

Tanium™ Criticality User Guide

Autonomous IT. Unstoppable Business.

2025H1 and 2025H2 Semiannual Release

Version 1.7

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

Criticality overview **7**

Criticality scale 7

Criticality rules 7

Schedule for criticality updates 8

Update to default endpoint criticality 8

Update to endpoint rules 8

Update to default user and group criticality 9

Update to user and group rules 9

Interoperability with other Tanium products 9

Benchmark 9

Impact 9

Reporting 9

Getting started with Criticality **10**

Step 1: Install and configure Criticality 10

Step 2: Review the default criticality level 10

Step 3: Create rules to assign criticality 10

Criticality requirements **11**

Core platform dependencies 11

Solution dependencies 11

Tanium recommended installation 11

Import specific solutions 11

Required dependencies 11

Tanium™ Module Server 12

Endpoints 12

Supported Internet protocols 12

Supported operating systems 12

Host and network security requirements 12

© 2025 Tanium Inc. All Rights Reserved

Ports ... 12
Security exclusions ... 13
User role requirements ... 13
Installing Tanium Criticality ... 16
Before you begin ... 16
Import Criticality with default settings ... 16
Import Criticality with custom settings ... 16
Manage solution dependencies ... 17
Verify Criticality version ... 17
Troubleshoot issues ... 17
Configuring Criticality ... 18
Configure user and group synchronization settings ... 18
Configure connections to domains ... 18
Collect and analyze data ... 18
Set up Criticality users ... 19
Assigning endpoint criticality ... 21
Assign default endpoint criticality ... 21
Create rules to assign criticality to specific endpoints ... 21
Work with existing criticality rules ... 24
View criticality rules ... 24
Prioritize criticality rules ... 24
Manage rules ... 25
Manage Tanium Risk Assessment rules ... 26
Work with endpoints ... 26
View endpoints ... 26
Customize columns ... 28
Export table ... 28
View status of endpoint updates ... 28
Assigning user and group criticality ... 30
Assign default user and group criticality ... 30

© 2025 Tanium Inc. All Rights Reserved

Create rules to assign criticality to specific users or groups 30
Work with existing criticality rules 31
View user and group criticality rules 32
Prioritize criticality rules 32
Manage rules 33
Work with users and groups 34
View users 34
View groups 34
Customize columns 36
View status of user and group updates 36
Troubleshooting Criticality **38**
Collect logs 38
Troubleshoot endpoint criticality 38
Troubleshoot user and group criticality 39
Uninstall Criticality 39
Contact Tanium Support 39

© 2025 Tanium Inc. All Rights Reserved

Criticality overview

With Criticality, you can define levels for each Tanium Client managed endpoint, user, or group that are available to other Tanium solutions, such as Tanium™ Impact and Tanium™ Benchmark, to add context about the endpoint.

Criticality scale

Possible criticality levels include the following values:

- **Critical**
- **High**
- **Medium**
- **Low**

By default, the criticality level is **Medium**. You can modify the default criticality level. For more information, see Assign default endpoint criticality on page 21 and Assign default user and group criticality on page 30.

All endpoints, users, and groups are assigned to the default level, unless they are assigned to rules. For more information on how rules work, see Criticality rules on page 7.

Criticality rules

Rules override default criticality for specific endpoints, users, or groups.

BEST PRACTICE

Create rules to override the default criticality based on attributes of the endpoints, for example, computer group or operating system. For example, you might create a rule to set all Windows endpoints in a specific domain to **High** criticality. If an endpoint is assigned to more than one unprioritized rule, the rule with a higher criticality level takes precedence. For example, if one rule sets all Windows endpoints to **Medium** and another rule sets all servers are set to **High**, a Windows server is always set to **High**.

You can prioritize rules to specify which rule takes precedence if an endpoint, user, or group is assigned to more than one rule. The priority of the rule overrides the criticality level of the rule. For example, if one rule is prioritized to 2 and sets all Windows endpoints to **Medium** and another rule is prioritized to 1 and sets Windows endpoints within a specific domain to **Low**, then Windows endpoints within the specified domain are set to **Low**.

When a rule is deleted, the endpoint criticality is set to the next highest applicable rule based on prioritization or criticality level (if no prioritized rules apply to the endpoint, user, or group). If no rule exists, Criticality assigns the default level to the endpoint, user, or group.

If you import Criticality with the **Tanium Recommended Installation**, Criticality contains the following default rules. You can edit or delete the default endpoint rules, but you cannot edit or delete the default group rule. To override the default group rule, you can create a prioritized group rule.

© 2025 Tanium Inc. All Rights Reserved

Default criticality rules

Default rule	Rule type	Criticality level
Domain Controllers	Endpoint	Critical
Servers	Endpoint	High
Workstations	Endpoint	Medium
Default Critical Active Directory Groups	Group	Critical

For more information, see Create rules to assign criticality to specific endpoints on page 21 and Create rules to assign criticality to specific users or groups on page 30.

Schedule for criticality updates

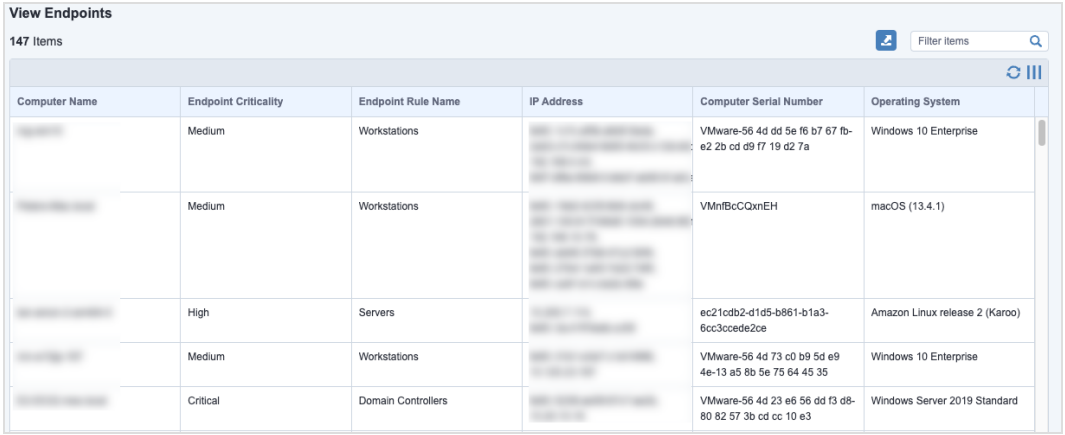
Criticality updates endpoints and reports with different frequencies, depending on if you update the default criticality level or criticality rules.

Benchmark uses a different update frequency than Criticality. Depending on your configuration, Benchmark can update risk scores from every two hours to once a day.

Update to default endpoint criticality

If you modify the default endpoint criticality, Criticality immediately updates the **Configuration > Endpoints > View Endpoints** table. Criticality updates the endpoints each hour. For more information, see View status of endpoint updates on page 28.

