TANIUM™

Hands on IT Operations Workshop 2.0

Lab Guide

Contents

Getting Started

Welcome to your Tanium Lab Guide! The exercises contained in this guide will introduce you to Tanium through hands-on use of the platform. You'll work through real-world scenarios that should hopefully give you an insight into how Tanium can improve the world of IT Operations in your own environment.

Your instructor will assign you a student number and explain how to access your own Tanium console. Whilst you are encouraged to explore the Tanium console and all of its features as much as possible please remember that it is a shared environment with all of your fellow students and thus no changes other than those described in this document should be made.

As you are working through the lab guide you may see sections where the tasks are split by designated student ID. Select the task instruction that matches your own student number. i.e. students 1 - 20 should ***only*** perform the designated actions assigned to that group.

Note: the screenshots provided are for guidance only and your own console may differ slightly from what is shown here. Your lab instructor can guide you through any differences.

Document Formatting Conventions

From this point onward, the following formatting conventions are in use:

- Words and terms in **Bold** refer to buttons or other console or interface elements
- Words in *Italics* refer to text to be entered, drop-down menu options to be selected or other forms of input or configuration required to achieve a specific goal or outcome.

Lab 1: Kicking the Tyres

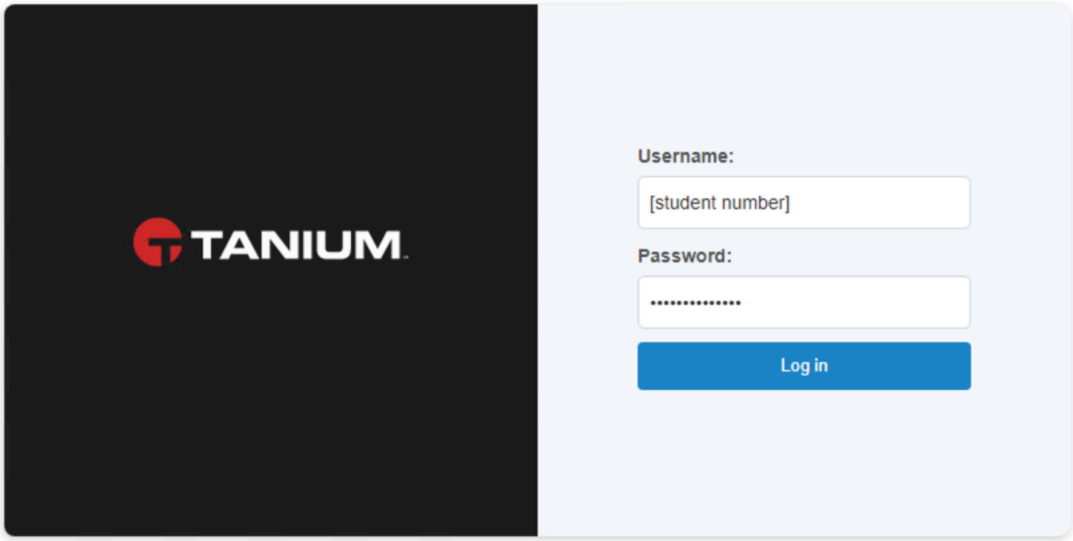
An introduction to Tanium, getting started and kicking the tyres!

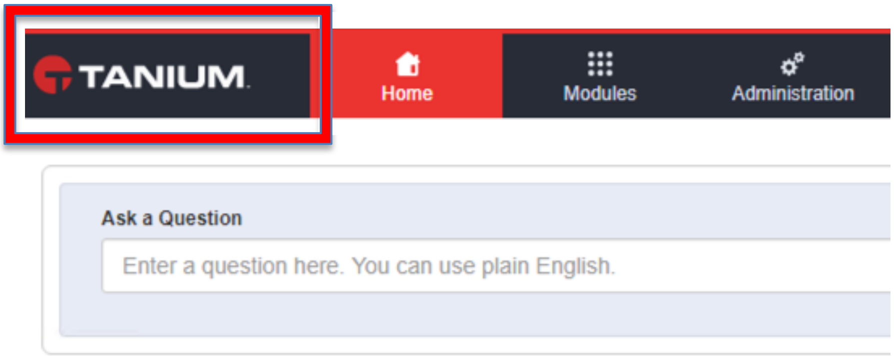
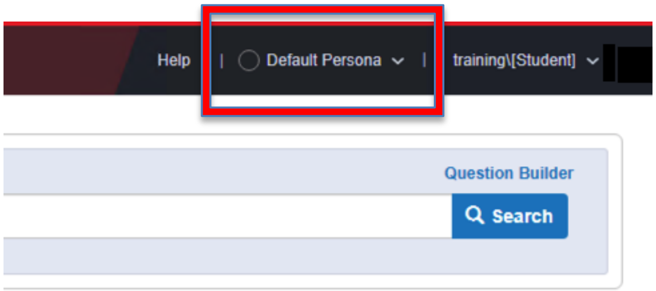
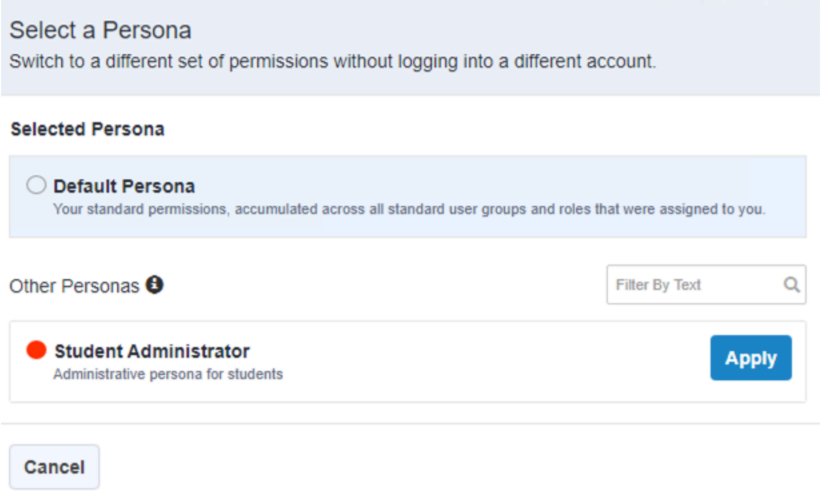
Objectives

By the end of this lab you will have completed the following objectives:

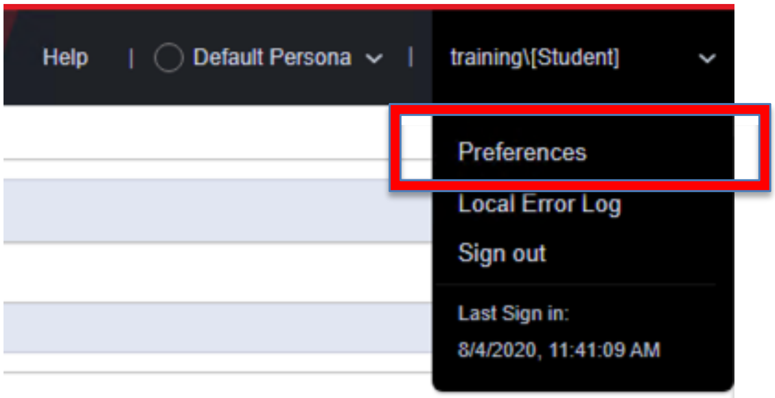
- Log into the Tanium console
- Explore the console and options available to you
- Explore your assigned permissions and personas
- Set your own user preferences
- View System Status screen

Lab Steps

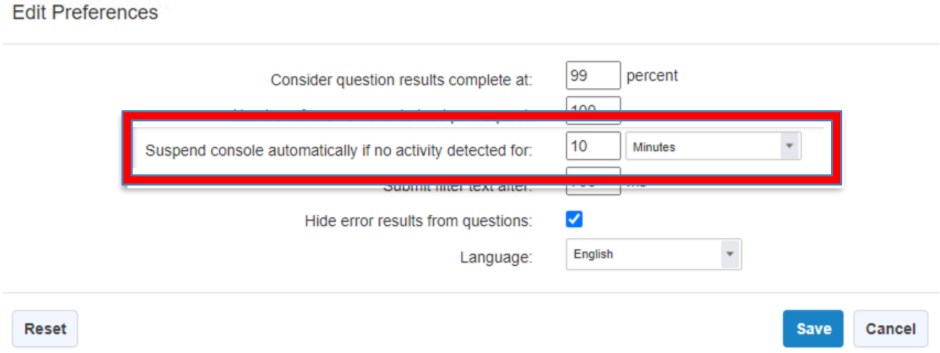
1.	Using the URL provided, open the Tanium console and enter your credentials  Username: [student number] Password: ••••••••••••••

2.	Explore the various options in the console and the screens presented. If you want to return to the home screen at any time you can use click on the **Tanium** icon in the top left-hand corner.  TANIUM Home Modules Administration Ask a Question Enter a question here. You can use plain English.
3.	Open the **Personas** menu to change your active persona.  Help Default Persona training\[Student] [redacted] Question Builder Search  Select a Persona Switch to a different set of permissions without logging into a different account. Selected Persona ○ Default Persona Your standard permissions, accumulated across all standard user groups and roles that were assigned to you. Other Personas Filter By Text ● Student Administrator Administrative persona for students

4. Access your personal **Preferences** section through the drop-down, top-right menu



Set your inactivity timeout to 60 minutes



Edit Preferences

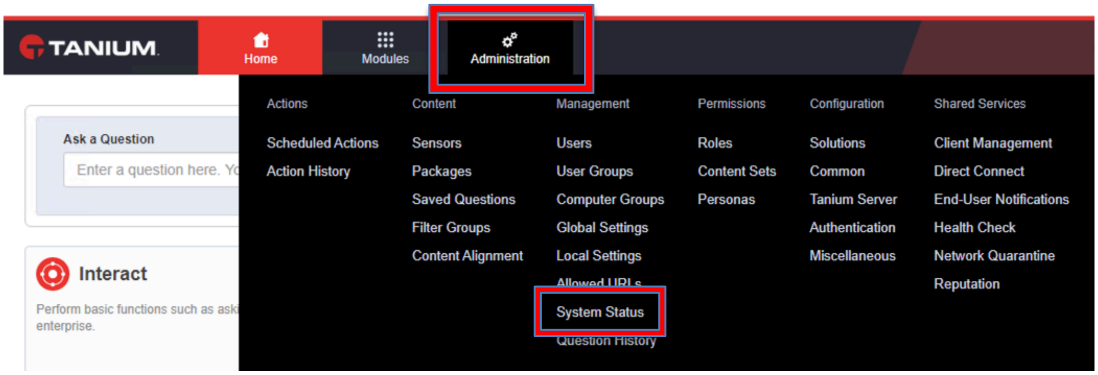
Consider question results complete at: 99 percent

Suspend console automatically if no activity detected for: 10 Minutes

Hide error results from questions: ☑

Language: English

5. Open the **Administration** menu and select **System Status**



Can't see that option in your menu? Perhaps you need to assume a different role for this particular task!

Now change your active persona back to the default by using the persona menu once again. You have now completed Lab 1.

Lab 2: Becoming Inquisitive

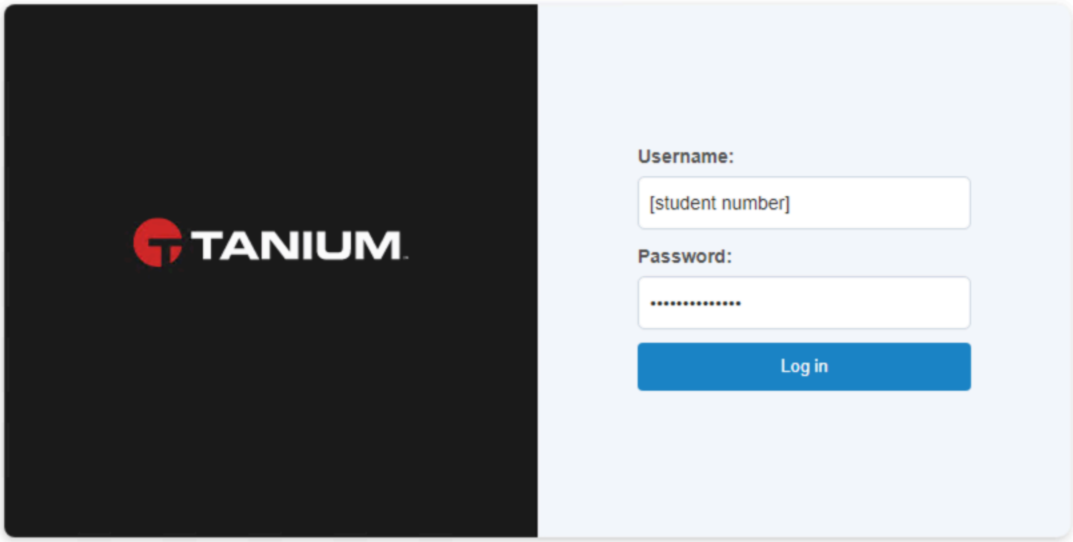
No such thing as a stupid question.

Objectives

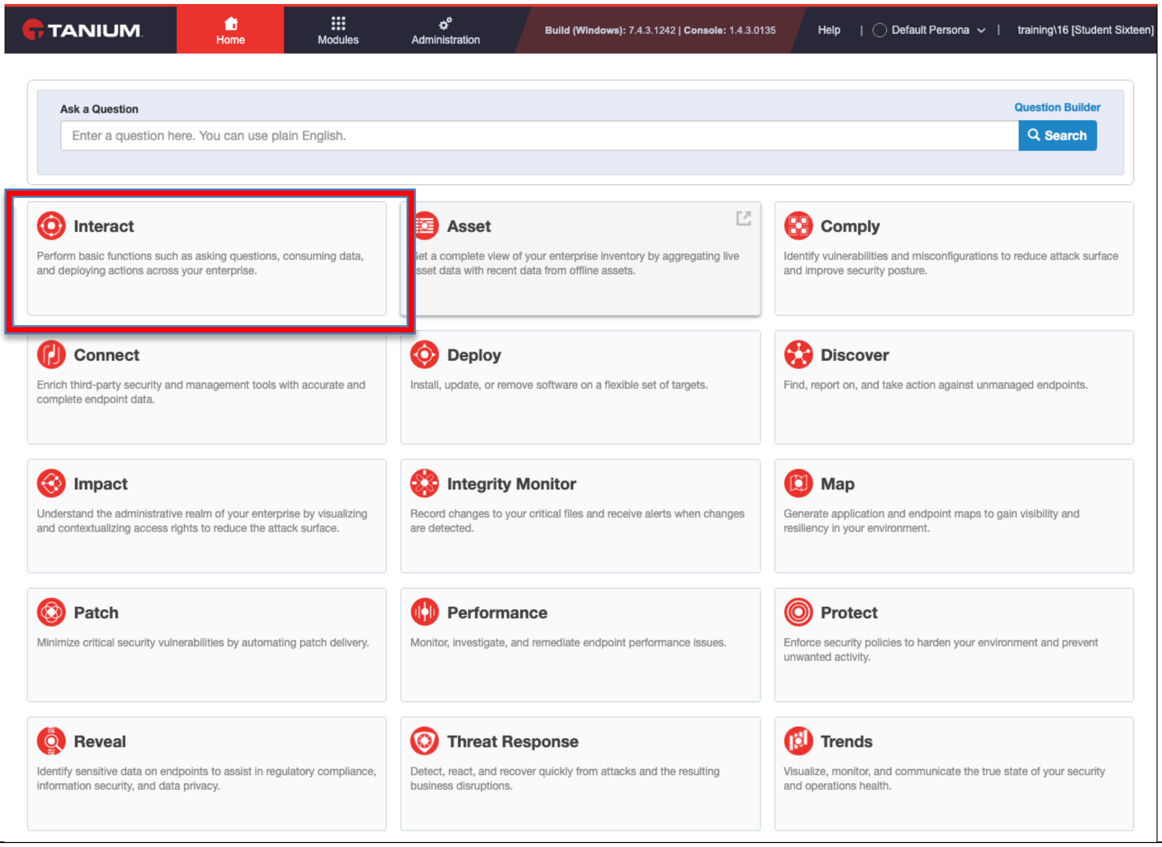
By the end of this lab you will have completed the following objectives:

- Ask a question and view the results
- Drill down the results to explore further
- Use the Question Builder

Lab Steps

1.	Using the URL provided, open the Tanium console and enter your credentials  Username: [student number] Password: ••••••••••••••

2. Click on the Interact “baseball card” to open the module.



Enter a question here. You can use plain English.

Interact
Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise.

Asset
Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets.

Comply
Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.

Connect
Enrich third-party security and management tools with accurate and complete endpoint data.

Deploy
Install, update, or remove software on a flexible set of targets.

Discover
Find, report on, and take action against unmanaged endpoints.

Impact
Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface.

Integrity Monitor
Record changes to your critical files and receive alerts when changes are detected.

Map
Generate application and endpoint maps to gain visibility and resiliency in your environment.

Patch
Minimize critical security vulnerabilities by automating patch delivery.

Performance
Monitor, investigate, and remediate endpoint performance issues.

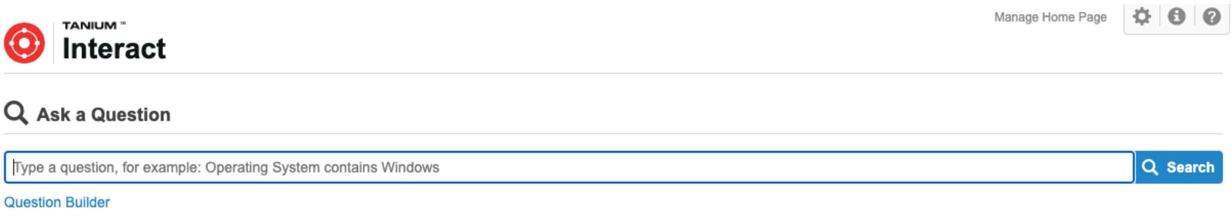
Protect
Enforce security policies to harden your environment and prevent unwanted activity.

Reveal
Identify sensitive data on endpoints to assist in regulatory compliance, information security, and data privacy.

Threat Response
Detect, react, and recover quickly from attacks and the resulting business disruptions.

Trends
Visualize, monitor, and communicate the true state of your security and operations health.

3. You will see an **Ask a Question** field at the top of the screen that looks similar to that shown below:

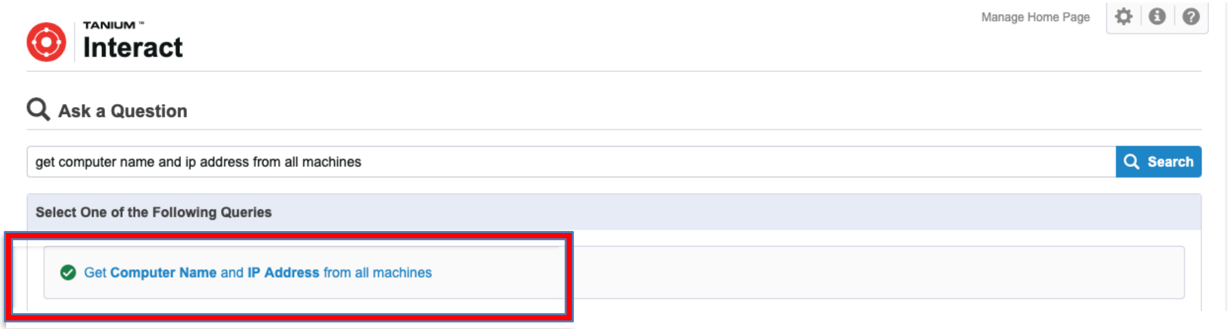


Type a question, for example: Operating System contains Windows

In this field, enter the following question, followed by pressing the Return key:

Get Computer Name and IP Address from all machines

4. Similar to a typical search engine, Tanium Interact will now parse the question and suggest queries which can be issued, based on the question entered:



Ask a Question

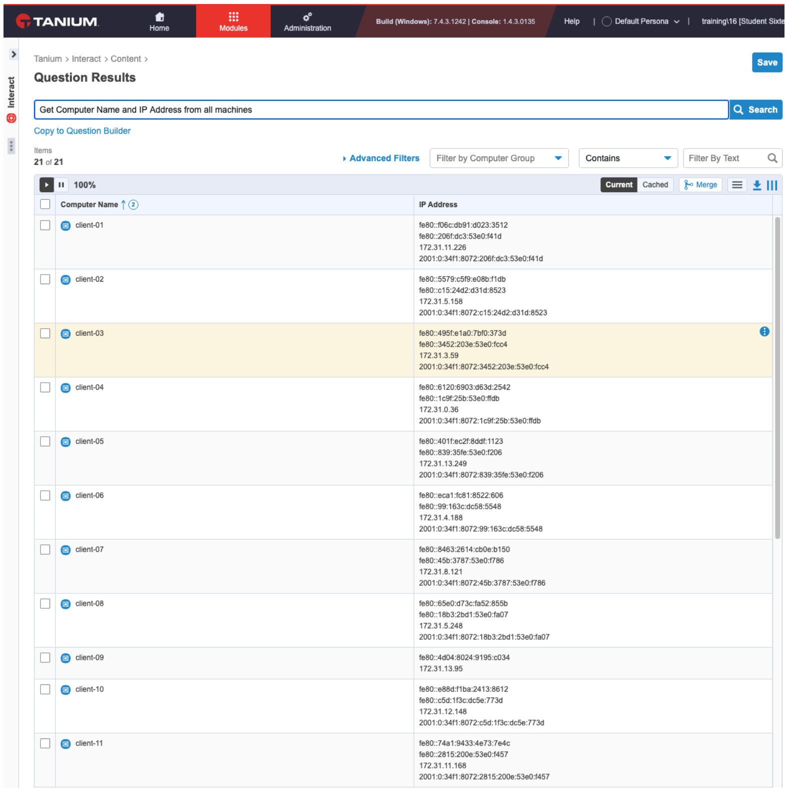
get computer name and ip address from all machines

Select One of the Following Queries

Get **Computer Name** and **IP Address** from all machines

You will notice that the words **Computer Name** and **IP Address** in the suggestion displayed are in bold. This signifies Tanium sensors which will be issued as part of your question. Click on the link to issue the question to managed endpoints.

5. The results will now be displayed:



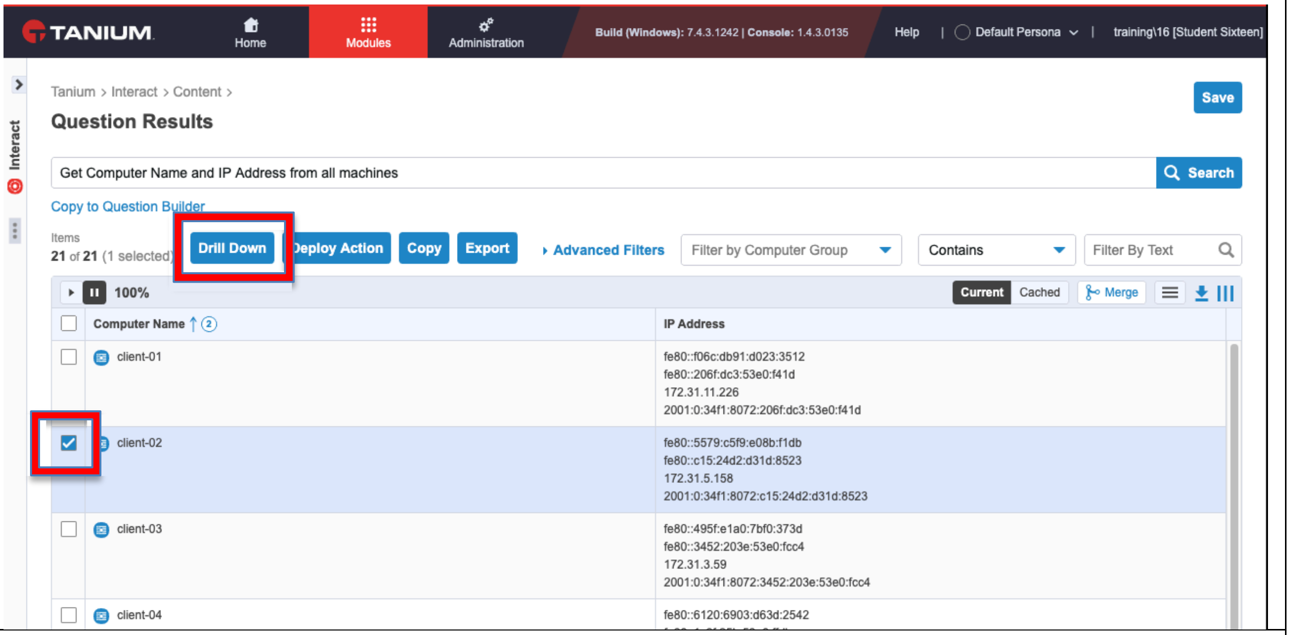
Question Results

Get Computer Name and IP Address from all machines

Items
21 of 21

Computer Name	IP Address
client-01	fe80::f06c:db91:d023:3512 fe80::206f:dc3:53e0:f41d 172.31.11.226 2001:0:34f1:8072:206f:dc3:53e0:f41d
client-02	fe80::5579:c5f9:e08b:f1db fe80::c15:24d2:d31d:8523 172.31.5.158 2001:0:34f1:8072:c15:24d2:d31d:8523
client-03	fe80::495f:e1a0:7bf0:373d fe80::3452:203e:53e0:fcc4 172.31.3.59 2001:0:34f1:8072:3452:203e:53e0:fcc4
client-04	fe80::6120:6903:d63d:2542 fe80::1c9f:25b:53e0:ffdb 172.31.0.36 2001:0:34f1:8072:1c9f:25b:53e0:ffdb
client-05	fe80::401f:ec2f:8ddf:1123 fe80::839:35fe:53e0:f206 172.31.13.249 2001:0:34f1:8072:839:35fe:53e0:f206
client-06	fe80::eca1:fc81:8522:606 fe80::99:163c:dc58:5548 172.31.4.188 2001:0:34f1:8072:99:163c:dc58:5548
client-07	fe80::8463:2614:cb0e:b150 fe80::45b:3787:53e0:f786 172.31.8.121 2001:0:34f1:8072:45b:3787:53e0:f786
client-08	fe80::65e0:d73c:fa52:855b fe80::18b3:2bd1:53e0:fa07 172.31.5.248 2001:0:34f1:8072:18b3:2bd1:53e0:fa07
client-09	fe80::4d04:8024:9195:c034 172.31.13.95
client-10	fe80::e88d:f1ba:2413:8612 fe80::c5d:1f3c:dc5e:773d 172.31.12.148 2001:0:34f1:8072:c5d:1f3c:dc5e:773d
client-11	fe80::74a1:9433:4e73:7e4c fe80::2815:200e:53e0:f457 172.31.11.168 2001:0:34f1:8072:2815:200e:53e0:f457

6. In the results list select any computer by marking the checkbox to the left of the computer name. A new series of options will now appear at the top. Select the option to **Drill Down**.



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135 | training\16 [Student Sixteen]

Tanium > Interact > Content >

Question Results

Get Computer Name and IP Address from all machines

Copy to Question Builder

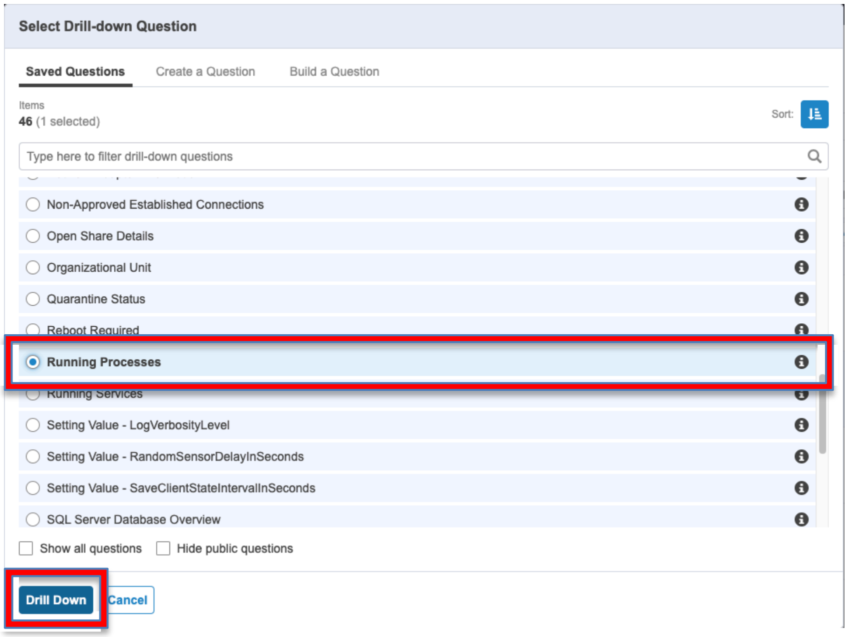
Items
21 of 21 (1 selected)

Filter by Computer Group | Contains | Filter By Text

100%

☐	Computer Name ↑ 2	IP Address
☐	client-01	fe80::f06c:db91:d023:3512 fe80::206f:dc3:53e0:f41d 172.31.11.226 2001:0:34f1:8072:206f:dc3:53e0:f41d
☑	client-02	fe80::5579:c5f9:e08b:f1db fe80::c15:24d2:d31d:8523 172.31.5.158 2001:0:34f1:8072:c15:24d2:d31d:8523
☐	client-03	fe80::495f:e1a0:7bf0:373d fe80::3452:203e:53e0:fcc4 172.31.3.59 2001:0:34f1:8072:3452:203e:53e0:fcc4
☐	client-04	fe80::6120:6903:d63d:2542

7. You will now be presented with a number of drilldown options. Select *Running Processes* and click Drill Down to issue the additional question:



Select Drill-down Question

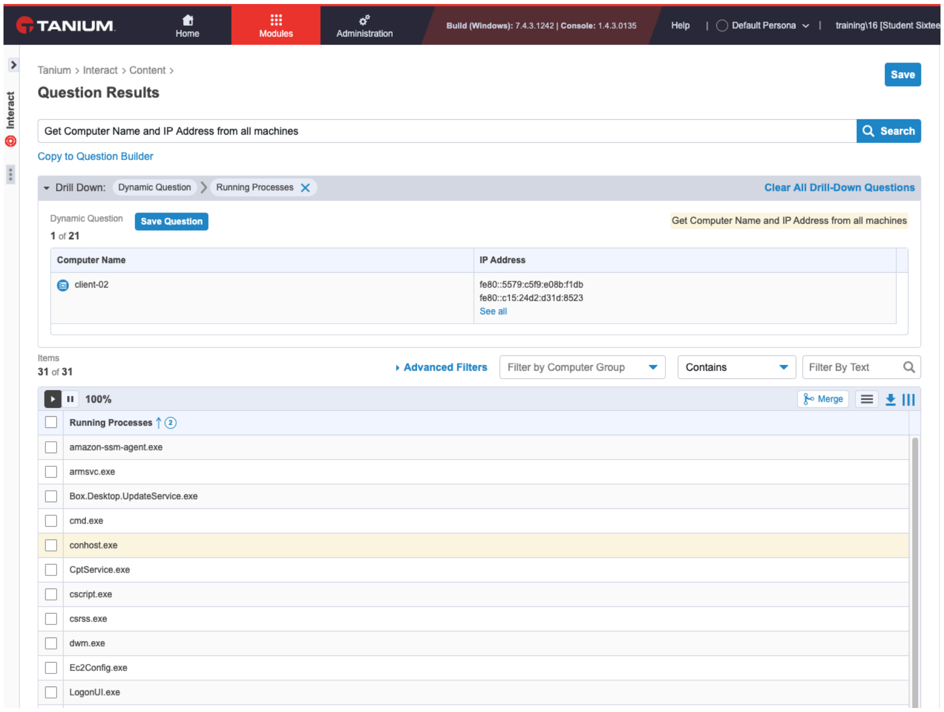
Items
46 (1 selected)

Type here to filter drill-down questions

○ Non-Approved Established Connections
○ Open Share Details
○ Organizational Unit
○ Quarantine Status
○ Reboot Required
● Running Processes
○ Running Services
○ Setting Value - LogVerbosityLevel
○ Setting Value - RandomSensorDelayInSeconds
○ Setting Value - SaveClientStateIntervalInSeconds
○ SQL Server Database Overview

☐ Show all questions ☐ Hide public questions

8. You will now be presented with the results based on a combination of the selection from the results of the original question, and the additional question issued:


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixtee
Interact
Tanium > Interact > Content >
Save
Search
Copy to Question Builder
Clear All Drill-Down Questions
Save Question
Advanced Filters
Merge

Question Results

Get Computer Name and IP Address from all machines

Drill Down: Dynamic Question > Running Processes

Dynamic Question

1 of 21

Get Computer Name and IP Address from all machines

Computer Name	IP Address
client-02	fe80::5579:c5f9:e08b:f1db fe80::c15:24d2:d31d:8523 See all

Items

31 of 31

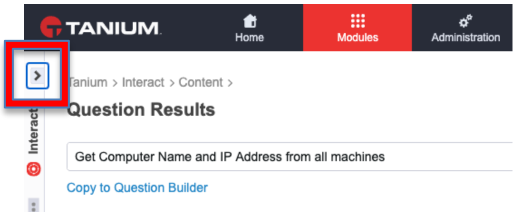
Filter by Computer Group | Contains | Filter By Text

100%

Running Processes
amazon-ssm-agent.exe
armsvc.exe
Box.Desktop.UpdateService.exe
cmd.exe
conhost.exe
CptService.exe
cscript.exe
csrss.exe
dwm.exe
Ec2Config.exe
LogonUI.exe

Note that this is a simple example, multiple selections can be made from initial question results and multiple drill down questions can be issued to construct complex and sophisticated queries.

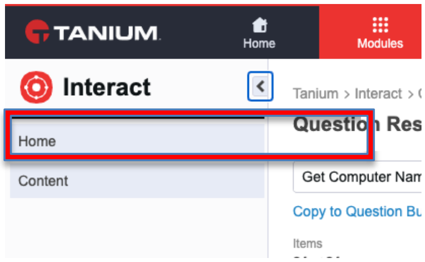
9. Return back to the Interact home page by expanding the menu on the left-hand side by clicking on the right-facing arrow as shown:

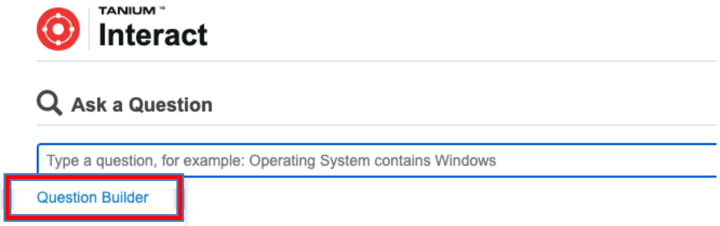
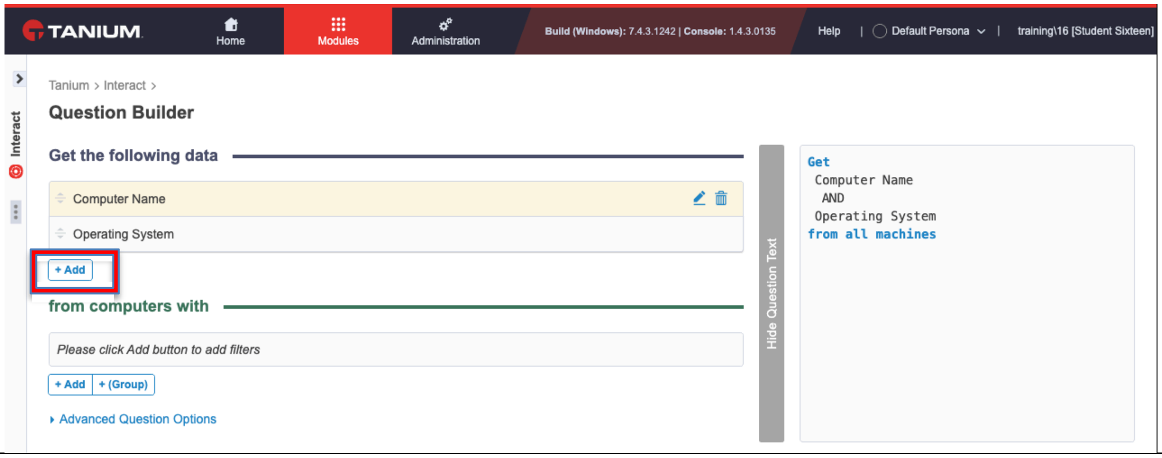
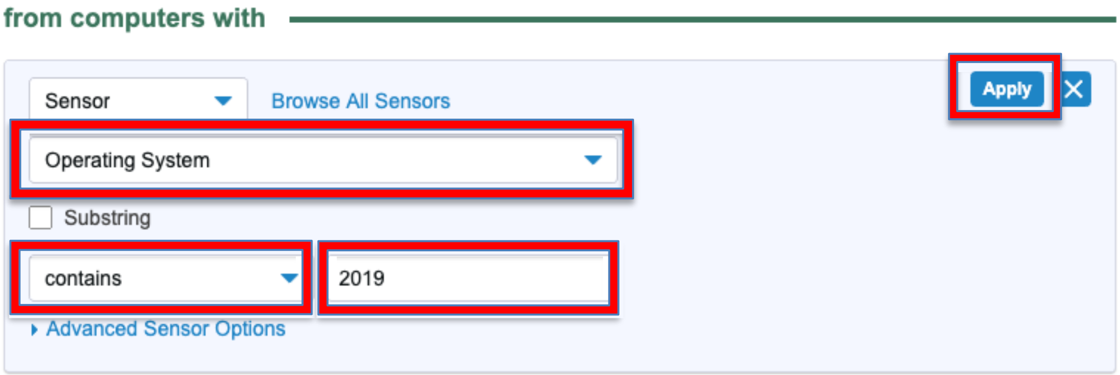


Question Results

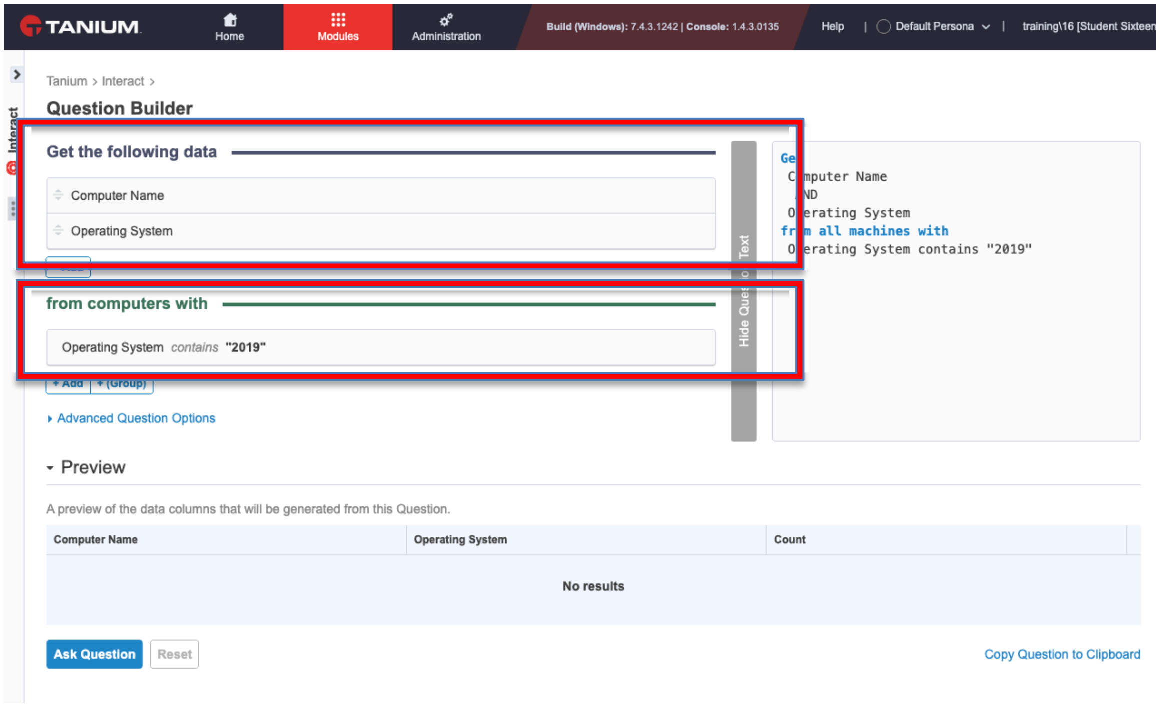
Get Computer Name and IP Address from all machines

Then click **Home**



10.	Click on the **Question Builder** link located under the field used in the previous steps to manually enter a question:  TANIUM Interact Ask a Question Type a question, for example: Operating System contains Windows Question Builder
11.	In the **Get the following data** section, click on **Add** and add the *Computer Name* and *Operating System* sensors  TANIUM Home Modules Administration Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135 Help Default Persona training\16 [Student Sixteen] Interact Tanium > Interact > Question Builder Get the following data + Add from computers with Please click Add button to add filters + Add + (Group) Advanced Question Options Hide Question Text Computer Name Operating System Get Computer Name AND Operating System from all machines
12.	Now click on the **Add** button in the **From computers with** section and select the *Operating System* sensor, then select the *contains* operator and enter the value *2019* as shown below , before clicking **Apply**:  from computers with Browse All Sensors Apply Advanced Sensor Options Sensor Operating System □ Substring contains 2019

13. The screen should now look similar to this with the information required at the top, and the selection criterion at the bottom.



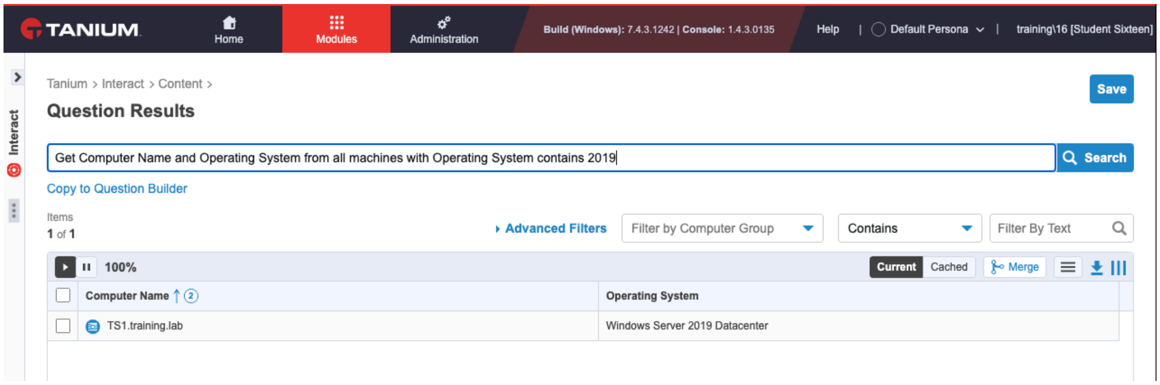
```
Ge
C mputer Name
 ND
O erating System
fr m all machines with
O erating System contains "2019"
```

A preview of the data columns that will be generated from this Question.

Computer Name	Operating System	Count
	No results	

Once the options are configured correctly, click on **Ask Question**.

14. The results will now be displayed:



Get Computer Name and Operating System from all machines with Operating System contains 2019

Items
1 of 1

☐	Computer Name	Operating System
☐	TS1.training.lab	Windows Server 2019 Datacenter

If all has been correctly configured, you should receive a single record back, for the Tanium server itself.

You have now completed Lab 2.

