Tanium (on-prem) getting started guide

Version 1.0

September 22, 2020

What's in this guide?

Howdy! In this guide, you'll find instructions on how to:

1. Enable and configure console access for the Expel SOC; and
2. Configure the technology in Expel Workbench™

Step 1 — Enable console access

Having read-only access to the interface of your technology allows Expel to dig deeper when performing incident investigations. Our device health team uses this access to investigate potential health issues with your tech.

When you create a Tanium user configuration, by default it has no computer management groups, alternative personas, user groups, or roles until you assign them. A user with no roles can log into the Tanium Console but cannot access anything. Do not create configurations for user accounts that you import from an LDAP server. https://docs.tanium.com/platform_user/platform_user/console_users.html#Create, https://docs.tanium.com/platform_user/platform_user/console_users.html#Assign_roles

We utilize the following Tanium API routes for our integration:

Route	Permission
/api/v2/session/login	Interact:Login
/api/v2/sensors/by-name	Interact:Read Sensor
/api/v2/parse_question	Interact:Ask Dynamic Questions
/api/v2/questions	Interact:Ask Dynamic Questions
/api/v2/result_data/question/	Interact:Ask Dynamic Questions
/plugin/products/detect3/api/v1/alerts	Threat Response: Detect Alert Read
/plugin/products/detect3/api/v1/intels	Threat Response: Detect Intel Read
/plugin/products/detect3/api/v1/sources	Threat Response: Detect Source Read
/plugin/products/detect3/api/v1/intels/<intel id>/labels	Threat Response: Detect Label Read

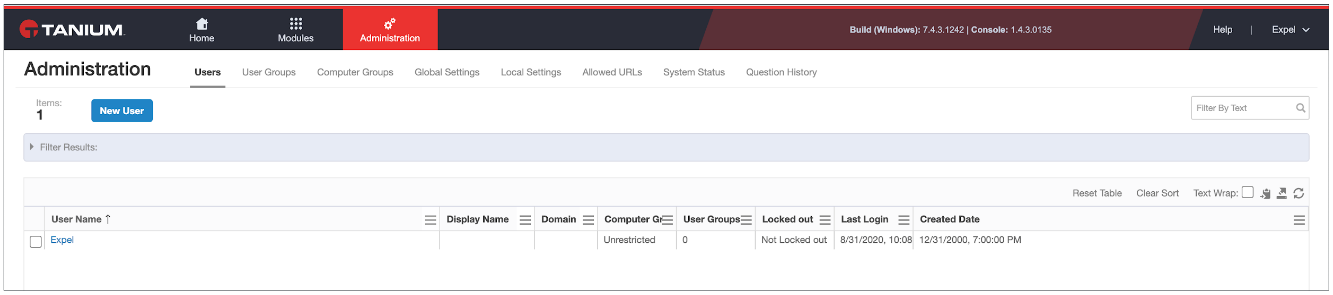
The **Interact Basic User** role will grant us all the necessary permissions we need to access the question/sensor APIs and Interact console. https://docs.tanium.com/interact/interact/requirements.html#table_Interact_module_roles

The **Threat Response Read Only User** role will grant us all the necessary permissions we need to access the alerts APIs and Threat Response console https://docs.tanium.com/threat_response/threat_response/requirements.html#user_roles. If you are using a custom role we will also need **"Detect Use API"** permission as well as the necessary permissions to make Threat Response available in console.

The Tanium client uses a username/password combination to create an authenticated session, the returned session token is set on the session header for all subsequent requests.