Endpoint criticality



Update to endpoint rules

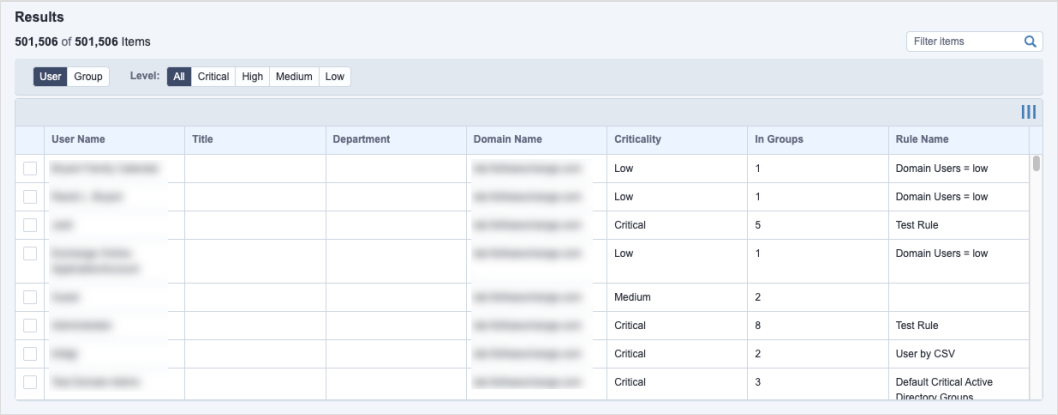
If you modify endpoint criticality rules, Criticality updates endpoints and reports each hour.

© 2025 Tanium Inc. All Rights Reserved

Update to default user and group criticality

If you modify the default user and group criticality, Criticality immediately updates the **Configuration > Users and Groups > Results** table.

Users and groups results



Update to user and group rules

If you modify user or group criticality rules, Criticality updates and reports according to the schedule that you configured in the **User/Group Settings** tab in the Criticality Settings. You can also manually request a sync from the **User/Group Schedule** tab in the Criticality Settings. For more information, see View status of user and group updates on page 36.

Interoperability with other Tanium products

Criticality works with Tanium™ Benchmark, Tanium™ Impact, and Tanium™ Reporting.

Benchmark

Benchmark uses the endpoint criticality levels when calculating endpoint risk scores. For more information, see Tanium Benchmark User Guide: Configuring Benchmark.

Impact

Impact includes criticality levels for users, groups, and endpoints. For more information, see Tanium Impact User Guide: Identifying high impact users, endpoints, and groups.

Reporting

Create and view reports in Reporting that include criticality levels. For more information, see Tanium Reporting User Guide: Working with reports.

© 2025 Tanium Inc. All Rights Reserved

Getting started with Criticality

Follow these steps to configure and use Criticality.

Step 1: Install and configure Criticality

See Installing Tanium Criticality on page 16 and Configuring Criticality on page 18.

Step 2: Review the default criticality level

The default criticality level is **Medium**. You can change the default.

For more information, see Assign default endpoint criticality on page 21 and Assigning user and group criticality on page 30.

Step 3: Create rules to assign criticality

Create rules to override the default criticality level for specified Tanium Client managed endpoints, users, or groups.

For more information, see Create rules to assign criticality to specific endpoints on page 21 and Create rules to assign criticality to specific users or groups on page 30.

© 2025 Tanium Inc. All Rights Reserved

Criticality requirements

Review the requirements before you install and use Criticality.

Core platform dependencies

Make sure that your environment meets the following requirements:

- **Tanium™ Core Platform servers**
- **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 Criticality to function (required dependencies) or for specific Criticality 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 Criticality dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 11. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Criticality requires.

Tanium recommended installation

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

Required dependencies

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

© 2025 Tanium Inc. All Rights Reserved

1. Tanium™ Interact
2. Tanium™ Data Service (TDS)
3. Tanium™ System User Service
4. Tanium™ RDB Service
5. Tanium™ Blob Service
6. Tanium™ Reporting
7. Tanium™ Directory Query

Tanium™ Module Server

Criticality 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 Internet protocols

Criticality supports IPv4 and IPv6 addresses.

Supported operating systems

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

Host and network security requirements

Specific ports and processes are needed to run Criticality.

Ports

The following ports are required for Criticality communication.

Ports for Tanium Criticality communication

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17532	TCP	Internal purposes, not externally accessible

© 2025 Tanium Inc. All Rights Reserved

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.

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

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\criticality-service\TaniumCriticalityService.exe`

User role requirements

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

- Criticality user role permissions on page 14
- Criticality administration and platform content permissions on page 14: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Criticality users on page 19.

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

© 2025 Tanium Inc. All Rights Reserved

- RBAC overview (provides an overview of roles, permissions, and content sets)
- Provided role permissions
- View effective role permissions
- Configure a custom role

IMPORTANT

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

Criticality user role permissions

Permission	Criticality Administrator[1]	Criticality Operator[1]	Criticality User[1]
Criticality Accesses the Criticality workbench	SHOW READ WRITE	SHOW READ WRITE	SHOW READ
Criticality Support Bundle Provides privileges for the support bundle	READ		
Criticality Sync Allows manually starting a user and group sync		START	

[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.

Criticality administration and platform content permissions

Permission	Permission Type	Criticality Administrator	Criticality Operator	Criticality User
Computer Group	Administration	READ	READ	READ
Filter Group	Platform Content	READ	READ	READ
Plugin	Platform Content	READ EXECUTE	READ EXECUTE	READ EXECUTE

© 2025 Tanium Inc. All Rights Reserved

Criticality administration and platform content permissions (continued)

Permission	Permission Type	Criticality Administrator	Criticality Operator	Criticality User
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 Tanium Criticality

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

- **Automatic configuration with default settings**: Criticality 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 Criticality, see Import Criticality with default settings on page 16.
- **Manual configuration with custom settings**: After installing Criticality, you must manually configure required settings. Select this option only if Criticality requires settings that differ from the recommended default settings. For more information, see Import Criticality with custom settings on page 16.

Before you begin

- Read the release notes.
- Review the Criticality requirements on page 11.
- Assign the correct roles to users for Criticality. Review the User role requirements on page 13.
    - To import the Criticality solution, you must be assigned the Administrator reserved role.

Import Criticality with default settings

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

Default settings for Tanium Criticality

Setting	Default value
Endpoint rules	• **Domain Controllers** • **Servers** • **Workstations**
Group rules	**Default Critical Active Directory Groups**

To import Criticality 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 Criticality version on page 17.

Import Criticality with custom settings

To import Criticality without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** option 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 Criticality version on page 17.

© 2025 Tanium Inc. All Rights Reserved

If you import with custom settings, the default criticality rules are not created.

Manage solution dependencies

Other Tanium solutions are required for Criticality to function (required dependencies) or for specific Criticality features to work (feature-specific dependencies). For more information, see Solution dependencies on page 11.

Verify Criticality version

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

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

Troubleshoot issues

If you experience issues with installing Criticality, see Troubleshooting Criticality on page 38.

© 2025 Tanium Inc. All Rights Reserved

Configuring Criticality

Configure user and group synchronization settings

1. From the Main menu, go to **Shared Services > Criticality**.
2. Click Settings and open the **User/Group 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**.

BEST PRACTICE

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

- Start at least one hour before Impact synchronizations start.
- Choose the same frequency or sync more frequently than Impact.

