not begin before the current scan completes.

   The **Ping Interval** lets you set the time between ping scan attempts. In most cases, you should not need to change the default of 0 milliseconds. This field is available for level 2 discovery (Windows and Linux endpoints only).

© 2026 Tanium Inc. All Rights Reserved

b. **Scan Window** (Windows, Mac, and Linux endpoints only): Configure specific times to run the discovery process on your endpoints.



If a scan is scheduled to run outside the scan window, nothing is run as a part of the scan.

The time can either be the local endpoint time of the Tanium Client (distributed scans) or satellite (satellite scans), or the local time of the Tanium user that is configuring the profile. For example, you can choose **Local Endpoint Time** and create a scan configuration to scan your endpoints daily, but restrict the scans to run during non-business hours, such

© 2026 Tanium Inc. All Rights Reserved

as from 6:30 PM to 11:30 PM. If some of your endpoints are offline during the scan window, you can choose the **Override** option to scan any endpoints that have a scan age older than a specified amount of time, in hours, days, or weeks.

The **Duration** of the scan window must be greater than or equal to the **Reissue every** plus **Distribute over** settings in the schedule section. If the value is set to less than the sum of these values, some endpoints never scan.

9. Click **Create**.

Discovery process

After you save a profile, the following actions occur:

1. Scheduled actions are created for the profile: **Discover Content - Execute Scan [*profile_name*]** and **Discover Content - Execute Scan for non-Windows [*profile_name*]**.
2. Scans run according to the defined schedule.
3. Results of discovery scans are imported into Discover at the configured **Import Frequency** interval. For more information, see Configure import frequency on page 60.

If you have enabled Endpoint Configuration approval, configuration changes must be approved in Endpoint Configuration before they deploy to endpoints.

Scan results

After you discover interfaces, the **Interfaces** pages list the interfaces with the following icons:

- : Managed interfaces that have Tanium Client installed.
- : Unmanaged interfaces that do not have Tanium Client installed, but might be a candidate for a Tanium Client installation.
- : Unmanageable interfaces are on devices that cannot run the Tanium Client. By default, unmanageable interfaces have an OS Platform that is not supported by the Tanium Client, defined by the **Unmanageable OS Platforms** predefined automatic label. Unmanageable interfaces are not included in the managed and unmanaged interface statistics.

The profile type and discovery method that were used to find the interface return varying columns on the **Interfaces** pages. For more information, see Reference: Data returned by profile type on page 133.

Force import of scan results

Instead of waiting for the **Reissue every** time to pass, you can force an import of the most recent scan results.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Discover > Profiles**.
2. Click **Reimport Scan Results**. When you click this button:
    - Distributed scan results are collected. If these methods are not active on the endpoints, no results are collected.
    - Centralized profile scan results are collected from the Tanium Module Server.
    - Satellite profile scan results are collected from the satellite.

    Clicking **Reimport Scan Results** does not force the execution of distributed, satellite, or centralized scans. The results for distributed scans are gathered if they are already distributed and active on the endpoints. For satellite scans, the results from the latest scan are collected from the associated satellite. For centralized scans, the results from the last scan are collected from the Tanium Module Server.

What to do next

- For more information about troubleshooting problems with scans, see Troubleshooting Discover on page 121.
- Manage your interfaces with labels. For more information, see Managing interfaces on page 96.
- Configure notifications for Discover events. For more information, see Create connection for event notifications on page 112.

© 2026 Tanium Inc. All Rights Reserved

Running satellite scans

Use satellite scans to scan from an endpoint configured as a satellite to remote subnets.

Scan unmanaged subnets with a satellite scan

Use satellite scans to find interfaces in unmanaged subnets. The Network Mapper (Nmap) utility finds information about network interfaces by running host discovery and OS fingerprinting from the satellite on a target network. The satellite that returned the data about an interface is listed in the **Satellite ID** column of the **Details** table on the **Interfaces** page.

The satellite scan is equivalent to a level 4 distributed scan.

Value on Interfaces pages: satellite nmap

By default, Discover scans 1000 commonly used TCP ports to calculate the **OS Generation** field. For more information, see Top 1,000 TCP and UDP ports (nmap default). In the profile settings you can configure different ports to scan and can change the source port from which the scan originates. The value of the **OS Generation** field is a “best guess” from Nmap, and is not displayed for managed interfaces.

The accuracy of OS fingerprinting and host name resolution depends on how remote the network is that you choose to scan. The more network hops away you search, the harder it is for Nmap to identify the operating system.

Satellite-based network scan results include MAC addresses when targeting subnets to which the satellite has direct connections. Scans of remote subnets do not have MAC addresses on the discovered interfaces, because the traffic must pass through a router. If a discovered interface does not have a MAC address, Discover uses the IP address as the unique identifier.

The Nmap utility is installed on the satellite after you create a satellite profile. If you remove all of the satellite profiles, the Nmap utility gets removed.

Configure profile for satellite scan

Configure a profile for the satellite scan by selecting the satellite to use, defining which networks to scan, and setting a scan schedule.



Create profiles according to your deployment plan. For more information, see Develop a deployment plan on page 21. For information about the data provided by each profile type, see Reference: Data returned by profile type on page 133.

© 2026 Tanium Inc. All Rights Reserved

Before you begin

- To scan portions of the network, you must know the IP ranges or the networks that you want to scan. Enter a network address or IP ranges for up to 4096 IP addresses (or the equivalent of a /20 network).
- You must have configured satellites in Tanium Direct Connect. Satellite configuration is available in Direct Connect version 2.1 and later. For more information about how to configure satellites, see Tanium Direct Connect User Guide: Managing satellites.

  NOTE

  You can designate only Windows, MacOS, or Linux endpoints as satellites. An endpoint running Windows 11 Arm cannot be used as a satellite.

- (Optional) Create a locations file to map physical locations to discovered interfaces. Assign users to specific locations to limit access to interface data to specific user groups. You can configure locations at any time because the locations are evaluated every time a Discover scan completes. For more information, see Locations on page 99.

  BEST PRACTICE

  For the most complete results from the scan, import locations before configuring a profile. You can update locations later as you find more information about your networks.

1. Add a profile. From the Discover menu, click **Profiles**, and then click **Create Profile**.
2. Give the profile a name and select the **Satellite** profile type.
3. Select how Tanium manages the Npcap driver on Windows endpoints.
   - To use the existing Npcap version on the endpoint and not update to a newer version, select **Use existing Npcap version**. Tanium installs Npcap on the endpoint if it is not already installed. This is the default setting.

     NOTE

     If you update to Discover 4.1.240 or later from an older version, be aware that the default Npcap management behavior changed to no longer automatically update Npcap. To have Tanium continue to update Npcap on endpoints, select the **Update Tanium version of Npcap** option.

     Select this option if you plan to manually update Npcap versions.
   - To use the Npcap version included with Discover, select **Update Tanium version of Npcap**.
     - Tanium updates Npcap if it is not on the endpoint or if Npcap was previously installed by Tanium. For Windows 7 and Windows Server 2008 endpoints, Tanium installs Npcap 1.20 for compatibility reasons. For all other endpoints, Tanium installs Npcap 1.75.
     - If Npcap was installed outside of Tanium, Tanium does not update Npcap.

© 2026 Tanium Inc. All Rights Reserved



Npcap updates might cause the endpoint to automatically reboot or to restart the network. If you want to manage when endpoints reboot, do not select the **Update Tanium version of Npcap** option.

4. Specify the ports to scan.
5. Configure scan inclusions and exclusions to specify the networks that are scanned by the satellite.
    a. **Scan Inclusions**: Specify networks that you want included in the scan. Select a network from the **Included Networks** list or click to add a network to scan. The satellite scans only the selected network.
    b. **Scan Exclusions**: To exclude a portion of the **Included Networks** from the scan, select **Specific Networks** and select a network from the list, or click to add a subnet or IP address to exclude from the scan. The IPs you exclude are not contacted during the scan process. For example, if you specify 192.168.0.0/20 in **Included Networks**, you might specify to exclude 192.168.1.0/24 and 192.168.0.1.

© 2026 Tanium Inc. All Rights Reserved

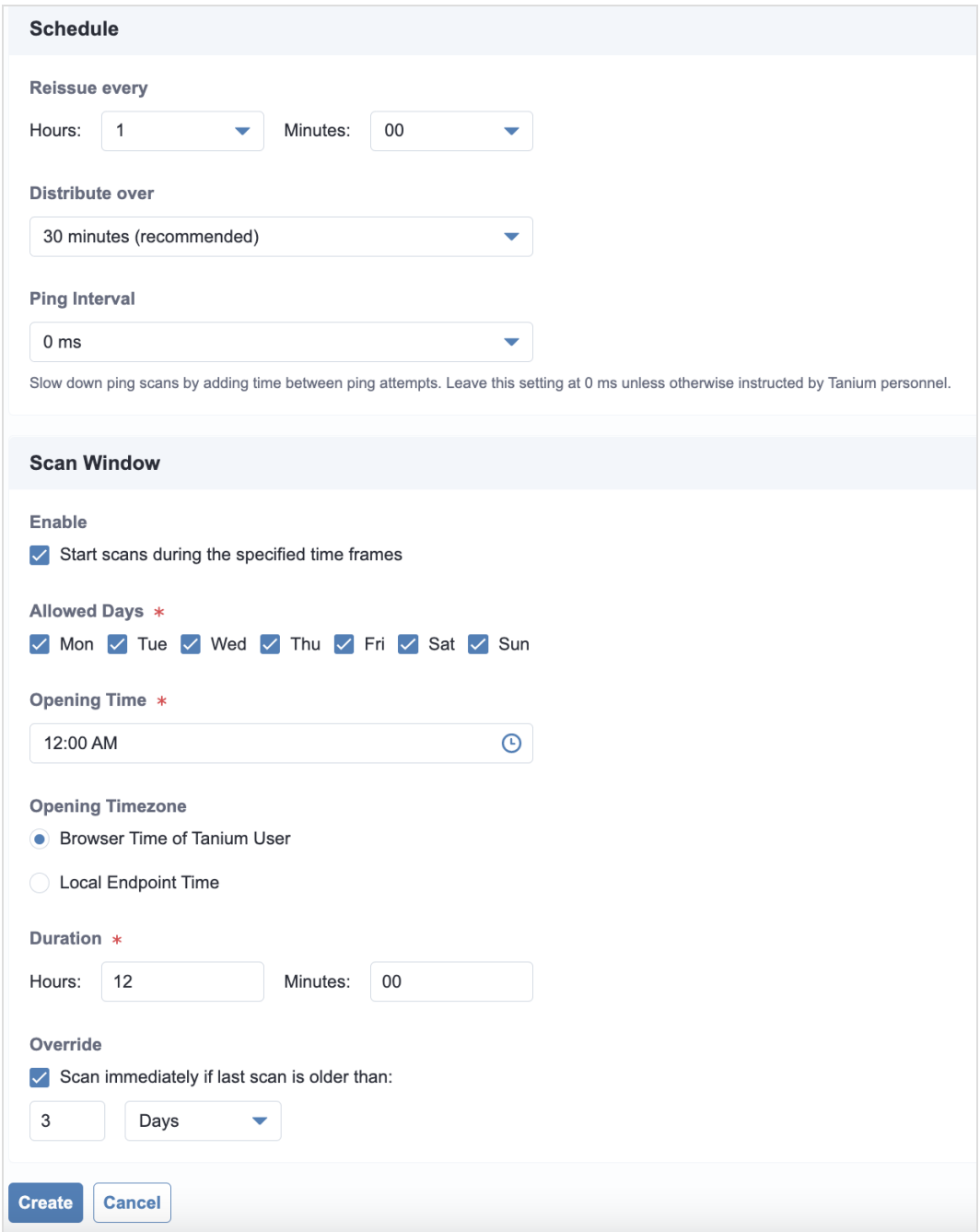
6. Configure the scan schedule and scan window.

© 2026 Tanium Inc. All Rights Reserved

a. **Schedule**: The schedule defines how often to run the scan.

> BEST PRACTICE
>
> Recommended scanning frequency is once an hour in most environments.

b. **Scan Window** (Windows, Mac, and Linux endpoints only): Configure specific times to run the discovery process on your endpoints.



If a scan is scheduled to run outside the scan window, nothing is run as a part of the scan.

© 2026 Tanium Inc. All Rights Reserved

The time can either be the local endpoint time of the Tanium Client (distributed scans) or satellite (satellite scans), or the local time of the Tanium user that is configuring the profile. For example, you can choose **Local Endpoint Time** and create a scan configuration to scan your endpoints daily, but restrict the scans to run during non-business hours, such as from 6:30 PM to 11:30 PM. If some of your endpoints are offline during the scan window, you can choose the **Override** option to scan any endpoints that have a scan age older than a specified amount of time, in hours, days, or weeks.

The **Duration** of the scan window must be greater than or equal to the **Reissue every** plus **Distribute over** settings in the schedule section. If the value is set to less than the sum of these values, some endpoints never scan.

7. Click **Create**.

Discovery process

The discovery process for each satellite scan is defined by its profile settings, including the network inclusions and exclusions, discovery methods, and scan schedule.

1. The scan runs on the targeted network at the scheduled interval. On the first run, the Nmap utility is installed on the satellite.
2. When the scan completes, scan results are sent to Discover.
3. The most recent valid scan results are imported into Discover at the **Reissue every** interval defined in the profile. Scan results expire when they are twice as old as the **Reissue every** setting. For example, if **Reissue every** is set to one hour, scan results expire when they are older than two hours.

To check the status of a satellite scan, from the Main menu, go to **Modules > Discover > Profiles**. Hover over the icon in the **Status** column to view the status message, or click  to expand the profile and view more detailed status and troubleshooting information.

Satellite scan results

Scan results

After you discover interfaces, the **Interfaces** pages list the interfaces with the following icons:

- : Managed interfaces that have Tanium Client installed.
- : Unmanaged interfaces that do not have Tanium Client installed, but might be a candidate for a Tanium Client installation.
- : Unmanageable interfaces are on devices that cannot run the Tanium Client. By default, unmanageable interfaces have an OS Platform that is not supported by the Tanium Client, defined by the **Unmanageable OS Platforms** predefined automatic label. Unmanageable interfaces are not included in the managed and unmanaged interface statistics.

The profile type and discovery method that were used to find the interface return varying columns on the **Interfaces** pages. For more information, see Reference: Data returned by profile type on page 133.

Unmanaged interfaces discovered by a satellite scan include the ID of the satellite that discovered them. This ID is displayed in the **Satellite ID** column of the **Details** table on the **Interfaces** page.

© 2026 Tanium Inc. All Rights Reserved

Force import of scan results

Instead of waiting for the **Reissue every** time to pass, you can force an import of the most recent scan results.

1. From the Main menu, go to **Modules > Discover > Profiles**.
2. Click **Reimport Scan Results**. When you click this button:
    - Distributed scan results are collected. If these methods are not active on the endpoints, no results are collected.
    - Centralized profile scan results are collected from the Tanium Module Server.
    - Satellite profile scan results are collected from the satellite.

    Clicking **Reimport Scan Results** does not force the execution of distributed, satellite, or centralized scans. The results for distributed scans are gathered if they are already distributed and active on the endpoints. For satellite scans, the results from the latest scan are collected from the associated satellite. For centralized scans, the results from the last scan are collected from the Tanium Module Server.

What to do next

- For more information about troubleshooting problems with scans, see Troubleshooting Discover on page 121.
- Manage your interfaces with labels. For more information, see Managing interfaces on page 96.
- Configure notifications for Discover events. For more information, see Create connection for event notifications on page 112.

© 2026 Tanium Inc. All Rights Reserved

Running centralized scans

Use centralized scans to scan from the Tanium Module server to unmanaged environments, such as Amazon EC2 or an unmanaged subnet.

IMPORTANT

Centralized scanning is a legacy feature that is not available to new customers of Discover. Instead, use satellite scans for NMAP scans, and Tanium™ Asset for AWS scans. If you used centralized scans before and want to re-enable centralized scans, contact Tanium Support. For information about satellite scans, see Running satellite scans on page 78. For information about AWS scans, see Tanium Asset User Guide: Configuring sources.

Scan unmanaged subnets with a centralized Nmap scan

BEST PRACTICE

Use satellite scans with satellites that are located close to the subnets that you want to scan for highest fidelity data. Operation system detection and open ports detection become less accurate as the scan traffic passes through routers, firewalls, and NAT gateways. For information about satellite scans, see Running satellite scans on page 78.

Use centralized Nmap scans to find interfaces in unmanaged subnets. The Network Mapper (Nmap) utility finds information about network interfaces by running host discovery and OS fingerprinting from the Module Server on a target network.

The centralized Nmap scan is an equivalent of a level 4 distributed scan.

Value on Interfaces pages: centralized nmap

By default, Discover scans 1000 commonly used TCP ports to calculate the **OS Generation** field. For more information, see Top 1,000 TCP and UDP ports (nmap default). In the profile settings you can configure different ports to scan and can change the source port from which the scan originates. The value of the **OS Generation** field is a “best guess” from Nmap, and is not displayed for managed interfaces.

The accuracy of OS fingerprinting and host name resolution depends on how remote the network is that you choose to scan. The more network hops away you search, the harder it is for Nmap to identify the operating system.

