Integrating Tanium™ with Chronicle

September 15, 2021

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

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

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

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

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

Tanium is committed to the highest accessibility standards to make interaction with Tanium software more intuitive and to accelerate the time to success. To ensure high accessibility standards, Tanium complies with the U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. We have conducted third-party accessibility assessments over the course of product development for many years, and most recently a comprehensive audit against the WCAG 2.1 / VPAT2.3 standards for all major product modules was completed in September 2019. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

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

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

Table of Contents

Introduction

Tanium provides a unified endpoint management and security platform that offers customers transformational scale, speed and reliability. From more efficient workflows between teams to eliminating gaps created by standalone solutions, Tanium helps simplify infrastructure in the most demanding IT environments.

Integrate Tanium with the Chronicle security analytics platform to help identify, investigate, and remediate sophisticated, long-lived attacks. Tanium™ Threat Response monitors activity in real time and generates alerts when potential malicious behavior is detected and continuously records key system activity for forensic and historical analysis. You can use the out-of-the-box Chronicle integration in Tanium to send all endpoint telemetry from Threat Response to Chronicle, which enables you to store and analyze up to a year of telemetry data. You can also use Tanium™ Connect to send additional data for a longer history available for analysis, including alerts for intel matches from Threat Response, data from saved questions, events, and native connection sources from other Tanium modules.

Requirements for integration

- Tanium™ Core Platform 7.3 or later
- Tanium Connect 4.12 or later (For more information, see Tanium Connect User Guide.)
- Tanium Threat Response 3.1 or later (For more information, see Tanium Threat Response User Guide.)
- (Optional) Other Tanium modules necessary for specific data that you want to send to Chronicle (Latest available version. Additional modules may require new licensing.)
- A Chronicle instance with a forwarder configured for Tanium data types, and a REST ingestion token

Chronicle forwarder setup

Review the Chronicle forwarder installation documentation within your Chronicle instance. During the setup process for the forwarder, complete the following basic steps:

1. Create a host system and install Docker.
2. Use the two configuration files provided during the provisioning process to install and configure the forwarder container. Add the Tanium data types you are using to the forwarder configuration file using the following examples, filling in the appropriate IP addresses (or host names).

> **Tip:** Take care when editing the configuration file and use a text editor such as VI that shows line endings. Copying an existing data_type modifying according to the following instructions is an option.

Data Type	Configuration example

Threat Response	`- syslog:`
	`common:`
	`enabled: true`
	`data_type: TANIUM_THREAT_RESPONSE`
	`data_hint:`
	`batch_n_seconds: 10`
	`batch_n_bytes: 1048576`
	`tcp_address: 0.0.0.0:10523`

	udp_address: *0.0.0.0*:10523 connection_timeout_sec: 60
Discover	- syslog: common: enabled: true data_type: TANIUM_DISCOVER data_hint: batch_n_seconds: 10 batch_n_bytes: 1048576 tcp_address: *0.0.0.0*:10524 udp_address: *0.0.0.0*:10524 connection_timeout_sec: 60
Comply	- syslog: common: enabled: true data_type: TANIUM_COMPLY data_hint: batch_n_seconds: 10 batch_n_bytes: 1048576 tcp_address: *0.0.0.0*:10525 udp_address: *0.0.0.0*:10525 connection_timeout_sec: 60
Asset	- syslog: common: enabled: true data_type: TANIUM_ASSET data_hint: batch_n_seconds: 10 batch_n_bytes: 1048576 tcp_address: *0.0.0.0*:10526 udp_address: *0.0.0.0*:10526 connection_timeout_sec: 60
Patch	- syslog: common: enabled: true data_type: TANIUM_PATCH data_hint: batch_n_seconds: 10 batch_n_bytes: 1048576 tcp_address: *0.0.0.0*:10527 udp_address: *0.0.0.0*:10527 connection_timeout_sec: 60 tcp_buffer_size: 192000
Reveal	- syslog: common: enabled: true data_type: TANIUM_REVEAL data_hint:

	batch_n_seconds: 10 batch_n_bytes: 1048576 tcp_address: *0.0.0.0*:10528 udp_address: *0.0.0.0*:10528 connection_timeout_sec: 60

3. Restart the forwarder container using the following command on the forwarder host system:
`sudo docker restart cfps`

4. Verify the forwarder configuration using the following command on the forwarder host system:
`docker logs cfps`

> **Tip:** If the forwarder is configured correctly, the following messages are returned:
>
> I0804 02:26:56.789558 333 syslog.go:227] Starting to listen for TCP syslog on 0.0.0.0:PORT
> I0804 02:26:56.792929 333 syslog.go:310] Starting to listen for UDP syslog on 0.0.0.0:PORT
> I0804 02:31:37.376903 333 syslog.go:359] Accepting new syslog TCP connection.