Configure connections to domains

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

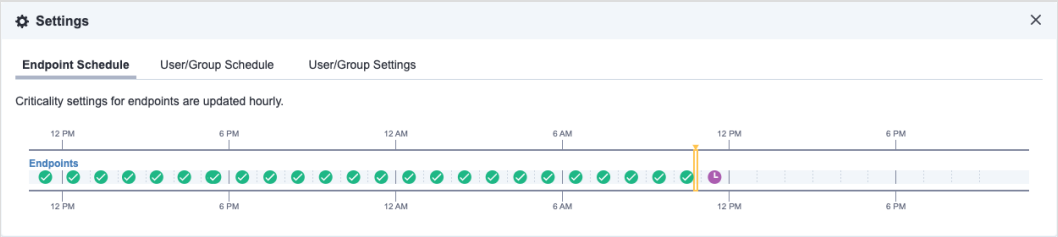
After you save the domain connection, data collection and analysis begins automatically at the next scheduled synchronization. For more information, see Collect and analyze data on page 18.

Collect and analyze data

For Tanium Client managed endpoints, data is automatically synchronized every hour. To view the last time that data was collected and analyzed, and the next scheduled collection and analysis, go to the **Endpoint Schedule** tab in Criticality Settings.

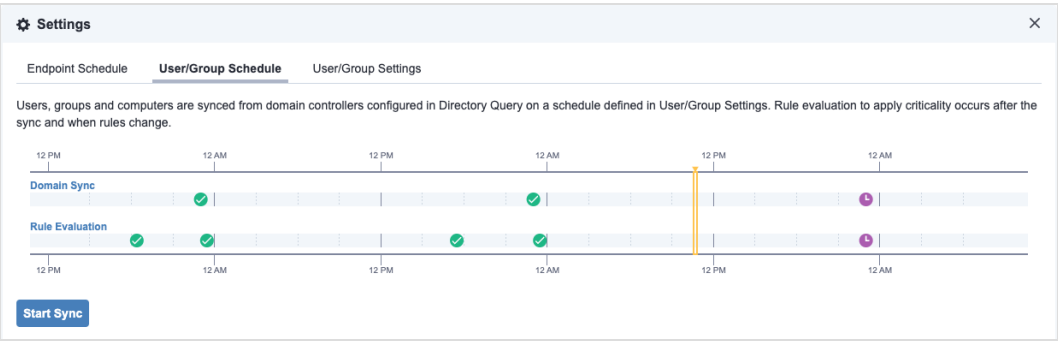
© 2025 Tanium Inc. All Rights Reserved

Endpoint schedule



For users and groups, data is automatically synchronized according to the schedule in **User/Group Settings**. To view the last time that data was collected and analyzed, and the next scheduled collection and analysis, go to the **User/Group Schedule** tab in Criticality Settings. To initiate data collection and analysis for users and groups manually, click **Start Sync**.

User/Group schedule



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 Criticality users

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

To review specific permissions for each role, see User role requirements on page 13.

IMPORTANT

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

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

© 2025 Tanium Inc. All Rights Reserved

Criticality Administrator

Assign the **Criticality Operator** role to users who manage the Criticality service.
This role can perform the following tasks:

- View the Criticality workbench.
- View and download Criticality data.
- Upload Criticality data.
- Download the Criticality support bundle.

Criticality Operator

Assign the **Criticality Operator** role to users who manage the Criticality service.
This role can perform the following tasks:

- View the Criticality workbench.
- View and download Criticality data.
- Upload Criticality data.

Criticality User

Assign the **Criticality User** role to users who view Criticality data.
This role can view the Criticality workbench.



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

© 2025 Tanium Inc. All Rights Reserved

Assigning endpoint criticality

Manage the criticality level of Tanium Client managed endpoints by assigning a default criticality level to apply to all endpoints or creating rules to override the default for specified endpoints.

For information on how often endpoints and reports are updated with criticality levels, see Schedule for criticality updates on page 8.

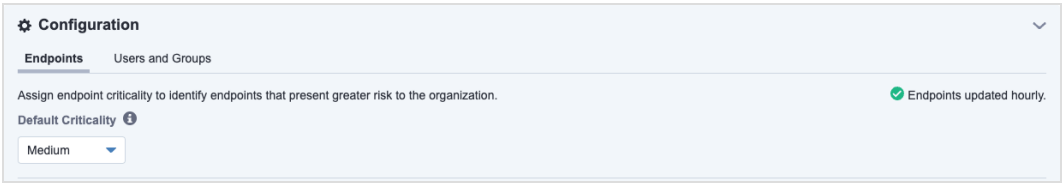
Assign default endpoint criticality

Assign a default criticality level to apply to all endpoints not targeted by a rule. By default, the criticality level is **Medium**.

TIP

The default **Workstations** rule (automatically created unless you selected a custom import) is similar to and overrides the default criticality level. If you want to change the default criticality level for endpoints with a rule, modify the **Workstations** rule. If you want to change the default criticality level for endpoints without a rule, delete the **Workstations** rule and set the criticality level using the **Default Criticality** drop-down list.

1. From the Main menu, go to **Shared Services > Criticality**.
2. Go to **Configuration > Endpoints** and select the **Default Criticality** level.



Create rules to assign criticality to specific endpoints

To specify different criticality levels for different groups of endpoints, create rules. You can create rules only for endpoints that you have permissions to manage.

You can create rules that use any Tanium sensor or computer group. You can also create rules by a static list of names. If you create a rule that uses a sensor that is not already registered, Tanium Server automatically registers the sensor.

1. From the Main menu, go to **Shared Services > Criticality**.
2. Go to the **Configuration > Endpoints > Rules** section.
3. Click **Create Rule** and enter the rule name.
4. Select the criticality level and priority number for the rule.
   If you select 1, for example, rule 1 is prioritized over rule 2. You can also set the priority after creating the rule. See Prioritize criticality rules on page 24.

© 2025 Tanium Inc. All Rights Reserved

5. Click **Select Computer Groups**, select the groups to assign to the rule, and click **Done**. You can select from computer groups to which you have write permission.

