

Tanium™ Direct Connect User Guide

Autonomous IT. Unstoppable Business.

2026H1 Semiannual Release

Version 2.10

August 10, 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

Direct Connect overview **9**

Monitoring endpoint sessions 9

Screen sharing 9

Managing satellites 9

Interoperability with other Tanium products 9

Tanium™ Comply 9

Tanium™ Connect 10

Tanium™ Client Management 10

Tanium™ Discover 10

Tanium™ Enforce 10

Tanium™ Gateway 10

Tanium™ Investigate and Tanium™ Reporting 10

Tanium™ Performance 10

Tanium™ Provision 10

Tanium™ Reveal 10

Tanium™ Threat Response 11

Getting started with Direct Connect **12**

Step 1: Install and configure Direct Connect 12

Step 2: Configure a Tanium™ Direct Connect Zone Proxy 12

Getting started with Screen Sharing **13**

Step 1: Install and configure Screen Sharing 13

Step 2: Create and sign in to a Tanium Account 13

Step 3: Configure security and network exclusions 13

Step 4: Configure users and user roles 13

Step 5: (Optional) Integrate with ServiceNow 14

Step 6: Initiate screen sharing sessions 14

Step 7: Monitor Screen Sharing license usage 14

© 2026 Tanium Inc. All Rights Reserved

Direct Connect requirements **15**
Core platform dependencies 15
Solution dependencies 15
Tanium recommended installation 15
Import specific solutions 15
Required dependencies 16
Feature-specific dependencies 16
Client extensions 16
Tanium Module Server 16
Endpoints 17
Supported operating systems (OSs) 17
Direct Connect OS support 17
Screen sharing OS support 17
Host and network security requirements 18
Ports 18
Ports and destinations for Direct Connect 18
Supported cipher suites for Direct Connect 19
Ports and destinations for Screen Sharing 20
Security exclusions 20
Security exclusions for Direct Connect 21
Security exclusions for Screen Sharing 22
Third-party internet URLs 22
Zone Proxy Server requirements 23
User role requirements 23
Direct Connect role requirements 23
Screen Sharing role requirements 28
Installing Direct Connect **32**
Before you begin 32
Import Direct Connect with default settings 32
Import Direct Connect with custom settings 33

© 2026 Tanium Inc. All Rights Reserved

Manage solution dependencies ... 33
Upgrade Direct Connect ... 34
Verify Direct Connect version ... 34
Configuring Direct Connect ... 35
Restricted targeting ... 35
Default settings ... 35
Install and configure Tanium Endpoint Configuration ... 36
Manage solution configurations with Tanium Endpoint Configuration ... 36
Configure Direct Connect ... 37
Configure the Direct Connect action group ... 37
Configure Endpoint Connection settings ... 37
Configure certificates ... 38
Set up Direct Connect users ... 39
Manage a Tanium™ Zone Proxy ... 40
Install or upgrade the Direct Connect Zone Proxy ... 40
Configure the Direct Connect Zone Proxy ... 43
Uninstall the Direct Connect Zone Proxy ... 44
Reviewing endpoint sessions ... 45
Testing direct endpoint connections ... 46
Working with screen sharing ... 48
Requirements ... 48
Integrate with ServiceNow ... 50
Configure personas to establish unattended screen sharing sessions ... 50
Open an endpoint screen sharing session ... 51
Open a screen sharing session from an endpoint ... 53
Open a screen sharing session from Direct Connect ... 54
Open a screen sharing session from Reporting ... 55
Open a screen sharing session from Performance ... 57
Open a screen sharing session with an endpoint that does not have a Tanium Client ... 58
View and join screen sharing sessions ... 59

© 2026 Tanium Inc. All Rights Reserved

Join active sessions in the list of sessions ... 59
Search for an endpoint to join the active session ... 59
View screen sharing session history ... 59
End an endpoint screen sharing session ... 59
End active sessions in the list of sessions ... 60
Search for an endpoint to end the active session ... 60
Configure ScreenMeet settings ... 60
Contact support ... 60
Working with audit logs ... **61**
View the audit log ... 61
Export an audit log ... 61
Before you begin ... 61
Create a connection ... 62
Test a connection and review data ... 62
Managing satellites ... **63**
Overview of satellites ... 63
View satellites ... 63
Create satellites ... 64
Designate satellites ... 64
Name and verify satellites ... 65
Delete satellites ... 66
Troubleshooting Direct Connect ... **67**
Generate a support package ... 67
Change the logging level ... 67
Troubleshoot endpoint connection issues ... 67
Connection process ... 67
Troubleshoot connections ... 68
Troubleshoot Zone Proxy connection issues ... 68
Screen sharing buttons unavailable ... 68
Poor Connection Quality message when attempting to join a screen sharing session ... 69

© 2026 Tanium Inc. All Rights Reserved

Verify endpoint tools ... 69
Verify the configuration version ... 69
Remove Direct Connect tools from endpoints ... 70
Uninstall Direct Connect ... 71
Uninstall the Direct Connect Zone Proxy ... 72
Contact Tanium Support ... 72
Reference: Gateway examples for Direct Connect ... 73
Open a connection to an endpoint ... 73
Open direct connection to endpoint ... 73
Get the status of a connection to an endpoint ... 74
Get direct connection status ... 74
Ping the connection to an endpoint ... 75
Ping direct connection to endpoint ... 75
Get data from an endpoint ... 76
Get data from endpoint ... 76
Get process from an endpoint ... 77
Get process from endpoint ... 77
Get alerts from an endpoint ... 79
Get past 24 hours of alerts from endpoint ... 79
Get 48 hours of alerts from endpoint ... 81
Get alerts from prior date from endpoint ... 82
Stop a process on an endpoint ... 83
Stop endpoint process ... 83
Close connection to an endpoint ... 84
Close endpoint connection ... 84

© 2026 Tanium Inc. All Rights Reserved

Direct Connect overview

Tanium solutions use the communication channels that Tanium Direct Connect provides for bidirectional, interactive sessions with an endpoint. The sessions enable operations such as browsing and retrieving files, exploring security information in an investigation, establishing remote sessions, and transferring large amounts of data from the endpoint. Direct Connect provides a central location in the Tanium user interface (UI) where you can configure and administer direct endpoint connections across all solutions. You also use Direct Connect for managing satellite endpoints that run secure workloads on other endpoints that the Tanium™ Module Server cannot directly reach.

Monitoring endpoint sessions

An endpoint session is a direct connection between the Tanium Module Server and a single endpoint. You can use the Direct Connect **Overview** page to review your active (open) and pending (waiting to connect) endpoint sessions across Tanium solutions for auditing and troubleshooting. For more information, see Reviewing endpoint sessions on page 45.

Screen sharing

If you have a license, you can use screen sharing capabilities to connect to endpoints for troubleshooting purposes. For more information, see Working with screen sharing on page 48.

Managing satellites

You use Direct Connect to designate Tanium Clients as satellites and monitor their status. *Satellites* are managed endpoints that can run secure workloads on other endpoints that the Tanium Module Server cannot directly reach. Satellites enable Tanium solutions to perform operations on those endpoints. For example, satellites can perform non-line-of-sight scans for Tanium™ Discover, perform remote authenticated scans for Tanium™ Comply, and create Preboot eXecution Environment (PXE) endpoints for Tanium™ Provision.

For more information about satellites, see Managing satellites on page 63. For more information about solution operations that use satellites, see Interoperability with other Tanium products on page 9.

Interoperability with other Tanium products

Tanium™ Comply

Use satellites for scan assessments to access unmanaged endpoints or endpoints that the Module Server cannot reach directly. Comply 2.11 or later is required to use Direct Connect. For more information, see

- Compliance assessments: Comply User Guide: Configure a remote authenticated scan assessment
- Vulnerability assessments: Comply User Guide: Creating vulnerability assessments

© 2026 Tanium Inc. All Rights Reserved

Tanium™ Connect

Use Direct Connect audit logs as a connection source. Connect 4.12 or later is required to use Direct Connect. For more information, see Working with audit logs on page 61.

Tanium™ Client Management

Client Management uses Direct Connect to access Tanium Client health information from endpoints. Client Management 1.5 or later is required to use Direct Connect. For more information, see Tanium Client Management User Guide: Access detailed client health and troubleshooting information on an endpoint.

Tanium™ Discover

Perform satellite scans. Discover 4.5 or later is required to perform satellite scans. For more information, see Discover User Guide: Running satellite scans.

Tanium™ Enforce

Enforce encryption management policies use Direct Connect to transfer encryption keys securely from the Tanium Client to the recovery key database during the encryption process. For more information see Enforce User Guide: Encryption management.

Tanium™ Gateway

Use Gateway to access the Direct Connect API. For more information about which features are available through Gateway, see Tanium Gateway User Guide: Schema reference.

Tanium™ Investigate and Tanium™ Reporting

Use Direct Connect with Investigate and Reporting to investigate performance, monitor activity history, browse the file system, and manage services on an endpoint. For more information, see Tanium Investigate User Guide and Tanium Reporting User Guide: Working with a single endpoint.

Tanium™ Performance

Use Direct Connect with Performance to view historical process-level data from a single endpoint for analysis and troubleshooting. For more information, see Performance User Guide: Connecting directly to endpoints.

Tanium™ Provision

Provision uses Direct Connect satellites to create Preboot eXecution Environment (PXE) endpoints and set up offline domain join for newly-provisioned Windows endpoints. For more information, see Provision User Guide: Deploy the Tanium PXE service and Provision User Guide: Create an ODJ endpoint.

Tanium™ Reveal

Reveal uses Direct Connect to view files on endpoints that match configured rules and patterns. Reveal 1.4 or later is required to use Direct Connect. For more information, see Reveal User Guide: Investigating rule matches and Reveal User Guide: Validating pattern matches.

© 2026 Tanium Inc. All Rights Reserved

Tanium™ Threat Response

Threat Response uses Direct Connect to connect to live endpoints and explore data. Threat Response 3.2 or later is required to use Direct Connect 2.1 or later. For more information, see Threat Response User Guide: Direct connecting to endpoints and exploring data.

© 2026 Tanium Inc. All Rights Reserved

Getting started with Direct Connect

Step 1: Install and configure Direct Connect

Install and configure Direct Connect, either through automatic configuration with default settings or through manual configuration with custom settings.

For more information, see Installing Direct Connect on page 32 and Configuring Direct Connect on page 35.

Step 2: Configure a Tanium™ Direct Connect Zone Proxy

If you want to use Direct Connect with endpoints that connect to the Tanium Module Server through a Tanium Zone Server, you must configure a Zone Proxy.

For more information, see Configure Zone Proxies.

© 2026 Tanium Inc. All Rights Reserved

Getting started with Screen Sharing

Step 1: Install and configure Screen Sharing

Install and configure Tanium Screen Sharing, either through automatic configuration with default settings or through manual configuration with custom settings.

For more information, see Installing Direct Connect on page 32 and Configuring Direct Connect on page 35.

Step 2: Create and sign in to a Tanium Account

Create and sign in to a Tanium Account to link the Tanium instance where you will use Screen Sharing. If your Tanium license includes Screen Sharing, it is automatically configured for your Tanium instance when your account is linked.

For more information, see Tanium Account User Guide: Creating and managing your Tanium Account.

Step 3: Configure security and network exclusions

Configure Tanium Core Platform, Tanium Client, Tanium Screen Sharing, and ScreenMeet security and network exclusions to ensure proper communications when establishing screen sharing sessions.

- For more information on Tanium Core Platform security exclusions, 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.
- For more information on Tanium Client port and network exclusions, see Tanium Client Management User Guide: Network connectivity, ports, and firewalls.
- For more information on Tanium Screen Sharing security and network exclusions, see Host and network security requirements, Security exclusions, and Internet URLs.
- For more information on ScreenMeet URLs and hosts to allow, see ScreenMeet Docs: Firewall configuration and ScreenMeet Docs: Egress IP Addresses.

Step 4: Configure users and user roles

Configure users, adding them to the **Integration Admin - ScreenMeet** user role to administrate screen sharing, and **Screen Sharing Agent** user role to use screen sharing.

If you want to customize screen sharing access, you can create custom user roles and assign them to personas. Tanium Console operators can select a persona to change their available permissions without changing user accounts. For example:

- Assign the **Screen Sharing Support Session Unattended** permission to a role and persona to allow users that select the persona to create unattended screen sharing sessions.
- Assign the **Screen Sharing Console Execute** permission to a role and persona to allow users that select the persona to access the ScreenMeet console without accessing administrator settings.

© 2026 Tanium Inc. All Rights Reserved

NOTE

By default, the **Screen Sharing Support Session Unattended** permission is not assigned to any user role, only Tanium administrators. For information on configuring a custom role and persona to establish unattended screen sharing sessions, see Configure personas to establish unattended screen sharing sessions.

For more information on user role permissions, see Screen Sharing user role permissions.

Step 5: (Optional) Integrate with ServiceNow

Integrate Screen Sharing with your ServiceNow instance to update ServiceNow tickets with audit logs from a related screen sharing session. With this integration, you have an additional option when opening screen sharing sessions: **Send audit log to ServiceNow**. If you select this option, you can add the ServiceNow Ticket ID that is associated with the screen sharing session.

For more information, see Integrate with ServiceNow.

Step 6: Initiate screen sharing sessions

Initiate screen sharing sessions using Direct Connect for Windows endpoints, Single Endpoint View for macOS endpoints, or the ScreenMeet console for mobile devices.

For more information, see Open an endpoint screen sharing session and ScreenMeet docs: Connecting to Mobile devices.

Step 7: Monitor Screen Sharing license usage

From the Direct Connect settings, monitor current Screen Sharing license usage, filter the list of users allocated a per-user license, and update the Alert Threshold for sending an alert if your ratio of allocated licenses to total licenses exceeds the percentage.

For more information, see Configure ScreenMeet settings.

© 2026 Tanium Inc. All Rights Reserved

Direct Connect requirements

Review the requirements before you install and use Direct Connect.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Direct Connect. For more information about how to get Direct Connect, see Tanium Solutions & Bundles.
- Tanium™ Core Platform servers
- **Tanium™ Appliance**:
  (Optional) If you are using a Tanium Appliance for your Zone Server, you must install the Direct Connect Zone Proxy through the Tanium Operations menu on the Zone Server appliance. For more information, see Appliance Deployment Guide: Install the Direct Connect Zone Proxy. To install the Direct Connect Zone Proxy on a Tanium Appliance with the All-in-One role, use the TanOS shell.
- **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.

Solution dependencies

Other Tanium solutions are required for Direct Connect to function. The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.



Some Direct Connect dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 16. Note that the links open the user guides for the latest version of each solution.

Tanium recommended installation

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

Import specific solutions

If you select only Direct Connect to import, you must manually import dependencies. For more information, see Tanium Console User Guide: Import, re-import, or update specific solutions.

© 2026 Tanium Inc. All Rights Reserved

Required dependencies

Direct Connect has the following required dependencies:

- Tanium™ Data Service (TDS)
- Tanium™ Endpoint Configuration
- Tanium™ Interact
- Tanium RDB Service

Feature-specific dependencies

If you select only Direct Connect to import, you must manually import its feature-specific dependencies. Direct Connect has the following feature-specific dependencies to use screen sharing functionality:

- Tanium™ Account
- Tanium™ Console
- Tanium™ Reporting
- Tanium™ Reporting Content
- Tanium Screen Sharing
- Tanium™ Secrets Service

Client extensions

Tanium Endpoint Configuration installs Client Extensions and other tools for Direct Connect 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 all Client Extensions and tools, see Tanium Client Management User Guide: Reference: Client extensions and endpoint tools used for Tanium solutions.

- **Config CX**: Provides installation and configuration of extensions on endpoints. Tanium Endpoint Configuration installs this Client Extension.
- **Core CX**: Provides a management framework API for all other Client Extensions and exposes operating system metrics. Tanium Endpoint Configuration installs this Client Extension.
- **DEC CX**: Provides a direct connection between endpoint and Module Server. Tanium Direct Connect installs this Client Extension.