When you first configure the Chronicle destination in Connect, you use the host name or IP address and the port that you configured for the forwarder container. For more information, see Configure the connection destination for Chronicle.

Enabling integration in Tanium

The Tanium integration with Chronicle uses stream in Threat Response to provide raw endpoint telemetry to Chronicle. You can also use Connect to send Threat Response alerts, data from saved questions, events, and native sources from other modules.

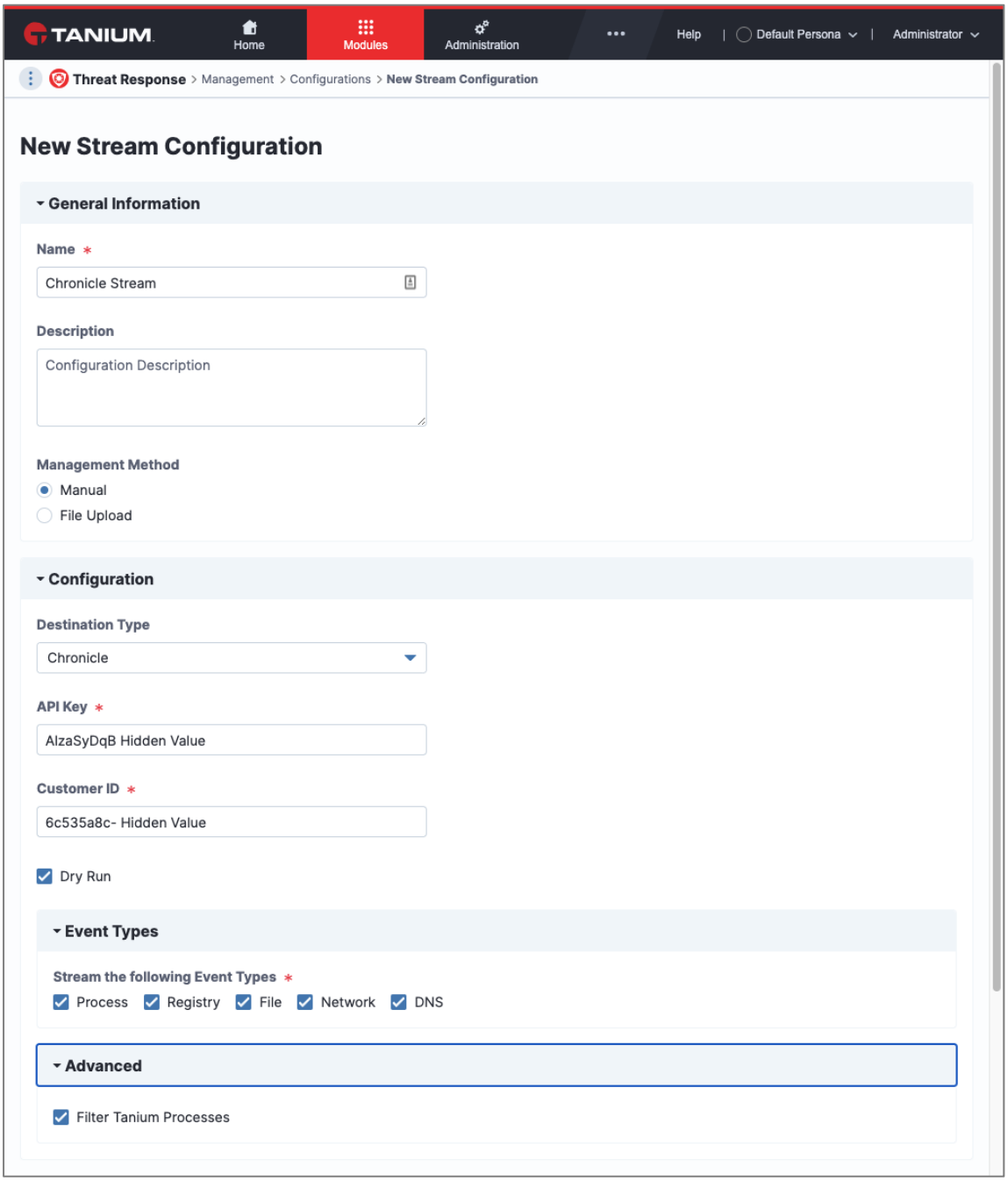
Enable streaming from Threat Response

1. Sign in to the Tanium Console using an account that has administrator privileges.
2. From the Main menu, go to **Modules > Threat Response**.
3. From the Threat Response menu, go to **Management > Configurations**, and click **Create > Stream**. Enter a **Name** and **Description** for the stream configuration.
4. In the **Configuration** section, configure the settings for your Chronicle environment.
    - Select **Chronicle** for the **Destination Type**.
    - For **API Key**, enter your Chronicle ingestion token (typically provided by Tanium Order Operations).
    - Enter the Chronicle **Customer ID** for your environment (typically provided by Tanium Order Operations).