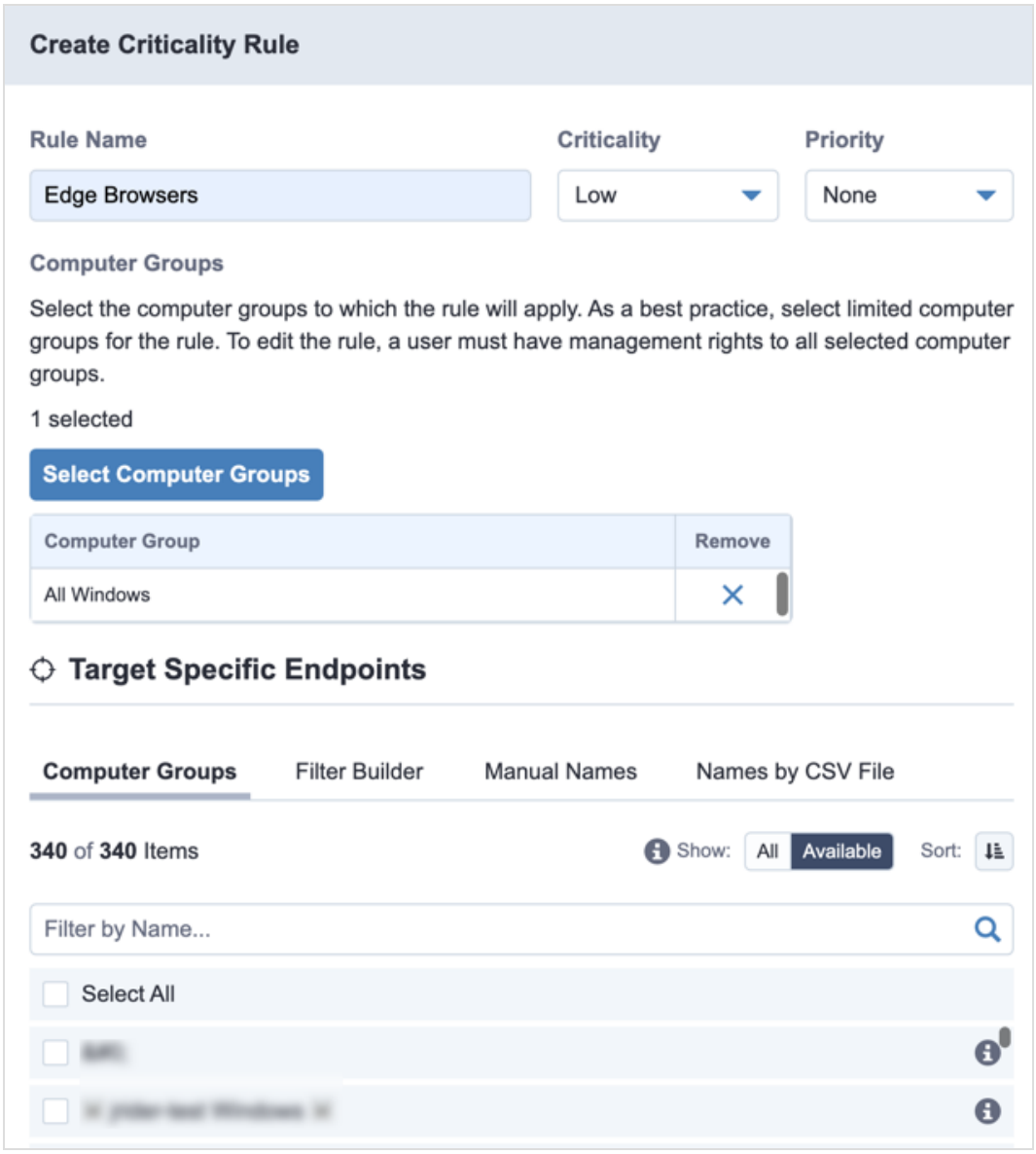
   

   Select limited computer groups for the rule. To edit the rule, a user must have management rights to all selected computer groups.

6. Use one of the following options to specify the endpoints to include in the rule.

   - **Computer Groups**: Select the computer groups to include.
   - **Filter Builder**: Specify the criteria to filter on all endpoints. For example, you can type `Operating System contains win` to target all Windows endpoints. The rule is applied to all endpoints that meet the criteria. Individual endpoints cannot be selected. Add rows or groupings to specify additional filter conditions.

© 2025 Tanium Inc. All Rights Reserved



- **Manual Names**: Enter the computer names, separated by commas. The names must be the exact names as returned by the **Computer Name** sensor.
- **Names by CSV File**: Upload a CSV file. The CSV file must contain each endpoint name on its own line without additional information. The endpoint name must be the name exactly as it is returned by the **Computer Name** sensor, similar to the following example:

```
computername1.domain.com
computername2.domain.com
```

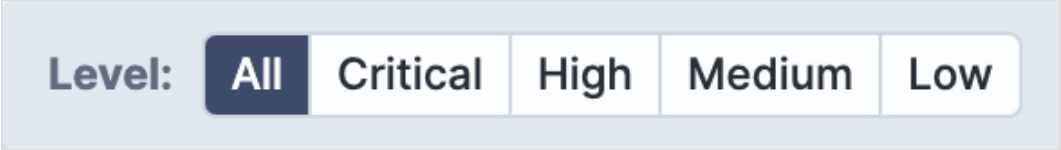
7. Click **Create Rule**.

© 2025 Tanium Inc. All Rights Reserved

Work with existing criticality rules

View criticality rules

1. From the Main menu, go to **Shared Services > Criticality**.
2. Go to the **Configuration > Endpoints > Rules** section.
3. View the rules. The table contains the following columns:
    - **Priority**: Numerical value indicating rule importance or **None** if no priority is set
    - **Status**: Status of the rule: New, Success, or Error
    - **Rule**: Name of the rule
    - **Criticality**: Criticality level of the rule
    - **Targeted Endpoints**: Endpoint targeting criteria for rule
    - **Endpoints**: Number of endpoints targeted by rule
    - **Actions**: Edit, delete, or other actions you can make on the rule depending on the rule details
4. To filter the rules based on criticality levels, click the corresponding toggle.



Prioritize criticality rules

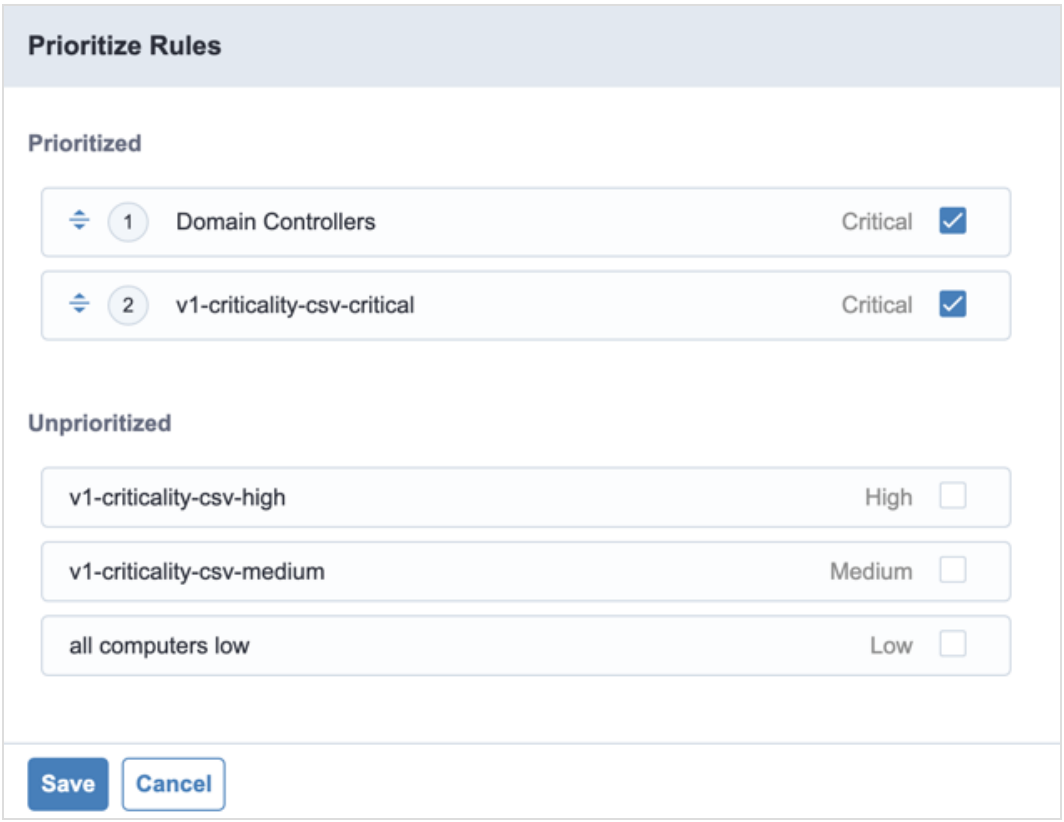
You can prioritize rules to specify which rule takes precedence if an endpoint is assigned to more than one rule.