Tanium Module Server

Direct Connect is installed and runs as a service on the Module Server. The impact on the Module Server is minimal and depends on usage.

© 2026 Tanium Inc. All Rights Reserved

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

Endpoints

Supported operating systems (OSs)

DIRECT CONNECT OS SUPPORT

Direct Connect supports the following endpoint OSs.

Supported operating systems for Direct Connect

Operating System	Version	Notes
Windows	• Windows 7 Service Pack 1 or later • Windows Server 2008 R2 Service Pack 1 or later	
macOS	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and host system requirements.	Only Direct Connect 2.2.103 or later supports Tanium Clients using the universal binary.
Linux	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and host system requirements.	

SCREEN SHARING OS SUPPORT

The following endpoint operating systems are supported for screen sharing through Tanium. For more information about the operating systems that ScreenMeet supports, see ScreenMeet Documentation: Requirements.



The first time a Tanium Console operator establishes a screen sharing session with a macOS endpoint, the endpoint user must select **ScreenMeetSupport** in the **Screen Recording** and **Accessibility** permissions in **System Settings**, then click **Later** when prompted. For more information, see ScreenMeet Documentation: Connecting to Mac devices.

© 2026 Tanium Inc. All Rights Reserved

Supported operating systems for Screen Sharing

Operating System	Version	Notes
Windows	• Windows 11	Windows operating systems also require .NET Framework 4.8 or later. Windows operating systems support attended and unattended screen sharing sessions.
Windows Server	• Windows Server 2025 • Windows Server 2022	
macOS	• 15 or later	macOS operating systems support only attended screen sharing sessions.

Host and network security requirements

Specific ports and processes are needed to run Direct Connect.

Ports

PORTS AND DESTINATIONS FOR DIRECT CONNECT

Direct Connect requires the following ports, which communicate over HTTPS using TLS 1.2 (RSA 2048-bit).



These ports are not required for screen sharing. For more information, see Ports and destinations for Screen Sharing on page 20.

Exclude port 17486 traffic from SSL inspection or interception if that is configured in your environment. The port does not support SSL inspection or interception.

Ports for Direct Connect communication

Source	Destination	Port	Protocol	Purpose
Tanium Client (internal)	Module Server	17475	TCP	Used by the Module Server for endpoint connections to internal Tanium Clients.
Tanium Client (external)	Zone Server[1]	17486	TCP	Used by the Zone Server for endpoint connections to external Clients. This port begins listening after the Zone Proxy provisioning process is complete on port `17488`. The default port number is `17486`. If needed, you can specify a different port number when you configure the Zone Proxy.

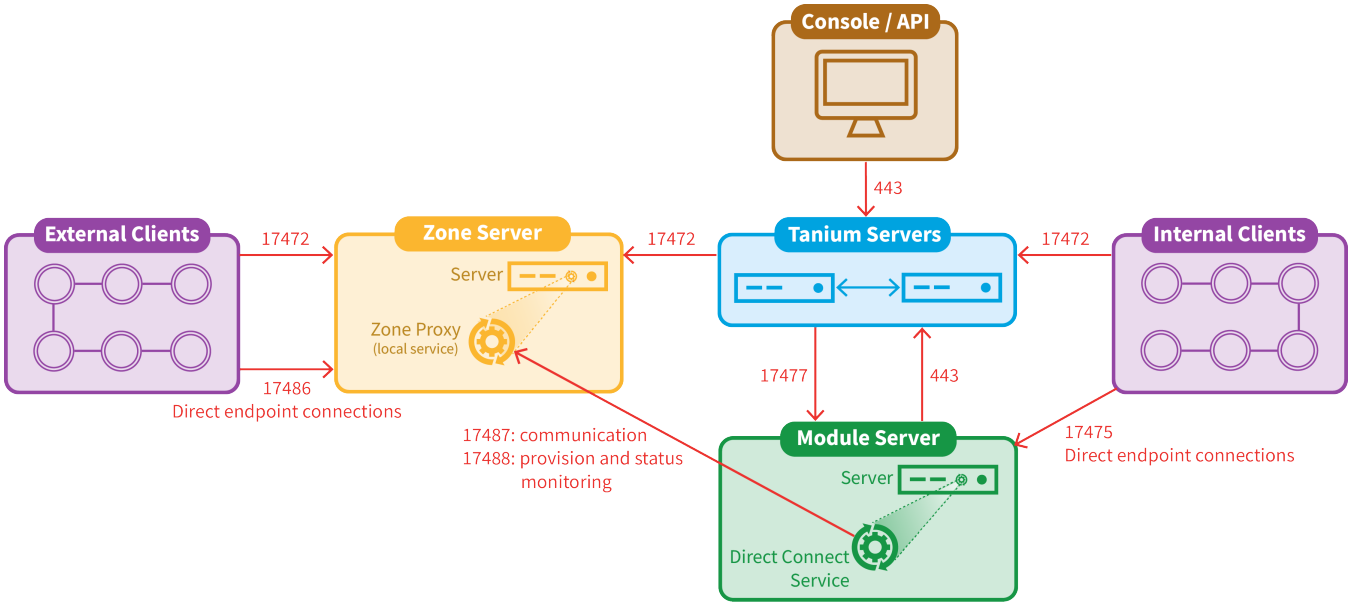
© 2026 Tanium Inc. All Rights Reserved

Ports for Direct Connect communication (continued)

Source	Destination	Port	Protocol	Purpose
Module Server	Zone Server[1]	17487	TCP	Used by the Zone Server for Module Server connections. This port begins listening after the Zone Proxy provisioning process is complete on port `17488`. The default port number is `17487`. If needed, you can specify a different port number when you configure the Zone Proxy.
		17488	TCP	Used by the Module Server to provision the Zone Proxy on the Zone Server. After the Zone Proxy is provisioned, used for connection status and diagnostics. On TanOS, the Direct Connect Zone Proxy installer automatically configures the firewall on the Zone Server to open port `17488`. You must manually configure the firewall to open this port on Windows. This port number is not configurable.
Tanium Server	Module Server	17477	TCP	Tanium Server initiates connections to the Module Server on port `17477`.

[1] These ports are required only when you use a Zone Server.

Required ports for Direct Connect



Supported cipher suites for Direct Connect

Direct Connect supports the following cipher suites for encrypting information in TLS communication:

- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`

© 2026 Tanium Inc. All Rights Reserved

- `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`

PORTS AND DESTINATIONS FOR SCREEN SHARING

Screen Sharing requires the following port.

Ports for Screen Sharing communication

Source	Destination	Port	Protocol	Purpose
Tanium Module Server	`*.cloud.tanium.com`	443	TCP	Required for the Tanium Module Server to connect to Tanium™ Account for provisioning an on-premises configuration



Screen Sharing also requires port 443/TCP and 443/UDP for ScreenMeet application traffic, which goes through TLS-encrypted connections. For more information, see ScreenMeet Documentation: Firewall configuration / whitelisting.

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.



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.

The following sections list the security exclusions that Direct Connect and Screen Sharing require:

- Security exclusions for Direct Connect on page 21
- Security exclusions for Screen Sharing on page 22



With the exception of the security exclusions listed at 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, Direct Connect security exclusions are not required to use Screen Sharing, and Screen Sharing security exclusions are not required to use Direct Connect.

© 2026 Tanium Inc. All Rights Reserved

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

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	<*Module Server*>\services\direct-connect-service\TaniumDirectConnectService.exe
		Process	<*Module Server*>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe
Zone Server		Process	<*Tanium Installation Directory*>\Tanium Direct Connect Zone Proxy\node.exe
		Process	<*Tanium Installation Directory*>\Tanium Direct Connect Zone Proxy\twsm.exe

Direct Connect security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		File	<*Tanium Client*>\TaniumClientExtensions.dll
		File	<*Tanium Client*>\TaniumClientExtensions.dll.sig
		File	<*Tanium Client*>\extensions\TaniumDEC.dll
		File	<*Tanium Client*>\extensions\TaniumDEC.dll.sig
		Process	<*Tanium Client*>\TaniumCX.exe
macOS		File	<*Tanium Client*>/libTaniumClientExtensions.dylib
		File	<*Tanium Client*>/libTaniumClientExtensions.dylib.sig
		File	<*Tanium Client*>/extensions/libTaniumDEC.dylib
		File	<*Tanium Client*>/extensions/libTaniumDEC.dylib.sig
		Process	<*Tanium Client*>/TaniumCX
Linux		File	<*Tanium Client*>/libTaniumClientExtensions.so
		File	<*Tanium Client*>/libTaniumClientExtensions.so.sig
		File	<*Tanium Client*>/extensions/libTaniumDEC.so
		File	<*Tanium Client*>/extensions/libTaniumDEC.so.sig
		Process	<*Tanium Client*>/TaniumCX

© 2026 Tanium Inc. All Rights Reserved

SECURITY EXCLUSIONS FOR SCREEN SHARING

When configuring security exclusions for Screen Sharing, 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

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

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\screen-sharing-service\TaniumScreenSharingService.exe`

Screen Sharing security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	`C:\ProgramData\Projector Inc\ScreenMeet Support\ScreenMeet.Support.exe`
		Process	`<Tanium Client>\Tools\ScreenSharing\ScreenMeet.Support.exe`
	for 32-bit operating system versions only	File	`C:\ProgramData\Projector Inc\ScreenMeet Support\<hash-value>\webrtcnative-x86.dll`
	for 64-bit operating system versions only	File	`C:\ProgramData\Projector Inc\ScreenMeet Support\<hash-value>\webrtcnative-x64.dll`
macOS		File	`/Applications/ScreenMeetSupport.app`

Third-party internet URLs

The endpoints in your environment require access to certain URLs to establish screen sharing sessions. If security software is deployed in the environment to monitor and block unknown URLs, your security administrator might need to allow the hosts and IP addresses listed at ScreenMeet Documentation: Firewall configuration / whitelisting and ScreenMeet Documentation: Egress IP Addresses, and allow the following URL.

NOTE

Allowing this URL is not required for Direct Connect.

© 2026 Tanium Inc. All Rights Reserved

Third-party URL required for Screen Sharing

URL	Source	Port	Protocol	Description
`*.screenmeet.com`	ScreenMeet client	443	TCP / UDP	Required for endpoints to establish screen sharing connections

NOTE

For the best results, allow traffic from the preceding URL to bypass proxy servers if you deployed such servers in your network. Screen sharing traffic that passes through proxy servers negatively impacts performance. For more information, see ScreenMeet Documentation: ScreenMeet Enterprise Deployment Guide.

Zone Proxy Server requirements

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.

To use Direct Connect for connecting with endpoints that route to the Module Server through a Zone Server, you must install and configure the Direct Connect Zone Proxy on that Zone Server. For more information, see Manage a Tanium™ Zone Proxy on page 40.

IMPORTANT

For best results, do not use a load balancer in front of your Zone Server. If you must use a load balancer, configure it for persistent TCP connections. The port that you configure in the Direct Connect Zone Proxy for the endpoint inbound port must be open on the load balancer. By default, this port is `17486`.

User role requirements

The following sections list the role permissions required to use Direct Connect and Screen Sharing.

- Direct Connect requirements on page 15
- Screen Sharing role requirements on page 28

For more information about role-based access control (RBAC), role permissions, and associated content sets, see Tanium Console User Guide: Managing RBAC.

Direct Connect role requirements

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

- Direct Connect solution permissions on page 24
- Direct Connect platform content and global permissions on page 27: The solution permissions automatically provide some of these permissions.

© 2026 Tanium Inc. All Rights Reserved

To review a summary of the predefined roles, see Set up Direct Connect users on page 39.

Some Direct Connect 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 Direct Connect. If you create custom roles for Direct Connect users, be sure to assign all the solution permissions and content set permissions that are required for Direct Connect 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 **Direct Connect Service Account** role to users. This role is for internal purposes only.

Direct Connect solution permissions

Permission	Direct Connect Administrator	Direct Connect User	Direct Connect Read Only User	Direct Connect Satellite Operator	Direct Connect Endpoint Configuration Approver	Direct Connect File Modifier
Client Stream View and configure connections to an on-premises destination that is not accessible from the external internet. These capabilitites also require **Direct Connect Satellite read** permission. For more information, see Tanium Connect User Guide: Configure sending data to an on-premises destination that is not accessible from the external internet.	✗	✗	✗	✗	✗	✗
Direct Connect Audit View Direct Connect audit events	✓ READ	✗	✗	✗	✗	✗
Direct Connect Core Query Issue queries on an endpoint	✓ READ	✓ READ	✗	✗	✗	✗

© 2026 Tanium Inc. All Rights Reserved

Direct Connect solution permissions (continued)

Permission	Direct Connect Administrator	Direct Connect User	Direct Connect Read Only User	Direct Connect Satellite Operator	Direct Connect Endpoint Configuration Approver	Direct Connect File Modifier
Direct Connect Cron Allows performing service account work	✗	✗	✗	✗	✗	✗
Direct Connect Endpoint Configuration Approve Endpoint Configuration items for Direct Connect	✗	✗	✗	✗	✓ APPROVE	✗
Direct Connect File Access and manage endpoint file systems through Direct Connect. For more information, see Tanium Investigate User Guide: Browsing the file system on an endpoint.	✓ READ WRITE	✓ READ	✗	✗	✗	✓ READ WRITE
Direct Connect Must Gather Access and run an Endpoint Must Gather (EMG) on an endpoint. For more information, see Tanium Reporting User Guide: Collect troubleshooting information.	✓ EXEC READ	✓ EXEC READ	✗	✗	✗	✓ EXEC READ
Direct Connect Registry View, add, edit, or delete Windows Registry values on the Endpoint Details page, **Remote Management** tab, **Browse & Edit Windows Registry** panel. For more information, see Tanium Investigate User Guide: Browse and edit the Windows registry.	✓ READ WRITE	✗	✗	✗	✗	✗

© 2026 Tanium Inc. All Rights Reserved

Direct Connect solution permissions (continued)

Permission	Direct Connect Administrator	Direct Connect User	Direct Connect Read Only User	Direct Connect Satellite Operator	Direct Connect Endpoint Configuration Approver	Direct Connect File Modifier
Direct Connect Satellite Manage satellites	✓ READ WRITE	✗	✗	✓ READ WRITE	✗	✗
Direct Connect Service Account For internal purposes only	✗	✗	✗	✗	✗	✗
Direct Connect Service State Start, stop, or restart services on Windows endpoints through the **Service Control** panel of the **Remote Management** tab in the Tanium™ Reporting Endpoint Details page. For more information, see Tanium Investigate User Guide: Service control.	✓ WRITE	✗	✗	✗	✗	✗
Direct Connect Session View, create, and manage endpoint connections View services on Windows endpoints through the **Service Control** panel of the **Remote Management** tab in the Tanium Reporting Endpoint Details page. For more information, see Tanium Investigate User Guide: Managing a single endpoint remotely.	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ WRITE	✗	✓ READ WRITE
Direct Connect Settings View and modify Direct Connect settings	✓ READ WRITE	✗	✗	✗	✓ READ	✗

© 2026 Tanium Inc. All Rights Reserved

Direct Connect solution permissions (continued)

Permission	Direct Connect Administrator	Direct Connect User	Direct Connect Read Only User	Direct Connect Satellite Operator	Direct Connect Endpoint Configuration Approver	Direct Connect File Modifier
Direct Connect Terminate Terminate processes on the Endpoint Details page, **Remote Management** tab, **Live Process Monitor** panel. For more information, see Tanium Investigate User Guide: Terminate one or multiple processes.	✓ PROCESS	✗	✗	✗	✗	✗
Directconnect View the Direct Connect workbench	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW

The permissions for these roles provide solution permissions for other solutions. To view the provided permissions, see Tanium Console User Guide: View effective role permissions.