A. From the Main menu, select **Administration** > **Management** > **Users**

B. Click **New User** (Figure 1)



Administration

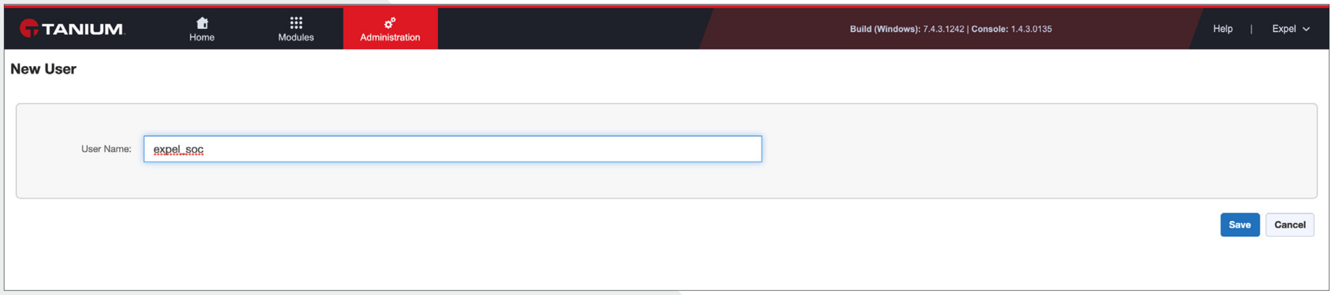
Items: 1

	User Name ↑	Display Name	Domain	Computer Gr	User Groups	Locked out	Last Login	Created Date
□	Expel			Unrestricted	0	Not Locked out	8/31/2020, 10:08	12/31/2000, 7:00:00 PM

Figure 1

C. Specify a user name that matches one of the following:

- A user account that is defined locally on the Tanium Server
- A user account that is defined in your IdP
- (Windows only) An AD account name. Specify just the user name, not the domain name. The Tanium Server uses Windows Authentication, and does not store or manage login credentials for the user (Figure 2)