Lab 3: Opening Your Eyes

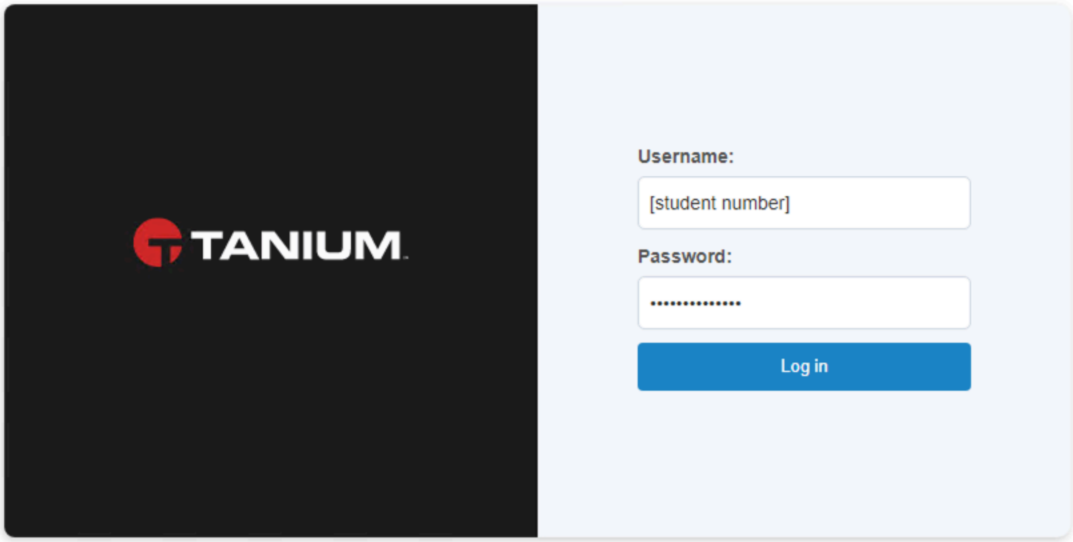
Using Tanium Discover to identify known and unknown interfaces in your environment

Objectives

By the end of this lab you will have completed the following objectives:

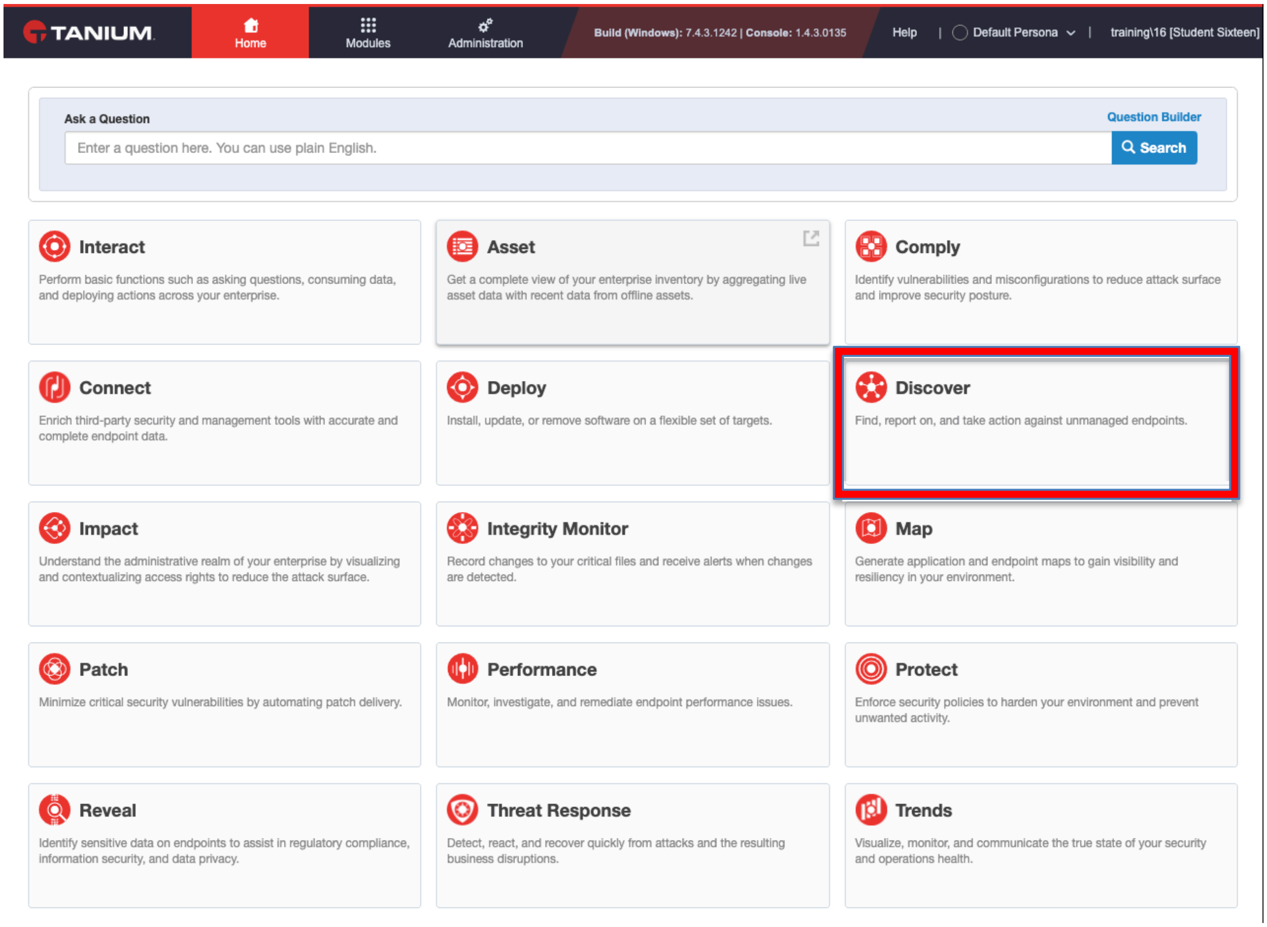
- Explore discovered interfaces
- Create a new discovery profile
- Working with Labels

Lab Steps

1.	Using the URL provided, open the Tanium console and enter your credentials  Username: [student number] Password: ••••••••••••••

2. Click on the **Tanium** logo at the top left-hand corner to return you to the home page if you aren’t there already.

You should see the homepage of the Tanium console, displaying the various “baseball cards” for the available modules. From here, click on **Discover**


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Ask a Question
Question Builder
Enter a question here. You can use plain English.
Search

Interact
Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise.

Asset
Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets.

Comply
Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.

Connect
Enrich third-party security and management tools with accurate and complete endpoint data.

Deploy
Install, update, or remove software on a flexible set of targets.

Discover
Find, report on, and take action against unmanaged endpoints.

Impact
Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface.

Integrity Monitor
Record changes to your critical files and receive alerts when changes are detected.

Map
Generate application and endpoint maps to gain visibility and resiliency in your environment.

Patch
Minimize critical security vulnerabilities by automating patch delivery.

Performance
Monitor, investigate, and remediate endpoint performance issues.

Protect
Enforce security policies to harden your environment and prevent unwanted activity.

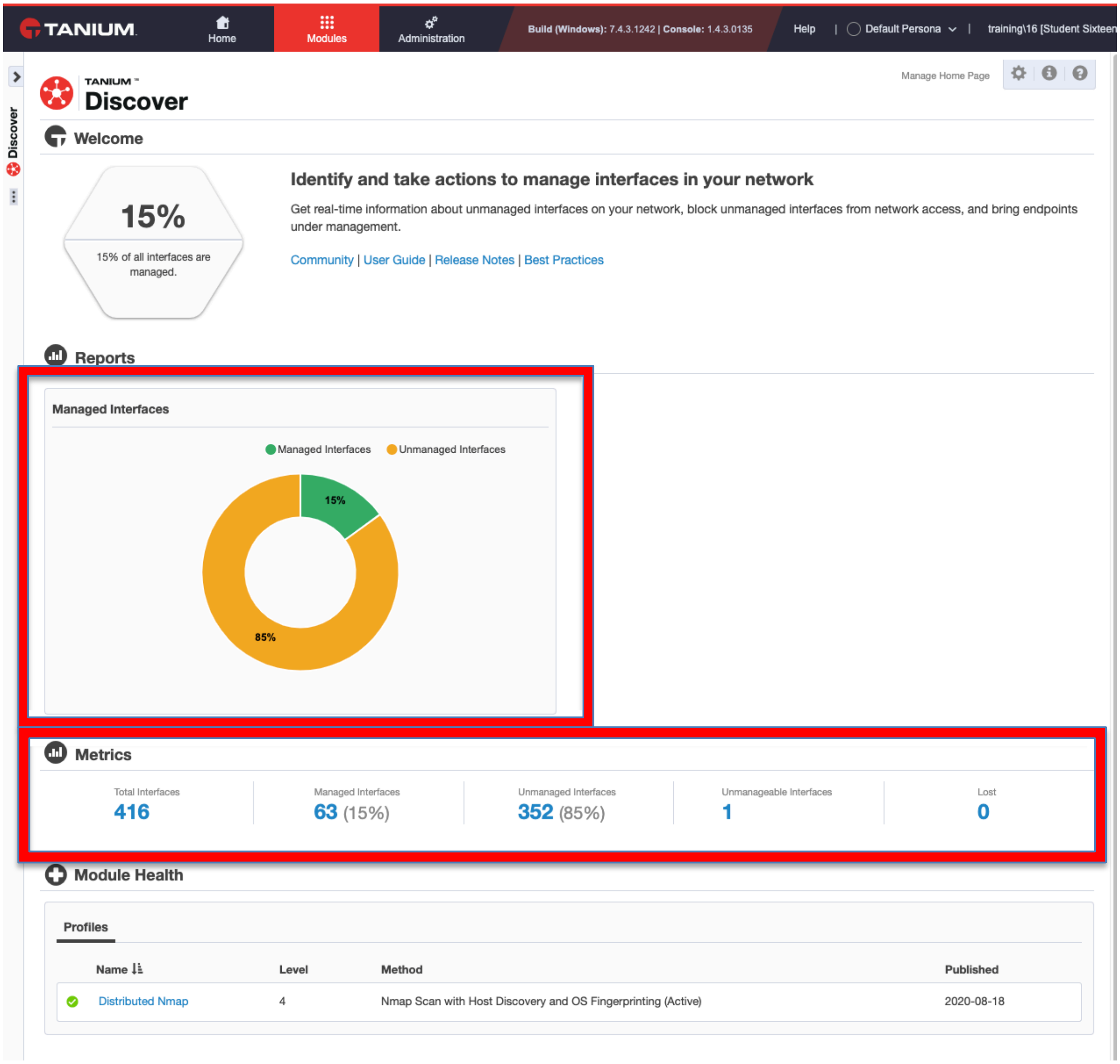
Reveal
Identify sensitive data on endpoints to assist in regulatory compliance, information security, and data privacy.

Threat Response
Detect, react, and recover quickly from attacks and the resulting business disruptions.

Trends
Visualize, monitor, and communicate the true state of your security and operations health.

This will now take you to the Discover workbench.

3. You will be presented with an overview of the percentage of managed vs. unmanaged interfaces discovered in the environment and a summary of metrics, along with other information such as overall module health and details on scanning profiles in use.



TANIUM™
Discover

Welcome

15%

15% of all interfaces are managed.

Identify and take actions to manage interfaces in your network

Get real-time information about unmanaged interfaces on your network, block unmanaged interfaces from network access, and bring endpoints under management.

Community | User Guide | Release Notes | Best Practices

Reports

Managed Interfaces

Metrics

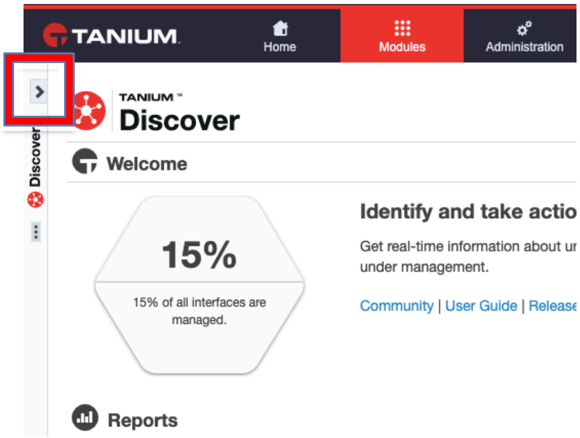
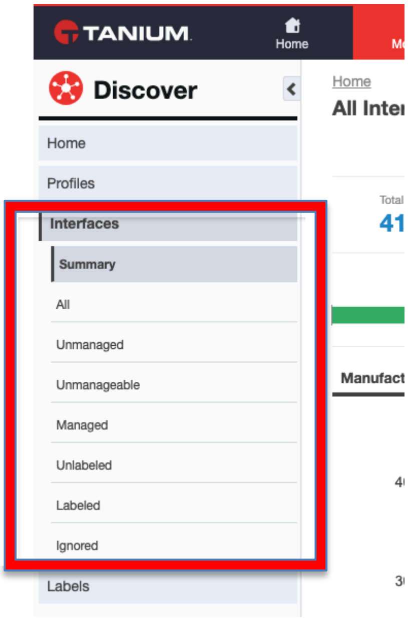
Total Interfaces	Managed Interfaces	Unmanaged Interfaces	Unmanageable Interfaces	Lost
416	63 (15%)	352 (85%)	1	0

Module Health

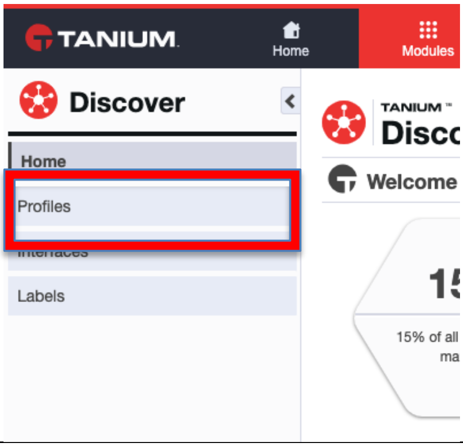
Profiles

Name	Level	Method	Published
✓ Distributed Nmap	4	Nmap Scan with Host Discovery and OS Fingerprinting (Active)	2020-08-18

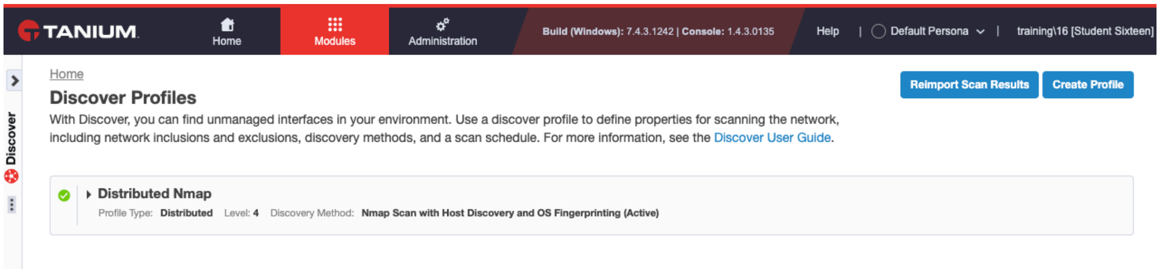
Clicking on each one of the metrics shown in bold numbers will drill down into the actual data identified during Discover scans. Have a look around these and see what kinds of information is available, and what extra information can be added.

4.	Another way to interrogate the interface data identified during discovery is to look at pre-prepared views that come with the module. Click on the right-facing arrow on the left-hand side of the screen to pop the menu out.  TANIUM Home Modules Administration TANIUM Discover Welcome 15% Reports Discover 15% of all interfaces are managed. Identify and take actio Get real-time information about ur under management. Community | User Guide | Release
5.	From here, click on **Interfaces** to expose a series of pre-defined views.  TANIUM Home Mo Discover Home All Inte Home Profiles Interfaces Summary All Unmanaged Unmanageable Managed Unlabeled Labeled Ignored Labels Total 41 Manufact 4 3

6. Return to the pop-out menu and this time, select **Profiles**.



7. This screen in the Discover workbench, shows the scan profiles which are currently configured and allows you to create new profiles.



Discover Profiles

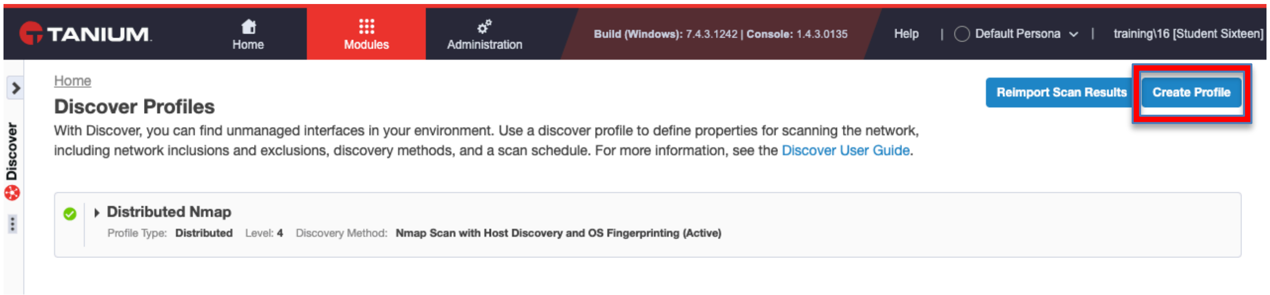
With Discover, you can find unmanaged interfaces in your environment. Use a discover profile to define properties for scanning the network, including network inclusions and exclusions, discovery methods, and a scan schedule. For more information, see the Discover User Guide.

Distributed Nmap
Profile Type: Distributed Level: 4 Discovery Method: Nmap Scan with Host Discovery and OS Fingerprinting (Active)

Hover your mouse over the Distributed NMAP scan profile and click on the ✎ icon to edit it. Take a look around the configuration and options, particularly around the various scan methods.

Navigate back to the previous workbench page which listed the available scan profiles

8. Click on **Create Profile**.



Discover Profiles

With Discover, you can find unmanaged interfaces in your environment. Use a discover profile to define properties for scanning the network, including network inclusions and exclusions, discovery methods, and a scan schedule. For more information, see the Discover User Guide.

Distributed Nmap
Profile Type: Distributed Level: 4 Discovery Method: Nmap Scan with Host Discovery and OS Fingerprinting (Active)

We will now work through an exercise which will involve taking a set of specific set of representative requirements and modelling these in a new scan profile.

9. Consider how you might setup a scan profile, which has the following specification:

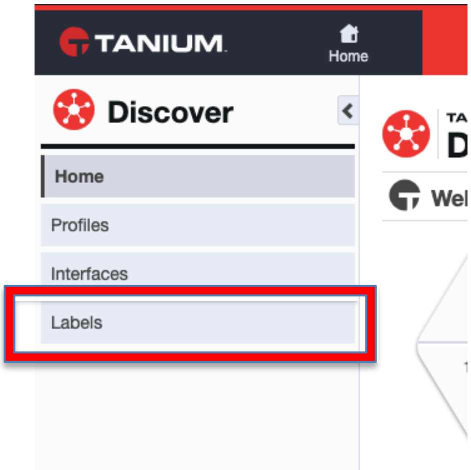
- Does not scan from a central server
- Requires OS information from Windows endpoints
- Only scans a specified IP range using the following network definition:
    - Name: *Student <Student ID number> Network*
    - IP Range: *10.10.<Student ID Number>.0/24*

  Important: When successfully configured, this option may read a value of *All*. This is expected and is simply because only one network is defined and selected.

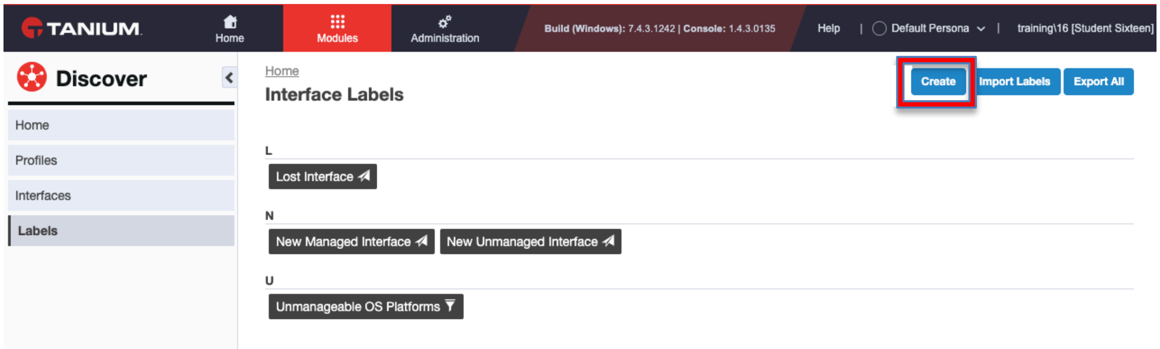
- Does not scan interfaces connected via an isolated subnet
- Scans every 2 hours, distributed over 1 hour
- Can only scan on weekdays from 10am for a period of 6 hours
- All other options unless specified, should remain as default

Create this scan profile and name it as *Student <Student ID number> scan profile.*

10. Return to the pop-out menu once more, and this time select the Labels menu option.



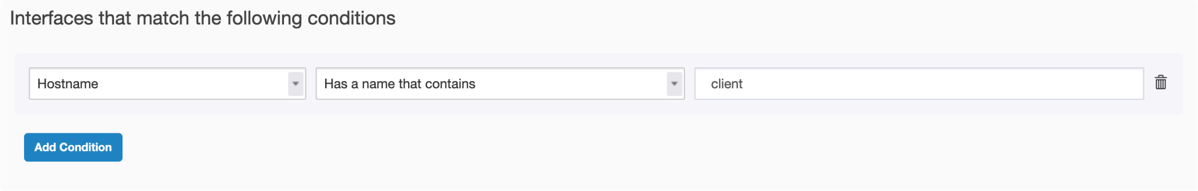
11. You will now be presented with the **Labels** workbench and the default set of labels. Labels can be used to tag, and group interfaces based on criteria defined within each label.



Review the labels which are available and then click on **Create**.

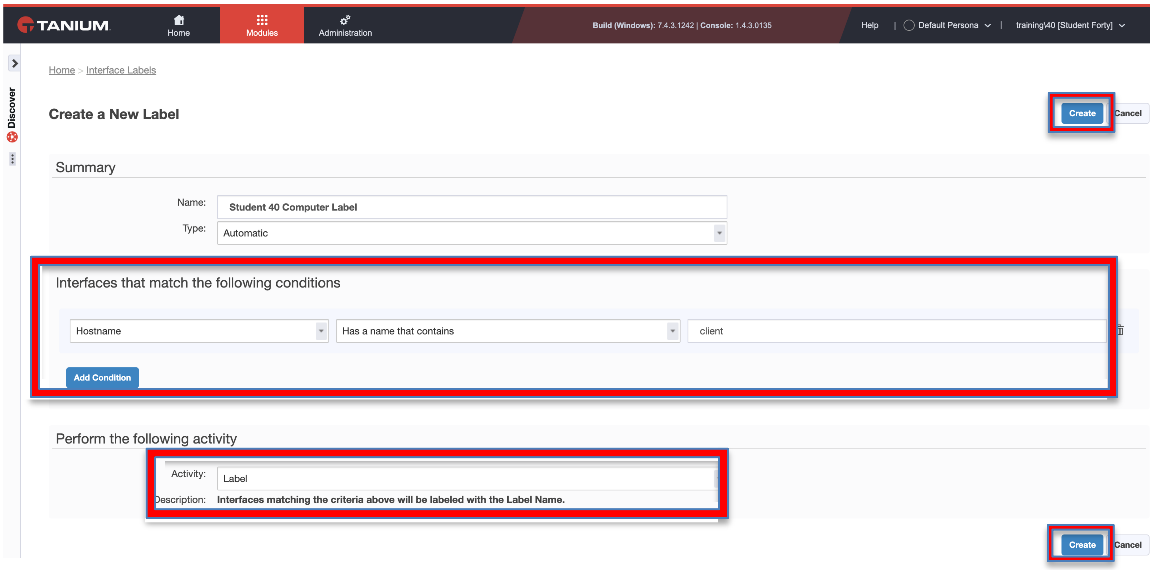
12. In the **Name** field, enter *Student <Student ID Number> Computer Label*.

In **the Interfaces that match the following conditions** section, explore the available options and then configure the condition as shown below:



Hostname | Has a name that contains | client

Your label definition should look similar to that shown below.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\40 [Student Forty]
Discover
Home > Interface Labels
Create a New Label
Create
Cancel
Summary
Interfaces that match the following conditions
Add Condition
Perform the following activity
Create
Cancel

Name: Student 40 Computer Label

Type: Automatic

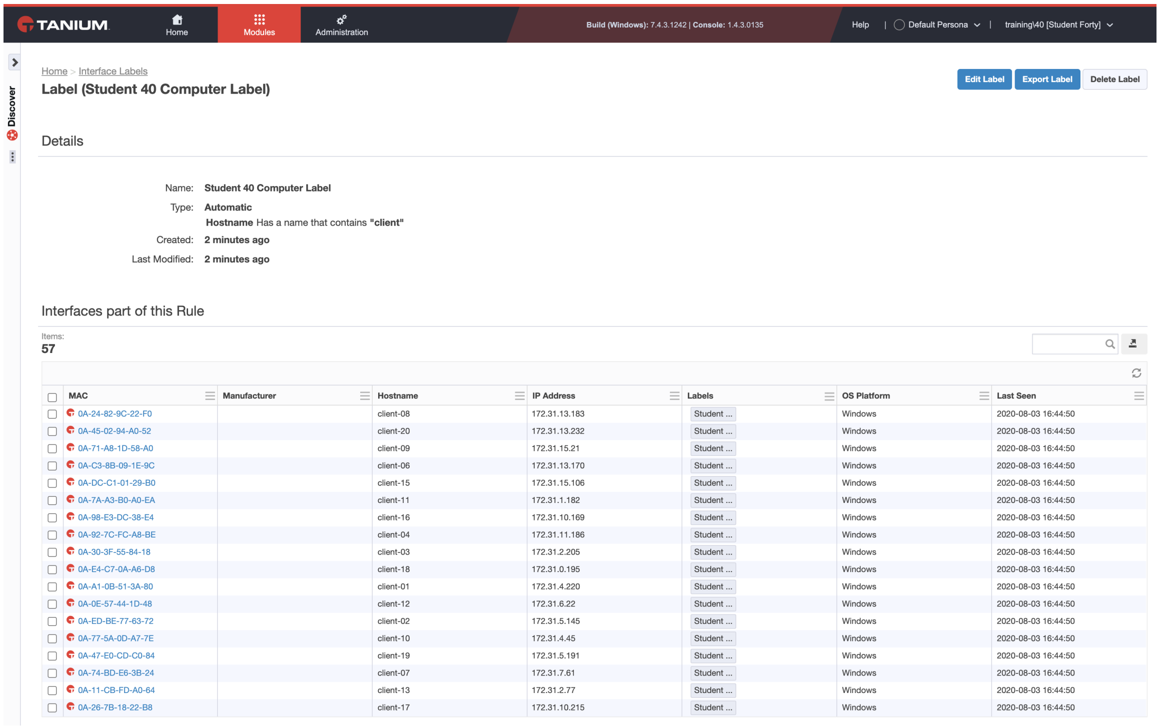
Hostname | Has a name that contains | client

Activity: Label

Description: Interfaces matching the criteria above will be labeled with the Label Name.

Explore the **Activity** options and investigate what actions can be applied to labelled interfaces. Once your label is correctly configured, click **Create** to commit your changes.

13. You will be returned now to the **Labels** workbench, and your label will be shown, along with the endpoints where the label is applicable based on the criteria specified. In this example all endpoints will be labelled.



Home > Interface Labels

Label (Student 40 Computer Label)

Details

Name: **Student 40 Computer Label**
Type: **Automatic**
Hostname Has a name that contains **"client"**
Created: **2 minutes ago**
Last Modified: **2 minutes ago**

Interfaces part of this Rule

Items:
57

□	MAC	Manufacturer	Hostname	IP Address	Labels	OS Platform	Last Seen
□	0A-24-82-9C-22-F0		client-08	172.31.13.183	Student ...	Windows	2020-08-03 16:44:50
□	0A-45-02-94-A0-52		client-20	172.31.13.232	Student ...	Windows	2020-08-03 16:44:50
□	0A-71-A8-1D-58-A0		client-09	172.31.15.21	Student ...	Windows	2020-08-03 16:44:50
□	0A-C3-8B-09-1E-9C		client-06	172.31.13.170	Student ...	Windows	2020-08-03 16:44:50
□	0A-DC-C1-01-29-B0		client-15	172.31.15.106	Student ...	Windows	2020-08-03 16:44:50
□	0A-7A-A3-B0-A0-EA		client-11	172.31.1.182	Student ...	Windows	2020-08-03 16:44:50
□	0A-98-E3-DC-38-E4		client-16	172.31.10.169	Student ...	Windows	2020-08-03 16:44:50
□	0A-92-7C-FC-A8-BE		client-04	172.31.11.186	Student ...	Windows	2020-08-03 16:44:50
□	0A-30-3F-55-84-18		client-03	172.31.2.205	Student ...	Windows	2020-08-03 16:44:50
□	0A-E4-C7-0A-A6-D8		client-18	172.31.0.195	Student ...	Windows	2020-08-03 16:44:50
□	0A-A1-0B-51-3A-80		client-01	172.31.4.220	Student ...	Windows	2020-08-03 16:44:50
□	0A-0E-57-44-1D-48		client-12	172.31.6.22	Student ...	Windows	2020-08-03 16:44:50
□	0A-ED-BE-77-63-72		client-02	172.31.5.145	Student ...	Windows	2020-08-03 16:44:50
□	0A-77-5A-0D-A7-7E		client-10	172.31.4.45	Student ...	Windows	2020-08-03 16:44:50
□	0A-47-E0-CD-C0-84		client-19	172.31.5.191	Student ...	Windows	2020-08-03 16:44:50
□	0A-74-BD-E6-3B-24		client-07	172.31.7.61	Student ...	Windows	2020-08-03 16:44:50
□	0A-11-CB-FD-A0-64		client-13	172.31.2.77	Student ...	Windows	2020-08-03 16:44:50
□	0A-26-7B-18-22-B8		client-17	172.31.10.215	Student ...	Windows	2020-08-03 16:44:50

You have now completed Lab 3.

Lab 4: T to the C to the M - Steps

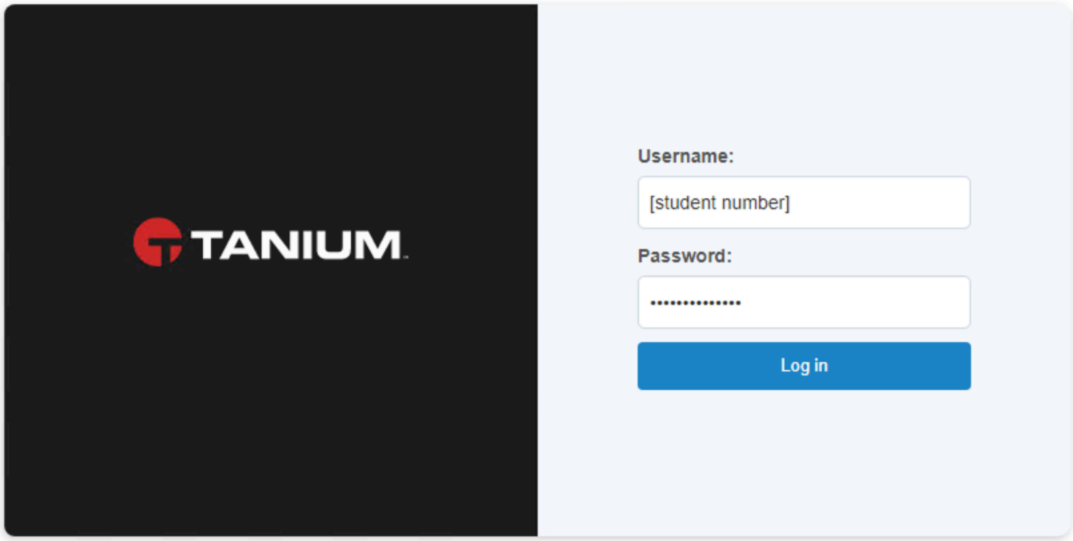
Verifying client health and getting the Tanium client out there!

Objectives

By the end of this lab you will have completed the following objectives:

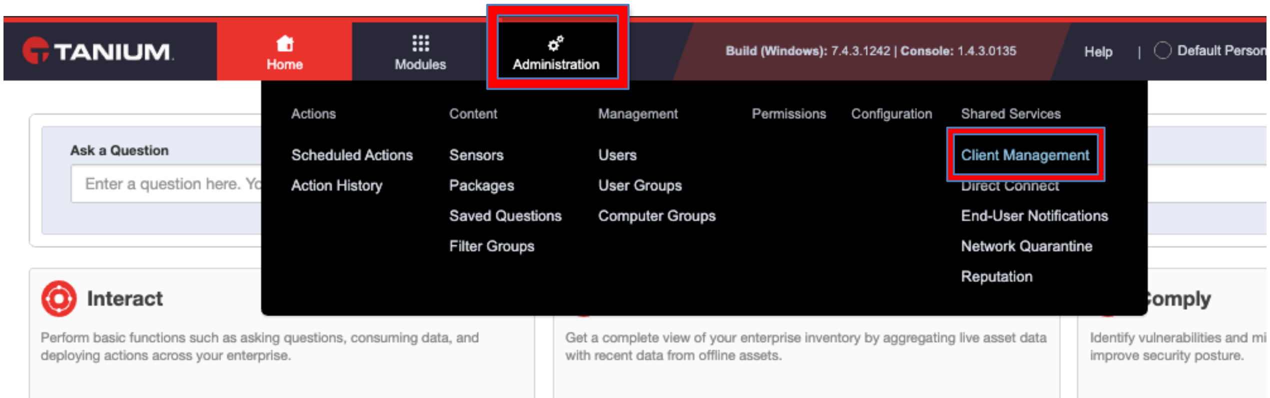
- Viewed the Client Health Page.
- Explore Tanium Client Management and agent deployment.
- Created an automated deployment based on your Discover label created in the previous lab.

Lab Steps

1.	Using the URL provided, open the Tanium console and enter your credentials  Username: [student number] Password: ••••••••••••••

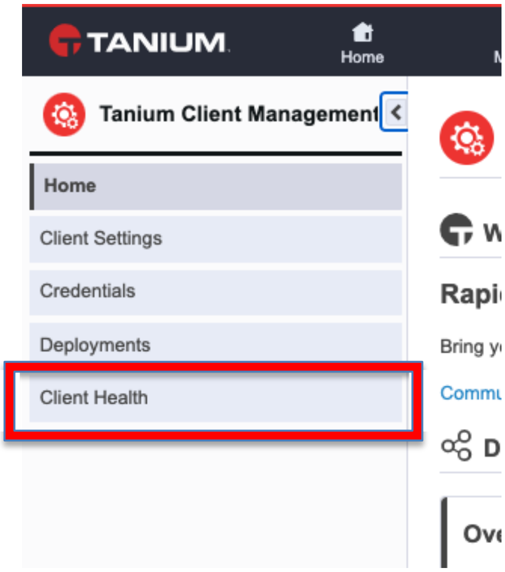
2. If you are not already at the homepage, click the Tanium logo top-left to return there.

Click on the **Administration** menu at the top, and then select **Client Management**


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Person
Ask a Question
Enter a question here. Yo
Actions
Scheduled Actions
Action History
Content
Sensors
Packages
Saved Questions
Filter Groups
Management
Users
User Groups
Computer Groups
Permissions
Configuration
Shared Services
Client Management
Direct Connect
End-User Notifications
Network Quarantine
Reputation
Interact
Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise.
Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets.
omply
Identify vulnerabilities and mi improve security posture.

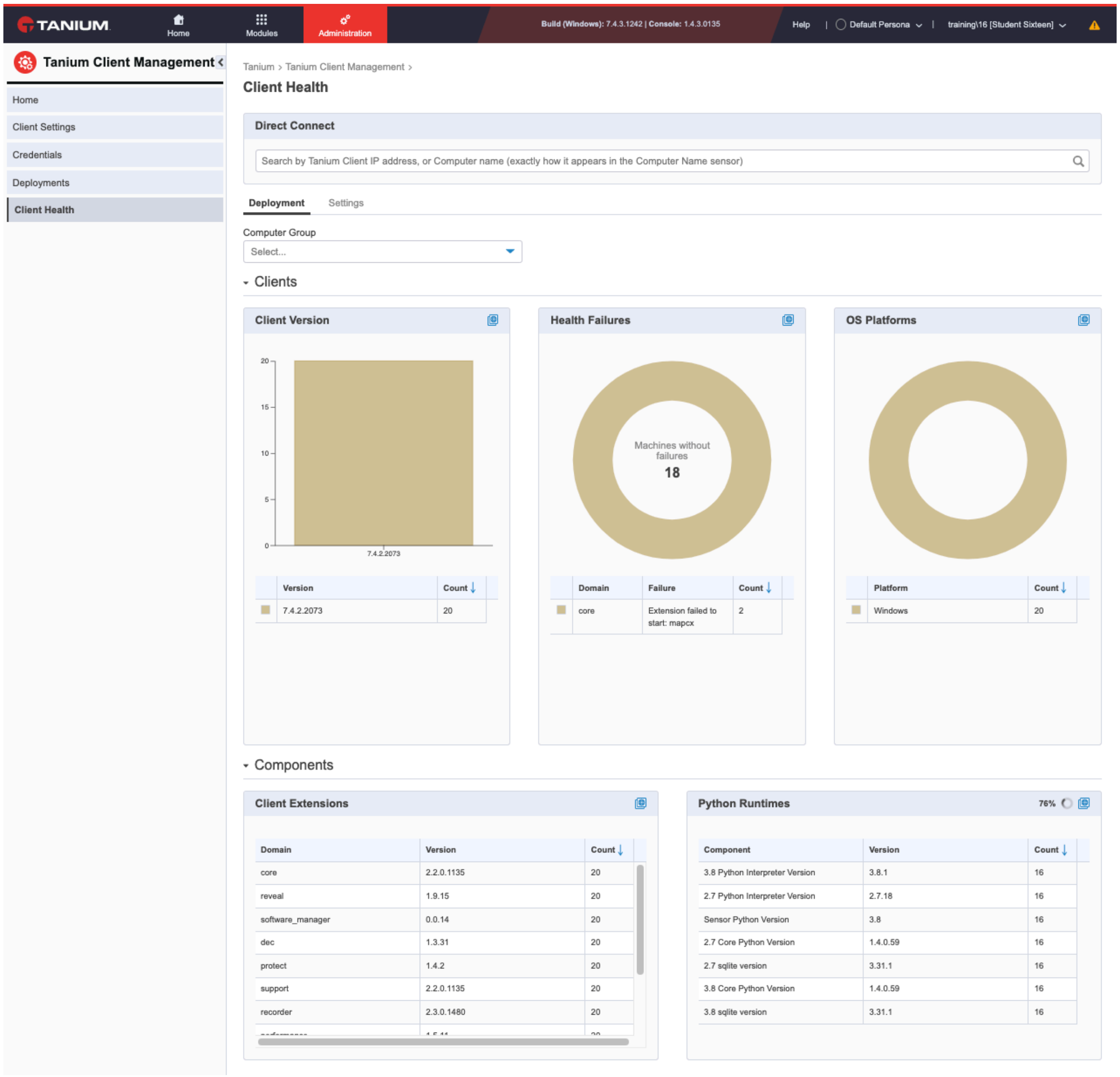
3. You will now be presented with the Tanium Client Management workbench.

Click on the pop-out menu on the left-side and select **Client Health**.



4. This dashboard displays a series of metrics and charts providing an overview of Tanium client health across the whole managed estate. You can see at a glance, information such as:

- Client versions and versions of client components deployed
- OS platforms being managed
- Endpoints reporting health failures.



Client Health

Direct Connect

Search by Tanium Client IP address, or Computer name (exactly how it appears in the Computer Name sensor)

Clients

Client Version

	Version	Count ↓
■	7.4.2.2073	20

Health Failures

	Domain	Failure	Count ↓
■	core	Extension failed to start: mapcx	2

OS Platforms

	Platform	Count ↓
■	Windows	20

Components

Client Extensions

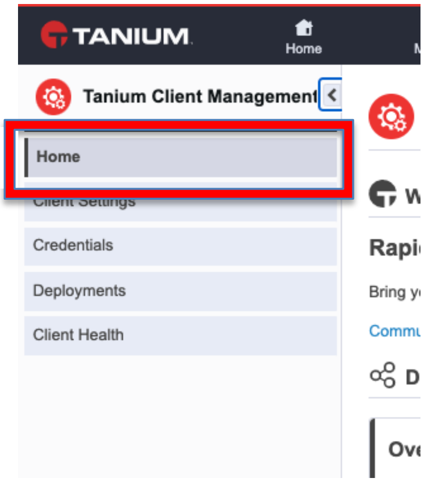
Domain	Version	Count ↓
core	2.2.0.1135	20
reveal	1.9.15	20
software_manager	0.0.14	20
dec	1.3.31	20
protect	1.4.2	20
support	2.2.0.1135	20
recorder	2.3.0.1480	20

Python Runtimes

Component	Version	Count ↓
3.8 Python Interpreter Version	3.8.1	16
2.7 Python Interpreter Version	2.7.18	16
Sensor Python Version	3.8	16
2.7 Core Python Version	1.4.0.59	16
2.7 sqlite version	3.31.1	16
3.8 Core Python Version	1.4.0.59	16
3.8 sqlite version	3.31.1	16

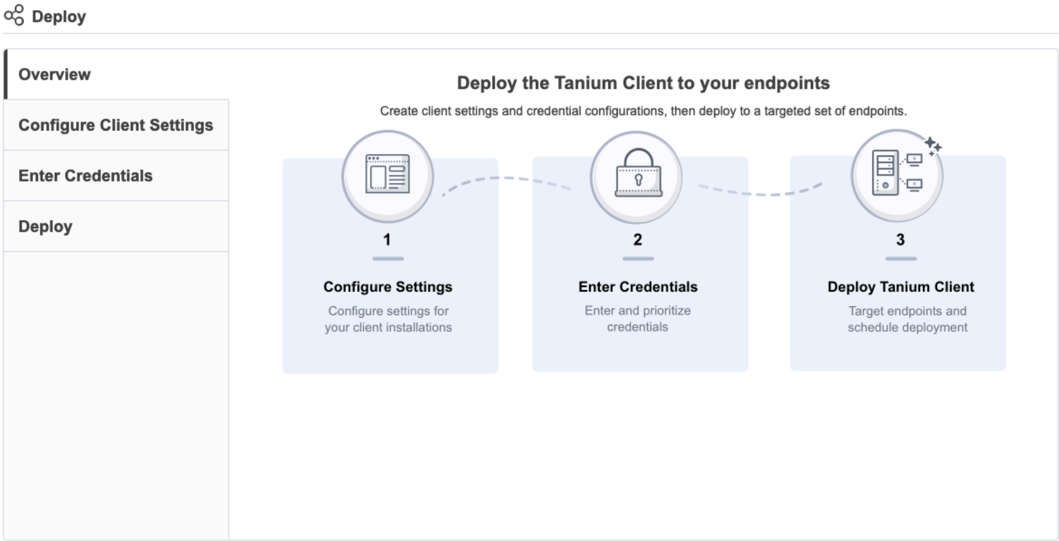
By clicking on the small ⧉ icon in each category, you can then drill down to find the actual endpoints to which the metrics relate.

5. Return back to the Tanium Client Management workbench homepage by opening the pop-out menu on the left and selecting the **Home** option.



6. On the homepage, you will see that there is an overview which describes the workflow for creating a deployment. Each deployment is configured in three stages:

   1. **Configure Client Settings -** Defines a set of client configuration settings. These include the Tanium server names, the client version to be deployed, log verbosity level etc.
   2. **Enter Credentials -** Allows creation of a set of user account credentials used to connect to the endpoints which are to receive client deployments
   3. **Deploy Tanium Client** - Creates a client deployment, which is a definition of which targets should receive the client deployment, which client configuration they should receive, and which credential set should be used to conduct the installation



Deploy the Tanium Client to your endpoints

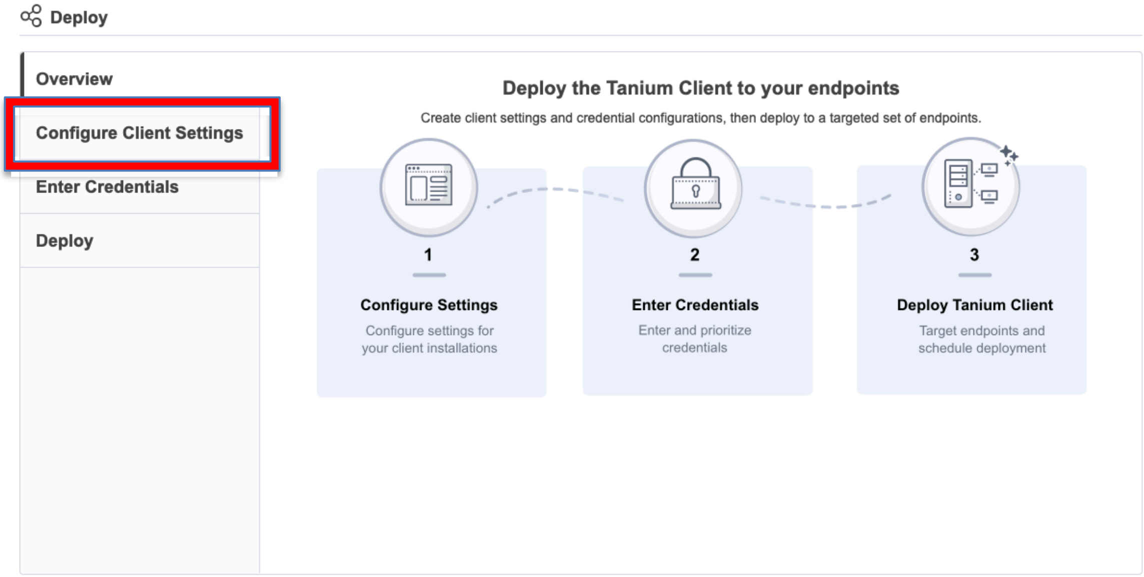
Create client settings and credential configurations, then deploy to a targeted set of endpoints.

1 Configure Settings — Configure settings for your client installations

2 Enter Credentials — Enter and prioritize credentials

3 Deploy Tanium Client — Target endpoints and schedule deployment

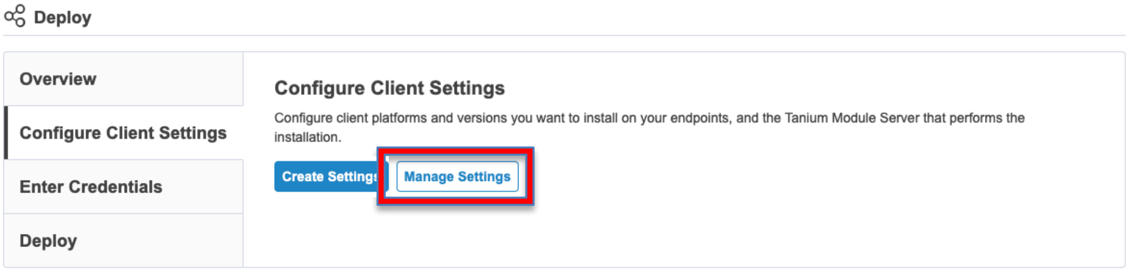
7. Click on **Configure Client Settings**.


Deploy
Overview
Configure Client Settings
Enter Credentials
Deploy
1
Configure Settings
Configure settings for your client installations
2
Enter Credentials
Enter and prioritize credentials
3
Deploy Tanium Client
Target endpoints and schedule deployment

Deploy the Tanium Client to your endpoints

Create client settings and credential configurations, then deploy to a targeted set of endpoints.

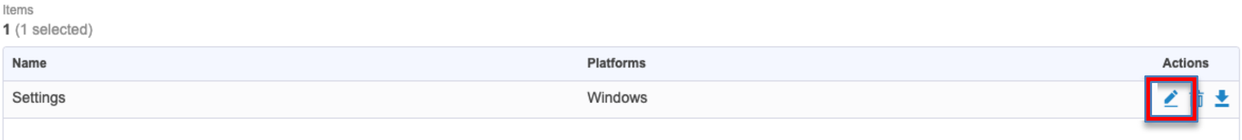
8. Click on **Manage Settings**.



Configure Client Settings

Configure client platforms and versions you want to install on your endpoints, and the Tanium Module Server that performs the installation.