Remote network scans might not return MAC addresses for discovered interfaces. If an interface does not have a MAC address, the IP address is used as the unique identifier.

The Nmap utility is installed on the Module Server after you create a centralized Nmap profile. If you remove all of the centralized Nmap profiles, the Nmap utility gets removed.

Configure profile for centralized Nmap scan

Configure a profile for the centralized Nmap scan by defining which networks to scan, the discovery method, and the scan schedule.

© 2026 Tanium Inc. All Rights Reserved

NOTE

For information about the data provided by each profile type, see Reference: Data returned by profile type on page 133.

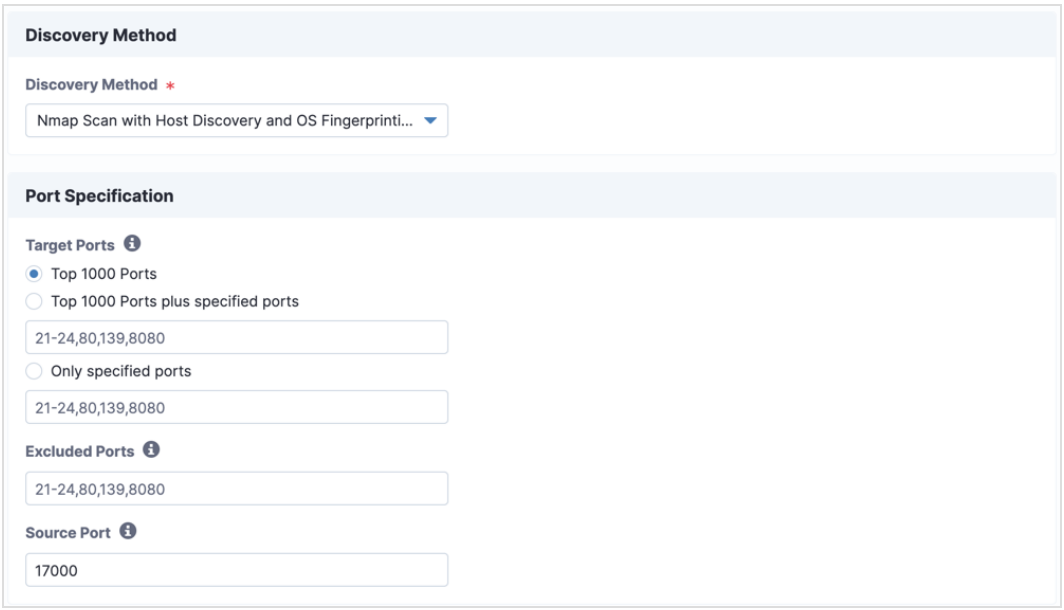
Before you begin

- Ensure that you have the target network information, which is a comma-separated list of CIDR addresses of up to 4096 IP addresses (or the equivalent of a /20 network).
- (Optional) Create a locations file to map physical locations to discovered interfaces. Assign users to specific locations to limit access to interface data to specific user groups. You can configure locations at any time because the locations are evaluated every time a Discover scan completes. For more information, see Locations on page 99.

  BEST PRACTICE

  For the most complete results from the scan, import locations before configuring a profile. You can update locations later as you find more information about your networks.

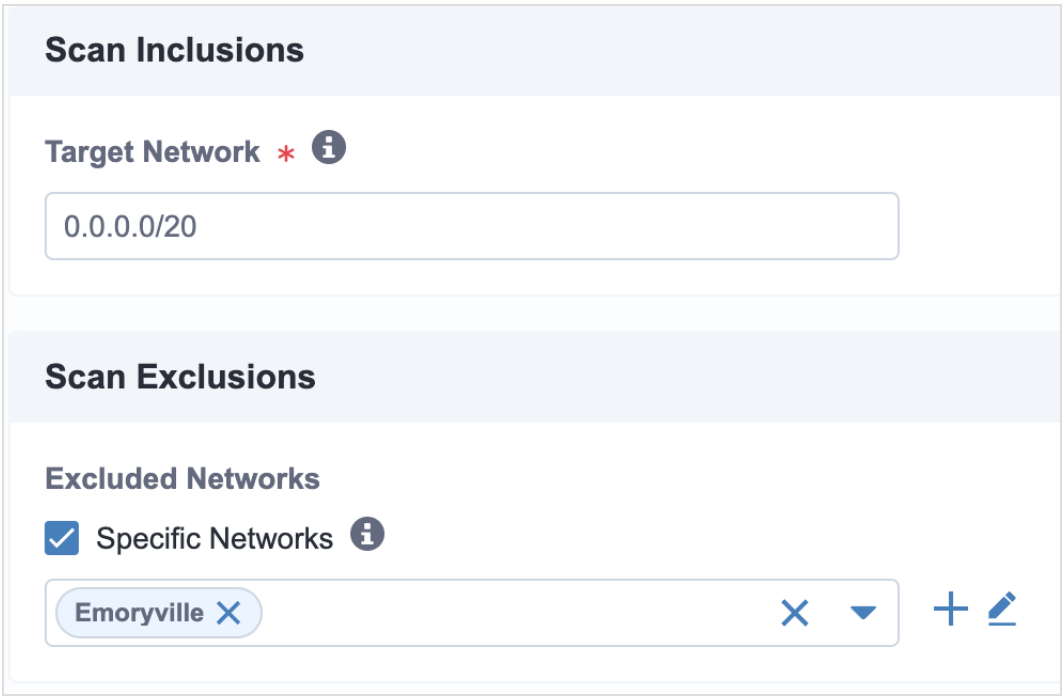
1. Add a profile. From the Discover menu, click **Profiles**, and then click **Create Profile**.
2. Give the profile a name and select the **Centralized** profile type.
3. For the **Discovery Method**, choose **Nmap Scan with Host Discovery and OS Fingerprinting**.



4. Specify the ports to scan.

© 2026 Tanium Inc. All Rights Reserved

5. When you define scan inclusions, indicate the set of CIDR addresses for the Tanium Module Server to target with the scan. Add exclusions (such as individual IP addresses or subnets) to limit the scan within the specified inclusion range. For example, if you specify the Target Network is 192.168.0.0/20, you might specify to exclude 192.168.1.0/24 and 192.168.0.1.



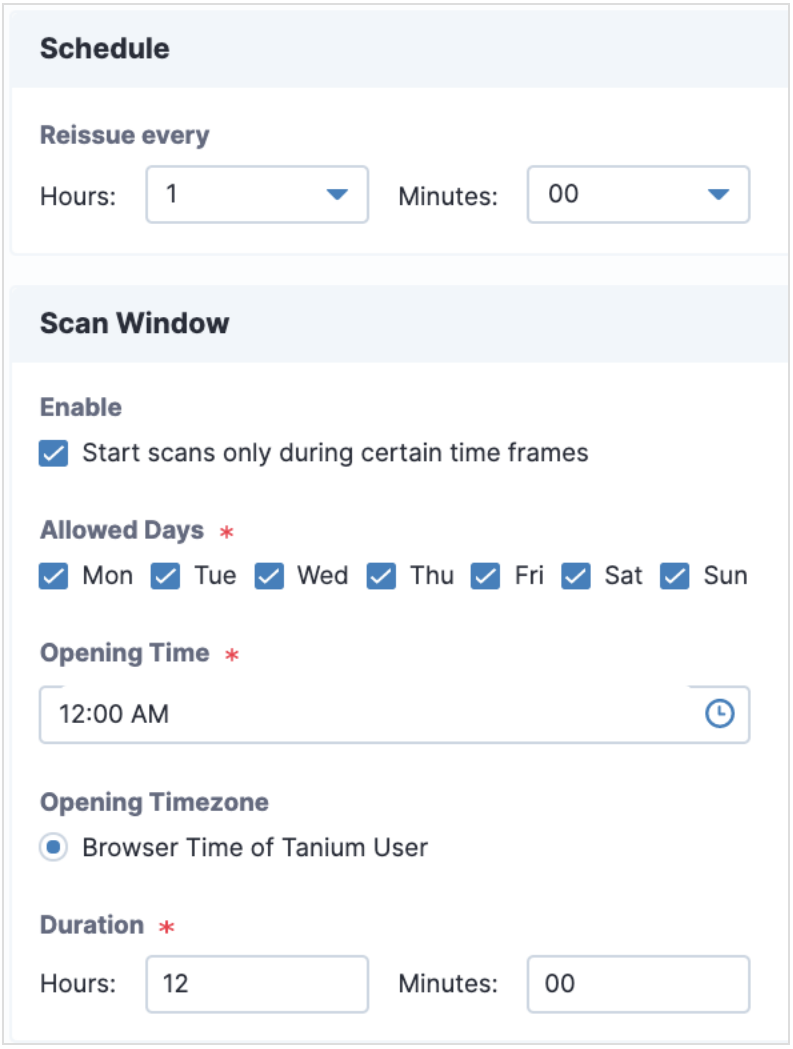
© 2026 Tanium Inc. All Rights Reserved

6. Configure the scan schedule and scan window.

   a. **Schedule**: The schedule defines how often to run the scan.

   > BEST PRACTICE
   >
   > Recommended scanning frequency is once an hour in most environments.

   b. **Scan Window**: Configure specific times to run the discovery process.



   If a scan is scheduled to run outside the scan window, nothing is run as a part of the scan. For example, you can create a scan configuration to scan daily, but restrict the scans to run during non-business hours, such as from 6:30 PM to 11:30 PM.

   The **Duration** of the scan window must be greater than or equal to the **Reissue every** setting in the schedule section or the scan might not run.

7. Click **Create**.

© 2026 Tanium Inc. All Rights Reserved

Discovery process

1. On the first run of a centralized Nmap profile, Discover installs the Nmap utility on the Module Server. The scan runs at the scheduled interval.
2. Perform an Nmap scan on the targeted network, as defined in the profile settings.
3. Import results into Discover at the **Import Frequency** interval that you defined. For more information, see Configure import frequency on page 60.

If you have enabled Endpoint Configuration approval, configuration changes must be approved in Endpoint Configuration before they deploy to endpoints.

Scan Amazon EC2 environments

BEST PRACTICE

Use Asset sources for AWS cloud inventories. Asset sources include enhancements such as enterprise authentication), and support additional cloud providers. For more information, see Tanium Asset User Guide: Configuring sources.

Discover unmanaged interfaces in an Amazon EC2 environment from the Tanium Module Server.

NOTE

Discover does not support creating a profile for an AWS organization that allows access to AWS accounts within that organizational hierarchy. You must create centralized AWS profile in Discover for each account that might contain an EC2 instance.

Value on Interfaces pages: aws api

Before you begin

- Configure your network to allow access from the Tanium Module Server to `ec2.*.amazonaws.com`, `sts.*.amazonaws.com`, and `ssm.*.amazonaws.com` on port 443.
- If you have a proxy server configured for your Tanium Module Server, confirm that it is the **Basic** server type. Amazon EC2 does not support the **NTLM** server type. For more information, see Tanium™ Appliance User Guide: Types of proxy servers or Tanium Core Platform User Guide for Windows Deployments: Types of proxy servers.
- (Optional) Create a locations file to map physical locations to discovered interfaces. Assign users to specific locations to limit access to interface data to specific user groups. You can configure locations at any time because the locations are evaluated every time a Discover scan completes. For more information, see Locations on page 99.

  BEST PRACTICE

  For the most complete results from the scan, import locations before configuring a profile. You can update locations later as you find more information about your networks.

© 2026 Tanium Inc. All Rights Reserved

Configure API user

To access the EC2 environment, you must have a user that has API access and the required permissions.

1. Create a user in Amazon Web Services (AWS) with programmatic access. This user must have an access key ID and secret access key. For more information, see AWS docs: Creating an IAM user in your AWS account.
2. Attach the following policy to the user you created in AWS. This policy limits the access of the user to the minimum requirements for Discover. For more information, see AWS docs: Create and Attach Your First Customer Managed Policy.

