Tanium™ Directory Query User Guide

Version 1.0.20

January 11, 2023

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

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

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

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

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

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years and has most recently completed certification against the WCAG 2.1 / VPAT 2.3 standards for all major product modules in summer 2021. In the recent testing the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.1 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

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

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

Table of contents

Directory Query overview

With Tanium™ Directory Query, administrators configure access to directory servers, such as Active Directory and Azure AD, for Tanium solutions that require directory access. This centralized location simplifies the administration of directory servers.

Supported directory servers

Directory Query supports the following directory servers:

- Active Directory Domain Services that are running on any version of Microsoft Windows Server that is currently supported by Microsoft
- Azure Active Directory Domain Services

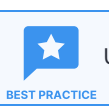
For supported versions, see Microsoft: Search Product and Services Lifecycle Information.

Directory server synchronization

In the Directory Query **Overview** page, you can add a domain for each directory server to which you want to connect. For each domain, you can specify how Tanium synchronizes with the directory server. You can use a combination of synchronization types across the domains you add.

- **Service synchronization**: The Tanium Module Server connects to the Active Directory server through proxy access. If you use this type, consider the following:
    - The connection to the LDAP server must use LDAP over TLS (also referred to as secure LDAP or LDAPS). For steps to configure LDAPS in Azure Active Directory Domain Services, see Microsoft: Configure secure LDAP for an Azure Active Directory Domain Services managed domain.
    - As a best practice, restrict network traffic to flow only between the IP range for your LDAP server and Tanium Cloud over the associated ports. For port information, see Ports on page 10.
    - If you are using Azure Active Directory Domain Services, you must configure Microsoft Azure to allow network connections from Tanium Cloud. For more information, see Microsoft: Lock down secure LDAP access over the internet.
- **Satellite synchronization**: The Tanium Module Server connects to endpoints that behave as satellites (or proxies) that enable the communication with the Active Directory server.

  The Active Directory domain must use TLS, and the satellite must trust the domain certificate. For more information about satellites, see Tanium Direct Connect User Guide: Managing satellites.

  Use Satellite synchronization to simplify the connection process.

Integration with other Tanium products

Directory Query has built in integration with Tanium™ Criticality and Tanium Direct™ Connect for additional visibility and reporting of related date.

Criticality

Criticality uses Directory Query to connect to directory servers to understand administrative rights in the directory server environment. For more information, see Tanium Criticality User Guide: Criticality overview.

Direct Connect

Use Direct Connect to create Windows satellites to use for satellite synchronization. For more information, see Tanium Direct Connect User Guide: Create satellites.

Getting started with Directory Query

Follow these steps to configure and use Directory Query.

Step 1: Install and configure Directory Query

Install and configure Directory Query. For more information, see Installing Directory Query on page 13 and Configuring Directory Query on page 15.

Step 2: Add domains to connect to Active Directory domains

Add a domain for each Active Directory domain to which you want to enable access.

See Managing connections to directory servers on page 17.

Directory Query requirements

Review the requirements before you install and use Directory Query.

Core platform dependencies

Make sure that your environment meets the following requirements:

- **Tanium™ Core Platform servers**: 7.4.3.1204 or later
- **Tanium™ Client**: Any supported version of Tanium Client. For the Tanium Client versions supported for each OS, 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 Directory Query to function (required dependencies).

> NOTE Some Directory Query dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 9 and Feature-specific dependencies on page 9. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Directory Query requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Directory Query, the Tanium Server automatically imports all your licensed solutions at the same time. See Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Directory Query to import and you are using Tanium Core Platform 7.5.2.3531 or later with Tanium Console 3.0.72 or later, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Directory Query, the server automatically updates those dependencies to the latest available versions.

If you select only Directory Query to import and you are using Tanium Core Platform 7.5.2.3503 or earlier with Tanium Console 3.0.64 or earlier, you must manually import or update required dependencies. See Tanium Console User Guide: Import, re-import, or update specific solutions.

Required dependencies

Directory Query has the following required dependencies at the specified minimum versions. You must install the dependencies in the listed order.