Direct Connect platform content and global permissions

Permission	Permission Type	Direct Connect Administrator	Direct Connect User	Direct Connect Read Only User	Direct Connect Satellite Operator	Direct Connect Endpoint Configuration Approver	Direct Connect File Modifier
Action	Platform Content	✓ READ WRITE	✓ READ WRITE	✗	✓ READ WRITE	✓ READ	✓ READ WRITE
Bypass Action Approval	Platform Content	✗	✓ SPECIAL	✗	✗	✗	✓ SPECIAL
Own Action	Platform Content	✓ READ	✓ READ	✗	✓ READ	✓ READ	✓ READ
Package	Platform Content	✓ READ	✓ READ	✗	✓ READ	✓ READ	✓ READ
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE

© 2026 Tanium Inc. All Rights Reserved

Direct Connect platform content and global permissions (continued)

Permission	Permission Type	Direct Connect Administrator	Direct Connect User	Direct Connect Read Only User	Direct Connect Satellite Operator	Direct Connect Endpoint Configuration Approver	Direct Connect File Modifier
Saved Question	Platform Content	READ	READ	READ	READ	READ	READ
Sensor	Platform Content	READ	READ		READ	READ	READ
Read Solution	Global	SPECIAL				SPECIAL	

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

Screen Sharing role requirements

The predefined Screen Sharing roles provide the following permissions. For descriptions of these roles, see Requirements on page 48.

NOTE

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

Screen Sharing user role permissions

Permission	Integration Admin - ScreenMeet	Screen Sharing Agent	Integration Viewer - ScreenMeet
Screen Sharing API Connect to Screen Sharing API	EXECUTE	EXECUTE	EXECUTE
Screen Sharing Audit Event Log View event log for auditing purposes	READ WRITE		
Screen Sharing Config For internal purposes only	READ WRITE	READ	READ
Screen Sharing Console Get magic URL for accessing ScreenMeet console	EXECUTE	EXECUTE	

© 2026 Tanium Inc. All Rights Reserved

Screen Sharing user role permissions (continued)

Permission	Integration Admin - ScreenMeet	Screen Sharing Agent	Integration Viewer - ScreenMeet
Screen Sharing Console Admin Get magic URL for accessing ScreenMeet console and organizational settings	✓ EXECUTE	✗	✗
Screen Sharing Feed Integration User Interact with notifications from Tanium Feed.	✓ ACCOUNT	✗	✗
Screen Sharing Gallery View ScreenMeet in the Integrations Gallery	✓ READ	✗	✓ READ
Screen Sharing Integration Configure ScreenMeet in the Integrations Gallery	✓ ADMIN	✗	✓ VIEWER
Screen Sharing Partner Integration User Set credentials via the Partner Integration service	✓ ACCOUNT	✗	✗
Screen Sharing Platform Integration User Interact with the platform	✓ ACCOUNT	✓ ACCOUNT	✗
Screen Sharing Product Options Retrieve ScreenMeet product options values: Show recording option (provided by **Screen Sharing Support Session** Write)	✓ READ	✓ READ	✗
Screen Sharing Provisioning Otp Set provisioning information through a one-time passcode (OTP)	✓ WRITE	✗	✗
Screen Sharing Reporting Metrics Get Reporting metrics for Screen Sharing	✓ READ	✓ READ	✓ READ
Screen Sharing Settings Configure screen sharing settings	✓ READ WRITE	✓ READ	✓ READ

© 2026 Tanium Inc. All Rights Reserved

Screen Sharing user role permissions (continued)

Permission	Integration Admin - ScreenMeet	Screen Sharing Agent	Integration Viewer - ScreenMeet
Screen Sharing Support Session Start a screen sharing session on a remote endpoint, requiring endpoint user permission	✓ READ WRITE EXECUTE DELETE	✓ READ WRITE EXECUTE DELETE	✓ READ
Screen Sharing Support Session All Join any screen sharing session, even if another user started the session	✓ READ EXECUTE DELETE	✗	✗
Screen Sharing Support Session Disable Autolock Disable automatic endpoint locking after ending an unattended session that the user established	✗	✗	✗
Screen Sharing Support Session Options Set screen sharing options that do not have corresponding settings available in the ScreenMeet console[2]	✓ READ WRITE	✓ READ	✓ READ
Screen Sharing Support Session Unattended Establish unattended sessions with Windows endpoints that do not require endpoint user permission	✗	✗	✗
Screen Sharing TDS Integration User Interact with data from Tanium Data Service	✓ ACCOUNT	✓ ACCOUNT	✓ ACCOUNT

The permissions for these roles provide solution permissions for other solutions. To view the provided permissions, see Tanium Console User Guide: View effective role permissions.

© 2026 Tanium Inc. All Rights Reserved

Provided Screen Sharing platform content permissions

Permission	Integration Admin - ScreenMeet	Screen Sharing Agent	Integration Viewer - ScreenMeet
Action	✓ READ WRITE	✓ READ WRITE	✗
Filter Group	✓ READ	✗	✓ READ
Own Action	✓ READ	✓ READ	✗
Package	✓ READ	✓ READ	✓ READ
Plugin	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Sensor	✓ READ	✓ READ	✓ READ

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

© 2026 Tanium Inc. All Rights Reserved

Installing Direct Connect

Use the **Solutions** page to install Direct Connect and choose either automatic or manual configuration:

- **Automatic configuration with default settings**: Direct Connect 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 Direct Connect, see Import Direct Connect with default settings on page 32.
- **Manual configuration with custom settings**: After installing Direct Connect, you must manually configure required settings. Select this option only if Direct Connect requires settings that differ from the recommended default settings. For more information, see Import Direct Connect with custom settings on page 33.



Use the **Automatic configuration with default settings** option.

Before you begin

- Read the Release Notes.
- Review the Direct Connect requirements on page 15.
- If you are upgrading from a previous version, see Upgrade Direct Connect.
- Assign the correct roles to users for Direct Connect. Review the User role requirements on page 23.
  - To import the Direct Connect solution, you must be assigned the Administrator reserved role.
  - To configure the Tanium Direct Connect action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group** write permission.
- Determine if some endpoints connect to the Module Server through a Tanium™ Zone Server. To enable connections to endpoints through a Zone Server, you must configure a Zone Proxy after you import Direct Connect. For more information, see Manage a Tanium™ Zone Proxy on page 40.

Import Direct Connect with default settings

You can set the Direct Connect action group to target the **No Computers** filter group by enabling restricted targeting before importing Direct Connect. This option enables you to control tools deployment through scheduled actions that are created during the import and that target the Tanium Direct Connect 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 Direct Connect with automatic configuration, the following default settings are configured:

© 2026 Tanium Inc. All Rights Reserved

Default values for Direct Connect settings

Setting	Default Value
Tanium Direct Connect action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group
Fully Qualified Domain Name for the Module Server	The **Fully Qualified Domain Name** setting is set to the first-detected IPv4 address that is closest to the Tanium Server IP address. This is often the IP address of the Module Server. After the initial installation and configuration completes, you can verify this value and update it if needed: go to **Shared Services > Direct Connect** and click Settings **> Endpoint Connection**. If the Module Server has multiple IP addresses or FQDNs that different endpoints use, or if your deployment has active and standby Module Servers, enter all IP addresses or FQDNs separated by commas. For example, groups of endpoints might connect to different interfaces or use different DNS servers. One of the IP addresses or FQDNs that you provide must resolve to the Module Server from all endpoints in all direct endpoint connections. Update the setting anytime the Module Server IP address or FQDN changes. For example, the IP address might change if you recover a Tanium Module Server Appliance from a backup. If the setting specifies an FQDN, you do not have to update the value when the IP address changes. In a deployment with active and standby Module Servers, you must update the setting after a failover if the setting value does not include the IP address or FQDN of the standby Module Server.

To import Direct Connect and configure default settings, see Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed: see Verify Direct Connect version on page 34.

Import Direct Connect with custom settings

To import Direct Connect 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. After the import, verify that the correct version is installed: see Verify Direct Connect version on page 34. Then configure settings as described in the following tasks:

- Configure the Direct Connect action group on page 37
- Configure Endpoint Connection settings on page 37
- Configure certificates on page 38

Manage solution dependencies

When you start the Direct Connect workbench for the first time, the Tanium Server checks whether all the Tanium modules and shared services (solutions) that are required for Direct Connect are installed at the required versions. The Direct Connect workbench cannot load unless all required dependencies are installed. If you selected **Tanium Recommended Installation** when you imported Direct Connect, the Tanium Server automatically imported all your licensed solutions at the same time. Otherwise, if you manually imported Direct Connect and did not import all its dependencies, Tanium Console displays a banner that lists the dependencies and the required versions. For more information, see Solution dependencies.

© 2026 Tanium Inc. All Rights Reserved

1. Install the dependencies as described in Tanium Console User Guide: Import or update specific solutions.
2. From the Main menu, go to **Shared Services > Direct Connect** to open the Direct Connect **Overview** page and verify that the Console no longer displays a banner to list missing dependencies.

Upgrade Direct Connect

For the steps to upgrade Direct Connect, see Tanium Console User Guide: Install a Tanium release update. After the upgrade, verify that the correct version is installed: see Verify Direct Connect version on page 34.

For the steps to upgrade a Direct Connect Zone Proxy, see Install or upgrade the Direct Connect Zone Proxy on page 40.

Verify Direct Connect version

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

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

© 2026 Tanium Inc. All Rights Reserved

Configuring Direct Connect

Configure Tanium Direct Connect to suit the requirements of your organization. For example, assign the predefined Direct Connect user roles to users who must perform Direct Connect operations.

If you did not install Direct Connect with the **Apply All Tanium recommended configurations**, you must manually enable and configure certain features, such as endpoint connection settings. Additionally, if you want to enable connections to endpoints through a Tanium™ Zone Server, you must Manage a Tanium™ Zone Proxy on page 40.

Restricted targeting

You can set the Direct Connect action group to target the **No Computers** filter group by enabling restricted targeting before importing Direct Connect. This option enables you to control tools deployment through scheduled actions that are created during the import and that target the Tanium Direct Connect 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.

Default settings

When you import Direct Connect with automatic configuration, the following default settings are configured:

Default values for Direct Connect settings

Setting	Default Value
Tanium Direct Connect action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group
Fully Qualified Domain Name for the Module Server	The **Fully Qualified Domain Name** setting is set to the first-detected IPv4 address that is closest to the Tanium Server IP address. This is often the IP address of the Module Server. After the initial installation and configuration completes, you can verify this value and update it if needed: go to **Shared Services > Direct Connect** and click Settings **> Endpoint Connection**. If the Module Server has multiple IP addresses or FQDNs that different endpoints use, or if your deployment has active and standby Module Servers, enter all IP addresses or FQDNs separated by commas. For example, groups of endpoints might connect to different interfaces or use different DNS servers. One of the IP addresses or FQDNs that you provide must resolve to the Module Server from all endpoints in all direct endpoint connections. Update the setting anytime the Module Server IP address or FQDN changes. For example, the IP address might change if you recover a Tanium Module Server Appliance from a backup. If the setting specifies an FQDN, you do not have to update the value when the IP address changes. In a deployment with active and standby Module Servers, you must update the setting after a failover if the setting value does not include the IP address or FQDN of the standby Module Server.

© 2026 Tanium Inc. All Rights Reserved

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

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

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

IMPORTANT

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

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

NOTE

For information about how to install Endpoint Configuration, see 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 Direct Connect, see User role requirements on page 23. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.

IMPORTANT

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

© 2026 Tanium Inc. All Rights Reserved

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

If you enabled configuration approvals, you must approve the deployment of Direct Connect tools in Endpoint Configuration before they deploy to endpoints.

Configure Direct Connect

Configure the Direct Connect action group

Importing the Direct Connect module automatically creates an action group to target specific endpoints. If you did not use automatic configuration or you enabled restricted targeting when you imported Direct Connect, the action group targets **No Computers**.

If you used automatic configuration and restricted targeting was disabled when you imported Direct Connect, configuring the Direct Connect action group is optional.

Select the computer groups to include in the Direct Connect action group.



Set the action group to **All Computers**, unless you want to block direct connections to some endpoints.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. In the **Name** column, click **Tanium Direct Connect**.
3. Select the computer groups that you want to include in the action group.
4. Select Boolean **AND** or **OR** logic if you select multiple computer groups.
5. Click **Save**.

Configure Endpoint Connection settings

Specify **Endpoint Connection** settings to define the fully qualified domain name (FQDN) or IP address for connecting to the Tanium Module Server and the port to use for connections.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services > Direct Connect** and then click Settings **> Endpoint Connection**.
2. Configure the following settings and click **Save**.

Endpoint connection settings

Setting	Description
Fully Qualified Domain Name	Enter the IP address or FQDN of the Module Server. If the Module Server has multiple IP addresses or FQDNs that different endpoints use, or if your deployment has active and standby Module Servers, enter all IP addresses or FQDNs separated by commas. For example, groups of endpoints might connect to different interfaces or use different DNS servers. One of the IP addresses or FQDNs that you provide must resolve to the Module Server from all endpoints in all direct endpoint connections. Update the setting anytime the Module Server IP address or FQDN changes. For example, the IP address might change if you recover a Tanium Module Server Appliance from a backup. If the setting specifies an FQDN, you do not have to update the value when the IP address changes. In a deployment with active and standby Module Servers, you must update the setting after a failover if the setting value does not include the IP address or FQDN of the standby Module Server.
Port	Modify the **Port** if endpoints use a port other than the default 17475 to connect to the Module Server. Make sure that applicable firewall configurations allow incoming connections to this port.
Bypass Action Lock	Select this option to allow Direct Connect to make connections to endpoints with action lock turned on. NOTE For more information about action locks, see Tanium Console User Guide: Managing action locks.

If the **Fully Qualified Domain Name** validates successfully, success messages are shown:

```
The endpoint connection settings saved successfully.
Content build is in progress. Connection settings will deploy to endpoints once complete.
```

If an error occurs, correct the FQDN and re-save.

If the information validates and saves successfully, Tanium Direct Connect creates packages for each supported operating system with the configuration information that is needed to use Tanium Direct Connect. A scheduled action deploys these packages to the **Tanium Direct Connect** action group.

Configure certificates

Configure certificates to authenticate connections between the Tanium Module Server and endpoints.

1. From the Main menu, go to **Shared Services > Direct Connect** and click Settings **> Certificates**.

   For both Module Server and Tanium Client certificates, you cannot change the default **Install a new certificate** option during initial configuration.

   A **Server Certificate** is generated and installed to authenticate the Module Server when an endpoint starts a connection. After a certificate is installed on the Module Server, the **Certificates** tab shows the certificate expiration date.

© 2026 Tanium Inc. All Rights Reserved

A **Client Certificate** is generated, installed, and deployed to endpoints to authenticate that they are managed endpoints (their Tanium Clients have registered) with permission to connect to the Module Server. After a certificate is installed, the **Certificates** tab shows the certificate expiration date.

2. Click **Renew** if you need to renew a **Server Certificate** or **Client Certificate**, and then click **Save**.

Set up Direct Connect users

You can use the following set of predefined user roles to set up Direct Connect users.

To review specific permissions for each role, see User role requirements on page 23.



On installation, Direct Connect creates a **Direct Connect** user to automatically manage the Direct Connect service account. Do not edit or delete the **Direct Connect** user.

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

Direct Connect Administrator

Assign the **Direct Connect Administrator** role to users who manage the configuration and deployment of Direct Connect functionality to endpoints.

This role can perform the following tasks:

- Configure Direct Connect settings
- Test direct endpoint connections
- View own active endpoint sessions

Direct Connect User

Assign the **Direct Connect User** role to users who test direct endpoint connections and who can review their own active endpoint sessions.

Direct Connect Read Only User

Assign the **Direct Connect Read Only User** role to users who can only review their own active endpoint sessions.

Direct Connect Satellite Operator

Assign the **Direct Connect Satellite Operator** role to users who create and manage satellites.

