

Tanium™ Impact User Guide

Autonomous IT. Unstoppable Business.

2025H1 and 2025H2 Semiannual Release

Version 2.5

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

Impact overview **8**

Reduce attack surface 8

Prioritize actions 8

Scope incidents 8

Credential dumping and lateral movement 8

Impact rating 12

Example 12

Interoperability with other Tanium products 13

Connect 13

Criticality 13

Trends 13

Threat Response 14

Gaining organizational effectiveness with Impact **15**

Change management 15

RACI chart 15

Operational metrics 19

Impact maturity 19

Benchmark metrics 19

Organizational alignment 21

Impact requirements **22**

Core platform dependencies 22

Solution dependencies 22

Tanium recommended installation 22

Import specific solutions 22

Required dependencies 22

Feature-specific dependencies 23

Client extensions and endpoint tools 23

© 2025 Tanium Inc. All Rights Reserved

Tanium™ Module Server ... 23
Endpoints ... 23
Supported operating systems ... 23
Host and network security requirements ... 24
Ports ... 24
Security exclusions ... 24
User role requirements ... 26
Installing Impact ... 29
Before you begin ... 29
Import Impact with default settings ... 29
Import Impact with custom settings ... 30
Manage solution dependencies ... 30
Upgrade Impact ... 30
Verify Impact version ... 30
Configuring Impact ... 31
Install and configure Tanium Endpoint Configuration ... 31
Manage solution configurations with Tanium Endpoint Configuration ... 31
Configure Impact ... 32
Configure the Impact action group ... 32
Configure synchronization settings ... 32
Configure connections to domains ... 33
Collect and analyze data ... 33
Set up Impact users ... 33
Identifying high impact users, endpoints, and groups ... 35
Overview ... 35
Impact rating ... 35
Before you begin ... 35
Explore the users with the highest impact rating ... 36
Explore the groups with the highest impact rating ... 37
Explore the endpoints with the highest impact rating ... 39

© 2025 Tanium Inc. All Rights Reserved

Exporting tables ... 41
Analyzing the impact ... **42**
Overview ... 42
Before you begin ... 42
Analyze the impact for a specific user, group, or endpoint ... 42
Explore impact graphs ... 42
View summary ... 43
View indirect / direct control ... 46
View outbound impact ... 48
View inbound impact ... 48
View sessions ... 49
View members ... 50
View shortest path maps ... 51
What to do next ... 52
Exporting Impact data ... **53**
Connections to create ... 53
Create connection to export Impact data ... 53
CSV example: Impact data export ... 53
JSON example: Threat Response alert with Impact data export ... 54
Maintaining Impact ... **59**
Perform monthly maintenance ... 59
Monitor and troubleshoot Impact Coverage ... 59
Troubleshooting Impact ... **61**
Collect logs ... 61
Upgrade Impact ... 61
Troubleshoot unresolved SIDs ... 62
Identify and resolve issues with Client Extensions ... 63
Review the Extensions log for an endpoint ... 65
Remove Impact tools from endpoints ... 65
Verify endpoint tools ... 66

© 2025 Tanium Inc. All Rights Reserved

Uninstall Impact 66
Contact Tanium Support 67
Reference: Impact sensors **68**
Reference: Remediation resources **70**

© 2025 Tanium Inc. All Rights Reserved

Impact overview

Use Impact to understand administrative rights in the Active Directory environment for your organization and the potential impact if a compromise occurs. Manage lateral movement impact within your organization by identifying, prioritizing and remediating access rights and dependencies to reduce attack surface, prioritize actions, and scope incidents.

Reduce attack surface

Identify and quantify the user accounts that have administrative access to key systems, such as high-profile workstations or Active Directory domain controllers. By limiting administrative access to these systems, you can reduce your attack surface.

Prioritize actions

Quickly identify the user accounts and systems that would have the most significant impact if compromised. With this information, you can focus on these high-impact accounts or systems to limit potential lateral movement in the event of an attack.

Scope incidents

If a user account or system is compromised, use Impact to quickly determine the potential lateral movement of the attack and take action to prevent additional compromise.

Credential dumping and lateral movement

When a user logs in to a computer, either locally or remotely, a session is created that caches the user credentials in memory for 72 hours and until a restart. Attackers can use malicious tools, often referred to as *credential dumpers*, to access these cached credentials. Attackers then use the credentials to impersonate the compromised user and gain access to other systems in your environment. This potential *lateral movement* is more severe if the compromised user is a member of privileged groups, which might contain additional nested groups, and can rapidly compromise a large number of systems in your environment.

For more information, see MITRE ATT&CK: Credential Dumping and MITRE ATT&CK: Lateral Movement.

In Impact, this potential lateral movement is broken down further into *outbound impact* and *inbound impact*.

outbound impact

The endpoints or users that an attacker can breach from the current endpoint, user, or group (*asset*). Use outbound impact to answer the question: what endpoints, users, and groups can an attacker potentially breach through lateral movement if this asset is compromised?

inbound impact

The endpoints or users that an attacker can use to breach the current endpoint, user, or group. Use inbound impact to answer the question: what lateral movement could an attacker potentially use to breach this asset?

© 2025 Tanium Inc. All Rights Reserved

Impact analyzes both *direct control* and *indirect control* when evaluating the potential movement of an endpoint, user, or group.

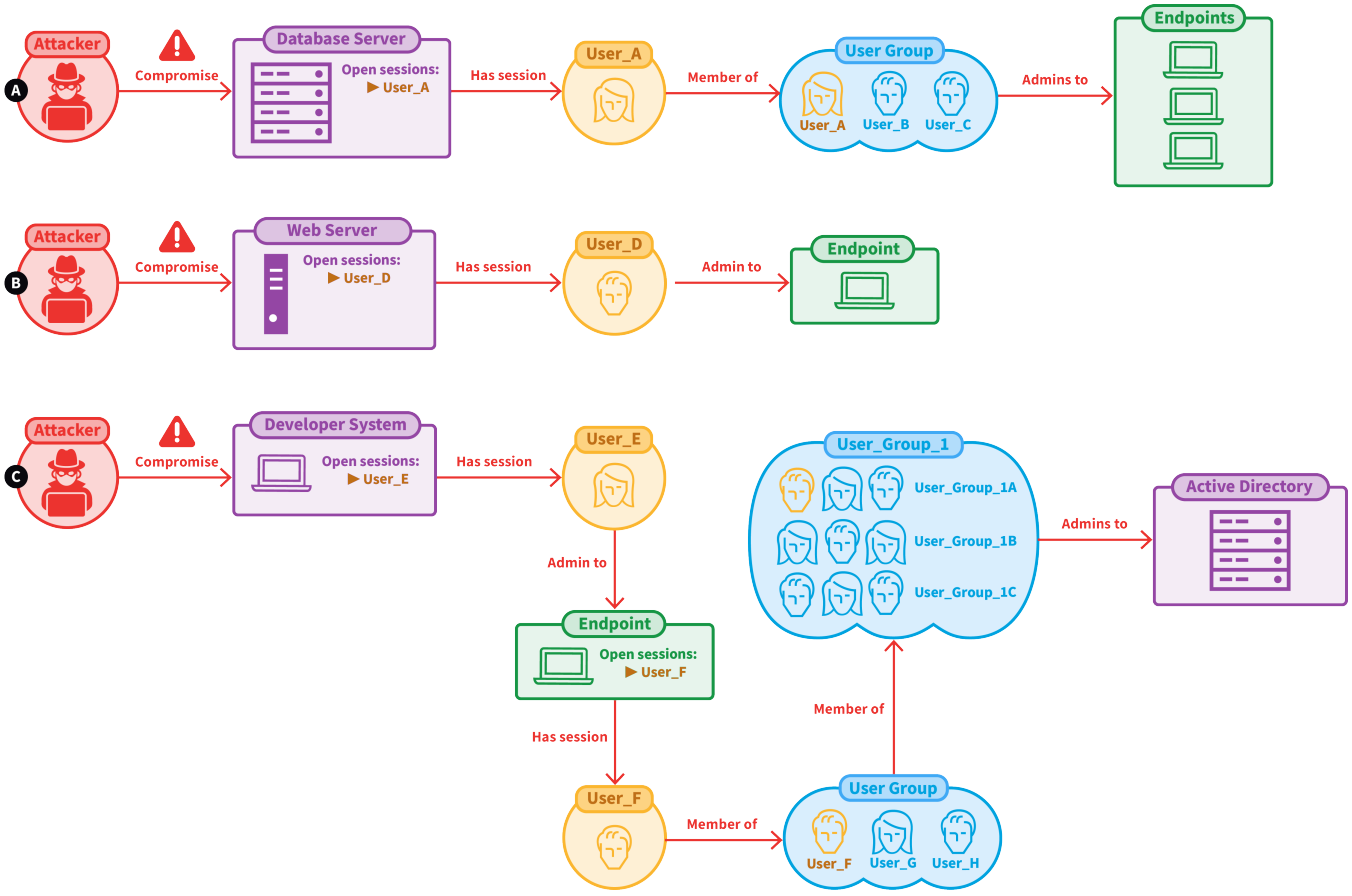
direct control

The user has administrative rights to a system through a direct entry in the local Administrators object on the system, not through an Active Directory group membership.

indirect control

The user has administrative rights to a system through an Active Directory group or nested group that has an entry in the local Administrators object on the system.

Using lateral movement to prioritize decision making

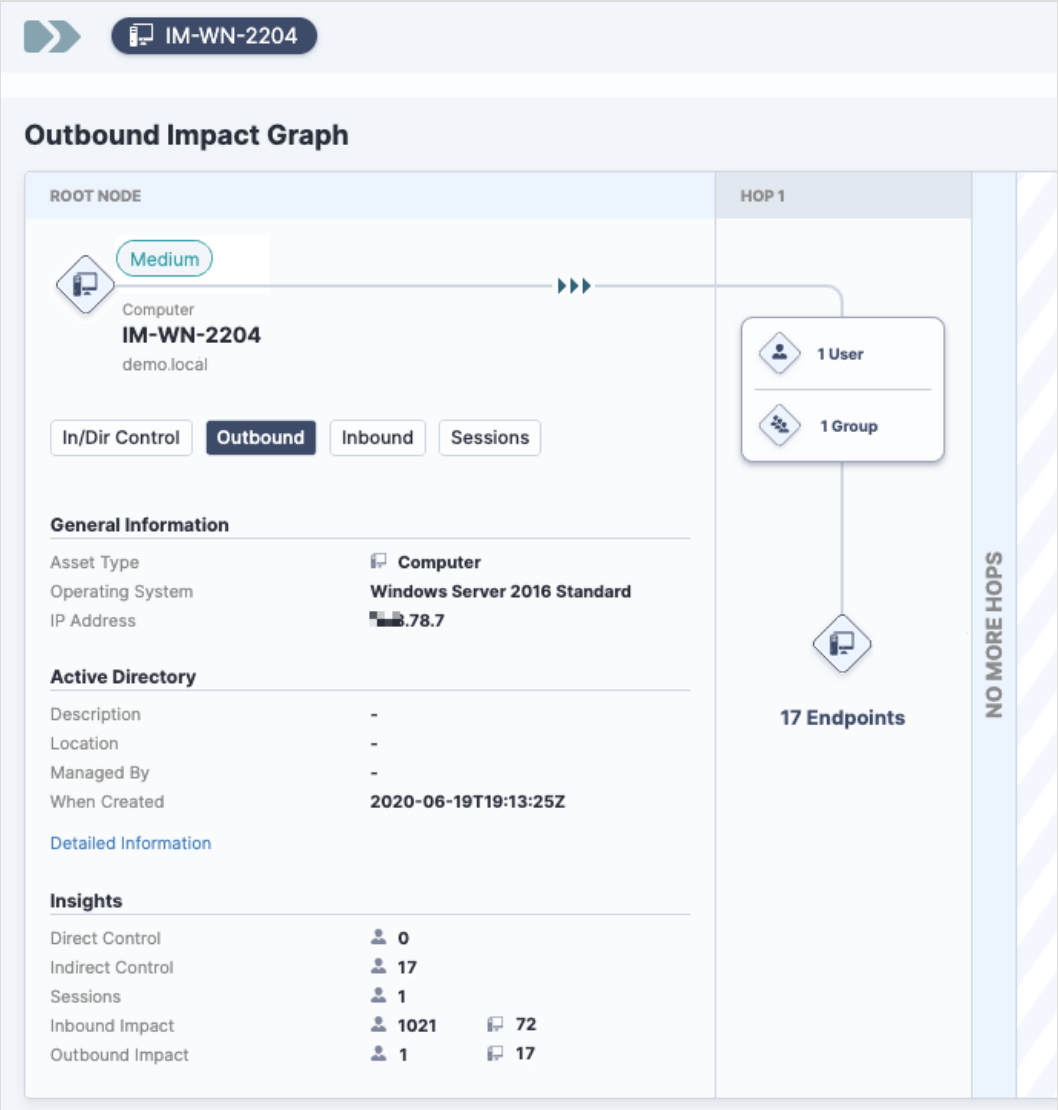


In scenario A in the preceding figure, the attacker compromises the database server, on which User_A has an open session. You can visualize the outbound impact of this breach and potential lateral movement by running an **Outbound Impact** search on the Database Server, IM-WN-2204.

The attacker uses User_A's session to obtain the credentials for User_A. Because User_A is a member of a user group, the attacker now has access to all endpoints on which there is an entry in the local Administrators object on the endpoint for this user group, which is shown in Impact through indirect control analysis.