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "ec2:DescribeImages",
                                "ec2:DescribeInstances",
                                "ssm:DescribeInstanceInformation"
                        ],
                        "Resource": "*"
                }
        ]
}
```

NOTE

Optionally, you can provide a role that the user must assume in AWS. If you provide this role, the user must have the appropriate IAM to assume the role and that role must have access to the appropriate policy to perform the scan. If you decide not to require the user to assume this role, then the Assume IAM Role field in Discover must remain empty.

Configure profile for Amazon EC2 centralized scan

Configure a profile for the centralized scan by defining the credentials for AWS and a scan schedule.

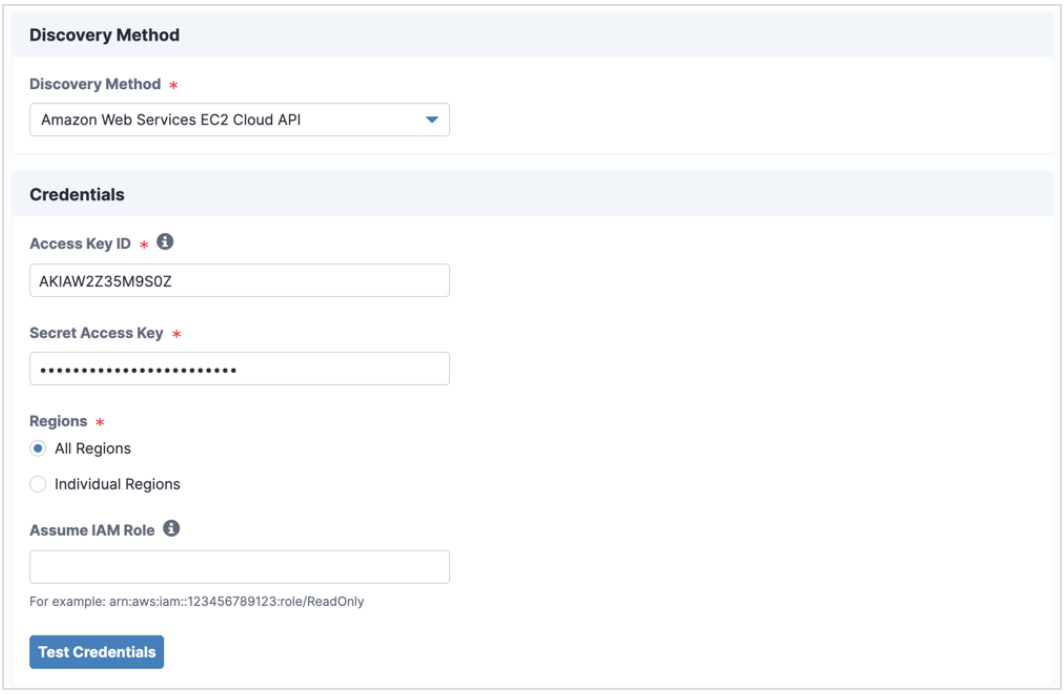
NOTE

For more information about the data provided by each profile type, see Reference: Data returned by profile type on page 133.

1. Add a profile. From the Discover menu, click **Profiles**, and then click **Create Profile**.
2. Give the profile a name and select the **Centralized** profile type.
3. For the **Discovery Method**, choose **Amazon Web Services EC2 Cloud API**.

© 2026 Tanium Inc. All Rights Reserved

4. Enter details for the discovery method to connect the Tanium Module Server to the Amazon EC2 environment.



TIP

The secret access key persists after you save the profile. You do not need to enter the key if you edit the profile later.

5. Test the connection to AWS. Click **Test Credentials**. The credentials are tested against all selected regions. Edit the **Regions** setting to include only regions to which the ID and key have access.
6. Configure the scan schedule, which defines how often to query AWS.
7. Click **Create**.

Discovery process

After you save an Amazon EC2 centralized scanning profile, the following actions occur:

1. On the scheduled interval, the Tanium Module Server uses the AWS API to query your EC2 environment.
2. The information from AWS comes from the AWS API. The individual EC2 instances are not contacted by Tanium.
3. Import results into Discover at the **Import Frequency** interval that you defined. For more information, see Configure import frequency on page 60.

IMPORTANT

An EC2 instance with multiple NICs results in multiple interfaces in Discover, one for each NIC.

© 2026 Tanium Inc. All Rights Reserved

If you have enabled Endpoint Configuration approval, configuration changes must be approved in Endpoint Configuration before they deploy to endpoints.

Centralized scan results

Scan results

After you discover interfaces, the **Interfaces** pages list the interfaces with the following icons:

- : Managed interfaces that have Tanium Client installed.
- : Unmanaged interfaces that do not have Tanium Client installed, but might be a candidate for a Tanium Client installation.
- : Unmanageable interfaces are on devices that cannot run the Tanium Client. By default, unmanageable interfaces have an OS Platform that is not supported by the Tanium Client, defined by the **Unmanageable OS Platforms** predefined automatic label. Unmanageable interfaces are not included in the managed and unmanaged interface statistics.

The profile type and discovery method that were used to find the interface return varying columns on the **Interfaces** pages. For more information, see Reference: Data returned by profile type on page 133.

Force import of scan results

Instead of waiting for the **Reissue every** time to pass, you can force an import of the most recent scan results.

1. From the Main menu, go to **Modules > Discover > Profiles**.
2. Click **Reimport Scan Results**. When you click this button:
   - Distributed scan results are collected. If these methods are not active on the endpoints, no results are collected.
   - Centralized profile scan results are collected from the Tanium Module Server.
   - Satellite profile scan results are collected from the satellite.

   Clicking **Reimport Scan Results** does not force the execution of distributed, satellite, or centralized scans. The results for distributed scans are gathered if they are already distributed and active on the endpoints. For satellite scans, the results from the latest scan are collected from the associated satellite. For centralized scans, the results from the last scan are collected from the Tanium Module Server.

© 2026 Tanium Inc. All Rights Reserved

What to do next

- For more information about troubleshooting problems with scans, see Troubleshooting Discover on page 121.
- Manage your interfaces with labels. For more information, see Managing interfaces on page 96.
- Configure notifications for Discover events. For more information, see Create connection for event notifications on page 112.

© 2026 Tanium Inc. All Rights Reserved

Managing Discover profiles

A profile is a configuration object that defines how Discover finds interfaces in your network. You create a profile when you configure a scan. You might need to update its configuration to address changes in your environment or to correct errors that prevent it from running scans. Maintain your profiles to ensure that your scans are accurate and efficient so you can quickly find unmanaged interfaces on your network.

For more information about creating profiles and configuring scans, see the following pages:

- Running distributed scans on page 65
- Running satellite scans on page 78
- Running centralized scans on page 85

View profiles

1. From the Main menu, go to **Modules > Discover > Profiles**.
2. (Optional) Filter the grid with the following methods. The grid lists only the rows that match all filters that you specify:
    - Enter an alphanumeric string in **Filter items** to match text in any column.
    - Expand the **Filters** section and enter text in a filter field to match text to the corresponding grid column.
3. View information about the profiles in the profiles grid, including the profile status. For profiles that are not deployed, hover over its status icon to view a message that explains the reason for its status:

Icon	Status	Description
	**Deployed**	The profile configuration is valid and runs scans.
	Needs Deployment	The profile configuration is valid but not yet deployed.
	**Error**	The profile configuration is not valid and does not run scans. Edit the profile to correct any errors.
	**Disabled**	The profile is disabled and is not running scans, and actions associated with the profile are removed from the scheduled actions list. For more information, see Disable a profile on page 95.  NOTE This status is only applicable for distributed and satellite scan profiles.

© 2026 Tanium Inc. All Rights Reserved

4. Click the name of a profile to view its configuration details. For more information about the configuration details for each profile type, see Running distributed scans on page 65, Running centralized scans on page 85 and Running satellite scans on page 78.

Disable a profile

Disable a profile for a distributed or satellite scan if you want to temporarily stop the profile from running scans. When you disable a profile, its associated actions are removed from the scheduled actions list.

You might want to disable a profile when you have planned network maintenance or to preserve a scan when you test a new configuration. For example, you might want to consolidate multiple smaller scans into a single, larger scan. You can disable the smaller scans when you verify the consolidated configuration.

1. From the Main menu, go to **Modules > Discover > Profiles**.
2. Select the checkbox on one or more profile rows, then click **Disable** > **Confirm**.

© 2026 Tanium Inc. All Rights Reserved

Managing interfaces

Organize interfaces by applying locations or labels. Locations are a user-defined hierarchy of networks and physical locations. Labels are attributes that are added to the interface based on a set of conditions, and you can set actions to ignore, purge, mark unmanageable, or send notifications on the interfaces that match the conditions of the label.

View interface data

On the **Interfaces** pages, you can view interfaces by several different categories. You can customize and filter these results, and export the results to a CSV file.



In addition to the **Summary** page, use the **Managed**, **Unmanaged**, **Unmanageable**, and **Ignored** pages.

View charts

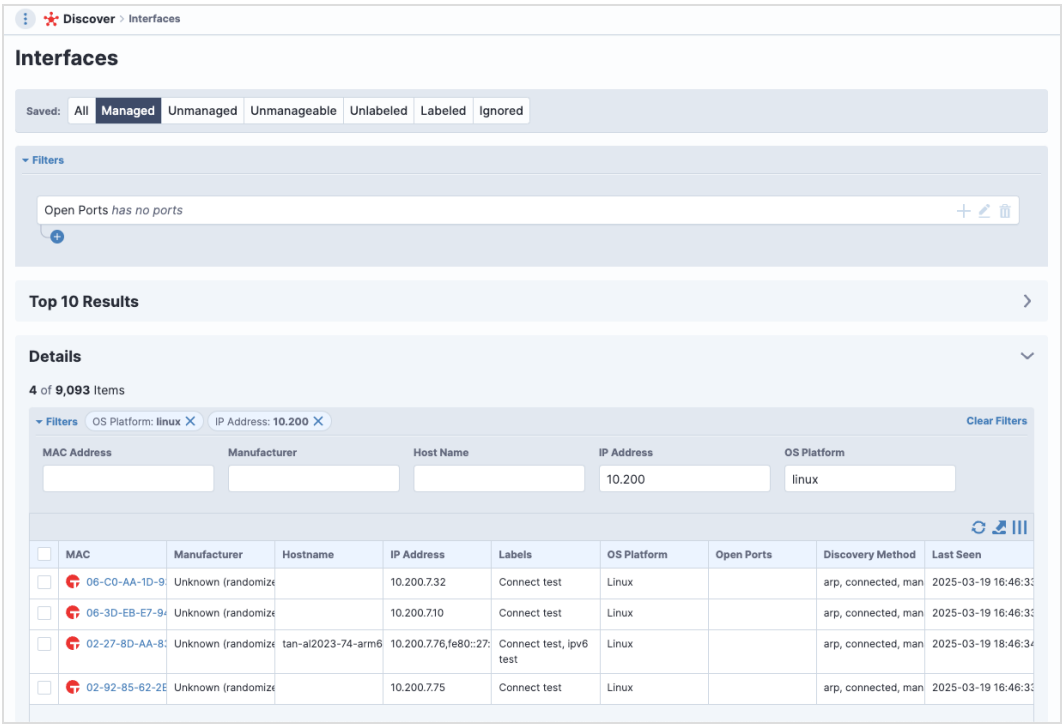
You can view bar charts that represent the device types, locations, and labels of interfaces.

1. From the Main menu, go to **Modules > Discover > Interfaces**.
   The **Interfaces** page opens and contains a **Top 10 Results** section and a **Details** section. The **Top 10 Results** section is collapsed by default.
2. Add filters at the top of the page to apply to data in both the **Top 10 Results** section and the **Details** section.
   - For the **Saved** filter, click an option to filter data by interface type, for example, **Managed** or **Unmanaged**.
   - To add advanced filters, expand **Filters** and then add individual or groups of filters. Advanced filter options are similar to the filter options available in the Tanium Interact **Question Builder**. For more information about how to configure filter options, see Tanium Console User Guide: Issue a question through the Question Builder.

     If you add a range of addresses with the **IP Address** filter, you can enter the range in CIDR notation or as starting and ending addresses separated by a dash character. If you enter starting and ending addresses, both addresses must be the same format (IPv4 or IPv6) and you must order the addresses from low to high. For example, `fe80::-fe80:ffff:ffff:ffff:ffff:ffff:ffff:ffff` is a valid range.
3. Expand the **Top 10 Results** section to view a graph of the top ten results by **Manufacturers**, **Locations**, or **Labels**.

© 2026 Tanium Inc. All Rights Reserved

4. The **Details** section contains a table with interface results. Any filters that you added at the top of the page apply to the table. To add additional filters to the table, expand the **Filters** section that appears above the table and enter any column filters.



NOTE

The **Manufacturer** column refers to the manufacturer of the network interface, not the endpoint. This value is derived from the organizationally unique identifier (OUI) in the first three octets of the MAC address assigned to the network interface.

- For a universally administered address (UAA) that was assigned by the device manufacturer, it displays the manufacturer's name.
- For a locally administered address (LAA) not assigned by the device manufacturer, it displays **Unknown (randomized MAC address)** or **Is Locally Administered MAC**. For example, an operating system randomly generates an LAA MAC address to enhance privacy.

Determine data source that found an interface

The value in the **Discovery Method** column in the **Details** table on the **Interfaces** page corresponds to the data source that discovered the interface.

Possible values for the Discovery Method column

Discovery Method	Data Source
arp	Distributed level 1 scan
connected	Distributed level 1 scan

© 2026 Tanium Inc. All Rights Reserved

Possible values for the Discovery Method column (continued)

Discovery Method	Data Source
ping	Distributed level 2 scan
nmap	Distributed level 3 or level 4 scan
aws api	Centralized Amazon EC2 environment scan
centralized nmap	Centralized nmap scan
satellite nmap	Satellite scan
managed	• If IPv6 compatibility is enabled, data comes from the **Discover - Managed Interfaces Include IPv6** saved question. • If IPv6 compatibility is disabled, data comes from the **Discover - Managed Interfaces** saved question.

Add columns to data grid

From any of the data grids on the **Interfaces** pages, you can customize the columns in the data grid. Click Customize Columns . Then, sort the results on that column, add columns to the data grid, and filter the results.

Export data

To export the current data grid of interfaces to a CSV file, click Export Data . The export includes the data that currently appears in the data grid.

The **Unmanageable** column in the CSV file indicates if the endpoint can be managed by the Tanium Client. The following table explains the numbers in the **Unmanageable** column.

Possible values for the Unmanageable column

Number	Label
0	Managed or Manageable (automatic)
1	Unmanageable (automatic)
2	Manually Marked Manageable
3	Manually Marked Unmanageable

Mark interfaces as manageable or unmanageable

You can automatically or manually mark interfaces as manageable or unmanageable. A manually applied label overrides an automatically applied label. For example, if an interface was automatically marked as unmanageable, you can override that label by manually marking the interface as manageable.

© 2026 Tanium Inc. All Rights Reserved

- You can use the **Mark Unmanageable** label activity to automatically mark interfaces as unmanageable with custom criteria. For more information, see Managing interfaces on page 96.
- You can manually mark an interface as manageable.
    1. From the Main menu, go to **Modules > Discover > Interfaces**.
    2. At the top of the page, select **Unmanageable**. By default, the **Unmanageable OS Platforms** predefined automatic label defines which interfaces are marked as unmanageable and shows on the **Unmanageable** page.
    3. Select an interface from the **Details** table.
    4. Click **Mark Manageable** to apply the **Manually Marked Manageable** label.
- You can manually mark an interface as unmanageable.
    1. From the Main menu, go to **Modules > Discover > Interfaces**.
    2. At the top of the page, select **Unmanaged**.
    3. Select an interface from the **Details** table.
    4. Click **Mark Unmanageable** to apply the **Manually Marked Unmanageable** label.

Ignore interfaces

When you ignore an interface, it is removed from the list of interfaces, and is added to the list on the **Interfaces > Ignored** page. An ignored interface is not included in views or counts.

- To ignore interfaces, select interfaces and click **Ignore**, or create an automatic label to ignore interfaces. For more information about how to create automatic labels, see Managing interfaces on page 96.
- To start tracking an interface again, update the interface on the **Interfaces > Ignored** page.

If you ignore an interface with an automatic label, you cannot override the ignore with a manual setting on the interface. If you have manually ignored an interface, locate the interface under Ignored in the Discover menu and click **Unignore**.

Locations



Locations does not support IPv6.

You can group discovered interfaces by mapping subnets to geographic or physical locations. After you map the network address and network address translation (NAT) address (CIDR, IP, or IP range) to your own hierarchy of locations, you can see information about how many devices are at a location on the **Interfaces** page. You can also assign access to network interface information to Tanium user groups.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

For location permissions to work with personas, user groups that are assigned to a location must be added to the default persona for a user, not to an alternative persona. For more information about personas and user groups, see Tanium Console User Guide: Managing personas and Tanium Console User Guide: Managing user groups.

BEST PRACTICE

To develop the location hierarchy, work with your network team. Typically, the network team has location information in an IP Address Management (IPAM) database.

TIP

You can support disjointed subnets by adding two separate lines to the same location. For example, 10.10.10.0/24 and 10.10.100.0/24.

Create location spreadsheet

Import locations by creating a comma-separated values (CSV) file. This file must be UTF-8 encoded.

CSV HEADER

The first row of the CSV file must contain at least three headers: Network, NAT, and at least one location column. You can have multiple headers for location to create a hierarchy of location information. The naming of the headers does not need to follow a certain pattern, but the first two columns must contain Network and NAT values.

CSV VALUES

CSV values can contain alphanumerics, white space, parenthesis (`()`), number signs (`#`), or hyphens (`-`).

- `Network` column: Values in the network column can contain a mix of CIDR and IP ranges.
- `NAT` column: Values in the NAT column can contain a mix of CIDR and IP ranges. This column must exist in the CSV file, but the values can be left blank by using `""` as the value.
- `Locations` columns: Headers and values for the locations are user-defined and generally go from largest geographical location (country, region) to smallest (city, office). Use a maximum of 5 columns for location (for example: Country, State, City, Building, Floor).

Confirm that each row ends in a unique location in the hierarchy specified in the file. For more information, see Problem: Error with locations CSV file on page 127.

CSV EXAMPLE