New User

User Name: expel_soc

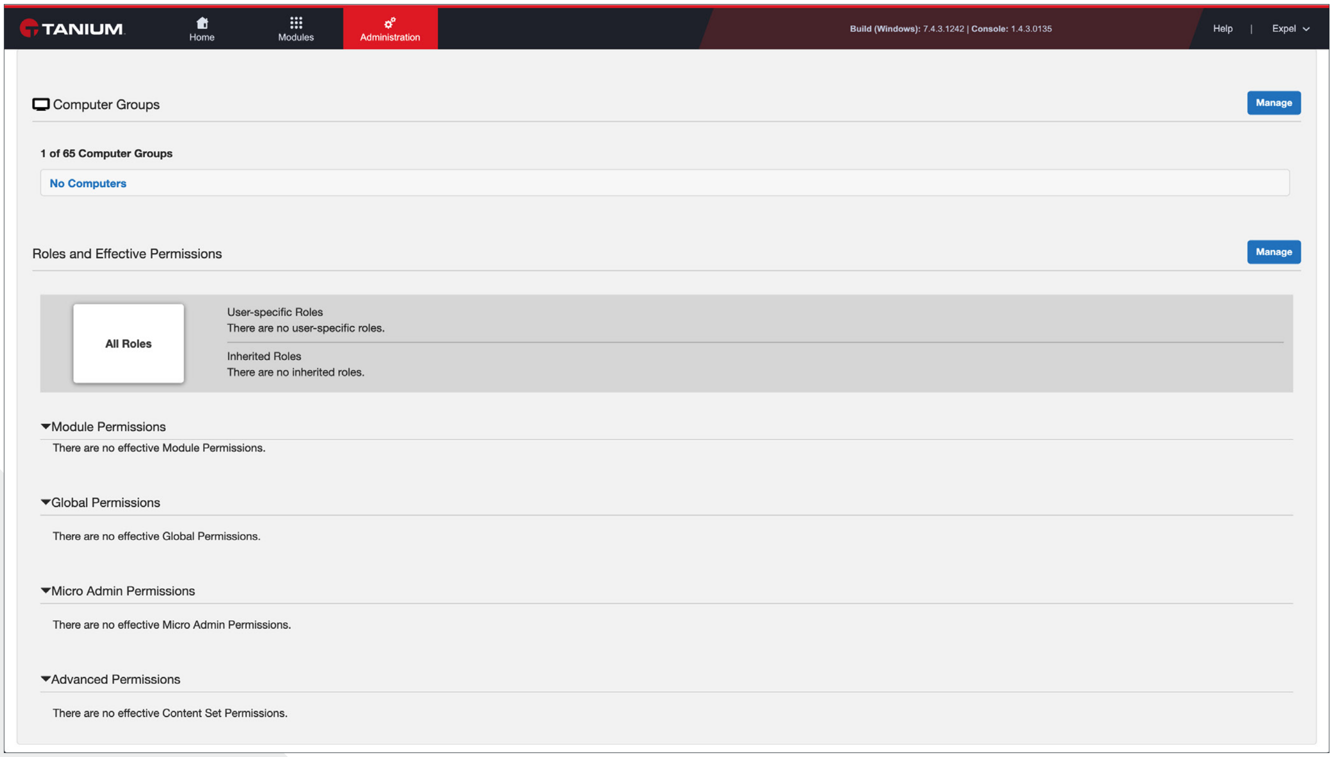
Figure 2

D. Save the configuration and get ready to assign roles to a user

E. From the Main menu, select **Administration** > **Management** > **Users**

F. Click the **User Name** of the user configuration that you want to edit

G. In the **Roles and Effective Permissions** section, click **Manage** (Figure 3)



Computer Groups Manage

1 of 65 Computer Groups

No Computers

Roles and Effective Permissions Manage

All Roles

User-specific Roles
There are no user-specific roles.

Inherited Roles
There are no inherited roles.

Module Permissions
There are no effective Module Permissions.

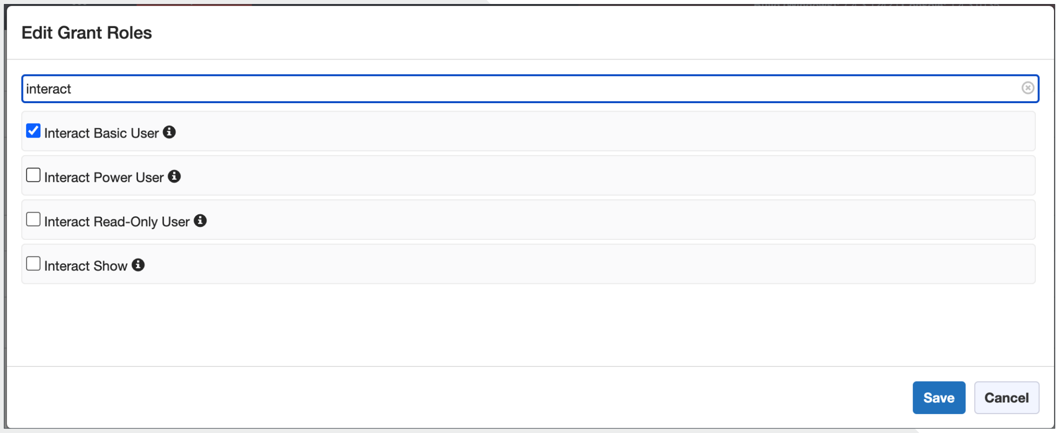
Global Permissions
There are no effective Global Permissions.

Micro Admin Permissions
There are no effective Micro Admin Permissions.

Advanced Permissions
There are no effective Content Set Permissions.

Figure 3

H. In the **Grant Roles** section, click **Edit**, select **Interact Basic User** and **Threat Response Read Only User**, and click **Save** (Figure 4 & 5)