© 2025 Tanium Inc. All Rights Reserved

Outbound impact graph

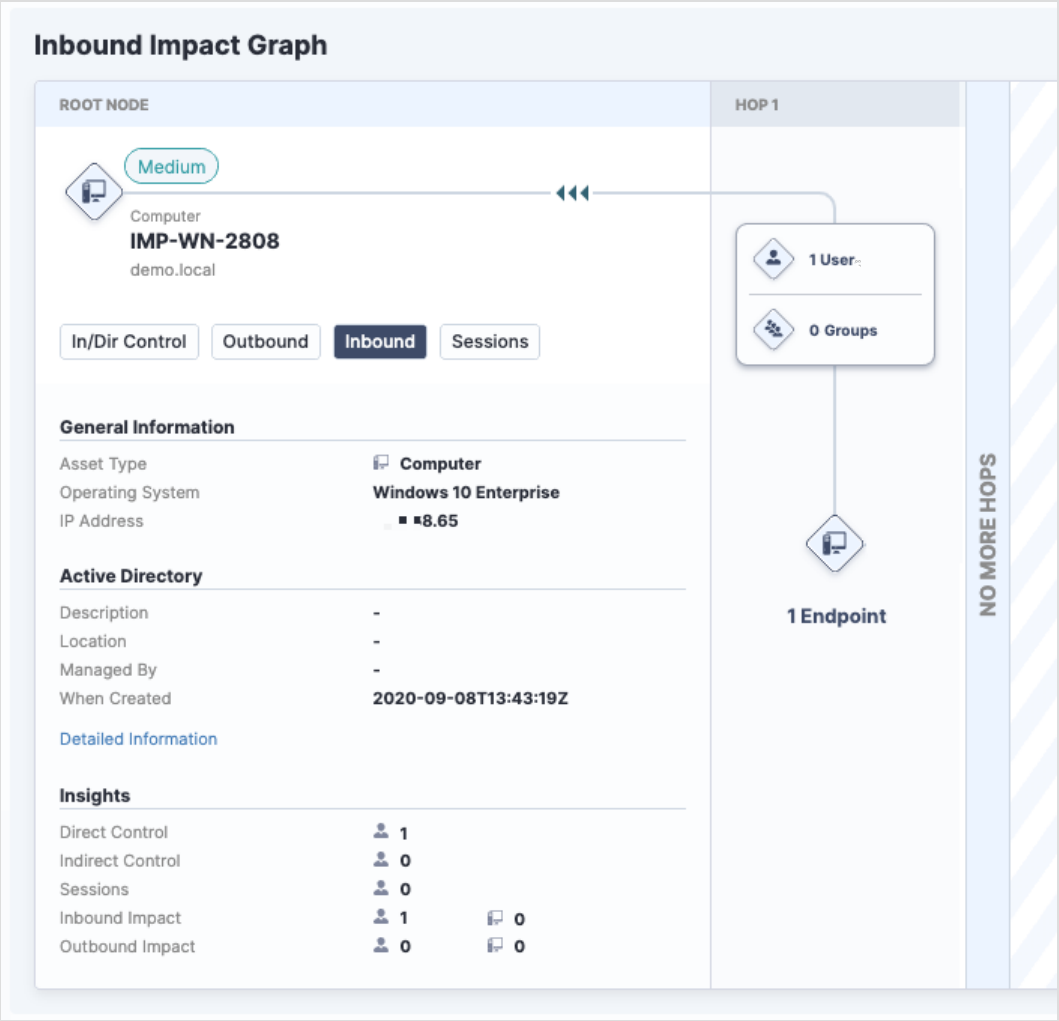


In scenario B in the preceding figure, suppose the target endpoint is the CEO's laptop. To determine how an attacker could potentially breach this high profile endpoint, run an **Inbound Impact** search for the endpoint, IMP-WN-2808.

The analysis by Impact shows that if an attacker breaches the Web Server, on which User_D has an open session, the attacker can use User_D's credentials to gain administrator access to this endpoint. Click a hop in the hop map to display the specific endpoints, users, and groups that are part of the potential lateral movement.

© 2025 Tanium Inc. All Rights Reserved

Inbound impact graph



In scenario C in the preceding figure, the attacker could potentially use both direct and indirect control to breach the Active Directory server. Impact provides multiple methods to analyze the various ways that an attacker could move through your network. For example, you can analyze the indirect and direct control for User_Group_1 to see which endpoints can be reached by this group, either through direct membership on an endpoint or nested groups.

You can run an **Inbound Impact** search on the Active Directory server to see how an attacker might gain access to that server.

You can run an **Outbound Impact** search on the developer's system to determine what users, endpoints, and groups might be compromised through potential lateral movement if an attacker breaches that endpoint.

If you do not have specific users, endpoints, or groups that you want to analyze, use the Impact ratings to quickly identify critical and high risk assets.

© 2025 Tanium Inc. All Rights Reserved

Impact rating

Impact analyzes the data from synchronized domains and calculates an *impact rating* for each endpoint, user, or group. Four factors influence an impact rating:

- Potential inbound impact by users
- Potential inbound impact by endpoints
- Potential outbound impact by users
- Potential outbound impact by endpoints

Impact calculates a percentage for each factor based on the total number of endpoints, users, and groups in the synchronized domains. Using this percentage, points are assigned to each factor:

- **0% - 25% of total users or endpoints**: 1 point
- **26% - 50% of total users or endpoints**: 2 points
- **51% - 75% of total users or endpoints**: 3 points
- **76% - 100% of total users or endpoints**: 4 points

Impact tallies the points for each factor and applies the following schema to reach the final impact rating:

- **Low**: 4 points
- **Medium**: 5 - 8 points
- **High**: 9 - 12 points
- **Critical**: 13 - 16 points



The Impact workbench displays the impact rating (**Low**, **Medium**, **High**, **Critical**) for each endpoint, user, or group. For simplicity, the workbench does not display the points. The total number of points for an endpoint, user, or group are available in the CSV and JSON outputs. For more information, see Exporting Impact data on page 53.

Endpoints, users, and groups with a critical impact rating have the highest potential lateral movement and are likely to be targeted for compromise. Potential inbound movement, which can compromise the endpoint, user, or group, and potential outbound movement, which can compromise other endpoints, users, and groups, are used to calculate this rating.

Example

Consider an organization that has synchronized two domains with Impact. These domains contain 1,000 users and 2,000 endpoints, for a total of 3,000 assets.

© 2025 Tanium Inc. All Rights Reserved

User A has the following inbound and outbound impact:

- **Inbound impact by users**: 620 users (62% of all users, 3 points)
- **Inbound impact by endpoints**: 630 endpoints (31.5% of all endpoints, 2 points)
- **Outbound impact by users**: 400 users (40% of all users, 2 points)
- **Outbound impact by endpoints**: 600 endpoints (30% of all endpoints, 2 points)

The points for all four factors total 9, so the impact rating for User A is `High`.

Interoperability with other Tanium products

Impact works with Tanium™ Connect, Tanium™ Criticality, Tanium™ Trends, and Tanium™ Threat Response for additional visibility and reporting of related data.

Connect

Use Connect to send Impact data to destinations, such as email, HTTP, socket receiver, Splunk, and SQL Server. For more information, see Connect User Guide: Connect overview.

Criticality

Impact uses Active Directory and criticality data from Criticality. For more information, see Tanium Criticality User Guide: Criticality overview.

Trends

Impact features a Trends board that provides data visualization of Impact concepts. The Impact board contains the following panels:

Impact Coverage Status

Shows the percentage of total Tanium-managed Windows endpoints where Impact is optimal, needs attention, or is not supported.

Impact Severity Rating for All Endpoints

Shows the severity rating for all domain-joined endpoints.

Impact Severity Rating for All Users

Shows the severity rating for all domain users.

Impact Severity Rating for All Groups

Shows the severity rating for all domain groups.

© 2025 Tanium Inc. All Rights Reserved

Impact Severity Rating for All Assets

Shows the severity rating for all domain users, groups, and computers.

Threat Response

Use Impact with Threat Response to see details from Impact in alerts. The Threat Response alerts results grid includes an **Outbound Impact** column, and the **Impact Details** section of the alert details provides information from Impact on the potential lateral movement of the endpoint to help prioritize alert remediation. For more information, see Threat Response User Guide: Manage the impact of lateral movement with Tanium Impact.

© 2025 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Impact

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

- Develop a dedicated change management process. See Change management on page 15.
- Define distinct roles and responsibilities. See RACI chart on page 15.
- Track operational maturity. See Operational metrics on page 19.
- Validate cross-functional alignment. See Organizational alignment on page 21.

Change management

Develop a tailored, dedicated change management process to monitor and remediate possible lateral movement activities and overly permissive administrative privileges, taking into account the new capabilities provided by Tanium.

- Update SLAs with elevated expectations for Tanium Impact activities across IT Security, IT Operations, and IT Risk/Compliance.
- Identify key resources in the organization to monitor asset privileges to reduce the attack surface and achieve the desirable Mean Impact Rating.
- Align activities to key resources for risk monitoring of endpoints, users and Active Directory (AD) groups across IT Security, IT Operations, and IT Risk/Compliance.
- Identify business critical assets for risk monitoring prioritization.
- Create a Tanium steering group (TSG) to expedite reviews and approvals of processes that align with SLAs that are associated with risk.

RACI chart

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

© 2025 Tanium Inc. All Rights Reserved

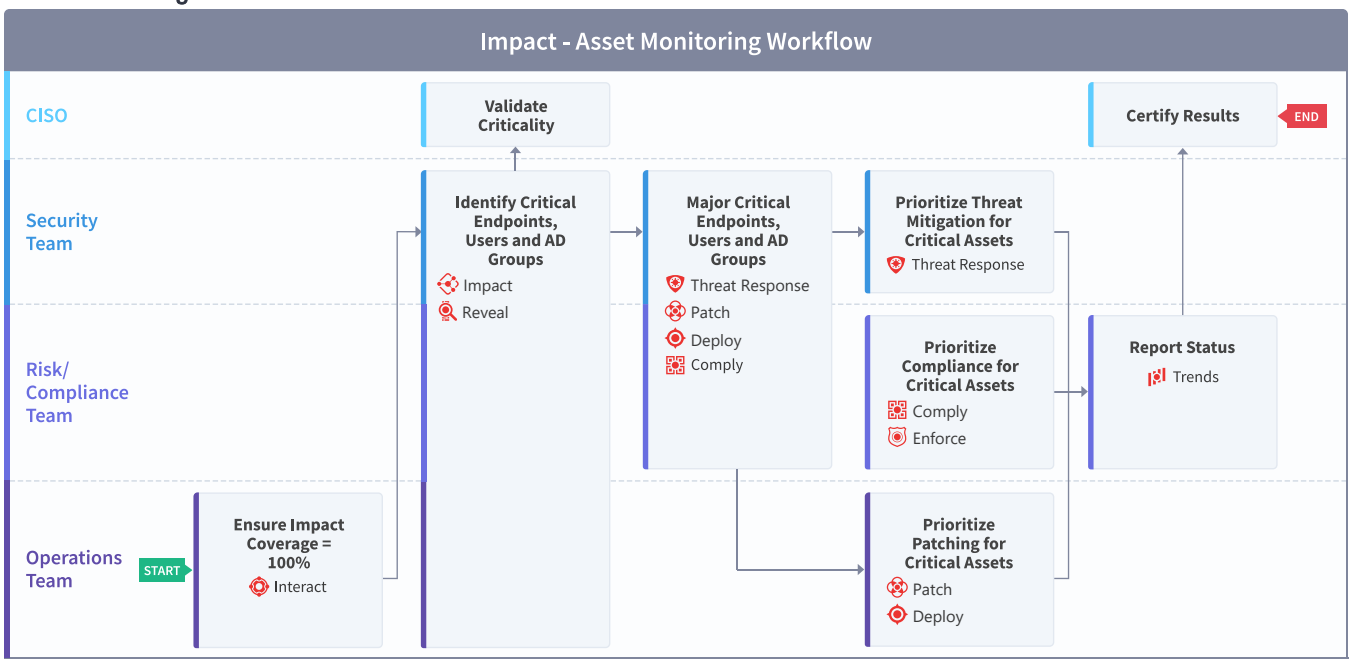
Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Impact coverage of domain-joined endpoints See Asset monitoring workflow on page 18.	C	A/R	C	-	The IT Operations team owns the Tanium platform and is accountable and responsible for the deployment of the Tanium agent, including the Impact module. Tanium agent coverage is essential to understand potential lateral movement across the environment. IT Operations consults with the IT Security and IT Compliance teams on the coverage to identify gaps.
Identify and monitor business critical endpoints	A	R	C	I	The IT Security team monitors business critical endpoints to ensure actions can be taken to reduce risk prior to being compromised. The IT Operations team identifies business critical assets and consults with the IT Compliance team to ensure accurate identification of those business critical endpoints. The Executive team is informed to monitor risk.
Identify and monitor users and AD groups with administrative rights to critical endpoints	A/R	C	C	I	The IT Security team identifies and monitors users with administrative rights to critical endpoints to analyze and remediate associated risks. The IT Security team consults with the IT Operations and IT Compliance teams to verify the criticality of endpoints, the privileges of users, and the coverage of Impact. The Executive team is informed in the assessment of potential lateral movement for assets.

© 2025 Tanium Inc. All Rights Reserved

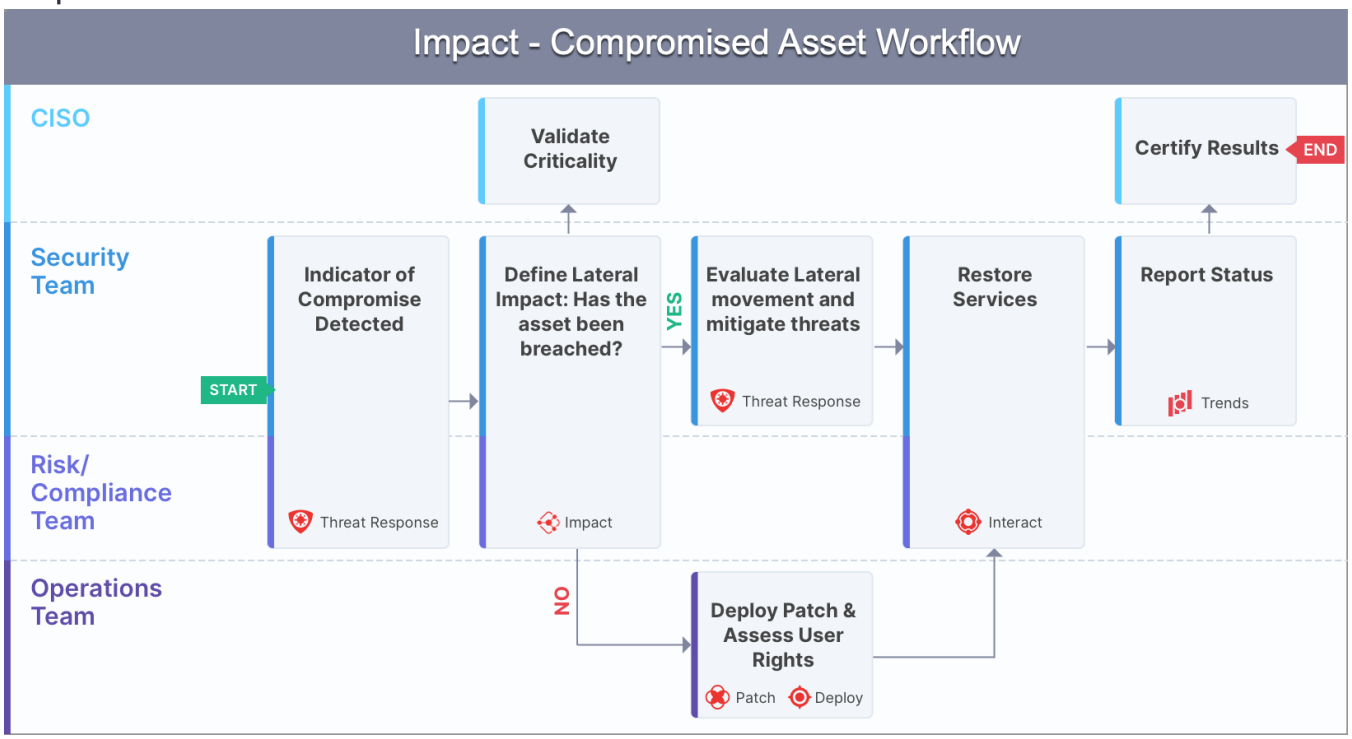
Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Monitor the mean impact rating for endpoints, users, and groups	A/R	R	R	C	The IT Security team monitors the mean impact rating for all endpoints, users, and groups so action can be taken if risk levels are too high. The IT Operations and IT Compliance teams verify asset criticality, ensure Impact coverage, and take necessary actions to reduce the mean impact rating over time. The Executive team is consulted on acceptable risk levels and the actions taken to reduce risk.
Assess lateral movement from a compromised asset See Compromised asset workflow on page 18.	A/R	R	C	I	The IT Security team is accountable and responsible for discovering the indicator of compromise, assessing lateral movement paths, scoping the incident, and mitigating the threat. The IT Operations team is responsible for remediation actions, such as patching vulnerabilities, with direction from the IT Security team. The IT Compliance team is consulted throughout the process to monitor risk and remediation efforts. The Executive team is informed of the discovery and remediation of the threat.