```
"Network","NAT","Country","State","Site","Building","Floor"
"10.0.0.0/24","","United States","New York","NYC","300 Madison","33"
"10.1.5.100-10.1.5.250","","United States","New York","NYC","300 Madison","30"
"10.2.1.0/24","10.2.2.200-10.2.2.205","United States","North Carolina","RTP","Pinnacle 3005","5"
```

© 2026 Tanium Inc. All Rights Reserved

Import locations

CAUTION

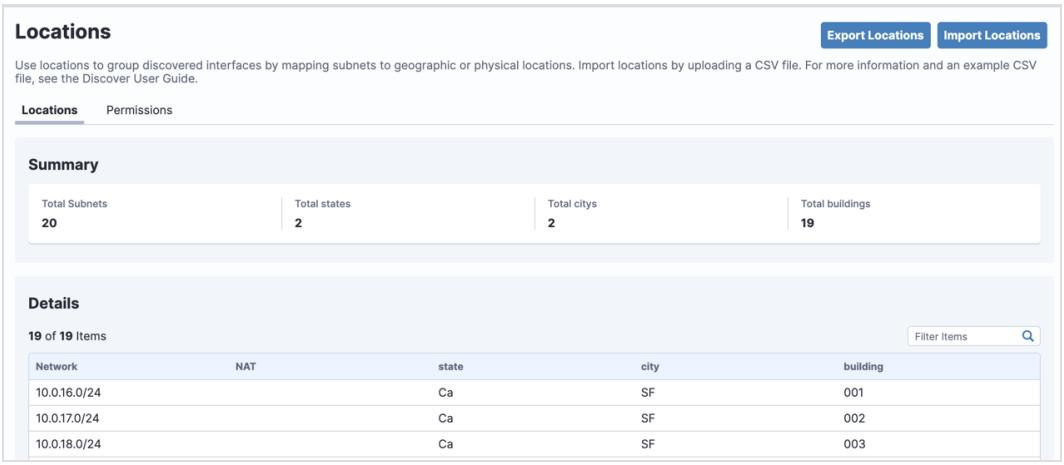
Each time you upload a CSV file that contains locations, any existing locations in Discover are removed and replaced with the hierarchy in the new file.

1. From the Main menu, go to **Modules > Discover > Locations**.
2. Click **Import Locations** and upload the CSV file you created. The location values are evaluated and applied to the interfaces list.

   TIP

   Make sure the CSV file matches the required formatting that appears on the **Import Locations** dialog. Additionally, any values in the CSV file that contain whitespace characters must be enclosed in double quotes ("). For example: `"123 Main St"`.

3. A list of locations is displayed on the **Locations** tab. You can search the locations as needed. To export a filtered CSV file based on the search results, click **Export Locations**.



Assign location permissions

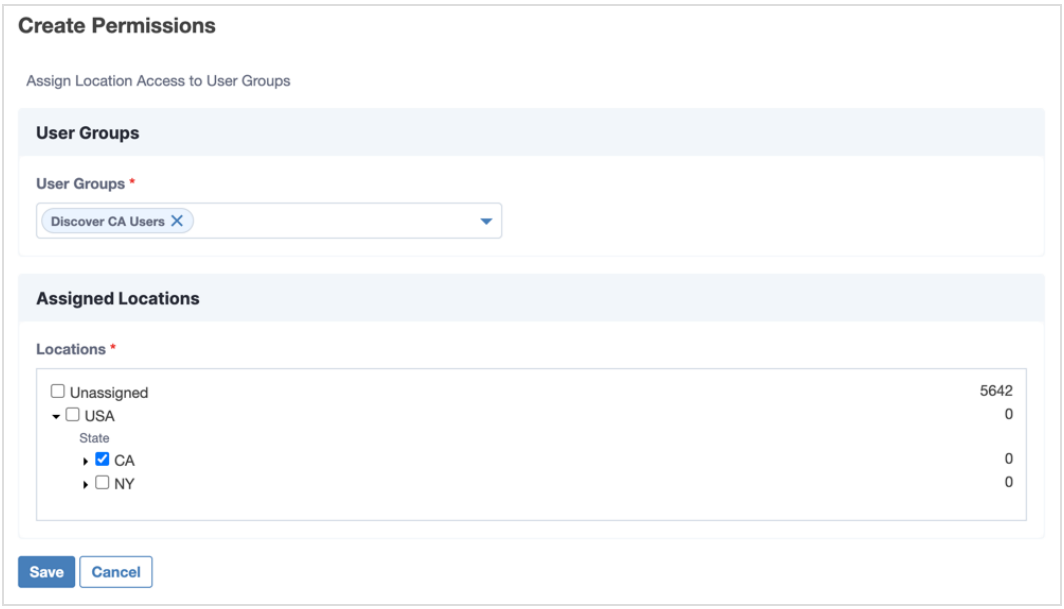
You can assign user group access to data in Discover based on location. When a user group is granted permission to a location, the users in that group can see only interfaces that are in the specified locations.

CAUTION

Before any locations are assigned permissions, all users can see all locations. After any permissions are assigned for locations, a user must be assigned location permissions to see interfaces. Tanium Administrator, Discover Administrator, and Discover Operator users can see all interfaces. If location permissions are defined, users with Discover User role can no longer create labels.

© 2026 Tanium Inc. All Rights Reserved

1. Create a user group that has access to the Discover module. For more information, see Tanium Console User Guide: Managing user groups.
2. From the Main menu, go to **Modules > Discover > Locations**, open the **Permissions** tab, and then click **Create Permission**.
3. Select user groups and associated locations. If a location has child locations, all the children are selected.

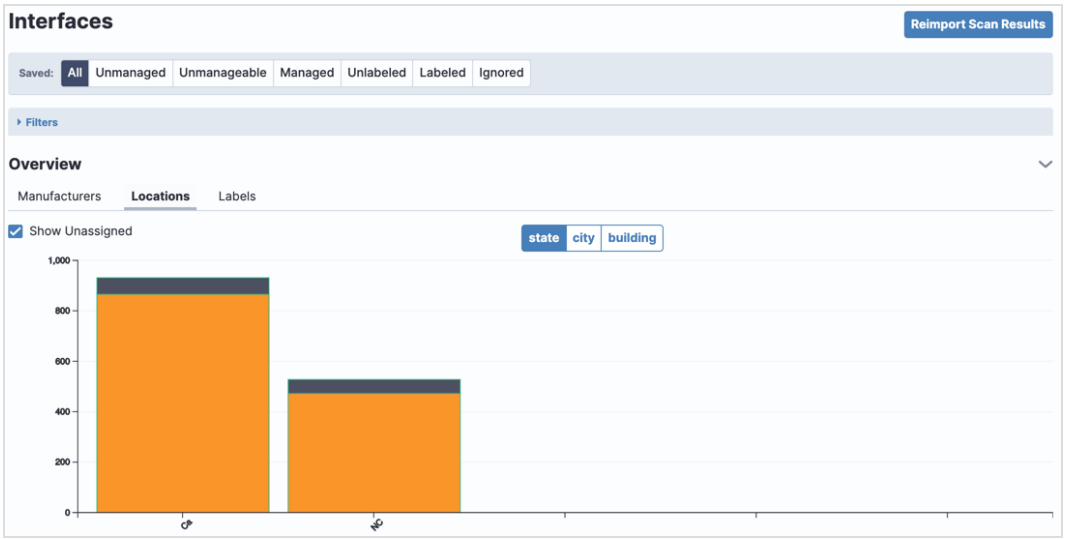


Click **Save**.

Location results

Locations are evaluated and applied to interfaces during the import process of a discovery scan. You can filter by location in the **Interfaces > Locations** chart.

Example Locations chart



© 2026 Tanium Inc. All Rights Reserved

The chart shows all interfaces regardless of assigned permissions, but the interfaces in the grid that follows the chart show only what is permitted for the user based on their assigned permissions.

Labels

Labels include descriptive information or metadata that you can use to identify and group interfaces. For example, labels let you group interfaces by attributes like device type, operating system, or business unit, making it easier to target specific interfaces for business processes and initiatives. You can also use labels to filter out interfaces that you do not want to manage to help maintain a clean and accurate interface inventory. For example, you can apply a label to ignore an interface to exclude it from views and lists, or you can purge it to remove it from Discover entirely. In addition, you can label interfaces that cannot run the Tanium Client as unmanageable, such as printers, IP phones, routers, and switches.

Types of labels

Tanium provides built-in labels and the Discovery Label Gallery so you can quickly get started applying labels to interfaces. These labels address many common use cases, but you can also create user-defined labels if you have custom requirements.

BUILT-IN LABELS

Discover provides the following built-in labels:

- Lost Interface: Any interface that was managed within the last 24 hours and was discovered in the last 4 hours
- New Managed Interface: A new interface in your environment that has the Tanium Client installed
- New Unmanaged Interface: A new interface in your environment that does not have the Tanium Client installed
- Promote Unmanaged Interface: Promotes the interface to Tanium™ Data Service (TDS) for use in other modules except in Tanium Reporting
- Purge Stale Interface: Purges any interface that has not been detected in seven days
- Unmanageable OS Platforms: An interface on a device that cannot run the Tanium Client, such as a router or printer

Discover uses these built-in labels to export events for Discover notifications through Tanium Direct Connect. If you delete any of these labels, Discover recreates them with their default definitions. For more information about sending event notifications, see Create connection for event notifications.

DISCOVER LABEL GALLERY LABELS

The Discover Label Gallery is a list of commonly defined labels and their definitions. You can use these labels to implement best practices, such as identifying common device types or maintaining your interface inventory. You can also edit these labels to adapt them to your environment. Each label has a link to its definition in JSON format that you can copy and import into Discover. For more information about importing labels, see Import labels on page 104.

For more information, see Discover Label Gallery.

USER-DEFINED LABELS

You can create your own labels and then import them for discovery scenarios that are not addressed by built-in or Discover Label Gallery labels.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

User-defined labels are included in exports for **Discover Label Notifications**. For more information, see Export interface data to a Connect destination on page 110.

Import labels

By default, Discover provides only built-in labels. You can import additional labels definitions in a JSON-formatted file so you can apply them to interfaces.

1. Create a JSON-formatted file that contains one or more label definitions that you want to import.

   BEST PRACTICE

   For best results, import labels from the Discover Label Gallery to address common use cases. You can also customize these labels to adapt them to your environment, or use them as templates for user-defined labels. The Discover Label Gallery is also available from Discover **Overview > Help**.

   After you locate the label collection that you want to download, right-click the link and select **Save Link As**. Save the file with a `.json` file extension. For example, `label.json`. For more information, see Labels for common use cases on page 107.

2. From the Menu menu, go to **Discover > Labels**, and click **Import Labels**.
3. Drag the JSON file into the **Import Labels** window, or browse the file system to upload your label file.
4. Click **Import**, then view which labels were created, and click **Close**.

Export labels

Export labels as a JSON file if you need to backup customized labels, share labels among environments, or preserve labels as you fine-tune their definitions.

1. From the Main Menu, go to **Modules > Discover > Labels**.
2. Select the labels that you want to export:
   - To export specific labels, click the checkbox on one or more label rows.
   - To export every label, click **Export All**.
3. Click **Export**.

View data in Tanium Trends

BEST PRACTICE

After you have well-defined labels, use the **Discover - Labels** board in Tanium Trends to view the current label count and the label count over time.

© 2026 Tanium Inc. All Rights Reserved

Automatically label interfaces

You can configure Discover to automatically apply a label to interfaces that match specified criteria. Each automatic label has two primary components: an activity and one or more conditions. When you create the automatic label, you select an activity that Discover performs on interfaces that match the conditions. Discover applies automatic labels to interfaces each time the Discover unmanaged interfaces operation runs.

ACTIVITIES

An activity is an action that Discover takes on an interface when it matches the label conditions. The activity determines whether the interface is kept, labeled, ignored, or removed. For example, you can select the **Purge** activity to remove from Discover any interface that matches a printer's MAC address.

LABEL CONDITIONS

A label condition is the set of criteria that determines when Discover automatically applies a label. For example, if you want to label interfaces on a specific subnet, you can create a condition that matches interfaces within an IP address range.

You create a label condition by defining a condition clause comprised of an attribute, operator, and value. A label can contain up to 900 conditions clauses. For more information about conditions and the information returned by each discovery method, see Reference: Data returned by profile type on page 133.

CONDITION OPERATORS

An operator defines how to compare the attribute to the value. Each operator has a positive form and a corresponding negative form. For example, there is a **contains** operator and a corresponding **does not contain** operator. Not every operator is supported for every attribute.



The **IP Address**, **Hostname**, and **Labels** attributes support matching on patterns and ranges. Regular expressions are not supported.

The following table describes operators that accept special value formats.

Condition operators

Operator	Description
equal to	An exact match, such as `192.168.1.195`.
has an address in the range	For **IP Address**, a range or CIDR block, such as `192.168.1.195-192.168.1.197` or `192.168.1.0/24`. If you enter starting and ending addresses, both addresses must use the same IP version, and you must order the addresses from low to high. For example, `fe80::-fe80:ffff:ffff:ffff:ffff:ffff:ffff:ffff` is a valid range.
matches pattern	Glob match that supports `*` (multiple characters) and `?` (single character), such as `192.168.1.???` matches IP that have three digits in the last octet. The pattern must match the entire value.

© 2026 Tanium Inc. All Rights Reserved

Condition operators (continued)

Operator	Description
contains	Partial match for a value.
has <value>	Match for at least one value.
is empty	No value present.

CONDITION WILDCARDS

You can use the underscore character (`_`) as a wildcard in a label condition to represent any number or literal character. For example, consider the following MAC addresses:

```
02-0F-B5-61-AB-01
02-0F-B5-38-1F-39
02-0F-B5-98-5B-69
02-0F-B5-55-0C-21
02-0F-B5-32-FA-E1
```

The condition `MAC contains B5-3_` matches the following MAC addresses:

