

Tanium™ Directory Query User Guide

Autonomous IT. Unstoppable Business.

2025H2 Semiannual Release

Version 1.5

May 26, 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/

© 2025 Tanium Inc. All Rights Reserved

© 2025 Tanium Inc. All rights reserved.

Table of contents

Directory Query overview **6**

Supported directory servers 6

Directory server synchronization 6

Interoperability with other Tanium products 7

Criticality 7

Direct Connect 7

Impact 7

Getting started with Directory Query **8**

Step 1: Install and configure Directory Query 8

Step 2: Add domains to connect to Active Directory domains 8

Directory Query requirements **9**

Core platform dependencies 9

Solution dependencies 9

Tanium recommended installation 9

Import specific solutions 9

Required dependencies 9

Feature-specific dependencies 10

Tanium™ Module Server 10

Endpoints 10

Third-party software 10

Active Directory user account 11

Host and network security requirements 11

Ports 11

Security exclusions 12

User role requirements 12

Installing Directory Query **15**

Before you begin 15

© 2025 Tanium Inc. All Rights Reserved

Import Directory Query ... 15
Manage solution dependencies ... 15
Verify Directory Query version ... 15
Configuring Directory Query ... 17
Satellite overview ... 17
Configure satellite settings ... 17
Set up Directory Query users ... 18
Managing connections to directory servers ... 19
Before you begin ... 19
Active Directory considerations ... 19
Active Directory user account ... 19
Add a domain ... 19
Work with domains ... 21
View domains ... 21
Manage domains ... 21
Troubleshooting Directory Query ... 22
Collect logs ... 22
Perform monthly maintenance ... 22
Troubleshooting satellite configuration ... 22
Uninstall Directory Query ... 24
Contact Tanium Support ... 24
Reference: Verify the SHA256 fingerprint of a certificate ... 25

© 2025 Tanium Inc. All Rights Reserved

Directory Query overview

With Tanium™ Directory Query, administrators configure access to directory servers, such as Active Directory and Microsoft Entra ID (formerly 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
- Entra ID (formerly Azure AD) Domain Services

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

Directory server synchronization

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 Entra ID DS (formerly Azure AD DS), see Microsoft: Configure secure LDAP for an Azure Active Directory Domain Services managed domain.
    - If you are using Entra ID DS (formerly Azure AD DS), you must configure Microsoft Azure to allow network connections from The Tanium Module Server. For more information, see Microsoft: Lock down secure LDAP access over the internet.

  Restrict network traffic to flow only between the IP range for your LDAP server and The Tanium Module Server over the associated ports. For port information, see Ports on page 11.

- **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.

© 2025 Tanium Inc. All Rights Reserved

Interoperability with other Tanium products

Directory Query works with Tanium™ Criticality and Tanium Direct™ Connect for additional visibility and reporting of related data.

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.

Impact

Impact uses Directory Query to connect to the Active Directory domains that you can analyze to understand administrative rights in the directory server environment. For more information, see Tanium Impact User Guide: Impact overview.

© 2025 Tanium Inc. All Rights Reserved

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 15 and Configuring Directory Query on page 17.

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 19.

© 2025 Tanium Inc. All Rights Reserved

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 license that includes Directory Query. For more information about how to get Directory Query, see Tanium Solutions & Bundles.
- **Tanium™ Core Platform server**
- **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 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 10. 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, 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.

Required dependencies

Directory Query has the following required dependencies. You must install the dependencies in the listed order.

© 2025 Tanium Inc. All Rights Reserved

- Tanium™ System User Service
- Tanium™ RDB Service
- Tanium™ Secrets Service

Feature-specific dependencies

Directory Query has the following feature-specific dependencies:

- Tanium™ Direct Connect 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 User Guide for Windows Deployments: 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
- Microsoft Entra ID (formerly Azure AD) 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.



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:

© 2025 Tanium Inc. All Rights Reserved

- 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 Entra ID AD DS (formerly Azure AD DS), see Microsoft: Configure secure LDAP for an Azure Active Directory Domain Services managed domain.
- If you are using Entra ID DS (formerly Azure AD DS), 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.

BEST PRACTICE

Restrict network traffic to flow only between the IP range for your LDAP server and The Tanium Module Server over the associated ports. For port information, see Ports on page 11.

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.

Ports for Tanium 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.

© 2025 Tanium Inc. All Rights Reserved

Ports for Tanium Directory Query communication (continued)

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 19.