© 2025 Tanium Inc. All Rights Reserved

Asset monitoring workflow



Compromised asset workflow



© 2025 Tanium Inc. All Rights Reserved

Operational metrics

Impact maturity

Managing enterprise risk successfully includes operationalization of the technology and measuring success through key benchmarking metrics. The four key processes to measure and guide operational maturity of your Tanium Impact program for lateral movement are as follows:

Process	Description
Usage	how and when Tanium Impact is used in your organization; is Impact the only tool used to provide an overview of administrative access rights with domain-joined Windows endpoints
Automation	how automated Tanium Impact is, across endpoints
Functional Integration	how integrated Tanium Impact is, across IT Security, IT Operations, and IT Risk/Compliance teams
Reporting	how automated Tanium Impact is; what is the frequency and who is the audience of Impact-related reporting

Benchmark metrics

In addition to the key Tanium Impact processes, the two key benchmark metrics that align to the operational maturity of the Tanium Impact program to achieve maximum value and success are as follows:

Executive Metrics	Impact Coverage
Description	Returns the number of endpoints in each of these categories: • **Initializing**: Endpoints where Impact tools are installing • **Optimal**: Endpoints where Impact is operational • **Needs attention**: Endpoints that do not have the Python tools installed or do not have a supported version of the Tanium Client installed • **Unsupported**: Endpoints with an operating system version that is not supported by Impact For steps to investigate endpoints that are categorized as **Needs Attention** or **Unsupported**, see Monitor and troubleshoot Impact Coverage. For operating system and Tanium Client versions supported by Impact, see Requirements.
Instrumentation	Uses the `Impact - Coverage Status` sensor to determine the endpoints where Impact is optimal, needs attention, and is unsupported.
Why this metric matters	If you do not have Impact running on all of your endpoints, you do not have insight into the administrative rights in your organization's Active Directory environment and their potential impact if compromised.

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

© 2025 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Impact is not fully or correctly configured and not active	Impact is configured and active, but lacks enough coverage (<70%) for sensors to correctly execute. Leverage default Tanium Criticality levels for prioritization of investigation.	Impact is configured and active, but lacks enough coverage (<70%) for sensors to correctly execute. Create custom rules for Tanium Criticality levels of prioritization.	Impact is configured, active, and coverage >95%. Create rules for low, medium, high, and critical Tanium Criticality levels for prioritization.	Impact is configured, active, and 100% of endpoints are covered. Create rules for all Tanium Criticality levels for endpoints, users, and groups in the environment.
	Automation	Manual	Manual	Manual	Manual	Manual
	Functional integration	Impact is functionally siloed within the IT Security team	Impact is functionally siloed within the IT Security team and only used to assess a breach	The IT Security team uses Impact to monitor the potential for lateral movement	Impact is integrated between the IT Security, IT Compliance and IT Operations teams to assess the potential for lateral movement	Impact is fully integrated across the IT Security, IT Compliance and IT Operations teams to assess the potential for lateral movement and take actions to proactively reduce risk
	Reporting	Unused	Ad hoc; Reporting tailored to stakeholders on request	Consistent; Reporting tailored to stakeholders on cadence	Automated; Reporting tailored to stakeholders ranging from Operator to Executive	Automated; Reporting tailored to stakeholders ranging from Operator to Executive
Metrics	Impact Coverage[1]	0-49%	50-69%	70-94%	95-99%	100%

[1] Coverage refers to the percentage of endpoints with the Tanium Client installed.

© 2025 Tanium Inc. All Rights Reserved

Organizational alignment

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

In the absence of cross-functional alignment, functional silos often spend time and effort in litigating data quality instead of making decisions to reduce the attack surface.

© 2025 Tanium Inc. All Rights Reserved

Impact requirements

Review the requirements before you install and use Impact.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Impact. For more information about how to get Impact, 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 Impact to function (required dependencies) or for specific Impact features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.



Some Impact dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 22 and Feature-specific dependencies on page 23. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Impact requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Impact, 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 Impact 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 Impact, the server automatically updates those dependencies to the latest available versions.

Required dependencies

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

© 2025 Tanium Inc. All Rights Reserved

- Tanium™ Interact
- Tanium™ System User Service
- Tanium™ RDB Service
- Tanium™ Directory Query
- Tanium™ Criticality
- Tanium™ Endpoint Configuration

Feature-specific dependencies

Impact has the following feature-specific dependencies:

- Tanium Connect is required to send Impact data to destinations.
- Tanium Threat Response is required to display Impact ratings for alerts in Threat Response.
- Tanium Trends is required to view the Impact Trends board.

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for Impact on endpoints. Client extensions perform tasks that are common to certain Tanium solutions. Each Client Extension and tool might have recommended security exclusions to allow them to run without interference. For more information, see Security exclusions. For a list of all Client Extensions and tools, see Tanium Client Management User Guide: Reference: Client extensions used for Tanium solutions.

Tanium™ Module Server

Impact 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

Supported operating systems

Supported operating systems for Tanium Impact

Operating system	OS version	Notes
Microsoft Windows Server	Microsoft Windows Server 2008 R2 (SP1) and later	Windows Server 2008 R2 SP1 requires Microsoft KB2758857.
Microsoft Windows Workstation	Microsoft Windows 7 (SP1) and later	Windows 7 Service Pack 1 requires Microsoft KB2758857.

© 2025 Tanium Inc. All Rights Reserved

Host and network security requirements

Specific ports and processes are needed to run Impact.

Ports

Ports for Tanium Impact communication

Source	Destination	Port	Protocol	Purpose
Module Server or satellite	Active Directory Server	389 / 636	LDAP / LDAPS	Connecting to the Active Directory server.
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 Configure connections to domains.

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.

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

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\impact-service\TaniumImpactService.exe`
		Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`

© 2025 Tanium Inc. All Rights Reserved

Impact security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows	Endpoints with a Toolset version earlier than 2.7	Process	`<Tanium Client>\Python38\TPython.exe`

© 2025 Tanium Inc. All Rights Reserved

Impact security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	Endpoints with a Toolset version earlier than 2.7	Folder	`<Tanium Client>\Python38`
	Endpoints with Toolset version 2.7 or later	Folder	`<Tanium Client>\TPython312`
	Endpoints with Toolset version 2.7 or later	Process	`<Tanium Client>\TPython312\TPython.exe`
	Endpoints with Toolset version 2.7 or later	Folder	`<Tanium Client>\python312`
		Process	`<Tanium Client>\TaniumCX.exe`
		File	`<Tanium Client>\TaniumClientExtensions.dll`
		File	`<Tanium Client>\TaniumClientExtensions.dll.sig`
	When Direct Connect is installed; satellite sync only	File	`<Tanium Client>\extensions\TaniumDEC.dll`
	When Direct Connect is installed; satellite sync only	File	`<Tanium Client>\extensions\TaniumDEC.dll.sig`

User role requirements

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

© 2025 Tanium Inc. All Rights Reserved

- Impact user role permissions on page 27
- Impact platform content permissions on page 28: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Impact users on page 33.

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

Impact user role permissions

Permission	Impact Administrator[1]	Impact Operator[1]	Impact User[1]	Impact Endpoint Configuration Approver
Impact View the Impact workbench	✓ SHOW	✓ SHOW	✓ SHOW	✗
Impact Asset Details View the details for an asset	✓ READ	✓ READ	✓ READ	✗
Impact Asset Impact View the impact rating for assets	✓ READ	✓ READ	✓ READ	✗
Impact Asset Items View the items for an asset	✓ READ	✓ READ	✓ READ	✗
Impact Endpoint Configuration Approve Impact items in Endpoint Configuration	✗	✗	✗	✓ APPROVE

© 2025 Tanium Inc. All Rights Reserved

Impact user role permissions (continued)

Permission	Impact Administrator[1]	Impact Operator[1]	Impact User[1]	Impact Endpoint Configuration Approver
Impact Settings View and edit Impact settings	✓ READ WRITE	✓ READ WRITE	✗	✗
Impact Shortest Path View the shortest path graphs	✓ READ	✓ READ	✓ READ	✗
Impact Support Bundle View the Impact support bundle	✓ READ	✗	✗	✗
Impact Sync Start the Impact synchronization	✓ START	✓ START	✗	✗
Impact Sync Status View the Impact synchronization status	✓ READ	✓ READ	✓ READ	✗

[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.

Impact platform content permissions

Permission	Permission Type	Impact Administrator	Impact Operator	Impact User	Impact Endpoint Configuration Approver
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
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 Impact

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

- **Automatic configuration with default settings**: Impact is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Impact, see Import Impact with default settings on page 29.
- **Manual configuration with custom settings**: After installing Impact, you must manually configure required settings. Select this option only if Impact requires settings that differ from the recommended default settings. For more information, see Import Impact with custom settings on page 30.

Before you begin

- Read the release notes.
- Review the Impact requirements on page 22.
- If you are upgrading from a previous version, see Upgrade Impact on page 30
- Assign the correct roles to users for Impact. Review the User role requirements on page 26.
    - To import the Impact solution, you must be assigned the Administrator reserved role.
    - To configure the Impact action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Write Action Group** permission.

Import Impact with default settings

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

Default settings for Tanium Impact

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group NOTE Because Impact is currently supported only on Windows endpoints, the **Targeting Criteria** for the action to distribute the Impact tools filters the group to Windows endpoints. • Restricted targeting enabled: `No Computers` computer group

To import Impact and configure default settings, see Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed: see Verify Impact version on page 30.

© 2025 Tanium Inc. All Rights Reserved

Import Impact with custom settings

To import Impact without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Import or update specific solutions. After the import, verify that the correct version is installed: see Verify Impact version on page 30.

To configure the Impact action group, see Configure the Impact action group on page 32.

To configure synchronization settings, see Configure synchronization settings on page 32.

To manually collect and analyze data or view the last time that data was collected and analyzed, see Collect and analyze data on page 33.



Data is automatically synchronized between endpoints, all configured domains, and Impact every 24 hours.

Manage solution dependencies

Other Tanium solutions are required for Impact to function (required dependencies) or for specific Impact features to work (feature-specific dependencies). For more information, see Solution dependencies on page 22.

Upgrade Impact



In Impact 2.0 or later, the steps required to configure the service account are no longer necessary due to the adoption of the System User Service, which performs these tasks automatically. Additionally, the Impact database is migrated to RDB in this release. Consequently, after upgrading to Impact 2.0 or later, it might take time for the database migration to complete and for RBAC privileges and other updates to sync properly. This migration could lead to issues and error messages when you first query Tanium Console. These issues should resolve on their own after a few minutes, but could take up to an hour or longer depending on system resources and the amount of data to migrate.

For the steps to upgrade Impact, see Tanium Console User Guide: Managing Tanium solutions. After the upgrade, verify that the correct version is installed: see Verify Impact version on page 30.

Verify Impact version

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

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

© 2025 Tanium Inc. All Rights Reserved

Configuring Impact

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

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

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

NOTE

For information about how to install Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Installing Endpoint Configuration.

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Impact, see User role requirements on page 26. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.

IMPORTANT

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

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

NOTE

Impact requires Python tools on endpoints. If the **Initial Content - Python** content pack is not already installed by another solution on the endpoints, Impact uses Endpoint Configuration to install the **Impact Tools** content pack, which also includes Python tools.

© 2025 Tanium Inc. All Rights Reserved

NOTE

If the Impact tooling was installed by anotherTanium solution, it is possible that you might see Impact data even if the Action Group for Impact is set to No Computers.

Configure Impact

Configure the Impact action group

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

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

Select the computer groups to include in the Impact action group.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Click **Tanium Impact**.
3. Select the computer groups that you want to include in the action group and click **Save**.
   If you select multiple computer groups, choose an operator (AND or OR) to combine the groups.

   NOTE

   Because Impact is currently supported only on Windows endpoints, the **Targeting Criteria** for the action to distribute the Impact tools filters the group to Windows endpoints.

Configure synchronization settings

Configure how Impact synchronizes data between the Active Directory server and Impact.

1. From the Main menu, go to **Modules > Impact** to open the Impact **Overview** page.
2. Click Settings and open the **Sync Settings** tab.
3. Select the schedule type:
   - **Basic**: Select the schedule, options, and time zone.
   - **Cron**: Select the time zone and enter a cron expression of five values representing minutes, hours, day of the month, month, and day of the week. For example, enter `0 2 * * 1,2,3,4,5` to set the schedule to run at 02:00 AM only on Monday, Tuesday, Wednesday, Thursday, and Friday.
4. Review the **Summary** and then click **Submit**.

© 2025 Tanium Inc. All Rights Reserved

BEST PRACTICE

To ensure that Criticality synchronizations are complete before Impact starts to sync, configure Impact synchronizations as follows:

- Start at least one hour after Criticality synchronizations start.
- Choose the same frequency or sync less frequently than Criticality.

Configure connections to domains

To configure connections to the Active Directory domains that you want to analyze with Impact, see Tanium Directory Query User Guide: Add a domain.

For more information on verifying the details of the host certificate, see Reference: Verify the SHA256 fingerprint of a certificate.

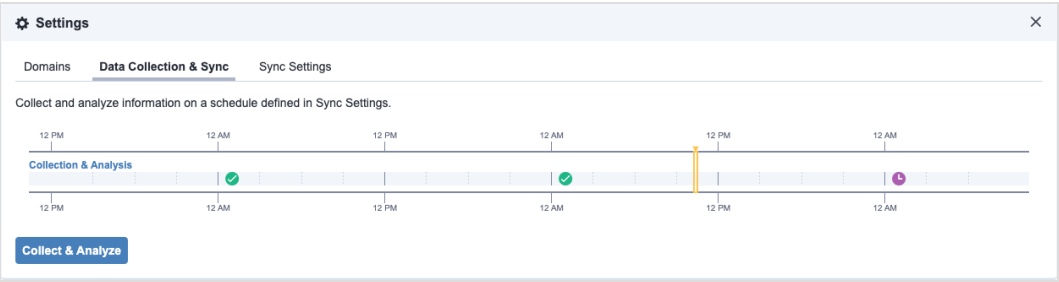
After you save the domain connection, data collection and analysis begins automatically at the next scheduled synchronization. For more information, see Collect and analyze data.

