Tanium™ Index User Guide

Version 3.1.904

September 17, 2021

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

Index overview

With Index, you can index the local file systems on Tanium Client endpoints that are running Windows, Linux, and macOS operating systems. Index is optimized to minimize endpoint resource utilization. The solution indexes local file systems, computes file hashes, and gathers file attributes and magic numbers. This information is recorded in an SQLite database for detection and reporting of threat indicators for files at rest.

Index is a feature common to many Tanium solution modules that exists as a client extension. Client extensions are an extensible framework of tools and processes that extend the functionality of the Tanium Client. Client extensions minimize the reproduction of code within different modules and solutions. A function or library is created once, then reused where necessary by Tanium solutions. Client extensions ultimately reduce the footprint of the Tanium Client on endpoints.

Overview

Index creates and maintains an inventory of the file system on an individual endpoint with the following operations:

- Detect file changes
- Compute file hashes
- Calculate magic number

The file system inventory is saved in the SQLite database on the endpoint.

Detect file changes

Any new file changes are captured in the database.

If a file is modified, the data in the database is updated. When a file creation or modification is detected, the file is indexed to include the file name, file size, file creation time, file modification time, and directory name.

Index does not detect changes made to only the attributes of a file, such as creation or modification timestamps. If the contents of a file are modified, Index records the new file modification timestamp but does not update the file creation timestamp.

If Tanium Recorder is deployed and operational on the endpoint, Index gets file change events from Recorder. If Recorder is not available, Index uses the platform-independent indexing method. With this method, changes take longer to pick up because Index gets file changes by traversing the directory tree.

Compute file hashes

Index computes and stores the hashes of files in the database. Index can record any combination of four different hash types: MD5, SHA-1, SHA-256, or SHA-512. You can disable calculation of hashes if desired.

Calculate magic number

The magic number is the first 4 bytes of the file. You can use the magic number to identify many types of files. Magic numbers are recorded for files that do not have a magic number entry.

Getting started

Follow these steps to configure and use Index.

Step 1: Install Client Index Extension

For more information, see Installing Client Index Extension.

Step 2: Use Client Index Extension as part of a Tanium solution to index file systems

For more information, see Indexing file systems.

Step 3: Use Index sensors to query indexed files

For more information, see Reference: Index sensors.

Index requirements

Review the requirements before you install and use Index.

Tanium dependencies

Make sure that your environment meets the following requirements.

Component	Requirement
Tanium™ Core Platform	7.3.314.4250 or later
Tanium™ Client	7.2.314.3211 or later. Some Tanium solutions that manage the deployment of configuration changes with Tanium Endpoint Configuration might require a higher client version.
Computer groups	When you first log into the Tanium Console after an installation of Tanium Server 7.4.2 or later, the server automatically imports the computer groups that Index requires. For earlier versions of the Tanium Server, or after upgrading from an earlier version, you must manually create the computer groups. See Create computer groups.

Endpoints

Supported operating systems

The following endpoint operating systems are supported with Index.

- Windows
- macOS
- Linux

Operating System	Version	Notes
Microsoft Windows Server	• Windows Server 2019 • Windows Server 2016 • Windows Server 2012, 2012 R2 • Windows Server 2008 R2	Standard, Enterprise, and Datacenter editions are supported, with or without the Server Core option enabled. The Nano Server option is not supported. Tanium modules that use Python Runtime Services require Windows Server 2008 R2 endpoints to have Service Pack 1 (SP1) or higher.
Microsoft Windows Workstations	• Windows 10 • Windows 8 • Windows 7	
macOS	• macOS 10.14 Mojave* • macOS 10.13 High Sierra • macOS 10.12 Sierra • OS X 10.11.1+ El Capitan	* Intel processor only If you enable the app notarization requirement (a security process that Apple introduced in macOS 10.15), you must install Tanium Client 7.2.314.3608 or later. See the Tanium™ Support Knowledge Base for the Minimum Tanium product versions required to support endpoints that run macOS 10.14 Mojave or later.