    Select **Dry Run** if you want to collect statistics about the data that would be streamed to the destination, but not actually send data.

> **Best Practice:** By default, Dry Run is enabled when you create a stream configuration. Analyze the amount of event data that would be streamed to a destination before you clear the Dry Run check box. While this setting is enabled, no data is streamed to a destination; it must be disabled for data streaming to occur.

You can use the `Threat Response - Daily Stream Stats` sensor to determine the amount of data to be sent.



5. In the **Event Types** subsection, select the event types that you want to stream.
6. In the **Advanced** subsection, select **Filter Tanium Processes** to filter all Tanium Client processes, and all child processes of the Tanium Client in the recorded events. For example, if the Tanium Client starts Python to run a sensor, this is filtered from the recorded events.
7. In the **Filters** section, click **Manage Filters** to add filters to use in the stream configuration. For more information, see Tanium Threat Response User Guide: Creating filters.

> **Tip:** Contact Tanium Support for specific filters for Chronicle.

8. Click **Save**.
9. From the Threat Response menu, go to **Management > Profiles.** Create or modify a profile to apply the stream configuration you created to one or more appropriate computer groups, and deploy the profile. For more information, see Tanium Threat Response User Guide: Creating profiles.
10. (Optional) If you selected **Dry Run**, review results for the question: `Get Threat Response - Daily Stream Stats from all machines`. After you have tuned the stream configuration as necessary, clear the **Dry Run** check box, save the configuration, and redeploy the profile to enable streaming.

Configure connections

Export additional data to Chronicle using Connect. The connection sources used in Connect include saved questions, events, and native sources from other modules. For the specific connection sources, see Reference: Connection sources.

Configure connections using saved questions

For saved question connection sources, prepare saved questions with the specific names used in the Chronicle configuration, and then configure the connection in Connect. You might need to work with your Tanium Account Manager to help define these data types for Chronicle data onboarding.

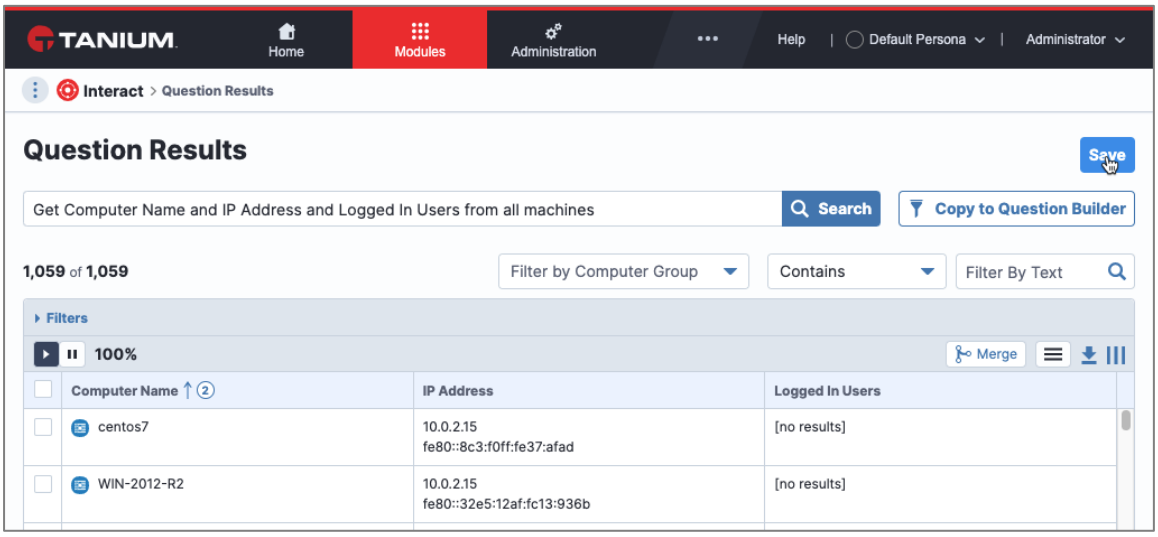
PREPARE SAVED QUESTIONS

Create a saved question for each context you want to use in Chronicle.