```
02-0F-B5-38-1F-39
02-0F-B5-32-FA-E1
```

CREATE AN AUTOMATIC LABEL

1. From the Main menu, go to **Modules > Discover > Labels**, and click **Create Label**.
2. For **Type**, select **Automatic**.
3. In the **Activity** section, select an activity to apply to interfaces. For more information, see Activities.
   If you select **Promote**, Discover stores the unmanaged interface data in TDS for use in other modules. Only unmanaged interfaces can be promoted. If found during a network scan, the interface must also have a MAC address.Discover automatically applies the conditions required to promote an interface. You do not need to define additional conditions. For more information about Tanium Data Service, see Tanium™ Interact User Guide: Managing Tanium Data Service.
4. Add one or more conditions that determine which interfaces match the label. For more information, see Label conditions on page 105.
5. (Optional) Click **Calculate Applicable Interfaces** in the **Applicable Interfaces** section to verify matching interfaces.
6. Click **Create** .

Discover applies automatic labels to interfaces each time it imports results from the discovery methods.

© 2026 Tanium Inc. All Rights Reserved

Manually label interfaces

NOTE

You can manually label an interface with user-defined labels only. You cannot manually add an automatic label to an interface. Discover applies automatic labels based on label conditions only. For more information, see Automatically label interfaces on page 105.

CREATE A MANUAL LABEL

Create custom labels for discovery scenarios that are not addressed by built-in or Discover Label Gallery labels. You might need to manually apply a user-defined label if you determine how you want to manage an interface after it is imported into Discover.

1. From the Main menu, go to **Modules > Discover > Labels**, and click **Create Label**
2. Give the label a **Name**. For **Type**, select **Manual**, then click **Create**.
3. From the Main menu, go to **Modules > Discover > Interfaces** and select the row of one or more interfaces that you want to label.
4. Click **Add Label**, and select the label from the list.

REMOVE A MANUAL LABEL

Remove a manually applied label from an interface when it is no longer needed to manage or track the interface.

1. From the Main menu, go to **Modules > Discover > Interfaces**.
2. In the **Details** section, find the interface in the grid, and click Interface Details  to open a side panel that shows information about the interface.
3. Beside **Labels**, find the manually applied label that you want to remove, and click  to remove the label from the interface.

Best practices for labels

Implement effective labeling strategies keep your interface inventory accurate and to support business processes.

LABELS FOR COMMON USE CASES

Many environments share the same requirements for devices that are typically unmanageable or irrelevant. For example, you cannot manage devices like routers or printers that cannot run the Tanium Client, and you do not want to track inactive devices in your interface inventory. To address these common use cases, Tanium provides **Collection of Labels for New Deployment or POC** in the Discover Label Gallery.

This collection include the following labels:

© 2026 Tanium Inc. All Rights Reserved

- **D99_Common_Unmanageable_by_Manufacturer_<*data-id*>**: These labels use manufacturer names to identify traditionally unmanageable interfaces and marks them as unmanageable.
- **D55_Managed_Systems_Disconnected_Interfaces**: This label ignores interfaces that are not in use by your managed endpoints.
- **M02_Purge old Interfaces**: This label purges interfaces that have not been seen for 30 days so you do not manage ephemeral or inactive devices.

  If you installed Discover for the first time with version 4.4 and used the Tanium Recommended Installation workflow, you also have the more aggressive **Purge Stale Interface** label. This label is configured to purge interfaces that have not been detected in seven days.

For more information, see Discover Label Gallery labels on page 103.

CREATE A CONNECT JOB FOR LOST INTERFACES

You can use the built-in **Lost Interface** label to create a Connect job that notifies you whenever a managed interface stops communicating with Tanium. A lost interface is any interface that was managed within the last 24 hours but is currently unmanaged. Typically, this occurs because the Tanium Client was uninstalled, or it is not registering with the Tanium Server. You should investigate lost interfaces to determine the cause of the communication issue.

You can send Connect notifications to event destinations such as email, SIEM, or Splunk. For more information about creating a Connect job for lost interfaces, see Create connection for event notifications.

APPLY LABELS BY LOCATION

Labels are applied globally across all interfaces and do not respect location permissions. To help organize your interfaces by location, you should apply labels to all interfaces that are associated with that location. For example, you can create a Boston label and apply it to all interfaces discovered in the Boston location.

Applying labels by location provides the following benefits:

- Users can filter and view interfaces associated with their location.
- Users apply labels only to interfaces allowed through their location permissions.
- You can implement location-based workflows with labels. For example, you can create a connect job for lost interfaces for each location, and you can create location-specific Tanium Client Management deployments. For more information about Connect jobs, see Create a Connect job for lost interfaces on page 108. For more information about deploying the Tanium Client with labels, see Endpoint onboarding on page 109.

To label interfaces by location, you must configure location permissions and create an automatic label with a condition that references the location. The following steps provide a high-level overview of the process.

1. Create location permissions that associate one or more user groups with a location. For more information, see Assign location permissions.
2. Create an automatic label that includes the condition: `Location has a location within location-value`. For more information about creating automatic labels, see Automatically label interfaces on page 105.

© 2026 Tanium Inc. All Rights Reserved

For more information about locations, see Locations on page 99.

ENDPOINT ONBOARDING

Endpoint onboarding is the process of installing the Tanium Client on unmanaged endpoints. Labels can help you identify endpoints that you want to bring under Tanium control. You can create a label and use that label as a deployment target to deploy the Tanium Client to unmanaged interfaces. For example, you can apply a label to all interfaces in the network for a new office location and then configure a satellite to deploy the Tanium Client on interfaces with that label.

For more information about using Discover labels to deploy the Tanium Client, see Tanium™ Client Management User Guide: Deploying the Tanium Client using Client Management.

© 2026 Tanium Inc. All Rights Reserved

Exporting Discover data

You can export interface and event information from Discover to Tanium™ Connect.

The preferred method for exporting data is to use the Discover data source in Connect. For more information, see Export interface data to a Connect destination on page 110.

NOTE

Discover exports dates in ISO 8601 format (`yyyy-MM-ddTHH:mm:ss.SSS`), set to Coordinated Universal Time (UTC). For example, `2025-08-22T13:05:12.789Z`.

Export to a CSV file

To export the current data grid of interfaces to a CSV file, click Export Data. The export includes the data that currently appears in the data grid.

The **Unmanageable** column in the CSV file indicates if the endpoint can be managed by the Tanium Client. The following table explains the numbers in the **Unmanageable** column.

Possible values for the Unmanageable column

Number	Label
0	Managed or Manageable (automatic)
1	Unmanageable (automatic)
2	Manually Marked Manageable
3	Manually Marked Unmanageable

Export interface data to a Connect destination

To create reports of the interfaces in Discover to Connect destinations such as Email, File, HTTP, Socket Receiver, Splunk, and SQL Server, create a connection. You must have Connect 4.10 or later.

You can export interfaces with the following reports:

All

Exports all interfaces in Discover.

Ignored

Exports interfaces marked as ignored. This list is also on the **Ignored Interfaces** page.

© 2026 Tanium Inc. All Rights Reserved

Labeled

Exports all interfaces that have a label applied, including configured automatic labels.

Managed

Exports interfaces that have the Tanium Client installed.

Unlabeled

Exports interfaces that do not have any labels applied.

Unmanageable

Exports interfaces that were marked as unmanageable.

Unmanaged

Exports interfaces that do not have the Tanium Client installed.

Connections to create



Create the following connections to track possible network issues, Tanium Client installations, and hard to inventory devices.

Connections to create for Discover in Tanium Connect

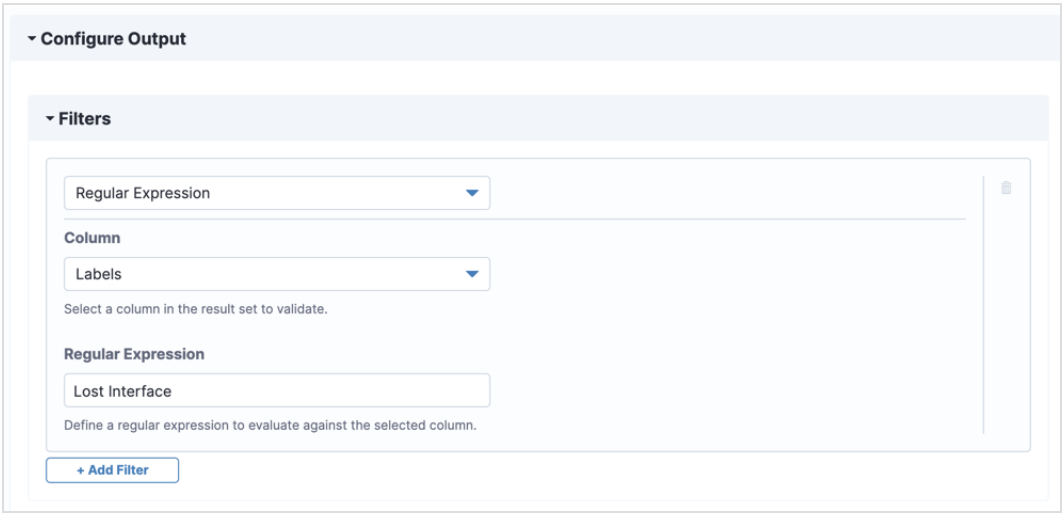
Purpose	Source Type	Select	Destination
Alert on clients that are no longer reporting to Tanium, which might identify network issues	**Event > Discover notifications**	**Lost Interface**	SIEM, helpdesk or email alerting
Generate executive rollup of interface status for multiple Tanium installations	**Tanium Discover**	**Managed, Unmanaged**	Reporting tool
Classify hard to inventory devices (IP Telephony, printers, security cameras, Internet of Things devices)	**Tanium Discover**	**Unmanageable**	Reporting tool

Create connection to export interfaces

1. Create the connection.
   a. From the Main menu, go to **Modules > Connect > Connections**. Click **Create Connection**.
   b. Name the connection.
2. In the Source section, select the **Tanium Discover** source. Select the report that you want to use.

© 2026 Tanium Inc. All Rights Reserved

3. Select a destination.
4. Apply filters. You might want to apply a filter if you are trying to export a specific label.



   For example, if you want to export all interfaces that are tagged with Lost Interface, apply a regular expression filter and type `Lost Interface` as the text to match on the **Labels** target column.
5. Choose format settings and schedule.
6. Click **Save**.

Create connection for event notifications

You can send data notifications about Discover events to destinations such as email, SIEM, or Splunk. To configure notifications, create a connection with Connect. The following Discover event groups are available for configuring notifications:

- **Discover Label Notifications**
    - Configure a notification based on a selected set of automatic notify labels. You can choose to create notifications for a single label or a group of labels. You must have custom notify labels defined to use this option.
- **Discover Notifications**
    - **All labels**: Create notifications for all configured automatic notify labels.
    - **New unmanaged interface**: Discover found a new unmanaged interface in your environment. This behavior is controlled by the pre-configured New Unmanaged Interface label.
    - **New managed interface**: Discover found a new managed endpoint in your environment. This behavior is controlled by the pre-configured New Managed Interface label.

© 2026 Tanium Inc. All Rights Reserved

- **Lost interface**: Discover found an unmanaged interface that was formerly managed. For an interface to be marked as lost, it must:
  - Not show up in the **Managed Interfaces** page for one day
  - Have a value in the **Last Discovered** column
  - Show up as an unmanaged interface as a result of active discovery methods in the last 4 hours (Nmap scan, connections, or simple ping script)

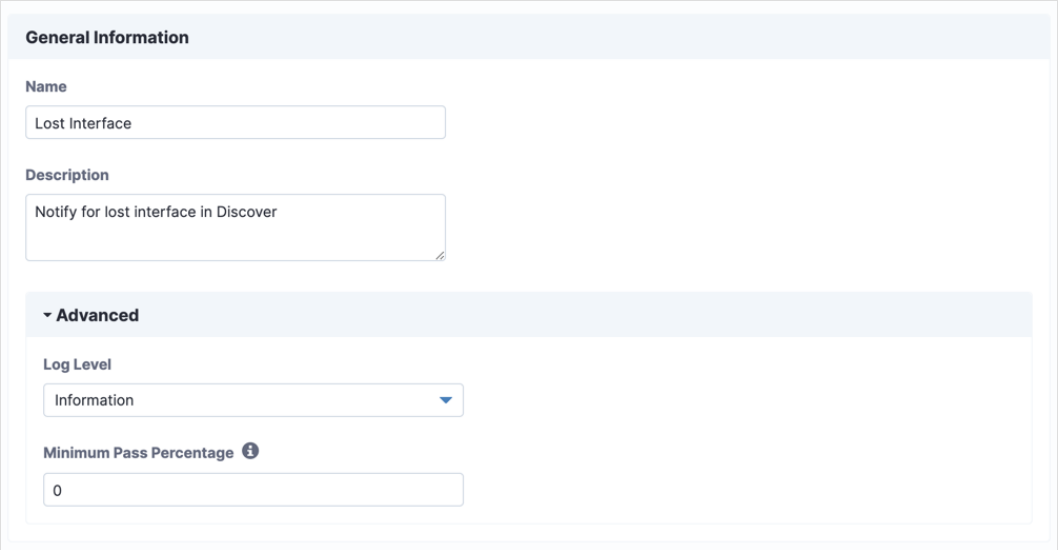
  This behavior is controlled by the pre-configured Lost Interface label. To update the conditions that determine a lost interface, change the default settings for the Lost Interface label.

Prerequisites

- You must have Connect installed. For more information, see Tanium Connect User Guide: Installing Tanium Connect.
- You must have the **Connect User** role to create a connection. For more information about how to configure user roles, see Tanium Core Platform User Guide: Manage role assignments for a user.
- Verify that the automatic labels that you want to use for the notifications are configured to generate a notify activity and provide the correct data. For more information about automatic labels, see Managing interfaces on page 96.

Configure notifications in Connect

1. Create the connection.
   a. From the Main menu, go to **Modules > Connect > Connections**. Click **Create Connection**.
   b. Name the connection.



© 2026 Tanium Inc. All Rights Reserved

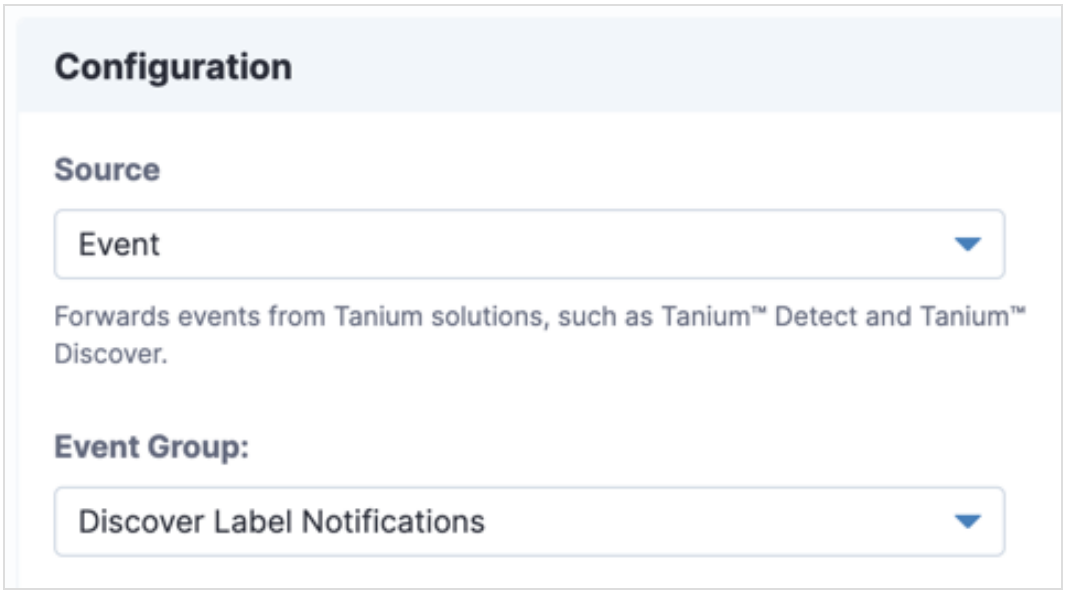
2. Configure the data source.

    a. In **Source**, select the **Event** source.

    b. Select **Discover Notifications** and choose the event group that you want to use.

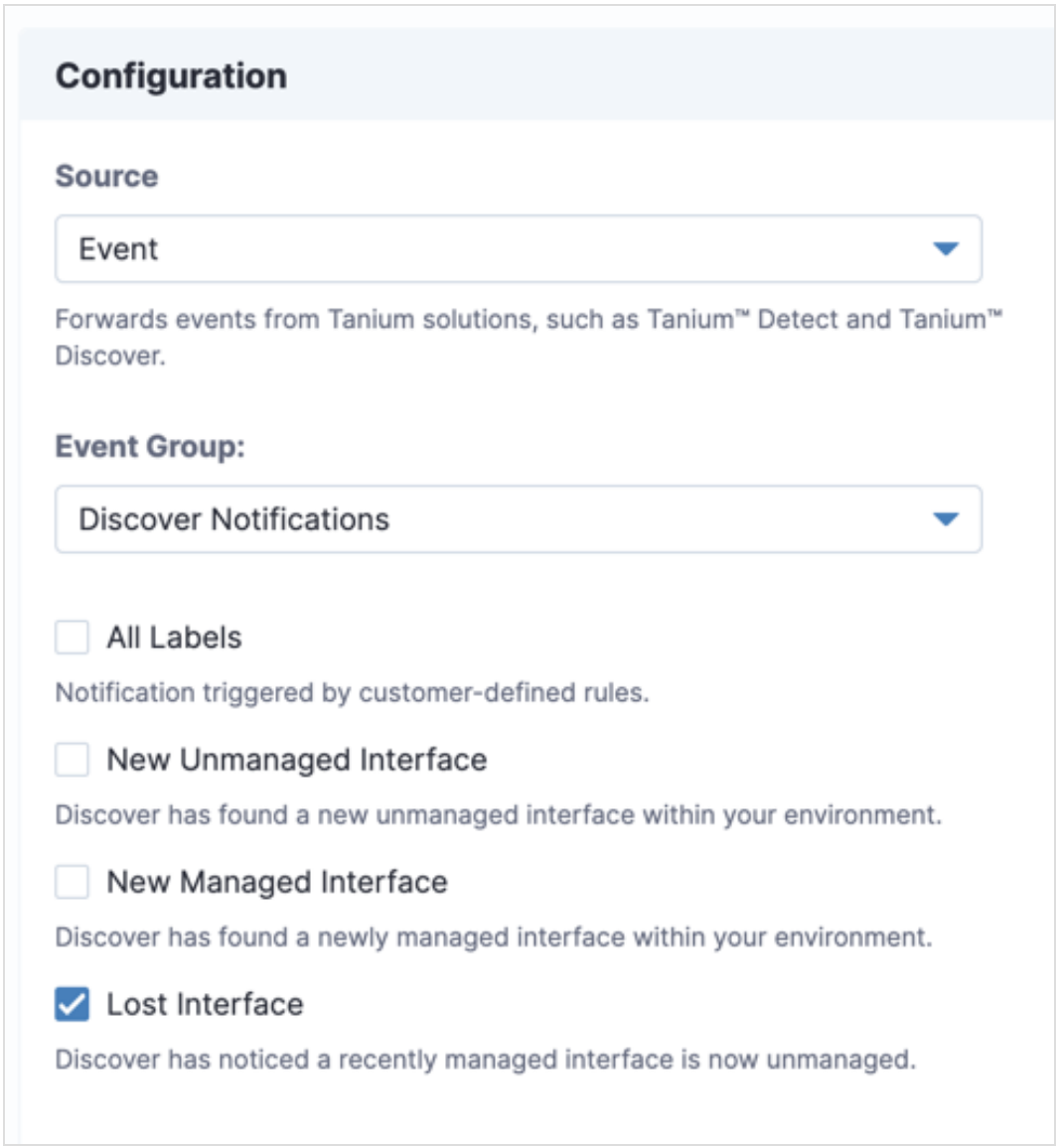
        - For the **Discover Label Notifications** event group, select the labels for which you want to send notifications. Label notifications are available for labels that you add, not for the predefined labels. If you do not have user-defined labels, you do not see the Discover Label Notification event group.

© 2026 Tanium Inc. All Rights Reserved



© 2026 Tanium Inc. All Rights Reserved

- For the **Discover Notifications** event group, select one or more Discover events for which to send notifications.



3. (Optional) Filter the data. You can optionally filter for new items, regular expressions, numeric operators, or unique values from data columns.
4. Configure the connection destination. Select any of the connection destinations that are listed in the **Select Destination** menu. Common choices for notifications include Email, SIEM, and Splunk. However, you can use any of the available destinations. For more information, see Tanium Connect User Guide.
5. Complete the required fields and click **Create Connection**.

© 2026 Tanium Inc. All Rights Reserved

Maintaining Discover

Perform monthly maintenance tasks to ensure that Discover successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Discover is not performing as expected, you might need to troubleshoot issues or change settings. For more information about how to view related procedures, see Troubleshooting Discover on page 121.

Review and remediate Discover resource usage on the Module Server

1. From the Main menu, go to **Modules > Trends > Boards**.
2. Click the **Discover - Module Health** board and review the panels for resource usage issues.
3. For more information about how to troubleshoot resource usage issues, see Troubleshooting Discover on page 121.

Review and update discovery methods

1. From the Main menu, go to **Modules > Discover > Profiles**.
   The **Profiles** page opens.
2. Review the **Status** of the profiles for warnings or errors. These conditions are the result of a profile mismatch between the Tanium Server and the Tanium Client.
3. Contact Tanium Support on page 131 if necessary to resolve any warning or error conditions.
4. Review profile configurations to verify that their discovery methods are optimal. For example:
   - Verify that scanning excludes virtual private network (VPN) connections. Clients that connect over a VPN are typically isolated leaders that do not peer with each other. For more information, see Tanium Client Management User Guide: Verify or remediate Tanium Client peering and leader connections.
   - Review unmanaged endpoints to determine if they are eligible for the Tanium Client. For more information, see View interface data on page 96.
5. Troubleshoot discovery issues if necessary. For more information, see Troubleshooting Discover on page 121.
6. Edit profiles if necessary to resolve discovery issues: go to the **Profiles** page, click the profile **Name** and reconfigure the settings. For detailed steps, see:
   - Configure profile for distributed scan on page 69
   - Configure profile for satellite scan on page 78
   - Configure profile for centralized Nmap scan on page 85
7. Delete or disable profiles that are no longer useful.
   - **Delete profiles**: From the **Profiles** page, select the profiles and click **Delete Profile**.
   - **Disable profiles**: From the **Profiles** page, select the profiles and click **Disable Profile**. Alternatively, to disable a single profile, in the **Action** column of the profile that you want to disable, click Action and select **Disable Profile**.

© 2026 Tanium Inc. All Rights Reserved

Monitor and troubleshoot endpoints managed

The following table lists contributing factors into why the **Endpoints Managed (%)** metric might be lower than expected, and corrective actions you can make.

Factors that contribute to a lower-than-expected Endpoints Managed metric

Contributing factor	Corrective action

Installation Method Gap	• Use existing tools that are already part of the infrastructure.
	• Use standard tools (might only cover a subset of potential systems in your environment) such as:
	  ◦ SCCM - easy deployment mechanism (Windows only)
	  ◦ Group Policy - with the correct setting can deploy Tanium Client (Windows only)
	  ◦ Salt - a common tool used for installation of software in any environment (cross-platform)
	• Use a Tanium-provided installation method such as Tanium Client Management.

Credential Gaps	Use of any of the Tanium-provided installation methods involves using credentials to access the systems. Work with various management teams and deployment teams to understand what credentials are available to do installations on systems. Work with server or workstation support teams to understand these areas.
Network Gaps	Installing clients on "protected" networks such as DMZs or other sensitive areas is often a problem. These issues are technical, but the technical hurdles are generally an issue with policies and permissions. Work with the correct stakeholders to understand how Tanium will be used in the environment. Negotiate restrictions to be lessened to allow installation of Tanium Clients in these protected networks.

Monitor and troubleshoot mean time to manage

The following table lists contributing factors into why the **Mean Time to Managed** metric might be higher than expected, and corrective actions you can make.

Factors that contribute to a higher-than-expected Mean Time to Managed metric

Contributing factor	Corrective action
No automation	Tanium Discover can find clients, but with no action, a project can stall. Automating installation with Discover labels to target installation with Tanium Client Management is key. Take the human interaction out when possible, or build a workflow around Discover labels when items are found to feed into Tanium Connect and create help desk tickets or simple email lists.

© 2026 Tanium Inc. All Rights Reserved

Factors that contribute to a higher-than-expected Mean Time to Managed metric (continued)

Contributing factor	Corrective action
Non-optimized Discover settings	• Adjust configuration settings. The key elements are how often to scan, and how often to import data. The Discover scans are built to be “low impact” on any network environment. Recommended scanning is once an hour in most environments. Scanning once an hour causes near zero impact and is fast enough to take action on unmanaged interfaces. Recommended importing is every thirty minutes and causes near zero impact to an environment. • Exclude scanning in parts of the network where you do not need scanning. To be successful in any enterprise, exceptions are always required. Discover has fine-grained control so you can exclude what you do not want to scan. For more information, see Knowledge Article: Getting Surgical with Endpoint Discovery: Using Targeting and Exclusions in Tanium Discover. • Select a discovery method that provides OS details. If installation requirements are governed by operating system (such as different teams are responsible for installation on different operating systems), selecting the right discovery method is key. Nmap with OS Fingerprinting (level 4 distributed scan, or centralized scans) are required to effectively understand the operating system. Level 2 ping scans can provide OS in some but not all cases. • Use Discover Labels to make better sense of your environment, so you can bring items under management. Use the Tanium label gallery to import common labels to help determine manageability of existing interfaces. For more information, see Knowledge Article: Discover Labels - Common labels available for import • Best practices ◦ Tanium Community discussion: How do I configure Tanium Discover so that home networks are not scanned? ◦ Tanium Community discussion: Visibility of discovered assets - Removing Devices from view ◦ Tanium Community discussion: Visibility of discovered assets - Finding likely manageable resources ◦ Tanium Community discussion: I see assets in my Tanium Discover data that are no longer online, how do I keep my Tanium Discover database clean?
Regional Ownership	Often various regions have different support structures in the larger enterprise. Understanding what systems belong to these regions is key to providing the guidance to the owning team they need to help install. Use locations to export or visualize data. For more information, see this three-part article: • Knowledge Article: Add a new dimension to your endpoint data with locations - Part 1 • Knowledge Article: Add a new dimension to your endpoint data with locations - Part 2 • Knowledge Article: Add a new dimension to your endpoint data with locations - Part 3

© 2026 Tanium Inc. All Rights Reserved

Factors that contribute to a higher-than-expected Mean Time to Managed metric (continued)

Contributing factor	Corrective action
Understand your environment	Proper deployment sometimes requires understanding what is working and what is not working. With the data grids and graphs in Discover, you have a real-time view the environment. With a high level view over time, you can understand how deployments are working and cross-pollinate various ideas that work across a larger group. To get a high level view, use the Discover boards in Tanium Trends. For more information, see Tanium Community article: Use Trends to visualize Discover interfaces over time.

© 2026 Tanium Inc. All Rights Reserved

Troubleshooting Discover

If Discover is not performing as expected, you might need to troubleshoot issues or change some settings. To send information to Tanium for troubleshooting, collect log and other relevant information.

Collect logs

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

To download logs, complete the following steps:

1. From the Discover **Overview** page, click Help .
2. From the **Troubleshooting** tab, select the solutions for which to gather troubleshooting packages and click **Create packages**. By default, all solutions are selected.
3. When the packages are ready, click **Download Support Bundle**. ZIP files of all the selected packages download to the local download directory.

   Some browsers might block multiple downloads by default. Make sure to configure your browser to permit multiple downloads from Tanium Console.
4. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 131.

Discover maintains logging information in the `discover.log` file in the `<Module Server>/services/discover-service-files/discover.log` directory.

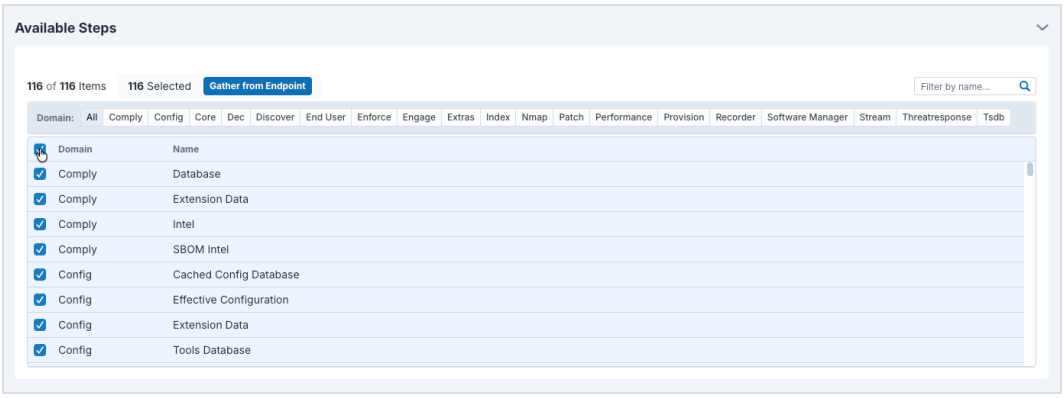
Collect troubleshooting information from endpoints

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 **Direct Connect** search box, enter all or part of an IP address or a computer name.
   Matching results appear after the search completes.
4. From the search results, click the computer name to connect to the endpoint.

© 2026 Tanium Inc. All Rights Reserved

5. Click the **Gather** tab. For the **Domain** filter, select the domain and category names for which you want to gather troubleshooting information. You can optionally filter the category list by domain, and you can select the check box in the header row to toggle the selection of all categories in the current filter.



6. 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.

7. 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 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.

Verify endpoint tools

If you are experiencing issues such as a feature not working on an endpoint or seeing incorrect data in the workbench, confirm that your endpoints have the latest toolset version. For more information, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client Extensions. For more information about Discover tools, see Reference: Discover endpoint tools on page 132.

Identify and resolve issues with Client Extensions

Use the following steps to troubleshoot issues with the Client Extensions that Discover installs and uses. During troubleshooting, consider environmental factors such as security exclusions, file locks, CPU usage, RAM usage, and disk failures.

For more information about the Client Extensions that Discover installs and uses, see Client Extensions.

© 2026 Tanium Inc. All Rights Reserved

1. If endpoints have Client Extension shared process mode enabled and you need to troubleshoot resource usage or crashes in the combined `TaniumCX.exe` or `TaniumCX` process, disable shared process mode on the affected endpoints, and then reproduce the issue if possible. For more information, see Endpoint Configuration User Guide: Manage Client Extension shared process mode.

2. To review the health of Client Extensions or to start an investigation into an existing error, ask a question using the `Client Extensions - Status` sensor.

   The results of these questions help to identify endpoints with errors and provide a starting point to deploy actions that might help correct the issue. Filter the results and drill down as necessary to investigate results that indicate errors.

   Consider whether endpoints with errors share common characteristics, such as operating system, domain or organization unit, or the antivirus software that is installed.

3. Target one or more endpoints with errors, and uninstall tools that report errors without blocking reinstallation. For more information, see Remove Discover tools from endpoints and Endpoint Configuration User Guide: Uninstall a tool installed by Endpoint Configuration.

   When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

   Wait for automatic reinstallation of the tool. If the reinstallation does not resolve the issue, continue to the next step.

4. Ask a question using the `Endpoint Configuration - Tools Status Details` sensor, and include filters to limit the results to the tool that you are investigating. For example:

   `Get Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains Discover from all machines with Endpoint Configuration - Tools Status:Tool Name contains Discover`

   Review the columns in the results for specific information about errors. The following table provides guidance for some common error conditions:

© 2026 Tanium Inc. All Rights Reserved

Potential errors returned by the Ednpoint Configuration - Tools Status Details sensor

Error Condition	Possible Resolution
No error appears, but an available new version has not been installed	Review the **Targeted Version** column to make sure that the endpoint has received the latest manifest. If the targeted version does not yet show the updated version, the Endpoint Configuration manifest has not updated on the endpoint, usually for one of the following reasons: • The manifest update is still pending. Either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest. • Action lock is enabled on the endpoint. Follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest to identify endpoints with action lock turned on. • Discover is no longer installed, or it is no longer targeting the endpoint. In some cases, Discover might stop targeting an endpoint because it no longer needs the endpoint for a particular workload. For example, if an endpoint is being used in a level 4 distributed scan, and peer endpoints appear with adjacent IP addresses, Discover no longer needs the original endpoint for the level 4 scan and no longer targets it. Consider whether Discover should still target the endpoint: ◦ If it is expected or intentional that Discover no longer targets the endpoint, you can optionally uninstall Discover tools and dependencies. For more information, see Remove Discover tools from endpoints. ◦ If Discover should still target the endpoint, make sure that the Discover action group includes the endpoint, and make sure Discover targets the endpoint in any expected configurations or profiles. Then, either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest.
Installation Blocker:`Unmet Dependencies: [Tool name]`	If no **Failure Message** or **Failure Step** appears, the endpoint might be waiting for the dependencies to install. Wait to see if the condition resolves on its own. If this condition remains for an extended period, ask the question again and review any error information in other columns, especially the **Failing Dependency** column.
Failing Dependency: *[Tool name]*	Ask the question: `Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains [Tool name] from all machines with Endpoint Configuration - Tools Status:Tool Name contains [Tool name]` Investigate further errors with the tool. If the dependency has not been installed on an endpoint, ask the question: `Get Endpoint Configuration - Tools Retry Status from all machines with Computer Name equals Computer_Name` to review the retry status for the tool installation. For more information, see Endpoint Configuration User Guide: Review tool installations that are scheduled for a retry.
Manually Blocked:`blocked`	The tool was previously blocked, either manually or during a previous uninstallation. Unblock the tool. For more information, see Endpoint Configuration User Guide: Block or unblock tools from installing on an endpoint.

5. Review the Extensions logs on the endpoint. Take note of entries that include `fail` or `error`. For more information, see Review the Extensions log for an endpoint on page 125.

© 2026 Tanium Inc. All Rights Reserved

For additional help, collect all logs for Tanium Discover, and contact Tanium Support.

Review the Extensions log for an endpoint

Use Client Management to directly connect to an endpoint and view and download extension logs.

1. From the Main menu, go to **Shared Services > Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Direct Connect** search box, enter all or part of an IP address or a computer name.
   Matching results are displayed after the search completes.
4. From the search results, click the computer name to connect to the endpoint.
5. Click the **Logs** tab, and select an **extensions*[#]*.log** file.
6. (Optional) To download the log, click **Download**.

For additional help, collect all logs for Tanium Discover, and contact Tanium Support.

View Discover scan ranges

You might want to see the ranges that are scanned before you run discovery, or to troubleshoot discovery that has already run. To see the calculated gaps between the managed interfaces, use the **Discover Scan Range** and **Discover Scan Range - Unix** sensors. The **Discover Scan Range - Unix** sensor is for the Solaris and AIX platforms.

For example, you might use the question: `Get Computer Name and Operating System and Tanium Client IP Address and Discover Scan Range and Discover Scan Range - Unix from all machines`. The results contain the range between each of the managed endpoints and its forward and backward peers.

Problem: No results from running a scan

To return results, Discover tools must be distributed to the endpoints. If you do not see results:

- Check the configuration of the Discover action group. For more information, see Installing Discover on page 58.
- Check the status of the Discover action group. From the Main menu, go to **Administration > Actions > Scheduled Actions**.

Problem: Some endpoints are not scanning

You might find that some endpoints are not scanning. For example, the question: `Get Discover Last Scan Range from all machines` returns `[no results]`.

Try adjusting the **Start at** time of the scheduled action to a few minutes after the **Opening Time** of the configured scan window in the profile.

© 2026 Tanium Inc. All Rights Reserved

1. Get the start time of the start window for your profile. From the Main menu, go to **Modules > Discover > Profiles**. Hover over the *profile_name* and click Edit . In the **Scan Window** section, note the value of the **Opening Time** setting.
2. From the Main menu, go to **Console > Actions > Scheduled Actions**. Click the **Tanium Discover** action group.
3. Select the scheduled action that is associated with the profile. Choose **Discover Content - Execute Scan [*profile_name*]** or **Discover Content - Execute Scan for non-Windows [*profile_name*]**. Click **Edit**.
4. Edit the **Start at** time to start a few minutes after the **Opening Time** you found in your profile.



Discover cannot perform satellite or distributed scans on endpoints with actions locks turned on. For more information, see Tanium Console User Guide: Managing action locks.

Problem: Satellite profile appears in ERRORED state

Symptom

When you view the **Profiles** page, a satellite profile appears with a status of **Needs Deployment**. When you expand the profile, the **Status Details** contains **ERRORED**.

Cause

Reasons why a profile appears in ERRORED state include the following:

- Tanium Direct Connect is not installed.
- The satellite in the profile is not available.
- The profile publish was interrupted.
- The profile targets more than 4,096 IP addresses.

Solution

Discover automatically tries to republish ERRORED profiles at regular intervals. After you resolve the underlying issue for an ERRORED profile, wait until Discover republishes the profile.

1. If all satellite profiles are in ERRORED state, verify Direct Connect is installed.
    a. From the Main menu, go to **Administration > Configuration > Solutions**.
    b. Navigate the **Content** section and use the filter to find `Direct Connect`.
    c. Verify that a version appears in the **Imported Version** column. If the **Imported Version** column is empty, install Direct Connect. For more information, see Tanium Direct Connect User Guide: Installing Direct Connect.

© 2026 Tanium Inc. All Rights Reserved

2. Make sure the satellite defined in the profile is available.
    a. From the Main menu, go to **Modules > Discover > Profiles**.
    b. Click the name of the profile to open the **Edit Profile** page.
    c. In the **Satellites** section, verify that one satellite is selected, and that the **Status** for the selected satellite is **Online**.
        - If a satellite is selected is online, continue to step 3.
        - If no satellite is selected, select another satellite and then click **Save**.
        - If the selected satellite is **Offline**, select another satellite and then click **Save**. Alternatively, you can investigate why the currently selected satellite is offline.
        - If necessary, edit the list of available satellites in Direct Connect. For more information about how to configure satellites, see Tanium Direct Connect User Guide: Managing satellites.
    d. If you made changes to the profile, click **Save**.
    The **Profiles** page opens and a notification appears if the profile saved successfully.
    e. Wait a few minutes and then refresh the **Profiles** page. If the profile publishes successfully, the status changes to Published or Scan Completed.
3. Edit the profile and make sure the combined total of any networks selected in the **Scan Inclusions** targets 4,096 IP addresses or less. If necessary, remove networks or add scan exclusions to reduce the number of targeted IP addresses. For more information, see Configure profile for satellite scan on page 78.
4. If Direct Connect is installed, the satellite in the profile is online and available, and the profile targets 4,096 IP addresses or less, it is possible that an interruption occurred when Discover attempted to publish the profile. In this situation, you can either re-save the profile to force Discover to publish the profile, or wait until Discover automatically publishes the profile.
    a. From the Main menu, go to **Modules > Discover > Profiles**.
    b. Click the name of the profile to open the **Edit Profile** page.
    c. Click **Save**.
    The **Profiles** page opens and a notification appears if the profile saved successfully.
    d. Wait a few minutes and then refresh the **Profiles** page. If the profile publishes successfully, the status changes to Published or Scan Completed.

Problem: Error with locations CSV file

If you see `Error: Network specified for a parent. Networks can only be specified at the lowest level of the hierarchy.` in the workbench and are unable to import the locations file, confirm that each row in the CSV file specifies a unique location in the hierarchy.

For example, consider the following CSV file:

Example locations CSV file

© 2026 Tanium Inc. All Rights Reserved