BEST PRACTICE

Consider limiting the number of rules you prioritize to simplify criticality level management.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services > Criticality**.
2. Go to the **Configuration > Endpoints > Rules** section.
3. Click **Prioritize**.



   a. For existing prioritized rules, drag and drop the rules into the order you want, or use the arrows to specify the position.
   b. To prioritize an unprioritized rule, select the box next to the rule and then assign priority.
   c. To remove a priority, clear the box next to the rule.
   d. Click **Save**.

Manage rules

Edit or delete a rule using the options available in the **Actions** column in the **Rules** table.

You can also select a rule and click Edit or Delete. Depending on how a user or group rule was created, you can take additional actions on the rule:

- **Manual Names**: Select the rule and click Copy or select **Copy Names** from the **Actions** column.
- **Names by CSV File**: Select the rule and click Download or select **Download CSV** from the **Actions** column.

You can download a `txt` file with the rule of each endpoint. To download the `txt` file, click **Download Criticality Status** in the **Rules** table heading.

© 2025 Tanium Inc. All Rights Reserved

Manage Tanium Risk Assessment rules

If you enabled Tanium Risk Assessment (TRA) data collection in Tanium Benchmark 2.10 or later, the following endpoint rules are automatically created:

- TRA - Database Servers
- TRA - EoL Operating Systems
- TRA - High Uptime
- TRA - Insecure Services Running
- TRA - Insecure Wireless Access
- TRA - System Requires Reboot
- TRA - Unencrypted Physical Disks



If you delete any of these TRA rules and want to recreate them, disable TRA data collection in Tanium Benchmark and then enable it again. For more information about enabling and disabling TRA data collection in Tanium Benchmark, see Tanium Benchmark User Guide: (Optional) Enable Tanium Risk Assessment data collection.

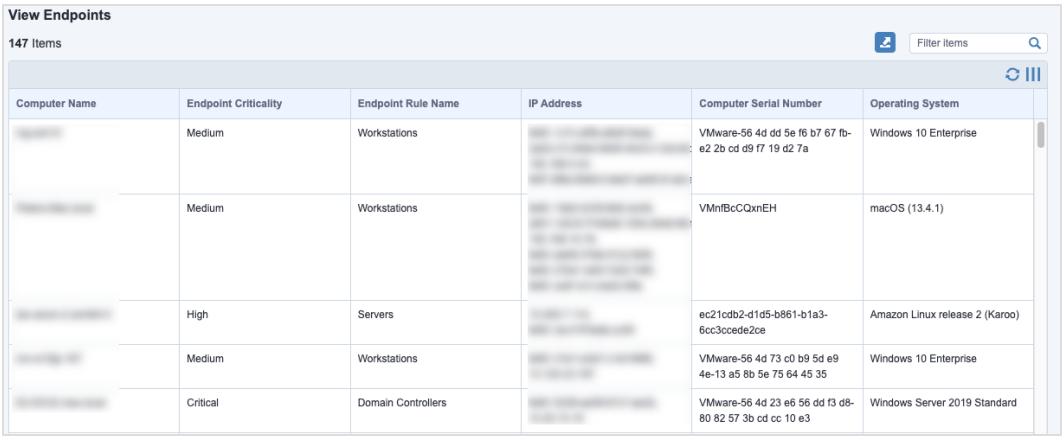
Work with endpoints

View endpoints

View all online and offline endpoints managed by Tanium, along with the corresponding criticality levels.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services > Criticality**.
2. Go to the **Configuration > Endpoints > View Endpoints** section.
3. View the endpoints. The table contains the following columns:

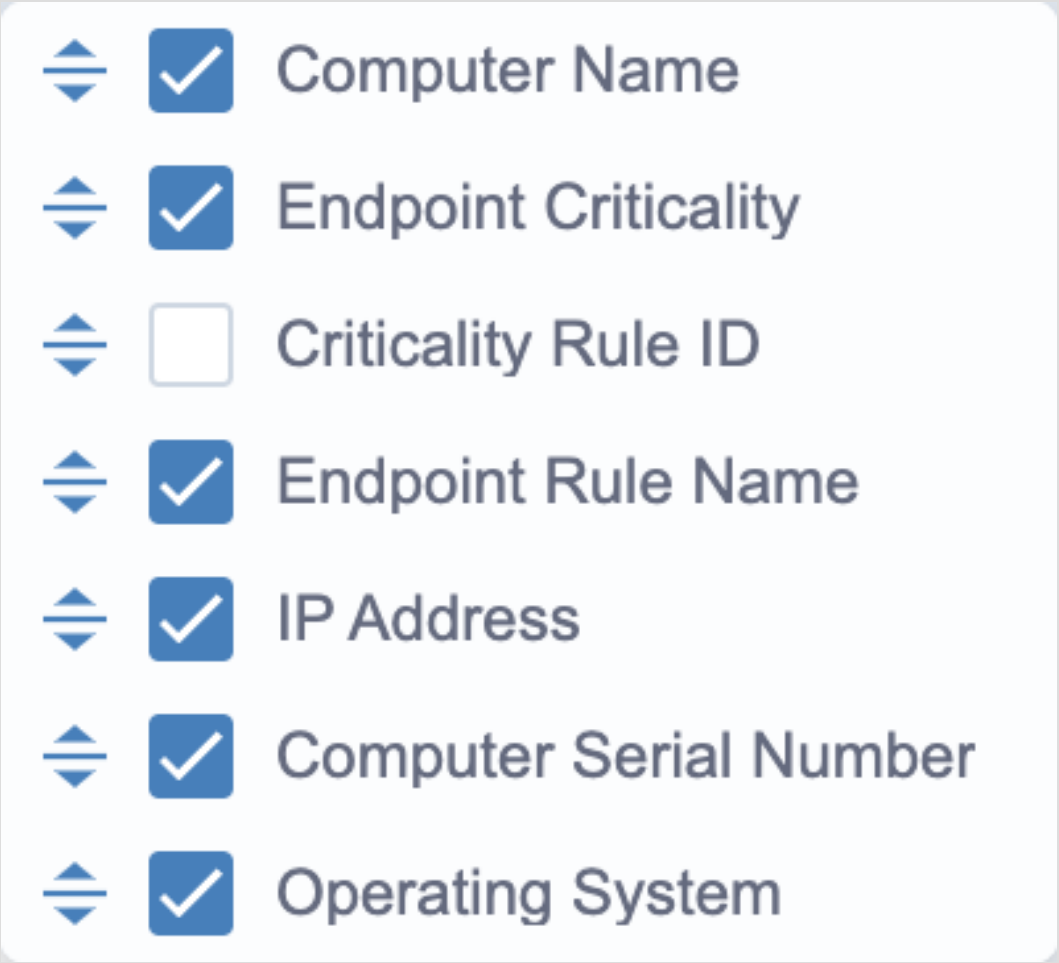


   - **Computer Name**: Result from **Computer Name** sensor
   - **Endpoint Criticality**: Criticality level assigned by default or a rule
   - **Endpoint Rule Name**: Rule assigned to the endpoint
     The column is blank if a rule is not assigned to the endpoint. (The endpoint is assigned the default criticality level.)
   - **IP Address**: Result from **IP Address** sensor
   - **Computer Serial Number**: Result from **Computer Serial Number** sensor
   - **Operating System**: Result from **Operating System** sensor
4. If necessary, filter the items by searching the table.