Operating System	Version	Notes
Linux	• Amazon Linux 2 LTS (2017.12) • Amazon Linux 1 AMI (2016.09, 2017.12, 2018.03) • Debian 10.x • Debian 9.x, 8.x • Debian 7.x, 6.x • Oracle Linux 8.x • Oracle Enterprise Linux 7.x, 6.x • Oracle Enterprise Linux 5.x • Red Hat Enterprise Linux (RHEL) 8.x • CentOS 8.x • Red Hat Enterprise Linux (RHEL) 7.x, 6.x • CentOS 7.x, 6.x • Red Hat Enterprise Linux (RHEL) 5.4 and later • CentOS 5.4 and later • SUSE Linux Enterprise Server (SLES) 15 • openSUSE 15.x • SUSE Linux Enterprise Server (SLES) 12 • openSUSE 12.x • SUSE Linux Enterprise Server (SLES) 11.3, 11.4 • openSUSE 11.3, 11.4 • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS • Ubuntu 16.04 LTS • Ubuntu 14.04 LTS	

Disk space requirements

To install Index normally, a minimum of 1 GB of free space must be available on the drive where Tanium Client is installed.

The amount of space the Index installation uses varies depending on how much space is used on the local disks that are being indexed. The actual space that is required for the Index database is proportional to the number of files and directories on the local disks and what hashes are configured. For a rough estimate, the Index database uses approximately 1 MB of space for each 1 GB of drive space that is used.

Host and network security requirements

Security exclusions

Your security administrator must create exclusions to allow Tanium processes to run without interference if security software monitoring system processes is in use. For a list of all security exclusions to define across Tanium, see Tanium Core Platform Deployment Reference Guide: Host system security exclusions.

Index security exclusions

Target Device	Notes	Process
Windows endpoints		*<Tanium Client>*\TaniumCX.exe
		<Tanium Client>\TaniumClientExtensions.dll
		<Tanium Client>\TaniumClientExtensions.dll.sig
		<Tanium Client>\extensions\TaniumIndex.dll
		<Tanium Client>\extensions\TaniumIndex.dll.sig
		<Tanium Client>\extensions\index\magic.mgc
Linux endpoints		*<Tanium Client>*/TaniumCX
		<Tanium Client>/libTaniumClientExtensions.so
		<Tanium Client>/libTaniumClientExtensions.so.sig
		<Tanium Client>/extensions/libTaniumIndex.so
		<Tanium Client>/extensions/libTaniumIndex.so.sig
		<Tanium Client>/extensions/index/magic.mgc
macOS endpoints		*<Tanium Client>*/TaniumCX
		<Tanium Client>/libTaniumClientExtensions.dylib
		<Tanium Client>/libTaniumClientExtensions.dylib.sig
		<Tanium Client>/extensions/libTaniumIndex.dylib
		<Tanium Client>/extensions/libTaniumIndex.dylib.sig
		<Tanium Client>/extensions/index/magic.mgc

Installing Client Index Extension on endpoints

Index is installed by a Tanium solution and serves the primary purpose of indexing files on endpoints. The following list details configuration files and software that is installed on endpoints for the modules that use Index.

/opt/Tanium/TaniumClient/extensions/libTaniumIndex.so (Linux)
/Library/Tanium/TaniumClient/extensions/libTaniumIndex.dylib (macOS)
C:\Program Files(x86)\Tanium\Tanium Client\extensions\TaniumIndex.dll (Windows)

The Index process.

/opt/Tanium/TaniumClient/extensions/libTaniumIndex.so.sig (Linux)
/Library/Tanium/TaniumClient/extensions/libTaniumIndex.dylib.sig (macOS)
C:\Program Files(x86)\Tanium\Tanium Client\extensions\TaniumIndex.dll.sig (Windows)

A signature file that you can use to verify that the contents of the SO, DYLIB, or DLL file is authentic and have not been tampered with.