Direct Connect File Modifier

Assign the **Direct Connect File Modifier** role to users who view, export, and delete files and directories in endpoint file systems through the Endpoint Details page (**File Browser** button) of the Tanium Reporting workbench. For more information, see Tanium Investigate User Guide: Browsing the file system on an endpoint.

© 2026 Tanium Inc. All Rights Reserved

Direct Connect Endpoint Configuration Approver

Assign the **Direct Connect Endpoint Configuration Approver** role to a user who approves or rejects Direct Connect configuration items in Tanium Endpoint Configuration.

NOTE

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

Manage a Tanium™ Zone Proxy

The Tanium Zone Proxy is a service that is hosted on a Tanium Zone Server, which you deploy in the DMZ. Use a Zone Server if the network security policies of your organization prohibit Tanium Clients in an external, untrusted network from initiating connections with Tanium Core Platform servers such as the Tanium Module Server. The Zone Proxy is required to enable direct connections between external Clients and the Module Server over the configured Direct Connect port (the default is 17486).

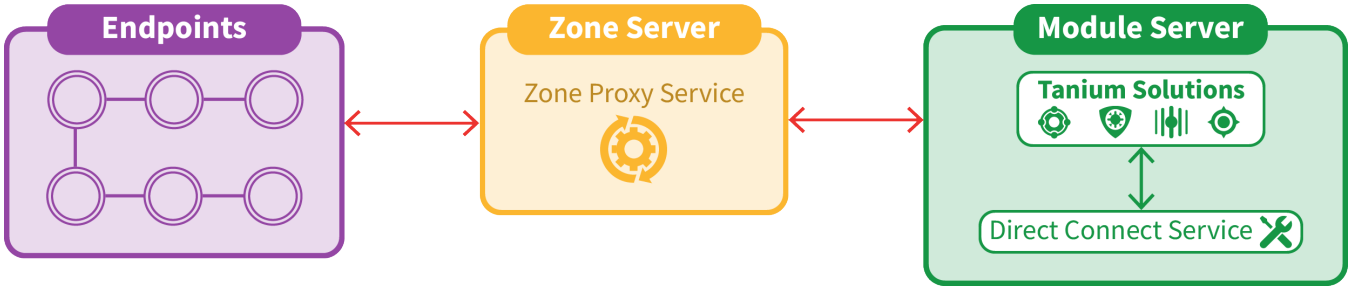
BEST PRACTICE

Configuring a Zone Proxy is optional but a best practice.

IMPORTANT

For best results, do not use a load balancer in front of your Zone Server. If you must use a load balancer, configure it for persistent TCP connections. The port that you configure in the Zone Proxy for connections to external endpoints must be open on the load balancer.

Direct Connect to Zone Server connections



Install or upgrade the Direct Connect Zone Proxy

Perform the following tasks before you install or upgrade the Direct Connect Zone Proxy:

- Contact Tanium Support on page 72 to obtain the Direct Connect Zone Proxy Installer file for your Zone Server operating system.
- Confirm that all required ports are available. For more information, see Host and network security requirements.

Perform the following steps to install or upgrade the Zone Proxy:

© 2026 Tanium Inc. All Rights Reserved

1. Copy the Zone Proxy Installer to the Zone Server.
2. Run the Zone Proxy Installer on the Zone Server:
    - **Windows**: Perform the steps in the **Tanium Direct Connect Zone Proxy Setup Wizard**.
    - **TanOS**: The available installation or upgrade method depends on the TanOS version:
        - **1.5.2 - 1.5.4**: You must use the TanOS shell to install the Direct Connect Zone Proxy.
        - **1.5.5 or later**: You can install the Direct Connect Zone Proxy through the Tanium Operations menu on the Zone Server appliance. For more information, see Appliance Deployment Guide: Installing and managing a Direct Connect Zone Proxy.
3. (Initial installations only) Copy the provision secret and certificate, which are known as the *provision payload*. You use the provision payload when you Configure the Direct Connect Zone Proxy on page 43.

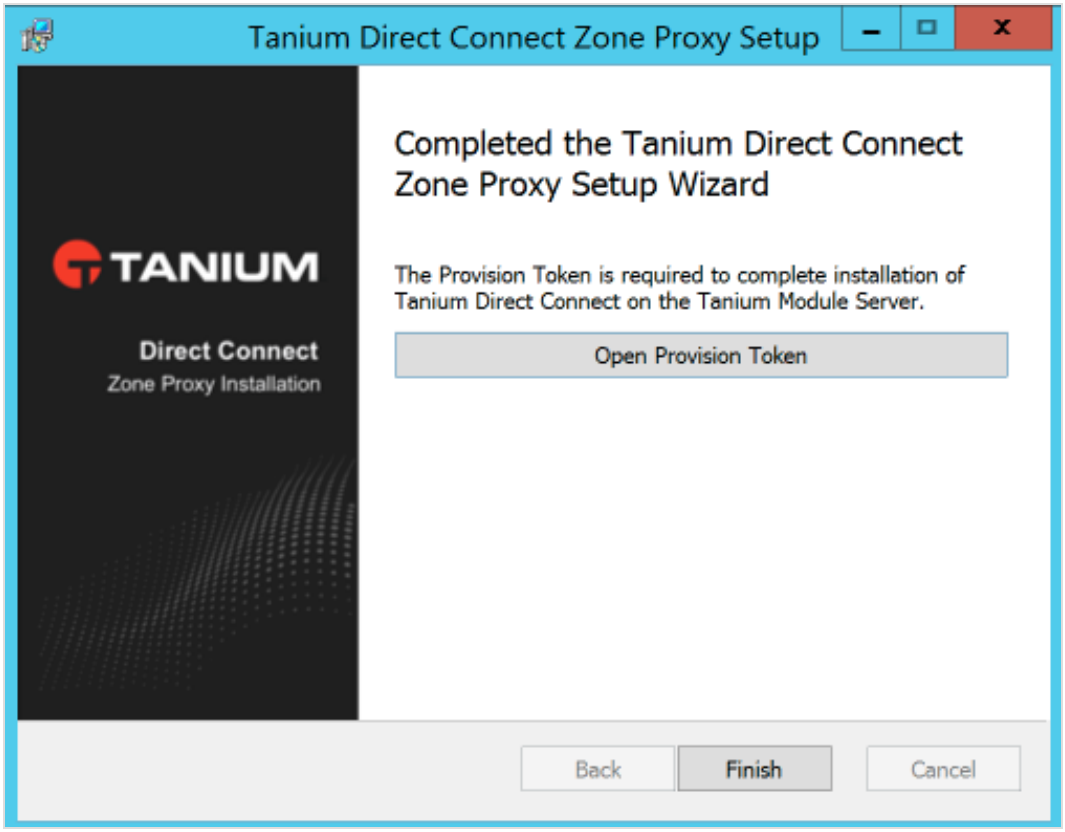
   The provision payload is stored in `provision.txt`, which is located in the following directories:
    - **TanOS**:
      `<Tanium Installation Directory>/TaniumDirectConnectZoneProxy/settings/PROVISION.txt`

      During the installation process on TanOS, the `Provision Secret` and `Certificate` also appear in the console where you run the installation. You can copy the `Provision Secret` and `Certificate` from the console or from the `PROVISION.txt` file.

© 2026 Tanium Inc. All Rights Reserved

- **Windows**: `<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\settings\PROVISION.txt`

  At the end of the installation on Windows, click **Open Provision Token** to open `PROVISION.txt`. You can copy the `Provision Secret` and `Certificate` from this file.



The following is an example of the provision payload:

```
-----BEGIN PROVISION SECRET-----
+EPQlEuUloBizbexjtshLuoxhNHA0JuMeOAEwFq/OKpEk6+jUJbFPx8Dol+vL22F
geNrd4/+wbsZwTgL3EUsqg==
-----END PROVISION SECRET-----
-----BEGIN CERTIFICATE-----
MIIC7TCCAdWgAwIBAgIgAwi2sO+h6dq/XIroZ1vK96/sHqxcMRWvkLXFrZrb5pAw
r3AxeSY2NpzDmVcQFNlYUhyR8QOr5hRE7AF9gGKDei6A
-----END CERTIFICATE-----
```

© 2026 Tanium Inc. All Rights Reserved

> **NOTE** The content in the preceding example is intentionally truncated and your configuration will fail if you use the example values in your environment. You must use the values from your installation for the certificate pinning to work.

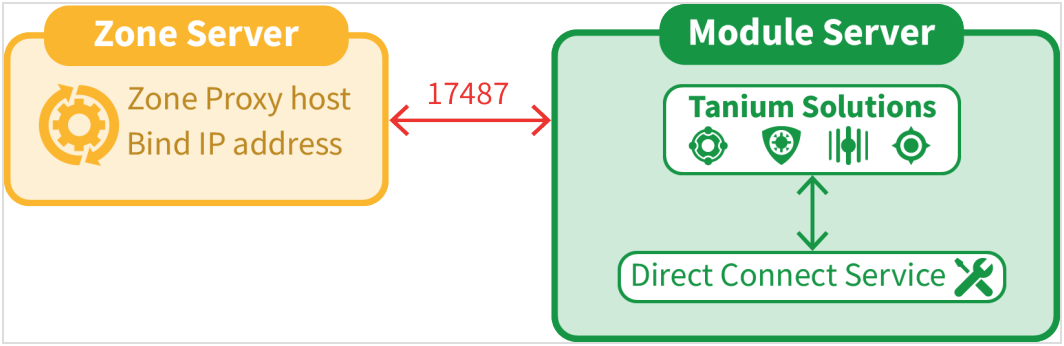
After an initial installation, you must Configure the Direct Connect Zone Proxy on page 43. After an upgrade, no further configuration is necessary.

Configure the Direct Connect Zone Proxy

Configuring a Direct Connect Zone Proxy is required only after you initially install it, not after an upgrade.

> **NOTE** Due to the provisioning process, you cannot modify existing Zone Proxy configurations. If necessary, you can delete the configuration and recreate it with different values. To delete a configuration, go to **Shared Services > Direct Connect > Zone Proxies**, hover over the configuration, and click **Delete**.

1. From the Main menu, go to **Shared Services > Direct Connect > Zone Proxies** and click **Add Zone Proxy**.
2. Enter a **Name** to identify the Zone Proxy.
3. In the **Provision Payload** field, paste the `Provision Secret` and `Certificate` that you saved during installation.
4. Configure the **Module Server Connection**:



Zone Server to Module Server connection settings

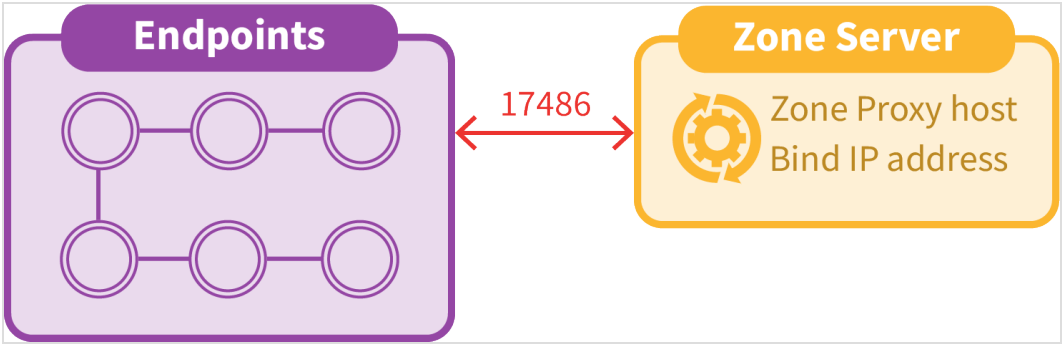
Setting	Description
Zone Proxy Host	Enter the internal IP address of the Zone Server that is accessible from the Module Server, or a host name or FQDN that the Module Server can resolve to an accessible address, such as `DMZZoneServer.internal.local`. You can enter only one value.

© 2026 Tanium Inc. All Rights Reserved

Zone Server to Module Server connection settings (continued)

Setting	Description
Bind IP Address	Enter the IPv4 network interface binding that the Zone Server uses to listen for Module Server connections. To listen on all interfaces, enter `0.0.0.0`.
Port	Enter the port that the Zone Server uses to listen for Module Server connections. The default value is `17487`.

5. Configure the **Endpoint Connection** and click **Save**:



Zone Server to endpoints connection settings

Setting	Description
Zone Proxy Host	Enter the public IP address of the Zone Server that is accessible from endpoints, or an FQDN that endpoints can resolve to the public address, such as `MyZoneServer.company.com`. If the Zone Server has multiple IP addresses or FQDNs that different endpoints use, enter all IP addresses or FQDNs separated by commas. For example, groups of endpoints might connect to different interfaces or use different DNS servers. In a deployment with multiple Zone Servers, you can add the IP addresses or FQDNs of all the Zone Servers.
Bind IP Address	Enter the IPv4 network interface binding that the Zone Server uses to listen for endpoint connections. To listen on all interfaces, enter `0.0.0.0`.
Port	Enter the port that the Zone Server uses to listen for endpoint connections. The default value is `17486`.

On the **Zone Proxies** page, the **Status** column shows the status of the Zone Proxy that you added. When the configuration is complete, the status is `Connected`. The page also shows the status and activity for existing Zone Proxies.

Uninstall the Direct Connect Zone Proxy

The steps to remove the Tanium Direct Connect Zone Proxy depend on your Tanium infrastructure:

- **Windows**: Sign in to the Tanium Zone Server as a user with Local Administrator rights, open **Control Panel > Programs > Programs and Features**, select the Tanium Direct Connect Zone Proxy, and click **Uninstall**.
- **TanOS**: See Appliance Deployment Guide: Remove the Direct Connect Zone Proxy.

© 2026 Tanium Inc. All Rights Reserved

Reviewing endpoint sessions

The Direct Connect **Overview** page shows details about your Direct Connect sessions that are active or pending (waiting to connect) across all Tanium solutions. Review the sessions to check which endpoints connect as expected or to find anomalies. For example, a prolonged `Waiting` status might indicate the need to troubleshoot outdated tools or connectivity issues for an endpoint.



The connections list does not include connections that other users initiated.

To review historical endpoint sessions, see Working with audit logs on page 61.

1. From the Main menu, go to **Shared Services > Direct Connect > Overview** and go to the **Direct Connect to an Endpoint** section.
2. In the **Direct Connections** tab, review the details for each session:
   - **Computer Name**: Endpoint computer name. Hover over the Information icon to see the **Platform**, connection **Latency**, and **Time to connect** for the endpoint.
   - **Tanium Client ID**: Endpoint ID that is used for the connection.
   - **IP Address**: Endpoint IP Address.
   - **Direct Connect Proxy**: Name of the Tanium Zone Proxy if you configured it. For more information, see Manage a Tanium™ Zone Proxy on page 40.
   - **Direct Connect Status**: Current status of the session. Active sessions show `Connected` status.
   - **Duration**: Time passed since the connection was first established from the endpoint.
   - **Last Message**: Time passed since the last message was received from the endpoint.

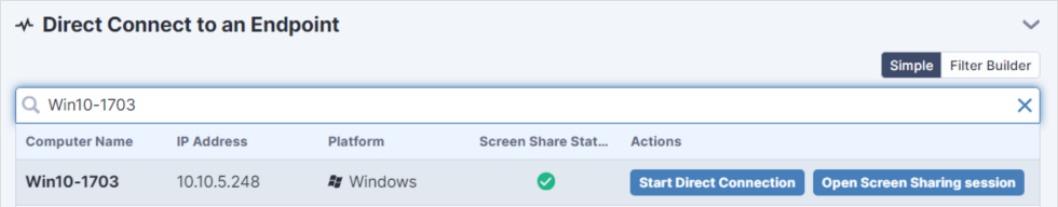
If the **Direct Connections** tab does not show all the expected sessions, or the **Direct Connect Status** indicates possible issues, see Troubleshoot endpoint connection issues on page 67.