© 2025 Tanium Inc. All Rights Reserved

Customize columns

You can change which columns are displayed in the table, and adjust the order of the columns.



1. In the report, click Customize Columns.
2. To remove a column, clear the box for the column.
3. To adjust the column order, click and drag the column names.

Export table

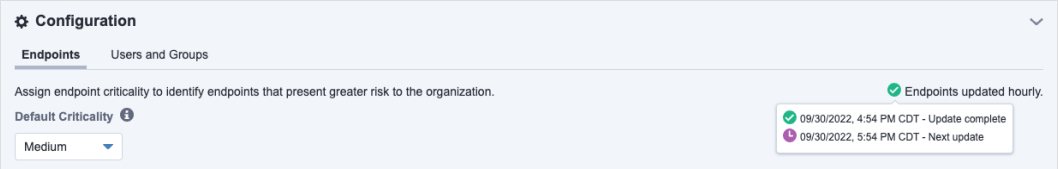
You can export the table to a CSV file that contains the data for each entry in the table, including column headings. To export a table, click Export in the **View Endpoints** table heading.

View status of endpoint updates

Each hour, Criticality updates the **Endpoint Criticality** sensor with any criticality changes (which you made to default level, rules, or priority), and then Tanium uses the results of this sensor to update impacted endpoints.

© 2025 Tanium Inc. All Rights Reserved

To view the status of endpoint updates, hover over the icon next to **Endpoints updated hourly** in the **Configuration > Endpoints** section. You can view the in-progress and planned update dates and times.



© 2025 Tanium Inc. All Rights Reserved

Assigning user and group criticality

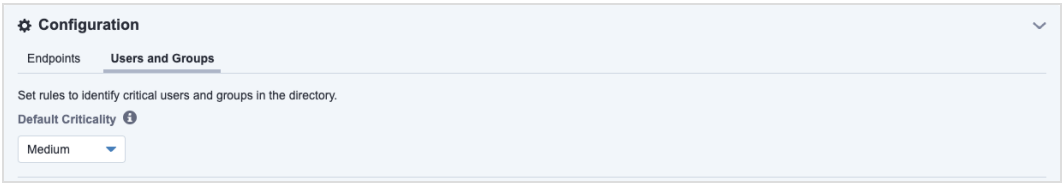
Manage the criticality level of users and groups by assigning a default criticality level to apply to all users and groups or by creating rules to override the default for specified users or groups.

For information on how often endpoints and reports are updated with criticality levels, see Configure user and group synchronization settings on page 18.

Assign default user and group criticality

Assign a default criticality level to apply to all users and groups not targeted by a rule. By default, the criticality level is **Medium**.

1. From the Main menu, go to **Shared Services > Criticality**.
2. Go to **Configuration > Users and Groups** and select the **Default Criticality** level.



Create rules to assign criticality to specific users or groups

To specify different criticality levels for different groups of users or groups, create rules. You can create rules only for users and groups that belong to domains that are configured in Directory Query.

1. From the Main menu, go to **Shared Services > Criticality**.
2. Go to the **Configuration > Users and Groups > Rules** section.
3. Click **Create Rule** and enter the rule name.
4. Select the type: **User** or **Group**.
5. Select the criticality level and priority number for the rule.
   If you select 1, for example, rule 1 is prioritized over rule 2. You can also set the priority after creating the rule. See Prioritize criticality rules on page 32.
6. Use one of the following options to specify the users or groups to include in the rule.
   - **Rule Builder**: Specify the criteria to filter on all users or groups. For example, if you are creating a user type rule, you can select **Name** and **starts with**, and then enter `John` to target all users whose name starts with John. The rule is applied to all users that meet the criteria. Individual users cannot be selected. Add rows or groupings to specify additional filter conditions.

© 2025 Tanium Inc. All Rights Reserved

- **Manual Names**: Enter the user or group names. Use separate lines for multiple entries. To specify users, enter the name as `DOMAIN\user1` or `user1@domain`. To specify groups, enter the name as `DOMAIN\group1` or `group1@domain`.
- **Names by CSV File**: Upload a CSV file. The CSV file must contain each user or group name on its own line without additional information, similar to the following example:

```
DOMAIN\someone
someone@domain.com
```

> **NOTE** Rules that apply to groups also apply to users and groups that are direct members of any groups that match the rule.

7. Click **Create Rule**.

Work with existing criticality rules

If you import Criticality with the **Tanium Recommended Installation**, the **Default Critical Active Directory Groups** rule is automatically created. This rule assigns a **Critical** level to the following groups and any groups or users in these groups:

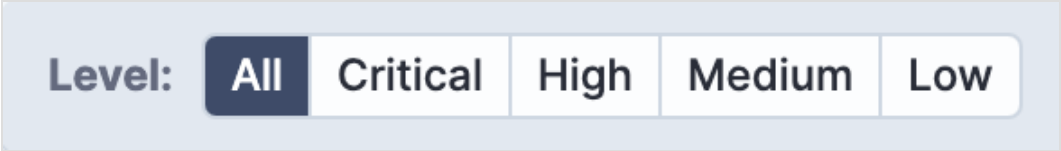
- Account Operators
- Administrators
- Backup Operators
- Cryptographic Operators
- Distributed COM Users
- Domain Admins
- Enterprise Admins
- Group Policy Creator Owners
- Print Operators
- Read-only Domain Controllers
- Schema Admins
- Server Operators

> **NOTE** If you imported Criticality with the **Tanium Recommended Installation**, you cannot edit, delete, or otherwise modify the **Default Critical Active Directory Groups** rule.

© 2025 Tanium Inc. All Rights Reserved

View user and group criticality rules

1. From the Main menu, go to **Shared Services > Criticality**.
2. Go to the **Configuration > Users and Groups > Rules** section.
3. View the rules. The table contains the following columns:
    - **Priority**: Numerical value indicating rule importance or **None** if no priority is set
    - **Rule**: Name of the rule
    - **Rule Type**: **User** or **Group** depending on the type of the rule
    - **Criticality**: Criticality level of the rule
    - **Rule Details**: Details of the rule depending on how the rule was created
    - **Groups**: Number of groups targeted by the rule
    - **Users**: Number of users targeted by the rule
    - **Actions**: Edit, delete, or other actions you can make on the rule depending on the rule details
4. To filter the rules based on criticality levels, click the corresponding toggle.