/opt/Tanium/TaniumClient/extensions/index/index.db (Linux)
/Library/Tanium/TaniumClient/extensions/index/index.db (macOS)
C:\Program Files(x86)\Tanium\Tanium Client\extensions\index\index.db (Windows)

The database that Index creates. It contains file details.

/opt/Tanium/TaniumClient/extensions/index/index.db-shm (Linux)
/Library/Tanium/TaniumClient/extensions/index/index.db-shm (macOS)
C:\Program Files(x86)\Tanium\Tanium Client\extensions\index\index.db-shm (Windows)

A shared memory file. Database connections that share the same db file must update the same memory location to prevent conflicts.

/opt/Tanium/TaniumClient/extensions/index/index.db-wal (Linux)
/Library/Tanium/TaniumClient/extensions/index/index.db-wal (macOS)
C:\Program Files(x86)\Tanium\Tanium Client\extensions\index\index.db-wal (Windows)

A write journal that is useful for commits and database rollback purposes.

/opt/Tanium/TaniumClient/extensions/index/magic.mgc
/Library/Tanium/TaniumClient/extensions/index/magic.mgc
C:\Program Files(x86)\Tanium\Tanium Client\extensions\index\magic.mgc

A binary file that contains patterns to be tested for, what message or MIME type to print if a particular pattern is found, and additional information to extract from the file.

Starting and stopping Index

You might need to manually start or stop Index. For example, when troubleshooting you must resolve the underlying issue first and then manually restart Index. Or, if you find that Index is using more system resources than expected, you can stop Index and troubleshoot the issue with the risk of additional resource consumption.

In the event of a troubleshooting situation contact Tanium Support for help. To contact Tanium Support, sign in to https://support.tanium.com.

Indexing file systems

The TaniumCX binary is the framework for client extensions. TaniumCX loads components into memory for use by the client and Tanium solutions. Client extension processes are initiated and controlled by the `TaniumClient.exe -m` process.

Client extensions are installed by Tanium Endpoint Configuration and primarily exist on the file system within the TC\extensions folder. Client Extension logging is written to `<Tanium Client>\Logs\extensions0.txt`.

Two directories exist in the `\extensions` directory on each endpoint:

- The first folder is the `\extensions\config` folder - which contains files to handle the manifest operations and maintains the tools database that contains all current tool versions and files
- The second folder is the `\extensions\core` folder - which contains files to handle the I/O operations of Tanium solutions and facilitate communicate with the Tanium Server and Tanium Module Server.

Index performs two different kinds of work on files:

- Work to generate properties about a file such as the time the file was created and the size of the file.
- Work to generate properties about the contents of a file, such as the file hash, MIME type, and magic number.

Index calculates file content properties only when a file is in the scope of a solution that uses Index.

A scope defines the parameters of an Index scan, including a single scan origin that acts as the starting point of the scope. This can be a single directory, drive, or all drives. If a system has two drives, and you use the ‘all drives’ predefined origin, Index creates two scopes, one for each drive. As a result, two scans run in parallel.

Index resolves scope paths that are symbolic links at both the creation time of the scan object and when a scan starts. The registration reply includes the requested path to the physical path mapping. All paths reported from Index from a journal or database represent the physical path.

Index determines the scopes to which a given path belongs. When a scope is removed, Index checks the scope root for overlapping scans. If a scope no longer applies to any other scopes, Index triggers a removal of the root directory and quickly removes the data from the database.

Tanium solutions using Index data register a subscription with a domain and a name pair that must be unique to the subscription. This is the main identifier consumers use to configure Index. A subscription contains one or more scopes, which then define how Index should interact with a given directory. Scopes can and will overlap within a subscription or across subscriptions. The configuration parameters of one scope do not impact other scopes.