© 2026 Tanium Inc. All Rights Reserved

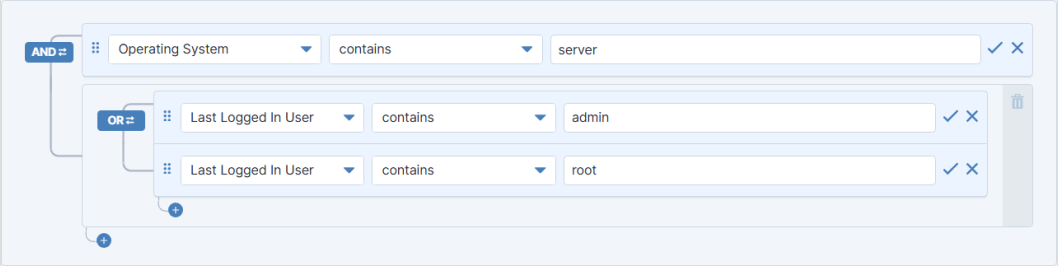
Testing direct endpoint connections

Test direct connections to endpoints to troubleshoot connection issues and to ensure that Tanium solutions can connect with endpoints during operations. You test connections by starting them.

1. From the Main menu, go to **Shared Services > Direct Connect > Overview**.
2. Go to the **Direct Connect to an Endpoint** section and select a search option to find the endpoint for which you want to start a connection:
   - **Simple**: Enter the IP address or computer name of the endpoint.



   - **Filter Builder**: Configure one or more sensor-based filters to find the endpoint. Select a sensor (such as **Last Logged In User**), select an operator (such as **contains**), enter the value to match, and click Apply. For each additional filter, hover over Add, select **Add Row** or **Add Group**, and repeat the configuration steps. Direct Connect processes group (nested) filters and applies Boolean AND/OR logic in the same way that Tanium Interact does for question results filters, and the configuration steps are similar. For more information, see Tanium Interact User Guide: Filter by advanced conditions.



3. If the **Computer Name** column shows a Warning icon for the endpoint, hover over the icon to show a tooltip that indicates one or both of the following states. Otherwise, skip to the next step.

Warning	Details
The most recent version of the configuration is not installed	The configuration has changed from what was last installed on the endpoint. The endpoint might not be able to connect depending on what was changed.
The Direct Endpoint Connection tools are not installed	Direct Connect client extensions are not installed or are not running.

© 2026 Tanium Inc. All Rights Reserved

These warning conditions usually resolve automatically if you wait for Tanium Endpoint Configuration to deploy the latest configuration and tools to endpoints. To troubleshoot configuration or tools issues that persist, see Verify endpoint tools on page 69 and Verify the configuration version on page 69.

4. Click **Start Direct Connection** in the row for the target endpoint.

   If the connection succeeded, the **Direct Connections** grid shows the endpoint with a **Direct Connect Status** of Connected .

   If the connection failed, see Troubleshoot endpoint connection issues on page 67. If your deployment uses the Direct Connect Zone Proxy, see also Troubleshoot Zone Proxy connection issues on page 68.

© 2026 Tanium Inc. All Rights Reserved

Working with screen sharing

You can open a screen sharing session to perform troubleshooting on remote endpoints. Help desk agents can use the screen sharing tools to escalate between L1 and L2 support in the same screen sharing session.

IMPORTANT

To enable this functionality, you must purchase the ScreenMeet offering. With the ScreenMeet offering provided through Tanium, you must initiate all interactions with ScreenMeet through Tanium Console. Contact Tanium for details.

Requirements

- Obtain Screen Sharing per-operator licenses based on the number of Tanium Console operators you expect to establish screen sharing sessions.
    - A per-operator license is allocated to each Tanium Console operator establishing a screen sharing session or accessing the ScreenMeet console from Tanium Console. Each Tanium Console operator can create unlimited concurrent screen sharing sessions.
    - The license allocation lasts for 30 days and counts as an active operator license. The 30-day license allocation restarts each time that a Tanium Console operator establishes a screen sharing session or opens the ScreenMeet console.
    - If the active operator license count exceeds your total per-seat license count, additional Tanium console operators cannot establish a screen sharing session.
- Set up screen sharing users in Tanium. For more information about permissions provided by these roles, see Screen Sharing user role permissions on page 28. For more information about configuring permissions to establish unattended screen sharing sessions, see Configure personas to establish unattended screen sharing sessions on page 50.
    - **Screen Sharing Administrator**: With this role, a user can change settings, features and policies; access data; and join active sessions created by active users. A user assigned this role in Tanium is automatically assigned the **ScreenMeet Admin** role in ScreenMeet and can access the ScreenMeet console to configure ScreenMeet settings for the organization using a magic link accessed from the Direct Connect settings. For more information, see Configure ScreenMeet settings.
    - **Screen Sharing Agent**: With this role, a user can start sharing sessions and use standard ScreenMeet features. A user assigned this role in Tanium is automatically assigned the **ScreenMeet Agent** role in ScreenMeet. This role includes the **Screen Sharing Console** permission, which allows access to the ScreenMeet console without the ability to modify organizational settings using a magic link accessed from the Direct Connect settings.
    - **Screen Sharing Support Session Unattended Execute** permission: Establish unattended sessions with Windows endpoints that do not require endpoint user permission. After the user ends the unattended session, the endpoint locks by default. This permission is not assigned to any default role.

© 2026 Tanium Inc. All Rights Reserved

- **Screen Sharing Support Session Disable Autolock Execute** permission: Disable automatic endpoint locking after ending an unattended session that the user established. This permission requires the **Screen Sharing Support Session Unattended Execute** permission to establish unattended sessions. This permission is not assigned to any default role.

  Use a least-privilege model for your screen sharing users.

- Verify endpoint operating systems. For more information, see Screen sharing OS support on page 17.
- Verify network requirements.
  - Configure the host and network security requirements. For more information, see Host and network security requirements.
  - Allow ScreenMeet application traffic through port 443/TCP and 443/UDP. ScreenMeet application traffic goes through TLS-encrypted connections.
  - The endpoints in your environment require access to certain URLs to establish screen sharing sessions. If security software is deployed in the environment to monitor and block unknown URLs, your security administrator might need to allow the hosts and IP addresses listed at ScreenMeet Documentation: Firewall configuration / whitelisting and ScreenMeet Documentation: Egress IP Addresses, and allow the following URL.

    Allowing this URL is not required for Direct Connect.

    Third-party URL required for Screen Sharing

URL	Source	Port	Protocol	Description
`*.screenmeet.com`	ScreenMeet client	443	TCP / UDP	Required for endpoints to establish screen sharing connections

    For the best results, allow traffic from the preceding URL to bypass proxy servers if you deployed such servers in your network. Screen sharing traffic that passes through proxy servers negatively impacts performance. For more information, see ScreenMeet Documentation: ScreenMeet Enterprise Deployment Guide.

  - Ensure that the ScreenMeet security requirements are configured. For more information, see ScreenMeet Documentation: Security.
  - Create and sign in to a Tanium Account to link the Tanium instance where you will use Screen Sharing. If your Tanium license includes Screen Sharing, it is automatically configured for your Tanium instance when your account is linked.

    For more information, see Tanium Account User Guide: Creating and managing your Tanium Account.

© 2026 Tanium Inc. All Rights Reserved

Integrate with ServiceNow

Integrate Screen Sharing with your ServiceNow instance to update ServiceNow tickets with audit logs from a related screen sharing session. With this integration, you have an additional option when opening screen sharing sessions: **Send audit log to ServiceNow**. If you select this option, you can add the ServiceNow Ticket ID that is associated with the screen sharing session.

1. From the Main menu, go to **Shared Services > Direct Connect**. Click Settings and then click **Screen Sharing**.
2. In the **ServiceNow Configuration** section, provide the **Host URL**, **Username** and **Password** for your ServiceNow instance. Click **Save**.

> NOTE
> The ITIL role in ServiceNow is required to integrate activities from ServiceNow.

For the steps to open a screen sharing session, see Open an endpoint screen sharing session on page 51. After you close a screen sharing session where you sent the audit log to ServiceNow, you can check the status of the sync on the **Audit Log** page in Direct Connect. From the Main menu, go to **Shared Services > Direct Connect> Audit Log > Screen Sharing Sessions**. Audit logs can have the following sync statuses:

Status	Meaning
Pending	The session is queued for session log syncing.
In Progress	Session log syncing is in progress.
Complete	The session log was successfully synced with ServiceNow.
Error	The session log failed to sync with ServiceNow.

Configure personas to establish unattended screen sharing sessions

The ability to establish unprompted (unattended) screen sharing sessions is intentionally limited by default to only Tanium administrators to prevent misuse. The default **Integration Admin - ScreenMeet**, **Screen Sharing Agent**, and **Integration Viewer - ScreenMeet** user roles do not have this permission. In addition, Tanium Console operators that establish an unattended screen sharing session with an endpoint and then close the session lock the endpoint by default.

You can configure a custom role and persona with permissions to establish unattended screen sharing sessions with an endpoint, and leave the endpoint unlocked after the unattended screen sharing session is closed. You can restrict the persona to a given computer group, and assign the persona to only certain Tanium Console operators.

For more information about creating a custom role, see Tanium Console User Guide: Configure a custom role. For more information about creating a persona, see Tanium Console User Guide: Create a persona.

1. From the Main menu, go to **Administration > Permissions > Roles** and click **New Role**.
2. Specify a **Role Name**, such as `Screen Sharing Unattended Role`.
3. Set the **Permission Type** to **Allow**.

© 2026 Tanium Inc. All Rights Reserved

4. Select the **Screen Sharing Support Session Unattended Execute** permission to allow users to establish unattended screen sharing sessions.
5. If you want a Tanium Console operator to have the option to leave an endpoint unlocked after closing an unattended screen sharing session, select **Screen Sharing Support Session Disable Autolock Execute**.
6. Click **Save**.
7. From the Main menu, go to **Administration > Permissions > Personas** and click **New Persona**.
8. Specify a persona **Name**, such as `Screen Sharing Unattended Persona`.
9. Click **Manage Roles**.
10. Select the following roles:
    - **Interact Basic User** for Interact access
    - **Screen Sharing Agent** for screen sharing access
    - **Screen Sharing Unattended Role** (or the name of the role you created) for unattended screen sharing session options
11. Click **Apply**.
    The Permissions table displays the union of permissions from these roles, including **Screen Sharing Support Session Unattended Execute** and, if you configured it, **Screen Sharing Support Session Disable Autolock Execute**.
12. Expand the **Computer Groups** section and click **Manage Computer Groups**.
13. Select the computer groups that contain the endpoints to which you want to establish unattended screen sharing sessions, then click **Select**.
14. If you configured a user group to contain your Tanium Console operators that will establish screen sharing sessions with endpoints, such as a help desk-related user group, expand the **User Groups** section and click **Manage User Groups**.
15. Select the user group, then click **Select**.
16. If you want to configure individual users to establish screen sharing sessions with endpoints, expand the **Users** section and click **Manage Users**.
17. Select the users, then click **Select**.
18. Click **Save**.
    Tanium Console operators assigned this persona can establish unattended screen sharing sessions when this persona is active.

Open an endpoint screen sharing session

To open a screen sharing session, you must have access to the endpoint in Tanium, and the endpoint must have Screen Sharing tools installed using Tanium Endpoint Configuration unless you are connecting to an endpoint without a Tanium Client. After you initiate a connection, the connection screen for the endpoint shows the status. Establishing connections can take between one and three minutes.

© 2026 Tanium Inc. All Rights Reserved

NOTE

After installing or upgrading Screen Sharing or Endpoint Configuration, or adding new endpoints to your environment, it might take several minutes for Endpoint Configuration to install Screen Sharing tools on an endpoint. If an endpoint does not have Screen Sharing tools installed, attempts to establish a screen sharing session with that endpoint fail. Wait several minutes for installation of Screen Sharing tools and then try again. For more information on Endpoint Configuration and endpoint tools, see Tanium Endpoint Configuration User Guide: Managing endpoint tools.

You can establish an attended connection, which requires the endpoint user to accept the screen sharing connection, or an unattended connection, which allows you to establish the connection without endpoint user permission.

IMPORTANT

Screen Sharing sessions are only established on endpoints that are included in the Screen Share action group. Therefore, the **Open Screen Sharing** button is only available for endpoints that are included in the Screen Share action group. By default, the action group is set to All Computers.

NOTE

The first time a Tanium Console operator establishes a screen sharing session with a macOS endpoint, the endpoint user must select **ScreenMeetSupport** in the **Screen Recording** and **Accessibility** permissions in **System Settings**, then click **Later** when prompted. For more information, see ScreenMeet Documentation: Connecting to Mac devices.

During the connection process, a ScreenMeet executable file is deployed to the endpoint with a Tanium Action. This executable file connects to the ScreenMeet services and establishes a connection with Tanium. The connection behavior depends on the endpoint operating system and whether you establish an attended or unattended connection:

- For attended connections to Windows endpoints, the endpoint user must accept the screen sharing session to continue. This establishes an active session and the Tanium Console operator takes control.
- For attended connections to macOS endpoints, if the endpoint user has allowed the proper screen sharing permissions on the endpoint, a view-only session is initially established. The Tanium Console operator must request control, and the endpoint user must accept, which then allows the operator to take control.
- For unattended connections to Windows endpoints, a new session is created without endpoint user permission and the Tanium Console operator takes control.
- Unattended connections to macOS endpoints are not supported.

IMPORTANT

If PowerShell is in the `ConstrainedLanguage` language mode on Windows endpoints, the Screen Sharing script to open a user session (`<Tanium Client installation directory>\Tools\ScreenSharing\start-session.ps1`), which is signed, must be allowed to run in `FullLanguage` mode through Windows Defender application control (WDAC) or other system policies.

© 2026 Tanium Inc. All Rights Reserved

NOTE

If no endpoint users are logged in to an endpoint and you establish an unattended connection, after you enter operating system login information, the session displays a disconnection message. Wait several seconds for the login process to complete and reestablish the connection.

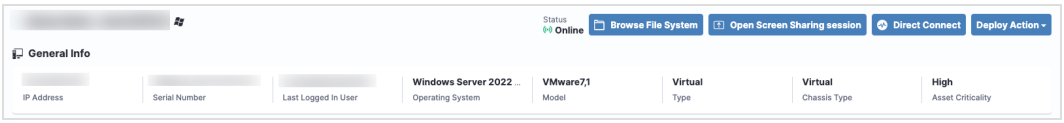
When you configure session recording in the ScreenMeet console (**Organization > Settings and Policies > Remote Support Features > Session Recording**), if you select:

- **Always**, the Tanium screen sharing session is always recorded.
- **Let the Agent Decide**, and the Tanium Console operator has the **Screen Sharing Product Options Read** permission, the Tanium Console operator has the option to record a screen sharing session. If the session is recorded, users have the option to disable recording before joining the session.
- **Never**, the Tanium screen sharing session is never recorded.

  For more information about configuring session recording, see ScreenMeet Docs: Remote Support Settings.

Open a screen sharing session from an endpoint

1. From the Tanium **Home** page, go to **Search for endpoints** and type the IP address or computer name of the computer, then click the computer name.
2. Click **Open Screen Sharing session**.



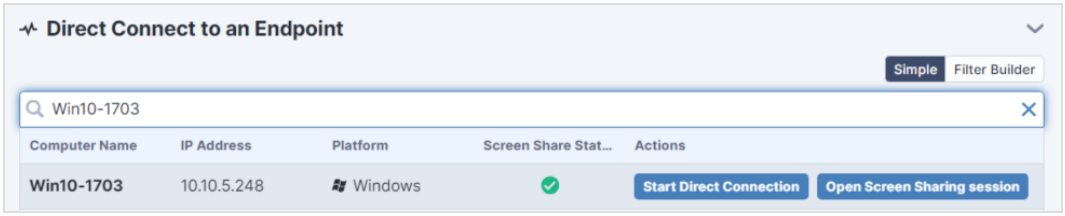
3. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** permission, you have the following options:
   - Select **Ask the endpoint user for permission** to start an attended session.
   - Clear **Ask the endpoint user for permission** to start an unattended session. After you end the session, by default, the endpoint locks.
4. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** and **Screen Sharing Support Session Disable Autolock Execute** permissions, then start an unattended session, you have the following options:
   - Select **Automatically lock after session ends** to lock the endpoint after you end the unattended session.
   - Clear **Automatically lock after session ends** to leave the endpoint unlocked after you end the unattended session.