Collect and analyze data

Data is automatically synchronized between endpoints, users, groups, all configured domains, and Impact according to the schedule in **Sync Settings**. To view the last time that data was collected and analyzed, and the next scheduled collection and analysis, go to the **Data Collection & Sync** tab in Impact Settings.

To initiate data collection and analysis manually, click **Collect & Analyze**.

Collect and analyze



BEST PRACTICE

Data collection and analysis is a long-running process. Do not initiate this process frequently. If a request is already in progress, the requested operation does not run.

Set up Impact users

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

To review specific permissions for each role, see User role requirements on page 26.

© 2025 Tanium Inc. All Rights Reserved

IMPORTANT

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

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

Impact Administrator

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

- Configure Impact service settings, including creating and editing domain connections
- Manually start a domain synchronization and check the status
- View all ratings, details, and graphs for endpoints, users, and groups
- Generate and view the Impact support bundle

Impact Operator

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

- Configure Impact service settings, including creating and editing domain connections
- Manually start a domain synchronization and check the status
- View all ratings, details, and graphs for endpoints, users, and groups

Impact User

Assign the **Impact User** role to users who perform analysis of Impact ratings.
This role can perform the following tasks:

- View the domain synchronization status
- View all ratings, details, and graphs for endpoints, users, and groups

Impact Endpoint Configuration Approver

Assign the **Impact Endpoint Configuration Approver** role to a user who approves or rejects Impact configuration items in Endpoint Configuration.
This role approves, rejects, or dismisses changes that target endpoints where Impact is installed.

NOTE

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

© 2025 Tanium Inc. All Rights Reserved

Identifying high impact users, endpoints, and groups

Identify the users, groups, and endpoints that have the highest potential impact in your organization if compromised, based on the impact rating.

Overview

The Impact **Overview** page includes three tables to show you the users, groups, and endpoints that have the highest potential impact.

The **Metrics** ribbon shows a high-level overview of the data used for analysis in Impact: **Total Endpoints**, **Total Users**, and **Total Groups**. This ribbon also shows the total number of assets with each impact rating: **Critical**, **High**, **Medium**, and **Low**.

Impact rating

Impact analyzes the data from synchronized domains and calculates an impact rating for each user, group, or endpoint. The impact rating is influenced by the following factors:

- Potential inbound impact by users
- Potential inbound impact by endpoints
- Potential outbound impact by users
- Potential outbound impact by endpoints

For additional details about the impact rating calculation, see Impact Rating.

The **Findings** section provides three tabs, each displaying a table to show you the users, groups, and endpoints that have the highest potential impact. The summary data at the top of this section is scoped to display data for the currently selected tab.

Before you begin

Configure a connection to one or more Active Directory domains. For more information, see Tanium Directory Query User Guide: Managing connections to directory servers.

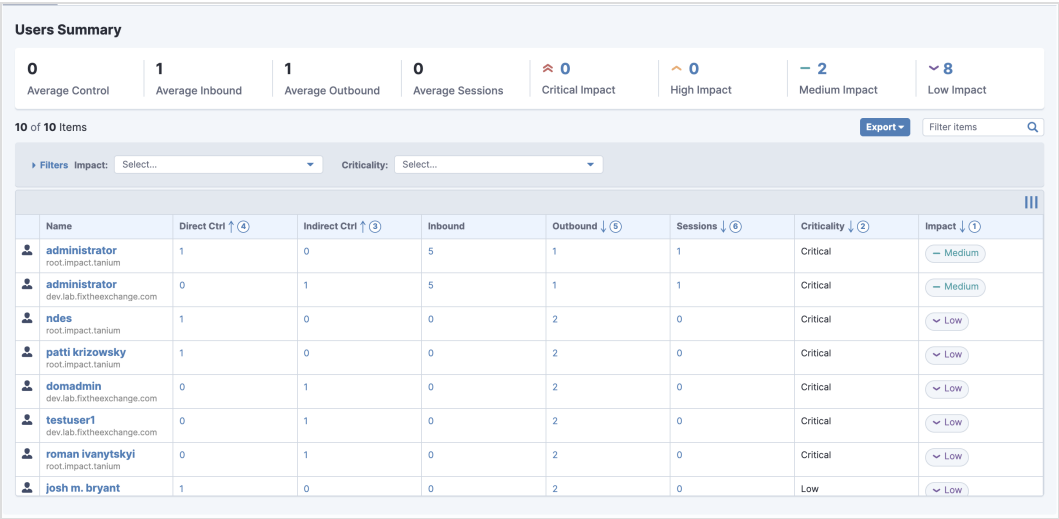
Impact analyzes data from domain-joined, Tanium-managed Windows endpoints with a domain that is configured in Directory Query and synchronized with Criticality. For more information on Tanium Criticality, see Tanium Criticality User Guide: User role requirements.

© 2025 Tanium Inc. All Rights Reserved

Explore the users with the highest impact rating

Select the **Users** tab under **Findings** to view the **Users Summary** table. The **Users Summary** table shows the users that have the highest impact rating in the domains that are synchronized with Impact.

Users summary



This table contains eight columns:

- **Name**: Name and domain of the user.
- **Direct Ctrl**: Number of endpoints on which this user has administrative rights through a direct entry in the local Administrators object, not through an Active Directory group membership.
- **Indirect Ctrl**: Number of endpoints on which the user has administrative rights through an Active Directory group or nested group that has an entry in the local Administrators object.
- **Inbound**: Sum of the endpoints and users that an attacker can use to move laterally to compromise the user credentials.
- **Outbound**: Sum of the endpoints and users that an attacker can reach by moving laterally using the compromised credentials.
- **Sessions**: Number of sessions in the last 72 hours that the user has opened on computers. Impact continues to count a session as long as the sensor reported it within the last 72 hours. In addition, a Windows endpoint retains session information in memory even after the user signs out and until that endpoint is restarted, so the sensor reports that session data back to Impact until it is restarted, after which the 72 hour counter starts.
- **Criticality**: Criticality level for the user: **Critical**, **High**, **Medium**, or **Low**. For more information on the default groups and users criticality rule, see Tanium Criticality User Guide: Work with existing criticality rules.
- **Impact**: Impact rating for the user: **Critical**, **High**, **Medium**, or **Low**.

The default sort order for the **Users Summary** table is **Impact** (highest to lowest), **Criticality** (highest to lowest), **Indirect Ctrl** (highest to lowest), **Direct Ctrl** (highest to lowest), **Outbound** (highest to lowest), and **Sessions** (highest to lowest).

© 2025 Tanium Inc. All Rights Reserved

To sort a table, click a column or **Shift**+click multiple columns. To reset the sort order, click a column multiple times, until the sort order arrow disappears.

To customize the columns in the table, click Customize Columns and then select which columns to keep or click and drag a column to change the column order.

The following columns are not displayed by default in the **Users Summary** table:

- **SID**: A unique value that is used to identify any security entity that the Windows operating system (OS) can authenticate.

You can filter the results that appear in the table. For example, you can select a value for **Impact** or **Criticality** to use as a filter. Expand **Filters** and click **Standard** to filter for members of a specific domain. For a more custom filter, expand **Filters** and click **Filter Builder**. Select an available attribute, an operator, and provide a value. Available operators and supported types of values can vary based on the attribute you select. You can add additional attributes that are joined with a logical `AND` or `OR` to make complex expressions for filtering data. Additionally you can add groups to build more robust and finely-tuned filter criteria.

The following filter attributes are available in filter builder for the **Users Summary** table:

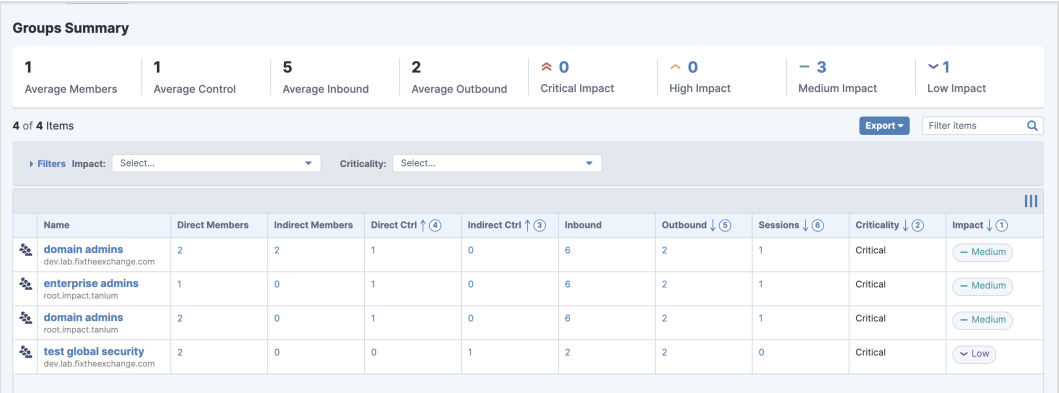
- Direct Control
- Indirect Control
- Inbound
- Outbound
- Sessions

Click an entry in a column to open a graph with additional details about that value. For more information, see Analyzing the impact.

Explore the groups with the highest impact rating

Select the **Groups** tab under **Findings** to view the **Groups Summary** table. The **Groups Summary** table shows groups that have the highest impact rating in the domains that are synchronized with Impact.

Groups summary



© 2025 Tanium Inc. All Rights Reserved

This table contains ten columns:

- **Name**: Name and domain of the group.
- **Direct Members**: Number of users in the group with a direct entry in the group, who are not a member due to group nesting.
- **Indirect Members**: Number of users in the group who are a member due to a nested group.
- **Direct Ctrl**: Number of endpoints on which this group has administrative rights through a direct entry in the local Administrators object, not through a nested group.
- **Indirect Ctrl**: Number of endpoints on which the group has administrative rights through a nested group.
- **Inbound**: Sum of the endpoints and users that an attacker can use to move laterally to compromise this group.
- **Outbound**: Sum of the endpoints and users that an attacker can reach by moving laterally using this group.
- **Sessions**: Number of sessions in the last 72 hours that used membership in this group to access the endpoint. Impact continues to count a session as long as the sensor reported it within the last 72 hours. In addition, a Windows endpoint retains session information in memory even after the user signs out and until that endpoint is restarted, so the sensor reports that session data back to Impact until it is restarted, after which the 72 hour counter starts.
- **Criticality**: Criticality level for the group: **Critical**, **High**, **Medium**, or **Low**. For more information on the default groups and users criticality rule, see Tanium Criticality User Guide: Work with existing criticality rules.
- **Impact**: Impact rating for the group: **Critical**, **High**, **Medium**, or **Low**.

The default sort order for the **Groups Summary** table is **Impact** (highest to lowest), **Criticality** (highest to lowest), **Direct Members** (highest to lowest), **Outbound** (highest to lowest), and **Sessions** (highest to lowest).

To sort a table, click a column or **Shift**+click multiple columns. To reset the sort order, click a column multiple times, until the sort order arrow disappears.

To customize the columns in the table, click Customize Columns and then select which columns to keep or click and drag a column to change the column order.

The following columns are not displayed by default in the **Groups Summary** table:

- **SID**: A unique value that is used to identify any security entity that the Windows operating system (OS) can authenticate.

You can filter the results that appear in the table. For example, you can select a value for **Impact** or **Criticality** to use as a filter. Expand **Filters** and click **Standard** to filter for members of a specific domain. For a more custom filter, expand **Filters** and click **Filter Builder**. Select an available attribute, an operator, and provide a value. Available operators and supported types of values can vary based on the attribute you select. You can add additional attributes that are joined with a logical `AND` or `OR` to make complex expressions for filtering data. Additionally you can add groups to build more robust and finely-tuned filter criteria.

The following filter attributes are available in filter builder for the **Groups Summary** table:

- Direct Control
- Indirect Control
- Inbound

© 2025 Tanium Inc. All Rights Reserved

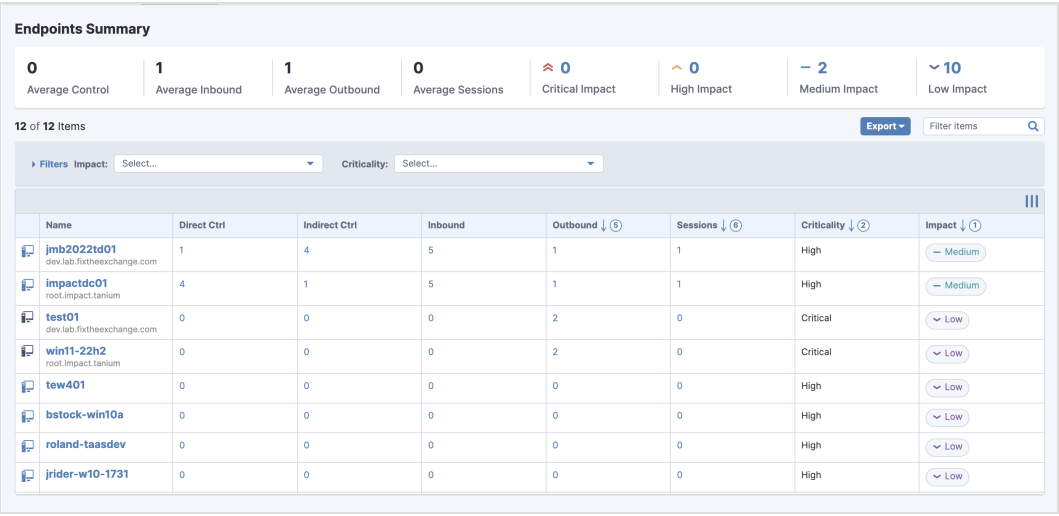
- Outbound
- Sessions
- Direct Members
- Indirect Members

Click an entry in a column to open a graph with additional details about that value. For more information, see Analyzing the impact.

Explore the endpoints with the highest impact rating

Select the **Endpoints** tab under **Findings** to view the **Endpoints Summary** table. The **Endpoints Summary** table shows endpoints that have the highest impact rating in the domains that are synchronized with Impact.

Endpoints summary



This table contains eight columns:

- **Name**: Name and domain of the endpoint. You can click the icon next to an endpoint to view additional information about the endpoint in the **Endpoint Details** page of Tanium Reporting. If the icon is disabled it indicates that the endpoint no longer exists.
- **Direct Ctrl**: Number of users that have administrative rights to this endpoint through a direct entry in the local Administrators object, not through an Active Directory group membership.
- **Indirect Ctrl**: Number of users that have administrative rights to this endpoint through an Active Directory group or nested group that has an entry in the local Administrators object.
- **Inbound**: Sum of the endpoints and users that an attacker can use to move laterally to compromise this endpoint.
- **Outbound**: Sum of the endpoints and users that an attacker can reach by moving laterally starting from this endpoint.