File system indexing occurs by "walking" the file system. A periodic crawl is necessary to ensure data correctness and integrity. Index cannot exclusively rely on the recorder for event data as it is entirely possible that a file has been modified offline. The walk frequency is controlled by the scope.

To walk a file system, the file tree must be complete. All scans start at the device root and walk subdirectories. When walking a file system, deleted files within a scope are detected. When entering a directory, Index checks the Index database to determine if the directory is listed. If the configured time has elapsed, Index compares the content in the database with what is presently detected on the filesystem. If it is time to enumerate, scope membership of the directory is determined. If no scopes include a particular directory, the walk stops.

If the scope membership specifies to open the file, the file modification time and last digested time values are compared with the database. If sufficient time has passed, or the mtime differs, the digested work is performed and changes stored in the database.

Customize Index endpoint settings

Customize Index configuration settings to provide functionality and database parameters. Making changes to Index settings can cause performance impacts.

To change the value of a setting, use the TaniumClient config command:
`./TaniumClient config set CX.index.<setting name> <value>`

Alternatively, you can use Tanium Interact to issue a question, analyze the question results, and determine which endpoints require administrative action and deploy actions to those endpoints. To target endpoints, issue a question in Interact. In the **Question Results** grid, select the rows for the endpoints that require the action, and click **Deploy Action**. From the Deploy Action page, use the Deployment Package search box typeaheads to select packages. Select the **Modify Tanium Client Setting** or **Modify Tanium Client Setting [Non-Windows]** package. For the Windows package, REG_SZ is string, and REG_DWORD is int. For the Non-Windows package, the type is either string or numeric. For **ValueName** provide the fully-qualified name of the setting; for example, `CX.index.DBCommitIntervalSeconds`. Provide a value. Configure a **Deployment Schedule** and **Targeting Criteria**. Click **Deploy Action**. For more information, see Deploying actions.

.

Setting	Value	Description
MaxHashSizeMB	INT	The maximum file size in MB to hash. (Default: 32)
FirstScanDistributeOverTimeMinutes	INT	The delay time (in minutes) after Index starts before starting the initial index scan. (Default: 1440)
FirstScanDistributeOverTimeTimeoutDays	INT	If a scan is overdue to start by more than this duration, reschedule the scan using the distribute over time logic. (Default: 7 days)

Reference: Index sensors

Use the Index sensors to get details about files that have been indexed.

Sensor	Description
Index - File Count	Returns count of index files that match one or more supplied inputs. The Index - File Count sensor supports both wildcards and regular expressions. Supported wildcard syntax includes the character to match any number of characters and the ? character to match one character. For example, you can use `pad.exe` to search for either `notepad.exe` or `wordpad.exe`. To use regular expressions in parameter values, select **Use Regular Expressions**. You can use regular expressions to search for more complex patterns and to further constrain the scope of the search. For example, `^(if|ip)config(.exe)?$` matches `ifconfig`, `ipconfig`, `ifconfig.exe`, and `ipconfig.exe`.
Index - File Details	Returns details of index files that match one or more supplied inputs. The Index -File Details sensor supports both wildcards and regular expressions in parameters with the exception of the Maximum Number of Rows. Supported wildcard syntax includes the character to match any number of characters and the ? character to match one character. For example, you can use `pad.exe` to search for either `notepad.exe` or `wordpad.exe`. To use regular expressions in parameter values, select **Use Regular Expressions**. You can use regular expressions to search for more complex patterns and to further constrain the scope of the search. For example, `^(if|ip)config(.exe)?$` matches `ifconfig`, `ipconfig`, `ifconfig.exe`, and `ipconfig.exe`.
Index - File Exists	Returns Yes or No, using Index to determine whether specified file exists based on the supplied input. The Index - File Exists sensor uses Tanium Index to determine whether the specified file(s) exist on the endpoints and returns "Yes" or "No". The Index - File Exists sensor supports both wildcards and regular expressions. Supported wildcard syntax includes the character to match any number of characters and the ? character to match one character. For example, you can use `pad.exe` to search for either `notepad.exe` or `wordpad.exe`. To use regular expressions in parameter values, select **Use Regular Expressions**. You can use regular expressions to search for more complex patterns and to further constrain the scope of the search. For example, `^(if|ip)config(.exe)?$` matches `ifconfig`, `ipconfig`, `ifconfig.exe`, and `ipconfig.exe`.