© 2026 Tanium Inc. All Rights Reserved

5. (Windows and macOS endpoints) If you have the **Screen Sharing Product Options Read** permission, and **Let the Agent Decide** is selected in the ScreenMeet console **Session Recording** settings, you have the following options:
    - Select **Record session** to record the screen sharing session. Users have the option to disable recording before joining the session.
    - Clear **Record session** to establish the screen sharing session without recording.
6. Click **Open**.
7. A Tanium action deploys to the endpoint that includes an executable file that connects to ScreenMeet services. Establishing connections can take between one and three minutes. If the attended session is on an end user's computer, the user must accept the session on the endpoint to continue.
8. When the screen sharing session is connected, your screen switches to ScreenMeet in Tanium. You can use Support Tools in ScreenMeet to run Windows commands, tasks, and tools.

Open a screen sharing session from Direct Connect

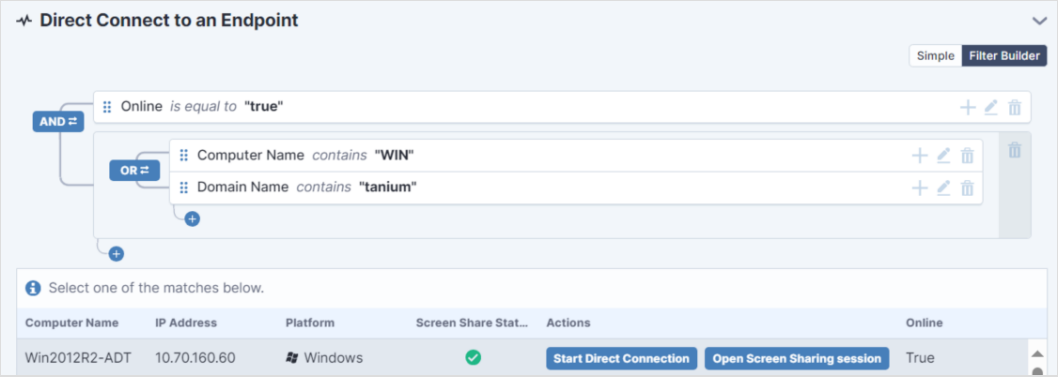
1. From the Main menu, go to **Shared Services > Direct Connect**.
2. Go to the **Direct Connect to an Endpoint** section and select a search option to find the endpoint for which you want to start a connection:
    - **Simple**: Enter the IP address or computer name of the endpoint.



    - **Filter Builder**: Configure one or more sensor-based filters to find the endpoint. Select a sensor (such as **Last Logged In User**), select an operator (such as **contains**), enter the value to match, and click Apply. For each additional filter, hover over Add, select **Add Row** or **Add Group**, and repeat the configuration steps. Direct Connect processes group (nested) filters and applies Boolean AND/OR logic in the same way that Tanium Interact does for question results filters, and the configuration steps are similar. For more information, see Tanium Interact User Guide: Filter by

© 2026 Tanium Inc. All Rights Reserved

advanced conditions.



3. In the result list, click **Open Screen Sharing session** for the endpoint.
4. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** permission, you have the following options:
    - Select **Ask the endpoint user for permission** to start an attended session.
    - Clear **Ask the endpoint user for permission** to start an unattended session. After you end the session, by default, the endpoint locks.
5. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** and **Screen Sharing Support Session Disable Autolock Execute** permissions, then start an unattended session, you have the following options:
    - Select **Automatically lock after session ends** to lock the endpoint after you end the unattended session.
    - Clear **Automatically lock after session ends** to leave the endpoint unlocked after you end the unattended session.
6. (Windows and macOS endpoints) If you have the **Screen Sharing Product Options Read** permission, and **Let the Agent Decide** is selected in the ScreenMeet console **Session Recording** settings, you have the following options:
    - Select **Record session** to record the screen sharing session. Users have the option to disable recording before joining the session.
    - Clear **Record session** to establish the screen sharing session without recording.
7. Click **Open**.
8. A Tanium action deploys to the endpoint that includes an executable file that connects to ScreenMeet services. Establishing connections can take between one and three minutes. If the attended session is on an end user's computer, the user must accept the session on the endpoint to continue.
9. When the screen sharing session is connected, your screen switches to ScreenMeet in Tanium. You can use Support Tools in ScreenMeet to run Windows commands, tasks, and tools.

Open a screen sharing session from Reporting



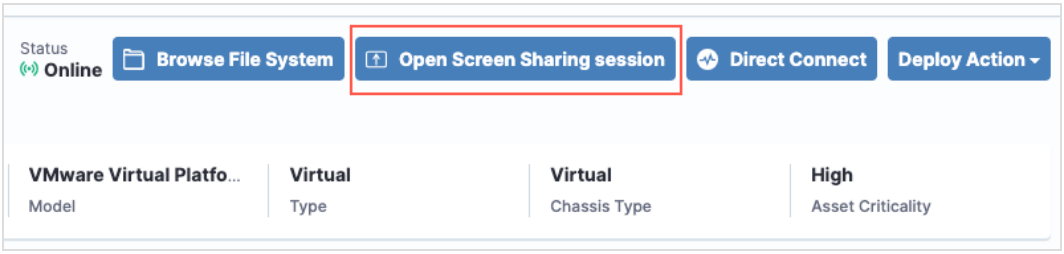
Tanium Reporting 1.43.40 or later is required to open screen sharing sessions in Reporting.

© 2026 Tanium Inc. All Rights Reserved

When you view, create, or edit a report that contains the **Computer Name** column, you can click an endpoint in the column to view details for the endpoint and to deploy an action to it. For information about Reporting, see Tanium Reporting User Guide: Working with a single endpoint.

1. Open a report that contains the **Computer Name** column.
2. Click Endpoint Details next to the name of an endpoint in the **Computer Name** column.

   An **Endpoint Details** dialog opens with basic details for the endpoint. If multiple endpoints have the same **Computer Name**, click Previous or Next in the **Multiple Results Found** banner to find the details for a specific endpoint.
3. Click **View Details** to open a page that shows a single endpoint view with detailed information.
4. Click **Open Screen Sharing session** to connect to the endpoint.



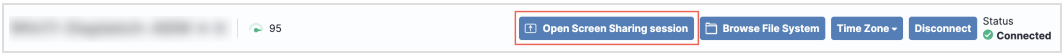
5. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** permission, you have the following options:
   - Select **Ask the endpoint user for permission** to start an attended session.
   - Clear **Ask the endpoint user for permission** to start an unattended session. After you end the session, by default, the endpoint locks.
6. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** and **Screen Sharing Support Session Disable Autolock Execute** permissions, then start an unattended session, you have the following options:
   - Select **Automatically lock after session ends** to lock the endpoint after you end the unattended session.
   - Clear **Automatically lock after session ends** to leave the endpoint unlocked after you end the unattended session.
7. (Windows and macOS endpoints) If you have the **Screen Sharing Product Options Read** permission, and **Let the Agent Decide** is selected in the ScreenMeet console **Session Recording** settings, you have the following options:
   - Select **Record session** to record the screen sharing session. Users have the option to disable recording before joining the session.
   - Clear **Record session** to establish the screen sharing session without recording.
8. Click **Open**.

© 2026 Tanium Inc. All Rights Reserved

9. A Tanium action deploys to the endpoint that includes an executable file that connects to ScreenMeet services. Establishing connections can take between one and three minutes. If the attended session is on an end user's computer, the user must accept the session on the endpoint to continue.
10. When the screen sharing session is connected, your screen switches to ScreenMeet in Tanium. You can use Support Tools in ScreenMeet to run Windows commands, tasks, and tools.

Open a screen sharing session from Performance

1. From the Main menu, go to **Modules > Performance > Direct Connect**. Search for the endpoint by IP address, computer name, or by using the Filter Builder.
2. From the results list, click the name of the endpoint in the **Computer Name** column.
3. After a connection is established, click **Open Screen Sharing session**.



4. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** permission, you have the following options:
    - Select **Ask the endpoint user for permission** to start an attended session.
    - Clear **Ask the endpoint user for permission** to start an unattended session. After you end the session, by default, the endpoint locks.
5. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** and **Screen Sharing Support Session Disable Autolock Execute** permissions, then start an unattended session, you have the following options:
    - Select **Automatically lock after session ends** to lock the endpoint after you end the unattended session.
    - Clear **Automatically lock after session ends** to leave the endpoint unlocked after you end the unattended session.
6. (Windows and macOS endpoints) If you have the **Screen Sharing Product Options Read** permission, and **Let the Agent Decide** is selected in the ScreenMeet console **Session Recording** settings, you have the following options:
    - Select **Record session** to record the screen sharing session. Users have the option to disable recording before joining the session.
    - Clear **Record session** to establish the screen sharing session without recording.
7. Click **Open**.
8. A Tanium action deploys to the endpoint that includes an executable file that connects to ScreenMeet services. Establishing connections can take between one and three minutes. If the attended session is on an end user's computer, the user must accept the session on the endpoint to continue.
9. When the screen sharing session is connected, your screen switches to ScreenMeet in Tanium. You can use Support Tools in ScreenMeet to run Windows commands, tasks, and tools.

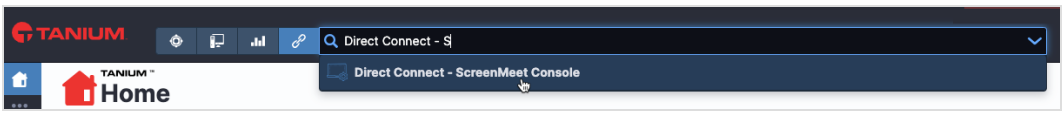
© 2026 Tanium Inc. All Rights Reserved

Open a screen sharing session with an endpoint that does not have a Tanium Client

You can open screen sharing sessions initiated from Tanium with unmanaged endpoints. This option can be helpful if you need to connect to the endpoint to troubleshoot issues with the Tanium Client. In this scenario, the user at the endpoint must manually download and install the ScreenMeet files since they cannot be distributed using Tanium. To use this method, you must be assigned a role that includes either the **Screen Sharing Console** or **Screen Sharing Console Admin** permission.

> NOTE
>
> Use this method to open a screen sharing session with a mobile device.

1. From the Tanium **Home** page, go to Navigate with quick links and enter **Direct Connect - ScreenMeet Console**. Click the **Direct Connect - ScreenMeet Console** quick link.



2. If you have more than one ScreenMeet product configured in your environment, click **Remote Support**.
3. Enter a **Description** for the session and configure the session options.

> NOTE
>
> Only the default ScreenMeet session options are available when you use this method to start the session.

4. Click **Create Session**.
5. Provide the user at the endpoint with the session URL and PIN code.
6. Ask the user at the endpoint to access the URL using a web browser and download and install the ScreenMeet client.
   For more information, see ScreenMeet documentation: Instructions to Person at End Point Device and ScreenMeet documentation: Providing Remote Support assistance to mobile devices.
7. After the user at the endpoint installs the ScreenMeet client and allows the session (if applicable), click **Enter Session** in the ScreenMeet console.

> NOTE
>
> The **Enter Session** button appears only when the user at the endpoint has installed the ScreenMeet client and allowed the session on the endpoint.

8. When the screen sharing session is connected, your screen switches to ScreenMeet in Tanium. You can use Support Tools in ScreenMeet to run Windows commands, tasks, and tools.

© 2026 Tanium Inc. All Rights Reserved

View and join screen sharing sessions

If you have **Integration Admin - ScreenMeet** role, you can see all sessions, and you can join sessions that were started by other Tanium Console operators.

If you have **Screen Sharing Agent** role, you can see and rejoin sessions that you started.



Multiple Tanium Console operators can join an endpoint screen sharing session, but only one operator at a time can take control of the session.

Join active sessions in the list of sessions

1. From the Main menu, go to **Shared Services > Direct Connect > Screen Sharing Sessions**. A list of sessions is displayed that includes active sessions.
2. Select one or more active sessions to an endpoint, then click **Join Screen Sharing** to join the sessions.

Search for an endpoint to join the active session

1. From the Main menu, go to **Shared Services > Direct Connect**. Search for the computer by IP address or computer name.
2. In the result list, click **Join Screen Sharing** for the endpoint.

View screen sharing session history

If you have **Integration Admin - ScreenMeet** role, you can go to the **Audit Log** page to view a history of screen sharing sessions.

From the Main menu, go to **Shared Services > Direct Connect > Audit Log**. Click the **Screen Sharing Sessions** tab.



The **Session Status** and **Ended At** audit log entry values might take up to 30 minutes to update.

End an endpoint screen sharing session

When you stop a session, screen sharing processes are removed from the endpoint.



For attended connections to macOS endpoints, after the Tanium Console operator ends the session, a message is displayed to the endpoint user that the session is closed. The endpoint user must close the ScreenMeet application before a Tanium Console operator can establish another connection to that endpoint.

© 2026 Tanium Inc. All Rights Reserved

End active sessions in the list of sessions

1. From the Main menu, go to **Shared Services > Direct Connect > Screen Sharing Sessions**. The tab contains a list of sessions that includes active sessions.
2. Select one or more endpoints and click **End Screen Sharing**.

Search for an endpoint to end the active session

1. From the Main menu, go to **Shared Services > Direct Connect**. Search for the computer by IP address or computer name.
2. In the result list, click **End Screen Sharing** for the endpoint.

Configure ScreenMeet settings

To configure settings in ScreenMeet, you must have a **Screen Sharing Administrator** role. Users with the **Screen Sharing Agent** role can access the ScreenMeet console using a magic link but cannot configure organizational settings.

1. From the Main menu, go to **Shared Services > Direct Connect**. Click Settings and then click **Screen Sharing**. The following options are available:
   - Click the **ScreenMeet console** link to use a magic link to open an authenticated session in the ScreenMeet console. In the ScreenMeet console, you can view session history, detailed logging of actions taken during a session, and so on. For more information, see ScreenMeet Docs: Remote Support Settings.

     NOTE

     Opening the ScreenMeet console from Tanium Console allocates a per-operator license to your user account, regardless of whether you establish a screen sharing session with this account.

   - In the **License Usage** section, click **Users** to expand the table and view a list of users allocated a per-user license, and the time that each user most recently signed in to Tanium Console.
   - Click **Export > Export to CSV** to export a comma-separated value (CSV) file containing the list of users.
   - Enter an **Alert Threshold** percentage to receive alerts in Tanium Console when the ratio of allocated per-user licenses to total licenses exceeds this percentage.

Contact support

If you require assistance with ScreenMeet tools, contact ScreenMeet. For more information, see ScreenMeet support.

© 2026 Tanium Inc. All Rights Reserved

Working with audit logs

The Direct Connect **Audit Log** page shows information about:

- Direct Connect sessions and actions that users performed on endpoints during the sessions. For example, you might use the page to check if Tanium Investigate users changed Windows registry keys on specific endpoints.
- Screen Sharing sessions that users initiated on endpoints.

You can create a connection in Tanium Connect to export the audit log to destinations such as an email, file (various formats), HTTP receiver, security information and event management (SIEM) system, or SQL server.

View the audit log

To view the Screen Sharing audit log, see View screen sharing session history on page 59.

To view the Direct Connect audit log:

1. From the Main menu, go to **Shared Services > Direct Connect > Audit Log** and select the **Direct Connections** tab.
   Certain columns are hidden by default, such as the **Command** that ran on an endpoint during a session.
2. (Optional) Click Customize Columns and select or clear columns based on the information that you want to see.