© 2025 Tanium Inc. All Rights Reserved

- **Sessions**: Number of sessions in the last 72 hours for this endpoint, which shows the number of users currently logged in to the endpoint, with those credentials stored in memory on the endpoint.Impact continues to count a session as long as the sensor reported it within the last 72 hours. In addition, a Windows endpoint retains session information in memory even after the user signs out and until that endpoint is restarted, so the sensor reports that session data back to Impact until it is restarted, after which the 72 hour counter starts.
- **Criticality**: Criticality level for the user: **Critical**, **High**, **Medium**, or **Low**.
- **Impact**: Impact rating for the endpoint: **Critical**, **High**, **Medium**, or **Low**.

The default sort order for the **Endpoints Summary** table is **Impact** (highest to lowest), **Criticality** (highest to lowest), **Indirect Ctrl** (highest to lowest), **Direct Ctrl** (highest to lowest), **Outbound** (highest to lowest), and **Sessions** (highest to lowest).

To sort a table, click a column or **Shift**+click multiple columns. To reset the sort order, click a column multiple times, until the sort order arrow disappears.

To customize the columns in the table, click Customize Columns and then select which columns to keep or click and drag a column to change the column order.

The following columns are not displayed by default in the **Endpoints Summary** table:

- **SID**: A unique value that is used to identify any security entity that the Windows operating system (OS) can authenticate.
- **Computer Name**: The name of the computer.
- **Serial Number**: An identifier assigned by the computer hardware manufacturer and retrieved from the BIOS.
- **Computer ID**: A unique ID assigned to each endpoint by Tanium Cloud or Tanium Server.
- **Operating System**: The full name of the operating system that is installed on the endpoint.
- **IP Address**: The IP address assigned to the endpoint.

You can filter the results that appear in the table. For example, you can select a value for **Impact** or **Criticality** to use as a filter. Expand **Filters** and click **Standard** to filter for members of a specific domain. For a more custom filter, expand **Filters** and click **Filter Builder**. Select an available attribute, an operator, and provide a value. Available operators and supported types of values can vary based on the attribute you select. You can add additional attributes that are joined with a logical `AND` or `OR` to make complex expressions for filtering data. Additionally you can add groups to build more robust and finely-tuned filter criteria.

The following filter attributes are available in filter builder for the **Endpoints Summary** table:

- Direct Control
- Indirect Control
- Inbound
- Outbound
- Sessions
- Serial Number
- Operating System
- IP Address

© 2025 Tanium Inc. All Rights Reserved

Click an entry in a column to open a graph with additional details about that value. For more information, see Analyzing the impact.

Exporting tables

You can export each of these tables to a CSV file that contains the data for each entry in the table, including column headings. To export a table, click **Export > Export to CSV** to export the selected data to a CSV file that is saved in the downloads directory of the web browser.

Click **Export > Copy to clipboard** to copy the data for each table in CSV format to the system clipboard.

© 2025 Tanium Inc. All Rights Reserved

Analyzing the impact

Overview

Analyze users, groups, and endpoints that have the highest impact ratings determine and prioritize where you should reduce administrative privileges, especially for critical assets, to reduce attack surface.

With Impact, you can build graphs that analyze the rights, dependencies, and relationships for endpoints, users, and groups. Use these graphs to visualize potential lateral movement and identify assets in your organization with a high impact rating.

Before you begin

Configure a connection to one or more Active Directory domains. For more information, see Tanium Directory Query User Guide: Managing connections to directory servers.

Impact analyzes data from domain-joined, Tanium-managed Windows endpoints with a domain that is configured in Directory Query and synchronized with Criticality. For more information on Tanium Criticality, see Tanium Criticality User Guide: User role requirements.

Analyze the impact for a specific user, group, or endpoint

Look up a specific user, group, or endpoint to analyze the potential impact.

1. From the Main menu, go to **Modules > Impact** to open the Impact **Overview** page.
2. In the **Impact Lookup** bar, enter a User, Group, or Endpoint to look up. You can select **All** to look up a value matching all of the available types.
3. Select **Outbound Impact** or **Inbound Impact** from the row in results table that matches the result you want to look up.

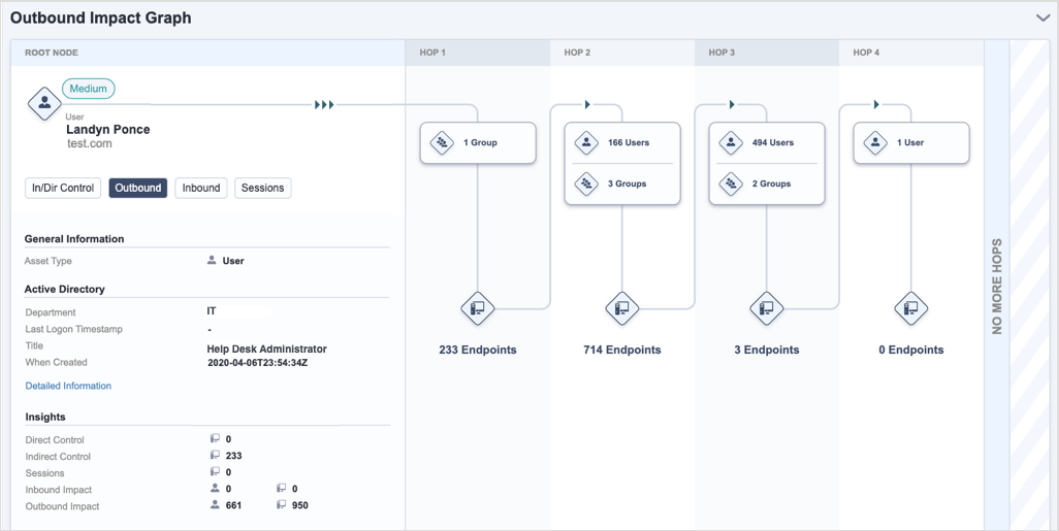
The resulting **Impact Graph** shows summary information and details about the potential impact if the asset is compromised. You can select **In/Dir Control**, **Outbound**, **Inbound**, **Sessions**, or **Members** (shows only for groups) to explore the potential impact. The graph starts with **Outbound** or **Inbound** selected, depending on whether you selected **Outbound Impact** or **Inbound Impact** for your lookup.

Explore impact graphs

A lookup generates an **Impact Graph** that contains a **Root Node** with summary information and additional graphs that you can select to see detailed information: **In/Dir Control**, **Outbound**, **Inbound**, **Sessions**, and **Members** (shows only for groups).

Outbound user graph

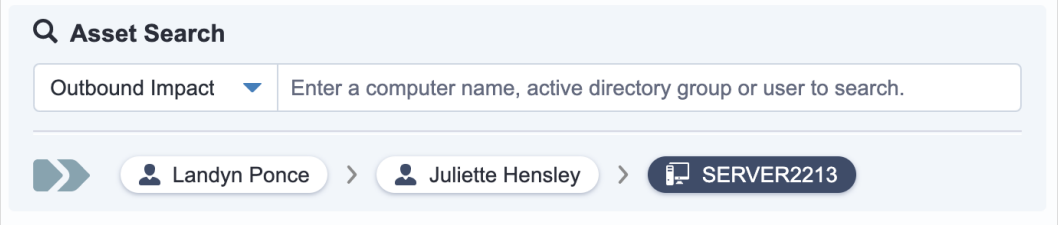
© 2025 Tanium Inc. All Rights Reserved



The **Users**, **Endpoints**, and **Groups** tables show the details for the associated asset type. You can click values in these tables to examine that data for the corresponding asset, such as direct control on an endpoint. To sort a table, click a column or **Shift**+click multiple columns. To reset the sort order, click a column multiple times, until the sort order arrow disappears. To customize the columns in the table, click Customize Columns and then select which columns to keep or click and drag a column to change the column order.

TIP

Use the breadcrumbs in the **Asset Search** section to return to the original asset as you explore different assets in the **Users**, **Endpoints**, and **Groups** tables.

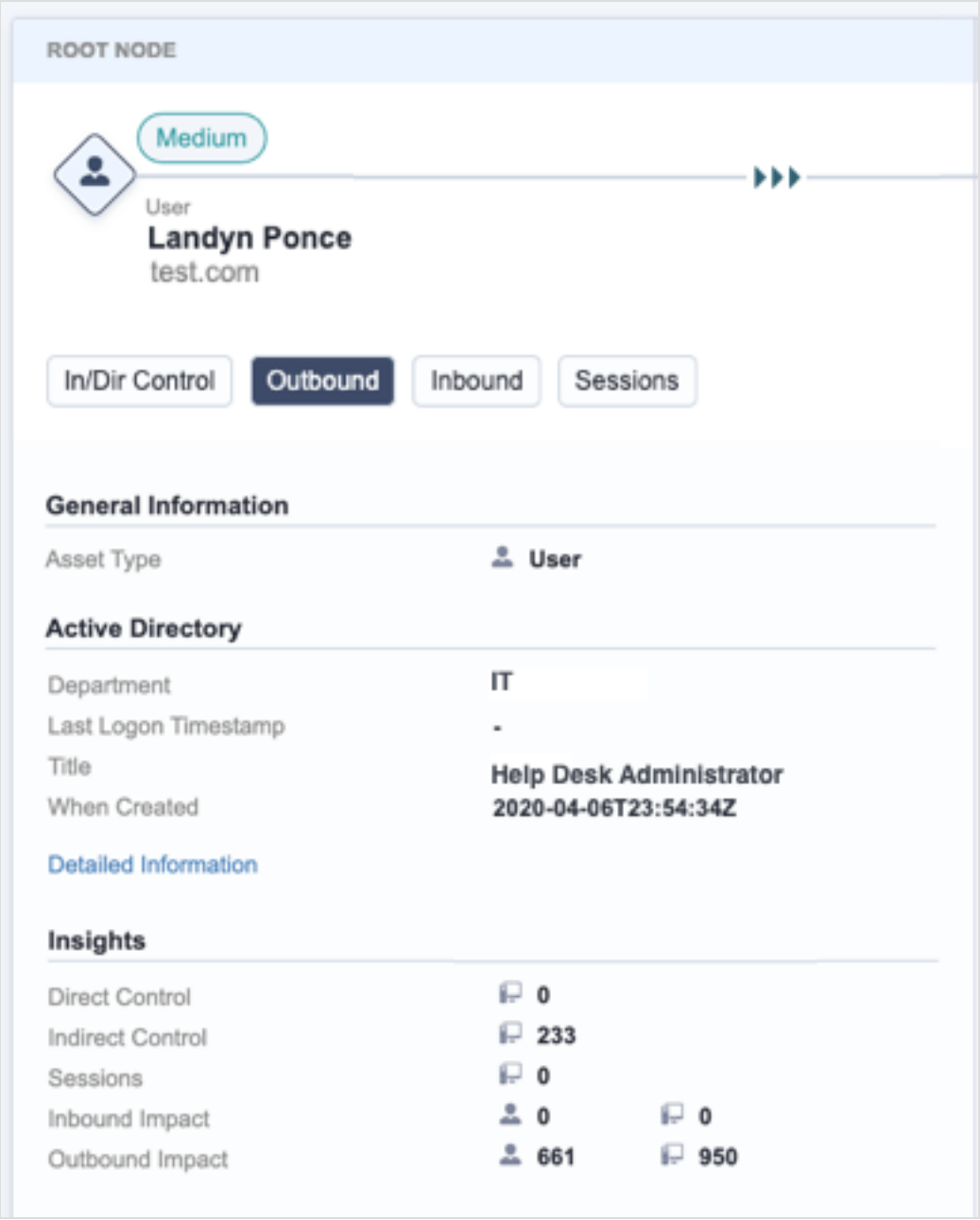


View summary

The **Root Node** section of the graph provides summary information about the asset and the analysis.

© 2025 Tanium Inc. All Rights Reserved

Root node



The **General Information** and **Active Directory** sections show details about the endpoint, user, or group. Details in these sections are pulled from Active Directory. If a field is empty, that field in the Active Directory record for the endpoint, user, or group is not populated.

© 2025 Tanium Inc. All Rights Reserved

The **Insights** section shows summarized details of the impact for the endpoint, user, or group. If you click an element in the **Insights** section, summarized details that correspond with the element you clicked appear in a table below the graph.

- **Direct Members**:
  - **Users:** Not applicable.
  - **Computers:** Not applicable.
  - **Groups:** A number of direct members of the group.
- **Indirect Members**:
  - **Users:** Not applicable.
  - **Computers:** Not applicable.
  - **Groups:** A number of indirect members of the group.
- **Direct Control**:
  - **Users:** The number of endpoints on which the user has administrative rights through a direct entry in the local Administrators object on the system, not through an Active Directory group membership.
  - **Computers:** The number of users that have administrative rights to the computer through a direct entry in the local Administrators object on the system, not through an Active Directory group membership.
  - **Groups:** The number of endpoints on which the group has administrative rights through a direct entry in the local Administrators object on the system, not through group nesting.
- **Indirect Control**:
  - **Users:** The number of endpoints on which the user has administrative rights through an Active Directory group or nested group that has an entry in the local Administrators object on the system.
  - **Computers:** The number of users that have administrative rights to the computer through an Active Directory group or nested group that has an entry in the local Administrators object on the system.
  - **Groups:** The number of endpoints on which the group has administrative rights through group nesting in the local Administrators object on the system.
- **Sessions**: A session is created when a user logs in to a computer, either locally or remotely. Impact counts a session for 72 hours and until the computer is rebooted.
  - **Users:** The number of sessions the user has open on computers.
  - **Computers:** The number of sessions on the computer.
  - **Groups:** The number of sessions that are using the group for access.