1. From the Main menu, go to **Modules > Interact**.
2. Ask a question (or copy a saved question) that matches a listing in Reference: Connection sources. For more information about asking questions and managing saved questions, see Tanium Interact User Guide.

> **Note:** Make sure to remove extra characters or smart quotes that might be copied from another location.

3. Click **Save.**

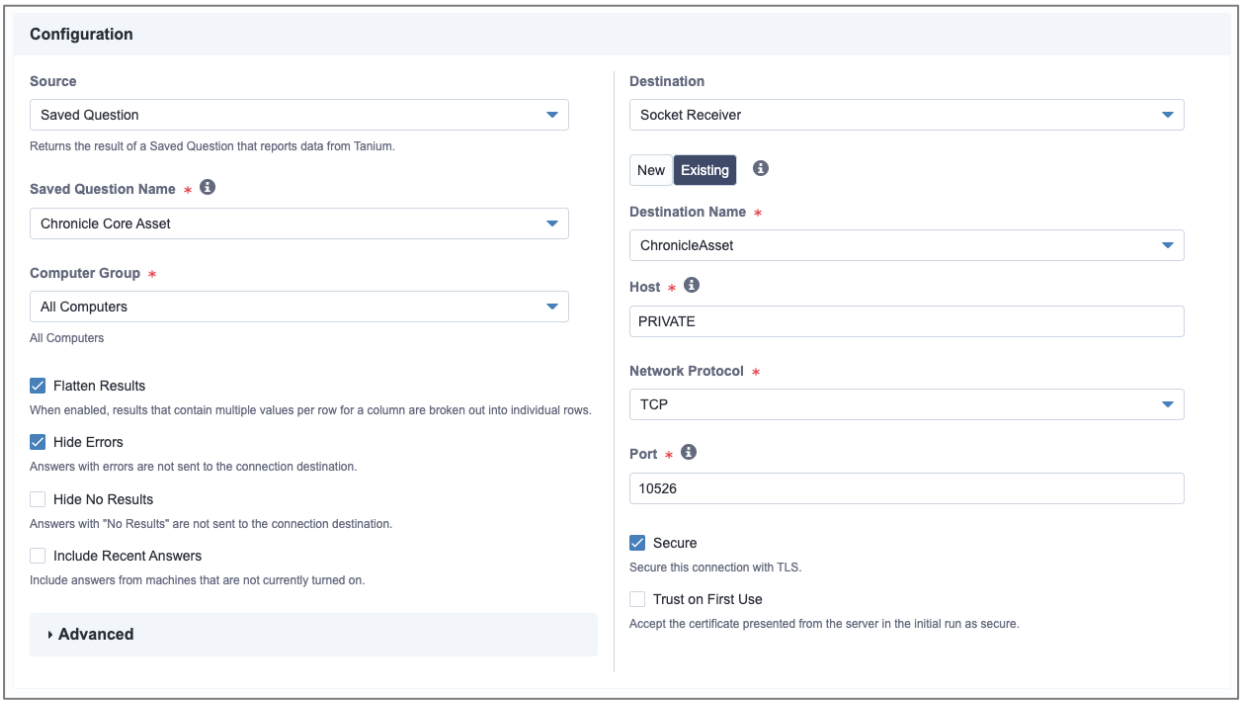


4. Name the saved question to match the listing in Reference: Connection sources. If you use a different name, you must also edit the Chronicle configuration to retrieve the data from this question.
5. Make sure that **Reissue this question every** is not selected (unless you are otherwise directed in Reference: Connection sources). Tanium Connect manages the scheduling and execution of the question.
6. Click **Create Saved Question**.

CONFIGURE CONNECT TO EXPORT DATA FROM SAVED QUESTIONS

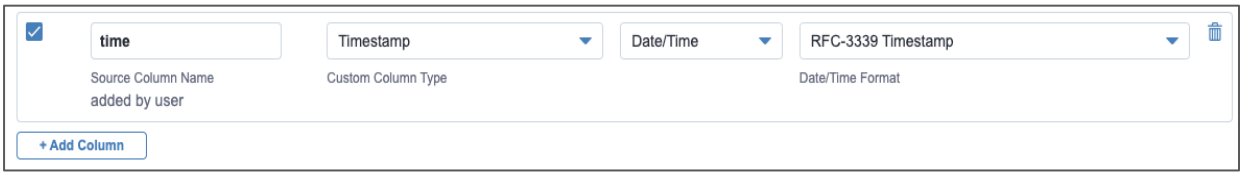
Configure Connect to execute saved questions and export the resulting data to Chronicle.