Export an audit log

Use Connect to export the Direct Connect audit log.

NOTE The export does not include the Screen Sharing audit log.

Before you begin

You must have access to Connect with the **Connect User** role. For more information, see Tanium Connect User Guide: Set up Connect users.

© 2026 Tanium Inc. All Rights Reserved

Create a connection

1. From the Main menu, go to **Modules > Connect > Connections** and click **Create Connection**.
2. In the **General Information** section, enter a **Name** and (optional) **Description** for your connection.
3. Expand the **Advanced** section and define the following settings:
    - **Log level**: By default, the logging is set to **Information**. To reduce the amount of logging, you can set the log level to **Warning**, **Error**, or **Fatal**.
    - **Minimum Pass Percentage**: Enter the minimum percentage of the expected rows that must be processed for the connection to succeed.
4. In the **Configuration** section, define the source and destination:
    - **Source**: Select **Tanium Direct Connect**.
    - **History Retrieval (Days)**: Enter the number of days of history that the exported audit log contains.
    - **Destination**: Select a connection destination and define the associated settings. For more information, see Tanium Connect User Guide: Connection destinations.
5. (Optional) In the **Configure Output** section, configure the following options:
    - **Filters**: Modify the data that you are retrieving from the connection source before Connect sends that data to the destination. For more information, see Tanium Connect User Guide: Reference: Filtering options.
    - **Format**: Select the data format (such as **JSON** or **HTML**) and configure the associated settings. For more information, see the Tanium Connect User Guide topic for the **Destination** type that you selected.
    - **Columns**: Expand the the **Columns** section, select the available **Source** items (columns), optionally change the column names in the **Destination Label**, select the **Value Type**, and specify the **Customization**. For more information, see the Tanium Connect User Guide topic for the **Destination** type that you selected.
6. (Optional) In the **Schedule** section, select **Enable Schedule** and configure a schedule for the connection. For more information about running connections on a schedule, see Tanium Connect User Guide: Schedule connections. If the schedule is not enabled, the connection only runs when you manually run it.
7. Click **Save** or **Save and Run**.

Test a connection and review data

1. From the Main menu, go to **Modules > Connect > Connections**.
2. Click the **Name** of the connection that you created for the Direct Connect audit log.
3. Click **Run Now** and view the summary of the run.
4. View the audit log in the destination that you configured for the connection.

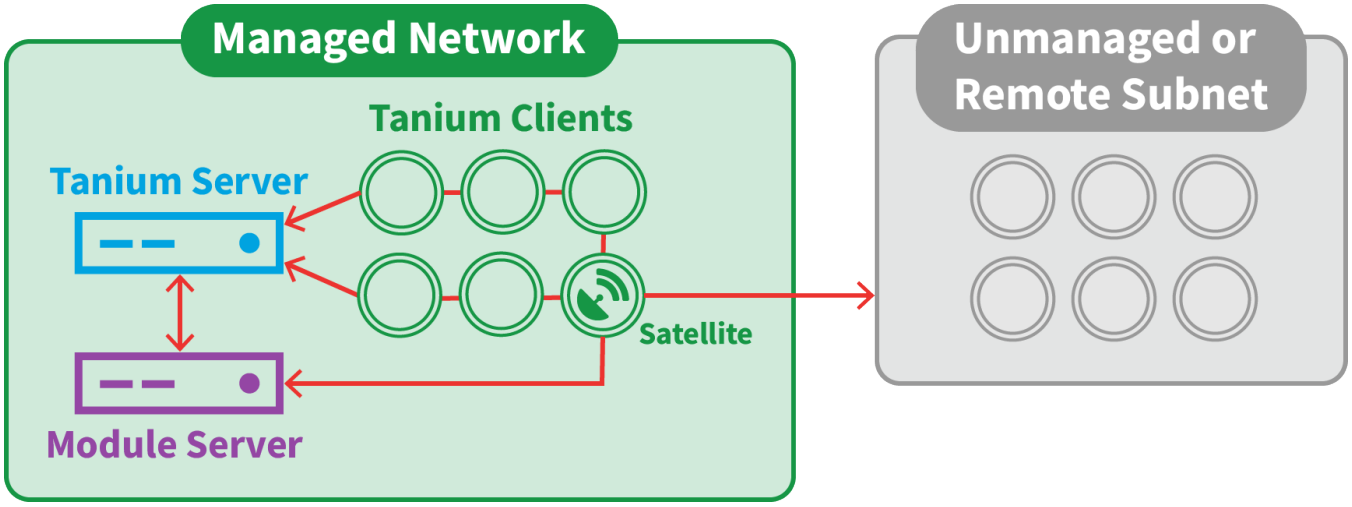
© 2026 Tanium Inc. All Rights Reserved

Managing satellites

Overview of satellites

Satellites are Tanium Clients that you designate to run secure workloads on endpoints that the Tanium Module Server cannot directly reach. Satellites enable Tanium solutions to perform operations on those endpoints, such as non-line-of-sight scans for Tanium Discover or remote authenticated scans for Tanium Comply.

Tanium Client designated as a satellite



For example, suppose you have a lab network with unmanaged endpoints on a subnet separated from your main network, and you want to use Comply to perform scans on the lab endpoints. Also suppose you are using a managed endpoint with multiple network interface controllers (NICs) to bridge the lab subnet to the main network. You can designate that endpoint as a satellite and then configure Comply to use it to perform scans on the unmanaged endpoints.

The Module Server might need to send sensitive, encrypted data (such as credentials) to a satellite when running a workload. Therefore, you must verify each Tanium Client that you designate as a satellite to prevent spoofing attacks. The Server never sends such sensitive data through the Client linear chain and the satellite does not store that data on disk.

View satellites

Perform the following steps to check the status and other details of Tanium Clients that are designated as satellites.

1. From the Main menu, go to **Shared Services > Direct Connect > Overview** and go to the **Satellites** section.
2. (Optional) In the **Filter items** field, enter an alphanumeric string that matches the value or values of any column except **State** or **Created** to show only the matching satellites.

© 2026 Tanium Inc. All Rights Reserved

Create satellites

IMPORTANT

For the best results, do not configure endpoints as satellites if the endpoints are internet-facing devices or might become internet-facing devices.

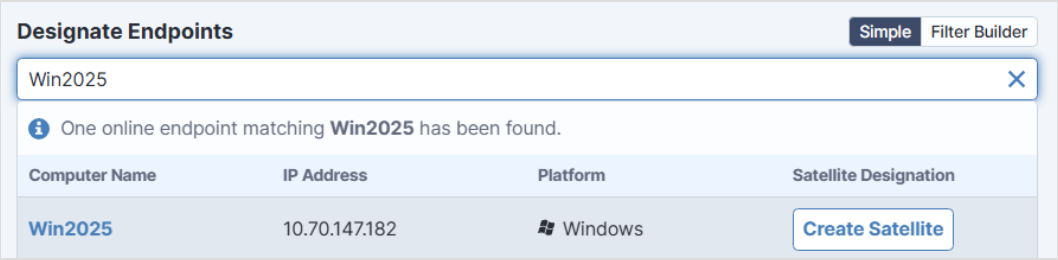
NOTE

You can designate only Windows, macOS, or Linux endpoints as satellites.

If you designate an Arm-based Windows endpoint as a satellite, Tanium solutions that do not support Arm-based Windows endpoints might not work with the Arm-based Windows satellite. To check if a particular solution supports Arm-based Windows endpoints, go to the Tanium Resource Center and view the requirements in the user guide for that solution.

Designate satellites

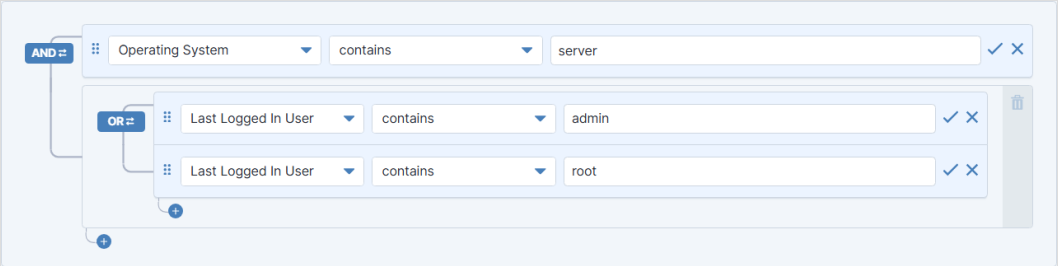
1. From the Main menu, go to **Shared Services > Direct Connect > Overview**.
2. Go to the **Satellites** section and click **Create Satellite**.
3. Go to the **Designate Endpoints** section and select a search option to find the endpoint that you want to designate as a satellite.
   - **Simple**: Enter the IP address or computer name of the endpoint.



   - **Filter Builder**: Configure one or more sensor-based filters to find the endpoint. Select a sensor (such as **Last Logged In User**), select an operator (such as **contains**), enter the value to match, and click Apply. For each additional filter, hover over Add, select **Add Row** or **Add Group**, and repeat the configuration steps. Direct Connect processes group (nested) filters and applies Boolean AND/OR logic in the same way that Tanium Interact does for question results filters, and the configuration steps are similar. For more information, see Tanium Interact User Guide: Filter by

© 2026 Tanium Inc. All Rights Reserved

advanced conditions.



4. Click **Create Satellite** in the row for each endpoint that you want to designate as a satellite, and then click Close to clear the search. Each new satellite is added to the **Satellites Pending Verification** list.
5. (Optional) Repeat the preceding steps to find additional endpoints to designate as satellites using different search criteria.
6. Click **Continue** after you finish adding endpoints. The **Verify Satellites** page opens and shows settings that you must configure to complete the designation process.

Name and verify satellites

Perform the following steps on the **Verify Satellites** page that opened after the preceding procedure.

1. Enter a meaningful **Satellite Name** for each designated endpoint. This name is separate from the computer name, and it appears in the selection list when you configure an activity that uses a satellite.
2. Sign in to each designated endpoint and view the endpoint fingerprint. In the following commands, replace `<Tanium Client>` with the installation directory of the Tanium Client.
   - **Windows endpoints**: Open a command prompt and run the following commands:

     ```
     cd <Tanium Client>\Tools\DirectConnect\scripts
     ```

     ```
     get_endpoint_fingerprint.cmd
     ```

   - **Non-Windows endpoints**: Open a terminal or command-line interface and run the following commands:

     ```
     cd <Tanium Client>/Tools/DirectConnect/scripts
     ```

     ```
     get_endpoint_fingerprint.sh
     ```

> **NOTE** An endpoint fingerprint is an endpoint identifier that is stable and usually unique for each endpoint. Verifying endpoint fingerprints ensures that you applied the satellite designation to the correct endpoints.

© 2026 Tanium Inc. All Rights Reserved

3. Record the fingerprint that the command returns on each endpoint and return to the **Verify Satellites** page in Tanium Console.

   The following is an example fingerprint: `43:75:cc:83:75:f7`.

   In the next step, you can achieve a higher level of security by clearing the selection for **Visually verify satellites instead** and manually entering the **Unique Identifier** for each designated endpoint.

4. Perform one of the following steps to verify the satellites, and then click **Save**.

   - **Unique Identifier**: Enter the fingerprint that you recorded for each endpoint.
   - **Visually verify satellites instead**: This option automatically populates the **Unique Identifier** for each endpoint. However, it is critical that you sign in to each endpoint and view its fingerprint using the preceding commands to verify that the fingerprint matches the automatically populated value on the **Verify Satellites** page. If you proceed without actual verification, an unintended endpoint might receive sensitive data such as credentials.

   The **Satellites** grid shows the new satellites with a **Status** of `Verified` to indicate that you successfully designated the endpoints.

Delete satellites

Perform the following steps to remove the satellite designation from endpoints. Deleting the designation does not remove the Tanium Client from endpoints, and therefore they remain managed endpoints within the Tanium environment.



Any scan profile in Tanium Discover or scan assessment in Tanium Comply becomes invalid if you remove the satellite designation from the satellite that the scan uses. For more information, see Tanium Discover User Guide: Running satellite scans and Tanium Comply User Guide.

1. From the Main menu, go to **Shared Services > Direct Connect > Overview** and go to the **Satellites** section.
2. Select the satellites and click Delete .

© 2026 Tanium Inc. All Rights Reserved

Troubleshooting Direct Connect

Generate a support package

Collect information about the current state of the Direct Connect service to use for troubleshooting. The information is saved as a ZIP file that you can download with your browser. The ZIP file is also known as a support bundle.

1. From the Main menu, go to **Shared Services > Direct Connect** and click Help **> Troubleshooting**.
2. Click **Generate Support Package** and then click **Download Support Package** to download the ZIP file to the local download directory.
3. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 72.

Change the logging level

The logging level determines how much detail Direct Connect records in its logs for events such as endpoint connection attempts. Select a level based on how much detail you need for troubleshooting. The level of detail from most to least is **DEBUG**, **INFO**, **WARN**, and **ERROR**.



Changes to the logging level apply only to future events. The changes do not affect the data that is available in the support package for events that occurred before the changes.

1. From the Main menu, go to **Shared Services > Direct Connect** and click Help.
2. Select the **Troubleshooting** tab and select the **Log Level**.

Troubleshoot endpoint connection issues

Connection process

Understanding how Tanium platform settings are involved in the endpoint connection process can help you troubleshoot connection issues. Each endpoint is configured to connect with a specific Tanium Server or Tanium Zone Server. An active-active deployment includes multiple Tanium Servers and Zone Servers. When you attempt a connection, Direct Connect iterates through the configured servers in the following order until a successful connection occurs:

1. The server specified in the **LastGoodServerName** setting (if available)
2. The last server used for a successful connection

© 2026 Tanium Inc. All Rights Reserved

3. The server with the most successful connections
4. The server specified in the **ServerName** setting (if configured)
5. Any servers specified in the **ServerNameList** setting

For more information about the preceding settings, see Tanium Client Management User Guide: Settings for connections to Tanium Core Platform servers.

Troubleshoot connections

Perform the following steps if you cannot establish an endpoint connection.

To include more details in the logs that record Direct Connect events on an endpoint, see Change the logging level on page 67.

1. Go to **Administration > Actions > Action History** and check the status of the action named `Deploy Direct Connect - Open Session - <operating system> - <session ID>`. If the page lists multiple Direct Connect actions, match an action with a particular connection attempt based on the **Start Time** value.
2. Perform one of the following tasks based on whether the action ran on the endpoint:
   - **Action ran but unsuccessfully**: Check the `<Tanium Client>/Logs/extensions0.txt` log on the endpoint. Make sure that the endpoint can connect to the Module Server using the **Fully Qualified Domain Name** and **Port** that you configured on the **Endpoint Connection** tab in the Direct Connect settings.
   - **Action did not run**: Verify that the endpoint meets the following conditions:
     - **Action group**: Verify that the endpoint is a member of the **Direct Connect** action group. If the endpoint is not a member, update the action group to include a computer group to which the endpoint is assigned. For more information, see Tanium Console User Guide: Managing action groups.
     - **Direct Connect tools**: Verify that the endpoint has the latest tools, as described in Verify endpoint tools on page 69.

Troubleshoot Zone Proxy connection issues

You install and configure the Tanium Direct Connect Zone Proxy if endpoints form Direct Connect connections to the Module Server through a Tanium Zone Server. If you cannot establish an endpoint connection after installing and configuring the Zone Proxy, check the Direct Connect Zone Proxy log for errors: `<Tanium>/TaniumDirectConnectZoneProxy/logs/proxy.log`. For more information, see Configure Zone Proxies.

Screen sharing buttons unavailable

Screen sharing buttons and related functionality might not be available in Tanium Console while the system rotates ScreenMeet key information. By default, this action occurs once every 30 days. Wait up to 30 minutes for this action to complete and then try accessing screen sharing functionality. For more information about next steps if you still cannot access screen sharing functionality,

© 2026 Tanium Inc. All Rights Reserved

see Contact Tanium Support.