BEST PRACTICE

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

Security exclusions

If antivirus (AV) or other security software is in use in the environment to monitor and block unknown host system processes, Tanium requires that a security administrator create exclusions to allow the Tanium processes to run without interference. This software can include security applications that are included with an endpoint operating system, such as `fapolicyd` on some Linux distributions, or Microsoft Defender on Windows. The configuration of these exclusions varies depending on the security software. For more information about security exclusions to define across Tanium, see Tanium Client Management Guide: Reference: Endpoint security exclusions and for Windows-based Tanium Core Platform deployments, see Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server security exclusions.

NOTE

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

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

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

User role requirements

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

- Directory Query user role permissions on page 13
- Directory Query platform content permissions on page 14: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Directory Query users on page 18.

© 2025 Tanium Inc. All Rights Reserved

Some Directory Query 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 Directory Query. If you create custom roles for Directory Query users, be sure to assign all the solution permissions and content set permissions that are required for Directory Query 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 **Directory Query Service Account** and **Directory Query Service Account - All Content Sets** roles to users. These roles are 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 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]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.

© 2025 Tanium Inc. All Rights Reserved

Directory Query platform content permissions

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

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

© 2025 Tanium Inc. All Rights Reserved

Installing Directory Query

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

Before you begin

- Read the release notes.
- Review the Directory Query requirements on page 9.
- Assign the correct roles to users for Directory Query. Review the User role requirements on page 12.
    - 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 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). For more information, see Solution dependencies on page 9.

Verify Directory Query version

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

© 2025 Tanium Inc. All Rights Reserved

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

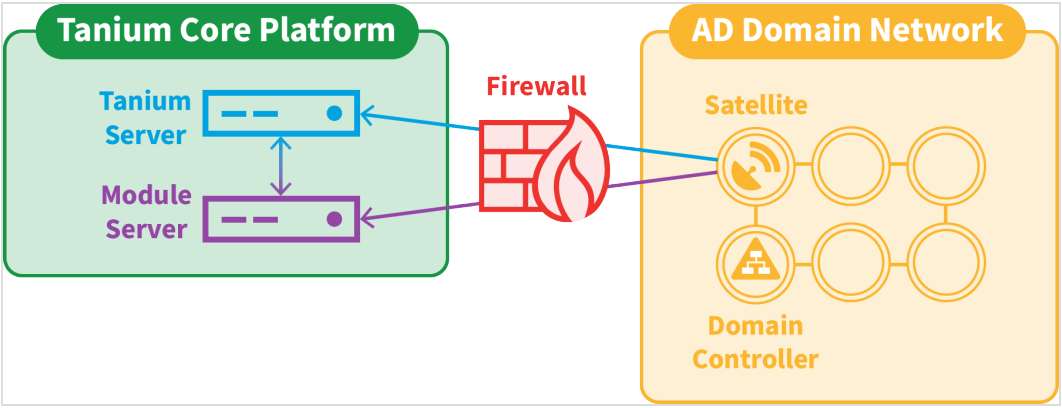
© 2025 Tanium Inc. All Rights Reserved

Configuring Directory Query

Satellite overview

Satellites are specific Tanium Clients that you designate to run certain targeted, secure workloads on behalf of the Tanium Module Server, such as connecting to a directory server on another network that is separate from the Module Server.

Tanium Client designated as a satellite



For example, use a satellite in Directory Query if the Tanium Module Server cannot directly connect to the Active Directory domain controller. This can happen when the Tanium Module Server resides on a different network segment where a firewall blocks traffic between it and the Active Directory domain controller. In such a scenario, use an endpoint as a satellite on the same network as the Active Directory domain controller to facilitate the connection.

Because the Module Server might need to send sensitive, encrypted data (such as credentials) to a satellite when running a workload, you must verify each endpoint that you designate as a satellite to prevent spoofing attacks. Any such sensitive data is never sent using the linear chain, nor is it stored on-disk on the satellite.

Configure satellite settings

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

1. From the Main menu, go to **Shared Services > Directory Query** and then 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 360 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 120 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 240 seconds.
5. Click **Submit**.

© 2025 Tanium Inc. All Rights Reserved

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 12.

IMPORTANT

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.

NOTE

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

© 2025 Tanium Inc. All Rights Reserved

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.
- Certificate pinning is used when establishing a session to a domain controller. This is a security technique where only authorized, or pinned, certificates are accepted when establishing a secure session. Any attempt to establish a secure session using a different certificate is rejected.
- Network load balancers are not supported to distribute network traffic to domain controllers.