1. From the Main menu, go to **Modules > Connect**.
2. Click **Create Connection**.
3. For **Name**, enter the name of the saved question you created.
4. In the **Source** section, click **Saved Question** and select the saved question you created.
5. For **Destination**, select **Socket Receiver**.
6. Click **Existing** and select the **Destination Name** for your Chronicle destination, or click **New** and create one if you have not yet done so.
7. (For a new destination) Enter the **Host** and **Port** that you configured for the data type in the Chronicle forwarder.

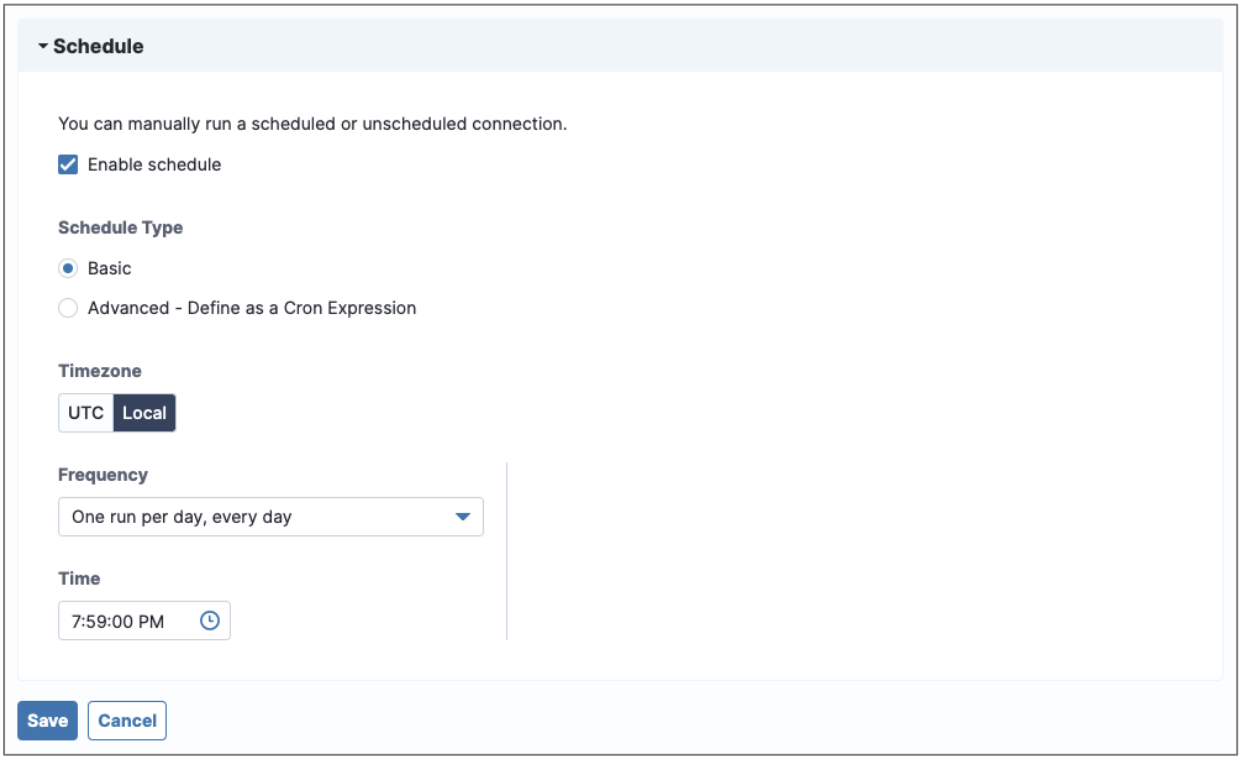


8. Expand the **Configure Output** section. For **Format**, select **JSON**.
9. Expand the **Columns** subsection, and click **Add Column**. Configure the new column as follows:
   - **Source Column Name:** `time`
   - **Custom Column Type: Timestamp** and **Date/Time**

- **Date/Time Format: RFC-3339 Timestamp**



10. Expand the **Schedule** section, and configure the times when Connect should send this saved question to the endpoints and return collected data to Chronicle. For example, security questions might be asked every 1 to 4 hours, and operational questions might be asked every 4 to 24 hours. Work with your Chronicle administrator and Tanium Support to configure and tune these values appropriately for your environment.