1. Tanium™ System User Service 1.0.77 or later
2. Tanium™ RDB Service 1.2.31 or later
3. Tanium™ Secrets Service 1.0.48 or later

Feature-specific dependencies

Directory Query has the following feature-specific dependencies at the specified minimum versions:

- Tanium™ Direct Connect 2.3 or later is required to sync from Windows satellites.

Tanium™ Module Server

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

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

Endpoints

Directory Query does not directly deploy packages to endpoints. For Tanium Client operating system support, see Tanium Client Management User Guide: Client version and host system requirements.

Third-party software

Directory Query is supported for use with the following directories:

- Active Directory Domain Services that are running on any version of Microsoft Windows Server that is currently supported by Microsoft.
- Azure Active Directory Domain Services

For supported versions, see Microsoft: Search Product and Services Lifecycle Information.

You can synchronize Impact with Active Directory in two different ways: service or satellite. As a best practice, use the satellite sync, which connects the Module Server to an endpoint that behaves as a satellite to enable communication with the Active Directory server. With service, the Module Server connects to the Active Directory server through proxy access. If you use the service type, consider the following:

NOTE

- The connection to the LDAP server must use LDAP over TLS (also referred to as secure LDAP or LDAPS). For steps to configure LDAPS in Azure Active Directory Domain Services, see Microsoft: Configure secure LDAP for an Azure Active Directory Domain Services managed domain.
- As a best practice, restrict network traffic to flow only between the IP range for your LDAP server and the Module Server over the associated ports. For port information, see Ports on page 10.
- If you are using Azure Active Directory Domain Services, you must configure Microsoft Azure to allow network connections from the Module Server. For more information, see Microsoft: Lock down secure LDAP access over the internet.

Active Directory user account

Directory Query uses the user account that you specify when you configure the connection to domains for Active Directory queries. This user should have limited access. You can specify any user, but if you modified the standard user permissions from the default settings, the user must meet the following minimum requirements so that Impact has access to read attribute data from Active Directory:

- Member of the Domain Users group
- Permission to read the `objectSID` attribute from the domain object in the configured domains
- Permission to read the `objectSID` attribute on all users, groups, and computers in the configured domains
- Permission to `Read members` on all groups in the configured domains
- (Optional, best practice) Assign `List Contents` and `Read all properties` access on all objects in the configured domains, including the domain object.

Host and network security requirements

Specific ports and processes are needed to run Directory Query.

Ports

The following ports are required for Directory Query communication.

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17515	TCP	Internal purposes, not externally accessible
Module Server or satellite	Active Directory Server	389 / 636	LDAP / LDAPS	Connecting to the Active Directory server.

Source	Destination	Port	Protocol	Purpose
Module Server or satellite	Active Directory Global Catalog Server	3268 / 3269	LDAP / LDAPS	Required only when connecting to the Active Directory Global Catalog server. For more information, see Managing connections to directory servers on page 17.

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

Security exclusions

If security software is in use in the environment to monitor and block unknown host system processes, Tanium recommends that a security administrator create exclusions to allow the Tanium processes to run without interference. The configuration of these exclusions varies depending on AV software. For a list of all security exclusions to define across Tanium, see Tanium Core Platform Deployment Reference Guide: Host system security exclusions.

Directory query security exclusions

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\directory-query-service\TaniumDirectoryQueryService.exe`

User role requirements

The following tables list the role permissions required to use Directory Query. To review a summary of the predefined roles, see Set up Directory Query users on page 15.

For more information about role permissions and associated content sets, see Tanium Console User Guide: Managing RBAC.

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

Directory Query user role permissions

Permission	Directory Query Administrator[1]	Directory Query Operator[1]	Directory Query User[1]
Directory Query Domains Configure domains	✓ QUERY READ WRITE	✓ QUERY READ WRITE	✓ QUERY READ

Directory Query user role permissions (continued)

Permission	Directory Query Administrator[1]	Directory Query Operator[1]	Directory Query User[1]
Directory Query Settings Configure Directory Query service settings	✓ READ WRITE	✓ READ WRITE	✓ READ
Directory Query Support Bundle Generate and view Directory Query support bundle	✓ READ	✗	✗
Directoryquery View the Directory Query workbench	✓ SHOW	✓ SHOW	✓ SHOW

[1]This role provides module permissions for Tanium Direct Connect. For more information, see Tanium Direct Connect User Guide: User role requirements.