```
1  network,nat,country,state,city,building,floor
2  10.70.0.0/24,,"United States",Michigan
3  10.70.1.0/24,,"United States",Ohio
4  10.70.2.0/24,,"United States",North Carolina
5  10.70.3.0/24,,"United States",California,Oakland,201,1
6  10.70.4.0/24,,Mexico,Oaxaca
7  10.70.5.0/24,,Canada,Ontario,Toronto
8  10.70.6.0/24,,France
9  10.70.7.0/24,,Poland
10 10.70.8.0/24,,Italy
11 10.70.9.0/24,,Germany,Berlin
12 10.70.10.0/24,,Germany,Baveria
13 10.70.11.0/24,,Germany
14 10.70.12.0/24,,Germany,Hesse
```

Think of the hierarchy specified in the CSV file as a tree, and each row is a branch. Line 1 creates a United States branch with a sub-branch for Michigan. Line 8 creates a France branch. Line 11 creates a branch for Germany and a sub-branch for Berlin.

Line 13 creates the error because it does not end in a unique place in the hierarchy. Line 11 creates the Germany branch and line 13 only specifies Germany. Line 13 ends in a location that is already created. If line 13 specified another German state, like line 14 does, then line 13 would not create an error.

Problem: Needs deployment profile status

This warning indicates there is a profile mismatch between the Tanium Server and the Tanium Client. Contact support for assistance.

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

For more information about how to submit a support case, see Case Submission Form.

FAQ: Why is the number of managed interfaces higher than the client status?

If you compare the number of managed interfaces in Discover, you might notice that the number is often higher than the number of Tanium Clients that are reported on the Client Status page.

This disparity is expected. Interfaces are unique MAC addresses. One Tanium Client with multiple network interface controllers (NICs) displays as multiple interfaces in Discover. Virtualization software can increase the number of interfaces reported for a computer, if the computer has multiple virtual machines running.

You can also view the Environment Status section in Tanium Console to view the discrepancy between the number of managed interfaces and the Total Endpoints.

Remove Npcap from endpoints

You can deploy an action to remove Npcap from an endpoint or computer group.

© 2026 Tanium Inc. All Rights Reserved

1. In Interact, target the computers from which you want to remove Npcap.
    - For computers with Npcap installed using Discover 4.3 or later, ask a targeting question:
      `Get Endpoint Configuration - Tools Status from all machines with Is Windows equals True`
    - For all other computers with Npcap installed or if you are not sure how Npcap was installed, ask a targeting question:
      `Get Discover - Installed Npcap Version from all machines`
2. In the results, select **Npcap** (if using the Endpoint Configuration package) or the versions (if using the Discover package), and select the targets from which you want to remove Npcap. For more information, see Tanium Interact User Guide: Managing question results in Interact.
3. Click **Deploy Action**.
4. On the **Deploy Action** page, select the package:
    - If using the Endpoint Configuration package, do the following:
        a. Enter `Endpoint Configuration - Uninstall` in the **Deployment Package** box, and select **Endpoint Configuration - Uninstall Tool [Windows]**.
        b. For **Tool Name**, select **Npcap**.
        c. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.
    - If using the Discover package, do the following:
        a. Enter `Discover - Uninstall Npcap` in the **Deployment Package** box.
        b. (Optional) By default, the package only uninstalls Tanium-installed versions of Npcap. To uninstall all installations of Npcap, select **Remove Any Npcap Version**.
5. Click **Show preview to continue**.
6. A results grid appears at the bottom of the page to show the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

Remove Discover tools from endpoints

You can deploy an action to remove Discover tools from an endpoint or computer group. Separate actions are available for Windows and non-Windows endpoints.

1. In Interact, target the endpoints from which you want to remove the tools. For example, ask a question that targets a specific operating system:
   `Get Endpoint Configuration - Tools Status from all machines with Is Windows equals true`
2. In the results, select the row for , drill down as necessary, and select the targets from which you want to remove Discover tools. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
5. For **Tool Name**, select .

© 2026 Tanium Inc. All Rights Reserved

6. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.

   NOTE

   If reinstallation is blocked, you must unblock it manually:

   - To allow Discover to reinstall tools, deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints).
   - If you reinstall tools manually, select **Unblock Tool** when you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.

7. (Optional) To remove all Discover databases and logs from the endpoints, clear the selection for **Soft uninstall**.

   CAUTION

   When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

8. (Optional) To also remove any tools that were dependencies of the Discover tools that are not dependencies for tools from other solutions, select **Remove unreferenced dependencies**.

9. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   BEST PRACTICE

   If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

10. Click **Show preview to continue**.

11. A results grid appears at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

NOTE

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

Uninstall Discover

1. From the Main menu, go to **Administration > Configuration > Solutions**. Under Discover, click **Uninstall**. Click **Proceed with Uninstall** to complete the process.

2. Delete any remaining Discover-related scheduled actions and action groups. For more information, see Tanium Console User Guide: Delete an action group.

© 2026 Tanium Inc. All Rights Reserved

3. Check for Discover artifacts on your endpoints. Ask the question: `Get Has Discover Artifacts = "true" from all machines`. If any endpoints are returned by this question and you want to clean the artifacts off the endpoint, contact Tanium Support. For more information, see Contact Tanium Support on page 131.
4. Check for Discover plugin schedules. From the Main menu, go to **Administration > Configuration > Common > Plugin Schedules**. If plugin schedules exist for Discover, contact Tanium Support.



After you uninstall Discover, Tanium no longer installs the **Discover** and **discover-cx** endpoint tools to new endpoints. The uninstall does not automatically remove endpoint tools from existing endpoints. For more information about how to remove the **Discover** and **discover-cx** endpoint tools from existing managed endpoints, see Tanium Endpoint Configuration User Guide: Uninstall tools installed by Endpoint Configuration.

Contact Tanium Support

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

For more information about how to submit a support case, see Case Submission Form.

© 2026 Tanium Inc. All Rights Reserved

Reference: Discover endpoint tools



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 Discover

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
discover-cx	Performs distributed ARP, NDP, Ping, Nmap scans, and satellite Nmap scans
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
Nmap	Network mapping tool used for certain scans in Comply and Discover
Npcap	Records process and command-line events on supported Windows endpoints to assist with Nmap scans

© 2026 Tanium Inc. All Rights Reserved

Reference: Data returned by profile type

Unique data is returned from profile scans. This data depends on the profile type and the scan that was performed. For example, EC2 and level 4 discovery return operating system information about the found interfaces, but other levels of discovery methods do not.

Information returned on interface pages for each profile types

	Level 1 (ARP)	Level 2 (Ping)	Level 3 (Nmap)	Level 4 (Nmap+Host)	Satellite	Centralized Nmap	Centralized AWS EC2	Returned for managed interfaces
Cloud Provider	✗	✗	✗	✗	✗	✗	✓	✗
Cloud Tags Tags assigned to an instance. AWS Docs: Tagging your Amazon EC2 resources	✗	✗	✗	✗	✗	✗	✓	✗
Computer Id	✓	✓	✓	✓	✓	✓	✗	✓
Discovery Method	✓	✓	✓	✓	✓	✓	✓	✓
First Managed	✗	✗	✗	✗	✗	✗	✗	✓[1]
First Seen	✓	✓	✓	✓	✓	✓	✓	✓
Hostname	✓	✓	✓	✓	✓	✓	✓	✓
Image Id Image from which the virtual machine was created.	✗	✗	✗	✗	✗	✗	✓	✗
Instance Id Unique identifier for the instance. Each instance can have multiple MAC addresses.	✗	✗	✗	✗	✗	✗	✓	✗

© 2026 Tanium Inc. All Rights Reserved

Information returned on interface pages for each profile types (continued)

	Level 1 (ARP)	Level 2 (Ping)	Level 3 (Nmap)	Level 4 (Nmap+Host)	Satellite	Centralized Nmap	Centralized AWS EC2	Returned for managed interfaces
Instance State Current phase of the instance lifecycle (such as running, stopped). AWS docs: Instance lifecycle	✗	✗	✗	✗	✗	✗	✓	✗
Instance Type Type of hardware of the host computer for the instance. AWS docs: Instance Types	✗	✗	✗	✗	✗	✗	✓	✗
Interfaces Number of interfaces that use the specific label. Only appears on the **Labels** page.	✓	✓	✓	✓	✓	✓	✓	✓
IP Address	✓	✓	✓	✓	✓	✓	✓	✓
Is Locally Administered MAC Value is `True` if the MAC address is assigned by a network administrator or software;.for example, when randomizing the address for privacy reasons. Locally-administered MAC addresses contain no information about the manufacturer of the interface, and the addresses might not be unique. Value is `False` if the address is universally administered, assigned by the manufacturer, and intended to be permanent and unique. Value is `null` if the interface has no MAC address.	✓	✓	✓	✓	✓[2]	✓	✓	✓

© 2026 Tanium Inc. All Rights Reserved

Information returned on interface pages for each profile types (continued)

	Level 1 (ARP)	Level 2 (Ping)	Level 3 (Nmap)	Level 4 (Nmap+Host)	Satellite	Centralized Nmap	Centralized AWS EC2	Returned for managed interfaces
Is Managed Value is `1` for any managed interfaces, `0` for unmanaged.	✓	✓	✓	✓	✓	✓	✓	✓
Labels Labels are applied to interfaces after they are imported by a profile. For more information, see Labels on page 103.	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Last Discovered The last time the interface was found. This attribute is used to determine when an interface is flagged as Lost.	✓ (connected results only)	✓	✓	✓	✓	✓	✓	✗
Last Managed The last time that the interface was returned as a managed interface. This attribute is used to determine when an interface is flagged as Lost.	✗	✗	✗	✗	✗	✗	✓	✓
Last Seen The last time the interface was found with any discovery method. All discovery methods return this value. This attribute is not used to determine when an interface is flagged as Lost.	✓	✓	✓	✓	✓	✓	✓	✓
Launch Time Time that the instance was started.	✗	✗	✗	✗	✗	✗	✓	✗

© 2026 Tanium Inc. All Rights Reserved

Information returned on interface pages for each profile types (continued)

	Level 1 (ARP)	Level 2 (Ping)	Level 3 (Nmap)	Level 4 (Nmap+Host)	Satellite	Centralized Nmap	Centralized AWS EC2	Returned for managed interfaces
Locations Location as determined by the uploaded CSV file. Locations are applied to interfaces after they are imported by a discovery method. Locations on page 99	✓	✓	✓	✓	✓	✓	✓	✓
MAC	✓	✓	✓	✓	✓[2]	✓[3]	✓	✓
Manually Ignored An interface that was marked as ignored by clicking **Ignore**.	✓	✓	✓	✓	✓	✓	✓	✓
Manufacturer The network card manufacturer, derived from the MAC address. If the MAC address is randomized, unknown, or unrecognized, this value appears as `Unknown`.	✓	✓	✓	✓	✓[2]	✓[3]	✓[4]	✓
NAT IP Address	✓	✓	✓	✓	✓	✓	✗	✓
Open Ports The most common 1000 ports that get scanned by Nmap, or from a list of ports provided in the discovery method configuration.	✗	✗	✗	✓	✓	✓	✗	✓

© 2026 Tanium Inc. All Rights Reserved

Information returned on interface pages for each profile types (continued)

	Level 1 (ARP)	Level 2 (Ping)	Level 3 (Nmap)	Level 4 (Nmap+Host)	Satellite	Centralized Nmap	Centralized AWS EC2	Returned for managed interfaces
OS Generation **Nmap (Level 4):** A "best guess" of OS version from OS fingerprinting. Consider carefully if you choose OS Generation as a label condition. OS generation is not displayed for managed interfaces. **AWS:** Specific operating system returned by the Amazon API. This information is discovered when the "`ssm:DescribeInstanceInformation`" permission is set on the IAM role, and the instance is configured with Amazon EC2 Simple Systems Manager (SSM).	✗	✗	✗	✓	✓	✓	✓	✗
OS Platform The operating system.	✗	✓[5]	✗	✓	✓	✓	✓	✓
Owner ID	✗	✗	✗	✗	✗	✗	✓	✗
Profile Name The profiles that found the interface.	✓	✓	✓	✓	✓	✓	✓	✓

© 2026 Tanium Inc. All Rights Reserved

Information returned on interface pages for each profile types (continued)

	Level 1 (ARP)	Level 2 (Ping)	Level 3 (Nmap)	Level 4 (Nmap+Host)	Satellite	Centralized Nmap	Centralized AWS EC2	Returned for managed interfaces
Unmanageable Unmanageable interfaces are on devices that cannot run the Tanium Client. By default, unmanageable interfaces have an OS Platform that is not supported by the Tanium Client, defined by the **Unmanageable OS Platforms** predefined automatic label.	✗	✗	✗	✓	✓	✓	✓	✓
Virtual Network Id Network that is configured in a virtual private cloud.	✗	✗	✗	✗	✗	✗	✓	✗
Zone Regions associated with the instance. AWS docs: Available regions	✗	✗	✗	✗	✗	✗	✓	✗

[1] First managed returned only for interfaces that changed from unmanaged to managed

[2] For satellite scans, `MAC` and `Manufacturer` are returned only if the scan runs on the same network as the satellite

[3] For centralized Nmap scans, `MAC` and `Manufacturer` are returned only if the scan runs on the same network as the Tanium Module Server

[4] For centralized AWS EC2 scans, `AWS` is returned as the manufacturer for all discovered interfaces

[5] Solaris endpoints do not detect OS platform

© 2026 Tanium Inc. All Rights Reserved

Reference: Discover columns for Connect exports

Use the following table to map the columns sent through Connect export jobs to the columns in the Discover database.

For more information about descriptions of the Discover columns, see Reference: Data returned by profile type on page 133.

Discover columns sent through Connect export jobs

Discover column	Exported name through Connect	Description
Cloud Provider	Provider	The cloud provider that hosts the endpoint. This field only applies to endpoints managed in Amazon Web Services.
Cloud Tags	CloudTags	Any labels assigned to the endpoint from the cloud provider. This field only applies to endpoints managed in Amazon Web Services.
Computer Id	TaniumComputerId	Custom Tanium ID for endpoints that have the Tanium Client. If an endpoint does not have the Tanium Client, the value is 0.
Discovery Method	Arp Ndp Nmap Ping Connected AwsApi CentralizedNmap (specific to scan profiles)	For each discovery method, the value is TRUE if Discover found the endpoint using that method. Otherwise, the value is FALSE. For any given endpoint, more than one discovery method can be TRUE.
First Managed	FirstManagedAt	The first time that the managed endpoint responded to Discover saved questions as part of the Discover import cycle.
First Seen	CreatedAt	The time when the endpoint was initially discovered and created in the Discover database.
Hostname	HostName	The hostname of the endpoint.
Image Id	ImageId	The image ID assigned by the cloud provider. This column only applies to endpoints managed in Amazon Web Services.
Instance Id	InstanceId	The instance ID assigned by the cloud provider. This column only applies to endpoints managed in Amazon Web Services.
Instance State	InstanceState	The instance state assigned by the cloud provider. This field only applies to endpoints managed in Amazon Web Services.

© 2026 Tanium Inc. All Rights Reserved

Discover columns sent through Connect export jobs (continued)

Discover column	Exported name through Connect	Description
Instance Type	InstanceType	The instance type assigned by the cloud provider. This field only applies to endpoints managed in Amazon Web Services.
IP Address	IpAddress	The IP address of the endpoint.
Is Locally Administered MAC	IsLocallyAdministeredMAC	Boolean to indicate if the MAC address is assigned by a network administrator or software.
Is Managed	Managed	Boolean to indicate if the endpoint is managed.
Labels	Labels	Any custom labels assigned to the endpoint. For more information about labels, see Labels on page 103.
Last Discovered	LastDiscoveredAt	The most recent time the endpoint was detected by a Discover scan.
Last Managed	LastManagedAt	For interfaces that were previously managed, this column contains the most recent time that the endpoint had the Tanium Client and answered Discover saved questions.
Last Seen	UpdatedAt	The time when the Discover scan detected a change in any column definition value for the endpoint.
Launch Time	LaunchTime	The time when the endpoint image was created in the cloud provider. This field only applies to endpoints managed in Amazon Web Services.
Locations	Locations	The location of the endpoint. This field only populates if you import locations in Discover. For more information about locations, see Locations on page 99.
MAC	MacAddress	The MAC address of the endpoint.
Manufacturer	MacOrganization	The organization to which the MAC address belongs.
NAT IP Address	NatIpAddress	The NAT IP address, if applicable.
Open Ports	Ports	Open ports on the endpoint.
OS Generation	OsGeneration	Specific generation or version of the operating system on the endpoint.
OS Platform	Os	The operating system on the endpoint.
Owner ID	OwnerId	The ID of the owner who owns the endpoint image on the cloud provider. This field only applies to endpoints managed in Amazon Web Services.
Profile Name	Profile	The scan profile that discovered the endpoint. For more information about profiles, see Configure profile for satellite scan on page 78.

© 2026 Tanium Inc. All Rights Reserved

Discover columns sent through Connect export jobs (continued)

Discover column	Exported name through Connect	Description
SatelliteDecId	SatelliteDecId	The ID of the satellite that discovered the interface during a satellite scan, if any.
SatelliteName	SatelliteName	The name of the satellite that discovered the interface during a satellite scan, if any.
SatelliteNmap	SatelliteNmap	Boolean to indicate if the endpoint was discovered by a satellite Nmap scan.
Unmanageable	Unmanageable	Possible values: • 0 - Managed or manageable (automatically marked) • 1 - Unmanageable (automatically marked) • 2 - Manageable (manually marked) • 3 - Unmanageable (manually marked)
Virtual Network Id	VirtualNetworkId	The ID of the virtual network on the cloud provider, if any. This field only applies to endpoints managed in Amazon Web Services.
Zone	Zone	The region where the endpoint image is hosted on a cloud provider. This field only applies to endpoints managed in Amazon Web Services.



Exported data in Connect also contains an **id** column. This column does not appear in the Discover workbench.

© 2026 Tanium Inc. All Rights Reserved

Reference: Gateway examples for Discover

For more information about how to view additional Gateway example syntax, see Tanium Gateway User Guide: Reference: Filter syntax and Tanium Gateway User Guide: Reference: Gateway examples.

Discover query filter syntax

Discover queries that request labels or interfaces using `discoverLabels` or `discoverInterfaces` support the `path` and `value` filter fields.

For more information on syntax, see `FieldFilter` in the **Documentation Explorer** pane of the query explorer.

Single column

You can filter on field values. Define a filter object using one of the following syntaxes:

```
discoverInterfaces (filter:
  {
    path: "field-path",
    op: "operator-value",
    value: "field-value"
  }
)
```

```
discoverLabels (filter:
  {
    path: "field-path",
    op: "operator-value",
    value: "field-value"
  }
)
```

Use dot notation for sub-fields not at the root level.

For example, the following query retrieves labels with a `createdTime value` greater than `2022` and returns the labels:

```
1  query exampleGetLabels {
2    discoverLabels(filter: {path: "createdTime", op: GT, value: "2023-01-01"}) {
3      edges {
4        node {
```

© 2026 Tanium Inc. All Rights Reserved

```
        name
        type
        createdTime
        modifiedTime
      }
    }
  }
}
```

Multiple columns

You can filter on multiple Discover-related columns. Define a filter object using one of the following syntaxes:

```
discoverInterfaces (filter:
  {any: boolean,
    filters: [
      {path: "field-path-1", op: "operator-1", value: "filter-value-1"},
      {path: "field-path-2", op: "operator-2", value: "filter-value-2"},
      {path: "field-path-n", op: "operator-n", value: "filter-value-n"}
    ]
  }
)
```

```
discoverLabels (filter:
  {any: boolean,
    filters: [
      {path: "field-path-1", op: "operator-1", value: "filter-value-1"},
      {path: "field-path-2", op: "operator-2", value: "filter-value-2"},
      {path: "field-path-n", op: "operator-n", value: "filter-value-n"}
    ]
  }
)
```

Use dot notation for sub-fields not at the root level.

For example, the following query retrieves interfaces associated with the label `Example_label` and an osPlatform of `Linux`, and returns matching interfaces:

© 2026 Tanium Inc. All Rights Reserved

```
query exampleGetInterfaces {
  discoverInterfaces(
    filter: {any: false, filters: [{path: "labels.name", op: EQ, value: "Example_label"},
{path: "osPlatform", op: EQ, value: "Linux"}]}
  ) {
    edges {
      node {
        id
        labels
        osPlatform
      }
    }
  }
}

```

Discover examples

The following queries and mutation require Discover, retrieve information about Discover labels and interfaces, and allow you to create or delete labels, or update labels applied to interfaces.

Discover requests have the following feature-specific dependencies at the specified minimum versions:

- Discover 4.8.298 or later is required to submit a request involving Discover interfaces or labels (`mutation.discoverInterfaceAddLabel`, `mutation.discoverInterfaceRemoveLabel`, `mutation.discoverLabelCreate`, `mutation.discoverLabelDelete`, `query.discoverInterface`, `query.discoverInterfaces`, `query.discoverLabel`, `query.discoverLabels`).

Add labels to interfaces (`mutation.discoverInterfaceAddLabel`)

ADD DISCOVER LABELS TO DISCOVER INTERFACES

The `discoverInterfaceAddLabel` mutation requires Discover 4.8.298 or later and the **Discover Tag write** permission.

The following mutation manually adds one or more standard labels to one or more specified interfaces. This mutation does not support automatic evaluation to apply labels.