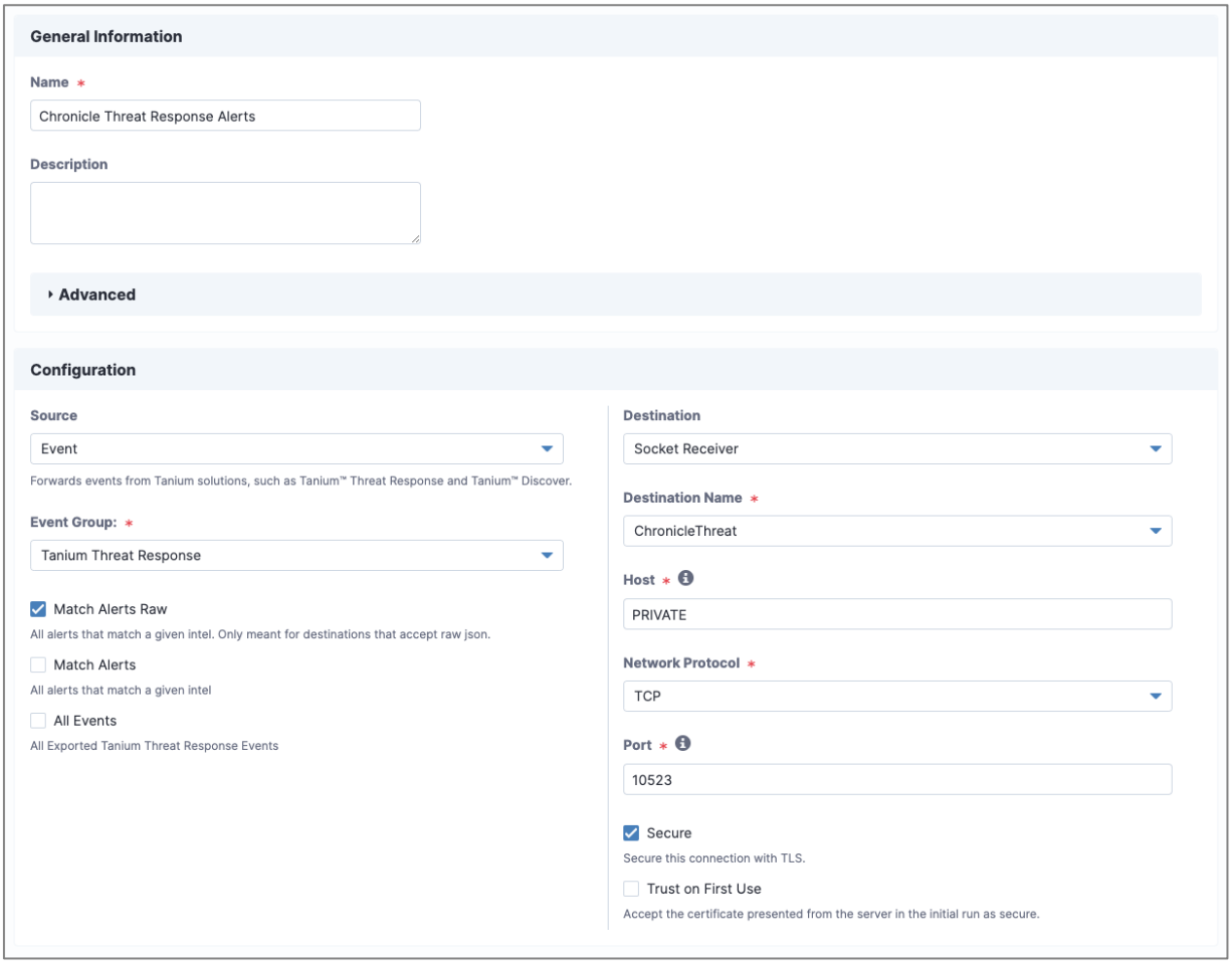
11. Click **Save**. To test the data connection, click **Run Now**.