Provided Directory Query platform content permissions

Permission	Directory Query Administrator	Directory Query Operator	Directory Query User
Plugin	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	✓ READ	✓ READ	✓ READ
Sensor	✓ READ	✓ READ	✓ READ

To view which content set permissions are granted to a role, see Tanium Console User Guide: View effective role permissions.

Installing Directory Query

Use the Tanium Console **Solutions** page to install Directory Query.

Before you begin

- Read the release notes.
- Review the Directory Query requirements on page 8.
- Assign the correct roles to users for Directory Query. Review the User role requirements on page 11.
    - To import the Directory Query solution, you must be assigned the Administrator reserved role.

Import Directory Query

Perform the following steps to install the Directory Query solution on the Tanium Server.

> **NOTE** If you have multiple Tanium Servers in an active-active configuration, you only need to perform these steps on one Tanium Server if you have Tanium Core Platform 7.4.3.1204 or later.

1. Sign in to the Tanium Console with an account that has the **Administrator** reserved role.
2. From the Main menu, go to **Administration > Configuration > Solutions**.
3. In the **Content** section, select the checkbox for **Directory Query** and click **Install**.

   > **TIP** If you need to install any prerequisite Tanium solutions or content, select the corresponding checkboxes for those solutions as well.

4. Review the content to import and click **Begin Install**.

Manage solution dependencies

Other Tanium solutions are required for Directory Query to function (required dependencies) or for specific Directory Query features to work (feature-specific dependencies). See Solution dependencies.

Verify Directory Query version

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

1. Refresh your browser.
2. From the Main menu, go to **Administration > Shared Services > Directory Query** to open the Directory Query **Overview** page.
3. To display version information, click Info  .

Configuring Directory Query

Configure satellite settings

You can modify the default satellite settings between all configured domains and Directory Query.

1. On the Directory Query **Overview** page, click Settings  to view the **Satellite Settings**.
2. To set the number of seconds to wait before timing out when connecting to a Direct Connect satellite, enter a value for **Connection Timeout**. The default value is 180 seconds.
3. To set the number of seconds to wait before timing out when performing validation actions on a Direct Connect satellite, enter a value for **Validation Timeout**. The default value is 60 seconds.
4. To set the number of seconds to wait to receive results when querying a Direct Connect satellite, enter a value for **Search Timeout**. The default value is 120 seconds.
5. Click **Submit**.

Set up Directory Query users

You can use the following set of predefined user roles to set up Directory Query users.

To review specific permissions for each role, see User role requirements on page 11.

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

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

Directory Query Administrator

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

- View the Directory Query workbench.
- Manage Directory Query domains.
- Configure Directory Query service settings.
- Generate and view the support bundle.

Directory Query Operator

Assign the **Directory Query Operator** role to users who manage the configuration and deployment of Directory Query functionality.
This role can perform the following tasks:

- View the Directory Query workbench.
- Manage Directory Query domains.
- Configure Directory Query service settings.

Directory Query User

Assign the **Directory Query User** role to users who need visibility into Directory Query data. This role can perform the following tasks:

- View the Directory Query workbench.
- View Directory Query domains.
- View Directory Query service settings.

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

Managing connections to directory servers

Manage connections to the Active Directory domains to which you want to enable access.

Before you begin

Active Directory considerations

- Active Directory referrals are not supported. You must create a connection for each domain that you want to synchronize.
- You can create a connection to a Global Catalog server to synchronize an entire Active Directory forest. To ensure accurate results, you must create a connection to every domain within each Active Directory forest.
- Domain resolution is also possible. However, all Domain Controllers that the domain resolves to must share a valid certificate. For LDAPS certificate requirements, see Microsoft: Requirements for an LDAPS certificate. If the domain resolves to a Domain Controller (DC) that has a certificate with a fingerprint that does not match the fingerprint returned by the DC that the domain resolved to when the domain configuration was saved, the connection fails.