```
mutation exampleAddInterfaceLabel($labelNames: [String!]!, $interfaceIDs: [ID!]!) {
```

© 2026 Tanium Inc. All Rights Reserved

```
  discoverInterfaceAddLabel(input: {names: $labelNames, interfaceIDs: $interfaceIDs}) {
    success
    error {
      message
    }
    cursor
  }
}
```

Include the interface variables in the **Variables** panel or in your variables dictionary:

```
{
    "labelNames": [
        "example_label",
        "example_label_2"
    ],
    "interfaceIDs": [
        12345,
        67890
    ]
}
```

Example response:

```
{
  "data": {
    "discoverInterfaceAddLabel": {
      "success": true,
      "error": null,
      "cursor": null
    }
  }
}
```

© 2026 Tanium Inc. All Rights Reserved

If your mutation request returns a cursor, the label is not yet added to the interfaces that you specify. You can pass the cursor as input to a subsequent `discoverInterfaceAddLabel` mutation to determine the status of the initial request.

```
mutation exampleAddInterfaceLabel ($labelNames: [String!]!, $interfaceIDs: [ID!]!){
  discoverInterfaceAddLabel (
    input: {
      labelNames: $labelNames,
      interfaceIDs: $interfaceIDs
      cursor: "Mg=="
    }
  ) {
    success
    error {
      message
    }
    cursor
  }
}
```

Create a label (`mutation.discoverLabelCreate`)

CREATE A DISCOVER LABEL

The `discoverLabelCreate` mutation requires Discover 4.8.298 or later and the **Discover Tag Write** permission. If you define at least one Discover location, this also requires the **Discover Location Permissions Write** permission.



Using Gateway, you can create a standard-type Discover label that you use to manually mark interfaces. You cannot create an automatic-type label that applies to interfaces based on configured criteria. To configure an automatic label to apply to interfaces, see Tanium Discover User Guide - Automatically label interfaces.

The following mutation creates a standard-type label.

```
mutation exampleCreateInterfaceLabel($labelName: String!) {
  discoverLabelCreate(input: {name: $labelName}) {
    label {
```

© 2026 Tanium Inc. All Rights Reserved

```
      name
      type
      createdTime
      modifiedTime
    }
    error {
      message
    }
  }
}
```

Include the name variable in the **Variables** panel or in your variables dictionary:

```
{
  "labelName": "Example_label"
}
```

Example response:

```
{
  "data": {
    "discoverLabelCreate": {
      "label": {
        "name": "Example_label",
        "type": "STANDARD",
        "createdTime": "2023-03-29T13:42:22.760Z",
        "modifiedTime": "2023-03-29T13:42:22.760Z"
      },
      "error": null
    }
  }
}
```

Delete a label by name (`mutation.discoverLabelDelete`)

© 2026 Tanium Inc. All Rights Reserved

DELETE A DISCOVER LABEL BY NAME

The `discoverLabelDelete` mutation requires Discover 4.8.298 or later and the **Discover Tag write** permission. If you define at least one Discover location, this also requires the **Discover Location Permissions write** permission.

The following mutation deletes a label. If you delete a label, the label is removed from all the related interfaces.

```
mutation exampleDeleteInterfaceLabel($labelName: String!) {
  discoverLabelDelete(ref: {name: $labelName}) {
    name
    error {
      message
    }
  }
}

```

Include the name variable in the **Variables** panel or in your variables dictionary:

```
{
  "labelName": "Example_label"
}
```

Example response:

```
{
  "data": {
    "discoverLabelDelete": {
      "name": "Example_label",
      "error": null
    }
  }
}
```

Get interface by ID (`query.discoverInterface`)

© 2026 Tanium Inc. All Rights Reserved

GET A DISCOVER INTERFACE BY ID

The `discoverInterface` query requires Discover 4.8.298 or later and the **Discover Asset read** permission. If you define at least one Discover location, this also requires either the **User Group read** permission (returns only matching interfaces to which the user group membership allows access) or the **Discover Location Permissions write** permission (returns all matching interfaces).

Discover versions earlier than 4.11 do not support the `locallyAdministeredMacAddress` field to determine whether a MAC address is locally administered.

The following query retrieves the Discover interface with the ID of `123`.

```
query exampleGetSpecificInterface($id: ID!) {
  discoverInterface(ref: {id: $id}) {
    id
    macAddress
    manufacturer
    locallyAdministeredMacAddress
    hostnames
    ipAddresses
    labels {
      name
      type
      createdTime
      modifiedTime
    }
    osPlatform
    openPorts
    discoveryMethods
    lastSeenTime
    computerId
    natIPAddresses
    osGeneration
    profiles {
      name
    }
    cloudInstances {
      id
```

© 2026 Tanium Inc. All Rights Reserved

```
      imageId
      type
      state
      launchTime
      zone
      provider
      networkId
      account
    }
    cloudTags {
      name
      value
    }
    firstSeenTime
    firstManagedTime
    lastManagedTime
    lastDiscoveredTime
    isManaged
    isUnmanageable
    isIgnored
    satellites {
      id
      name
    }
  }
}
```

Include the ID variable in the **Variables** panel or in your variables dictionary:

```
{
  "id": "123"
}
```

Example response:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "data": {
    "discoverInterface": {
      "id": "123",
      "macAddress": "01-23-45-67-89-AB",
      "manufacturer": "Microsoft Corporation",
      "locallyAdministeredMacAddress": true,
      "hostnames": [
        "example_hostname"
      ],
      "ipAddresses": [
        "192.0.2.0"
      ],
      "labels": [
        {
          "name": "Example label 2",
          "type": "STANDARD",
          "createdTime": "2021-02-23T03:03:31.897Z",
          "modifiedTime": "2021-02-23T03:03:31.897Z"
        }
      ],
      "osPlatform": "Windows",
      "openPorts": [
        80,
        443
      ],
      "discoveryMethods": [
        "NMAP",
        "MANAGED"
      ],
      "lastSeenTime": "2023-03-29T14:07:32.384Z",
      "computerId": "123456789",
      "natIPAddresses": [
        "198.51.100.10"
```


© 2026 Tanium Inc. All Rights Reserved

```
        ],
        "osGeneration": null,
        "profiles": [
          {
            "name": "Distributed Nmap"
          },
          {
            "name": "Level 4 - Test"
          }
        ],
        "cloudInstances": [],
        "cloudTags": [],
        "firstSeenTime": "2021-03-02T16:14:17.000Z",
        "firstManagedTime": null,
        "lastManagedTime": "2023-03-29T14:07:32.384Z",
        "lastDiscoveredTime": "2022-11-09T03:22:32.140Z",
        "isManaged": true,
        "isUnmanageable": false,
        "isIgnored": false,
        "satellites": []
      }
    }
}
```


Get multiple interfaces (`query.discoverInterfaces`)

GET MULTIPLE DISCOVER INTERFACES

The `discoverInterfaces` query requires Discover 4.8.298 or later and the **Discover Asset read** permission. If you define at least one Discover location, this also requires either the **User Group read** permission (returns only matching interfaces to which the user group membership allows access) or the **Discover Location Permissions write** permission (returns all matching interfaces).

Discover versions earlier than 4.11 do not support the `locallyAdministeredMacAddress` field to determine whether a MAC address is locally administered.

The following query retrieves the first `2` Discover interfaces.

© 2026 Tanium Inc. All Rights Reserved

```
query exampleGetInterfaces($first: Int) {
  discoverInterfaces(first: $first) {
    edges {
      node {
        id
        macAddress
        manufacturer
        locallyAdministeredMacAddress
        hostnames
        ipAddresses
        labels {
          name
          type
          createdTime
          modifiedTime
        }
        osPlatform
        openPorts
        discoveryMethods
        lastSeenTime
        computerId
        natIPAddresses
        osGeneration
        profiles {
          name
        }
        cloudInstances {
          id
          imageId
          type
          state
          launchTime
          zone
          provider
```

© 2026 Tanium Inc. All Rights Reserved

```
            networkId
            account
          }
          cloudTags {
            name
            value
          }
          firstSeenTime
          firstManagedTime
          lastManagedTime
          lastDiscoveredTime
          isManaged
          isUnmanageable
          isIgnored
          satellites {
            id
            name
          }
        }
      }
    }
}
```

Include the pagination variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 2
}
```

Example response:

```
{
  "data": {
```

© 2026 Tanium Inc. All Rights Reserved

```
    "discoverInterfaces": {
      "edges": [
        {
          "node": {
            "id": "123",
            "macAddress": "01-23-45-67-89-AB",
            "manufacturer": "Microsoft Corporation",
            "locallyAdministeredMacAddress": true,
            "hostnames": [
              "example_hostname"
            ],
            "ipAddresses": [
              "192.0.2.10"
            ],
            "labels": [
              {
                "name": "Example label 2",
                "type": "STANDARD",
                "createdTime": "2021-02-23T03:03:31.897Z",
                "modifiedTime": "2021-02-23T03:03:31.897Z"
              }
            ],
            "osPlatform": "Windows",
            "openPorts": [
              80,
              443
            ],
            "discoveryMethods": [
              "NMAP",
              "MANAGED"
            ],
            "lastSeenTime": "2023-03-29T14:07:32.384Z",
            "computerId": "123456789",
            "natIPAddresses": [
```


© 2026 Tanium Inc. All Rights Reserved

```
              "198.51.100.10"
            ],
            "osGeneration": null,
            "profiles": [
              {
                "name": "Distributed Nmap"
              },
              {
                "name": "Level 4 - Test"
              }
            ],
            "cloudInstances": [],
            "cloudTags": [],
            "firstSeenTime": "2021-03-02T16:14:17.000Z",
            "firstManagedTime": null,
            "lastManagedTime": "2023-03-29T14:07:32.384Z",
            "lastDiscoveredTime": "2022-11-09T03:22:32.140Z",
            "isManaged": true,
            "isUnmanageable": false,
            "isIgnored": false,
            "satellites": []
          }
        },
        {
          "node": {
            "id": "456",
            "macAddress": "CD-EF-01-23-45-67",
            "manufacturer": "Microsoft Corporation",
            "locallyAdministeredMacAddress": true,
            "hostnames": [
              "example_hostname_2"
            ],
            "ipAddresses": [
              "192.0.2.20"
```


© 2026 Tanium Inc. All Rights Reserved

```
            ],
            "labels": [
              {
                "name": "Example label 2",
                "type": "STANDARD",
                "createdTime": "2021-02-23T03:03:31.897Z",
                "modifiedTime": "2021-02-23T03:03:31.897Z"
              }
            ],
            "osPlatform": "Windows",
            "openPorts": [
              80,
              443
            ],
            "discoveryMethods": [
              "PING",
              "NMAP",
              "MANAGED"
            ],
            "lastSeenTime": "2023-03-29T14:07:32.384Z",
            "computerId": "987654321",
            "natIPAddresses": [
              "198.51.100.20"
            ],
            "osGeneration": null,
            "profiles": [
              {
                "name": "Distributed Nmap"
              }
            ],
            "cloudInstances": [],
            "cloudTags": [],
            "firstSeenTime": "2021-03-03T19:58:04.000Z",
            "firstManagedTime": "2021-03-09T18:31:43.000Z",
```


© 2026 Tanium Inc. All Rights Reserved

```
            "lastManagedTime": "2023-03-29T14:07:32.384Z",
            "lastDiscoveredTime": "2022-11-09T12:52:32.261Z",
            "isManaged": true,
            "isUnmanageable": false,
            "isIgnored": false,
            "satellites": []
          }
        }
      ]
    }
  }
}
```

Get label by name (`query.discoverLabel`)

GET A DISCOVER LABEL BY NAME

The `discoverLabel` query requires Discover 4.8.298 or later and the **Discover Asset read** permission.

The following query retrieves the Discover label with the name of `Example_label`.

```
query exampleGetSpecificLabel($name: String!) {
  discoverLabel(ref: {name: $name}) {
    name
    type
    createdTime
    modifiedTime
  }
}
```

Include the name variable in the **Variables** panel or in your variables dictionary:

```
{
  "name": "Example_label"
}
```

© 2026 Tanium Inc. All Rights Reserved

Example response:

```
{
  "data": {
    "discoverLabel": {
      "name": "Example_label",
      "type": "STANDARD",
      "createdTime": "2025-03-29T19:32:26.942Z",
      "modifiedTime": "2025-05-06T19:46:15.844Z"
    }
  }
}
```

Get multiple labels (`query.discoverLabels`)

GET MULTIPLE DISCOVER LABELS

The `discoverLabels` query requires Discover 4.8.298 or later and the **Discover Asset read** permission.

The following query retrieves the first `2` Discover labels.

```
query exampleGetLabels($first: Int) {
  discoverLabels(first: $first) {
    edges {
      node {
        name
        type
        createdTime
        modifiedTime
      }
    }
  }
}
```

Include the pagination variable in the **Variables** panel or in your variables dictionary:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "first": 2
}
```

Example response:

```
{
  "data": {
    "discoverLabels": {
      "edges": [
        {
          "node": {
            "name": "Example label 1",
            "type": "AUTOMATIC",
            "createdTime": "2025-08-22T12:57:09.717Z",
            "modifiedTime": "2025-08-22T12:57:09.717Z"
          }
        },
        {
          "node": {
            "name": "Example label 2",
            "type": "STANDARD",
            "createdTime": "2025-08-22T12:57:09.718Z",
            "modifiedTime": "2025-08-22T12:57:09.718Z"
          }
        }
      ],
      "pageInfo": {
        "startCursor": "MA==",
        "endCursor": "MQ==",
        "hasNextPage": true,
        "hasPreviousPage": false
      },
      "totalRecords": 200
```

© 2026 Tanium Inc. All Rights Reserved

```
    }
  }
}
```

Remove labels from interfaces (`mutation.discoverInterfaceRemoveLabel`)

REMOVE DISCOVER LABELS FROM DISCOVER INTERFACES

The `discoverInterfaceRemoveLabel` mutation requires Discover 4.8.298 or later and the **Discover Tag write** permission.

The following mutation manually removes one or more standard labels from one or more specified interfaces.

```
mutation exampleRemoveInterfaceLabel($labelNames: [String!]!, $interfaceIDs: [ID!]!) {
  discoverInterfaceRemoveLabel(input: {names: $labelNames, interfaceIDs: $interfaceIDs}) {
    success
    error {
      message
    }
    cursor
  }
}
```

Include the interface variables in the **Variables** panel or in your variables dictionary:

```
{
  "labelNames": [
    "example_label",
    "example_label_2"
  ],
  "interfaceIDs": [
    12345,
    67890
  ]
}
```

Example response:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "data": {
    "discoverInterfaceRemoveLabel": {
      "success": true,
      "error": null,
      "cursor": null
    }
  }
}
```

If your mutation request returns a cursor, the label is not yet removed from the interfaces that you specify. You can pass the cursor as input to a subsequent `discoverInterfaceRemoveLabel` mutation to determine the status of the initial request.

```
mutation exampleRemoveInterfaceLabel($labelNames: [String!]!, $interfaceIDs: [ID!]!) {
  discoverInterfaceRemoveLabel(
    labelNames: $labelNames,
    ids: $interfaceIDs,
    cursor: "Mg=="
    }
  ) {
    success
    error {
      message
    }
    cursor
  }
}
```

© 2026 Tanium Inc. All Rights Reserved