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.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services > Directory Query** and then click **Add Domain**.
2. Specify the settings for the connection to the domain:
   a. **Name**: Specify a unique value that easily identifies the connection. For example: `myDomainA.com`.
   b. **Satellite**: If you are using satellite synchronization, select the satellite to use for this domain. The satellite should be in the domain. To select an endpoint not included in the list, add the endpoint as a satellite in Direct Connect. For more information, see Tanium Direct Connect User Guide: Managing satellites.

      NOTE

      The default selection is **Sync from the Tanium Module Server**. To use service synchronization, do not select a satellite.

   c. **LDAP Server**: Specify the LDAP connection string for the domain controller. For example: `dc.domain.com/` or `10.0.0.5`.

      Port: Specify the port to use when the Module Server connects to the Active Directory server. The default port is `636`.

      Use TLS is selected by default. TLS requires certificates on your domain controller. TLS is required for satellite synchronization.

      CAUTION

      Disabling TLS sends data over the network in plain text. Always use TLS unless you are working in a lab or test environment with test data.

   d. **Certificate**: If you are using LDAPS, verify the details of the host certificate before you provide the credentials. For more information on verifying the details of the host certificate, see Reference: Verify the SHA256 fingerprint of a certificate.

      NOTE

      For LDAPS certificate requirements, see Microsoft: Requirements for an LDAPS certificate. The same requirements apply to certificates issued by an internal certificate authority (CA). Because Directory Query uses a trust on first use authentication method, intermediate certificates are not required.

   e. **Username**: Specify the user name to use when connecting to the domain controller.
      The user name can be in `DOMAIN\User` format or UPN format (`user@domain`). UPN format works only for user accounts that have the UPN attribute populated.

      IMPORTANT

      Use an account with read-only permissions to the domain controller. For detailed requirements for this user, see Active Directory user account.

   f. **Password**: Provide the password for the user.
3. Click **Validate** to verify that the information entered is valid.

© 2025 Tanium Inc. All Rights Reserved

4. After you validate the credentials, click **Save**.

Work with domains

View domains

1. From the Main menu, click **Shared Services > Directory Query**.
2. In the **Domains** section, 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.

© 2025 Tanium Inc. All Rights Reserved

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. The ZIP file is also known as a support bundle.

1. From the Main menu, go to **Shared Services > Directory Query** and then 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 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.

Perform monthly maintenance

1. From the Main menu, go to **Shared Services > Directory Query**.
2. Review the **Domains** grid for errors. Hover over an Error icon to display a popup with the error message.
3. To troubleshoot errors, see Troubleshooting satellite configuration on page 22.

Troubleshooting satellite configuration

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

Contributing factors and corrective actions for Tanium™ Directory Query

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 19.

© 2025 Tanium Inc. All Rights Reserved

Contributing factors and corrective actions for Tanium™ Directory Query (continued)

Contributing factor or error message	Corrective action
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

© 2025 Tanium Inc. All Rights Reserved

Uninstall Directory Query

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

1. Sign in to 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 the Tanium Customer Community.

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

© 2025 Tanium Inc. All Rights Reserved

Reference: Verify the SHA256 fingerprint of a certificate

When you add or edit a domain in Directory Query a message appears in the **Add Domain** or **Edit Domain** panel of the Directory Query workbench that requests that you verify the SHA256 fingerprint of the host certificate before you provide credentials. You can edit and run the following PowerShell script on the server that was entered in **LDAP Server** in the **Add Domain** or **Edit Domain** panel to verify the SHA256 fingerprint of the host certificate. For more information on adding or editing domains, see Add a domain.

```
$myFingerprint =
"B9:4B:42:22:FF:EB:4A:C6:4E:57:5E:26:2A:E6:74:4A:7F:AC:74:67:9A:73:7C:D9:44:A6:6B:9A:F8:F7:FF:F
3"
$myCerts = (Get-ChildItem "Cert:\LocalMachine\My")
$sha256 = [System.Security.Cryptography.SHA256]::Create()
ForEach ($Cert in $myCerts) {
    $hashBytes = $sha256.ComputeHash($Cert.RawData)
    $hashString = -join ($hashBytes | ForEach-Object { $_.ToString("x2") })
    if ($hashString -eq ($myFingerprint -replace ":")) {
        Write-Output "Found Certficate with matching SHA256 Fingerprint!"
        Write-Output "Input SHA256 Fingerprint: $($myFingerprint -replace ":")"
        Write-Output "Certificate SHA256 Fingerprint: $($hashString.ToUpper())"
        Write-Output "Certificate Details:"
        $Cert | FL
    }
}
```