Prioritize criticality rules

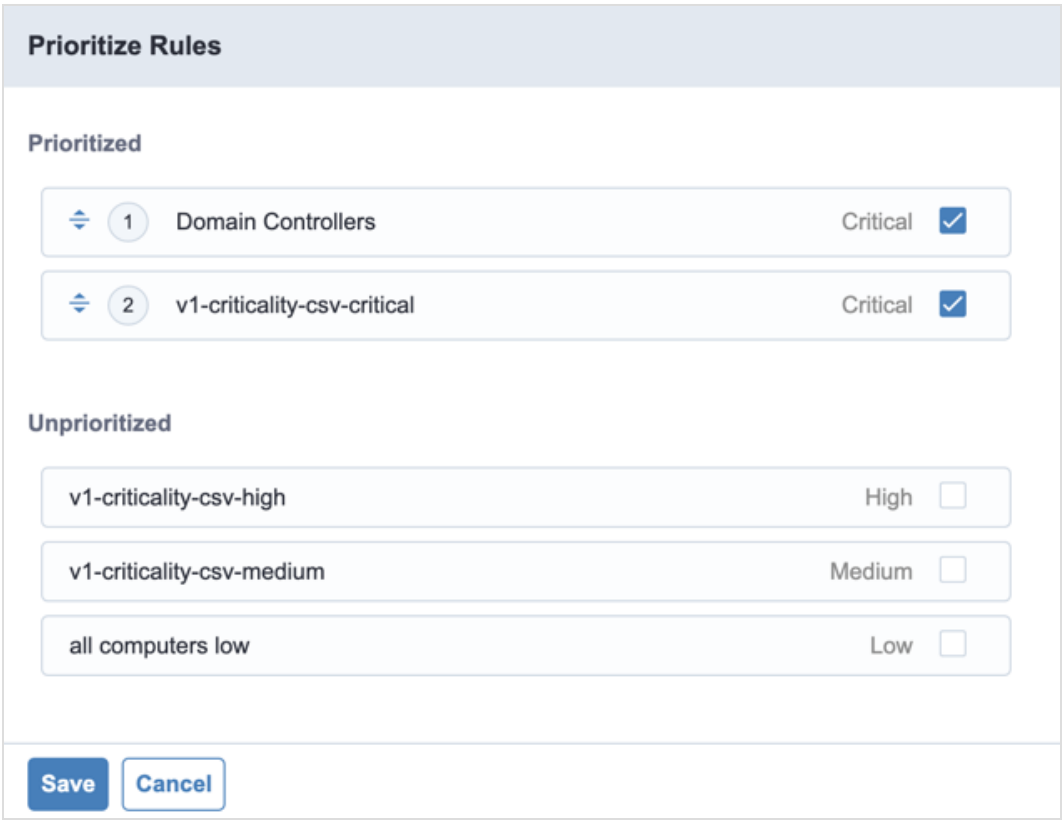
You can prioritize rules to specify which rule takes precedence if a user or group is assigned to more than one rule.

BEST PRACTICE

Consider limiting the number of rules you prioritize to simplify criticality level management.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services > Criticality**.
2. Go to the **Configuration > Users and Groups > Rules** section.
3. Click **Prioritize**.



   a. For existing prioritized rules, drag and drop the rules into the order you want, or use the arrows to specify the position.
   b. To prioritize an unprioritized rule, select the box next to the rule and then assign priority.
   c. To remove a priority, clear the box next to the rule.
   d. Click **Save**.

Manage rules

Edit or delete a rule using the options available in the **Actions** column in the **Rules** table.

You can also select a rule and click Edit or Delete. Depending on how a user or group rule was created, you can take additional actions on the rule:

- **Manual Names**: Select the rule and click Copy or select **Copy Names** from the **Actions** column.
- **Names by CSV File**: Select the rule and click Download or select **Download CSV** from the **Actions** column.

© 2025 Tanium Inc. All Rights Reserved

NOTE

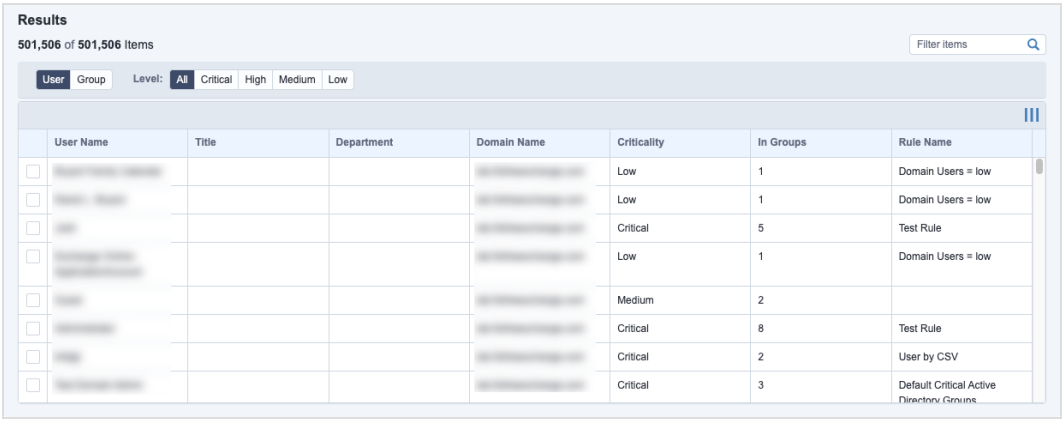
If you imported Criticality with the **Tanium Recommended Installation**, you cannot edit, delete, or otherwise modify the **Default Critical Active Directory Groups** rule.

Work with users and groups

View users

View all users managed by Tanium, along with the corresponding criticality levels.

1. From the Main menu, go to **Shared Services > Criticality**.
2. Go to the **Configuration > Users and Groups > Rules** section.
3. To view the users, click **User**. The table contains the following columns:



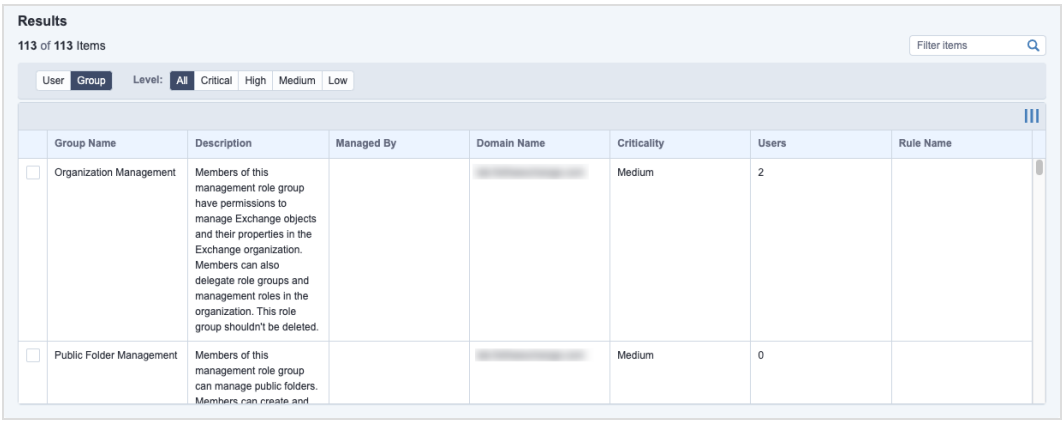
   - **User Name**: Name of the user
   - **Title**: Title of the user
   - **Department**: Department of the user
   - **Domain Name**: Domain of the user
   - **Criticality**: Criticality level assigned by default or a rule
   - **In Groups**: Number of groups in which the user belongs
   - **Rule Name**: Rule assigned to the endpoint
     The column is blank if a rule is not assigned to the user. (The user is assigned the default criticality level.)
4. If necessary, filter the items by searching the table.