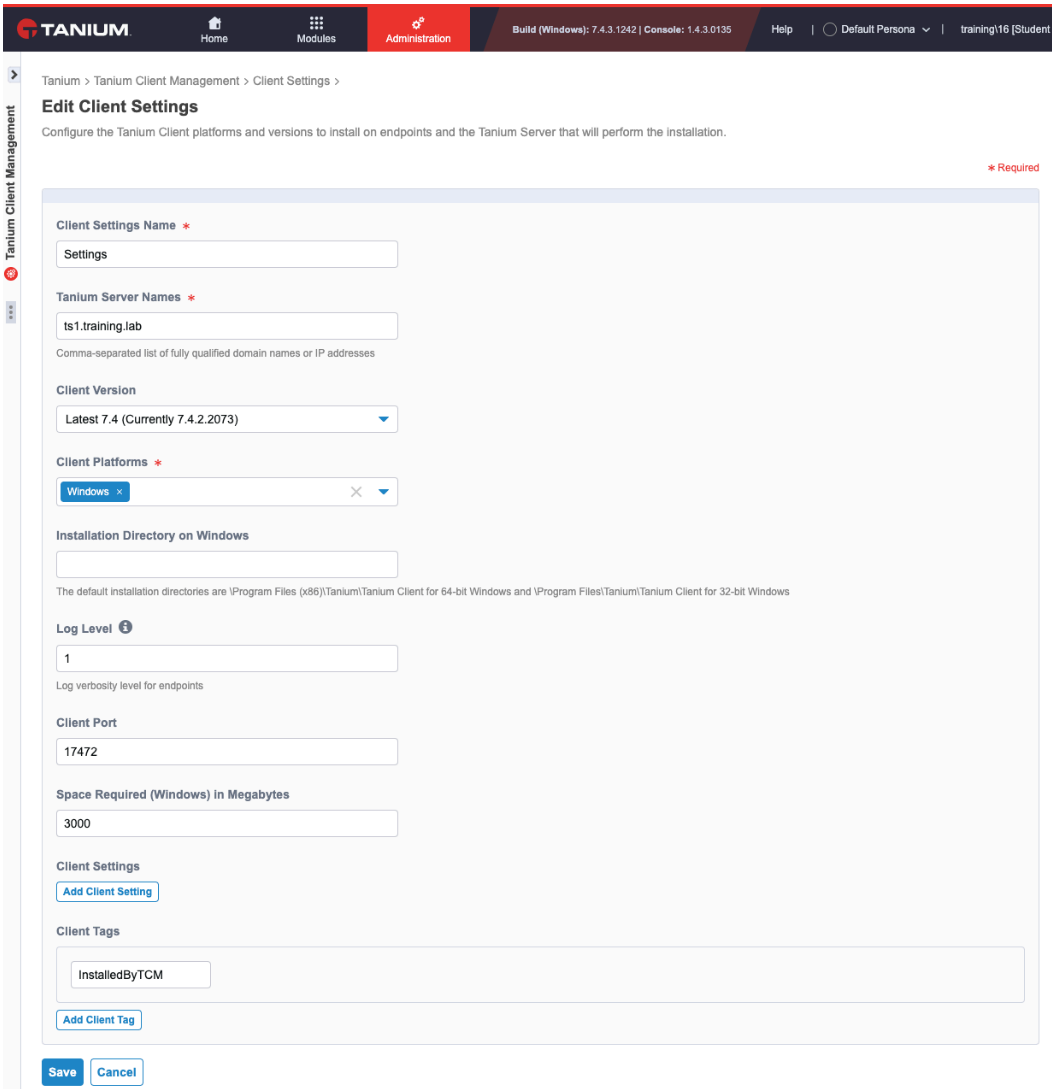
Now click on the little pencil icon to the right-hand side of the settings which are present.



Items
1 (1 selected)

Name	Platforms	Actions
Settings	Windows	✎ 🗑 ⤓

9. Explore the available options.



Tanium > Tanium Client Management > Client Settings >

Edit Client Settings

Configure the Tanium Client platforms and versions to install on endpoints and the Tanium Server that will perform the installation.

* Required

Client Settings Name *: Settings

Tanium Server Names *: ts1.training.lab

Comma-separated list of fully qualified domain names or IP addresses

Client Version: Latest 7.4 (Currently 7.4.2.2073)

Client Platforms *: Windows ×

Installation Directory on Windows:

The default installation directories are \Program Files (x86)\Tanium\Tanium Client for 64-bit Windows and \Program Files\Tanium\Tanium Client for 32-bit Windows

Log Level: 1

Log verbosity level for endpoints

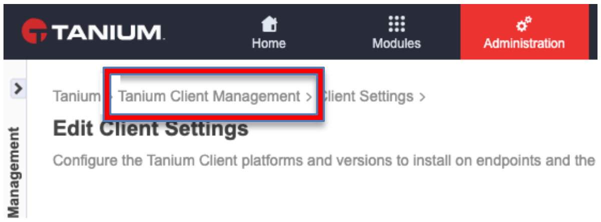
Client Port: 17472

Space Required (Windows) in Megabytes: 3000

Client Settings

Client Tags: InstalledByTCM

Return to the solution homepage using the breadcrumb bar at the top of the page by clicking **Tanium Client Management**.

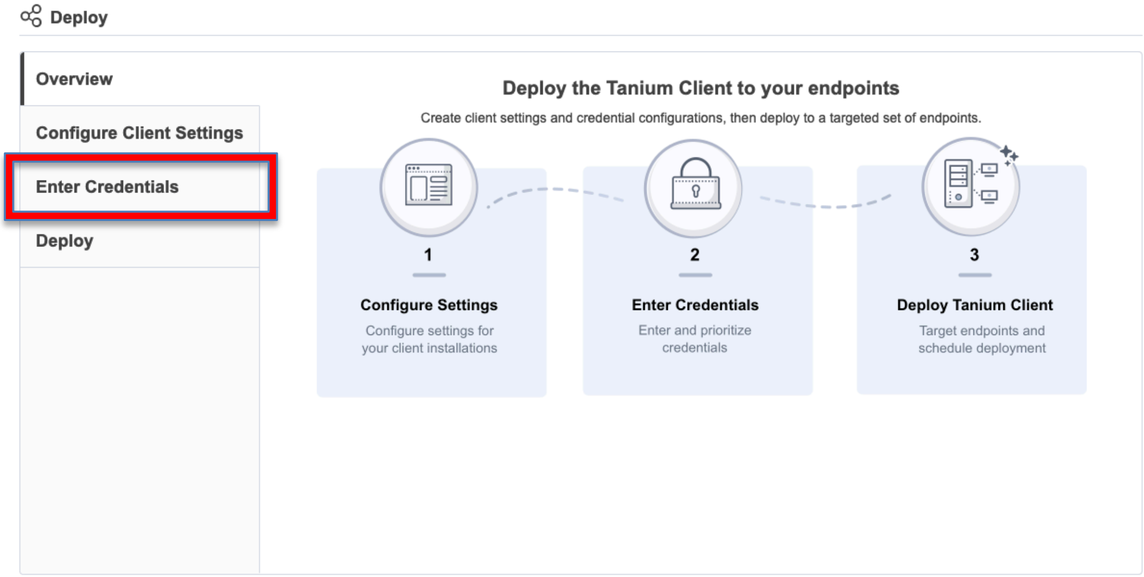


Tanium > Tanium Client Management > Client Settings >

Edit Client Settings

Configure the Tanium Client platforms and versions to install on endpoints and the

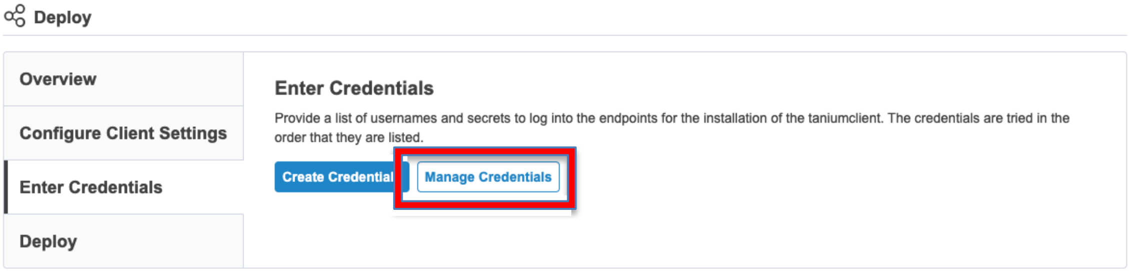
10. Click on **Enter Credentials**.


Deploy
Overview
Configure Client Settings
Enter Credentials
Deploy
1
Configure Settings
Configure settings for your client installations
2
Enter Credentials
Enter and prioritize credentials
3
Deploy Tanium Client
Target endpoints and schedule deployment

Deploy the Tanium Client to your endpoints

Create client settings and credential configurations, then deploy to a targeted set of endpoints.

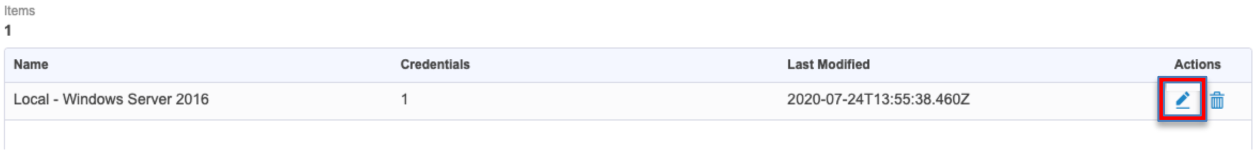
11. Click on **Manage Credentials**.



Enter Credentials

Provide a list of usernames and secrets to log into the endpoints for the installation of the taniumclient. The credentials are tried in the order that they are listed.

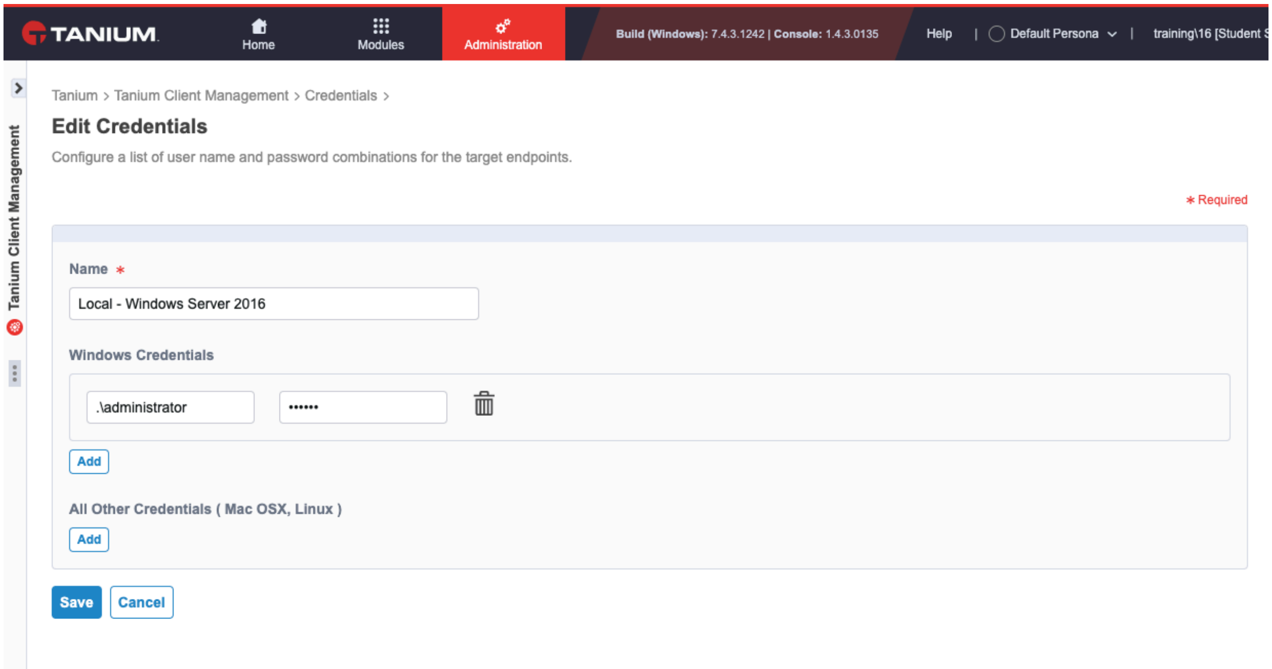
Now click on the little pencil icon on the right-hand side to edit the credential set which is currently configured.



Items
1

Name	Credentials	Last Modified	Actions
Local - Windows Server 2016	1	2020-07-24T13:55:38.460Z	✎ 🗑

12. Explore the available options.



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135

Tanium > Tanium Client Management > Credentials >

Edit Credentials

Configure a list of user name and password combinations for the target endpoints.

* Required

Name * : Local - Windows Server 2016

Windows Credentials: .\administrator ••••••

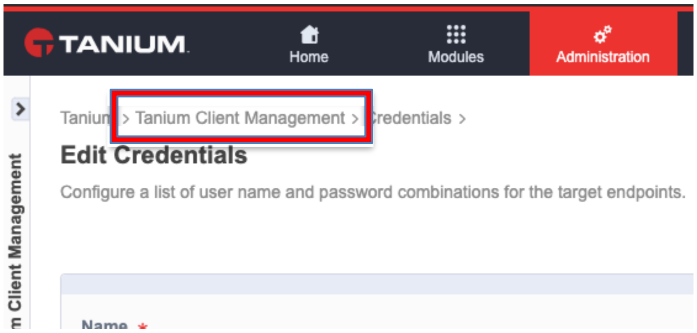
Add

All Other Credentials (Mac OSX, Linux)

Add

Save Cancel

Once you are finished, return back to the solution homepage by using the breadcrumb bar at the top of the page, and clicking **Tanium Client Management**.

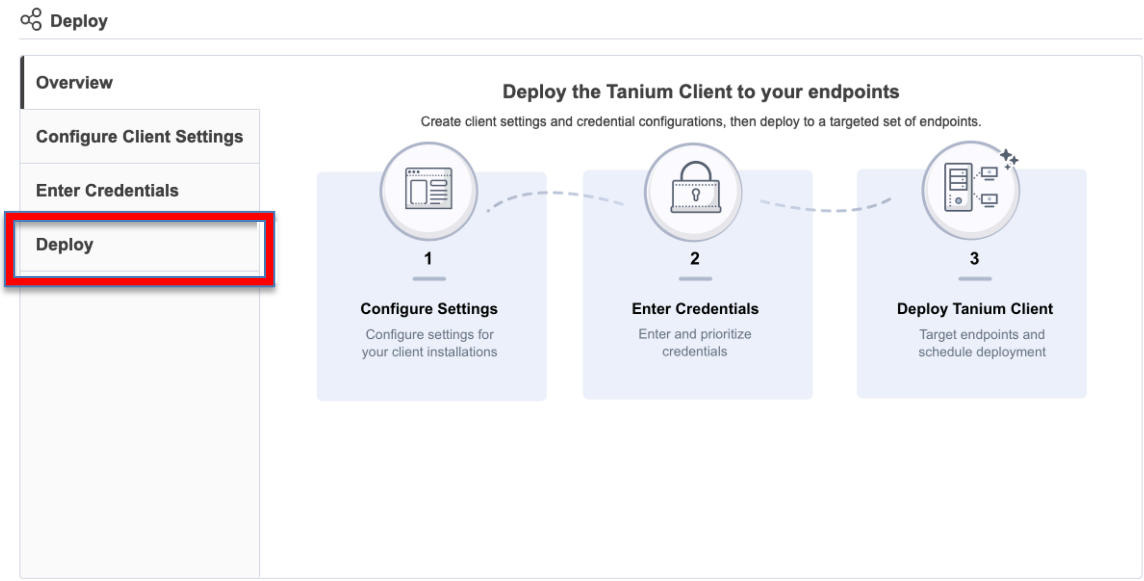


Tanium > Tanium Client Management > Credentials >

Edit Credentials

Configure a list of user name and password combinations for the target endpoints.

13. Click on **Deploy**.

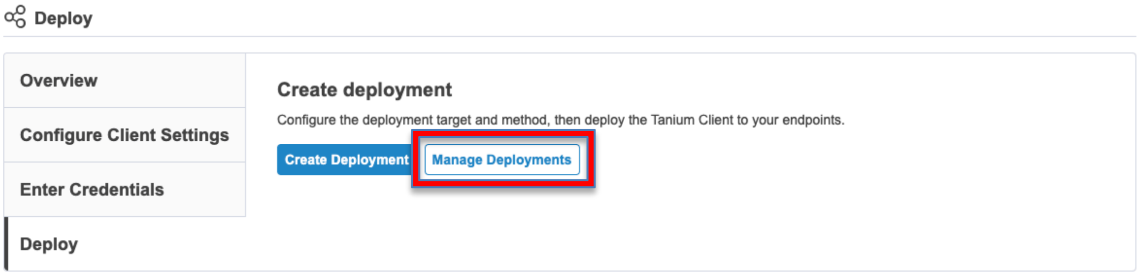

Deploy
Overview
Configure Client Settings
Enter Credentials
Deploy

Deploy the Tanium Client to your endpoints

Create client settings and credential configurations, then deploy to a targeted set of endpoints.

1
Configure Settings
Configure settings for your client installations
2
Enter Credentials
Enter and prioritize credentials
3
Deploy Tanium Client
Target endpoints and schedule deployment

14. Click on **Manage Deployments**.

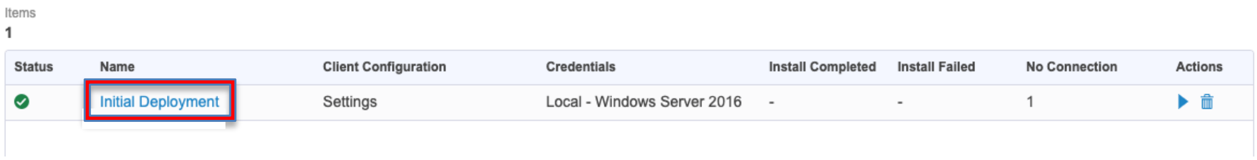


Create deployment

Configure the deployment target and method, then deploy the Tanium Client to your endpoints.

There will be an existing, previous deployment shown. Notice how it shows which Client Configuration and Credentials sets were used as part of the deployment issued, along with a summary of the status of the deployment

Now click on the name of the deployment to take a look at this deployment which has already been defined and executed.

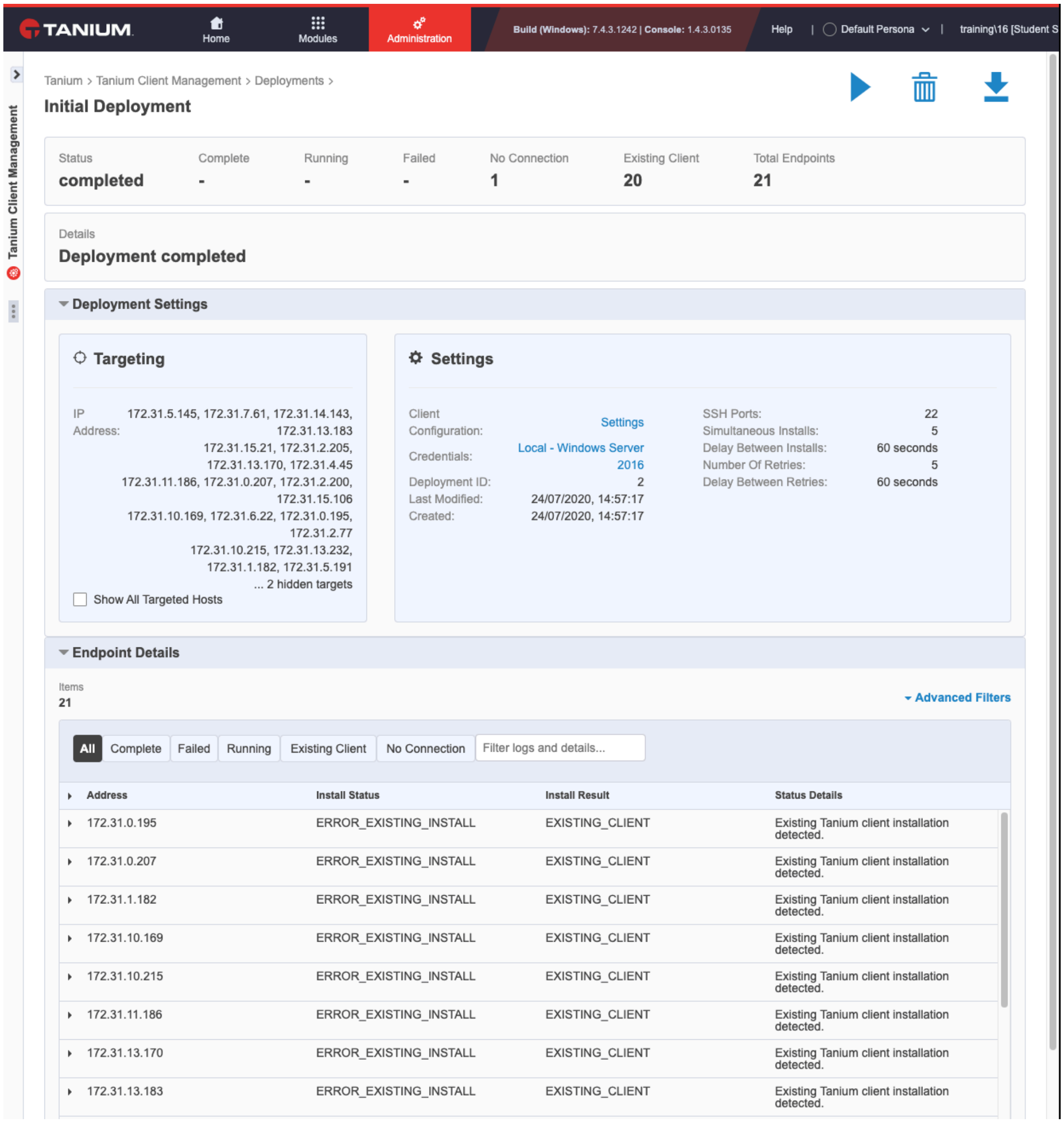


Items
1

Status	Name	Client Configuration	Credentials	Install Completed	Install Failed	No Connection	Actions
✓	Initial Deployment	Settings	Local - Windows Server 2016	-	-	1	▶ 🗑

15. You will now see a more detailed breakdown of the deployment status including:

- The configuration used, including how many simultaneous client installs can occur at the same time and how may retries should be attempted
- The endpoints which were targeted in this deployment
- Detailed results of each client install on each individual endpoint targeted



Tanium > Tanium Client Management > Deployments >

Initial Deployment

Status	Complete	Running	Failed	No Connection	Existing Client	Total Endpoints
completed	-	-	-	1	20	21

Details

Deployment completed

Deployment Settings

Targeting

IP Address: 172.31.5.145, 172.31.7.61, 172.31.14.143, 172.31.13.183
172.31.15.21, 172.31.2.205, 172.31.13.170, 172.31.4.45
172.31.11.186, 172.31.0.207, 172.31.2.200, 172.31.15.106
172.31.10.169, 172.31.6.22, 172.31.0.195, 172.31.2.77
172.31.10.215, 172.31.13.232, 172.31.1.182, 172.31.5.191
... 2 hidden targets

□ Show All Targeted Hosts

Settings

Client Configuration: Settings
Credentials: Local - Windows Server 2016
Deployment ID: 2
Last Modified: 24/07/2020, 14:57:17
Created: 24/07/2020, 14:57:17

SSH Ports: 22
Simultaneous Installs: 5
Delay Between Installs: 60 seconds
Number Of Retries: 5
Delay Between Retries: 60 seconds

Endpoint Details

Items
21

Advanced Filters

Address	Install Status	Install Result	Status Details
172.31.0.195	ERROR_EXISTING_INSTALL	EXISTING_CLIENT	Existing Tanium client installation detected.
172.31.0.207	ERROR_EXISTING_INSTALL	EXISTING_CLIENT	Existing Tanium client installation detected.
172.31.1.182	ERROR_EXISTING_INSTALL	EXISTING_CLIENT	Existing Tanium client installation detected.
172.31.10.169	ERROR_EXISTING_INSTALL	EXISTING_CLIENT	Existing Tanium client installation detected.
172.31.10.215	ERROR_EXISTING_INSTALL	EXISTING_CLIENT	Existing Tanium client installation detected.
172.31.11.186	ERROR_EXISTING_INSTALL	EXISTING_CLIENT	Existing Tanium client installation detected.
172.31.13.170	ERROR_EXISTING_INSTALL	EXISTING_CLIENT	Existing Tanium client installation detected.
172.31.13.183	ERROR_EXISTING_INSTALL	EXISTING_CLIENT	Existing Tanium client installation detected.

Review this page.

You have now completed Lab 4.

Lab 5: Roll Call

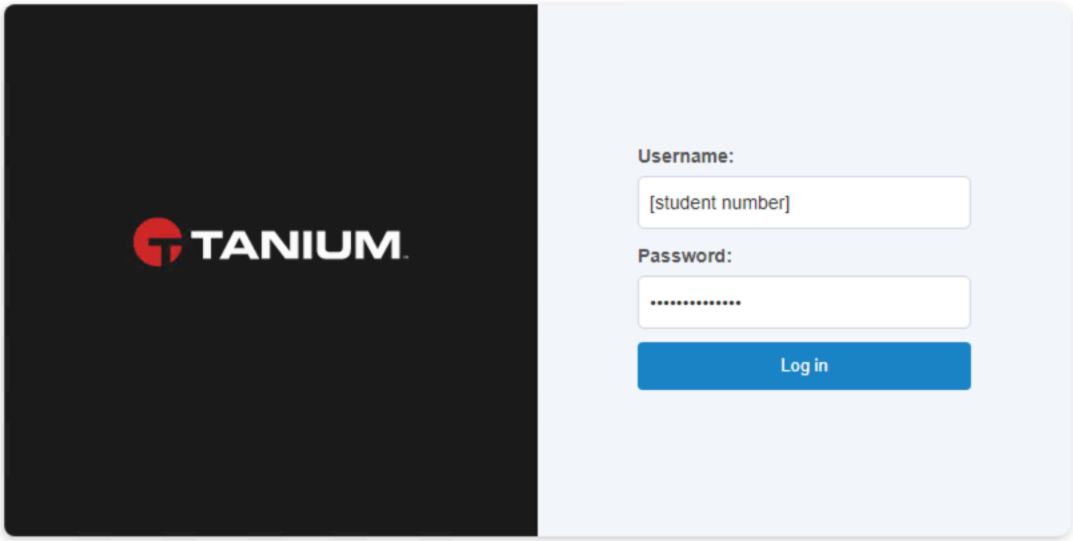
Getting the low down on your managed endpoints using Tanium Asset

Objectives

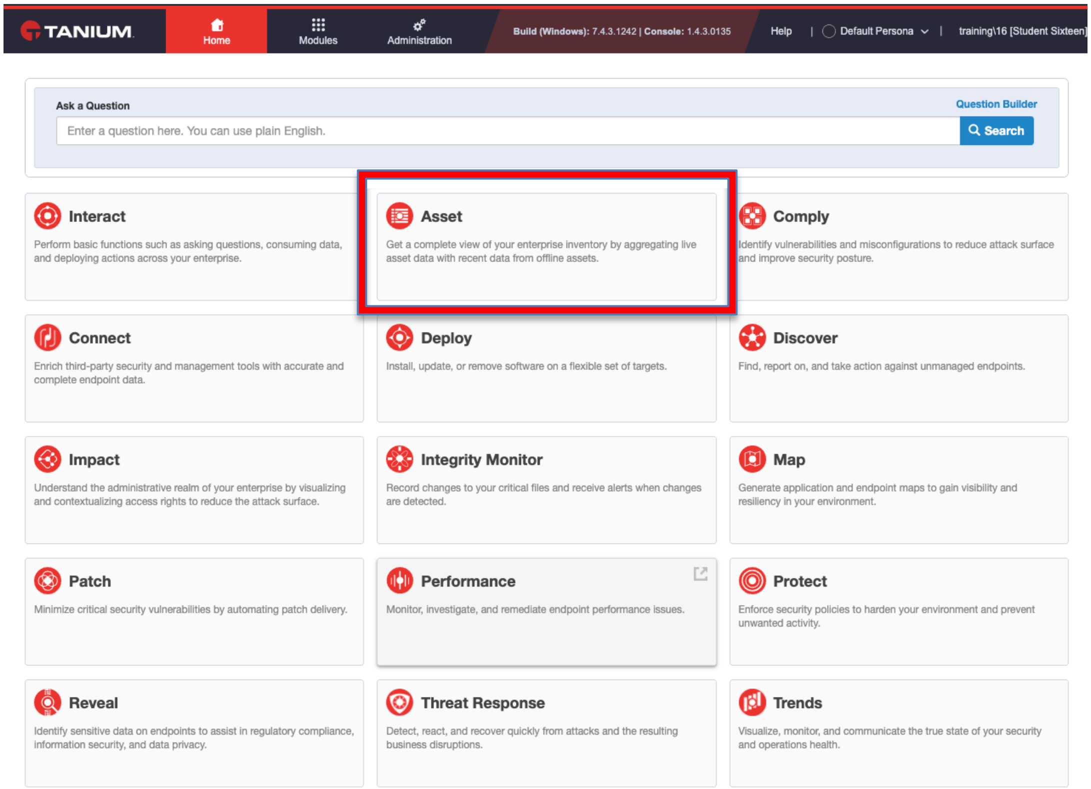
By the end of this lab you will have completed the following objectives:

- Create your own report in Tanium Asset
- Use Tanium Connect to export asset data to a SQL database

Lab Steps

1.	Using the URL provided, open the Tanium console and enter your credentials  Username: [student number] Password: ••••••••••••••

2. If you are not already at the homepage, click the Tanium logo top-left to return there. Click on the **Asset** "baseball card" to enter the Tanium Asset module workbench.



TANIUM | Home | Modules | Administration | **Build (Windows):** 7.4.3.1242 | **Console:** 1.4.3.0135 | Help | Default Persona | training\16 [Student Sixteen]

Ask a Question — Question Builder

Enter a question here. You can use plain English. — Search

Interact — Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise.

Asset — Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets.

Comply — Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.

Connect — Enrich third-party security and management tools with accurate and complete endpoint data.

Deploy — Install, update, or remove software on a flexible set of targets.

Discover — Find, report on, and take action against unmanaged endpoints.

Impact — Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface.

Integrity Monitor — Record changes to your critical files and receive alerts when changes are detected.

Map — Generate application and endpoint maps to gain visibility and resiliency in your environment.

Patch — Minimize critical security vulnerabilities by automating patch delivery.

Performance — Monitor, investigate, and remediate endpoint performance issues.

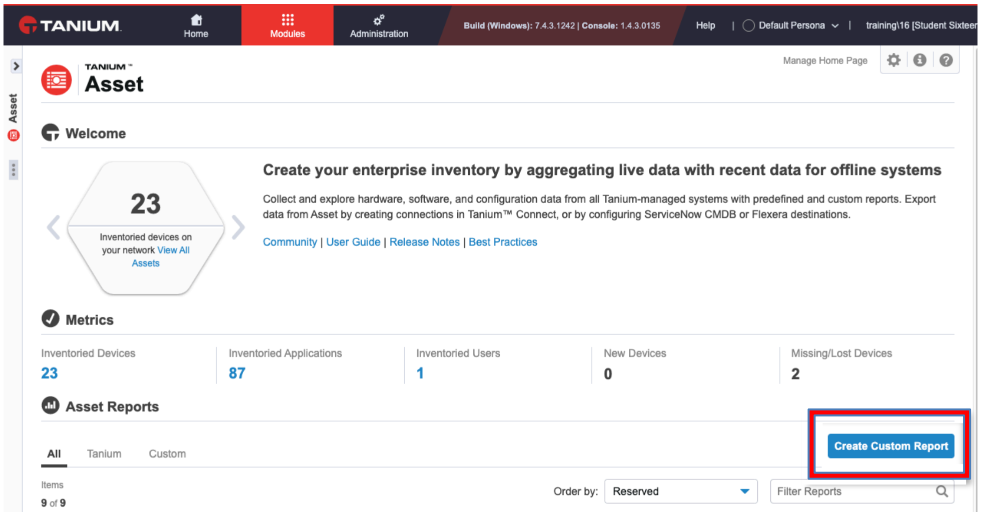
Protect — Enforce security policies to harden your environment and prevent unwanted activity.

Reveal — Identify sensitive data on endpoints to assist in regulatory compliance, information security, and data privacy.

Threat Response — Detect, react, and recover quickly from attacks and the resulting business disruptions.

Trends — Visualize, monitor, and communicate the true state of your security and operations health.

3. Review the Asset workbench. You will see some detail on the asset data import schedule, module health and you will also see a list of reports that can be run. At the top are some metrics around the asset data being collected as shown below. Click on **Create Custom Report** to continue.



TANIUM | Home | Modules | Administration | **Build (Windows):** 7.4.3.1242 | **Console:** 1.4.3.0135 | Help | Default Persona | training\16 [Student Sixteen]

TANIUM™ **Asset** — Manage Home Page

Welcome

23 — Inventoried devices on your network View All Assets

Create your enterprise inventory by aggregating live data with recent data for offline systems

Collect and explore hardware, software, and configuration data from all Tanium-managed systems with predefined and custom reports. Export data from Asset by creating connections in Tanium™ Connect, or by configuring ServiceNow CMDB or Flexera destinations.

Community | User Guide | Release Notes | Best Practices

Metrics

Inventoried Devices	Inventoried Applications	Inventoried Users	New Devices	Missing/Lost Devices
23	87	1	0	2

Asset Reports — Create Custom Report

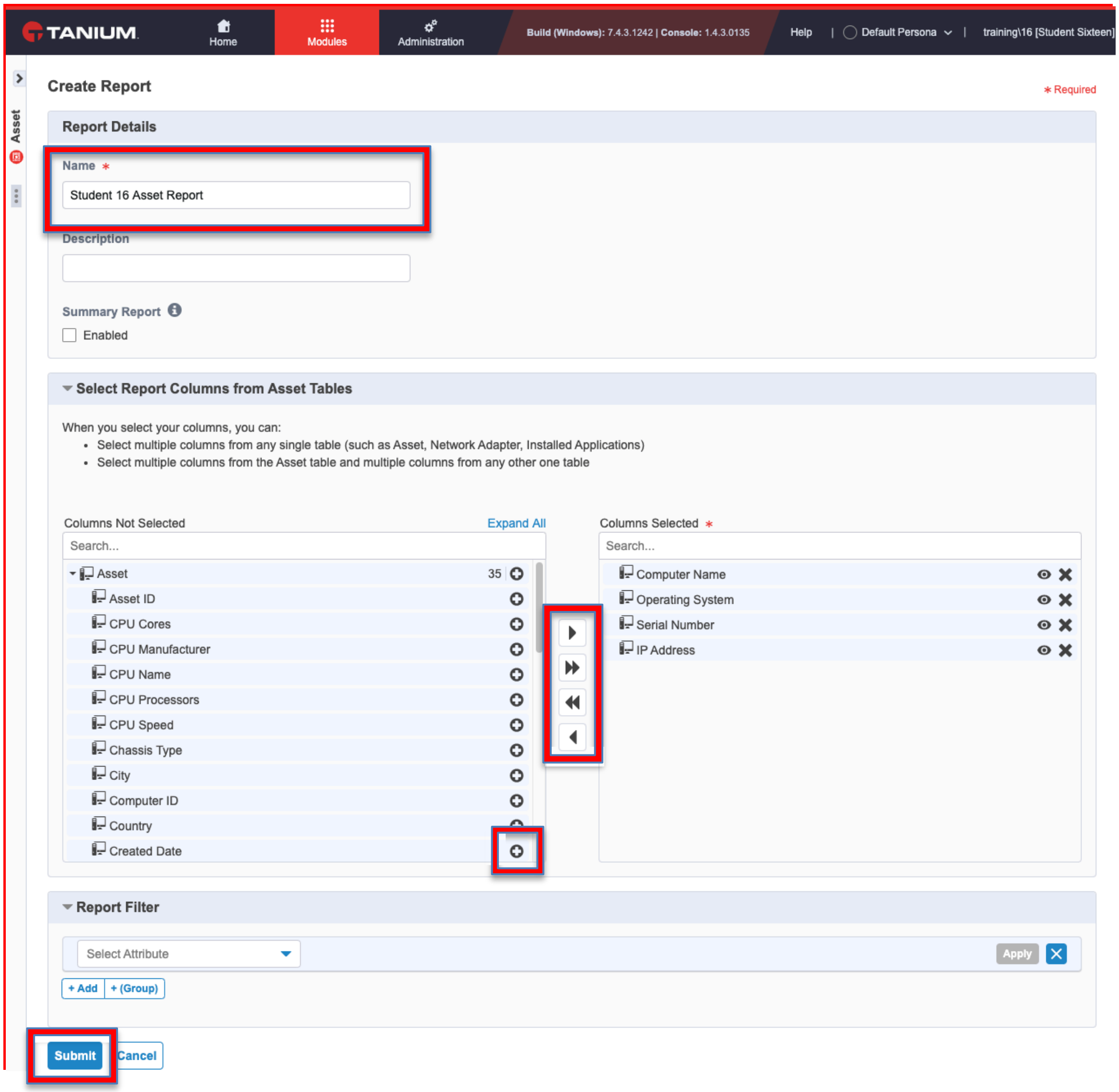
All | Tanium | Custom

Items 9 of 9 — Order by: Reserved — Filter Reports

4. Enter the name of the report as *Student <Student ID Number> Asset Report*.

From the **Select Report Columns from Asset Tables** section, choose the following columns, all from the **Asset** category by either selecting the column and using the arrow icons in the middle, or clicking on the ⊕ icon next to the desired column name:

- Computer Name
- Operating System
- Serial Number
- IP Address



Name * Student 16 Asset Report

When you select your columns, you can:

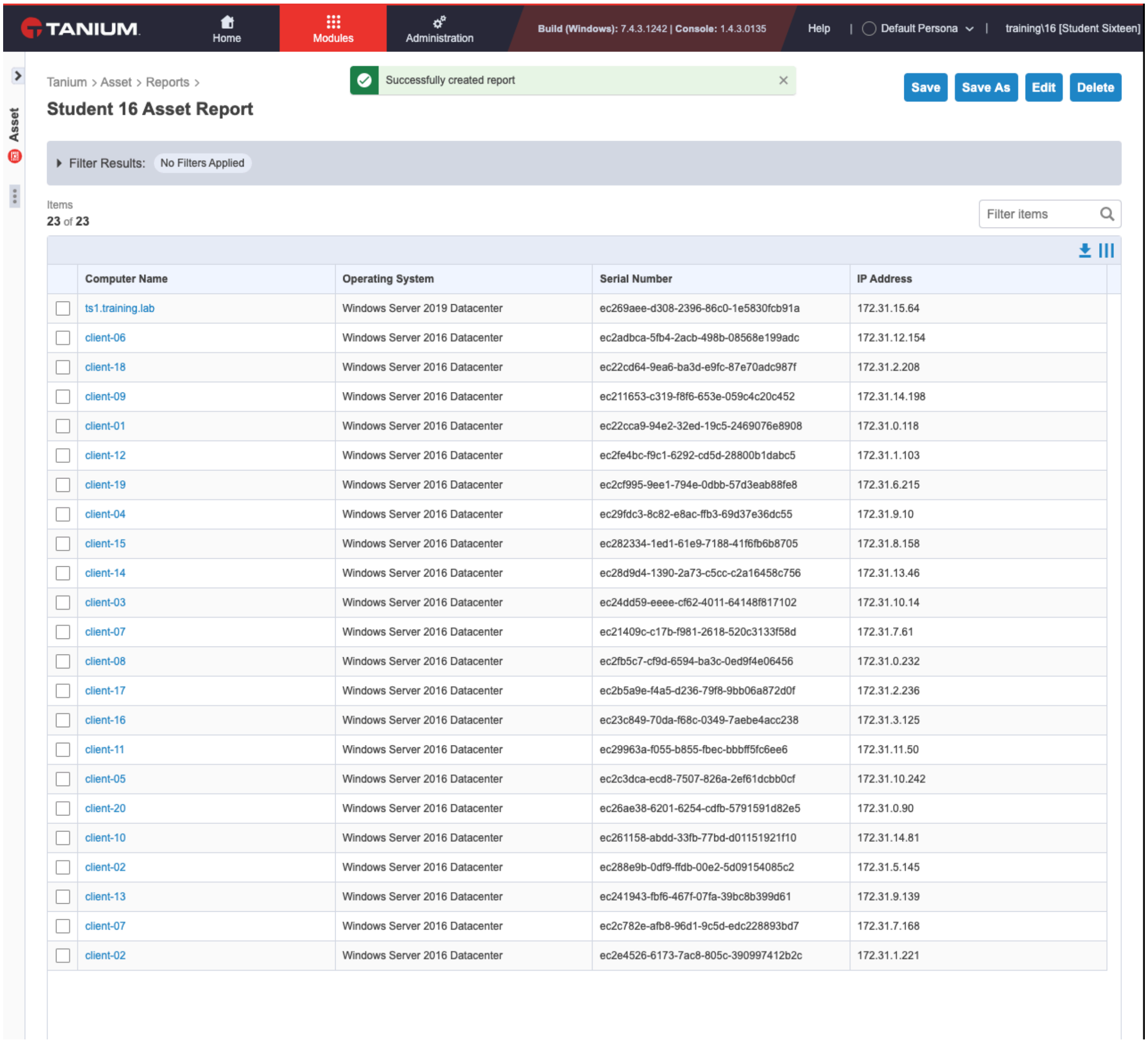
- Select multiple columns from any single table (such as Asset, Network Adapter, Installed Applications)
- Select multiple columns from the Asset table and multiple columns from any other one table

Columns Selected:

- Computer Name
- Operating System
- Serial Number
- IP Address

Click on **Submit** once complete.

5. Your new report will now be created and displayed.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Asset
Save
Save As
Edit
Delete

Tanium > Asset > Reports >

Successfully created report

Student 16 Asset Report

Filter Results: No Filters Applied

Items
23 of 23

Filter items

	Computer Name	Operating System	Serial Number	IP Address
□	ts1.training.lab	Windows Server 2019 Datacenter	ec269aee-d308-2396-86c0-1e5830fcb91a	172.31.15.64
□	client-06	Windows Server 2016 Datacenter	ec2adbca-5fb4-2acb-498b-08568e199adc	172.31.12.154
□	client-18	Windows Server 2016 Datacenter	ec22cd64-9ea6-ba3d-e9fc-87e70adc987f	172.31.2.208
□	client-09	Windows Server 2016 Datacenter	ec211653-c319-f8f6-653e-059c4c20c452	172.31.14.198
□	client-01	Windows Server 2016 Datacenter	ec22cca9-94e2-32ed-19c5-2469076e8908	172.31.0.118
□	client-12	Windows Server 2016 Datacenter	ec2fe4bc-f9c1-6292-cd5d-28800b1dabc5	172.31.1.103
□	client-19	Windows Server 2016 Datacenter	ec2cf995-9ee1-794e-0dbb-57d3eab88fe8	172.31.6.215
□	client-04	Windows Server 2016 Datacenter	ec29fdc3-8c82-e8ac-ffb3-69d37e36dc55	172.31.9.10
□	client-15	Windows Server 2016 Datacenter	ec282334-1ed1-61e9-7188-41f6fb6b8705	172.31.8.158
□	client-14	Windows Server 2016 Datacenter	ec28d9d4-1390-2a73-c5cc-c2a16458c756	172.31.13.46
□	client-03	Windows Server 2016 Datacenter	ec24dd59-eeee-cf62-4011-64148f817102	172.31.10.14
□	client-07	Windows Server 2016 Datacenter	ec21409c-c17b-f981-2618-520c3133f58d	172.31.7.61
□	client-08	Windows Server 2016 Datacenter	ec2fb5c7-cf9d-6594-ba3c-0ed9f4e06456	172.31.0.232
□	client-17	Windows Server 2016 Datacenter	ec2b5a9e-f4a5-d236-79f8-9bb06a872d0f	172.31.2.236
□	client-16	Windows Server 2016 Datacenter	ec23c849-70da-f68c-0349-7aebe4acc238	172.31.3.125
□	client-11	Windows Server 2016 Datacenter	ec29963a-f055-b855-fbec-bbbff5fc6ee6	172.31.11.50
□	client-05	Windows Server 2016 Datacenter	ec2c3dca-ecd8-7507-826a-2ef61dcbb0cf	172.31.10.242
□	client-20	Windows Server 2016 Datacenter	ec26ae38-6201-6254-cdfb-5791591d82e5	172.31.0.90
□	client-10	Windows Server 2016 Datacenter	ec261158-abdd-33fb-77bd-d01151921f10	172.31.14.81
□	client-02	Windows Server 2016 Datacenter	ec288e9b-0df9-ffdb-00e2-5d09154085c2	172.31.5.145
□	client-13	Windows Server 2016 Datacenter	ec241943-fbf6-467f-07fa-39bc8b399d61	172.31.9.139
□	client-07	Windows Server 2016 Datacenter	ec2c782e-afb8-96d1-9c5d-edc228893bd7	172.31.7.168
□	client-02	Windows Server 2016 Datacenter	ec2e4526-6173-7ac8-805c-390997412b2c	172.31.1.221

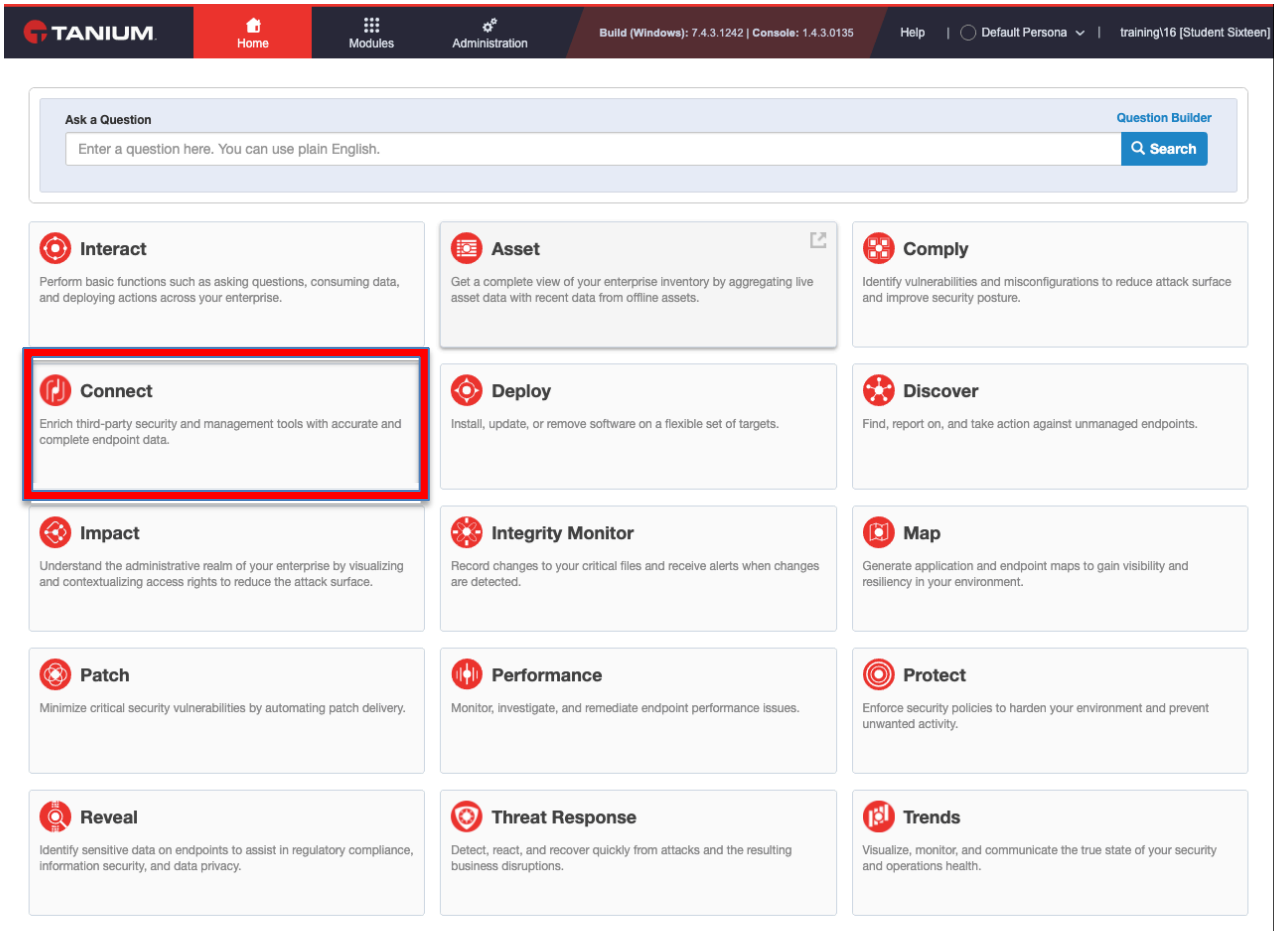
Review the report.