Edit Grant Roles

interact

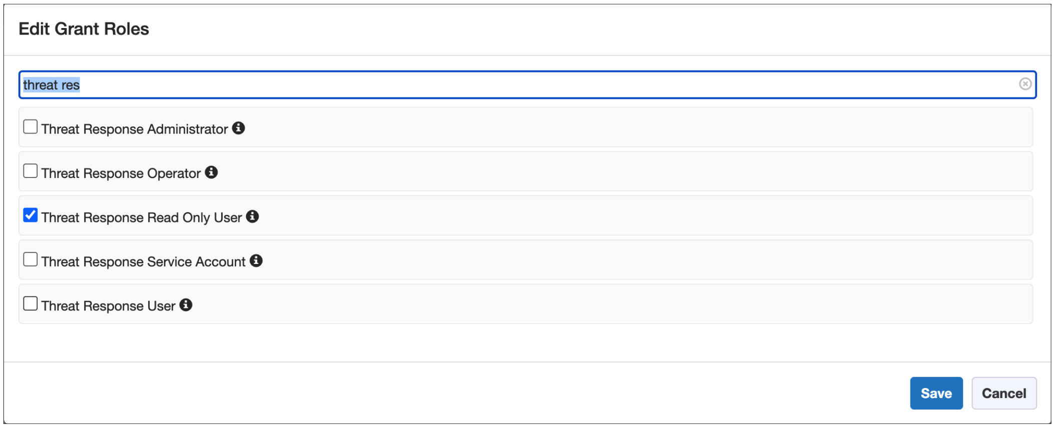
☑ Interact Basic User

□ Interact Power User

□ Interact Read-Only User

□ Interact Show

Figure 4



threat res

☐ Threat Response Administrator

☐ Threat Response Operator

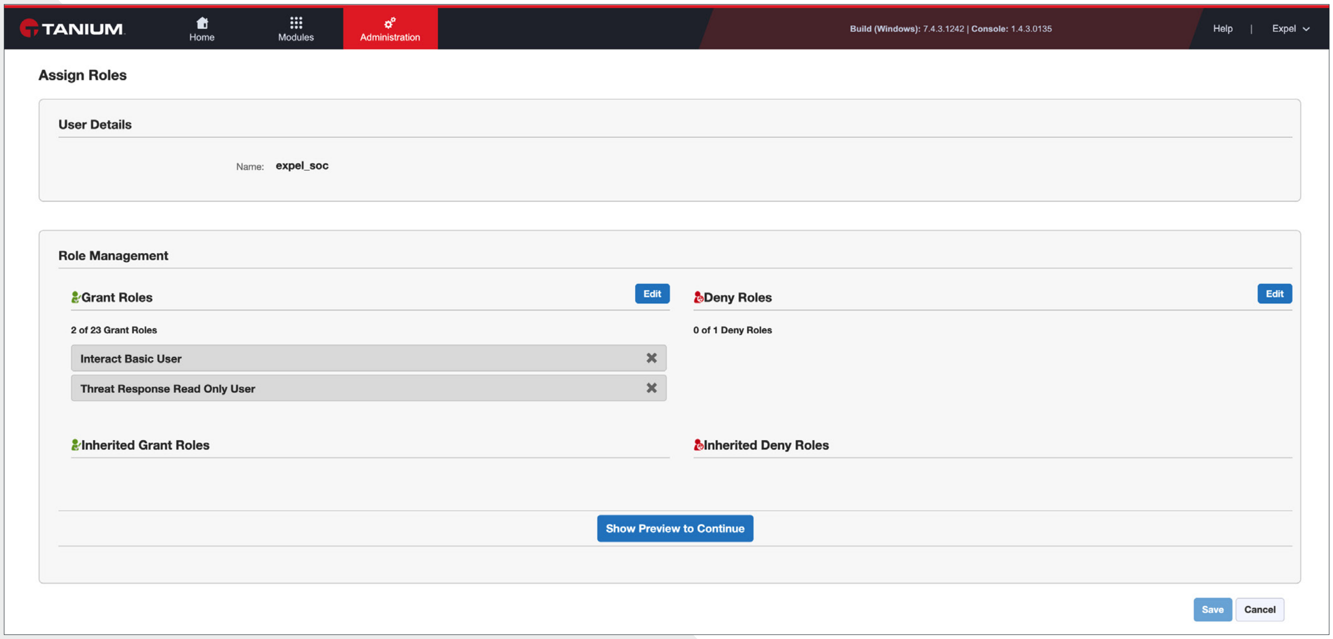
☑ Threat Response Read Only User

☐ Threat Response Service Account

☐ Threat Response User

Figure 5

I. Click **Show Preview to Continue** to review the impact of your changes (Figure 6)



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135

Assign Roles

User Details

Name: expel_soc

Role Management

Grant Roles

2 of 23 Grant Roles

- Interact Basic User
- Threat Response Read Only User

Deny Roles

0 of 1 Deny Roles

Inherited Grant Roles

Inherited Deny Roles

Figure 6

Step 2 — Configure the technology in Workbench

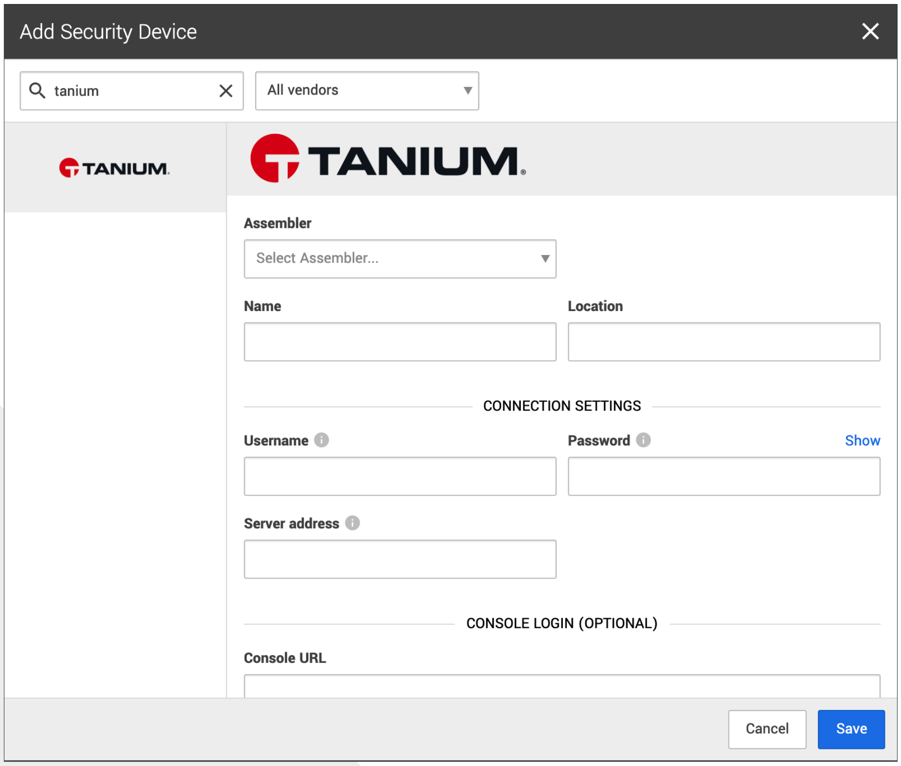
Now that we have all the correct access configured and have noted the credentials, we can integrate your tech with Expel.

A. Login to https://workbench.expel.io

B. Navigate to **Settings > Security Devices**

C. At the top right of the page, select **Add New Device**

D. Search for and select your technology Tanium (Figure 7)



Add Security Device

tanium

All vendors

TANIUM

Assembler

Select Assembler...

Name

Location

CONNECTION SETTINGS

Username

Password

Show

Server address

CONSOLE LOGIN (OPTIONAL)

Console URL

Figure 7

E. Complete all fields using the credentials and information you collected in *Step 1* above

F. For **Name** enter the hostname of the Tanium device

G. For **Location** enter the geographic location of the appliance

H. For **Server address** enter the hostname or IP address of the Tanium device

I. For **Username** and **Password** fields enter the username and password created in *Step 1*

J. Select **Save**

K. After a few minutes (between 1 and 15), refresh the **Security Devices** page and you should see your device reporting as *Healthy* or if there is an issue, it will provide more details of what the issue may be

That's it! Give yourself a pat on the back — you're done!

If you have any issues, concerns, questions or feedback,
please don't hesitate to contact Expel at devicehealth@expel.io.