Configure a connection for Threat Response alerts

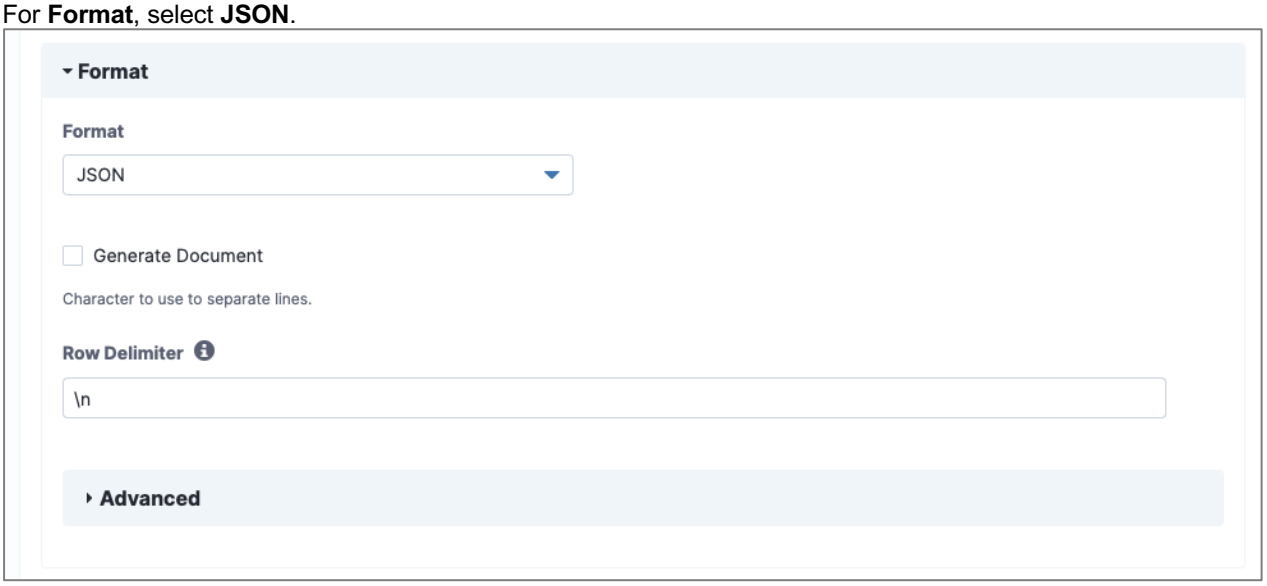
Configure Connect to send events from Threat Response to Chronicle.

1. From the Main menu, go to **Modules > Connect**.
2. Click Create Connection.
3. For **Name**, enter Tanium Threat Response Alerts.
4. For **Source**, select **Event**, and for **Event Group**, select **Tanium Threat Response**. Select only the **Match Alerts Raw** option.
5. For **Destination**, select **Socket Receiver**.
6. Click **Existing** and select the **Destination Name** for your Chronicle destination, or click **New** and create one if you have not yet done so.

7. (For a new destination) Enter the **Host** you configured for the Chronicle forwarder, enter `10523` for the **Port**, and select the **Network Protocol** you configured.



8. For **Format**, select **JSON**.



9. Click **Save**.

Note: Event connections cannot be scheduled, and the **Run Now** button is disabled. Alert events must be generated by Threat Response to pass through the Connection.

Important: Do not use filters with this connection. Filters can interfere with the Match Details field in the results.

Configure connections for native sources from other modules

To configure connections using other modules as sources, see the connection settings and any additional instructions for the specific source in Reference: Connection sources. For general information about configuring connections, including using the listed settings for native sources from other modules, see Tanium Connect User Guide: Configuring SIEM destinations.

Verify Data in Chronicle

After you complete the configuration, verify that logs are sent by Tanium and processed by Chronicle by running the following command on the Chronicle forwarder host:

```
docker logs cfps
```

If the integration is configured correctly, the log includes a statement noting a successful upload of the data type `TANIUM_EDR` for Threat Response alerts or `TANIUM_QUESTION` for saved questions.

The following example shows log messages for successful uploads—first for Threat Response alerts, followed by saved questions for Asset.

```
I0813 03:28:44.163290     333 syslog.go:359] Accepting new syslog TCP connection.
I0813 03:28:47.861668     333 uploader.go:213] Batch (2, TANIUM_THREAT_RESPONSE) successfully uploaded.
I0813 03:31:29.402796     333 syslog.go:359] Accepting new syslog TCP connection.
I0813 03:31:37.852677     333 uploader.go:213] Batch (4, TANIUM_ASSET) successfully uploaded.
```

Reference: Connection sources

When you export data to Chronicle using Connect, you can use saved questions, events, and native sources from other modules as connection sources.

The connection sources in this section are grouped into the dashboards available in Chronicle, organized according to functionality and relevant modules.

Configuring connections

For general information about configuring connections, including using the listed settings for native sources from other modules, see Tanium Connect User Guide: Configuring SIEM destinations. Some native sources list additional specific instructions.

For more information about creating connections using the listed saved questions, see Configure connections using saved questions.