6. **The following steps are optional and will not be covered by the instructor. If you have the time then have a go at completing them!**

What else can we do with the data that Tanium is collecting? Whether it is your Asset data or any other data, Tanium support integrations into many third-party solutions.

Now we'll take your saved question from the earlier lab and push this data into a database. However, as a 'rule of thumb' almost any data from Tanium can be integrated into a third-party solution, including the Asset report you just created.

Return to the Tanium homepage and click on **Connect** module card. The Connect module is the interface between the Tanium platform and 3rd-party systems.



TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Ask a Question
Question Builder
Enter a question here. You can use plain English.
Search

Interact
Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise.

Asset
Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets.

Comply
Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.

Connect
Enrich third-party security and management tools with accurate and complete endpoint data.

Deploy
Install, update, or remove software on a flexible set of targets.

Discover
Find, report on, and take action against unmanaged endpoints.

Impact
Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface.

Integrity Monitor
Record changes to your critical files and receive alerts when changes are detected.

Map
Generate application and endpoint maps to gain visibility and resiliency in your environment.

Patch
Minimize critical security vulnerabilities by automating patch delivery.

Performance
Monitor, investigate, and remediate endpoint performance issues.

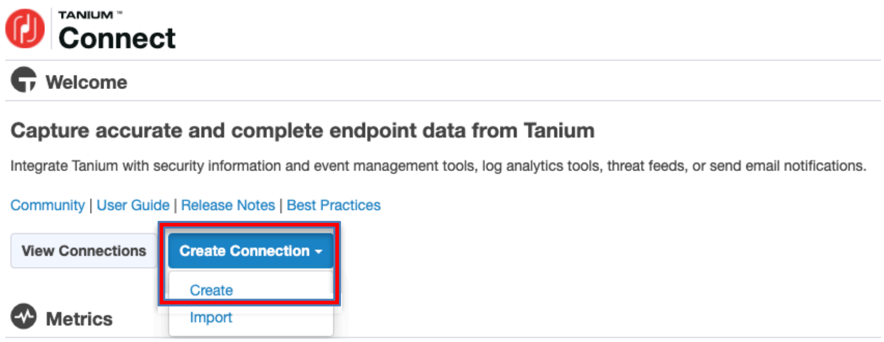
Protect
Enforce security policies to harden your environment and prevent unwanted activity.

Reveal
Identify sensitive data on endpoints to assist in regulatory compliance, information security, and data privacy.

Threat Response
Detect, react, and recover quickly from attacks and the resulting business disruptions.

Trends
Visualize, monitor, and communicate the true state of your security and operations health.

7. Press the **Create Connection** button and then click on **Create**.



TANIUM Connect

Welcome

Capture accurate and complete endpoint data from Tanium

Integrate Tanium with security information and event management tools, log analytics tools, threat feeds, or send email notifications.

8. From the **Create Connection** screen, populate the following fields with the below data leaving all other fields as their default setting:

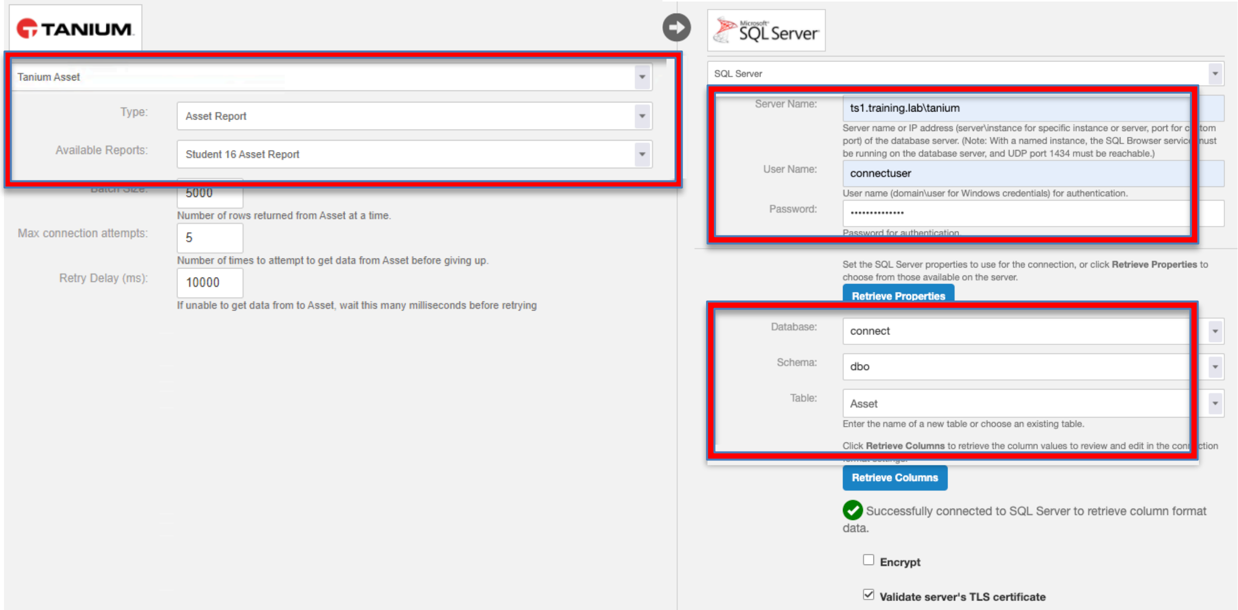
- **Name**: Student <Student ID Number> SQL Connection
- **Source**: Tanium Asset
- **Type**: Asset Report
- **Available Reports**: <your Asset report created previously>

- **Destination**: SQL Server (browse the list to see other destinations available)
- **Server Name**: ts1.training.lab\tanium
- **User Name**: connectuser
- **Password**: <your Tanium password>

Now press **Retrieve Properties**, then set the following values:

- **Database**: connect
- **Scheme**: dbo
- **Table**: dbo.Asset

Press the **Retrieve Columns** button now.



Tanium Asset

Type: Asset Report

Available Reports: Student 16 Asset Report

Batch Size: 5000

Number of rows returned from Asset at a time.

Max connection attempts: 5

Number of times to attempt to get data from Asset before giving up.

Retry Delay (ms): 10000

If unable to get data from to Asset, wait this many milliseconds before retrying

SQL Server

Server Name: ts1.training.lab\tanium

Server name or IP address (server\instance for specific instance or server, port for custom port) of the database server. (Note: With a named instance, the SQL Browser service must be running on the database server, and UDP port 1434 must be reachable.)

User Name: connectuser

User name (domain\user for Windows credentials) for authentication.

Password: ....

Password for authentication.

Set the SQL Server properties to use for the connection, or click **Retrieve Properties** to choose from those available on the server.

Database: connect

Schema: dbo

Table: Asset

Enter the name of a new table or choose an existing table.

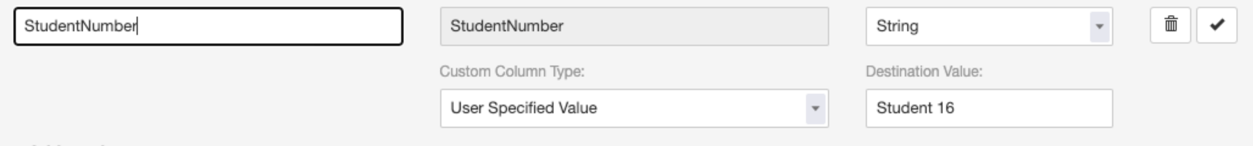
Click **Retrieve Columns** to retrieve the column values to review and edit in the connection format settings.

✓ Successfully connected to SQL Server to retrieve column format data.

□ **Encrypt**

☑ **Validate server's TLS certificate**

9. Scroll down further and expand the Columns section. Press the **+ Add a column** item and configure it as below, substituting in your own student ID number.



StudentNumber

StudentNumber

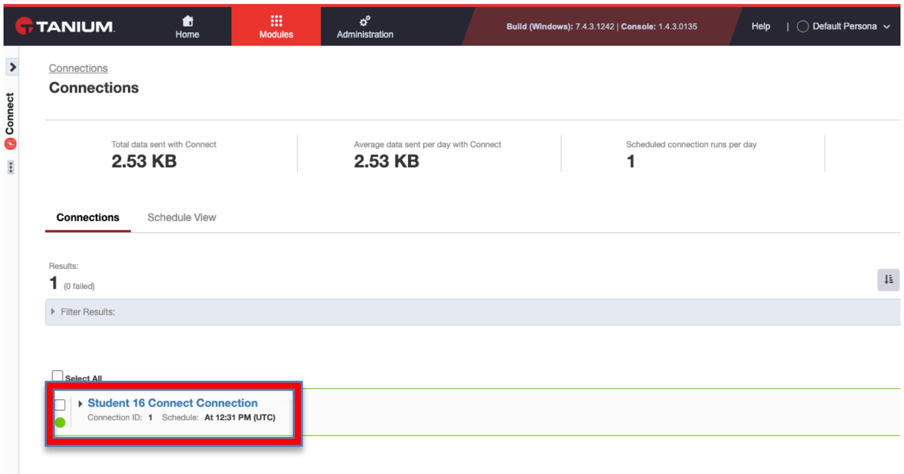
String

Custom Column Type: User Specified Value

Destination Value: Student 16

Accept the changes using the tick button, and then scroll down and press the **Create Connection** button.

10. You will be returned to the summary screen where you should see your newly created connection.



Connections

Connections

Total data sent with Connect 2.53 KB

Average data sent per day with Connect 2.53 KB

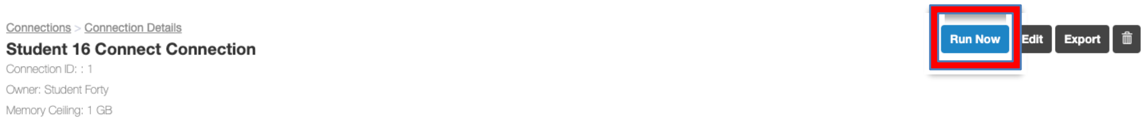
Scheduled connection runs per day 1

Results: 1 (0 failed)

Student 16 Connect Connection

Connection ID: 1 Schedule: At 12:31 PM (UTC)

Click on your connection and then on the **Run Now** button on the following screen that loads and confirm the action. This will now run the Saved Question and send the data through Connect to the SQL Server.



Connections > Connection Details

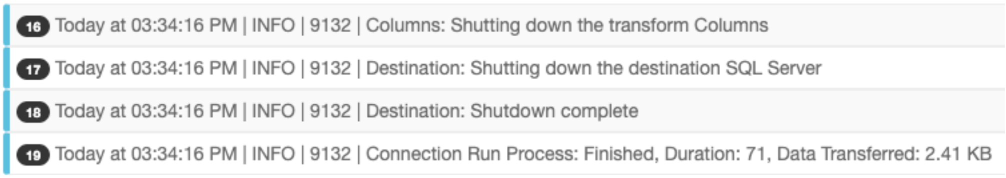
Student 16 Connect Connection

Connection ID: : 1

Owner: Student Forty

Memory Ceiling: 1 GB

You can follow the summary log screen that will be displayed to watch as the process executes.



```
16 Today at 03:34:16 PM | INFO | 9132 | Columns: Shutting down the transform Columns
17 Today at 03:34:16 PM | INFO | 9132 | Destination: Shutting down the destination SQL Server
18 Today at 03:34:16 PM | INFO | 9132 | Destination: Shutdown complete
19 Today at 03:34:16 PM | INFO | 9132 | Connection Run Process: Finished, Duration: 71, Data Transferred: 2.41 KB
```

You have now completed Lab 5.

Lab 6: Schedules and Snipers

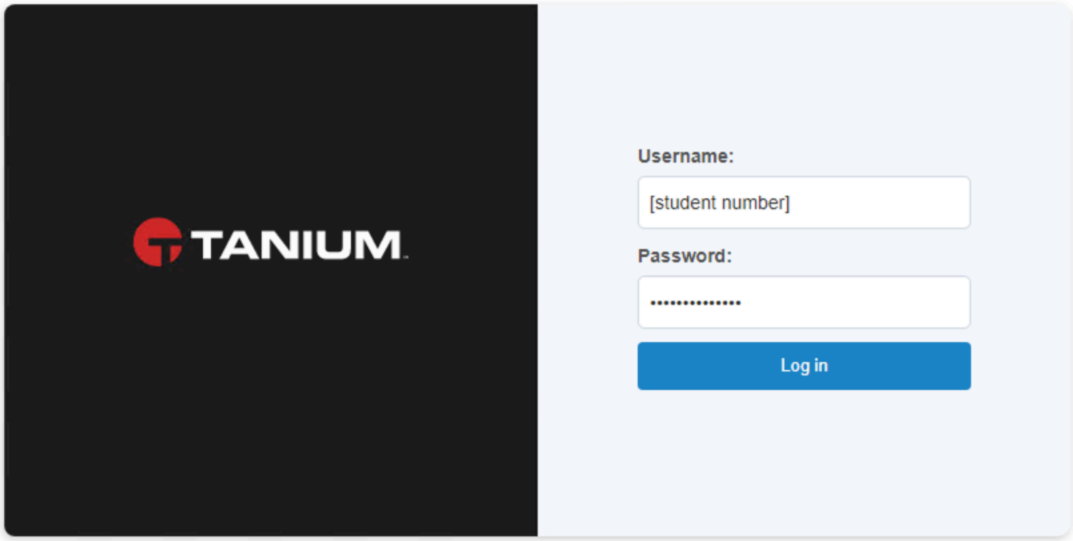
Getting up to date with Tanium Patch.

Objectives

By the end of this lab you will have completed the following objectives:

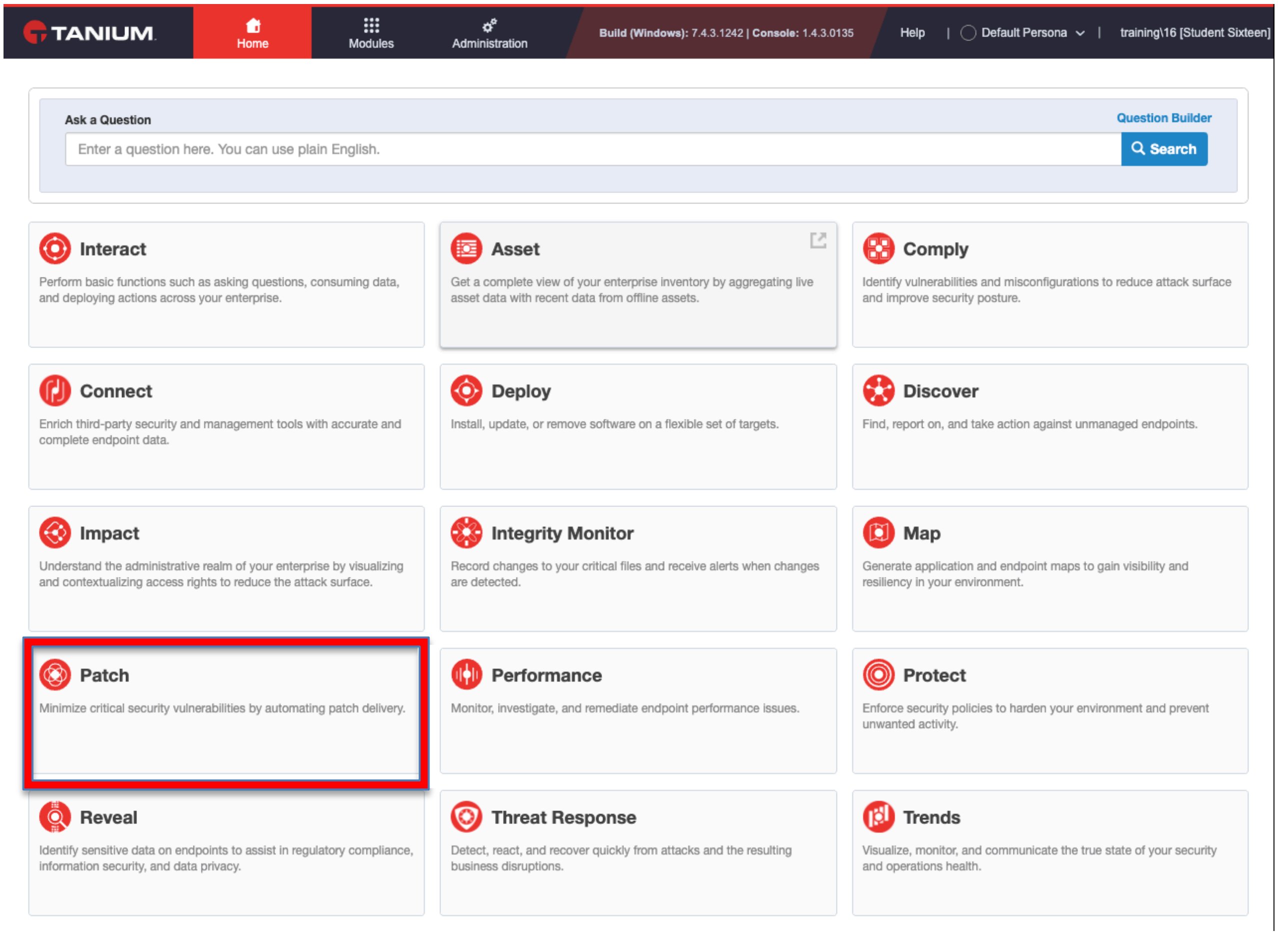
- Review Tanium Scan for Windows configuration
- Sniper patching
  - **Students 1 – 20** : Deploy KB890830
  - **Students 21 – 40** : Deploy KB4565511
- Track progress of patching

Lab Steps

1.	Using the URL provided, open the Tanium console and enter your credentials  Username: [student number] Password: ••••••••••••••

2. Click on the **Tanium** logo at the top left-hand corner to return you to the home page if you aren't there already.

You should see the homepage of the Tanium console, displaying the various "baseball cards" for the available modules. From here, click on **Patch**.



Build (Windows): 7.4.3.1242 | **Console:** 1.4.3.0135

training\16 [Student Sixteen]

Ask a Question

Enter a question here. You can use plain English.

Interact
Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise.

Asset
Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets.

Comply
Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.

Connect
Enrich third-party security and management tools with accurate and complete endpoint data.

Deploy
Install, update, or remove software on a flexible set of targets.

Discover
Find, report on, and take action against unmanaged endpoints.

Impact
Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface.

Integrity Monitor
Record changes to your critical files and receive alerts when changes are detected.

Map
Generate application and endpoint maps to gain visibility and resiliency in your environment.

Patch
Minimize critical security vulnerabilities by automating patch delivery.

Performance
Monitor, investigate, and remediate endpoint performance issues.

Protect
Enforce security policies to harden your environment and prevent unwanted activity.

Reveal
Identify sensitive data on endpoints to assist in regulatory compliance, information security, and data privacy.

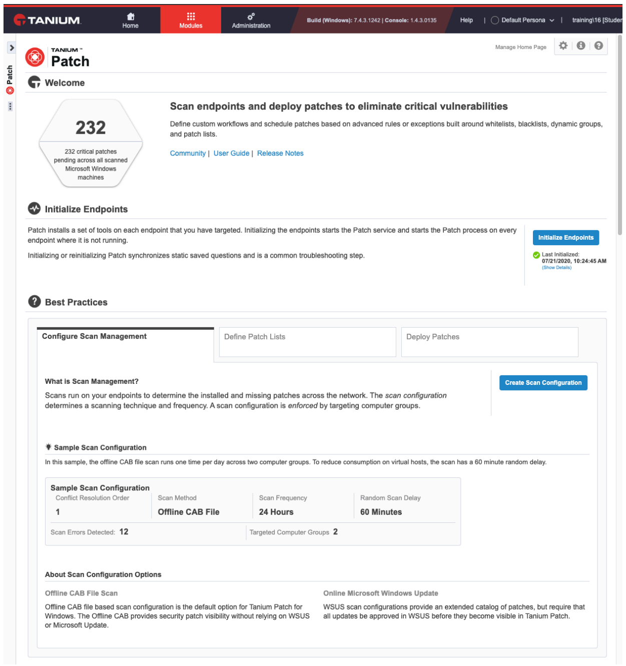
Threat Response
Detect, react, and recover quickly from attacks and the resulting business disruptions.

Trends
Visualize, monitor, and communicate the true state of your security and operations health.

This will now take you to the Patch workbench.

3. Explore the Patch workbench. Here you will find details on:

- Best Practices
- Patch management health
- Scheduled patching activity
- Patching metrics
- High level reports on patch applicability.



Welcome

232

232 critical patches pending across all scanned Microsoft Windows machines

Scan endpoints and deploy patches to eliminate critical vulnerabilities

Define custom workflows and schedule patches based on advanced rules or exceptions built around whitelists, blacklists, dynamic groups, and patch lists.

Community | User Guide | Release Notes

Initialize Endpoints

Patch installs a set of tools on each endpoint that you have targeted. Initializing the endpoints starts the Patch service and starts the Patch process on every endpoint where it is not running.

Initializing or reinitializing Patch synchronizes static saved questions and is a common troubleshooting step.

Initialize Endpoints

Last Initialized: 07/21/2020, 10:24:45 AM (Show Details)

Best Practices

Configure Scan Management | Define Patch Lists | Deploy Patches

What is Scan Management?

Scans run on your endpoints to determine the installed and missing patches across the network. The *scan configuration* determines a scanning technique and frequency. A scan configuration is *enforced* by targeting computer groups.

Create Scan Configuration

Sample Scan Configuration

In this sample, the offline CAB file scan runs one time per day across two computer groups. To reduce consumption on virtual hosts, the scan has a 60 minute random delay.

Sample Scan Configuration

Conflict Resolution Order	Scan Method	Scan Frequency	Random Scan Delay
1	Offline CAB File	24 Hours	60 Minutes

Scan Errors Detected: 12 | Targeted Computer Groups 2

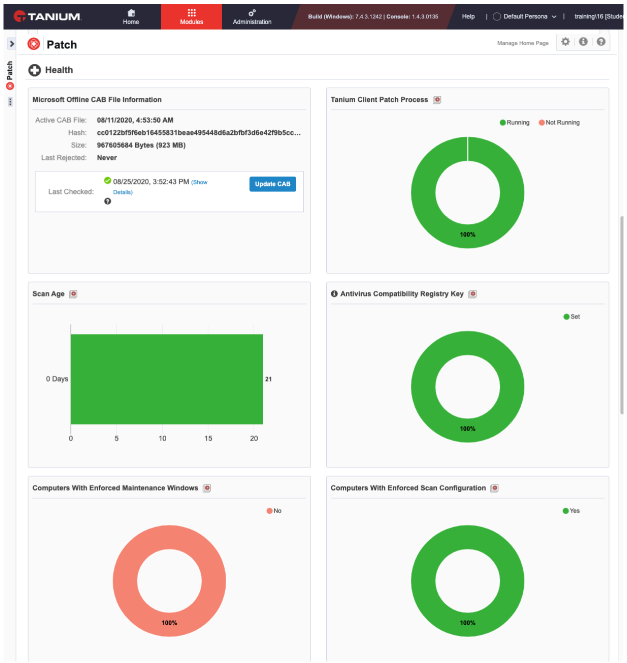
About Scan Configuration Options

Offline CAB File Scan

Offline CAB file based scan configuration is the default option for Tanium Patch for Windows. The Offline CAB provides security patch visibility without relying on WSUS or Microsoft Update.

Online Microsoft Windows Update

WSUS scan configurations provide an extended catalog of patches, but require that all updates be approved in WSUS before they become visible in Tanium Patch.



Patch

Health

Microsoft Offline CAB File Information

Active CAB File: 08/11/2020, 4:53:50 AM
Hash: cc0122bf5f6eb16455831beae495448d6a2bfbf3d6e42f9b5cc...
Size: 967605684 Bytes (923 MB)
Last Rejected: Never

Last Checked: 08/25/2020, 3:52:43 PM (Show Details)

Update CAB

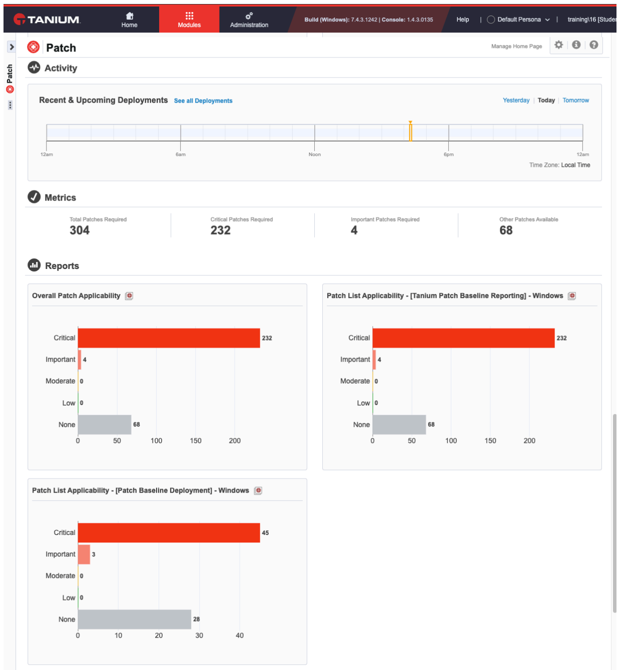
Tanium Client Patch Process

Scan Age

Antivirus Compatibility Registry Key

Computers With Enforced Maintenance Windows

Computers With Enforced Scan Configuration



Patch

Activity

Recent & Upcoming Deployments See all Deployments

Yesterday | Today | Tomorrow

Time Zone: Local Time

Metrics

Total Patches Required	Critical Patches Required	Important Patches Required	Other Patches Available
304	232	4	68

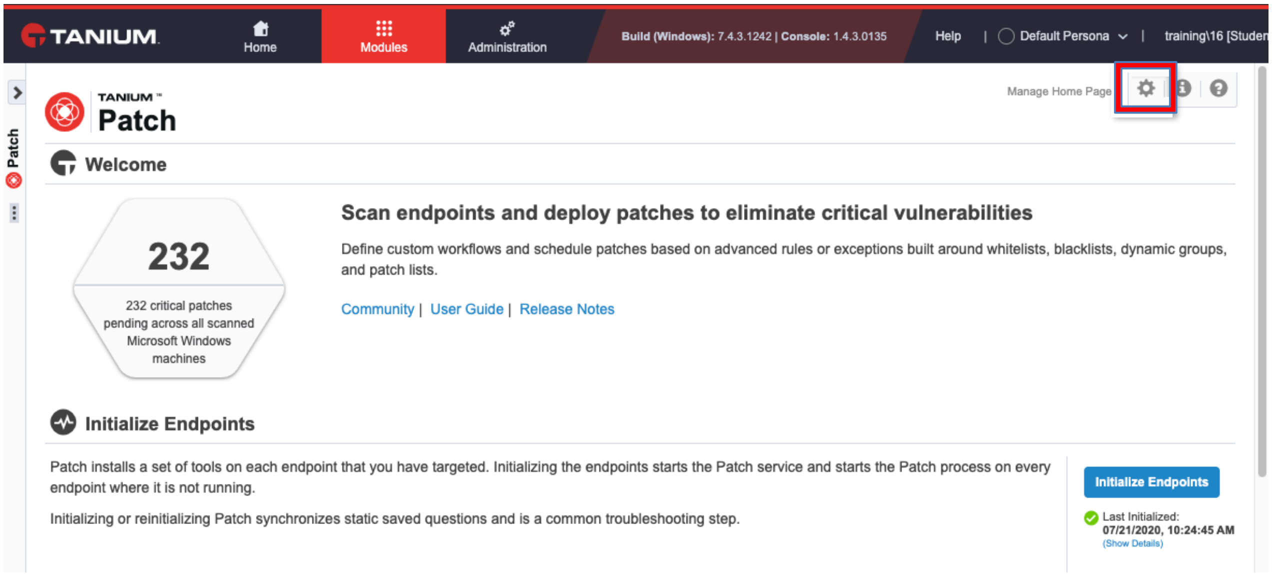
Reports

Overall Patch Applicability

Patch List Applicability - [Tanium Patch Baseline Reporting] - Windows

Patch List Applicability - [Patch Baseline Deployment] - Windows

4. Click on the ⚙ icon at the top right-hand side to access module configuration settings.



232

232 critical patches pending across all scanned Microsoft Windows machines

Scan endpoints and deploy patches to eliminate critical vulnerabilities

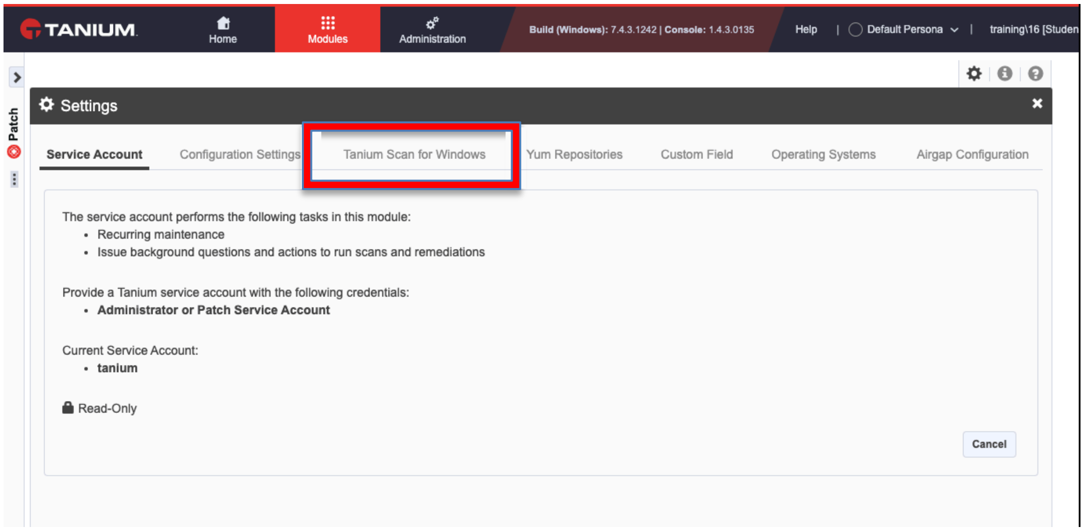
Define custom workflows and schedule patches based on advanced rules or exceptions built around whitelists, blacklists, dynamic groups, and patch lists.

Patch installs a set of tools on each endpoint that you have targeted. Initializing the endpoints starts the Patch service and starts the Patch process on every endpoint where it is not running.

Initializing or reinitializing Patch synchronizes static saved questions and is a common troubleshooting step.

Last Initialized: 07/21/2020, 10:24:45 AM

5. Click on **Tanium Scan for Windows**.



The service account performs the following tasks in this module:

- Recurring maintenance
- Issue background questions and actions to run scans and remediations

Provide a Tanium service account with the following credentials:

- **Administrator or Patch Service Account**

Current Service Account:

- **tanium**

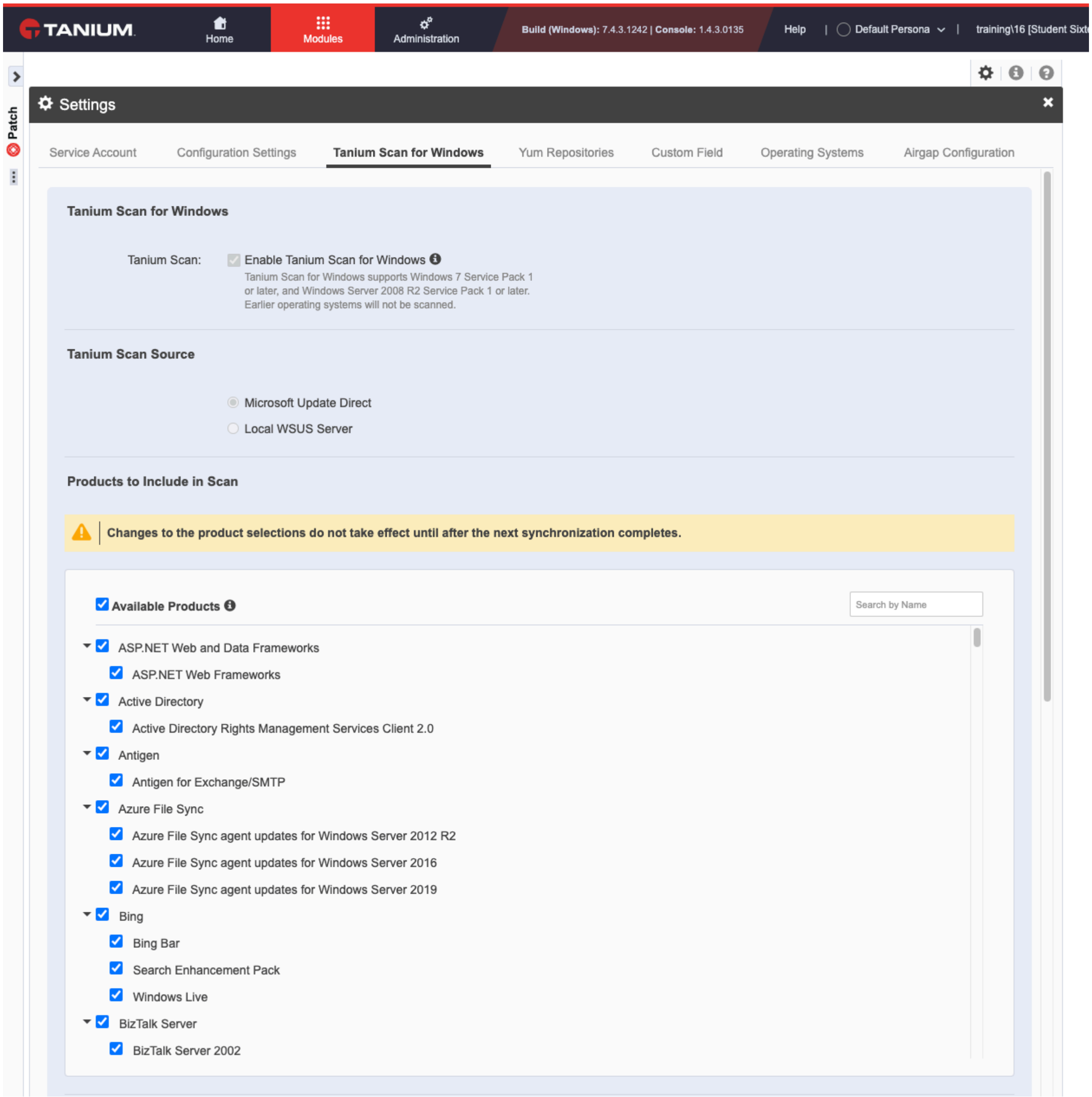
🔒 Read-Only

This is an optimised scan engine, unique to Tanium, which allows the clients to download only the metadata and detection rules for those updates which apply to it. This allows scanning and patching to be conducted quickly and more efficiently, resulting in a much-reduced patch payload to be downloaded to each client through the Tanium linear chain architecture, or direct from the vendor where appropriate.

The settings found here, manage which software products can be patched by Tanium Scan for Windows, the classification of those updates which are synchronised, and where the updates are sourced from to allow Tanium to make them available for distribution by Tanium Patch.

6. Review the available settings. The top half of the screen, as shown below, will allow you to:

- Enable or disable Tanium Scan for Windows as an available scan engine.
- Allow you to specify the source for updates synchronised to Tanium Patch
- Select the products and product families where you want to deploy and manage updates.



Tanium Scan for Windows

Tanium Scan: ☑ Enable Tanium Scan for Windows
Tanium Scan for Windows supports Windows 7 Service Pack 1 or later, and Windows Server 2008 R2 Service Pack 1 or later. Earlier operating systems will not be scanned.

Tanium Scan Source

● Microsoft Update Direct
○ Local WSUS Server

Products to Include in Scan

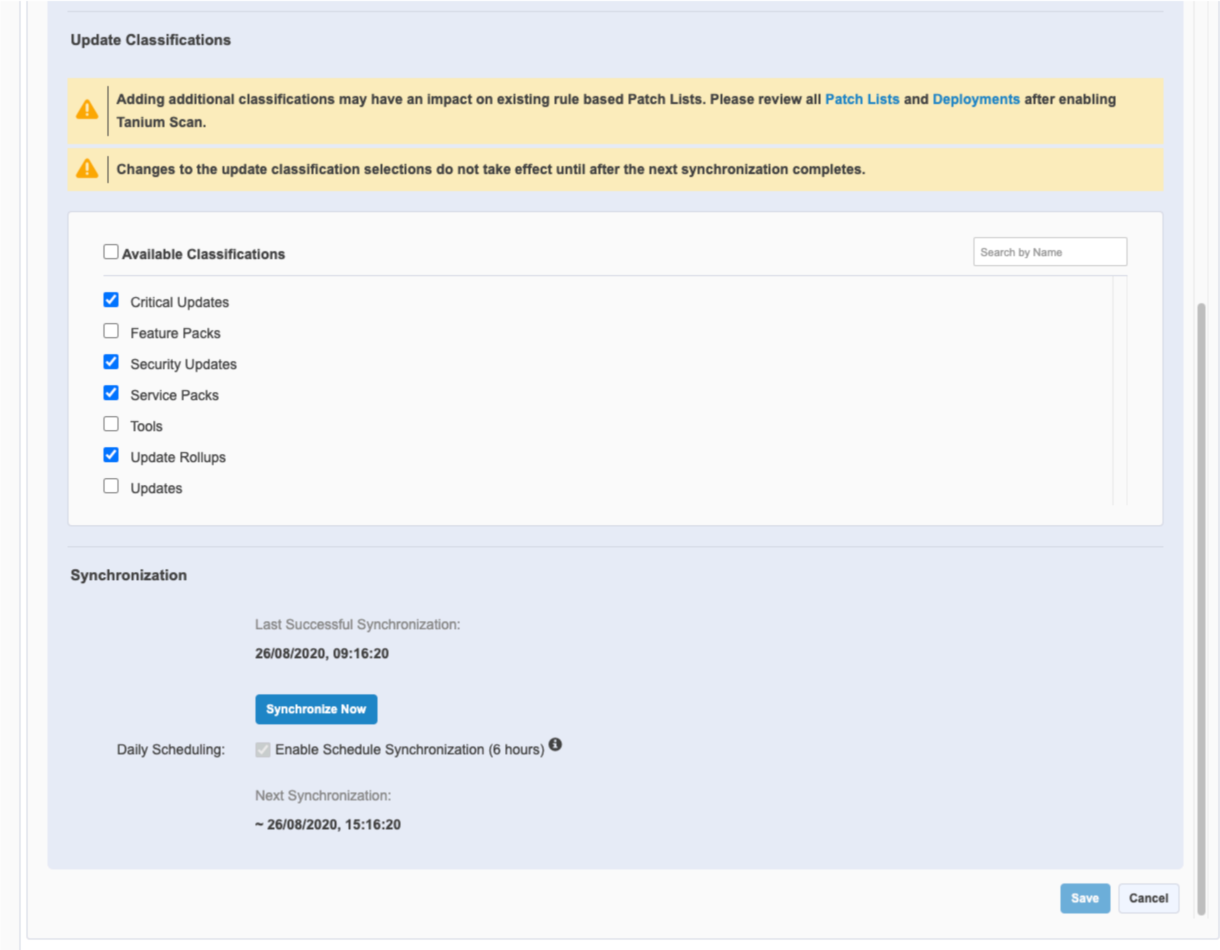
Changes to the product selections do not take effect until after the next synchronization completes.

☑ **Available Products**

- ☑ ASP.NET Web and Data Frameworks
  - ☑ ASP.NET Web Frameworks
- ☑ Active Directory
  - ☑ Active Directory Rights Management Services Client 2.0
- ☑ Antigen
  - ☑ Antigen for Exchange/SMTP
- ☑ Azure File Sync
  - ☑ Azure File Sync agent updates for Windows Server 2012 R2
  - ☑ Azure File Sync agent updates for Windows Server 2016
  - ☑ Azure File Sync agent updates for Windows Server 2019
- ☑ Bing
  - ☑ Bing Bar
  - ☑ Search Enhancement Pack
  - ☑ Windows Live
- ☑ BizTalk Server
  - ☑ BizTalk Server 2002

7. The lower half of the screen allows you to determine which classifications of update should be synchronised and made available.

You can also configure the synchronisation schedule and conduct a manual synchronisation should this be necessary outside the configured schedule.



Update Classifications

⚠ Adding additional classifications may have an impact on existing rule based Patch Lists. Please review all Patch Lists and Deployments after enabling Tanium Scan.

⚠ Changes to the update classification selections do not take effect until after the next synchronization completes.

□ Available Classifications

- ☑ Critical Updates
- □ Feature Packs
- ☑ Security Updates
- ☑ Service Packs
- □ Tools
- ☑ Update Rollups
- □ Updates

Synchronization

Last Successful Synchronization:
26/08/2020, 09:16:20

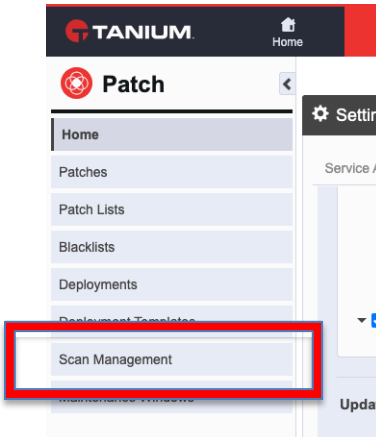
Daily Scheduling: ☑ Enable Schedule Synchronization (6 hours)

Next Synchronization:
~ 26/08/2020, 15:16:20

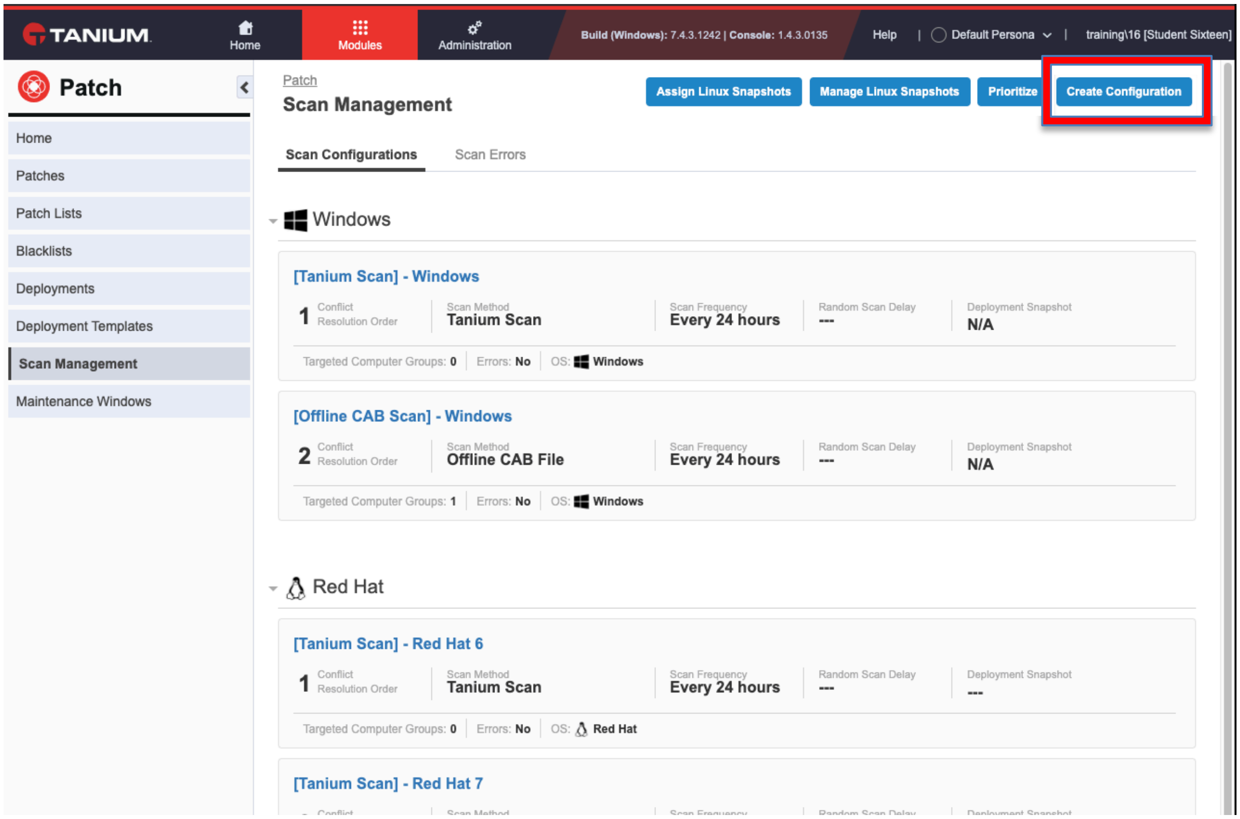
Click on **Cancel** to return to the Patch workbench homepage.

8. Now that we have reviewed the Tanium Scan for Windows configuration used by the Tanium Patch module to determine which updates are managed, and how they are obtained, we will now look at the configuration of the scan engine which is used on the endpoint.