Active Directory user account

When you add a domain, you specify the Active Directory user account. This user should have limited access. You can specify any user, but if you modified the standard user permissions from the default settings, the user must meet the following minimum requirements so that Directory Query has access to read attribute data from Active Directory:

- Member of the Domain Users group
- Permission to read the `objectSID` attribute from the domain object in the configured domains
- Permission to read the `objectSID` attribute on all users, groups, and computers in the configured domains
- Permission to `Read members` on all groups in the configured domains
- (Optional, best practice) Assign `List Contents` and `Read all properties` access on all objects in the configured domains, including the domain object.

Add a domain

Add a domain for each Active Directory domain to which you want to enable access.

1. From the Main menu, go to **Administration > Directory Query** to open the Directory Query **Overview** page.
2. Click **New Domain**.

3. Specify the settings for the connection to the domain:

4. Click **Validate** to verify that the information entered is valid.
5. After you validate the credentials, click **Save**.

Work with domains

View domains

1. From the **Directory Query** Overview page, go to the **Domains** section.
2. View the domains. The table contains the details that were specified when adding the domain and the time it was last updated.

Manage domains

To edit a domain, click Edit and then save your changes.

To delete a domain click Delete and then confirm your action.

Troubleshooting Directory Query

If Directory Query is not performing as expected, you might need to troubleshoot issues or change settings.

Collect logs

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

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

   Some browsers might block multiple downloads by default. Make sure to configure your browser to permit multiple downloads from the Tanium Console.
4. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 24.

Tanium Directory Query maintains logging information in the `Directory Query.log` file in the `\Program Files\Tanium\Tanium Module Server\services\Directory Query` directory.

Unable to connect to the domain: 204 No Content

Issue

Newly created domains show a pending status with a **204 No Content** message when you hover over the status. This missing status does not indicate a failure.

Solution

Run a Criticality sync or restart the Directory Query service.

Troubleshooting satellite configuration

If satellite synchronization is not working as expected, go to the Directory Query **Overview** page and check for error messages. The following table lists contributing factors into satellite synchronization issues and corrective actions you can make.

Contributing factor or error message	Corrective action
`A domain does not use TLS. Update the domain connection to use TLS.`	Edit the domain connection to use TLS. See Add a domain on page 17.
One of the following error messages: • `Failed to connect to Direct Connect. Test the Direct Connect connection to the endpoints, then try again.` • `Failed to authenticate a satellite. Test the Direct Connect connection to the endpoints, then try again.` • `Failed to establish a connection to a satellite. Test the Direct Connect connection to the endpoints, then try again.` • `Satellite not found. Test the Direct Connect connection to the endpoints, then try again.`	Confirm that Direct Connect can connect to the satellite. See Tanium Direct Connect User Guide: Troubleshoot endpoint connection issues.
`A satellite does not have the latest version of Direct Connect. Deploy the latest version of Direct Connect to the satellites.`	1. Verify that all endpoints have the latest version of Direct Connect installed using the following sensor: `Get Computer Name and Endpoint Configuration - Tools Status matches Direct Connect|.* from all machines with Endpoint Configuration - Tools Status matches Direct Connect|.*` 2. Deploy the `Endpoint Configuration- Reinstall Tools [Windows]` package to any endpoints with older Direct Connect versions. See Tanium Endpoint Configuration User Guide: Reinstall one or more tools installed by Endpoint Configuration.
`An error occurred saving sync settings. Try again.`	Try again. If that does not work, Contact Tanium Support on page 24.
Connection issues between the satellite and the Active Directory server.	See the following Microsoft Documentation articles: • Microsoft Documentation: Troubleshoot LDAP over SSL connection problems • Microsoft Documentation: Troubleshoot secure LDAP connectivity issues to an Azure Active Directory Domain Services managed domain • Microsoft Documentation: Valid root CA certificates distributed using GPO might intermittently appear as untrusted

Uninstall Directory Query

If you need to uninstall Directory Query, perform the following steps.

1. Sign in to the Tanium Console as a user with the Administrator role.
2. From the Main menu, go to **Administration > Configuration > Solutions**.
3. In the **Content** section, select the **Directory Query** row and click **Uninstall**.
4. Review the summary and click **Yes** to proceed with the uninstallation.
5. When prompted to confirm, enter your password.

Contact Tanium Support

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