© 2025 Tanium Inc. All Rights Reserved

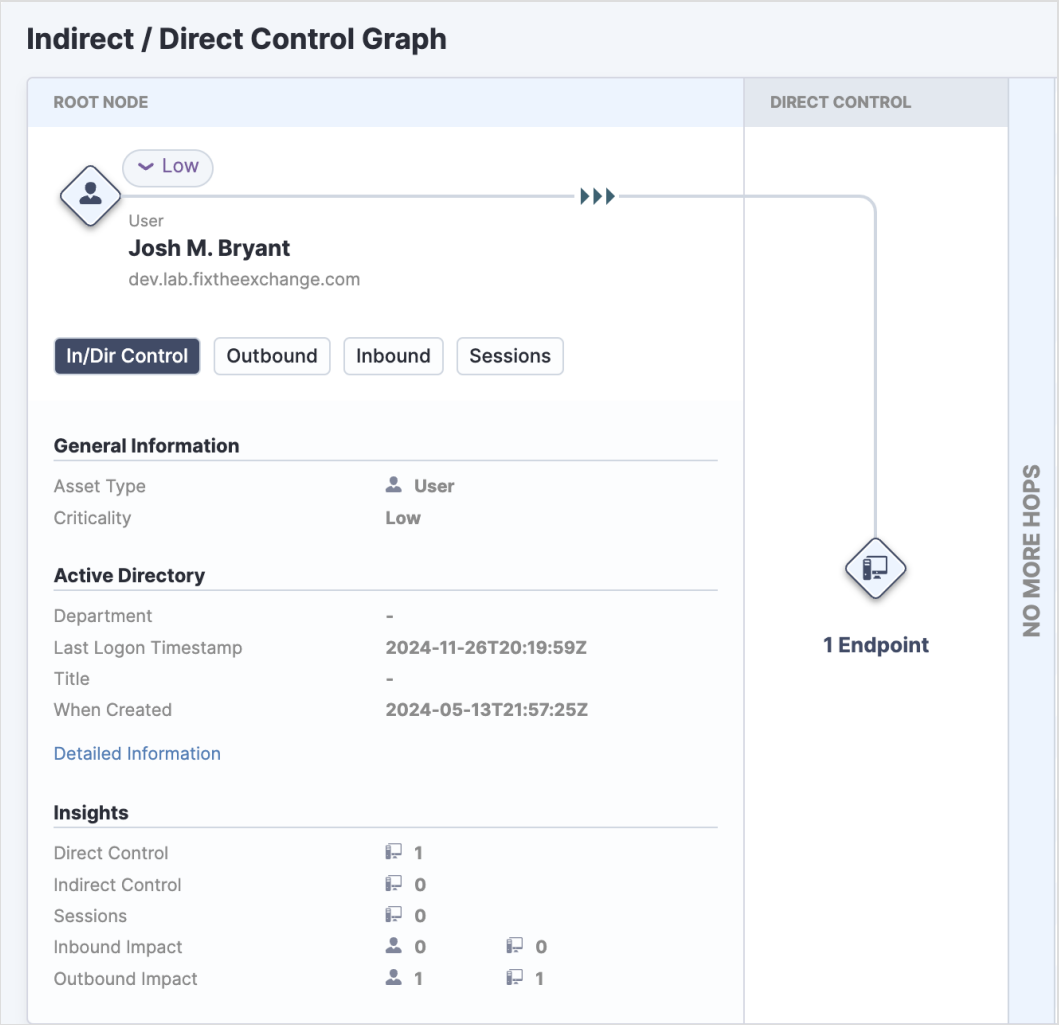
- **Inbound Impact**:
    - **Users:** The number of user accounts and endpoints that can be used to breach this user through potential lateral movement.
    - **Computers:** The number of user accounts and endpoints that can be used to breach this computer through potential lateral movement.
    - **Groups:** The number of user accounts and endpoints that can be used to breach this group through potential lateral movement.
- **Outbound Impact**:
    - **Users:** The number of user accounts and endpoints that this user can be used to breach through potential lateral movement.
    - **Computers:** The number of user accounts and endpoints that this computer can be used to breach through potential lateral movement.
    - **Groups:** The number of user accounts and endpoints that this group can be used to breach through potential lateral movement.

View indirect / direct control

Select **In/Dir Control** to show the **Indirect / Direct Control** graph.

© 2025 Tanium Inc. All Rights Reserved

Indirect / Direct Control Graph



The details shown depend on the type of asset that you are analyzing:

- **Users:** Displays a map that shows the endpoints on which the user has administrative access, either through direct control or indirect control. The first column after the **Root Node** always has a **Direct Control** heading and indicates endpoints on which the user has administrative access through direct control. Any subsequent columns have an **Indirect Control** heading and shows the endpoints on which the user has administrative access through indirect control. Indirect control indicates nesting within the endpoints displayed in the **Direct Control** column. This model of nesting applies for each subsequent **Indirect Control** column.
- **Computers:** Displays a map that shows the users and groups that have administrative access to the computer, either through direct control or indirect control. The first column after the **Root Node** always has a **Direct Control** heading and indicates users and groups that have administrative access through direct control. Any subsequent columns have an **Indirect Control** heading and shows the users and groups that have administrative access through indirect control. Indirect control indicates nesting within the groups displayed in the **Direct Control** column. This model of nesting applies for each subsequent **Indirect Control** column.

© 2025 Tanium Inc. All Rights Reserved

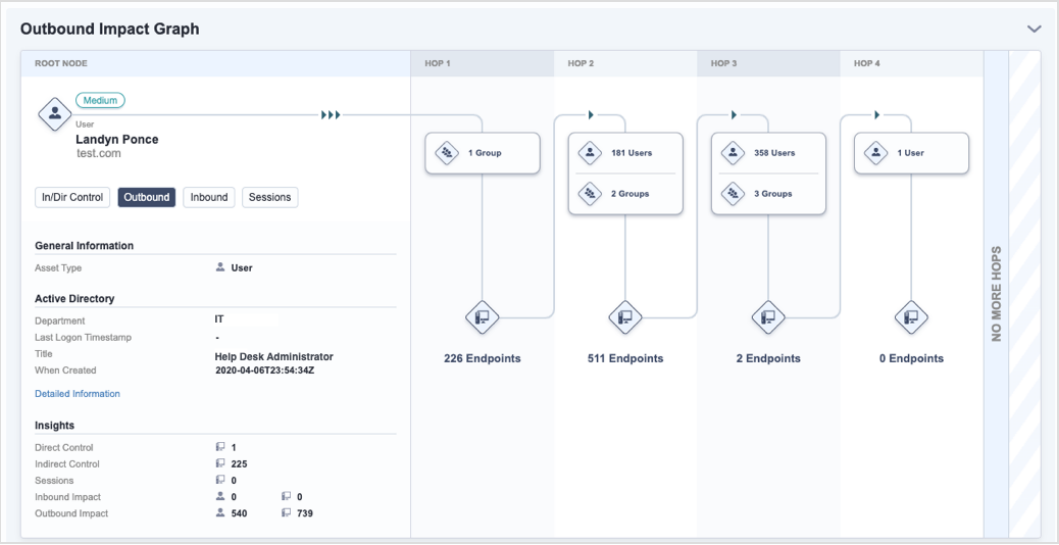
- **Groups:** Displays a map that shows the endpoints on which the group has administrative access, either through direct control or indirect control. The first column after the **Root Node** always has a **Direct Control** heading and indicates groups that have administrative access through direct control. Any subsequent columns have an **Indirect Control** heading and shows the groups that have administrative access through indirect control. Indirect control indicates nesting within the groups displayed in the **Direct Control** column. This model of nesting applies for each subsequent **Indirect Control** column.

The **Users**, **Endpoints**, and **Groups** tables show the details for the associated asset type. Click a node in the map to filter the tables based on that level of nesting.

View outbound impact

Select **Outbound** to analyze the outbound impact for the asset. This graph shows by default when you select **Outbound Impact** for an asset search.

Outbound impact graph



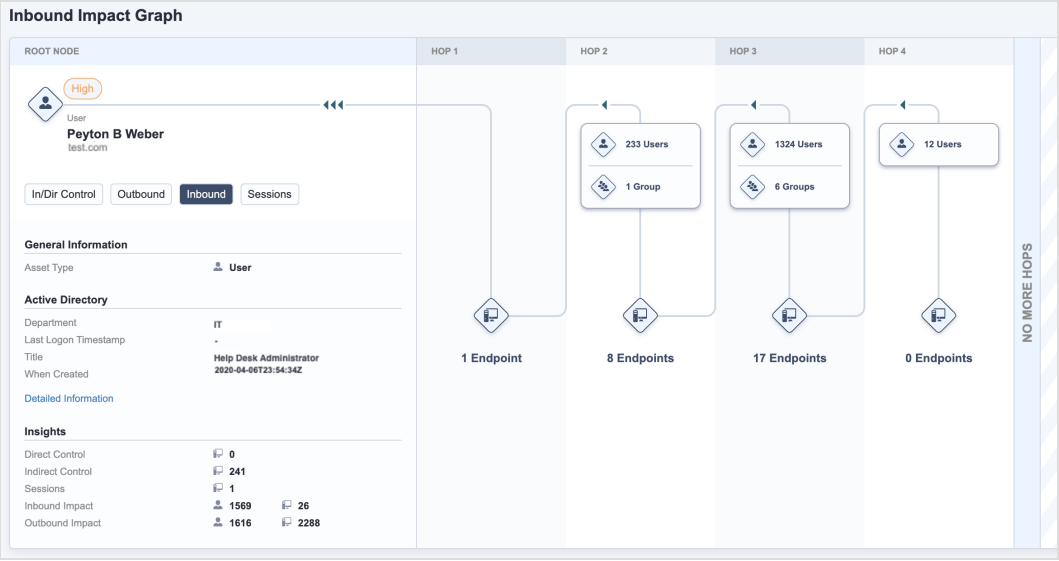
A hop map shows the endpoints, groups, and users that the asset could reach with potential outbound lateral movement. The **Users**, **Endpoints**, and **Groups** tables show the details for the associated asset type. Click a node in the hop map to filter the tables based on that hop.

View inbound impact

Select **Inbound** to analyze the inbound impact for the asset. This graph shows by default when you select **Inbound Impact** for an asset search.

© 2025 Tanium Inc. All Rights Reserved

Inbound impact graph



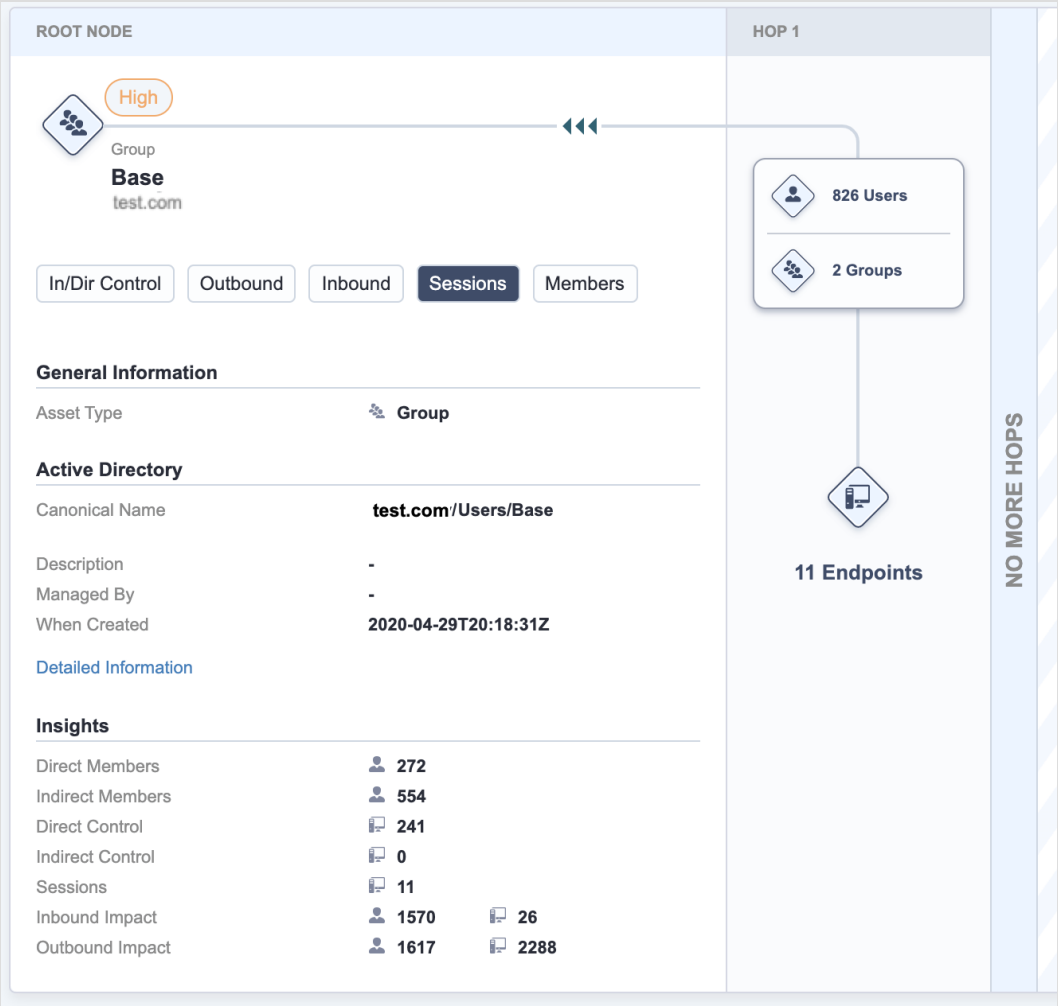
A hop map shows the endpoints, groups, and users that could reach the asset with potential inbound lateral movement. The **Users**, **Endpoints**, and **Groups** tables show the details for the associated asset type. Click a node in the hop map to filter the tables based on that hop.

View sessions

Select **Sessions** to analyze the sessions for the asset.

© 2025 Tanium Inc. All Rights Reserved

Sessions



A hop map shows the sessions for that asset. The **Users**, **Endpoints**, and **Groups** tables show the details for the associated asset type. Click a node in the hop map to filter the tables based on that hop.

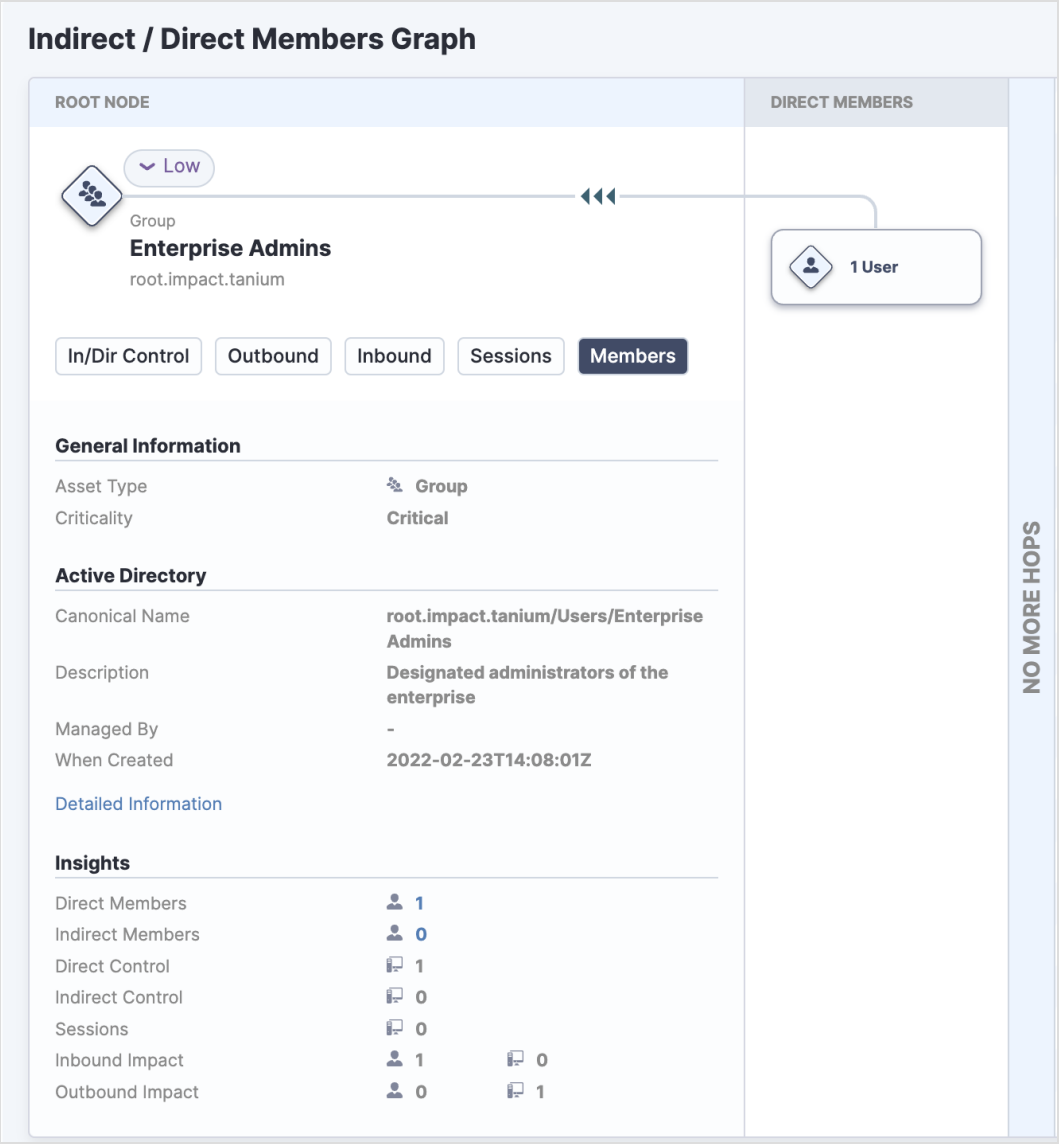
View members

> NOTE
>
> This view is only available for groups.