Pop out the menu on the left-hand side and select **Scan Management**.



9. You will now see a list of scan profiles available for supported platforms. Click on **Create Configuration**.



Patch

Scan Management

Windows

[Tanium Scan] - Windows
1 Conflict Resolution Order | Scan Method: Tanium Scan | Scan Frequency: Every 24 hours | Random Scan Delay: --- | Deployment Snapshot: N/A
Targeted Computer Groups: 0 | Errors: No | OS: Windows

[Offline CAB Scan] - Windows
2 Conflict Resolution Order | Scan Method: Offline CAB File | Scan Frequency: Every 24 hours | Random Scan Delay: --- | Deployment Snapshot: N/A
Targeted Computer Groups: 1 | Errors: No | OS: Windows

Red Hat

[Tanium Scan] - Red Hat 6
1 Conflict Resolution Order | Scan Method: Tanium Scan | Scan Frequency: Every 24 hours | Random Scan Delay: --- | Deployment Snapshot: ---
Targeted Computer Groups: 0 | Errors: No | OS: Red Hat

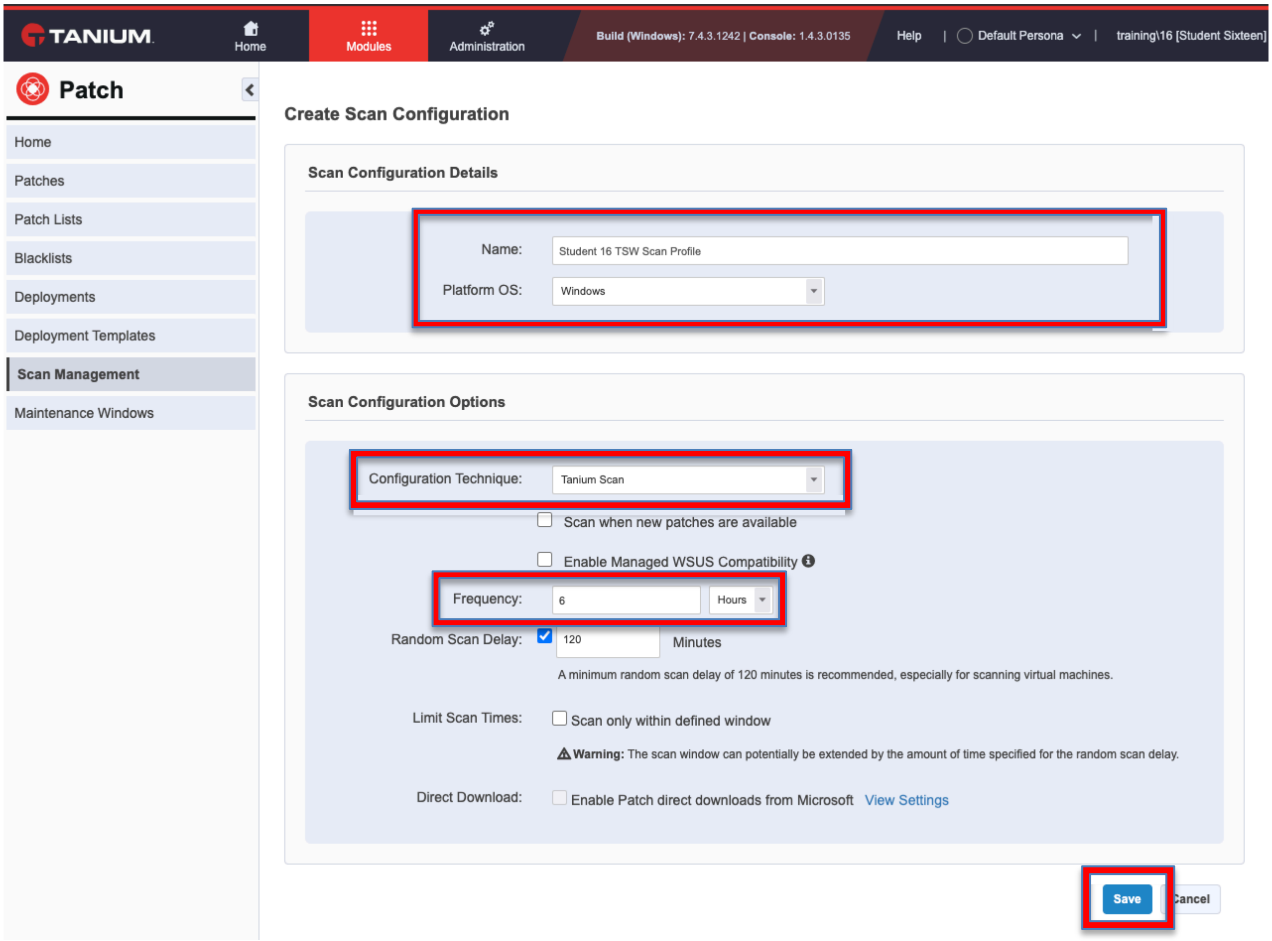
[Tanium Scan] - Red Hat 7
Conflict | Scan Method | Scan Frequency | Random Scan Delay | Deployment Snapshot

10. Name your scan profile *Student <Student ID Number> TSW Scan Profile* and in the **Platform OS** drop-down, select *Windows*.

Some new options will appear under the category **Scan Configuration Options** which are specific to the platform OS specified. Configure your scan profile as follows:

- In the **Configuration Technique** drop-down, review the available options and then choose *Tanium Scan.*
- In the **Frequency** drop-down, set this to *6 hours.*
- Review the other available options but leave these as default.

Your configuration profile should look similar to that shown below:



Create Scan Configuration

Scan Configuration Details

Name: Student 16 TSW Scan Profile

Platform OS: Windows

Scan Configuration Options

Configuration Technique: Tanium Scan

□ Scan when new patches are available

□ Enable Managed WSUS Compatibility

Frequency: 6 Hours

Random Scan Delay: ☑ 120 Minutes

A minimum random scan delay of 120 minutes is recommended, especially for scanning virtual machines.

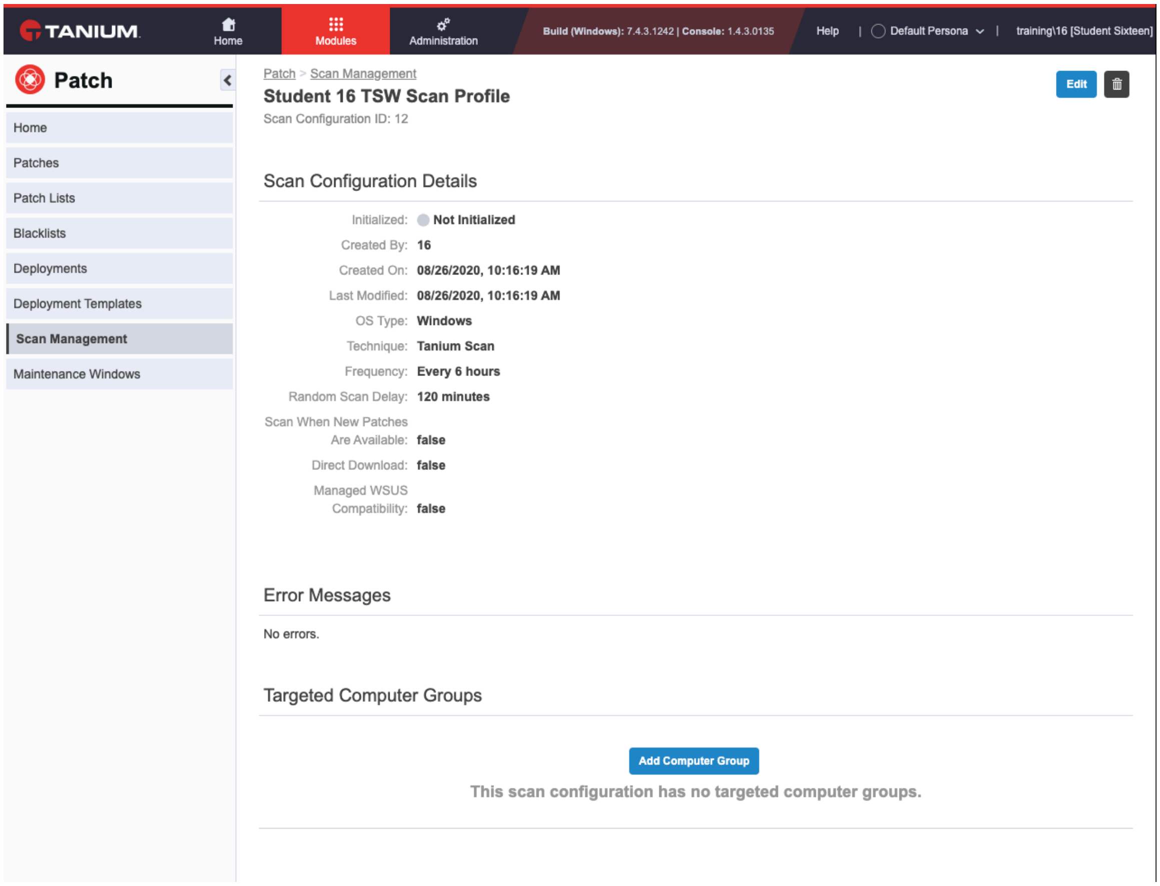
Limit Scan Times: □ Scan only within defined window

⚠ **Warning:** The scan window can potentially be extended by the amount of time specified for the random scan delay.

Direct Download: □ Enable Patch direct downloads from Microsoft View Settings

Click on **Save** to create your new profile.

11. A summary will be displayed showing your configuration options selected. From here, you would also use **Add Computer Group** to select which computer groups would receive this profile. We will not be deploying this profile in this lab so there is no need to add any computer groups.



Student 16 TSW Scan Profile

Scan Configuration ID: 12

Scan Configuration Details

Initialized: Not Initialized
Created By: 16
Created On: 08/26/2020, 10:16:19 AM
Last Modified: 08/26/2020, 10:16:19 AM
OS Type: Windows
Technique: Tanium Scan
Frequency: Every 6 hours
Random Scan Delay: 120 minutes
Scan When New Patches Are Available: false
Direct Download: false
Managed WSUS Compatibility: false

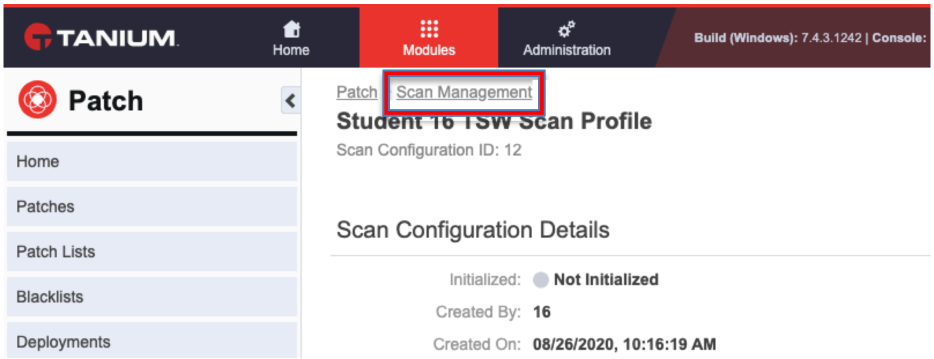
Error Messages

No errors.

Targeted Computer Groups

This scan configuration has no targeted computer groups.

Click on **Scan Management** on the breadcrumb bar at the top to return you to the list of available scan profiles.



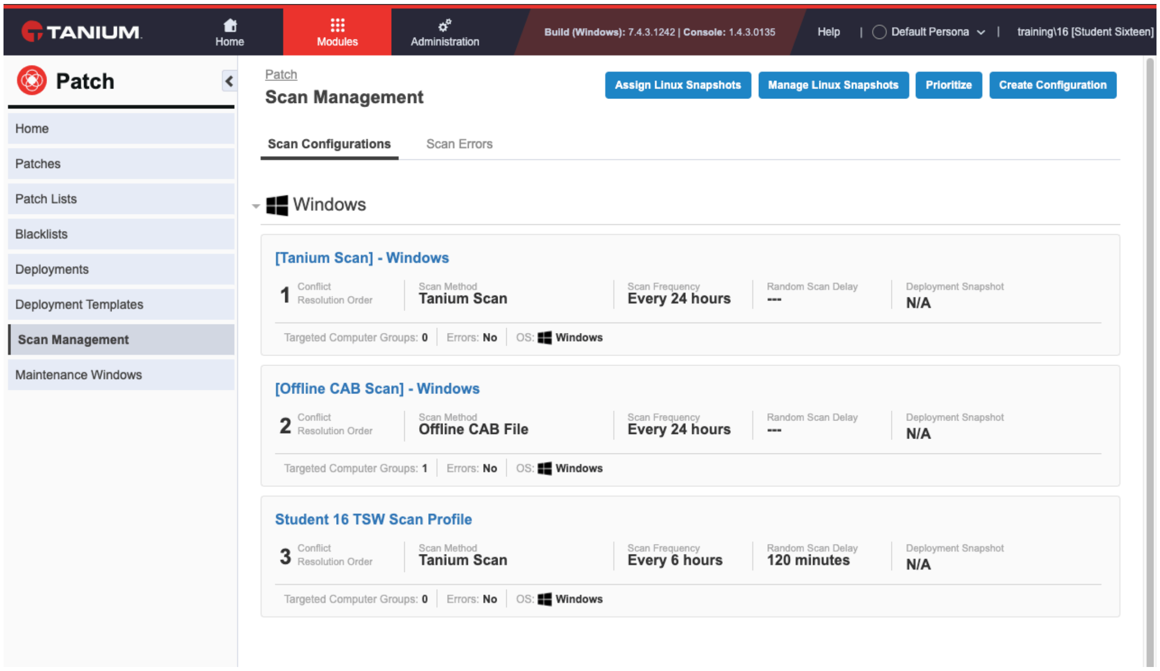
Student 16 TSW Scan Profile

Scan Configuration ID: 12

Scan Configuration Details

Initialized: Not Initialized
Created By: 16
Created On: 08/26/2020, 10:16:19 AM

12. You will now see your new profile in the list.



Patch
Scan Management

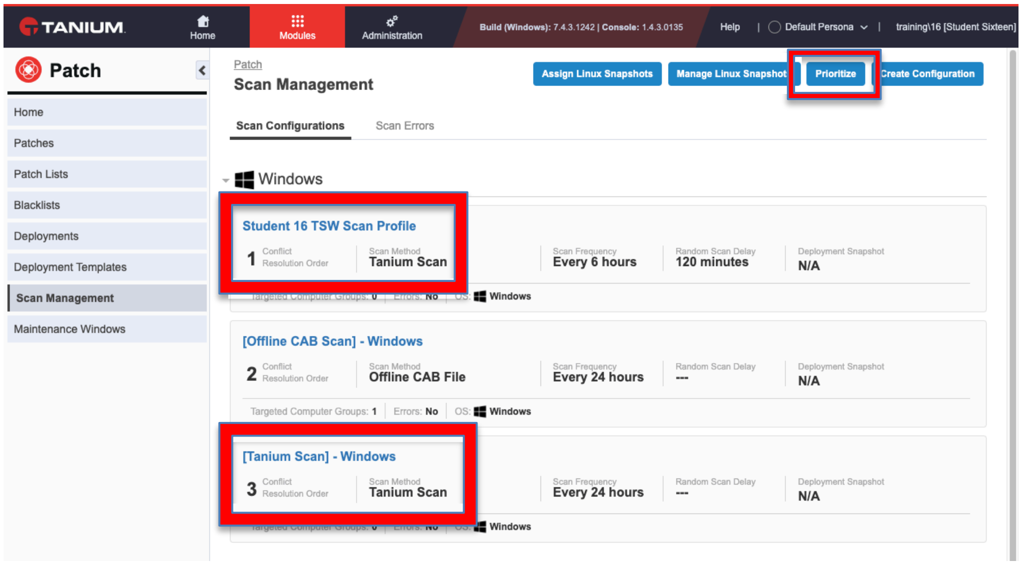
Windows

[Tanium Scan] - Windows
1 Conflict Resolution Order | Scan Method: Tanium Scan | Scan Frequency: Every 24 hours | Random Scan Delay: --- | Deployment Snapshot: N/A
Targeted Computer Groups: 0 | Errors: No | OS: Windows

[Offline CAB Scan] - Windows
2 Conflict Resolution Order | Scan Method: Offline CAB File | Scan Frequency: Every 24 hours | Random Scan Delay: --- | Deployment Snapshot: N/A
Targeted Computer Groups: 1 | Errors: No | OS: Windows

Student 16 TSW Scan Profile
3 Conflict Resolution Order | Scan Method: Tanium Scan | Scan Frequency: Every 6 hours | Random Scan Delay: 120 minutes | Deployment Snapshot: N/A
Targeted Computer Groups: 0 | Errors: No | OS: Windows

Important Note: There may be occasions where more than one scan profile may apply to a group of endpoints. As only one scan profile can be applied, you can use the Prioritize button to manage this. If multiple profiles are applicable, the profile with the lowest number receives the highest priority. In the example below, if you wanted the new scan profile to win in a profile conflict, you could change the **Conflict Resolution Order** for the new profile to a value of *1* and the **[Tanium Scan] - Windows** profile to value of *3* by dragging and dropping them into the desired order, and thus your new policy would now apply to endpoints where both are potentially applicable.



Patch
Scan Management

Windows

Student 16 TSW Scan Profile
1 Conflict Resolution Order | Scan Method: Tanium Scan | Scan Frequency: Every 6 hours | Random Scan Delay: 120 minutes | Deployment Snapshot: N/A
Targeted Computer Groups: 0 | Errors: No | OS: Windows

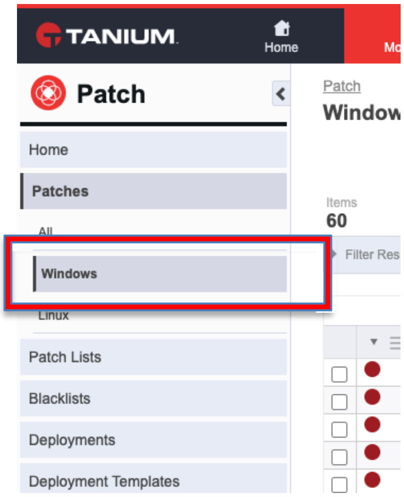
[Offline CAB Scan] - Windows
2 Conflict Resolution Order | Scan Method: Offline CAB File | Scan Frequency: Every 24 hours | Random Scan Delay: --- | Deployment Snapshot: N/A
Targeted Computer Groups: 1 | Errors: No | OS: Windows

[Tanium Scan] - Windows
3 Conflict Resolution Order | Scan Method: Tanium Scan | Scan Frequency: Every 24 hours | Random Scan Delay: --- | Deployment Snapshot: N/A
Targeted Computer Groups: 0 | Errors: No | OS: Windows

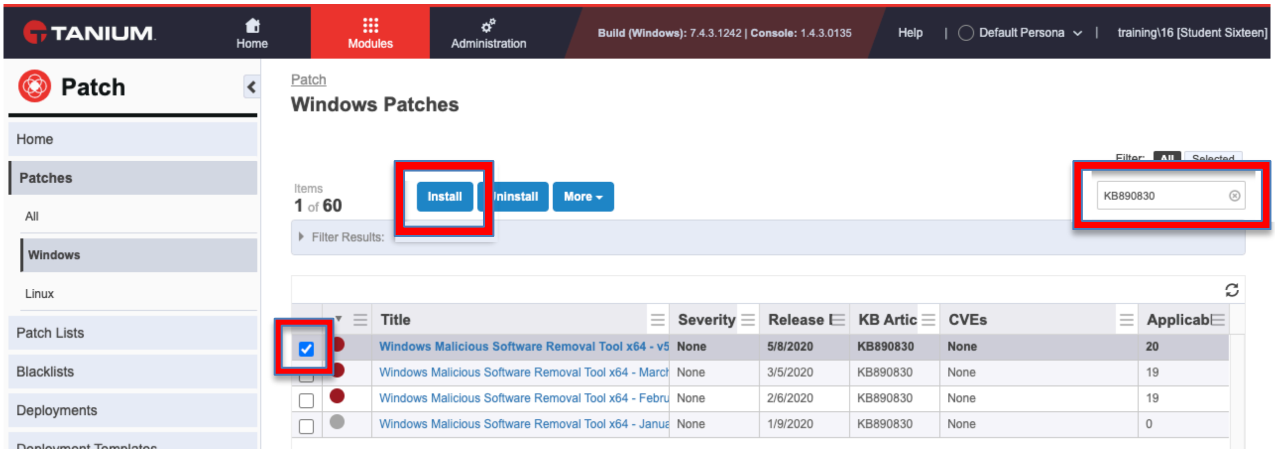
13. We will now work through an exercise called “sniper patching”. This is the commonly used term for applying one or more individual patches to address specific vulnerabilities or concerns, typically conducted “out of band” of any routine patching cycle.

- **Students 1 - 20** : Deploy KB890830 to your designated lab client
- **Students 21 - 40** : Deploy KB4565511 to your designated lab client

Expand the menu on the left-hand side and select **Patches**, then **Windows**.



14. In the **Filter by Text** field, enter the KB number you will be deploying. Where multiples may be shown, choose the latest release by checking the checkbox. We will use *KB890830* in this example.

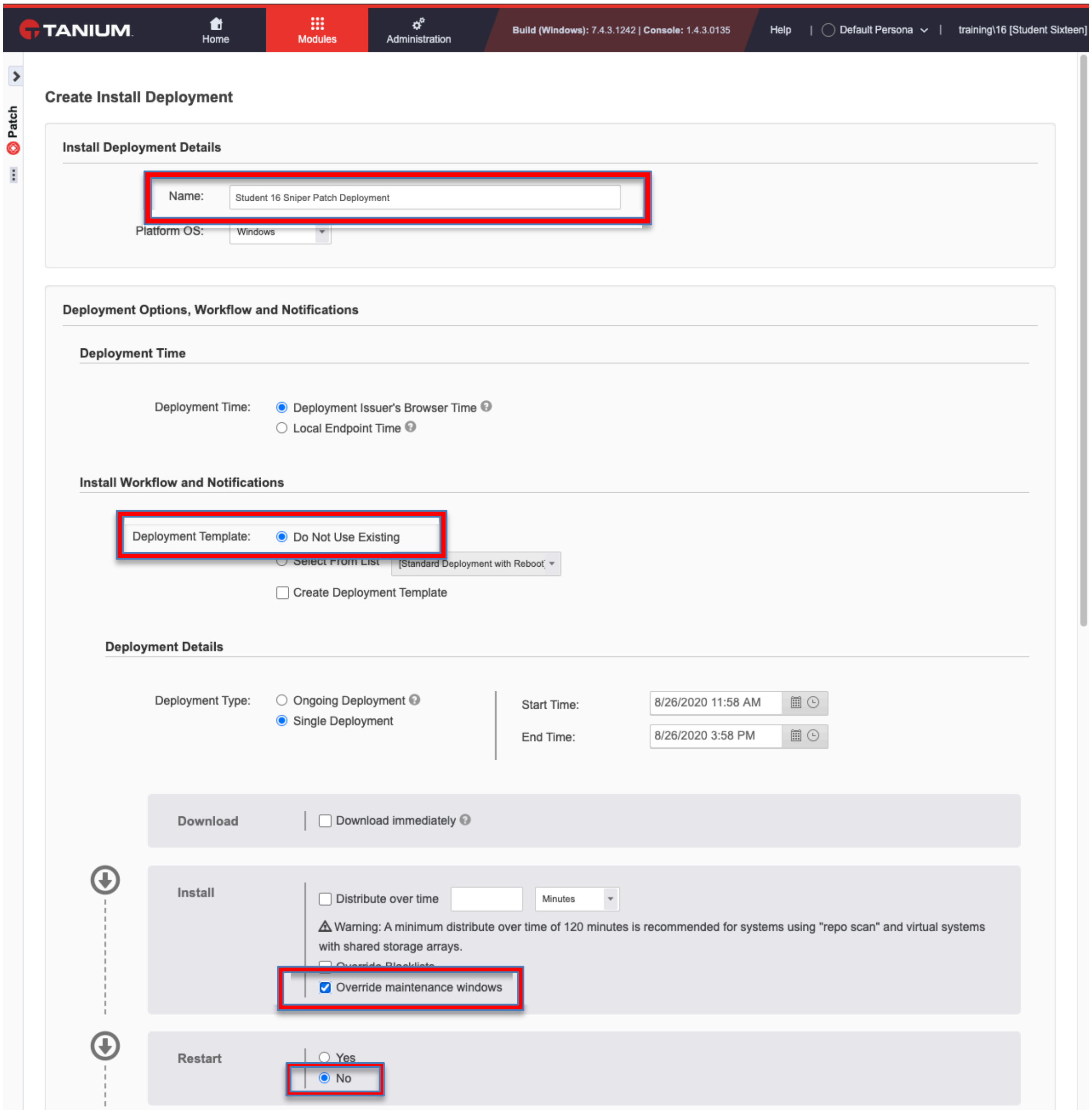


		Title	Severity	Release D	KB Artic	CVEs	Applicabl
☑	●	Windows Malicious Software Removal Tool x64 - v5	None	5/8/2020	KB890830	None	20
□	●	Windows Malicious Software Removal Tool x64 - March	None	3/5/2020	KB890830	None	19
□	●	Windows Malicious Software Removal Tool x64 - Febru	None	2/6/2020	KB890830	None	19
□	●	Windows Malicious Software Removal Tool x64 - Janua	None	1/9/2020	KB890830	None	0

Click on **Install** once selected.

15. Configure your patch deployment as follows:

- Change the name of the deployment to *Student <Student ID Number> Sniper Patch Deployment*.
- Under the **Install Workflows and Notifications** section, change the **Deployment Template** option to *Do Not Use Existing*.
- Under **Deployment Details**
  - In the **Install** subcategory, check the box for **Override Maintenance Windows.**
  - In the **Restart** subcategory, select *No*.
  - Leave all other settings as default.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Patch

Create Install Deployment

Install Deployment Details

Name: Student 16 Sniper Patch Deployment

Platform OS: Windows

Deployment Options, Workflow and Notifications

Deployment Time

Deployment Time: ● Deployment Issuer's Browser Time ○ Local Endpoint Time

Install Workflow and Notifications

Deployment Template: ● Do Not Use Existing ○ Select From List [Standard Deployment with Reboot]

□ Create Deployment Template

Deployment Details

Deployment Type: ○ Ongoing Deployment ● Single Deployment

Start Time: 8/26/2020 11:58 AM

End Time: 8/26/2020 3:58 PM

Download: □ Download immediately

Install: □ Distribute over time [Minutes]

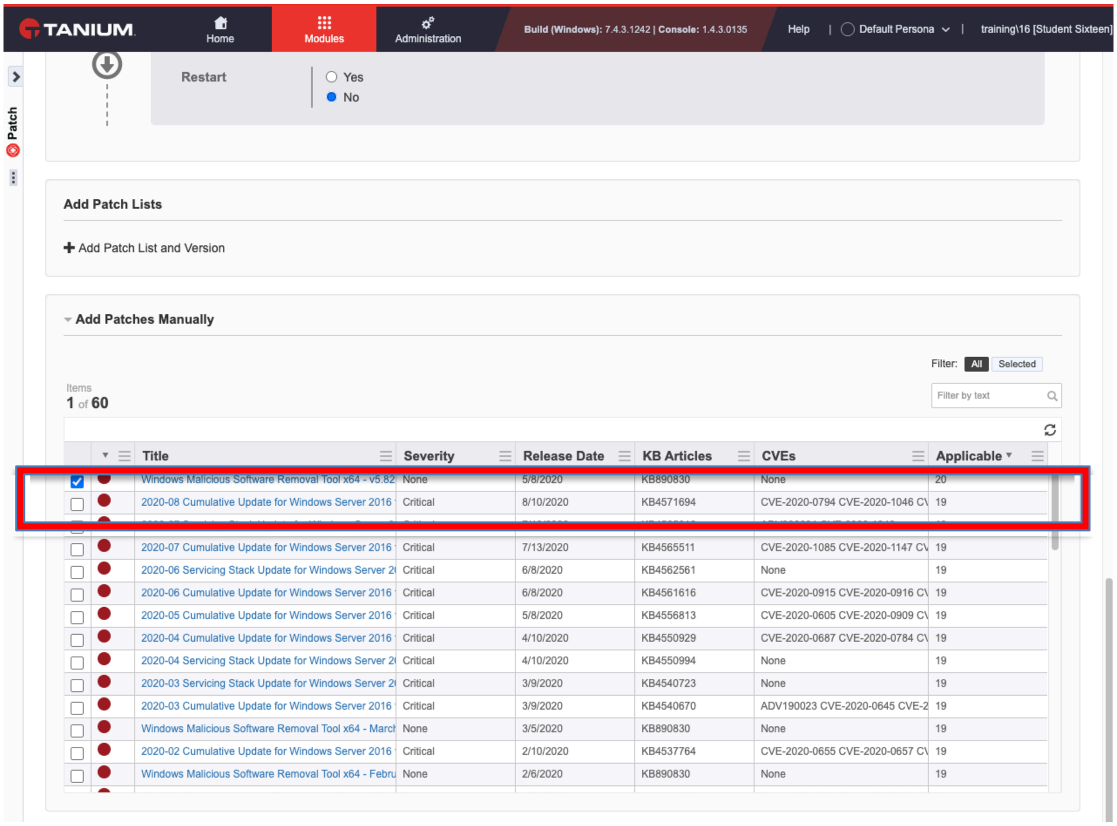
⚠ Warning: A minimum distribute over time of 120 minutes is recommended for systems using "repo scan" and virtual systems with shared storage arrays.

□ Override Blacklists

☑ Override maintenance windows

Restart: ○ Yes ● No

16. Scroll to the bottom of the screen and ensure your patch is selected under the **Add Patches Manually** section.



TANIUM | Home | Modules | Administration | **Build (Windows):** 7.4.3.1242 | **Console:** 1.4.3.0135 | Help | ○ Default Persona | training\16 [Student Sixteen]

Patch

Restart ○ Yes ● No

Add Patch Lists

+ Add Patch List and Version

Add Patches Manually

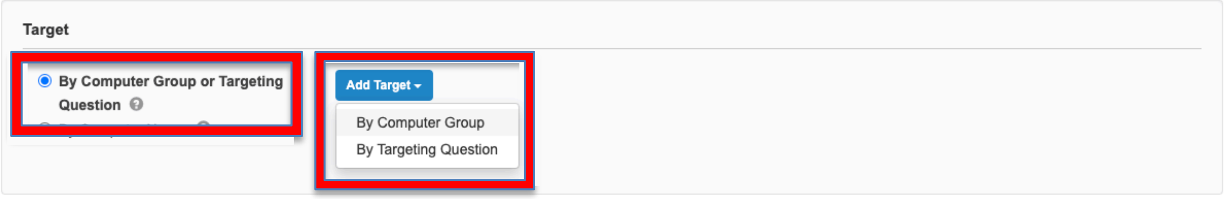
Filter: All Selected

Items 1 of 60

Filter by text

		Title	Severity	Release Date	KB Articles	CVEs	Applicable
☑	●	Windows Malicious Software Removal Tool x64 - v5.82	None	5/8/2020	KB890830	None	20
□	●	2020-08 Cumulative Update for Windows Server 2016	Critical	8/10/2020	KB4571694	CVE-2020-0794 CVE-2020-1046 C\	19
□	●	2020-07 Cumulative Update for Windows Server 2016	Critical	7/13/2020	KB4565511	CVE-2020-1085 CVE-2020-1147 C\	19
□	●	2020-06 Servicing Stack Update for Windows Server 2(	Critical	6/8/2020	KB4562561	None	19
□	●	2020-06 Cumulative Update for Windows Server 2016	Critical	6/8/2020	KB4561616	CVE-2020-0915 CVE-2020-0916 C\	19
□	●	2020-05 Cumulative Update for Windows Server 2016	Critical	5/8/2020	KB4556813	CVE-2020-0605 CVE-2020-0909 C\	19
□	●	2020-04 Cumulative Update for Windows Server 2016	Critical	4/10/2020	KB4550929	CVE-2020-0687 CVE-2020-0784 C\	19
□	●	2020-04 Servicing Stack Update for Windows Server 2(	Critical	4/10/2020	KB4550994	None	19
□	●	2020-03 Servicing Stack Update for Windows Server 2(	Critical	3/9/2020	KB4540723	None	19
□	●	2020-03 Cumulative Update for Windows Server 2016	Critical	3/9/2020	KB4540670	ADV190023 CVE-2020-0645 CVE-2	19
□	●	Windows Malicious Software Removal Tool x64 - March	None	3/5/2020	KB890830	None	19
□	●	2020-02 Cumulative Update for Windows Server 2016	Critical	2/10/2020	KB4537764	CVE-2020-0655 CVE-2020-0657 C\	19
□	●	Windows Malicious Software Removal Tool x64 - Febru	None	2/6/2020	KB890830	None	19

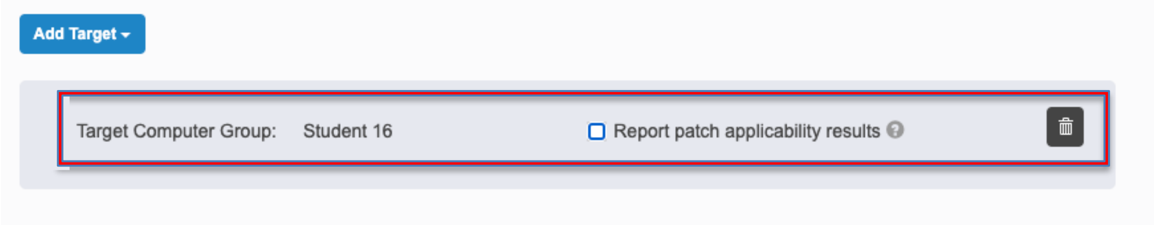
17. Under the **Target** section, ensure the **By Computer Group or Targeting Question** option is enabled and click **Add Target,** then **By Computer Group.**



Target

● By Computer Group or Targeting Question

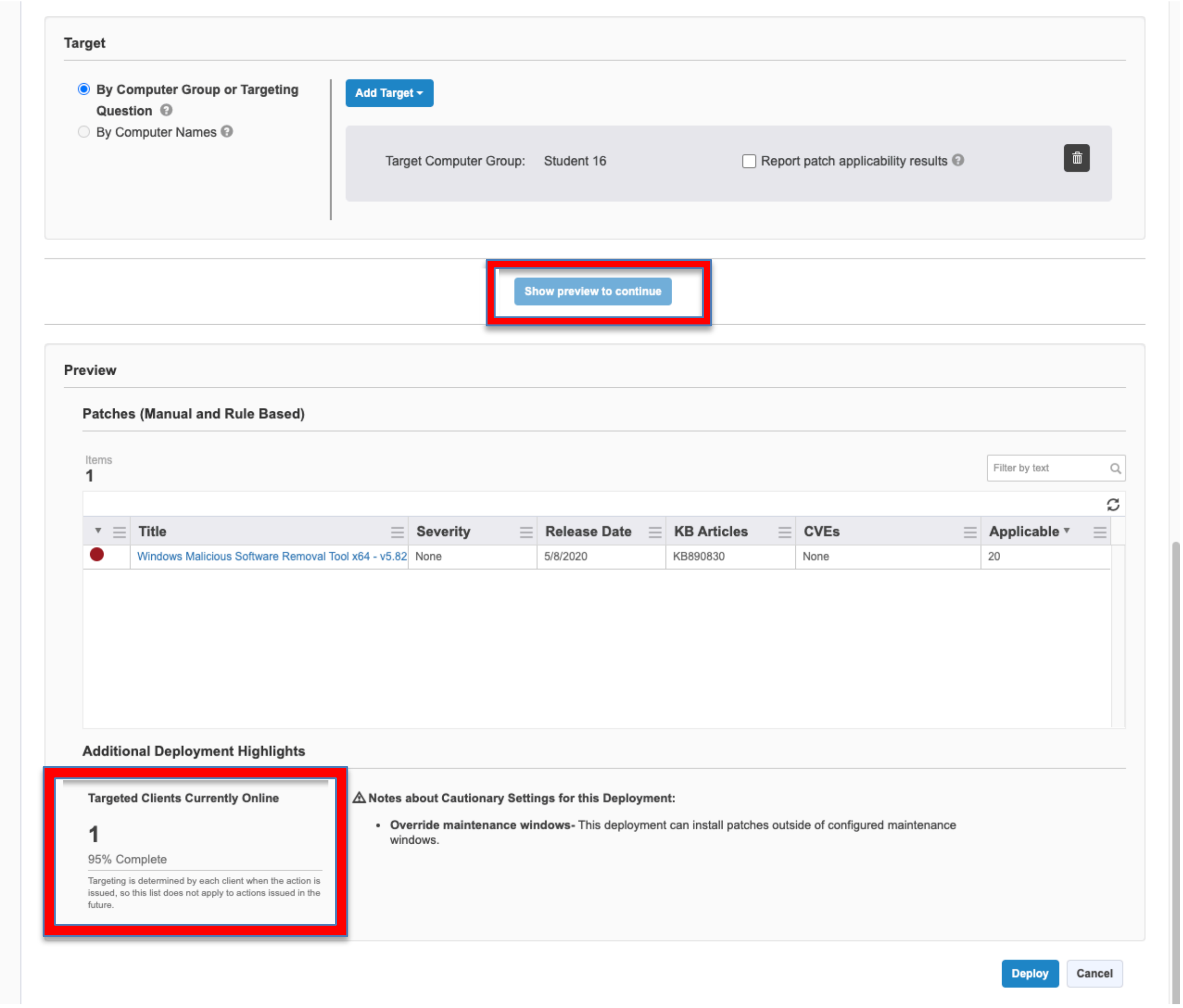
Select the computer group applicable to your designated student ID as assigned by the instructor.



Target Computer Group: Student 16

□ Report patch applicability results

18. Click on Show Preview to Continue. This will then enumerate the number of clients being targeted which are currently online. You should see only one as the computer group being targeted should only contain your designated lab client.



Target

● By Computer Group or Targeting Question
○ By Computer Names

Target Computer Group: Student 16

□ Report patch applicability results

Preview

Patches (Manual and Rule Based)

Items
1

	Title	Severity	Release Date	KB Articles	CVEs	Applicable
●	Windows Malicious Software Removal Tool x64 - v5.82	None	5/8/2020	KB890830	None	20

Additional Deployment Highlights

Targeted Clients Currently Online

1

95% Complete

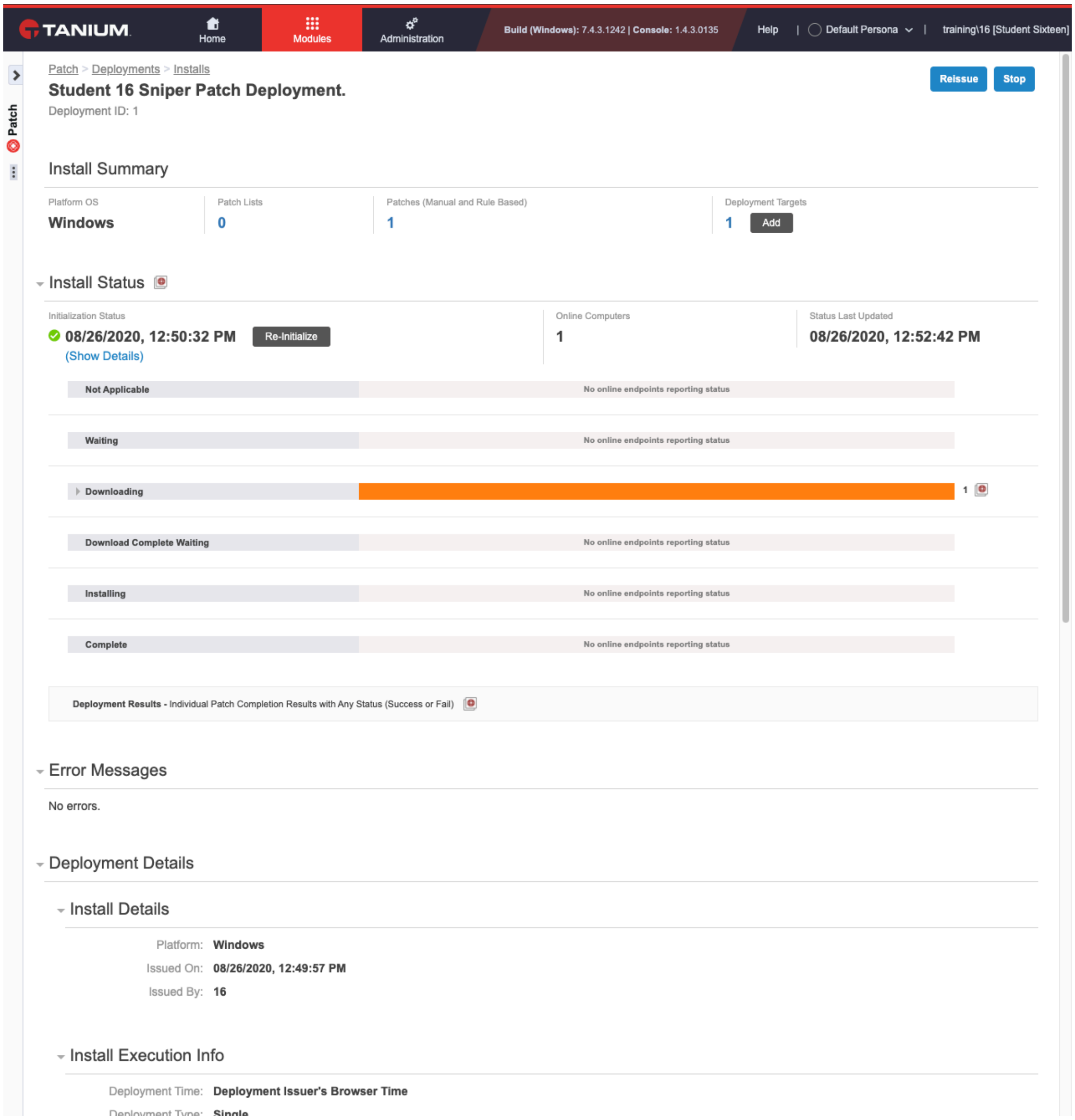
Targeting is determined by each client when the action is issued, so this list does not apply to actions issued in the future.

⚠ Notes about Cautionary Settings for this Deployment:

- **Override maintenance windows-** This deployment can install patches outside of configured maintenance windows.

Once happy with your selections, click on **Deploy** and then confirm the action by clicking **Yes**.

19. Your one-time deployment will now be executed. A summary of the deployment and deployment progress will be displayed. As each targeted endpoint moves through the various phases of patch deployment, the progress will be reported back to the console, along with any errors.



TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Patch
Reissue
Stop

Patch > Deployments > Installs

Student 16 Sniper Patch Deployment.

Deployment ID: 1

Install Summary

Platform OS	Patch Lists	Patches (Manual and Rule Based)	Deployment Targets
Windows	0	1	1 Add

Install Status

Initialization Status	Online Computers	Status Last Updated
08/26/2020, 12:50:32 PM Re-Initialize (Show Details)	1	08/26/2020, 12:52:42 PM

Not Applicable	No online endpoints reporting status	
Waiting	No online endpoints reporting status	
Downloading		1
Download Complete Waiting	No online endpoints reporting status	
Installing	No online endpoints reporting status	
Complete	No online endpoints reporting status	

Deployment Results - Individual Patch Completion Results with Any Status (Success or Fail)

Error Messages

No errors.

Deployment Details

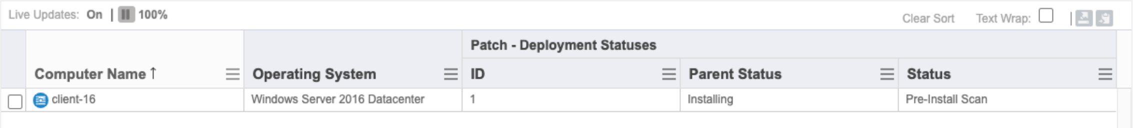
Install Details

Platform: Windows
Issued On: 08/26/2020, 12:49:57 PM
Issued By: 16

Install Execution Info

Deployment Time: Deployment Issuer's Browser Time
Deployment Type: Single

At any stage, clicking on any of the available icons which look like this ⊡ will allow you to pivot to interact and issue questions which will give specific details on each deployment phase and overall deployment status.

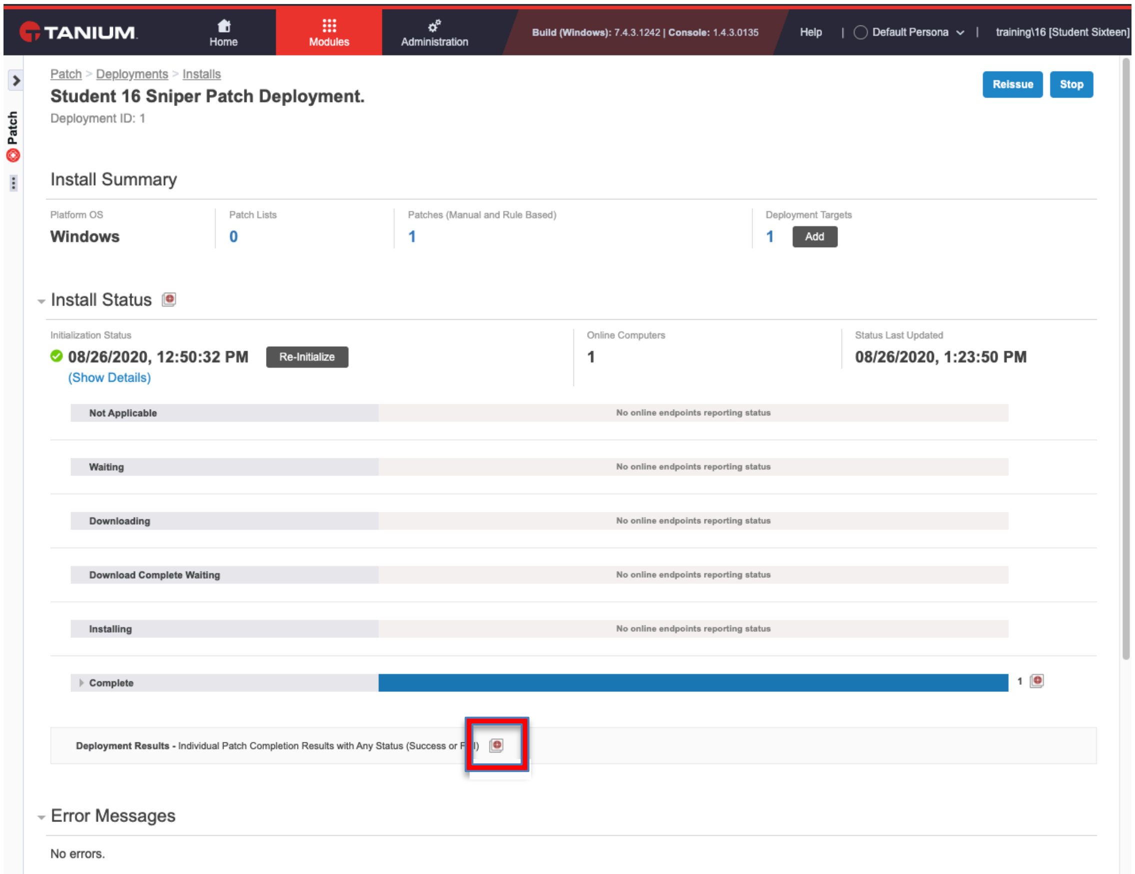


Live Updates: On | 100%

			Patch - Deployment Statuses		
	Computer Name ↑	Operating System	ID	Parent Status	Status
□	client-16	Windows Server 2016 Datacenter	1	Installing	Pre-Install Scan

20. Once the patches have fully installed, you should see this confirmed in the console. Note that it can take around 10 minutes or so before you see the deployment show as fully completed. If you wish to continue with the lab and let this run in the background you may do so.