Sensor	Description
Index - File Hash Recently Changed	Returns filename and hash(es) of file created or modified in previous N hours. The Index - File Hash Recently Changed sensor returns filenames and hashes for files that have been created or modified within a given number of hours. For example, you can search for binary files that have been created or modified under `C:\WindowsSystem32` in the previous 8 hours. By searching for files with a File Magic Number glob of 4D5A, you can focus your search on Windows PE binary files (EXEs and DLLs). The Index - File Hash Recently Changed sensor supports both wildcards and regular expressions in parameters with the exception of the Maximum Number of Rows and Lookback Hours parameters. Supported wildcard syntax includes the character to match any number of characters and the ? character to match one character. For example, you can use `pad.exe` to search for either `notepad.exe` or `wordpad.exe`. To use regular expressions select **Use Regular Expressions**. You can use regular expressions to search for more complex patterns and to further constrain the scope of the search. For example, `^(if|ip)config(.exe)?$` matches `ifconfig`, `ipconfig`, `ifconfig.exe`, and `ipconfig.exe`.

There is no longer an Index DB Size Sensor for Index. Use the Sensor "File Size" from default content.

```
Get File Size["c:\Program Files (x86)\Tanium\Tanium
Client\extensions\index\index.db"] from all machines
```

The following Index sensors have been deprecated:

- Index Has Latest Tools
- Index Query File Count
- Index Query File Details
- Index Query File Details by Last Modified
- Index Query File Details Using Name
- Index Query File Details Using Name Sort By Largest
- Index Query File Exists
- Index Query File Hash Recently Changed
- Index Query File Path and Hash
- Index Query File Path Using Name
- Index Query File Permissions
- Index Query Find Blacklist Matches

- Index Resolved Config
- Index Status
- Index Version

Reference: Manage high-priority paths

Tanium Threat Response uses Index to scan the entire disk on an endpoint at regular intervals that typically occur between once a day and once a week. Index does not use recorder events to update file data across the entire disk. Many Threat Response users want more frequent updates for files in certain regions of the disk. To provide this visibility, in addition to the baseline disk scan, Threat Response enables you to specify high priority paths that use recorder events to update data and also scans every 24 hours by default.

A high priority path must include a `file.path starts with` clause in Tanium signal syntax. Escape backslash characters in paths. For example, use C:\\Users\\Administrator to make C:\Users\Administrator a high profile path.

- Supported: `file.path starts with 'C:\\Users\\Administrator'`
- Unsupported: `file.path starts with 'C:\'`

A high priority path, in addition to the `file.path starts with` clause, can additionally specify one or more `file.path ends with` clauses to narrow the file types to inspect.

- Supported: `file.path starts with 'C:\\Users\Administrator' and file.path ends with '.dat'`
- Supported: `file.path starts with 'C:\\Windows\\System32' and file.path ends with '.dll' and file.path ends with '.exe'`
- Unsupported: `file.path ends with '.dat'` (Note that the `file.path ends with` must be combined with a `file.path starts with` filter)

A high priority path can include one wildcard, indicated by an asterisk, in the `starts with` clause. The wildcard must appear two or more levels deeper than the disk root.

- Supported: `file.path starts with 'C:\\Users\\*\\Downloads'`
- Unsupported: `file.path starts with 'C:\*\Tanium'`
- Unsupported: `file.path starts with '*:\Program Files'`