Select **Members** to analyze the direct and indirect members of the group. The first column after the **Root Node** always has a **Direct Members** heading. Any subsequent columns have an **Indirect Members** heading and represents a layer of group nesting.

© 2025 Tanium Inc. All Rights Reserved

Members



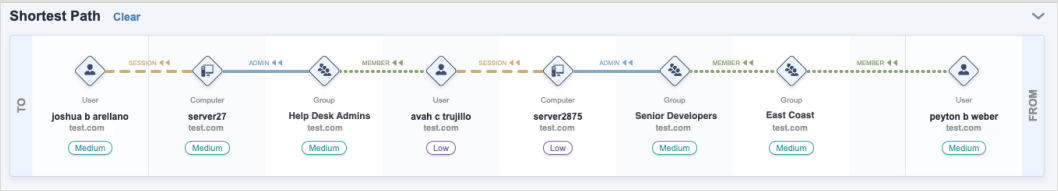
A map shows the users (Direct Members) and nested groups (Indirect Members) in that group.

View shortest path maps

Click the target icon next to a user, endpoint or group in one of the **Users**, **Endpoints** or **Groups** tables to show a **Shortest Path** map from that user, endpoint, or group to the asset. The **Shortest Path** map shows the shortest path from the target user, endpoint, or group by means of direct access, group membership, or sessions.

© 2025 Tanium Inc. All Rights Reserved

Shortest path



What to do next

Implement a least-privilege security model for your Active Directory environment, modifying assets that need administrative rights reduced based on your Impact data analysis. For more information, see Reference: Remediation resources.

© 2025 Tanium Inc. All Rights Reserved

Exporting Impact data

You can export data from Impact to Tanium Connect. You can export data using the Tanium Impact or Tanium Threat Response data sources in Connect.

Connections to create

Connections to create

Purpose	Source type	Instructions	Sample output
Export inbound and outbound Impact data for users, groups, or endpoints.	Tanium Impact	Create connection to export Impact data on page 53	CSV example: Impact data export on page 53
Export Impact and outbound Impact scores as part of a Threat Response alert.	Tanium Threat Response	Tanium Threat Response User Guide: Export data to Tanium Connect	JSON example: Threat Response alert with Impact data export on page 54

Create connection to export Impact data

1. Create the connection.
   a. From the Main menu, open Tanium Connect. Click **Create Connection**.
   b. Name the connection.
2. In the Source section, select the **Tanium Impact** source. Select the asset type to include.
3. Select a destination. For more information, see Tanium Connect User Guide.
4. Apply filters.
5. Choose format settings and schedule.
6. Click **Save**.

CSV example: Impact data export

The following is an example of Impact data exported to a CSV output using the Tanium Impact source in Connect.

The CSV output contains two columns that do not display in the Impact workbench.

© 2025 Tanium Inc. All Rights Reserved

- The **impactRating** column contains numeric values that map to the following impact ratings:
  - 0= **Low**
  - 1= **Medium**
  - 2= **High**
  - 3= **Critical**
- The **impactScore** column is the total number of points for the endpoint, user, or group. The impact rating is determined from these points.

For more information, see Impact rating on page 12.

CSV of export data



id	name	sid	assetType	directCtrl	indirectCtrl	directMembers	indirectMembers	inboundAssetCount	outboundAssetCount	sessionCount	impactRating	impactScore	domainName
2	Administrator	S-1-5-21-196915329	user	0	1			14	1	1	2	10	
4	tanium	S-1-5-21-196915329	user	1	0			0	2	0	0	4	
6	Demo D. Admin	S-1-5-21-196915329	user	0	1			0	2	0	0	4	
7	Test Domain Admin	S-1-5-21-196915329	user	0	1			0	2	0	0	4	
11	Test	S-1-5-21-196915329	user	0	1			0	2	0	0	4	
20	test%user	S-1-5-21-196915329	user	0	1			0	2	0	0	4	

JSON example: Threat Response alert with Impact data export

The following is an example of Impact data exported as part of a Threat Response alert in Connect. Note the Impact data in line 74.

The JSON includes the **impactScore**, which does not display in the Impact workbench. The **impactScore** is the total number of points for the endpoint, user, or group. The impact rating is determined from these points. For more information, see Impact rating on page 12.


```
1 [{"id":"1311","state":"unresolved","type":"detect.match","guid":"00000000-0000-0000-7da5-
15056817fd17","priority"
2 :"high","severity":"info","intelDocId":149,"intelDocRevisionId":null,"scanConfigId":10,"sca
nConfigRevisionId":1,
3 "computerName":"My-
verybadlaptop","computerIpAddress":"192.168.8.2","matchType":"process","eid":2001,"detail
s":
4 "{\"finding\":{\"whats\":[{\"intel_intra_ids\":[{\"id\":1855798049},{\"id\":3033354457},
{\"id\":3426971627}],\
5 "source_name\":\"recorder\",\"artifact_activity\":{\"relevant_actions\":
[{\"verb\":6,\"target\":{\"file\":{\
6 "path\":\"C:\\\\Program Files\\\\Microsoft
Office\\\\Updates\\\\Download\\\\PackageFiles\\\\6E48D237-4AC5-484B-
```


© 2025 Tanium Inc. All Rights Reserved

```
BF23-2F5E628DD32D\\\\root\\\\Office16\\\\Library\\\\Analysis\\\\ANALYS32.XLL\",\"size_bytes\":\"245760\",\
"modification_time\":\"2022-02-24T09:07:36.000Z\",\"instance_hash_salt\":\"132897442232920173\"},\"instance_hash\"
:\"308809884249771034\",\"artifact_hash\":\"10579797389185226535\"},\"timestamp\":\"2022-02-24T09:07:36.000Z\",\
"tanium_recorder_event_table_id\":\"4611686018476368681\"},{\"verb\":8,\"target\":{\"file\":{\"path\":\"C:\\\\
WINDOWS\\\\system32\\\\config\\\\systemprofile\\\\AppData\\\\Local\\\\Microsoft\\\\Office\\\\OTele\\\\
officeclicktorun.exe.db-wal\",\"size_bytes\":\"12392\",\"modification_time\":\"2022-02-24T09:06:08.000Z\
",\"instance_hash_salt\":\"132899412650062637\"},\"instance_hash\":\"12150348097614906623\",\"artifact_hash\":
\"8976838609497398981\"},\"timestamp\":\"2022-02-24T09:06:08.000Z\",\"tanium_recorder_event_table_id\":\
"4611686018476365859\"},{\"verb\":6,\"target\":{\"file\":{\"path\":\"C:\\\\Program Files\\\\Microsoft Office
\\\\Updates\\\\Download\\\\PackageFiles\\\\6E48D237-4AC5-484B-BF23-2F5E628DD32D\\\\root\\\\Office16\\\\Library
\\\\Analysis\\\\ANALYS32.XLL\",\"size_bytes\":\"245760\",\"modification_time\":\"2022-02-24T09:07:36.000Z\",\
"instance_hash_salt\":\"132897442232920173\"},\"instance_hash\":\"308809884249771034\",\"artifact_hash\":\
"10579797389185226535\"},\"timestamp\":\"2022-02-24T09:07:36.000Z\",\"tanium_recorder_event_table_id\":\
"4611686018476368681\"}],\"acting_artifact\":{\"process\":{\"handles\":[],\"pid\":9320,\"arguments\"
:\"OfficeClickToRun.exe /update\",\"file\":{\"file\":{\"path\":\"C:\\\\Program Files\\\\Common Files\\\\
microsoft shared\\\\ClickToRun\\\\Updates\\\\16.0.14827.20198\\\\OfficeClickToRun.exe\",\"hash\":{\"md5\":
\"9af1a2a7cdf7521012e843a2c0c94d02\"}},\"instance_hash\":\"16551595934051318733\",\"artifact_hash\":\
```


© 2025 Tanium Inc. All Rights Reserved

```
"16551595934051318733\"},\"user\":{\"user\":{\"name\":\"SYSTEM\",\"domain\":\"NT AUTHORITY\"}},\"parent\":
{\"process\":{\"handles\":[],\"pid\":3240,\"arguments\":\"\\\"C:\\\\Program Files\\\\Common Files\\\\Microsoft
Shared\\\\ClickToRun\\\\OfficeClickToRun.exe\\\" /service\",\"file\":{\"file\":{\"path\":\"C:\\\\Program Files
\\\\Common Files\\\\microsoft shared\\\\ClickToRun\\\\OfficeClickToRun.exe\",\"hash\":{\"md5\":\
"67abab5bdbf1738078ee8609519ae756\"}},\"instance_hash\":\"9683604588018453200\",\"artifact_hash\":\
"9683604588018453200\"},\"user\":{\"user\":{\"name\":\"SYSTEM\",\"domain\":\"NT AUTHORITY\"}},\"parent\"
:{\"process\":{\"handles\":
[],\"pid\":696,\"arguments\":\"C:\\\\WINDOWS\\\\system32\\\\services.exe\",\"file\":
{\"file\":{\"path\":\"C:\\\\Windows\\\\System32\\\\services.exe\",\"hash\":{\"md5\":\
"d8e577bf078c45954f4531885478d5a9\"}},\"instance_hash\":\"6947451072025863585\",\"artifact_hash\":\
"6947451072025863585\"},\"user\":{\"user\":{\"name\":\"SYSTEM\",\"domain\":\"NT AUTHORITY\"}},\"parent\":
{\"process\":{\"handles\":[],\"pid\":564,\"arguments\":\"wininit.exe\",\"file\":{\"file\":{\"path\":\"C:\\\\
Windows\\\\System32\\\\wininit.exe\",\"hash\":
{\"md5\":\"f3828d75795d5ae4b2d8b828026a4eaa\"}},\"instance_hash\":
\"17707501397744506371\",\"artifact_hash\":\"17707501397744506371\"},\"user\":{\"user\":{\"name\":\"SYSTEM\",\
"domain\":\"NT AUTHORITY\"}},\"parent\":{\"process\":{\"handles\":
[],\"pid\":464},\"instance_hash\":\
"12417824902308500885\",\"artifact_hash\":\"133628619820746138\"},\"start_time\":\"2022-02-21T18:20:54.000Z\",\
"tanium_unique_id\":\"1217629972152873483\"},\"instance_
hash\":\"1219598035047296839\",\"artifact_hash\":\
"11849315847930828064\"},\"start_time\":\"2022-02-21T18:20:54.000Z\",\"tanium_unique_
id\":\"11375085314266065265\"},
\"instance_hash\":\"5014940827374301866\",\"artifact_
hash\":\"16653308074585833820\"},\"start_time\":\"2022-02-
```


© 2025 Tanium Inc. All Rights Reserved

```
21T18:20:59.000Z\",\"tanium_unique_id\":\"8043614338822129387\"},\"instance_
hash\":\"4937418741321620235\",\
"artifact_hash\":\"9064172419262849089\"},\"start_time\":\"2022-02-
24T09:06:03.000Z\",\"tanium_unique_id\":\
"4638862404773214281\"},\"instance_hash\":\"16504704767541148257\",\"artifact_
hash\":\"14589750266879349142\",\
"is_intel_target\":true}}}],\"intel_id\":\"149:3\",\"hunt_id\":\"10\",\"threat_
id\":\"1855798049,3033354457,
3426971627\",\"source_name\":\"recorder\",\"system_info\":{\"os\":\"Microsoft Windows 10
Pro\",\"bits\"
:64,\"platform\":\"Windows\",\"build_number\":\"19044\",\"patch_
level\":\"10.0.19044.0.0\"},\"first_seen\":\
"2022-02-24T09:07:37.000Z\",\"last_seen\":\"2022-02-24T09:07:37.000Z\",\"finding_
id\":\"9053665738863672599\",
\"reporting_id\":\"reporting-id-placeholder\"},\"match\":
{\"version\":1,\"type\":\"process\",\"source\":\
"recorder\",\"hash\":\"14589750266879349142\",\"properties\":
{\"pid\":9320,\"args\":\"OfficeClickToRun.exe /
update\",\"recorder_unique_id\":\"4638862404773214281\",\"start_time\":\"2022-02-
24T09:06:03.000Z\",\"ppid\
":3240,\"user\":\"NT AUTHORITY\\\\SYSTEM\",\"file\":
{\"md5\":\"9af1a2a7cdf7521012e843a2c0c94d02\",\"fullpath\
":\"C:\\\\Program Files\\\\Common Files\\\\microsoft
shared\\\\ClickToRun\\\\Updates\\\\16.0.14827.20198\\\\
OfficeClickToRun.exe\"},\"parent\":{\"pid\":3240,\"args\":\"\\\"C:\\\\Program
Files\\\\Common Files\\\\Microsoft
Shared\\\\ClickToRun\\\\OfficeClickToRun.exe\\\" /service\",\"recorder_unique_
id\":\"8043614338822129387\",\
"start_time\":\"2022-02-21T18:20:59.000Z\",\"ppid\":696,\"user\":\"NT
AUTHORITY\\\\SYSTEM\",\"file\":{\"md5\":\
"67abab5bdbf1738078ee8609519ae756\",\"fullpath\":\"C:\\\\Program Files\\\\Common
Files\\\\microsoft shared\\\\
ClickToRun\\\\OfficeClickToRun.exe\"},\"parent\":
{\"pid\":696,\"args\":\"C:\\\\WINDOWS\\\\system32\\\\
```