Click on the interact icon next to **Deployment Results Individual Patch Completion Results with Any Status (Success or Fail).**



TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Patch
Reissue
Stop

Patch > Deployments > Installs

Student 16 Sniper Patch Deployment.

Deployment ID: 1

Install Summary

Platform OS	Patch Lists	Patches (Manual and Rule Based)	Deployment Targets
Windows	0	1	1 Add

Install Status

Initialization Status	Online Computers	Status Last Updated
08/26/2020, 12:50:32 PM Re-Initialize (Show Details)	1	08/26/2020, 1:23:50 PM

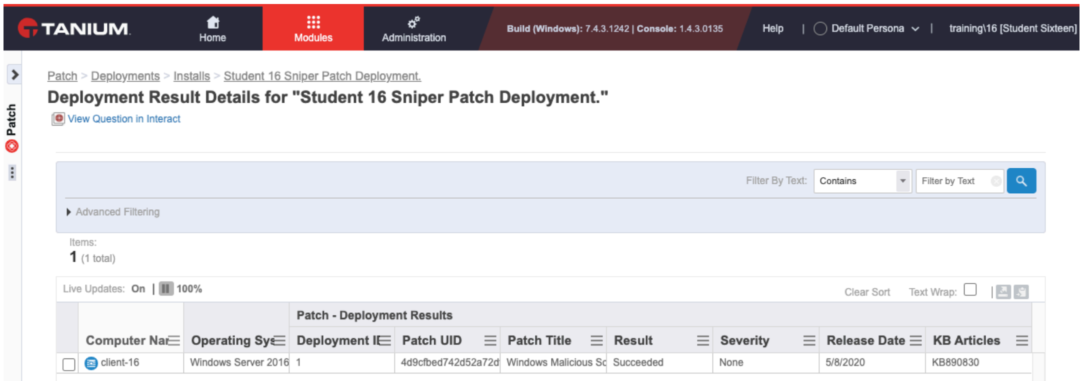
Not Applicable	No online endpoints reporting status
Waiting	No online endpoints reporting status
Downloading	No online endpoints reporting status
Download Complete Waiting	No online endpoints reporting status
Installing	No online endpoints reporting status
Complete	1

Deployment Results - Individual Patch Completion Results with Any Status (Success or Fail)

Error Messages

No errors.

You will now see the status of the overall deployment.



Patch > Deployments > Installs > Student 16 Sniper Patch Deployment.

Deployment Result Details for "Student 16 Sniper Patch Deployment."

View Question in Interact

Items:
1 (1 total)

Live Updates: On | 100%

		Patch - Deployment Results						
Computer Nar	Operating Sys	Deployment I	Patch UID	Patch Title	Result	Severity	Release Date	KB Articles
client-16	Windows Server 2016	1	4d9cfbed742d52a72d	Windows Malicious Sc	Succeeded	None	5/8/2020	KB890830

You have completed lab 6.

Lab 7: Sending Out the Bits

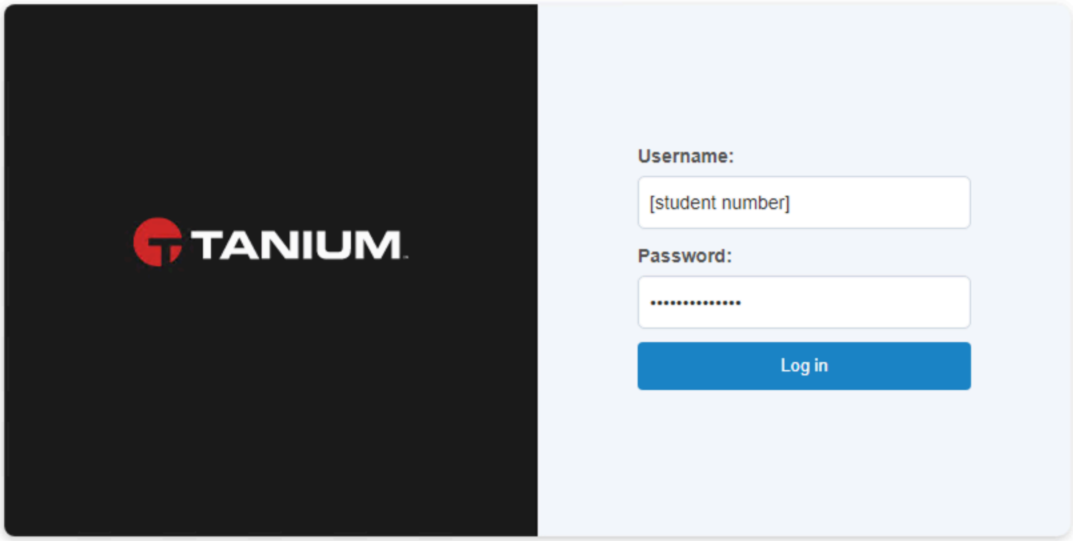
Deploying and managing software using Tanium Deploy

Objectives

By the end of this lab you will have completed the following objectives:

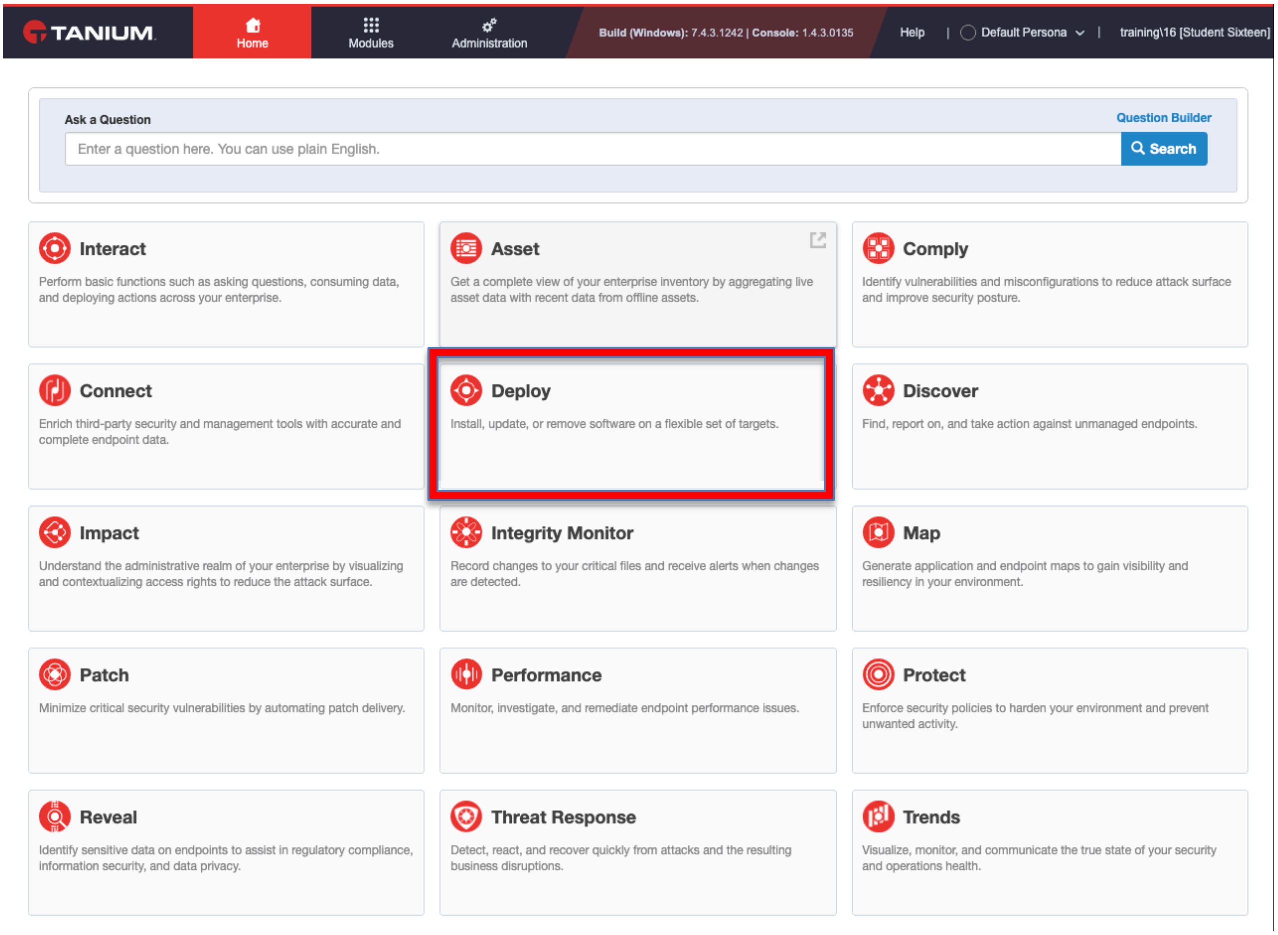
- Create a software package
- Upgraded out-of-date software
    - ○ **Students 1 – 20:** Upgrade Adobe Acrobat Reader DC
    - ○ **Students 21 – 40**: Upgrade VLC Media Player
- Explore Software Bundles
- Explore Windows 10 in-place upgrade

Lab Steps

1.	Using the URL provided, open the Tanium console and enter your credentials  Username: [student number] Password: ••••••••••••••

2. Click on the **Tanium** logo at the top left-hand corner to return you to the home page if you aren't there already.

You should see the homepage of the Tanium console, displaying the various "baseball cards" for the available modules. From here, click on **Deploy**.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Ask a Question
Question Builder
Enter a question here. You can use plain English.
Search

Interact
Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise.

Asset
Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets.

Comply
Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.

Connect
Enrich third-party security and management tools with accurate and complete endpoint data.

Deploy
Install, update, or remove software on a flexible set of targets.

Discover
Find, report on, and take action against unmanaged endpoints.

Impact
Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface.

Integrity Monitor
Record changes to your critical files and receive alerts when changes are detected.

Map
Generate application and endpoint maps to gain visibility and resiliency in your environment.

Patch
Minimize critical security vulnerabilities by automating patch delivery.

Performance
Monitor, investigate, and remediate endpoint performance issues.

Protect
Enforce security policies to harden your environment and prevent unwanted activity.

Reveal
Identify sensitive data on endpoints to assist in regulatory compliance, information security, and data privacy.

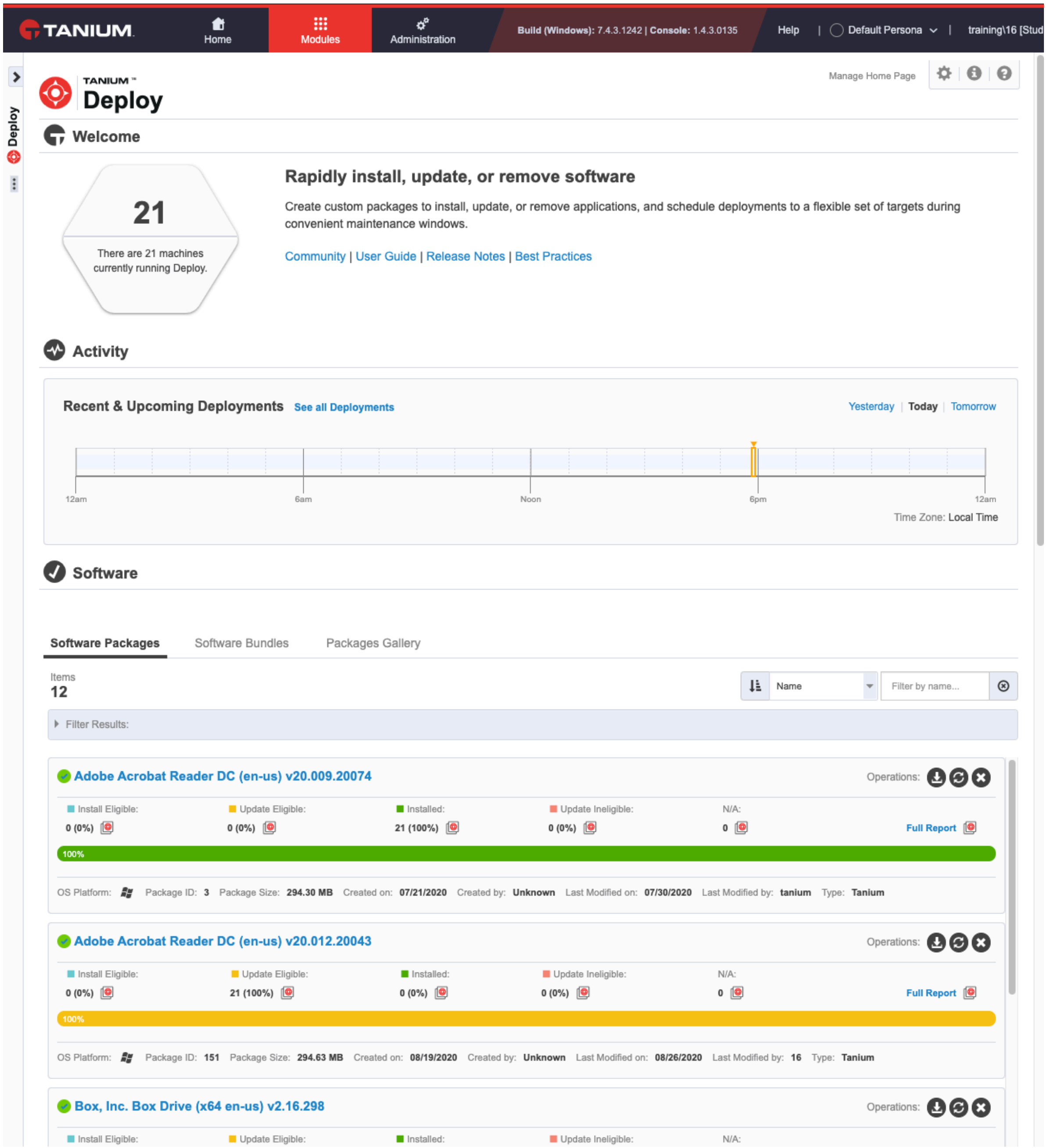
Threat Response
Detect, react, and recover quickly from attacks and the resulting business disruptions.

Trends
Visualize, monitor, and communicate the true state of your security and operations health.

This will now take you to the Deploy workbench.

3. The Deploy workbench homepage will display a range of information including:

- Number of assets currently running Deploy
- Timeline of activity including past, current and future deployment events
- List of software packages and bundles available for deployment
- The software gallery where pre-packaged applications are made available for download



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135

training\16 [Stud

TANIUM™ Deploy

Welcome

21

There are 21 machines currently running Deploy.

Rapidly install, update, or remove software

Create custom packages to install, update, or remove applications, and schedule deployments to a flexible set of targets during convenient maintenance windows.

Activity

Recent & Upcoming Deployments

Time Zone: Local Time

Software

Software Packages | Software Bundles | Packages Gallery

Items
12

Name ▾ | Filter by name...

Filter Results:

Adobe Acrobat Reader DC (en-us) v20.009.20074

Install Eligible:	Update Eligible:	Installed:	Update Ineligible:	N/A:
0 (0%)	0 (0%)	21 (100%)	0 (0%)	0

OS Platform: Package ID: 3 Package Size: 294.30 MB Created on: 07/21/2020 Created by: Unknown Last Modified on: 07/30/2020 Last Modified by: tanium Type: Tanium

Adobe Acrobat Reader DC (en-us) v20.012.20043

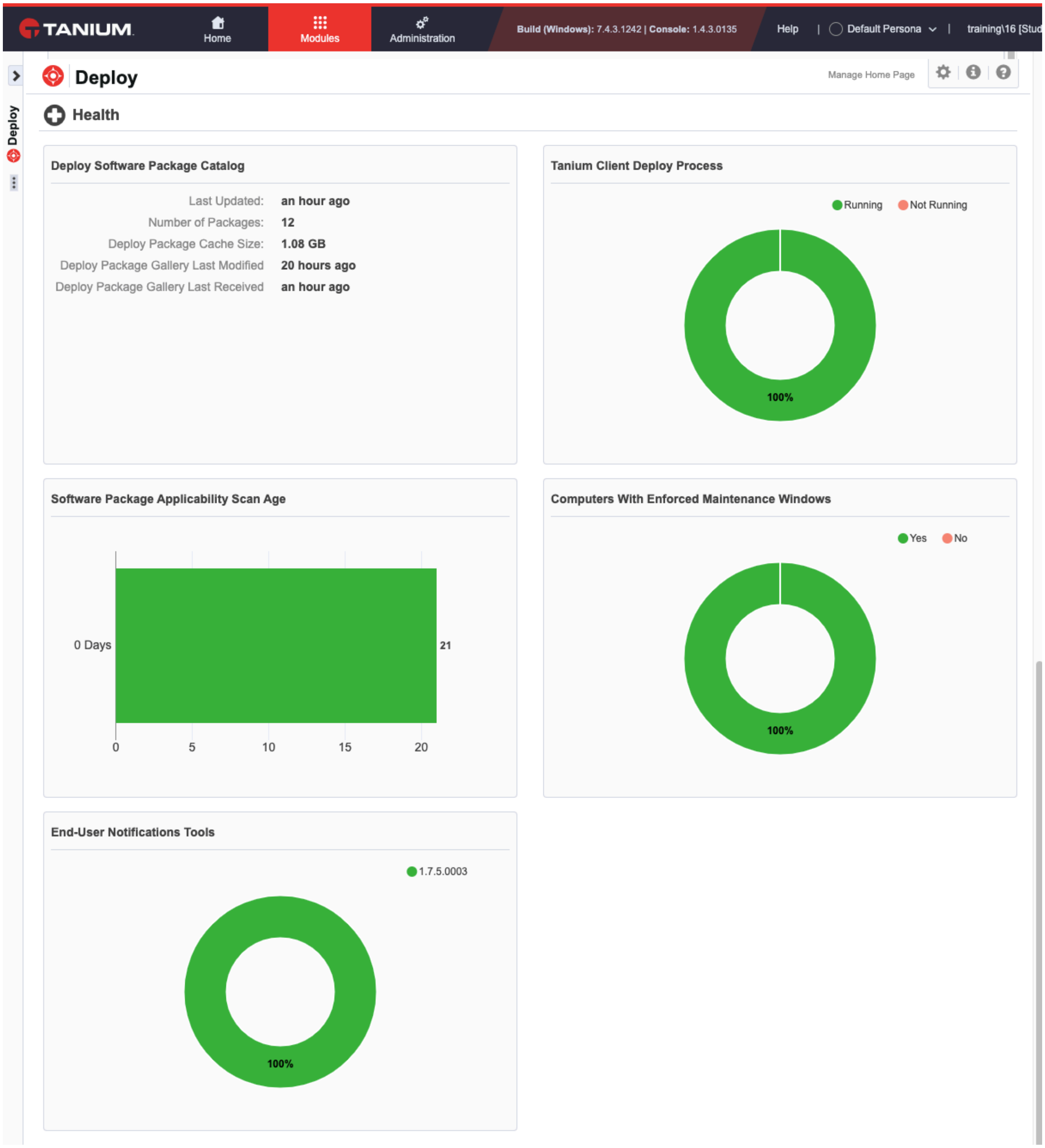
Install Eligible:	Update Eligible:	Installed:	Update Ineligible:	N/A:
0 (0%)	21 (100%)	0 (0%)	0 (0%)	0

OS Platform: Package ID: 151 Package Size: 294.63 MB Created on: 08/19/2020 Created by: Unknown Last Modified on: 08/26/2020 Last Modified by: 16 Type: Tanium

Box, Inc. Box Drive (x64 en-us) v2.16.298

Install Eligible: Update Eligible: Installed: Update Ineligible: N/A:

4. It also shows the overall health of the module:


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Stud
Deploy
Manage Home Page
Deploy
Health

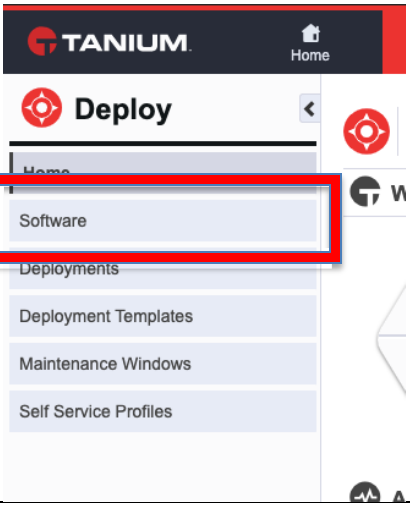
Deploy Software Package Catalog

Last Updated: an hour ago
Number of Packages: 12
Deploy Package Cache Size: 1.08 GB
Deploy Package Gallery Last Modified 20 hours ago
Deploy Package Gallery Last Received an hour ago

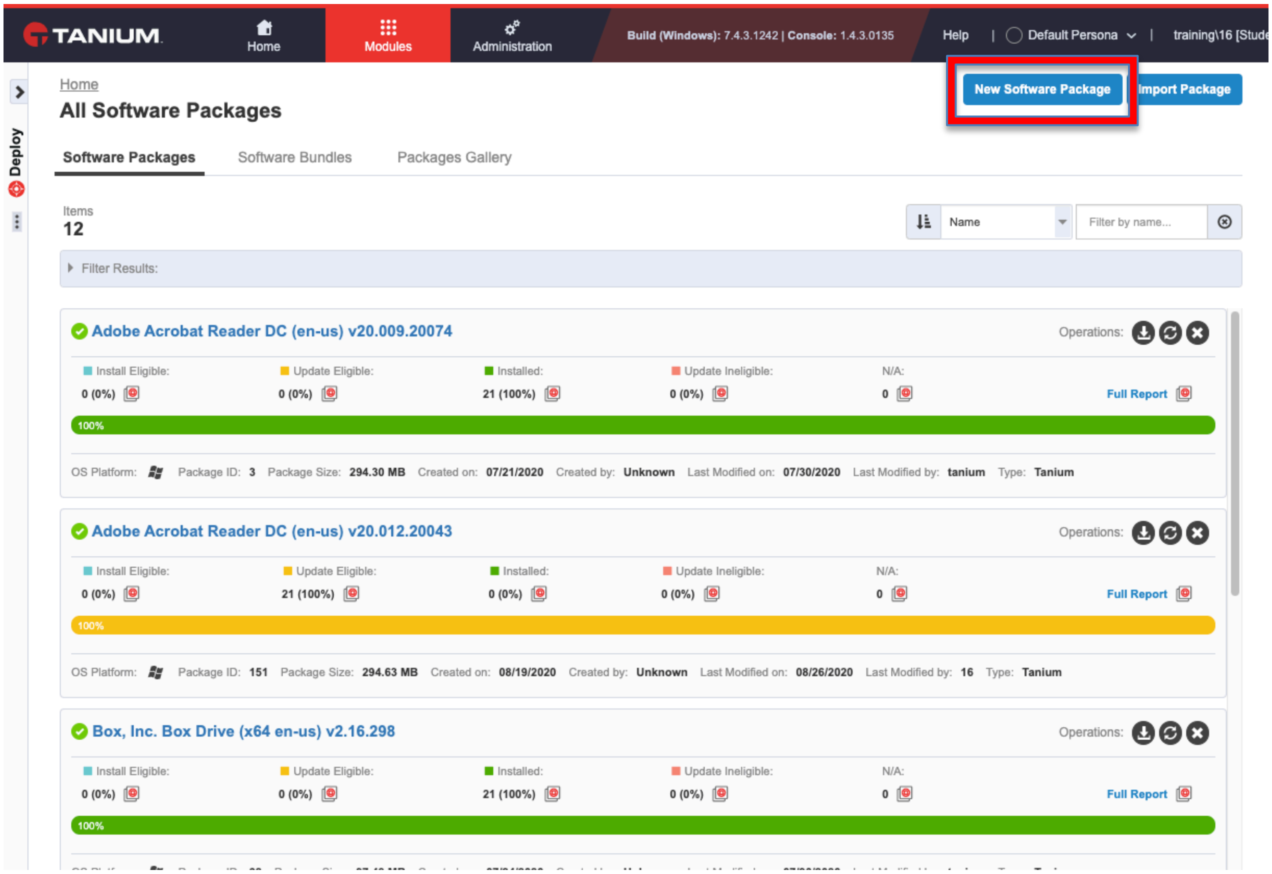
Tanium Client Deploy Process
● Running ● Not Running
100%
Software Package Applicability Scan Age
0 Days
21
0
5
10
15
20
Computers With Enforced Maintenance Windows
● Yes ● No
100%
End-User Notifications Tools
● 1.7.5.0003
100%

Explore the homepage and take a look at the various items of information available

5. Pop out the menu at the left-hand side and click on **Software**.



6. You will now see the list of available software packages. Click on New Software Package.



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135

Home

All Software Packages

Items
12

Adobe Acrobat Reader DC (en-us) v20.009.20074

Install Eligible: 0 (0%) | Update Eligible: 0 (0%) | Installed: 21 (100%) | Update Ineligible: 0 (0%) | N/A: 0

100%

OS Platform: Package ID: 3 Package Size: 294.30 MB Created on: 07/21/2020 Created by: Unknown Last Modified on: 07/30/2020 Last Modified by: tanium Type: Tanium

Adobe Acrobat Reader DC (en-us) v20.012.20043

Install Eligible: 0 (0%) | Update Eligible: 21 (100%) | Installed: 0 (0%) | Update Ineligible: 0 (0%) | N/A: 0

100%

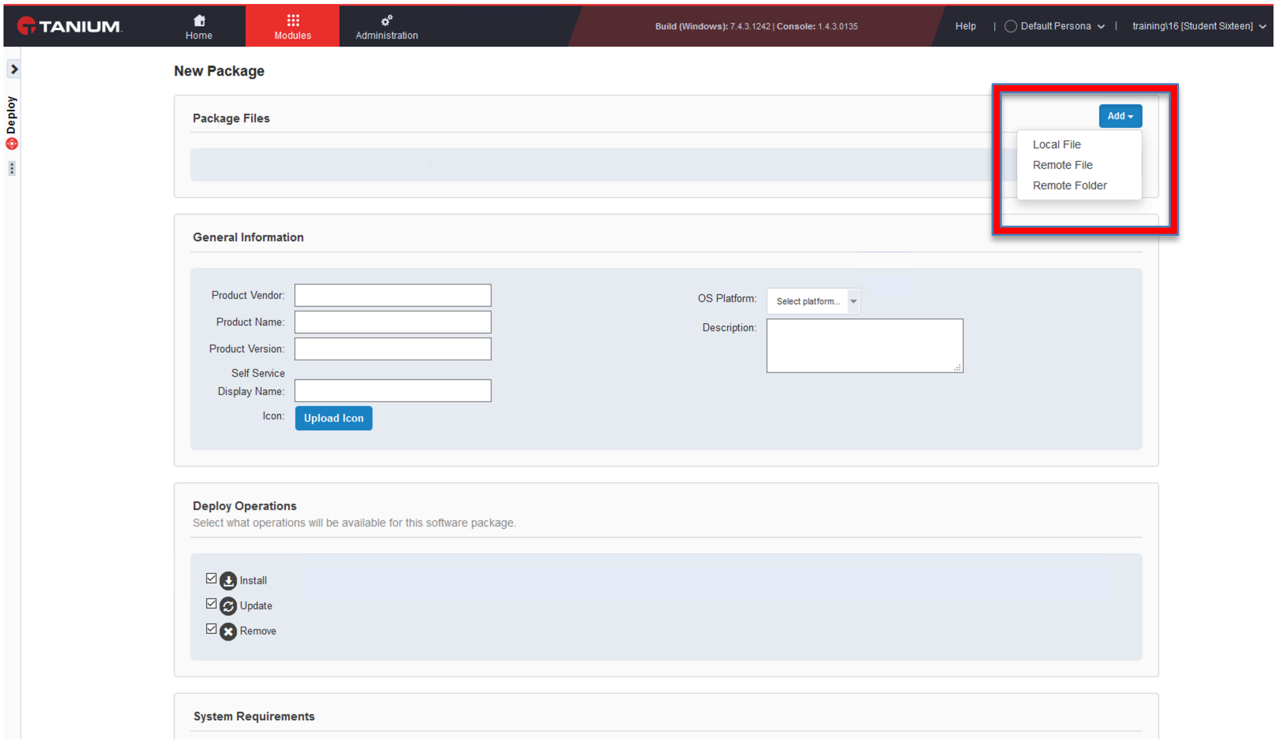
OS Platform: Package ID: 151 Package Size: 294.63 MB Created on: 08/19/2020 Created by: Unknown Last Modified on: 08/26/2020 Last Modified by: 16 Type: Tanium

Box, Inc. Box Drive (x64 en-us) v2.16.298

Install Eligible: 0 (0%) | Update Eligible: 0 (0%) | Installed: 21 (100%) | Update Ineligible: 0 (0%) | N/A: 0

100%

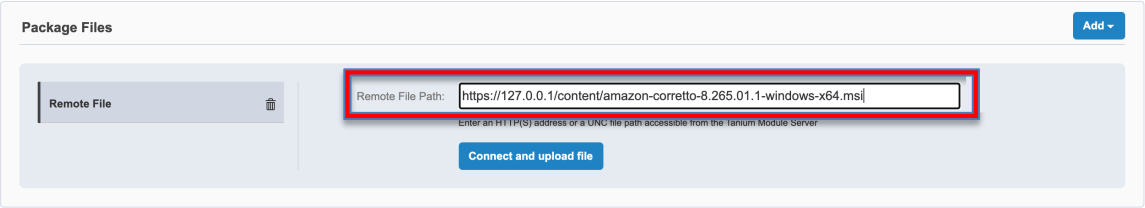
7. Click on **Add**, then select **Remote File**.



8. Add the following URL for the Remote File Path:

https://127.0.0.1/content/amazon-corretto-8.222.10.3-windows-x64.msi

For simplicity the MSI file that we will use is hosted already on the Tanium server, but this file could be hosted in any remote location.

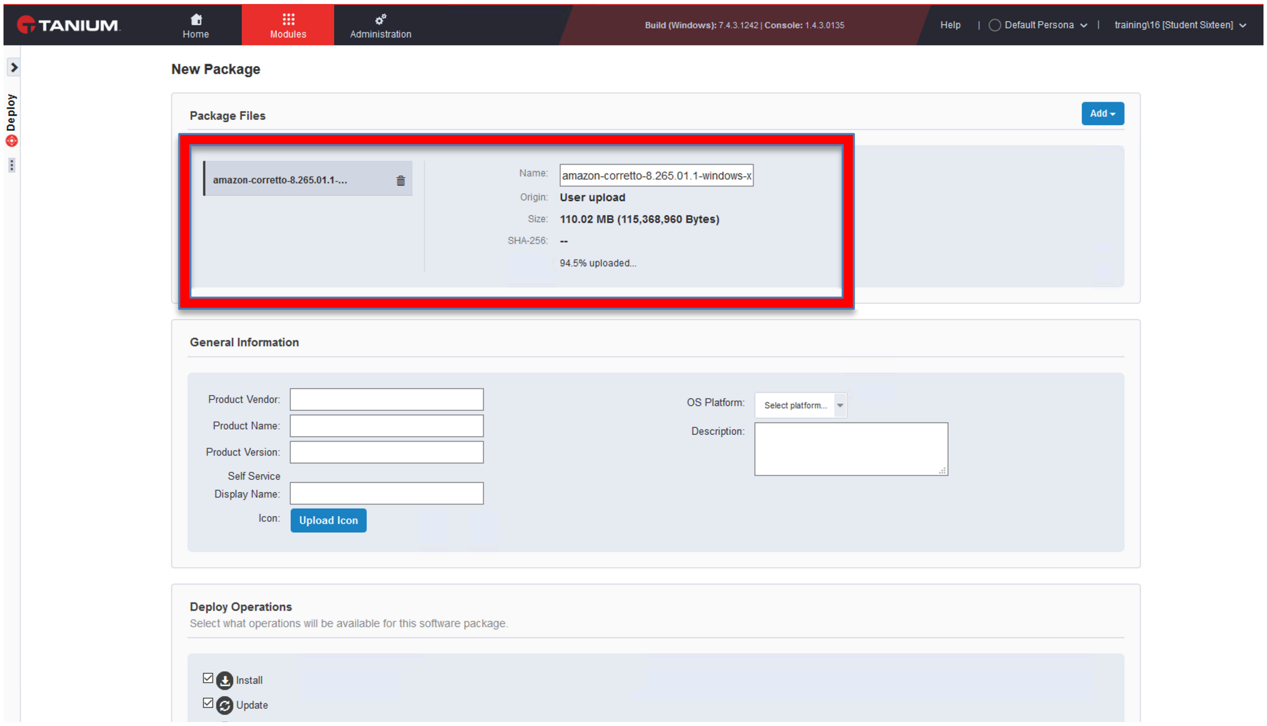


Remote File Path: https://127.0.0.1/content/amazon-corretto-8.265.01.1-windows-x64.msi

Package Files
Add
Remote File
Enter an HTTP(S) address or a UNC file path accessible from the Tanium Module Server
Connect and upload file

Now press **Connect and upload file**.

9. Your package file will now begin to upload, and upload progress will be displayed.



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135

training\16 [Student Sixteen]

New Package

Package Files

amazon-corretto-8.265.01.1-...

Name: amazon-corretto-8.265.01.1-windows-x

Origin: User upload

Size: 110.02 MB (115,368,960 Bytes)

SHA-256: --

94.5% uploaded...

General Information

Product Vendor:

Product Name:

Product Version:

Self Service Display Name:

Icon:

OS Platform: Select platform...

Description:

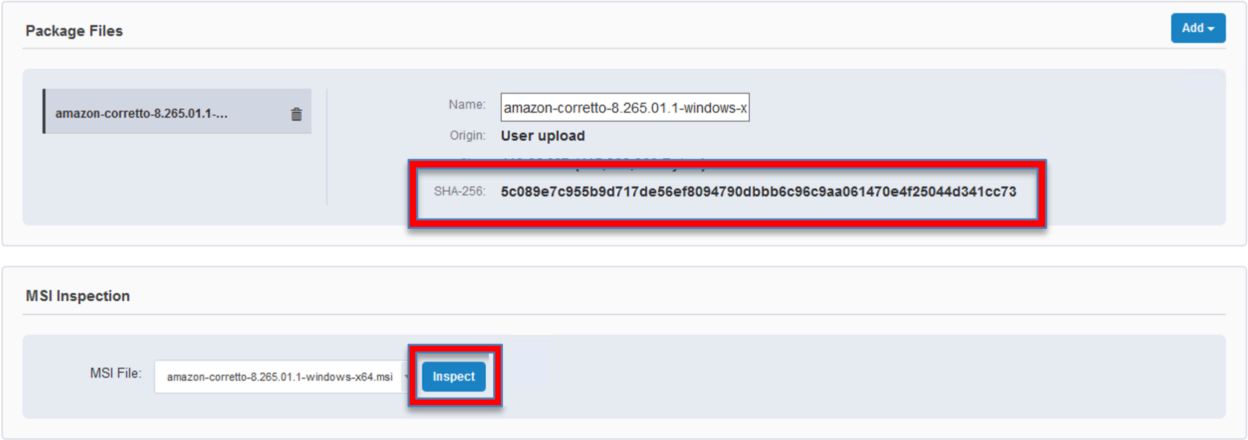
Deploy Operations

Select what operations will be available for this software package.

☑ Install

☑ Update

10. Once the upload is complete, the SHA-256 hash of the resulting file will be calculated and displayed.



Package Files

amazon-corretto-8.265.01.1-...

Name: amazon-corretto-8.265.01.1-windows-x

Origin: User upload

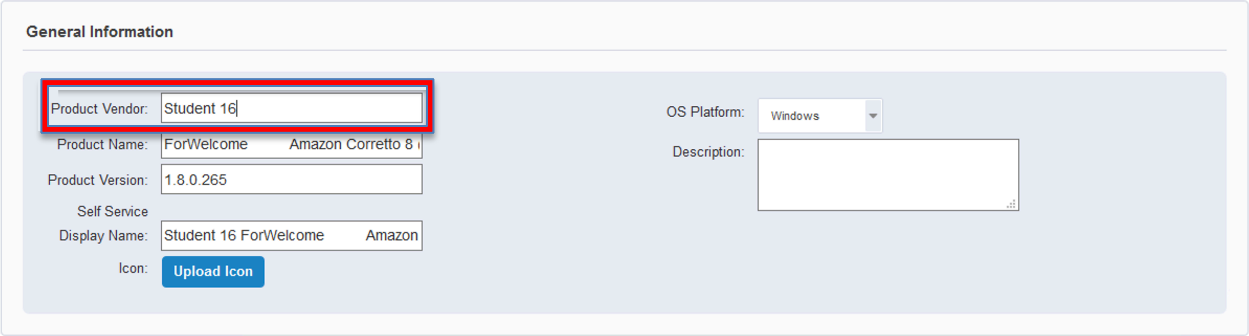
SHA-256: 5c089e7c955b9d717de56ef8094790dbbb6c96c9aa061470e4f25044d341cc73

MSI Inspection

MSI File: amazon-corretto-8.265.01.1-windows-x64.msi

As the package is an MSI file, you can now use the **Inspect** button to automatically populate the software package details using the details contained within the MSI. Click **Inspect** to complete the other fields.

11. The **General Information** section will now be populated. Change the **Product Vendor** to *Student <Student ID Number>* to ensure that your package is unique. Leave all other fields as-is.



General Information

Product Vendor: Student 16

Product Name: ForWelcome Amazon Corretto 8

Product Version: 1.8.0.265

Self Service Display Name: Student 16 ForWelcome Amazon

Icon: Upload Icon

OS Platform: Windows

Description:

Continue scrolling down the page to review the other configuration options.

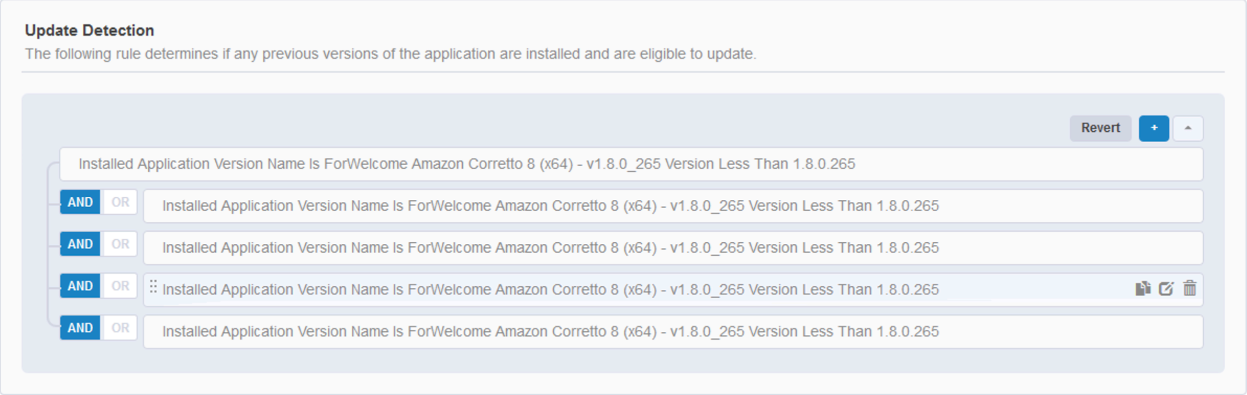
12. Further down the screen, you will see the following sections:

- **Deploy Operations** – This allows you to select which operations can be conducted with this package.
- **System Requirements** – Allows minimum requirements to be met by endpoints before the package becomes applicable, such as:
  - Minimum RAM
  - Minimum free disk space
  - Target OS version or revision level.
- **Requirements –** This allows more specific requirements to be bet before an endpoint is considered applicable, such as
  - A specific file or file version must be present or not present
  - A specific application must be installed or must not be installed
  - Specific Registry keys or values must or must not be present
  - A service name must or must not exist
  - System uptime must be less than or greater than a specific value
  - A specified WMI query either returns or does not return results

Note that your own view in the console and the data that it shows may differ slightly from what is shown in this guide. Investigate these options but leave all values as default and continue down the page.

13. The **Update Detection** section is used to determine if a package is eligible for update as opposed to installation, where a previous version of the software being delivered by the package is already installed.

If any of the conditions defined are true, an update will be conducted instead of a new install.



Update Detection

The following rule determines if any previous versions of the application are installed and are eligible to update.

Installed Application Version Name Is ForWelcome Amazon Corretto 8 (x64) - v1.8.0_265 Version Less Than 1.8.0.265

AND OR Installed Application Version Name Is ForWelcome Amazon Corretto 8 (x64) - v1.8.0_265 Version Less Than 1.8.0.265

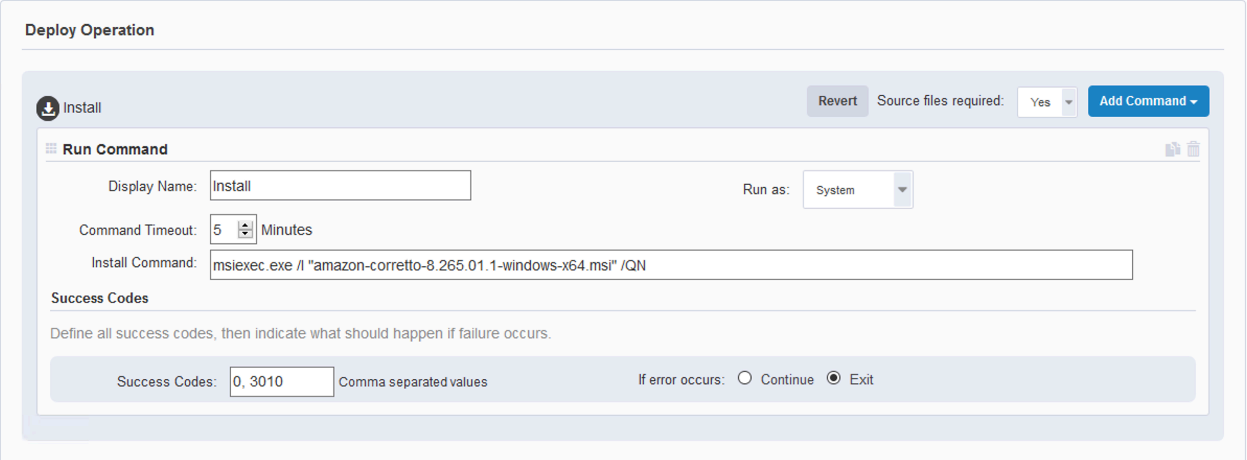
AND OR Installed Application Version Name Is ForWelcome Amazon Corretto 8 (x64) - v1.8.0_265 Version Less Than 1.8.0.265

AND OR Installed Application Version Name Is ForWelcome Amazon Corretto 8 (x64) - v1.8.0_265 Version Less Than 1.8.0.265

AND OR Installed Application Version Name Is ForWelcome Amazon Corretto 8 (x64) - v1.8.0_265 Version Less Than 1.8.0.265

14. Below this are the configuration sections which determine the activities which are conducted as part of the three possible activities enabled in the **Deploy Operations** section:

- **Install** – Carried out on eligible endpoints which have no existing version of the software



Deploy Operation

Install

Source files required: Yes

Run Command

Display Name: Install

Run as: System

Command Timeout: 5 Minutes

Install Command: msiexec.exe /I "amazon-corretto-8.265.01.1-windows-x64.msi" /QN

Success Codes

Define all success codes, then indicate what should happen if failure occurs.

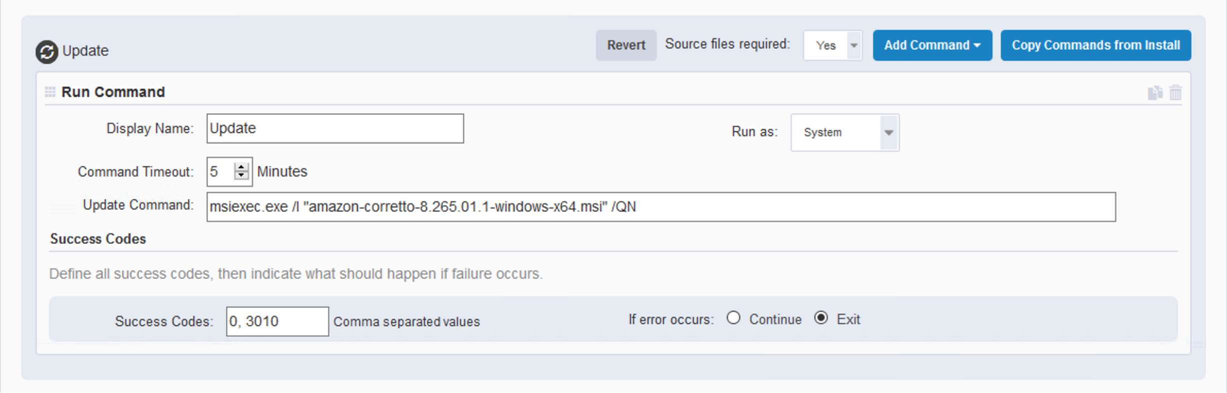
Success Codes: 0, 3010 Comma separated values

If error occurs: ○ Continue ● Exit

In this example, the MSI itself has populated the installation command line based on the detail contained within the MSI database. Additional commands can be added if need be

15.

- **Update** – Should an endpoint satisfy one of the conditions configured in **Update Detection**, then an update will be conducted as opposed to an installation.