1. Copy the above script and paste it into a text editor.
2. Edit the value of the `$myFingerprint` variable to match the value that appears in the **Add Domain** or **Edit Domain** panel where you are requested to verify the SHA256 fingerprint of the host certificate before you provide credentials.
3. Save the file as `Get-CertificateSHA256Fingerprint.ps1`.
4. Copy the file to the server that was entered in **LDAP Server** in the **Add Domain** or **Edit Domain** panel.
5. Run the script on the server that was entered in **LDAP Server** in the **Add Domain** or **Edit Domain** panel as an administrator. Right-click the PowerShell icon and select **Run as administrator**.

The following example shows sample output of the provided script:

© 2025 Tanium Inc. All Rights Reserved

```
Found Certificate with matching SHA256 Fingerprint!
Input SHA256 Fingerprint: B94B4222FFEB4AC64E575E262AE6744A7FAC74679A737CD944A66B9AF8F7FFF3
Certificate SHA256 Fingerprint: B94B4222FFEB4AC64E575E262AE6744A7FAC74679A737CD944A66B9AF8F7FFF3
Certificate Details:



Subject      : CN=2022DC01.lab.example.com
Issuer       : CN=lab-2022CA01-CA, DC=lab, DC=example, DC=com
Thumbprint   : EBD63F4C09747C5293D3DF86F0A0D85C69726811
FriendlyName :
NotBefore    : 10/8/2024 2:30:01 PM
NotAfter     : 10/8/2025 2:30:01 PM
Extensions   : {System.Security.Cryptography.Oid, System.Security.Cryptography.Oid,
System.Security.Cryptography.Oid, System.Security.Cryptography.Oid...}
```

6. Ensure that the **Input SHA256 Fingerprint** and **Certificate SHA256 Fingerprint** values match to verify the SHA256 fingerprint of the certificate.



If you encounter an error about the execution policy, you can run the following command before you run the script: `Set-ExecutionPolicy RemoteSigned -Scope CurrentUser`

An alternative to running the provided script to verify the SHA256 fingerprint of the certificate is to issue the following commands on the server that was entered in **LDAP Server** in the **Add Domain** or **Edit Domain** panel:

```
certutil -store my <serialnumber> <outputfile>
certutil -hashfile <outputfile> sha256
```

In the commands, `<serialnumber>` corresponds to the serial number displayed in the **Add Domain** or **Edit Domain** panel and `<outputfile>` corresponds to a file to which you want to write the results.

For example:

```
PS C:\Users\Administrator.DEV> certutil -store my 123456789xzy output.cer
My "Personal"
================ Certificate 1 ================
```

© 2025 Tanium Inc. All Rights Reserved

```
Serial Number: 330000001edf2612e59ed68e9300000000001e
Issuer: CN=lab-2022CA01-CA, DC=lab, DC=example, DC=com
 NotBefore: 10/8/2024 12:27 PM
 NotAfter: 10/8/2025 12:27 PM
Subject: CN=2022DC02.dev.lab.example.com
Certificate Template Name (Certificate Type): DomainController
Non-root Certificate
Template: DomainController, Domain Controller
Cert Hash(sha1): d2ad6c2cb9a45b7997082e289e1abe7e7a20c2b2
  Key Container = d52364ec8ae4afabdf2705f81d51136b_bffa39fb-090b-42c0-b90a-8ab4432a94da
  Simple container name: te-DomainController-cc6b99e0-5d20-403a-9d8c-e964e2834660
  Provider = Microsoft RSA SChannel Cryptographic Provider
Private key is NOT exportable
Encryption test passed
CertUtil: -store command completed successfully.
```

Calculate the SHA256 hash of the certificate to verify the SHA256 fingerprint of the certificate:

```
PS C:\Users\Administrator.DEV> certutil -hashfile output.cer sha256
SHA256 hash of output.cer:
8be7eb2635927e413ac348f0b475cfd95fd01fd057c3cbcc8ecbe1ededb2a626
CertUtil: -hashfile command completed successfully.
```

The SHA256 hash of the output should correspond with the value of the SHA256 fingerprint of the certificate that appears in the **Add Domain** or **Edit Domain** panel.

© 2025 Tanium Inc. All Rights Reserved