View groups

View all users managed by Tanium, along with the corresponding criticality levels.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services > Criticality**.
2. Go to the **Configuration > Users and Groups > Rules** section.
3. To view the groups, click **Group**. The table contains the following columns:

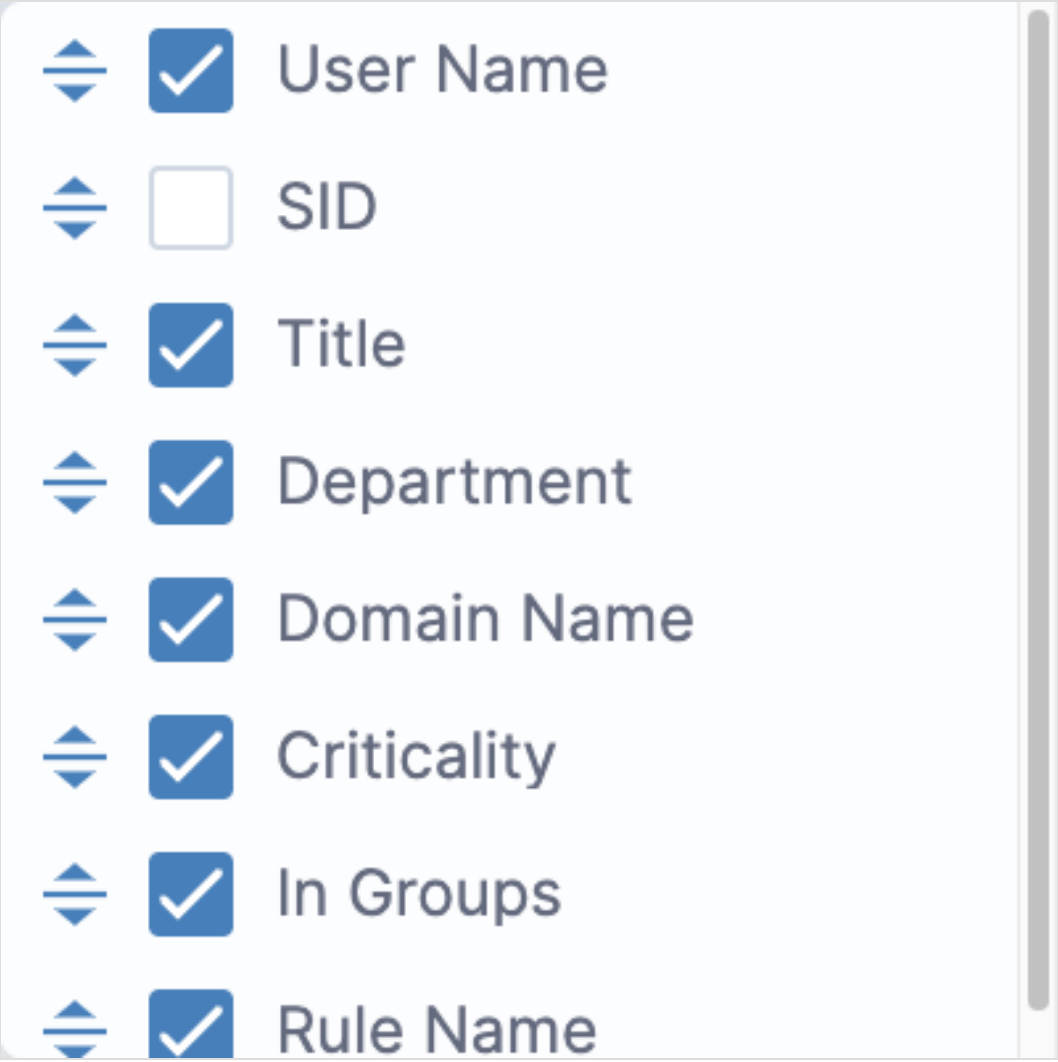


   - **Group Name**: Name of the group
   - **Description**: Description of the group
   - **Managed By**: Management of the group
   - **Domain Name**: Domain of the group
   - **Criticality**: Criticality level assigned by default or a rule
   - **Users**: Number of users in the group
   - **Rule Name**: Rule assigned to the group
     The column is blank if a rule is not assigned to the user. (The user is assigned the default criticality level.)
4. If necessary, filter the items by searching the table.

© 2025 Tanium Inc. All Rights Reserved

Customize columns

You can change which columns are displayed in the table, and adjust the order of the columns.



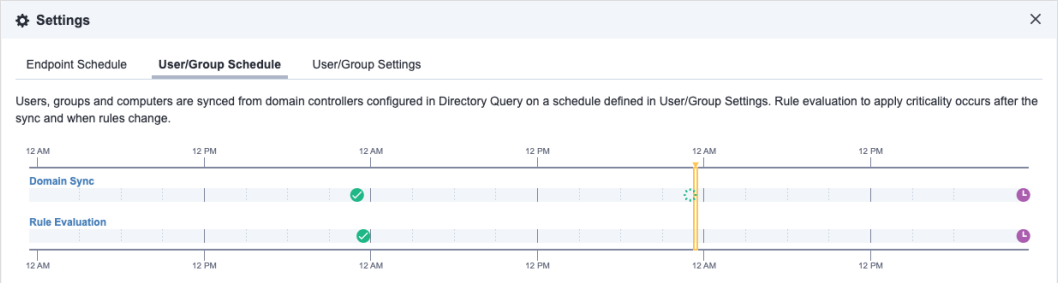
1. In the report, click Customize Columns.
2. To remove a column, clear the box for the column.
3. To adjust the column order, click and drag the column names.

View status of user and group updates

Users, groups, and computers are synchronized from domain controllers that are configured in Tanium Directory Query on a schedule that is defined in **User/Group Settings** tab in the Criticality Settings. Rule evaluation to apply the criticality occurs after the domain sync, when rules change, or when you manually request a sync from the **User/Group Schedule** tab in the Criticality Settings. For more information, see Tanium Directory Query User Guide: Managing connections to directory servers and Configure user and group synchronization settings on page 18.

© 2025 Tanium Inc. All Rights Reserved

To view the status of user and group updates, go to Criticality Settings and click **User/Group Schedule**. You can view the in-progress and planned update dates and times.



© 2025 Tanium Inc. All Rights Reserved

Troubleshooting Criticality

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

Collect logs

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

To download logs:

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

   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 39.

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

Troubleshoot endpoint criticality

If a Tanium Client managed endpoint has an unexpected criticality level or an unexpected Tanium risk score based on criticality level, consider the following resolutions:

- In the **View Endpoints** table, identify the rule assigned to the endpoint in the **Endpoint Rule Name** column. If the column is blank, the endpoint does not have a rule assigned to it and is assigned the default criticality level.
- If the assigned rule has an Error status in the **Rules** section, expand the rule to view the error. If the error lists a computer group name, verify that the computer group exists and that the endpoint is correctly assigned to that computer group.
- If you want the endpoint to be assigned to a different rule, edit the desired rule or its rule priority in the **Rules** section.
- Confirm that your environment has the required Criticality dependencies. For more information, see Solution

© 2025 Tanium Inc. All Rights Reserved

dependencies on page 11.

- Confirm that the endpoint status is healthy. For more information, see Tanium Client Management User Guide: Troubleshooting Tanium Clients and Client Management.

Troubleshoot user and group criticality

If a user or group has an unexpected criticality level, consider the following resolutions:

- In the **Results** table, identify the rule assigned to the user or group in the **Rule Name** column. If the column is blank, the user or group does not have a rule assigned to it and is assigned the default criticality level.
- If you want the user or group to be assigned to a different rule, edit the desired rule or its rule priority in the **Rules** section.
- Confirm that your environment has the required Criticality dependencies. For more information, see Solution dependencies on page 11.

Uninstall Criticality

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

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

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

© 2025 Tanium Inc. All Rights Reserved