Source files required: Yes

Display Name: Update

Run as: System

Command Timeout: 5 Minutes

Update Command: msiexec.exe /I "amazon-corretto-8.265.01.1-windows-x64.msi" /QN

Success Codes

Define all success codes, then indicate what should happen if failure occurs.

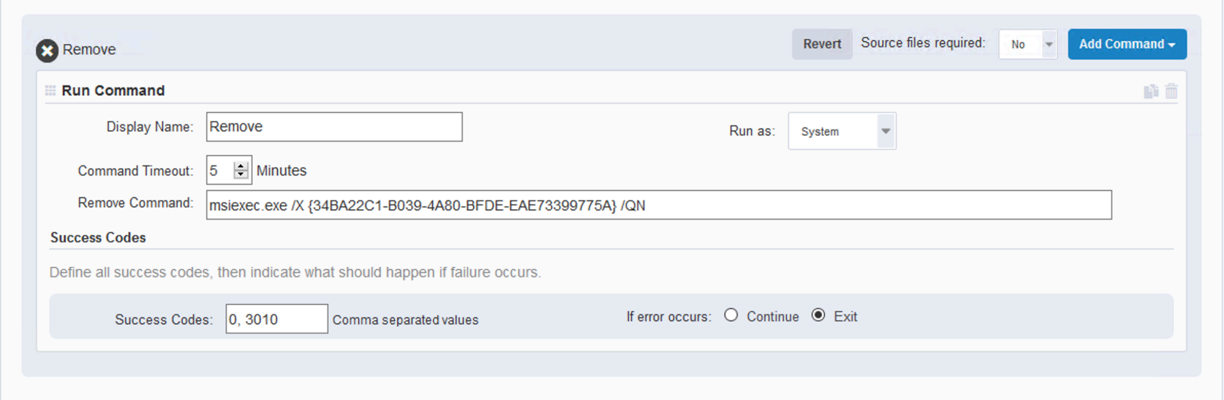
Success Codes: 0, 3010 Comma separated values

If error occurs: ○ Continue ● Exit

The update command line has also been provided via the MSI inspection and the detail returned from within the software package MSI database.

16.

- **Remove –** This is used to cleanly remove managed software packages



Source files required: No

Display Name: Remove

Run as: System

Command Timeout: 5 Minutes

Remove Command: msiexec.exe /X {34BA22C1-B039-4A80-BFDE-EAE73399775A} /QN

Success Codes

Define all success codes, then indicate what should happen if failure occurs.

Success Codes: 0, 3010 Comma separated values

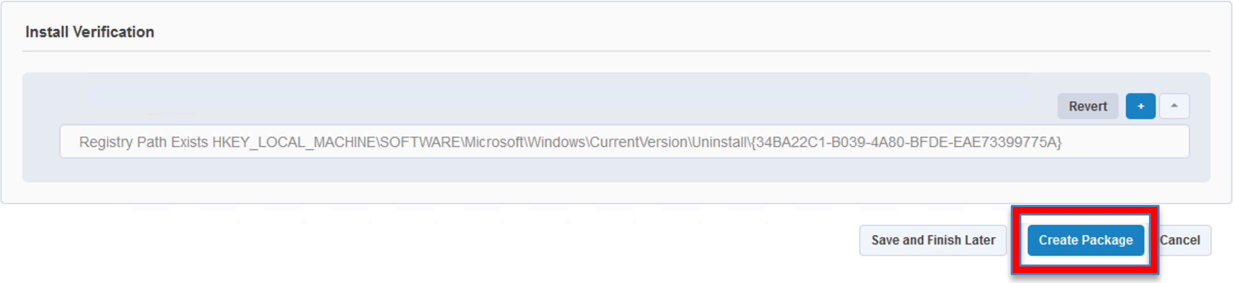
If error occurs: ○ Continue ● Exit

Once again, you can see here that the command line has been auto-populate by MSI inspection.

17. Finally, the **Install Verification** section is located at the bottom.

This allows Tanium to verify is a package has been successfully delivered. If a package is evaluated against an endpoint and it passes the verification criteria set, the install will have been considered successful, the package registered as installed and will not be attempted again. Here again, you can see that MSI inspection has completed this for us.

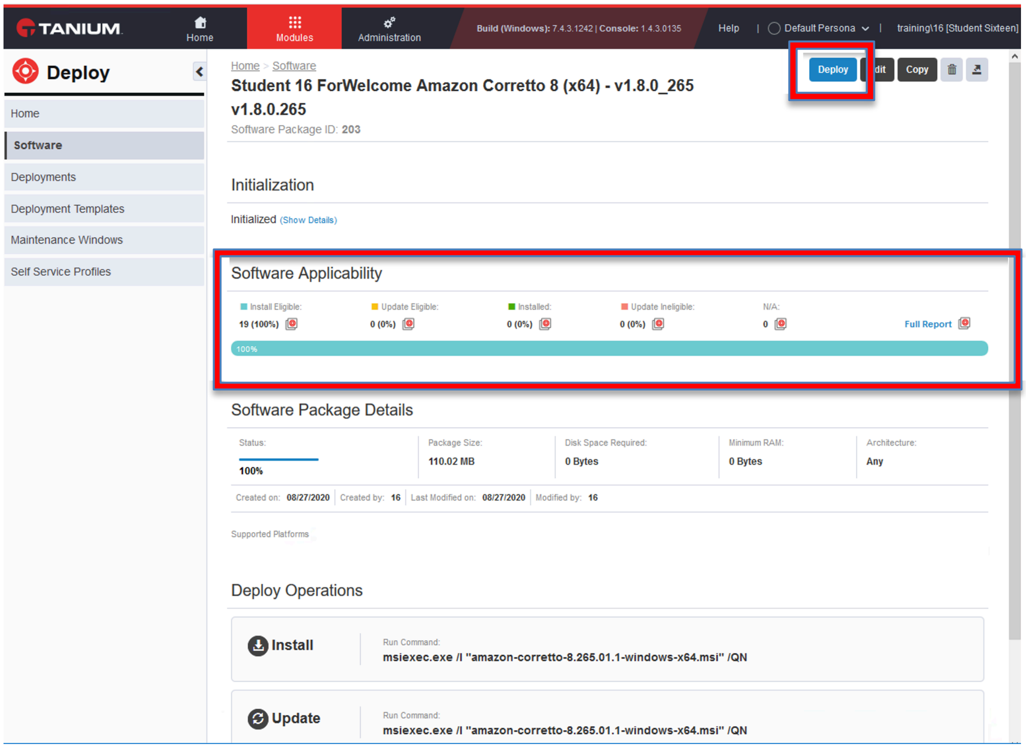
Once you have reviewed all settings, click on **Create Package** then **Yes** to commit the changes.



Install Verification

Registry Path Exists HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{34BA22C1-B039-4A80-BFDE-EAE73399775A}

18. You will now see a summary of the package you created. The software catalogue will be updated behind the scenes and the endpoints will then evaluate eligibility against all packages in the catalogue. After a short time, you will see the results in the Software Applicability section.



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135

training\16 [Student Sixteen]

Home > Software

Student 16 ForWelcome Amazon Corretto 8 (x64) - v1.8.0_265 v1.8.0.265

Software Package ID: 203

Initialization

Initialized (Show Details)

Software Applicability

Install Eligible:	Update Eligible:	Installed:	Update Ineligible:	N/A:
19 (100%)	0 (0%)	0 (0%)	0 (0%)	0

100%

Software Package Details

Status:	Package Size:	Disk Space Required:	Minimum RAM:	Architecture:
100%	110.02 MB	0 Bytes	0 Bytes	Any

Created on: 08/27/2020 | Created by: 16 | Last Modified on: 08/27/2020 | Modified by: 16

Supported Platforms

Deploy Operations

Install — Run Command:

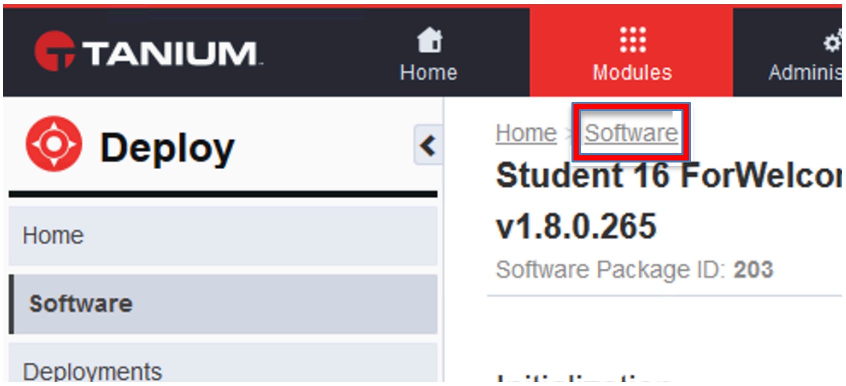
```
msiexec.exe /I "amazon-corretto-8.265.01.1-windows-x64.msi" /QN
```

Update — Run Command:

```
msiexec.exe /I "amazon-corretto-8.265.01.1-windows-x64.msi" /QN
```

Clicking on the **Deploy** button here would allow us to create a deployment. Click the button and explore the options but do not actually deploy the software. Click **Cancel** to exit when ready.

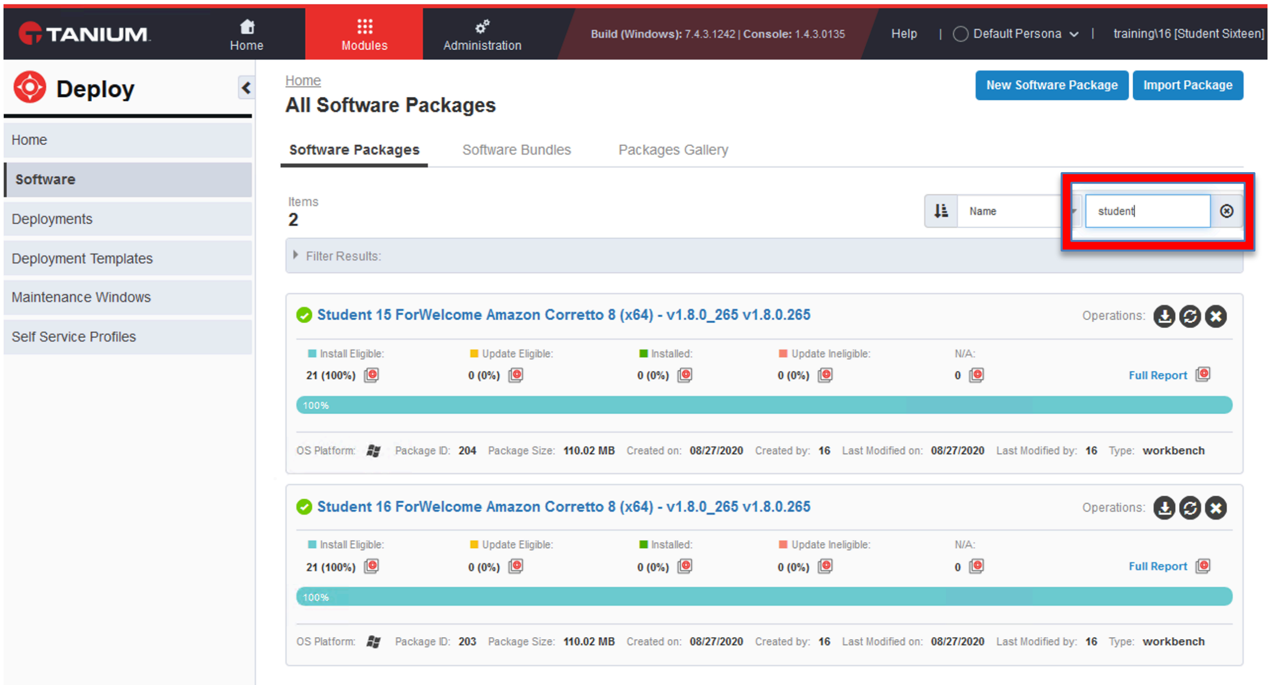
19. Click **Software** on the Breadcrumb bar at the top to return to the Software workbench.



Student 16 ForWelcoı
v1.8.0.265
Software Package ID: 203

20. Enter the word *student* into the **Filter by Name** field on the left-hand side. This will filter the list of available packages and only display your own, and the other students' packages, along with the eligibility of the packages on each endpoint in the lab environment.

Make sure your package is present.



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135 | training\16 [Student Sixteen]

All Software Packages

Items 2

student

Student 15 ForWelcome Amazon Corretto 8 (x64) - v1.8.0_265 v1.8.0.265

Install Eligible:	Update Eligible:	Installed:	Update Ineligible:	N/A:
21 (100%)	0 (0%)	0 (0%)	0 (0%)	0

100%

OS Platform: Package ID: 204 Package Size: 110.02 MB Created on: 08/27/2020 Created by: 16 Last Modified on: 08/27/2020 Last Modified by: 16 Type: workbench

Student 16 ForWelcome Amazon Corretto 8 (x64) - v1.8.0_265 v1.8.0.265

Install Eligible:	Update Eligible:	Installed:	Update Ineligible:	N/A:
21 (100%)	0 (0%)	0 (0%)	0 (0%)	0

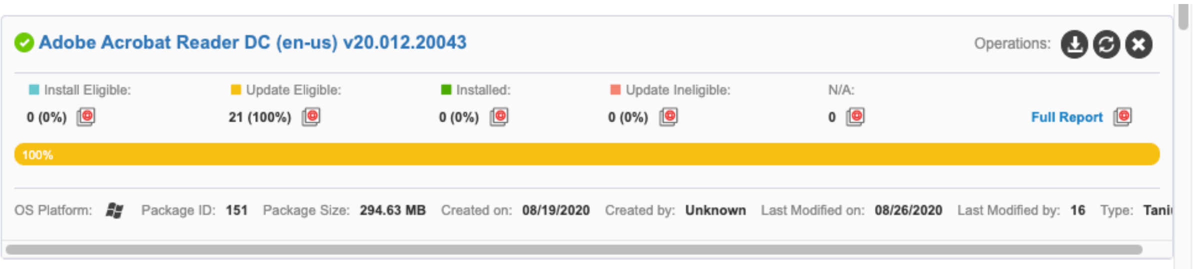
100%

OS Platform: Package ID: 203 Package Size: 110.02 MB Created on: 08/27/2020 Created by: 16 Last Modified on: 08/27/2020 Last Modified by: 16 Type: workbench

You have now successfully created a software package!

21. We will now look at upgrading an existing software package where a previous version exists. First of all, clear the word *student* from the **Filter by Name** field to display all packages.

Students 1 – 20: Locate the package named *Adobe Acrobat Reader DC (en-us)*



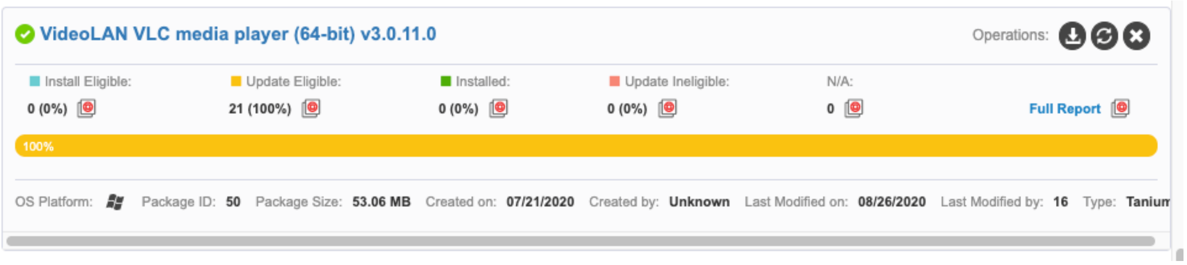
✓ Adobe Acrobat Reader DC (en-us) v20.012.20043 — Operations: ⬇ ⟳ ✖

Install Eligible:	Update Eligible:	Installed:	Update Ineligible:	N/A:	
0 (0%)	21 (100%)	0 (0%)	0 (0%)	0	Full Report

100%

OS Platform: Package ID: 151 Package Size: 294.63 MB Created on: 08/19/2020 Created by: Unknown Last Modified on: 08/26/2020 Last Modified by: 16 Type: Tani

Students 21 – 40: Locate the package named *VideoLAN VLC media player (64-bit)*



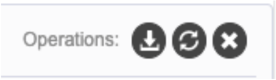
✓ VideoLAN VLC media player (64-bit) v3.0.11.0 — Operations: ⬇ ⟳ ✖

Install Eligible:	Update Eligible:	Installed:	Update Ineligible:	N/A:	
0 (0%)	21 (100%)	0 (0%)	0 (0%)	0	Full Report

100%

OS Platform: Package ID: 50 Package Size: 53.06 MB Created on: 07/21/2020 Created by: Unknown Last Modified on: 08/26/2020 Last Modified by: 16 Type: Taniur

We will use *Adobe Acrobat Reader DC (en-us) v20.012.20043* in the following examples for the purposes of this lab guide but the same process applies if you are deploying the VideoLAN package.
As you can see, both packages show all lab clients as eligible for upgrade. When you have located the package, you will see an Operations section to the right of the package entry as shown below.



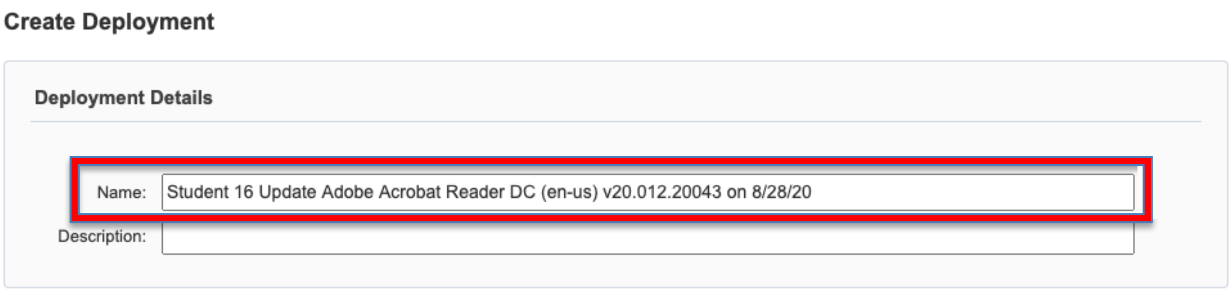
Operations: ⬇ ⟳ ✖

These icons correspond to the available operations configured in the **Deploy Operations** section of the package. Only those enabled within the package will be show. These are as follows:

- ⬇ Install
- ⟳ Update
- ✖ Remove

Click on ⟳ to create a new update deployment of the package assigned to you in line with your assigned student ID number.

22. The **Create Deployment** page will now be displayed. In the **Deployment Details** section, change the **Name** field so that it is prefixed by *Student <student ID number>* as shown below:



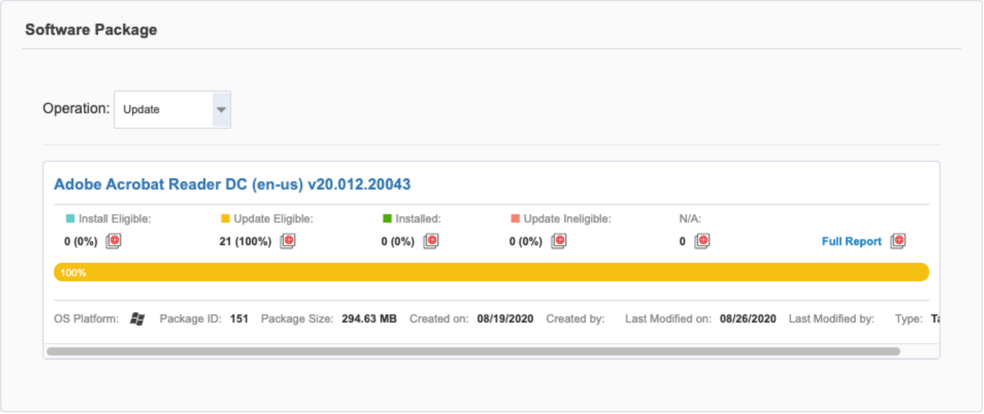
Create Deployment

Deployment Details

Name: Student 16 Update Adobe Acrobat Reader DC (en-us) v20.012.20043 on 8/28/20

Description:

The **Software Package** section should show the package you selected, and the **Operation** should say *Update*. Leave this as it is.



Software Package

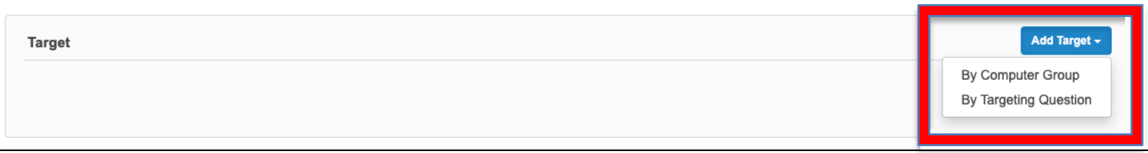
Operation: Update

Adobe Acrobat Reader DC (en-us) v20.012.20043

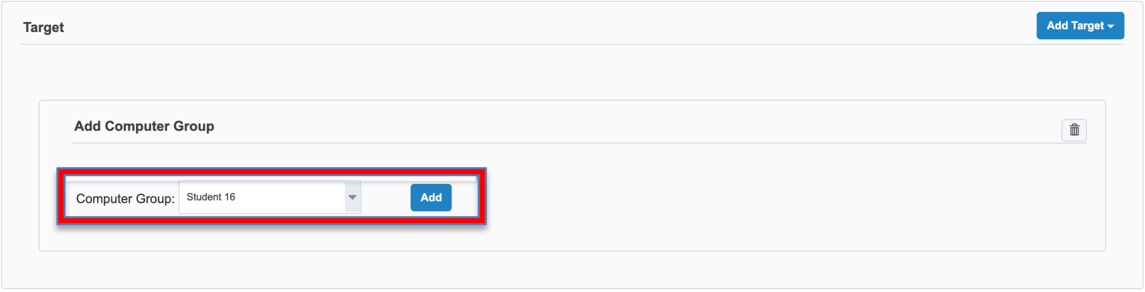
Install Eligible:	Update Eligible:	Installed:	Update Ineligible:	N/A:
0 (0%)	21 (100%)	0 (0%)	0 (0%)	0

OS Platform: Package ID: 151 Package Size: 294.63 MB Created on: 08/19/2020 Created by: Last Modified on: 08/26/2020 Last Modified by: Type: T

Under the **Target** section, you now need to specify which endpoints will receive the deployment. Click on **Add Target** and choose *By Computer Group*.



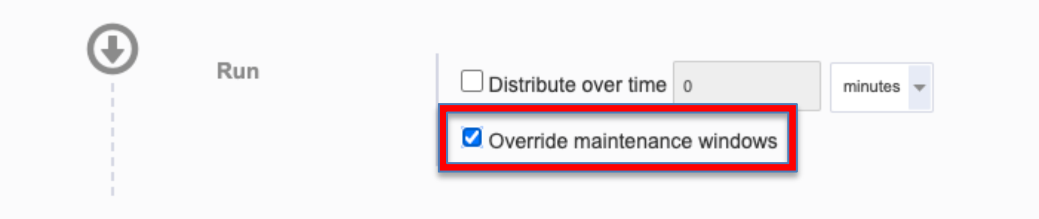
23. From the **Computer** Group dropdown control select the computer group that applies to your assigned student number, then press **Add**.



Computer Group: Student 16

24. Scroll down and review the other settings but leave them unchanged until you reach the **Run** section.

Here, enable the checkbox against **Override maintenance windows**.



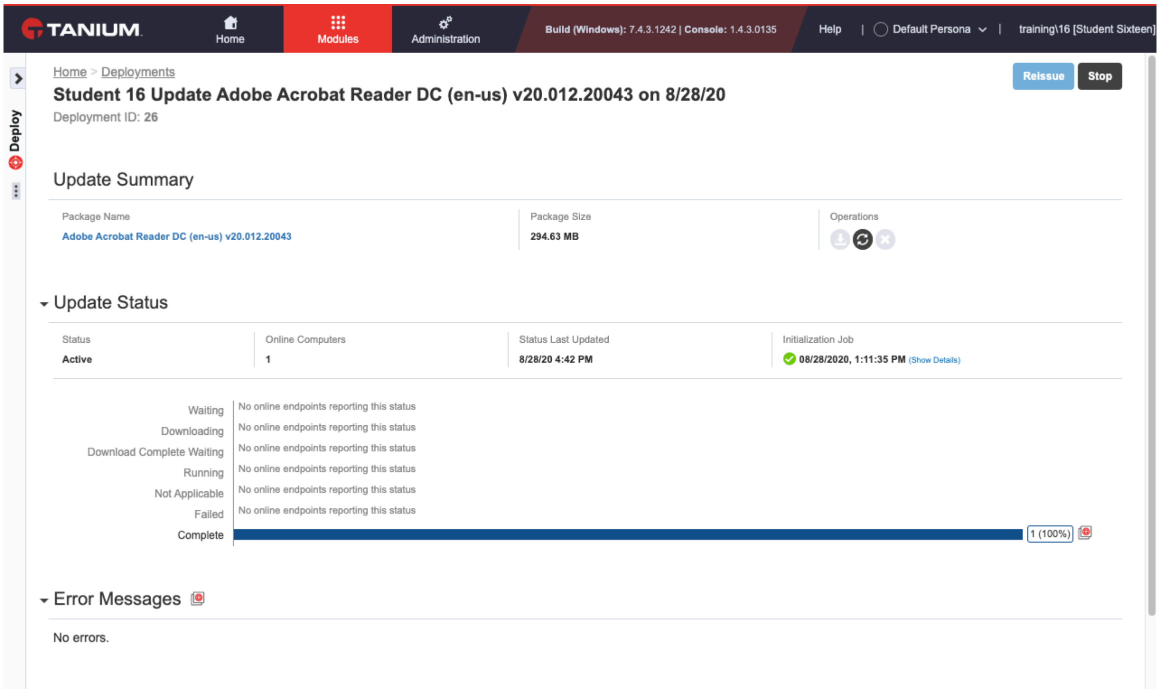
Run

□ Distribute over time 0 minutes

☑ Override maintenance windows

Leave all other settings as default and click on **Create Deployment** at the bottom of the page and confirm by clicking **Yes** to commit your changes.

25. A summary of your deployment will now appear, similar to that shown previously when you created deployed a patch in lab 6.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Deploy
Reissue
Stop

Home > Deployments

Student 16 Update Adobe Acrobat Reader DC (en-us) v20.012.20043 on 8/28/20

Deployment ID: 26

Update Summary

Package Name	Package Size	Operations
Adobe Acrobat Reader DC (en-us) v20.012.20043	294.63 MB	

Update Status

Status	Online Computers	Status Last Updated	Initialization Job
Active	1	8/28/20 4:42 PM	✓ 08/28/2020, 1:11:35 PM (Show Details)

Waiting	No online endpoints reporting this status
Downloading	No online endpoints reporting this status
Download Complete Waiting	No online endpoints reporting this status
Running	No online endpoints reporting this status
Not Applicable	No online endpoints reporting this status
Failed	No online endpoints reporting this status
Complete	1 (100%)

Error Messages

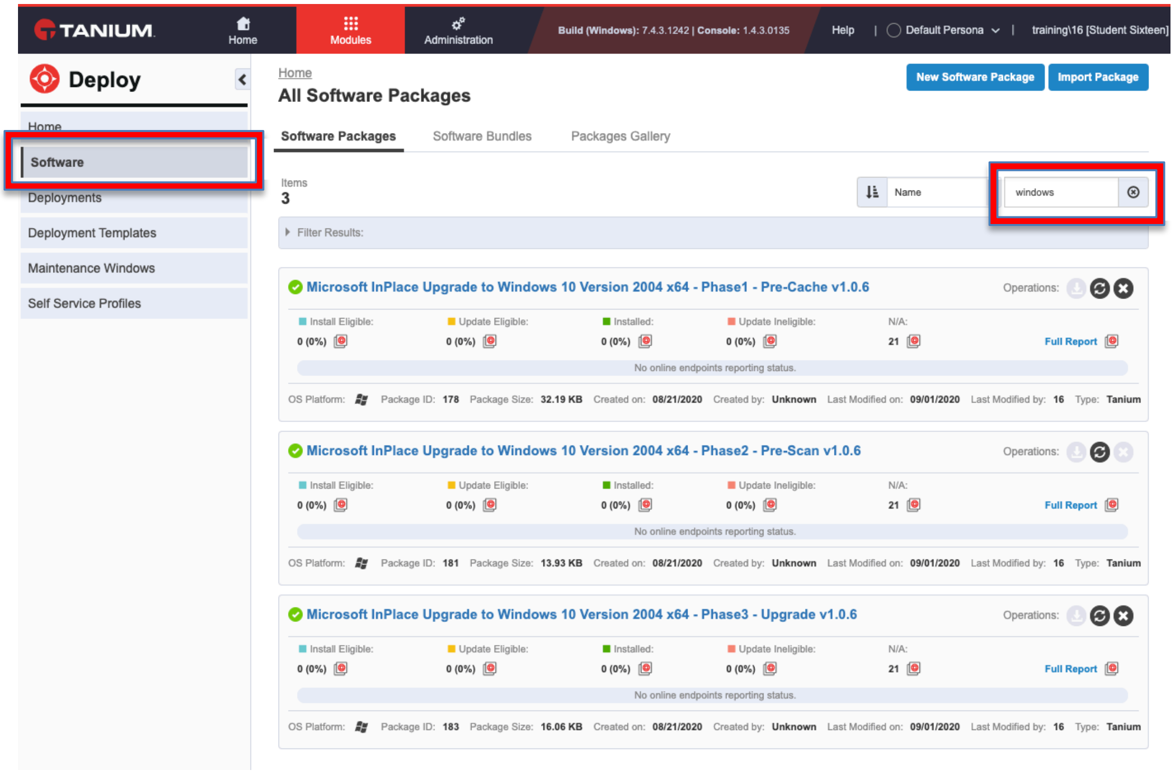
No errors.

Once the software has been updated, it will be reflected as complete as shown above. You can wait here at this screen until the deployment has completed or continue onwards with the remaining steps in this lab.

26. Alongside software management, Tanium Deploy will also perform Windows 10 operating system upgrades using Windows in-place servicing capabilities.

The packages that you will use for the remainder of this lab have already been imported by your instructor. These can be found in the Deploy software package list, accessible from the Software option in the pop-out menu as shown below.

Use the term *windows* in the **Filter by name** field to find them.



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135

training\16 [Student Sixteen]

Home

All Software Packages

Items 3

windows

Microsoft InPlace Upgrade to Windows 10 Version 2004 x64 - Phase1 - Pre-Cache v1.0.6

Install Eligible: 0 (0%) Update Eligible: 0 (0%) Installed: 0 (0%) Update Ineligible: 0 (0%) N/A: 21

No online endpoints reporting status.

OS Platform: Package ID: 178 Package Size: 32.19 KB Created on: 08/21/2020 Created by: Unknown Last Modified on: 09/01/2020 Last Modified by: 16 Type: Tanium

Microsoft InPlace Upgrade to Windows 10 Version 2004 x64 - Phase2 - Pre-Scan v1.0.6

Install Eligible: 0 (0%) Update Eligible: 0 (0%) Installed: 0 (0%) Update Ineligible: 0 (0%) N/A: 21

No online endpoints reporting status.

OS Platform: Package ID: 181 Package Size: 13.93 KB Created on: 08/21/2020 Created by: Unknown Last Modified on: 09/01/2020 Last Modified by: 16 Type: Tanium

Microsoft InPlace Upgrade to Windows 10 Version 2004 x64 - Phase3 - Upgrade v1.0.6

Install Eligible: 0 (0%) Update Eligible: 0 (0%) Installed: 0 (0%) Update Ineligible: 0 (0%) N/A: 21

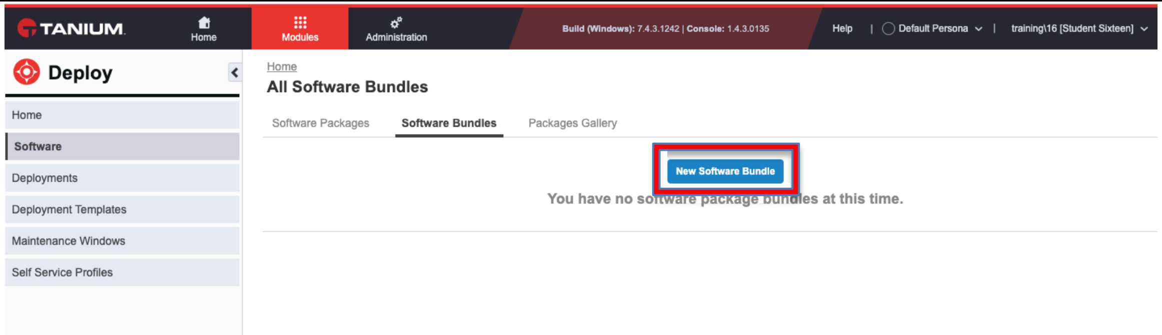
No online endpoints reporting status.

OS Platform: Package ID: 183 Package Size: 16.06 KB Created on: 08/21/2020 Created by: Unknown Last Modified on: 09/01/2020 Last Modified by: 16 Type: Tanium

Investigate the packages to get an understanding of the overall workflow, and the part each package plays in the upgrade process. Further detail is available online or speaking with a Technical Account Manager.

27. Perhaps you have a deployment that consists of multiple pieces, such as dependencies and middleware required for an application to function. Tanium can manage the installation of all of these pieces as one single deployment by employing a **Software Bundle**. In this section we will now link some packages together for deployment.

From the **Software** section, select **Software Bundles**. Then press **New Software Bundle**.



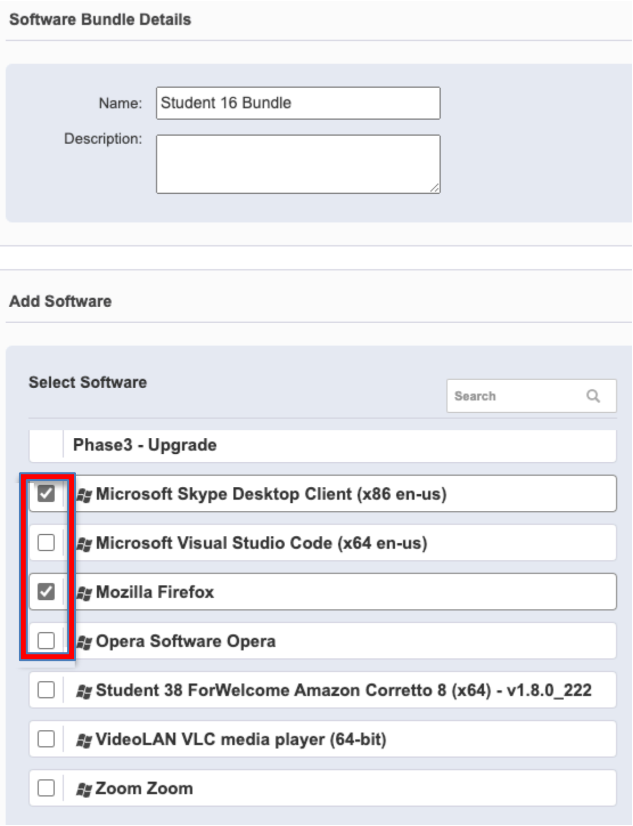
All Software Bundles

You have no software package bundles at this time.

28. In this step you are going to create, and enforce, a common baseline of components that are to be deployed on all managed endpoints. If any of these components are missing or uninstalled, Tanium will return them to an installed state quickly.

Configure the following items:

- **Name**: Student 16 Bundle
- **Select Software**: Adobe Acrobat Reader DC (en-us), Igor Pavlov 7-Zip x64, Microsoft Skype Desktop Client (x86 en-us), Mozilla Firefox



Software Bundle Details

Name: Student 16 Bundle

Description:

Add Software

Select Software

Phase3 - Upgrade

☑ Microsoft Skype Desktop Client (x86 en-us)

□ Microsoft Visual Studio Code (x64 en-us)

☑ Mozilla Firefox

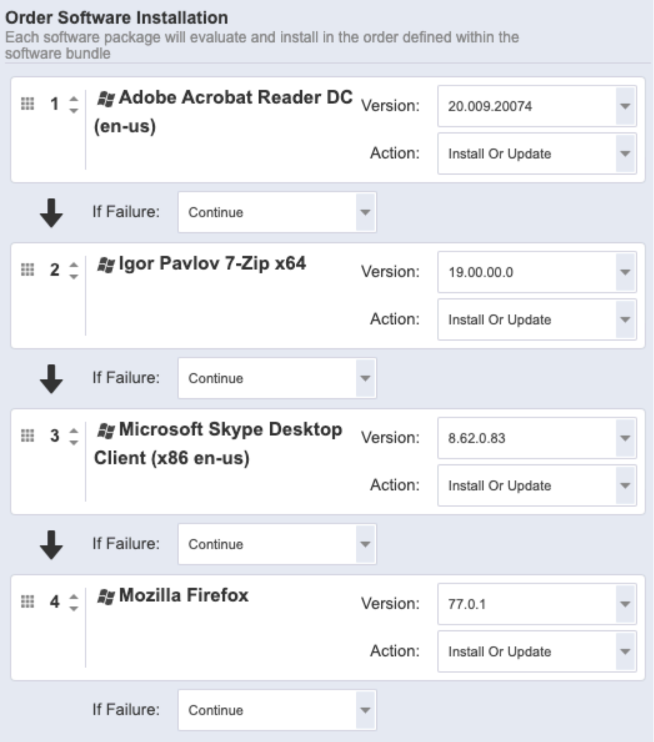
□ Opera Software Opera

□ Student 38 ForWelcome Amazon Corretto 8 (x64) - v1.8.0_222

□ VideoLAN VLC media player (64-bit)

□ Zoom Zoom

29. In the **Order Software Installation** section, configure it exactly as shown in the screenshot below.



Order Software Installation

Each software package will evaluate and install in the order defined within the software bundle

1 Adobe Acrobat Reader DC (en-us) Version: 20.009.20074 Action: Install Or Update

If Failure: Continue

2 Igor Pavlov 7-Zip x64 Version: 19.00.00.0 Action: Install Or Update

If Failure: Continue

3 Microsoft Skype Desktop Client (x86 en-us) Version: 8.62.0.83 Action: Install Or Update

If Failure: Continue

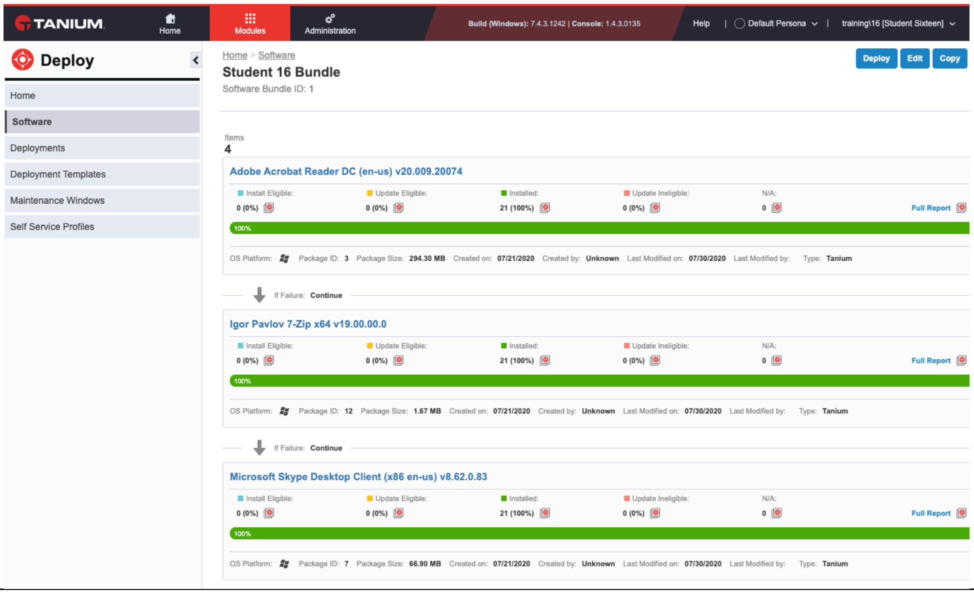
4 Mozilla Firefox Version: 77.0.1 Action: Install Or Update

If Failure: Continue

These settings will ensure that specific versions of these applications are always maintained in an installed state on all managed endpoints.

Press the **Create Bundle** button.

30. You will now be shown the summary page for this bundle.



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135

training\16 [Student Sixteen]

Home > Software

Student 16 Bundle

Software Bundle ID: 1

Items
4

Adobe Acrobat Reader DC (en-us) v20.009.20074

Install Eligible: 0 (0%) Update Eligible: 0 (0%) Installed: 21 (100%) Update Ineligible: 0 (0%) N/A: 0

100%

OS Platform: Package ID: 3 Package Size: 294.30 MB Created on: 07/21/2020 Created by: Unknown Last Modified on: 07/30/2020 Last Modified by: Type: Tanium

If Failure: Continue

Igor Pavlov 7-Zip x64 v19.00.00.0

Install Eligible: 0 (0%) Update Eligible: 0 (0%) Installed: 21 (100%) Update Ineligible: 0 (0%) N/A: 0

100%

OS Platform: Package ID: 12 Package Size: 1.67 MB Created on: 07/21/2020 Created by: Unknown Last Modified on: 07/30/2020 Last Modified by: Type: Tanium

If Failure: Continue

Microsoft Skype Desktop Client (x86 en-us) v8.62.0.83

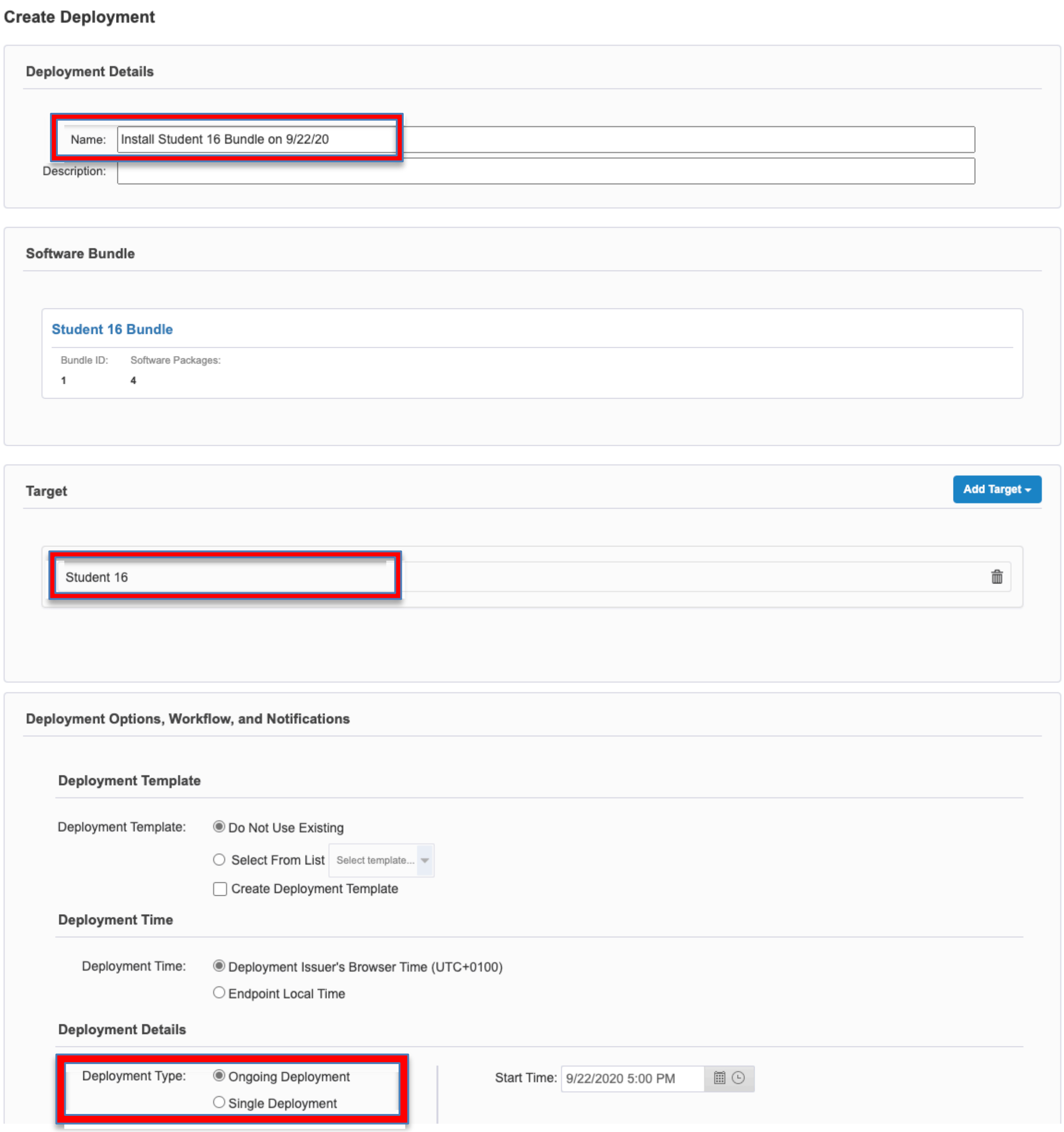
Install Eligible: 0 (0%) Update Eligible: 0 (0%) Installed: 21 (100%) Update Ineligible: 0 (0%) N/A: 0

100%

OS Platform: Package ID: 7 Package Size: 66.90 MB Created on: 07/21/2020 Created by: Unknown Last Modified on: 07/30/2020 Last Modified by: Type: Tanium

31. Press the **Deploy** button to now realise the installation. Make sure that you configure the following items, leaving all other settings as their default:

Name: Install Student <Student ID Number> Bundle
Target: *By Computer Group* and select your associated student group
Deployment Type: Ongoing Deployment



Create Deployment

Deployment Details

Name: Install Student 16 Bundle on 9/22/20
Description:

Software Bundle

Student 16 Bundle

Bundle ID:	Software Packages:
1	4

Target

Student 16

Deployment Options, Workflow, and Notifications

Deployment Template

Deployment Template: ● Do Not Use Existing
○ Select From List Select template...
□ Create Deployment Template

Deployment Time

Deployment Time: ● Deployment Issuer's Browser Time (UTC+0100)
○ Endpoint Local Time

Deployment Details

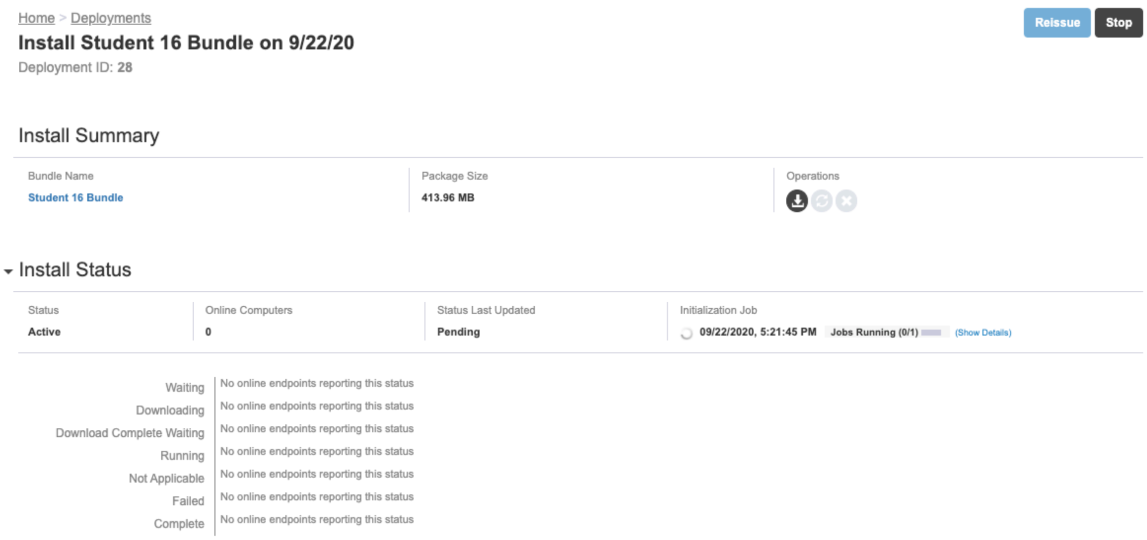
Deployment Type: ● Ongoing Deployment
○ Single Deployment

Start Time: 9/22/2020 5:00 PM

Press the **Create Deployment** button.