© 2025 Tanium Inc. All Rights Reserved

```
services.exe\",\"recorder_unique_id\":\"11375085314266065265\",\"start_time\":\"2022-02-21T18:20:54.000Z\",\
"ppid\":564,\"user\":\"NT AUTHORITY\\\\SYSTEM\",\"file\":{\"md5\":\"d8e577bf078c45954f4531885478d5a9\",\
"fullpath\":\"C:\\\\Windows\\\\System32\\\\services.exe\"},\"parent\":{\"pid\":564,\"args\":\"wininit.exe\",
\"recorder_unique_id\":\"1217629972152873483\",\"start_time\":\"2022-02-21T18:20:54.000Z\",\"ppid\":464,\
"user\":\"NT AUTHORITY\\\\SYSTEM\",\"file\":{\"md5\":\"f3828d75795d5ae4b2d8b828026a4eaa\",\"fullpath\":\
"C:\\\\Windows\\\\System32\\\\wininit.exe\"},\"parent\":{\"pid\":464}}}}}}}","alertedAt":"2022-02-24T09:10:
03.319Z","createdAt":"2022-02-24T09:10:03.369Z","updatedAt":"2022-02-24T09:10:03.369Z","Endpoint":
{"id":3,"impactScore":15,"impactAssetId":20,"impactOutboundAssetCount":7},"
intelDocName":"Persistence
using Office Templates and Trusts","eventType":"process","path":"C:\\Program Files\\Common Files\\microsoft
shared\\ClickToRun\\Updates\\16.0.14827.20198\\OfficeClickToRun.exe","hash":"9af1a2a7cdf7521012e843a2c0c94d02"
,"platform":"Windows","os":"Microsoft Windows 10 Pro","intelDocType":"tanium-signal","intelSourceId":4,
"intelSourceName":"Tanium Signals","mitreAttack":"{\"techniques\":[{\"id\":\"T1221\",\"name\":\"Template
Injection\"},{\"id\":\"T1137\",\"name\":\"Office Application Startup\"},{\"id\":\"T1137.001\",\"name\":\"Office
Application Startup: Office Template Macros\"},{\"id\":\"T1137.006\",\"name\":\"Office Application Startup:
Add-ins\"},{\"id\":\"T1059\",\"name\":\"Command and Scripting Interpreter\"},{\"id\":\"T1059.003\",\
"name\":\"Command and Scripting Interpreter: Windows Command Shell\"}]}"}]
```


© 2025 Tanium Inc. All Rights Reserved

Maintaining Impact

Perform regular maintenance tasks to ensure that Impact successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Impact is not performing as expected, you might need to troubleshoot issues or change settings. See Troubleshooting Impact on page 61 for related procedures.

Perform monthly maintenance

1. From the Main menu, go to **Modules > Trends > Boards**.
2. Click the **Impact** board and review the **Impact Coverage Status** panel for endpoints with the following status:
   - **Needs Attention**: Python tools that are required for Impact sensors are not installed.
   - **Unsupported**: Impact does not support the operating system.
3. To investigate endpoints that need attention, click the **Needs Attention** bar in the chart and select **View Current Endpoint Details filtered by Needs Attention**. The Tanium Server issues the following question:
   `Get Computer Name and Operating System and IP Address and Impact - Coverage Status equals Needs Attention from all machines with Impact - Coverage Status equals Needs Attention`
4. To investigate endpoints that do not support Impact, click the **Unsupported** bar in the chart and select **View Current Endpoint Details filtered by Unsupported**. The Tanium Server issues the following question:
   `Get Computer Name and Operating System and IP Address and Impact - Coverage Status equals Unsupported from all machines with Impact - Coverage Status equals Unsupported`
5. To troubleshoot Impact coverage, see Monitor and troubleshoot Impact Coverage on page 59.

Monitor and troubleshoot Impact Coverage

The following table lists contributing factors into why the Impact coverage metric might report endpoints as **Needs Attention** or **Unsupported**, and corrective actions you can make.

Contributing factors and corrective actions for Tanium Impact

Contributing factor	Corrective action
Domain is not configured properly	• Impact only includes data from endpoints for which the domain controller can be reached. Ensure that the domain is configured correctly in the **Domains** configuration in the Impact settings, and that all of your domains are covered and configured correctly. • In the **Domains** configuration, verify all domain connections. The verification process includes a network connection test and verifies the provided credentials. • Make sure the provided account has permissions to read Active Directory information.

© 2025 Tanium Inc. All Rights Reserved

Contributing factors and corrective actions for Tanium Impact (continued)

Contributing factor	Corrective action
Python tools are not installed	• The Impact sensors are written in Python and require the `Tanium Python Tools` to be deployed to the endpoints. • Verify that all endpoints have the latest version of the `Tanium Python Tools` installed using the following sensor: `Get Python - Tools Version from all machines with Operating System contains windows` • Deploy the `Distribute Python - Tools [Windows]` package to any endpoints that return `Windows Package Required`.

© 2025 Tanium Inc. All Rights Reserved

Troubleshooting Impact

To collect and send information to Tanium for troubleshooting, collect logs and other relevant information.

Collect logs

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

To download logs:

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

   TIP

   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 files. For information, see Contact Tanium Support on page 67.

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

Upgrade Impact

Impact 2.0 or later requires the installation of Tanium Directory Query and Tanium Criticality. Additionally, you must install Directory Query first, followed by Criticality, and then Impact, in that order.

IMPORTANT

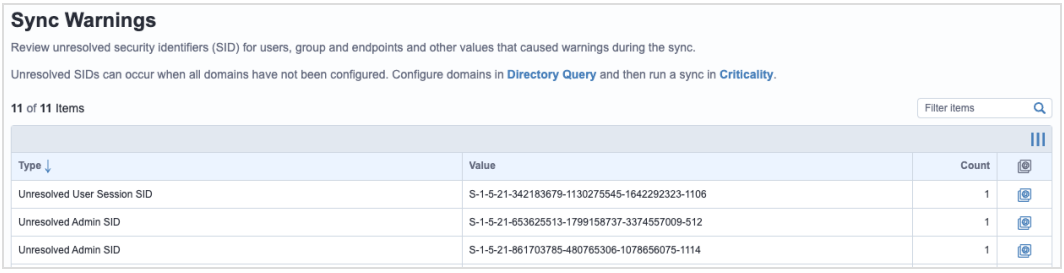
In Impact 2.0 or later, the steps required to configure the service account are no longer necessary due to the adoption of the System User Service, which performs these tasks automatically. Additionally, the Impact database is migrated to RDB in this release. Consequently, after upgrading to Impact 2.0 or later, it might take time for the database migration to complete and for RBAC privileges and other updates to sync properly. This migration could lead to issues and error messages when you first query Tanium Console. These issues should resolve on their own after a few minutes, but could take up to an hour or longer depending on system resources and the amount of data to migrate.

© 2025 Tanium Inc. All Rights Reserved

Troubleshoot unresolved SIDs

If the domain for an endpoint is not configured in Directory Query, you might see assets on the **Sync Warnings** page with unresolved SIDs.

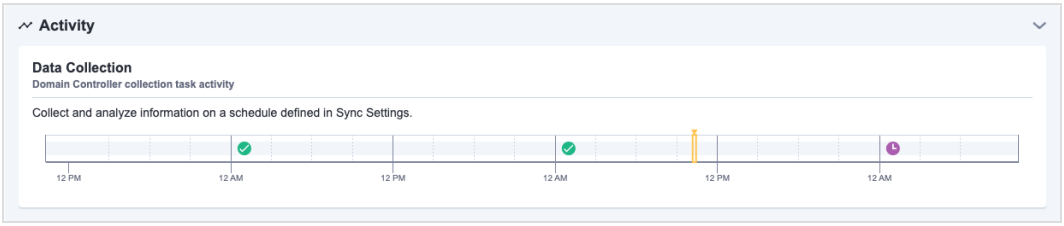
1. From the Main menu, go to **Impact > Sync Warnings**.



2. For each asset with an unresolved SID type, click Interact to view more information about the asset.
3. The **AD Domain** column of the question results shows the name of the domain for which Impact could not resolve assets.



4. Verify the domain is configured in Directory Query. For more information, see Tanium Directory Query User Guide: Managing connections to directory servers.
5. Verify that the specified account has sufficient permissions. For more information, see Impact requirements on page 22.
6. After all domains are configured and permissions are validated, verify that a successful data collection and sync completes. You can see the latest status in the **Activity** section of the Impact **Overview** page.



BEST PRACTICE

Run a sync in Tanium Criticality before running a sync in Impact.

© 2025 Tanium Inc. All Rights Reserved

Identify and resolve issues with Client Extensions

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

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

1. If endpoints have Client Extension shared process mode enabled and you need to troubleshoot resource usage or crashes in the combined `TaniumCX.exe` or `TaniumCX` process, disable shared process mode on the affected endpoints, and then reproduce the issue if possible. For more information, see Endpoint Configuration User Guide: Manage Client Extension shared process mode.
2. To review the health of Client Extensions or to start an investigation into an existing error, ask a question using the `Client Extensions - Status` sensor.

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

   Consider whether endpoints with errors share common characteristics, such as operating system, domain or organization unit, or the antivirus software that is installed.
3. Target one or more endpoints with errors, and uninstall tools that report errors without blocking reinstallation. For more information, see Remove Impact tools from endpoints and Endpoint Configuration User Guide: Uninstall a tool installed by Endpoint Configuration.

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

   Wait for automatic reinstallation of the tool. If the reinstallation does not resolve the issue, continue to the next step.
4. Ask a question using the `Endpoint Configuration - Tools Status Details` sensor, and include filters to limit the results to the tool that you are investigating. For example:

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

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

© 2025 Tanium Inc. All Rights Reserved

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

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

5. Review the Extensions logs on the endpoint. Take note of entries that include `fail` or `error`. For more information, see Review the Extensions log for an endpoint on page 65.

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

© 2025 Tanium Inc. All Rights Reserved

Review the Extensions log for an endpoint

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

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

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

Remove Impact tools from endpoints

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

1. In Interact, target the endpoints from which you want to remove the tools. For example, ask a question that targets a specific operating system:
   `Get Endpoint Configuration - Tools Status from all machines with Is Windows equals true`
2. In the results, select the row for **Impact**, drill down as necessary, and select the targets from which you want to remove Impact tools. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
5. For **Tool Name**, select **Impact**.
6. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.

   NOTE

   If reinstallation is blocked, you must unblock it manually:

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

© 2025 Tanium Inc. All Rights Reserved

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

   CAUTION

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

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

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

   BEST PRACTICE

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

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

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

NOTE

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

Verify endpoint tools

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

Uninstall Impact

1. From the Main menu, click **Administration > Configuration > Solutions**.
2. In the Impact section, click **Uninstall**.
3. Review the content that will be removed and click **Uninstall**.
4. Depending on your configuration, enter your password or click **Yes** to start the uninstall process.
5. Return to the **Solutions** page and verify that the **Import** button is available for Impact.

© 2025 Tanium Inc. All Rights Reserved

NOTE

The uninstall process does not remove the Impact action group. If you are sure that this action group is not used by another solution, you can manually remove it. If you uninstall Impact, do not remove the computer group, and later reinstall Impact, the action group target remains set to the original computer group.

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: Impact sensors

Use the Impact sensors to get details about Impact functionality on endpoints.

Impact sensors

Sensor	Description
Impact - Active User Session SIDs	Get the SIDs of users with an active session. This sensor provides a function to determine whether or not an endpoint is joined to a domain. If it is not, the sensor exits. If it is, this same function is used to obtain the local computer SID. This sensor uses a WMI query to determine if the sensor is being executed on a domain controller. Each user session SID is compared against the local computer SID. If the User SID contains the local computer SID, it is a local account and is ignored. Since all accounts on a domain controller are domain accounts, the local computer SID comparison is skipped to ensure accurate results if the sensor is running on a domain controller. Only domain SIDs with a LogonType that can be used for credential theft and reuse are returned by the sensor.
Impact - Administrator SIDs	Get the SIDs of the domain users and groups in the Administrators group. This sensor uses a function to determine whether or not the endpoint is joined to a domain. If it is not, the sensor exits. If it is, this same function is used to obtain the local computer SID. This sensor uses A WMI query to determine if the sensor is being executed on a domain controller. This sensor ensures the correct group name is returned for enumeration as the name may vary depending on language/localization settings on the endpoint, or a user might have renamed it. This sensor uses a function to ensure it is run against the local system. If the SID contains the local computer SID, it is a local account, and is ignored. Because all accounts on a domain controller are domain accounts, the local Computer SID comparison is skipped to ensure accurate results if the sensor is running on a domain controller. All domain SIDs that are a member of the local Administrators group on the endpoint are returned by the sensor.
Impact - Computer Domain SID	Get the SID of the domain to which the computer is joined. This sensor uses a function to retrieve the SID for the Domain that the computer is joined to. This SID is stored locally on the endpoint and only present if the endpoint has been joined to a Domain. It differs from the local computer SID which is created when the operating system is installed.
Impact - Physical NetBIOS Computer Name	Get the NetBIOS name of an endpoint. The results of this sensor provide a reliable match that can be used by the Tanium Impact Service on the Module Server to perform an LDAP query to retrieve the Computer Account SID from Active Directory.

© 2025 Tanium Inc. All Rights Reserved

Impact sensors (continued)

Sensor	Description
Impact - Tools Version	Reports support and installation details. If tools have been installed, reports the version of tools and if all the required tools are present. Example (unsupported) Incoming Claim=Unsupported Client Version Unsupported Example (uninstalled): Not Installed Linux Package Required Example (installed): 1.0.0.0057 Linux Package Installed

© 2025 Tanium Inc. All Rights Reserved

Reference: Remediation resources



Test changes to Active Directory in a lab or staging environment before you make the change in a production environment.

Before making any changes to Active Directory, be sure that you understand the potential repercussions, including loss of control or access to business critical assets.

Use the data that you gather from Impact to identify the users, groups, and endpoints with the highest potential impact in your organization, considering the following guidelines:

- Analyze both inbound and outbound potential lateral movement:
    - An asset with a high potential inbound impact might be easily compromised due to the variety of paths that can be used to reach this asset. Examine any business critical assets with a high inbound impact to determine where access can be reduced.
    - An asset with a high potential outbound impact can be used to compromise other assets in your environment. Examine any assets with a high outbound impact and minimize access to other assets where possible.
- A complex **Shortest Path** to reach a business critical asset does not indicate that the asset is safe from attack. Although the **Shortest Path** for an asset might appear complex, sophisticated attackers often automate path traversal. Complex paths can be traversed quickly using automation.
- Users with a high potential outbound impact are one successful phishing attack away from an attacker potentially reaching the assets to which they have administrative control. Limit users to the administrative access that they need to perform their work.

Where possible, reduce privileges to implement a least-privilege model for your Active Directory environment. For more information, see Microsoft: Implementing Least-Privilege Administrative Models.

© 2025 Tanium Inc. All Rights Reserved