Poor Connection Quality message when attempting to join a screen sharing session

When attempting to join a screen sharing session, a user accessing Screen Sharing using Microsoft Edge receives this message: **Poor connection quality. Attempting to reduce video bitrate... Activate Low Performance Mode**. This message can occur if the Microsoft Edge setting **Control if audio and video play automatically on sites** is set to **Blocked**. To resolve the issue, set this value to **Limit** (default setting) or **Allow**. For more information about this setting, see Microsoft: How to manage autoplay in Microsoft Edge.

Verify endpoint tools

Perform the following steps to diagnose issues such as a Direct Connect feature not working on an endpoint or incorrect data in the Direct Connect workbench. For example, you might see the following message when attempting to start an endpoint connection:

⚠ `The Direct Endpoint Connection tools are not installed`

1. Verify that endpoints have the latest Direct Connect tools installed by using any Tanium Console or Interact question field to issue the following question.

   ```
   Get Endpoint Configuration - Tools Status contains Direct Connect from all
   machines with Endpoint Configuration - Tools Status contains Direct Connect
   ```

   To view the tools version on a single endpoint, add a filter to the `from` clause of the question that identifies the endpoint. For example, if you know the computer name, you can issue the following question.

   ```
   Get Endpoint Configuration - Tools Status contains Direct Connect from all
   machines with ( Endpoint Configuration - Tools Status contains Direct Connect
   and Computer Name equals <computer name>)
   ```

   The **Installed Version** is lower than the **Targeted Version** on endpoints that do not have the latest tools.

2. If the latest tools are not installed, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or client extensions.

Verify the configuration version

On the Direct Connect **Overview** page, the following warning means that the Direct Connect configuration has changed from what was last installed on the endpoint:

⚠ `The most recent version of the configuration is not installed for endpoints`

The endpoint might not be able to connect depending on what changed. This condition usually resolves automatically if you wait for Tanium Endpoint Configuration to deploy the latest configuration to endpoints. Perform the following steps to diagnose the condition if it persists:

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services > Endpoint Configuration > Configurations**.
2. Expand the **Filters** and enter `dec` as the **Domain** to show only Direct Connect configurations.
3. Record the revision number in the **Description** column. For example, the value might be `Direct Connect config revision 15`.
4. View the Direct Connect revision on endpoints by using any Tanium Console or Interact question field to issue the following question.

   ```
   Direct Connect - Connection Configuration and "Client Configuration and Support - Is Container" from all machines
   ```

   To view the revision on a single endpoint, add a filter to the `from` clause of the question that identifies the endpoint. For example, if you know the computer name, you can issue the following question.

   ```
   Direct Connect - Connection Configuration and "Client Configuration and Support - Is Container" from all machines with Computer Name equals <computer name>
   ```

5. If the endpoint does not have the latest Direct Connect configuration revision, verify that the endpoint has the latest manifest and update the manifest if necessary. For more information, see Tanium Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest.

Remove Direct Connect tools from endpoints

You can deploy an action to remove Direct Connect 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 **Direct Connect**, drill down as necessary, and select the targets from which you want to remove Direct Connect 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 **Direct Connect**.
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:

© 2026 Tanium Inc. All Rights Reserved

NOTE

- To allow Direct Connect 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 Direct Connect 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 Direct Connect 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 Direct Connect

CAUTION

Direct Connect is a shared service that is used by several Tanium solutions. If Direct Connect is in use by another Tanium solution, uninstalling Direct Connect or removing the tools from endpoints could have unintended consequences. Contact support@tanium.com to determine whether uninstalling Direct Connect is advisable in your environment.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Configuration > Solutions**.
2. In the **Content** section, select the **Direct Connect** row.
3. Click **Uninstall**.

Uninstall the Direct Connect Zone Proxy

The steps to remove the Tanium Direct Connect Zone Proxy depend on your Tanium infrastructure:

- **Windows**: Sign in to the Tanium Zone Server as a user with Local Administrator rights, open **Control Panel > Programs > Programs and Features**, select the Tanium Direct Connect Zone Proxy, and click **Uninstall**.
- **TanOS**: See Appliance Deployment Guide: Remove the Direct Connect Zone Proxy.

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: Gateway examples for Direct Connect

Tanium Gateway provides a GraphQL API integration point for Tanium solutions, including Direct Connect. The following example query and mutation requests pertain to Direct Connect functionality. You can use these examples as a reference to create custom GraphQL API requests that connect to a single endpoint, retrieve data, stop a process, and then close the connection. Queries that retrieve information from endpoints or terminate processes on endpoints require Tanium Performance.

For additional Gateway example syntax, see Tanium Gateway User Guide: Reference: Filter syntax and Tanium Gateway User Guide: Reference: Gateway examples.

Open a connection to an endpoint

`mutation.directConnectOpen`

OPEN DIRECT CONNECTION TO ENDPOINT

The following mutation uses Direct Connect to establish a connection to the endpoint with an ID of `12323`. You can retrieve IDs through the Get endpoints IDs from Tanium Data Service query. If a direct connection status is not `READY` (such as `CONNECTING` or `UNKNOWN`) after you use this mutation, you can use the Get direct connection status query to check the direct connection status.

Connections opened with `directConnectOpen` are compatible with stable Direct Connect APIs, including `directConnectEndpoint`, `directConnectPing`, `directConnectProcessTerminate`, and `directConnectClose`. Connections opened with `directConnectOpen` are not compatible with legacy Direct Connect APIs, including `directEndpoint`, `pingDirectConnection`, `killProcess`, and `closeDirectConnection`.



Direct Connect connections close after five minutes of inactivity.

```
mutation exampleOpenEndpointConnection($id: ID!) {
  directConnectOpen(input: {endpointID: $id}) {
    connectionID
    status
  }
}
```

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

```
{
```

© 2026 Tanium Inc. All Rights Reserved

```
  "id": "12323"
}
```

Example response:

```
{
  "data": {
    "directConnectOpen": {
      "connectionID": "86d9a9ac-0229-481b-9d88-5f1bcb1b177b",
      "status": "READY"
    }
  }
}
```

Get the status of a connection to an endpoint

`query.directConnectConnectionStatus`

GET DIRECT CONNECTION STATUS

The following query uses Direct Connect to retrieve the status of a direct connection. If a direct connection status is not `READY` (such as `CONNECTING` or `UNKNOWN`) after you use the Open direct connection to endpoint mutation to establish a direct connection to an endpoint, you can use the connection ID from that response in this query to determine whether the direct connection is established.

The input requires a direct endpoint connection opened using `directConnectOpen`.



Direct Connect connections close after five minutes of inactivity.

```
query exampleGetDCStatus($id: ID!) {
  directConnectConnectionStatus(input: {connectionID: $id}) {
    status
  }
}
```

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

© 2026 Tanium Inc. All Rights Reserved

```
{
  "id": "86d9a9ac-0229-481b-9d88-5f1bcb1b177b"
}
```

Example response:

```
{
  "data": {
    "directConnectConnectionStatus": {
      "status": "READY"
    }
  }
}
```

Ping the connection to an endpoint

`mutation.directConnectPing`

PING DIRECT CONNECTION TO ENDPOINT

The following mutation retrieves whether a Direct Connect connection is active. Use this mutation to check connection details or to keep the connection active.

The input requires a direct endpoint connection opened using `directConnectOpen`.



Direct Connect connections close after five minutes of inactivity.

```
mutation examplePingDirectConnection($connectionID: ID!) {
  directConnectPing(input: {connectionID: $connectionID}) {
    result
  }
}
```

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

© 2026 Tanium Inc. All Rights Reserved

```
{
  "connectionID": "5fc564d6-5767-47fc-abb6-25cba65409d8"
}
```

Example response:

```
{
  "data": {
    "directConnectPing": {
      "result": true
    }
  }
}
```

Get data from an endpoint

`query.directConnectEndpoint.performance`

GET DATA FROM ENDPOINT

After you establish a connection to an endpoint through Direct Connect, you can query the endpoint for specific information. The input requires a direct endpoint connection opened using `directConnectOpen`.

The following query retrieves the CPU usage on the endpoint:

```
query exampleGetEndpointData($id: ID!) {
  directConnectEndpoint(input : {ConnectionID: $id}) {
    performance {
      cpuUsagePercent
    }
  }
}
```

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

© 2026 Tanium Inc. All Rights Reserved

```
{
  "id": "12345678-90ab-cdef-1234-567890abcdef"
}
```

Example response:

```
{
  "data": {
    "directConnectEndpoint": {
      "performance": {
        "cpuUsagePercent": 28.751501243887798
      }
    }
  }
}
```

Get process from an endpoint

`query.directConnectEndpoint.processes`

GET PROCESS FROM ENDPOINT

After you establish a connection to an endpoint through Direct Connect, you can query the endpoint for process information. The input requires a direct endpoint connection opened using `directConnectOpen`.

The following query retrieves the state of all processes running on the endpoint.

```
query exampleGetEndpointProcess ($id: ID!) {
  directConnectEndpoint(input : {connectionID: $id}) {
    processes {
      all {
        pid
        ppid
        name
        commandLine
```

© 2026 Tanium Inc. All Rights Reserved

```
          userName
          groupName
          memoryResidentBytes
        }
      }
    }
  }
```

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

```
{
  "id": "12323"
}
```

Example response:

```
{
  "data": {
    "directConnectEndpoint": {
      "processes": {
        "all": [
          {
            "pid": 2092,
            "ppid": 496,
            "name": "TaniumReceiver.exe",
            "commandLine": "\"C:\\Program Files\\Tanium\\Tanium
Server\\TaniumReceiver.exe\" --service",
            "userName": "admin",
            "groupName": "test-group",
            "memoryResidentBytes": 59842560
          },
          {
            "pid": 5760,
```

© 2026 Tanium Inc. All Rights Reserved

```
            "ppid": 1112,
            "name": "TaniumClient.exe",
            "commandLine": "\"C:\\Program Files (x86)\\Tanium\\Tanium Client\\TaniumClient.exe\" -c",
            "userName": "SYSTEM",
            "groupName": "NT AUTHORITY",
            "memoryResidentBytes": 17965056
          },
          {
            "pid": 1036,
            "ppid": 496,
            "name": "TaniumBlobService.exe",
            "commandLine": "\"C:\\Program Files\\Tanium\\Tanium Module Server\\services\\blob-service\\TaniumBlobService.exe\"",
            "userName": "SYSTEM",
            "groupName": "NT AUTHORITY",
            "memoryResidentBytes": 7426048
          }
        ]
      }
    }
  }
}
```


Get alerts from an endpoint

`query.directConnectEndpoint.alerts`

GET PAST 24 HOURS OF ALERTS FROM ENDPOINT

After you establish a connection to an endpoint through Direct Connect, you can query the endpoint for alert information. You can also define a time period for retrieving events based on the following rules:

- The end time must be before the current time.
- The start time must be before the end time.
- If you define a start time without an end time, the request time period retrieves alerts from the start time to the current

© 2026 Tanium Inc. All Rights Reserved

time.

- If you do not define a start time or end time, the request defaults to the past 24 hours.

The input requires a direct endpoint connection opened using `directConnectOpen`.

The following query retrieves alerts from an endpoint that occurred during the past 24 hours.

```
query exampleGetEndpointAlerts($id: ID!) {
  directConnectEndpoint(input : {connectionID: $id}) {
    alerts {
      all {
        schema
        key
        type
        ref
        topProcessesExpr
        labels
        pendingAt
        start
        resolvedAt
        leadup
        value
      }
    }
  }
}
```

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

```
{
  "id": "12345678-90ab-cdef-1234-567890abcdef"
}
```

Example response:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "data": {
    "directConnectEndpoint": {
      "alerts": {
        "all": [
          {
            "schema": 1,
            "key": "available-mem{heuristic=\"available-mem\"}",
            "type": "available-mem",
            "ref": null,
            "topProcessesExpr": null,
            "labels": {
              "heuristic": "available-mem"
            },
            "pendingAt": "2022-03-15T15:54:38.574990164Z",
            "start": "2022-03-15T15:54:38.574990164Z",
            "resolvedAt": null,
            "leadup": 300000000000,
            "value": 168.48828125
          }
        ]
      }
    }
  }
}
```


GET 48 HOURS OF ALERTS FROM ENDPOINT

The following query sets a time period of 48 hours from January 1, 2022 to January 3, 2022 and retrieves alerts for an endpoint from that period.

```
query exampleGetEndpointAlerts48Hours($id: ID!, $startTime: Time!, $endTime: Time) {
  directConnectEndpoint(input : {connectionID: $id}) {
    alerts {
      all (scope: {startTime: $startTime, endTime: $endTime}) {
```

© 2026 Tanium Inc. All Rights Reserved

```
        schema
        key
        type
        ref
        topProcessesExpr
        labels
        pendingAt
        start
        resolvedAt
        leadup
        value
      }
    }
  }
}
```

Include the connection ID and time period variables in the **Variables** panel or in your variables dictionary:

```
{
  "id": "12345678-90ab-cdef-1234-567890abcdef",
  "startTime": "2022-01-01T00:00:00Z",
  "endTime": "2022-01-03T00:00:00Z"
}
```

GET ALERTS FROM PRIOR DATE FROM ENDPOINT

The following query sets a time period start date of January 1, 2022 and retrieves alerts for an endpoint from that date to the current time.

```
query exampleGetEndpointAlertsPriorDate($id: ID!, $startTime: Time!) {
  directConnectEndpoint(input: {connectionID: $id}) {
    alerts {
      all(scope: {startTime: $startTime}) {
        schema
        key
```

© 2026 Tanium Inc. All Rights Reserved

```
        type
        ref
        topProcessesExpr
        labels
        pendingAt
        start
        resolvedAt
        leadup
        value
      }
    }
  }
}
```

Include the connection ID and start time variables in the **Variables** panel or in your variables dictionary:

```
{
  "id": "12345678-90ab-cdef-1234-567890abcdef",
  "startTime": "2022-01-01T00:00:00Z"
}
```

Stop a process on an endpoint

`mutation.directConnectProcessTerminate`

STOP ENDPOINT PROCESS

After you establish a connection to an endpoint through Direct Connect, you can stop running processes on the endpoint. The following mutation stops a process named `notepad.exe` on an endpoint.

The input requires a direct endpoint connection opened using `directConnectOpen`.

```
mutation exampleStopEndpointProcess($connectionID: ID!, $processName: String!, $pid: Int!,
$signal: Signal!) {
  directConnectProcessTerminate(
```

© 2026 Tanium Inc. All Rights Reserved

```
    input: {connectionID: $connectionID, name: $processName, pid: $pid, signal: $signal}
  ) {
    result
  }
}
```

Include the connection ID and process name variables in the **Variables** panel or in your variables dictionary:

```
{
  "connectionID": "5fc564d6-5767-47fc-abb6-25cba65409d8",
  "processName": "notepad.exe",
  "pid": 7056,
  "signal": "SIGKILL"
}
```

Example response:

```
{
  "data": {
    "directConnectProcessTerminate": {
      "result": true
    }
  }
}
```

Close connection to an endpoint

`mutation.directConnectClose`

CLOSE ENDPOINT CONNECTION

The following mutation closes a Direct Connect connection to an endpoint.



Direct Connect connections close after five minutes of inactivity.

© 2026 Tanium Inc. All Rights Reserved

```
mutation exampleCloseEndpointConnection($connectionID: ID!) {
  directConnectClose(input: {connectionID: $connectionID}) {
    result
  }
}
```

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

```
{
  "connectionID": "5fc564d6-5767-47fc-abb6-25cba65409d8"
}
```

Example response:

```
{
  "data": {
    "directConnectClose": {
      "result": true
    }
  }
}
```

© 2026 Tanium Inc. All Rights Reserved