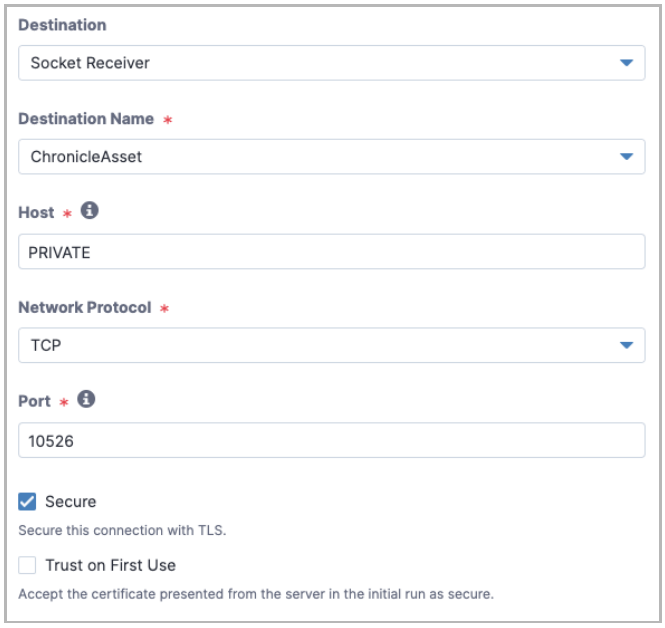
For information about creating connections for events from Threat Response, see Configure connections for Threat Response alerts.

Name each saved question and corresponding connection to match the listing in this guide. If you use a different name for a saved question, you must also edit the Chronicle configuration to retrieve the data from this question.

Configure the Chronicle connection destination for each data type

When creating a connection for any of the sources listed in this section, follow these steps to configure a destination that is associated with the data type for the source.

1. For **Destination**, select **Socket Receiver**.
2. Click **Existing** and select the **Destination Name** for your Chronicle destination, or click **New** and create one if you have not yet done so.
3. (For a new destination) Enter a **Destination Name** that can be associated with the data type (such as `ChronicleAsset` or `ChronicleDiscover`) Enter the **Host** and **Port** that you configured for the Chronicle forwarder.



Tanium Core Asset

The saved questions and connection sources for **Tanium Core Asset** use default functionality within Tanium Core Platform to send asset related information from the endpoint, including manufacturer, and last logged-in user to track an asset within an environment.

Tanium Core Asset saved question connection source

Question name	Saved question
Chronicle Basic Asset	`Get Computer Name and Last Logged In User and Last Reboot and Operating System and IP Address and MAC Address and Chassis Type and Manufacturer and Computer Serial Number from all machines`

Tanium Discover

The connection source for **Tanium Discover** uses functionality from Tanium Core Platform and Tanium™ Discover to send asset and interface related information. Events include Lost, New Unmanaged, and New Managed Interfaces, as well as system data such as device type, open ports, and operating system.

Tanium Discover native connection source

Source	Connection details
Chronicle Discover Reports	**Name:** `Chronicle Discover Reports` **Source: Tanium Discover** **Report: Unmanaged**

Tanium Patch

The saved question for **Tanium Patch** uses Tanium™ Patch to monitor for patch applicability and reboot status for Windows and Linux. This data can be used to identify OS patches that are not installed, and the data can be enriched by Tanium Asset.

Tanium Patch saved question connection source

Question name	Saved question
Chronicle Patch List Applicability	`Get Computer Name and Last Reboot and Operating System and Last Logged In User and Patch - Patch List Applicability from all machines`

Tanium Comply

The connection source for **Tanium Comply** uses vulnerability and configuration reports to help monitor import metrics. Tanium™ Comply enables operating system-level configuration checks and vulnerability scanning at scale using the Tanium architecture.

Tanium Comply native connection sources

Source	Connection details
Chronicle Comply Module *REPORT_NAME* Example: `Chronicle Comply Module Linux`	**Name:** `Chronicle Vulnerability` **Source: Tanium Comply (Assessments)** **Assessment Type: Vulnerability** **Assessment Name**: The vulnerability assessment to send **Include Endpoint findings:** selected

Tanium Reveal

The saved question for **Tanium Reveal** uses Tanium™ Reveal to monitor sensitive data on endpoints. This data can be used to assist with regulatory compliance and help identify sensitive data leakage or security violations.

Tanium Reveal saved question connection source

Question name	Saved question
Chronicle Reveal	`Get Reveal - Background Scan Results[*] and Reveal - Endpoints with Confirmed Sensitive Data and Reveal - Endpoints with Unconfirmed Sensitive Data and Reveal - Label Results and Computer Name and Computer ID from all machines with (Reveal - Endpoints with Confirmed Sensitive Data contains Yes or Reveal - Endpoints with Unconfirmed Sensitive Data contains Yes)`

Tanium Threat Response

The connection source for **Tanium Threat Response** sends alerts from intel matches in Threat Response to help identify malicious software and attacks.

To configure Threat Response Alerts, see Configure connections for Threat Response alerts.

Tanium Threat Response alerts connection source

Source	Connection details
Chronicle Threat Response Alerts	See Configure connections for Threat Response alerts.