The use of a **Continuous Deployment** for this bundle means that the deployment is open-ended, and thus Tanium will repeatedly evaluate the conditions that it contains and resolve them should any deviation occur.

A summary screen is displayed.



Home > Deployments

Install Student 16 Bundle on 9/22/20

Deployment ID: 28

Install Summary

Bundle Name	Package Size	Operations
Student 16 Bundle	413.96 MB	

Install Status

Status	Online Computers	Status Last Updated	Initialization Job
Active	0	Pending	09/22/2020, 5:21:45 PM Jobs Running (0/1) (Show Details)

Waiting	No online endpoints reporting this status
Downloading	No online endpoints reporting this status
Download Complete Waiting	No online endpoints reporting this status
Running	No online endpoints reporting this status
Not Applicable	No online endpoints reporting this status
Failed	No online endpoints reporting this status
Complete	No online endpoints reporting this status

You have now completed Lab 7.

Lab 8: Shields Up!

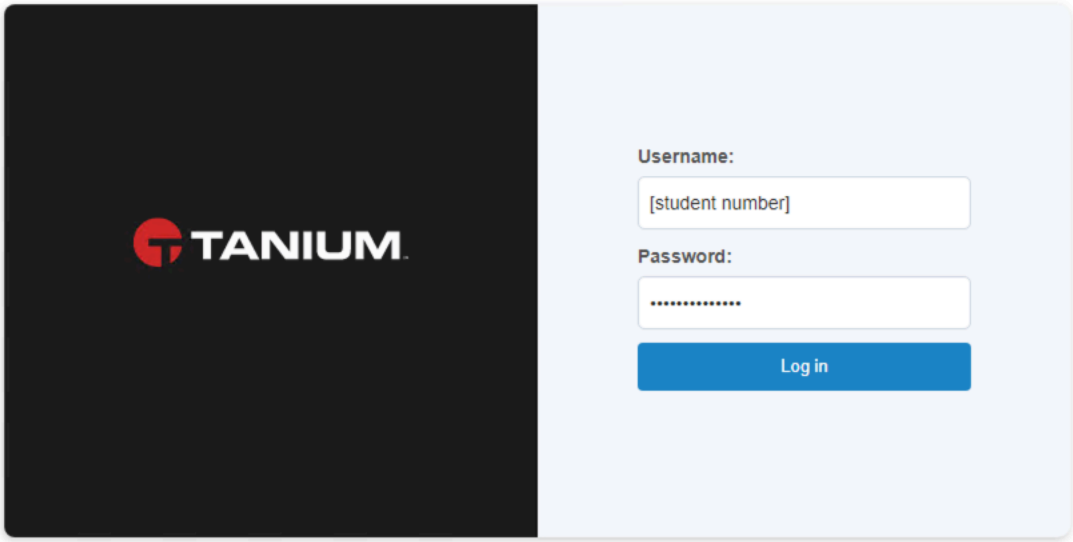
Defending your assets using Tanium Protect.

Objectives

By the end of this lab you will have completed the following objectives:

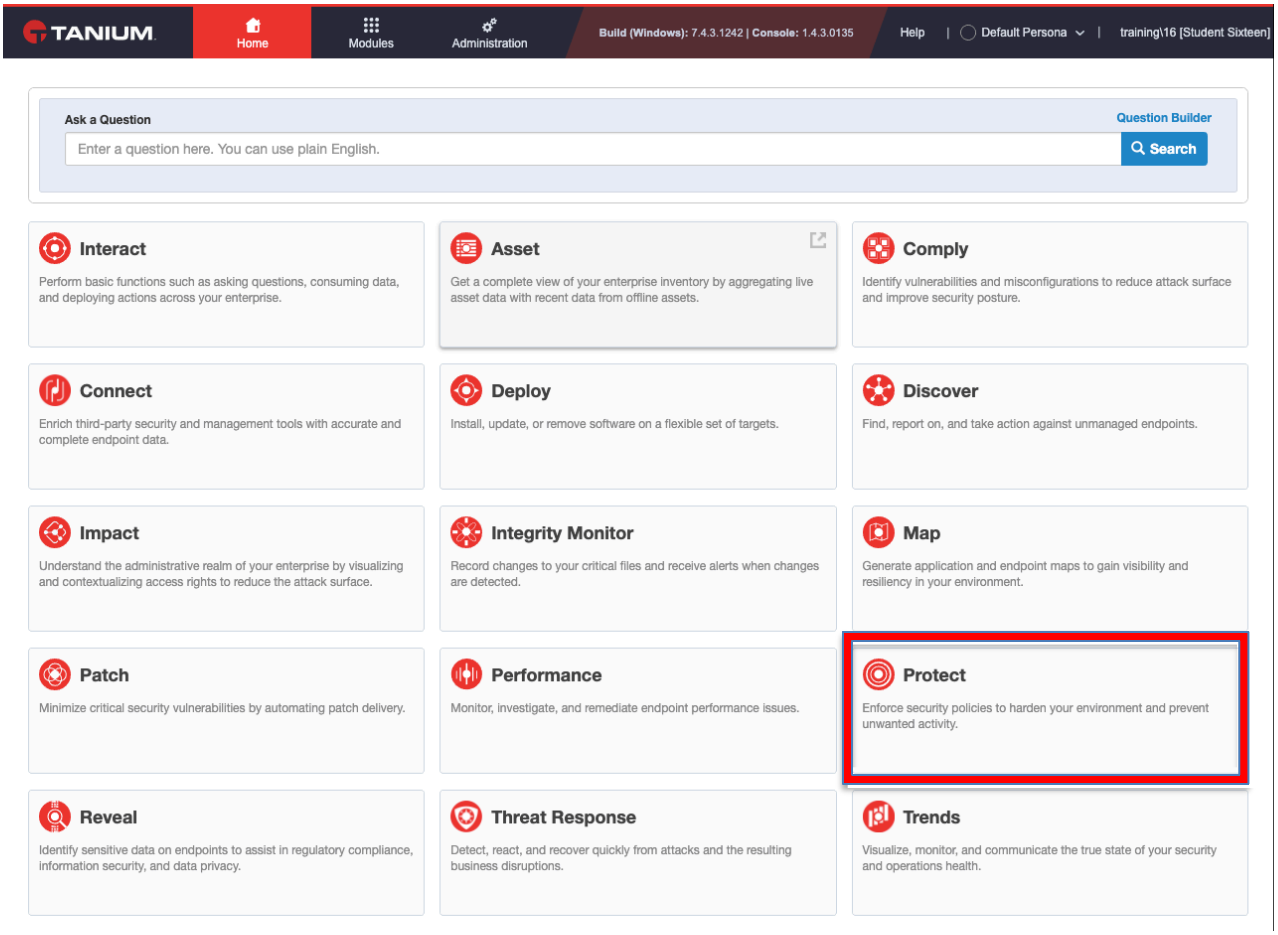
- Create a Windows Firewall and USB policy
- Configure enforcement
- Test remediation

Lab Steps

1.	Using the URL provided, open the Tanium console and enter your credentials  Username: [student number] Password: ••••••••••••••

2. Click on the **Tanium** logo at the top left-hand corner to return you to the home page if you aren't there already.

You should see the homepage of the Tanium console, displaying the various "baseball cards" for the available modules. From here, click on **Protect**.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Ask a Question
Question Builder
Enter a question here. You can use plain English.
Search

Interact
Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise.

Asset
Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets.

Comply
Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.

Connect
Enrich third-party security and management tools with accurate and complete endpoint data.

Deploy
Install, update, or remove software on a flexible set of targets.

Discover
Find, report on, and take action against unmanaged endpoints.

Impact
Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface.

Integrity Monitor
Record changes to your critical files and receive alerts when changes are detected.

Map
Generate application and endpoint maps to gain visibility and resiliency in your environment.

Patch
Minimize critical security vulnerabilities by automating patch delivery.

Performance
Monitor, investigate, and remediate endpoint performance issues.

Protect
Enforce security policies to harden your environment and prevent unwanted activity.

Reveal
Identify sensitive data on endpoints to assist in regulatory compliance, information security, and data privacy.

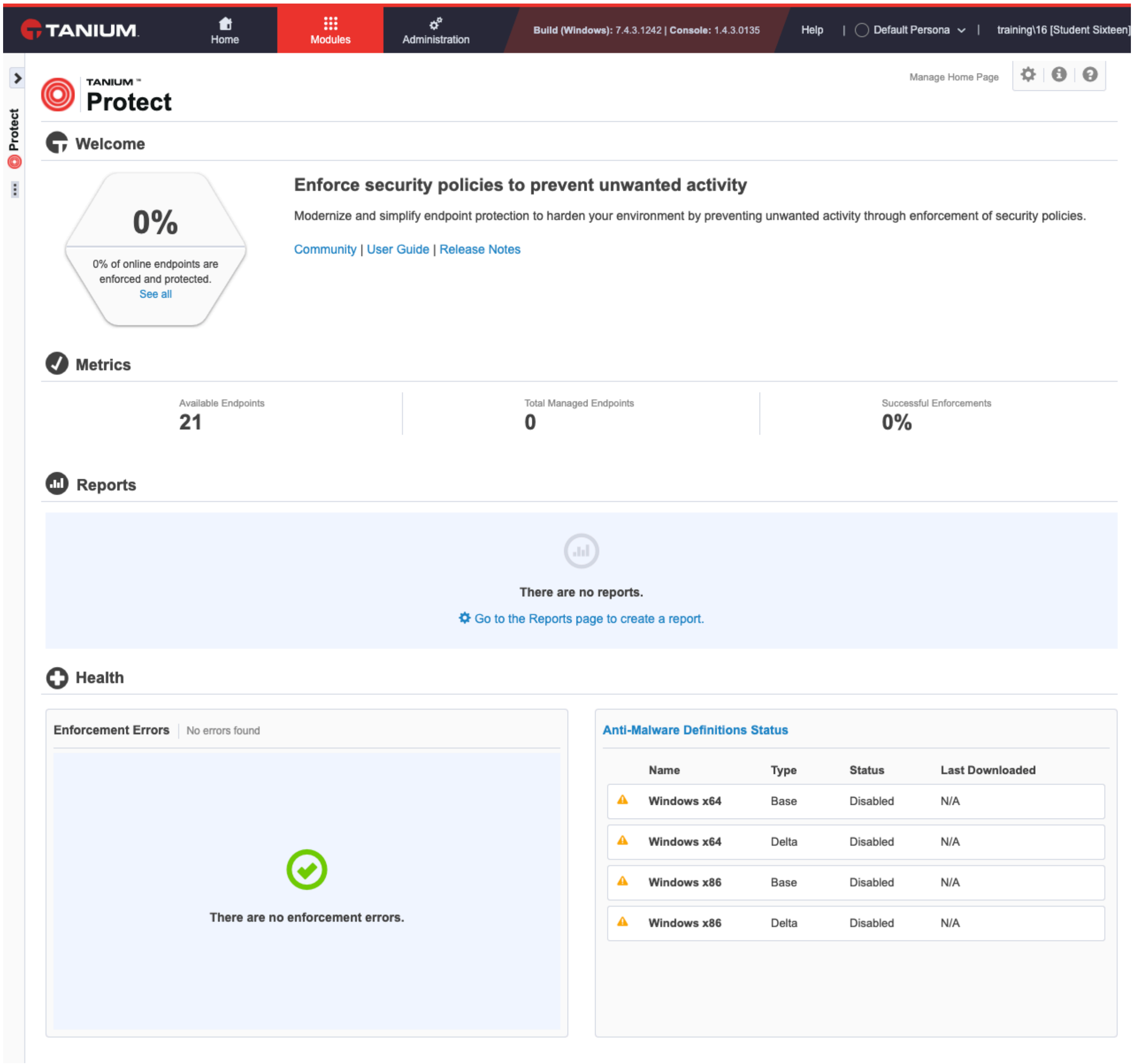
Threat Response
Detect, react, and recover quickly from attacks and the resulting business disruptions.

Trends
Visualize, monitor, and communicate the true state of your security and operations health.

This will now take you to the Protect workbench.

3. The protect workbench homepage displays a summary of the important information, such as:

- Number of available endpoints online
- Number of endpoints which are managed
- Percentage of successful enforcements
- Available reports
- Module health
- Windows Defender anti-malware definitions versions being managed by Protect.



Build (Windows): 7.4.3.1242 | **Console:** 1.4.3.0135

TANIUM™ Protect

Welcome

0%

0% of online endpoints are enforced and protected.
See all

Enforce security policies to prevent unwanted activity

Modernize and simplify endpoint protection to harden your environment by preventing unwanted activity through enforcement of security policies.

Community | User Guide | Release Notes

Metrics

Available Endpoints	Total Managed Endpoints	Successful Enforcements
21	0	0%

Reports

There are no reports.

Go to the Reports page to create a report.

Health

Enforcement Errors | No errors found

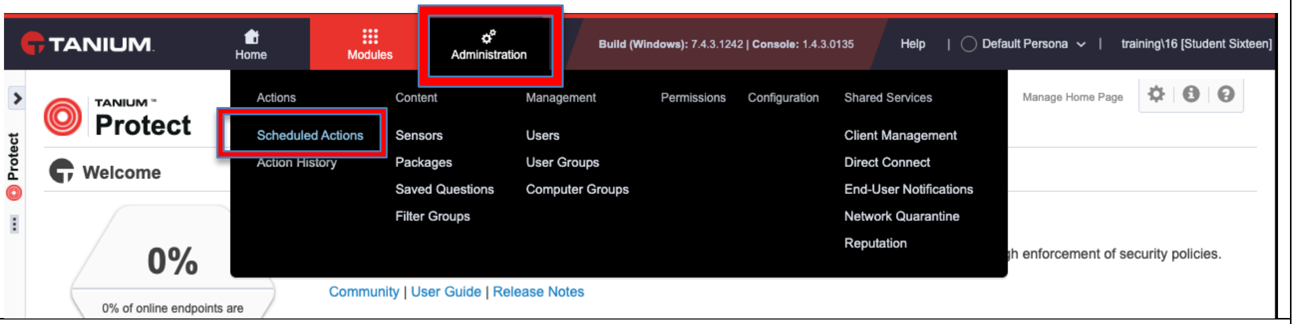
There are no enforcement errors.

Anti-Malware Definitions Status

	Name	Type	Status	Last Downloaded
⚠	Windows x64	Base	Disabled	N/A
⚠	Windows x64	Delta	Disabled	N/A
⚠	Windows x86	Base	Disabled	N/A
⚠	Windows x86	Delta	Disabled	N/A

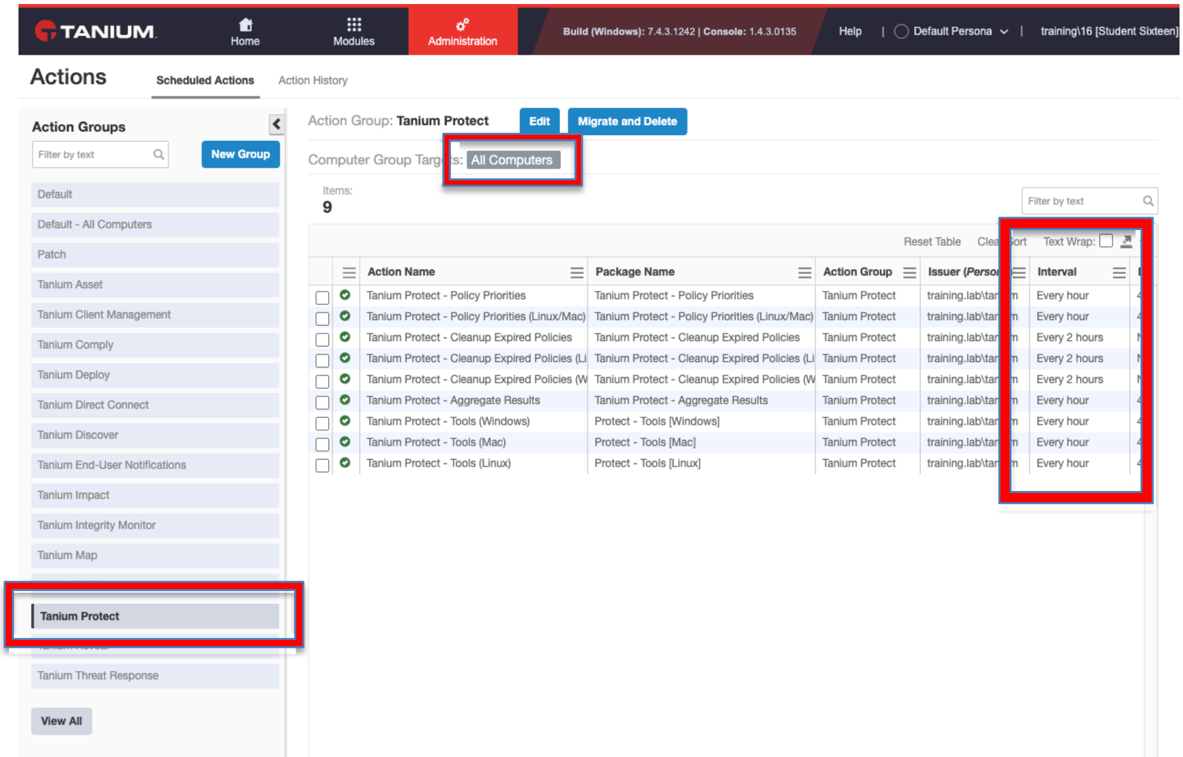
4. Let’s make sure our Protect tools are being deployed and are available on the endpoints.

Hover over the **Administration** menu and then select **Scheduled Actions**.



5. In here, we will find all actions which are reissued regularly to ensure that changes that we want to apply, are received by all managed endpoints. For example, tool deployments and configuration or policy updates, where we don’t want to rely on manually reissuing actions.

Click on the **Tanium Protect** action group on the left and ensure that **Computer Group Targets** is targeting the **All Computers** group. Notice the list of packages being issued to the Computer Group targets which are members of the action group, and how often the actions are reissued.



Action Group: **Tanium Protect**

Computer Group Targ s: All Computers

Items: 9

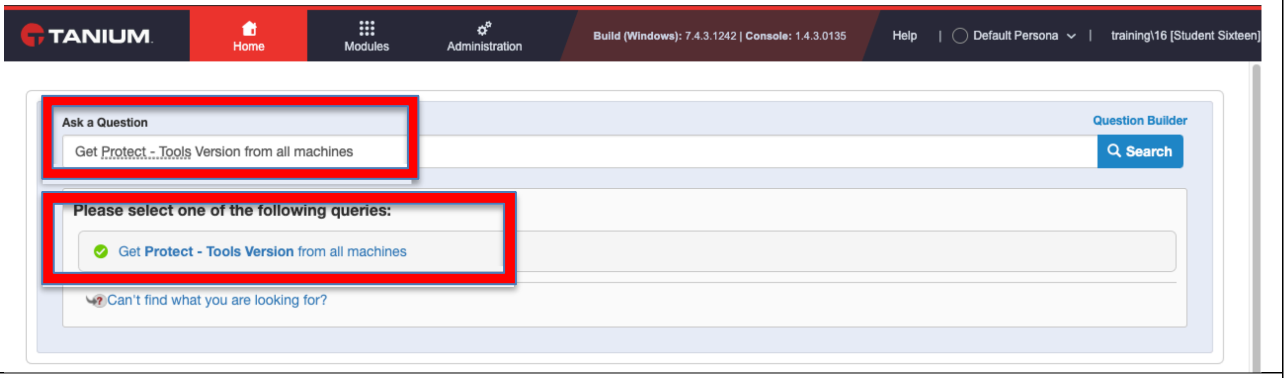
	Action Name	Package Name	Action Group	Issuer (Perso	Interval
□ ✓	Tanium Protect - Policy Priorities	Tanium Protect - Policy Priorities	Tanium Protect	training.lab\tar m	Every hour
□ ✓	Tanium Protect - Policy Priorities (Linux/Mac)	Tanium Protect - Policy Priorities (Linux/Mac)	Tanium Protect	training.lab\tar m	Every hour
□ ✓	Tanium Protect - Cleanup Expired Policies	Tanium Protect - Cleanup Expired Policies	Tanium Protect	training.lab\tar m	Every 2 hours
□ ✓	Tanium Protect - Cleanup Expired Policies (Li	Tanium Protect - Cleanup Expired Policies (Li	Tanium Protect	training.lab\tar m	Every 2 hours
□ ✓	Tanium Protect - Cleanup Expired Policies (W	Tanium Protect - Cleanup Expired Policies (W	Tanium Protect	training.lab\tar m	Every 2 hours
□ ✓	Tanium Protect - Aggregate Results	Tanium Protect - Aggregate Results	Tanium Protect	training.lab\tar m	Every hour
□ ✓	Tanium Protect - Tools (Windows)	Protect - Tools [Windows]	Tanium Protect	training.lab\tar m	Every hour
□ ✓	Tanium Protect - Tools (Mac)	Protect - Tools [Mac]	Tanium Protect	training.lab\tar m	Every hour
□ ✓	Tanium Protect - Tools (Linux)	Protect - Tools [Linux]	Tanium Protect	training.lab\tar m	Every hour

6. Now we know the correct computer group is being targeted by the action group which issues the Protect tools, we will now ensure the endpoints actually have them installed and available for use.

Click on the Tanium logo top-left to return to the main homepage. In the **Ask a Question** box, issue the following question:

Get protect – tools version from all machines

Once the parser finds the correct query, click on the link to issue it.



TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Question Builder
Search

Ask a Question

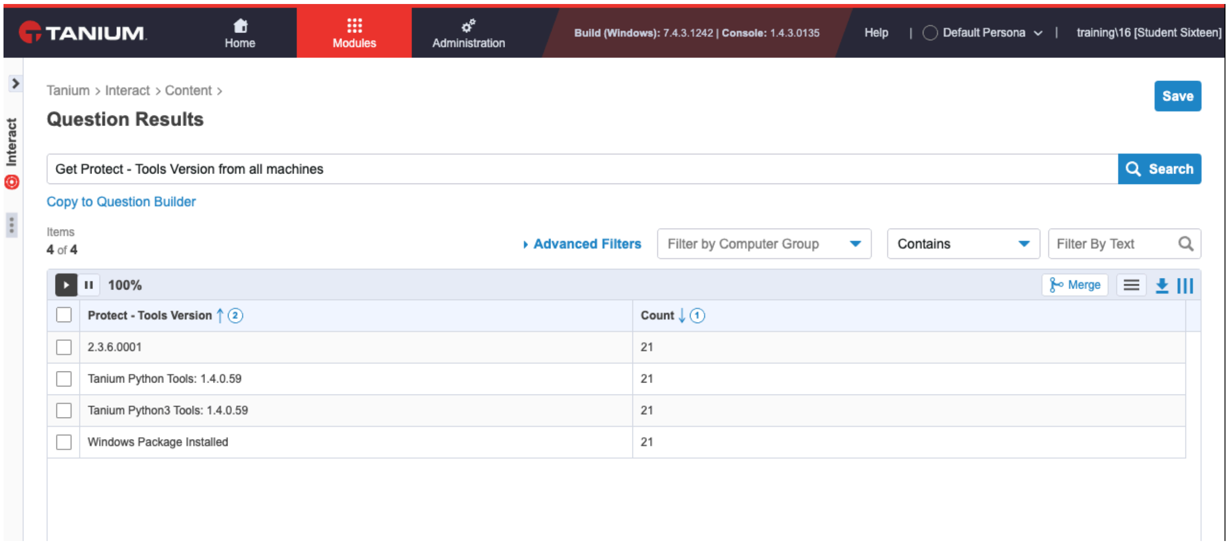
Get Protect - Tools Version from all machines

Please select one of the following queries:

Get Protect - Tools Version from all machines

Can't find what you are looking for?

7. You should see something similar to that show below. This shows that all 20 lab clients, plus the Tanium server itself, have the Windows package installed, the Tanium Python tools installed and shows the version of the Tanium Protect tools which are present. If this looks correct, then all tooling has been deployed successfully and you are good to proceed.



Tanium › Interact › Content ›

Question Results

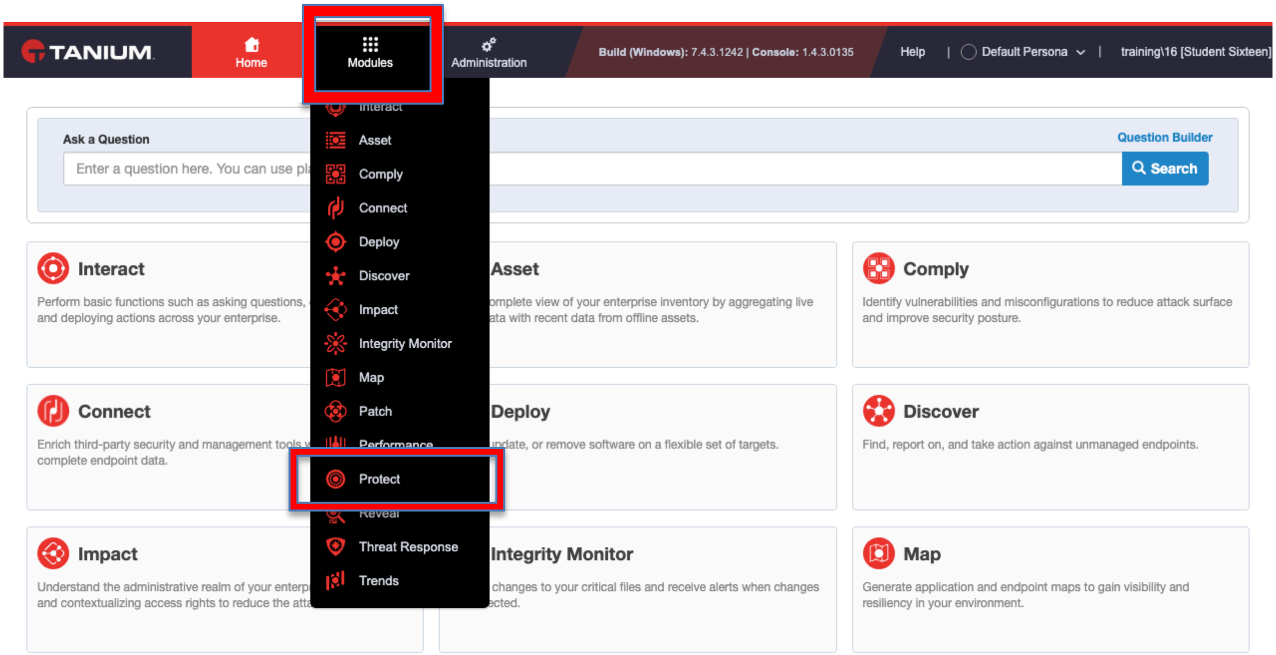
Get Protect - Tools Version from all machines

Items
4 of 4

100%

Protect - Tools Version	Count
2.3.6.0001	21
Tanium Python Tools: 1.4.0.59	21
Tanium Python3 Tools: 1.4.0.59	21
Windows Package Installed	21

8. Hover over the **Modules** menu option at the top and then select **Protect**.



Interact: Perform basic functions such as asking questions, and deploying actions across your enterprise.

Asset: omplete view of your enterprise inventory by aggregating live ata with recent data from offline assets.

Comply: Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.

Connect: Enrich third-party security and management tools complete endpoint data.

Deploy: pdate, or remove software on a flexible set of targets.

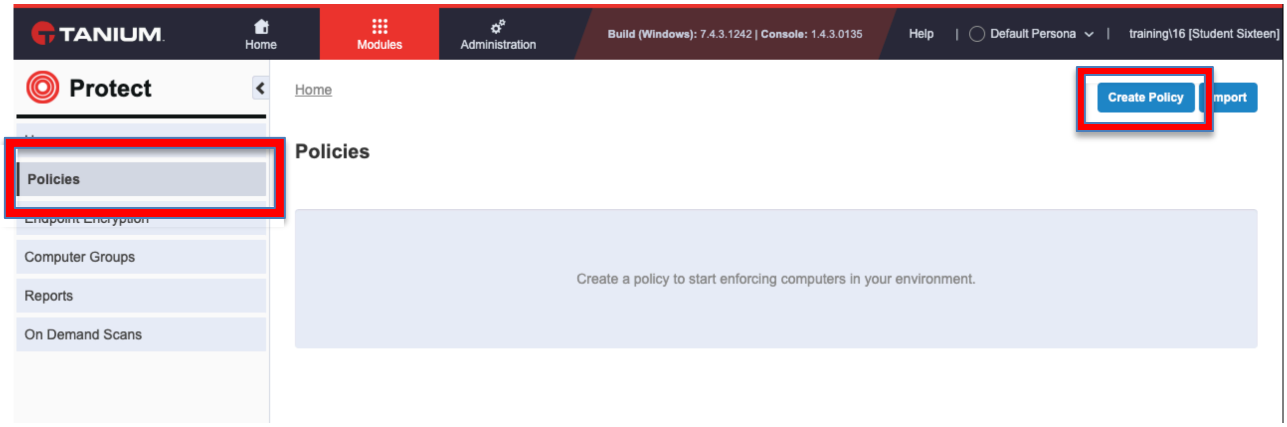
Discover: Find, report on, and take action against unmanaged endpoints.

Impact: Understand the administrative realm of your enterp and contextualizing access rights to reduce the att

Integrity Monitor: changes to your critical files and receive alerts when changes ected.

Map: Generate application and endpoint maps to gain visibility and resiliency in your environment.

9. Once back in the Protect workbench, expand the left-hand menu and select **Policies**.



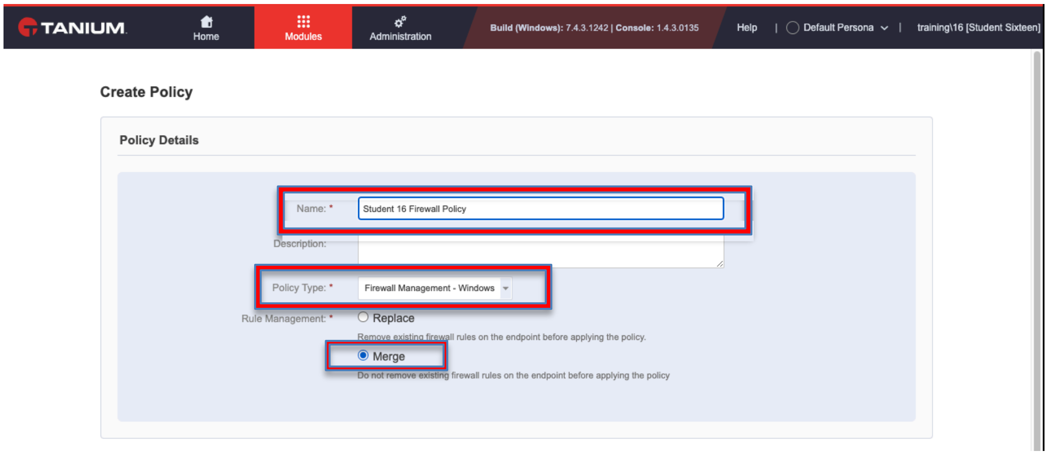
Create a policy to start enforcing computers in your environment.

You will see that no policies are currently configured.

Click on **Create Policy** to begin creating a new Protect policy.

10. **Students 1 – 20**: Create a Firewall policy named *Student <Student ID Number> Firewall Policy*. Continue onwards from this point.
Students 21 – 40: Create a device control policy named *Student <Student ID Number> USB Policy*. Move ahead to step 15 in this lab for your steps.

Students 1 – 20
Create a Firewall policy, name the policy and select *Firewall Management – Windows* in the **Policy Type** drop-down. Under **Rule Management**, select the *Merge* option.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]

Create Policy

Policy Details

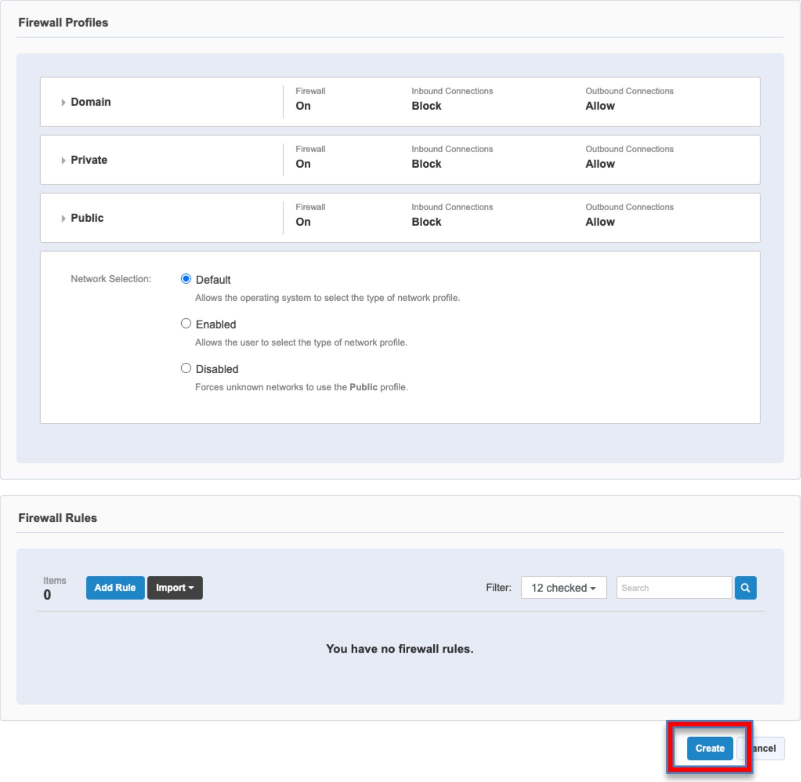
Name: * Student 16 Firewall Policy

Description:

Policy Type: * Firewall Management - Windows

Rule Management: *
○ Replace
Remove existing firewall rules on the endpoint before applying the policy.
● Merge
Do not remove existing firewall rules on the endpoint before applying the policy

Leave all settings unchanged under the Firewall Profiles and Firewall Rules sections. Click **Create**.



Firewall Profiles

	Firewall	Inbound Connections	Outbound Connections
Domain	On	Block	Allow
Private	On	Block	Allow
Public	On	Block	Allow

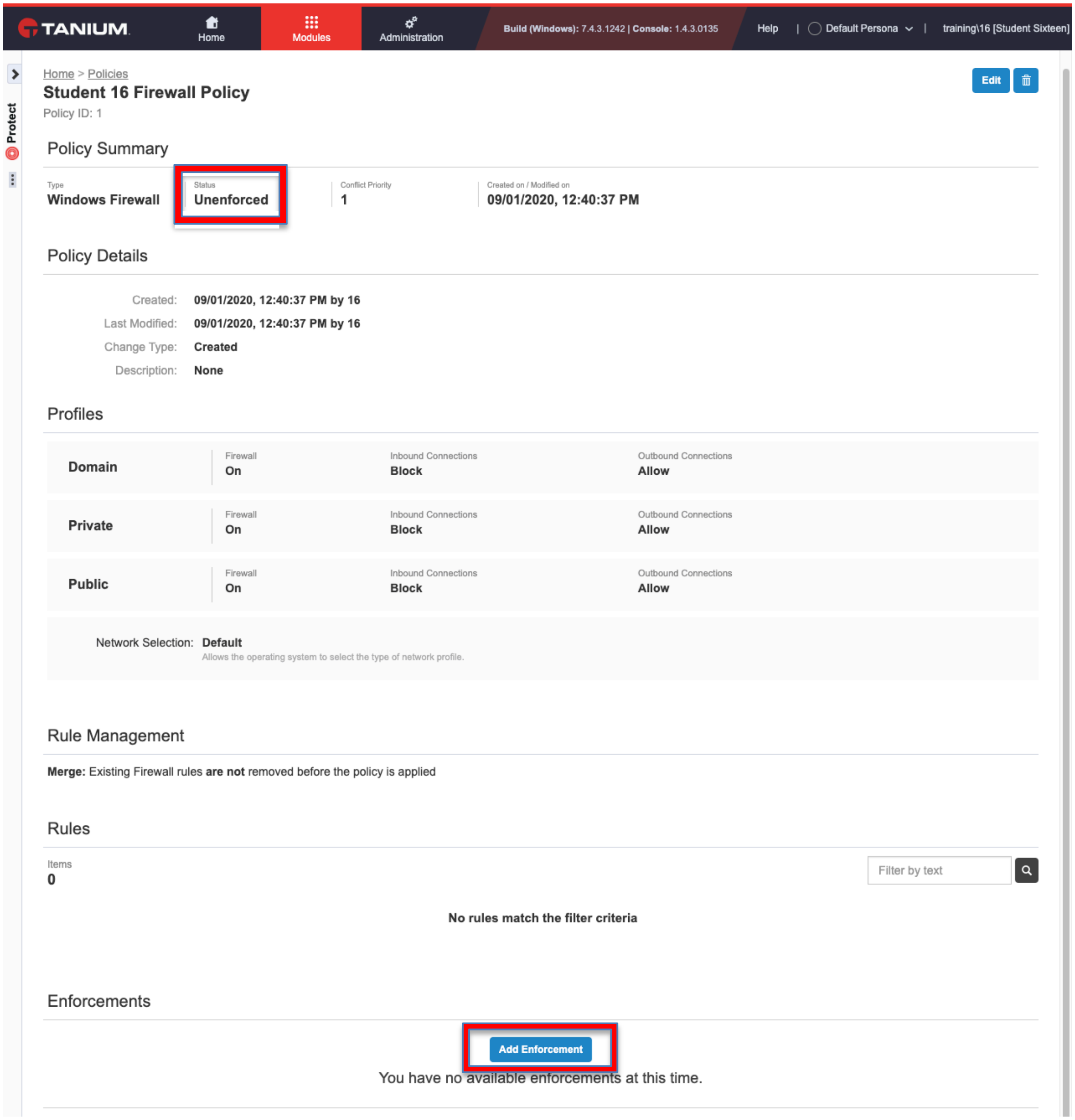
Network Selection:
● Default
Allows the operating system to select the type of network profile.
○ Enabled
Allows the user to select the type of network profile.
○ Disabled
Forces unknown networks to use the **Public** profile.

Firewall Rules

Items 0

You have no firewall rules.

11. You will now see a summary of your policy. Note that the **Status** shows as **Unenforced**.



TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Protect
Edit

Home > Policies

Student 16 Firewall Policy

Policy ID: 1

Policy Summary

Type	Status	Conflict Priority	Created on / Modified on
Windows Firewall	Unenforced	1	09/01/2020, 12:40:37 PM

Policy Details

Created: 09/01/2020, 12:40:37 PM by 16

Last Modified: 09/01/2020, 12:40:37 PM by 16

Change Type: Created

Description: None

Profiles

	Firewall	Inbound Connections	Outbound Connections
Domain	On	Block	Allow
Private	On	Block	Allow
Public	On	Block	Allow

Network Selection: Default

Allows the operating system to select the type of network profile.

Rule Management

Merge: Existing Firewall rules **are not** removed before the policy is applied

Rules

Items

0

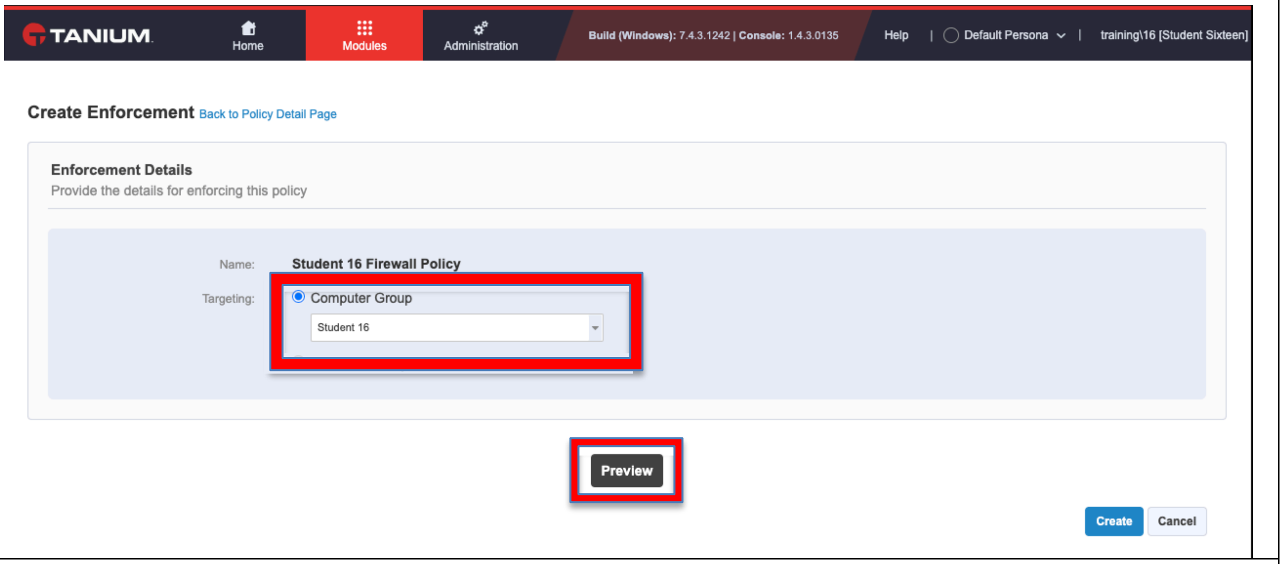
No rules match the filter criteria

Enforcements

You have no available enforcements at this time.

Click on **Add Enforcement**.

12. In the **Targeting** section, select **Computer Group** and in the drop-down menu, select the computer group associated with your student ID number. Now click **Preview**.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Back to Policy Detail Page
Preview
Create
Cancel

Create Enforcement

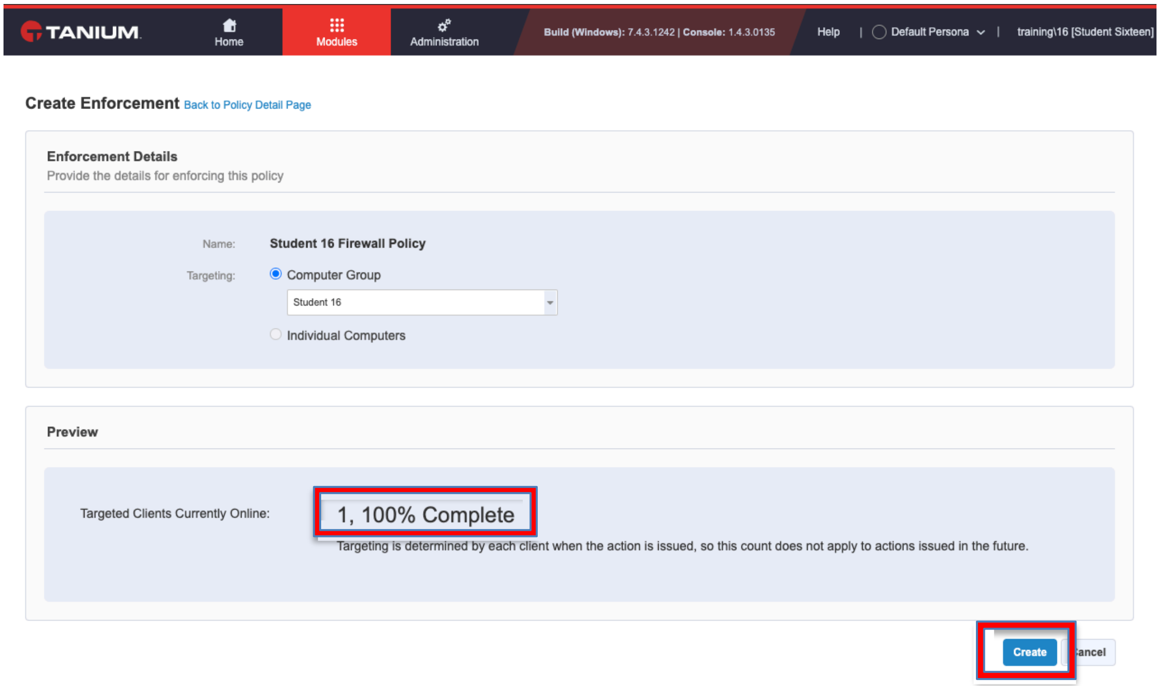
Enforcement Details
Provide the details for enforcing this policy

Name: Student 16 Firewall Policy

Targeting: ● Computer Group

Student 16

13. You will now see how many endpoints your enforcement will apply to. This should only apply to 1 endpoint, which is your lab client which is a member of the computer group you have targeted. Once ready, click on **Create,** then click **Yes** to confirm and create the new enforcement.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Back to Policy Detail Page
Create
Cancel

Create Enforcement

Enforcement Details
Provide the details for enforcing this policy

Name: Student 16 Firewall Policy

Targeting: ● Computer Group

Student 16

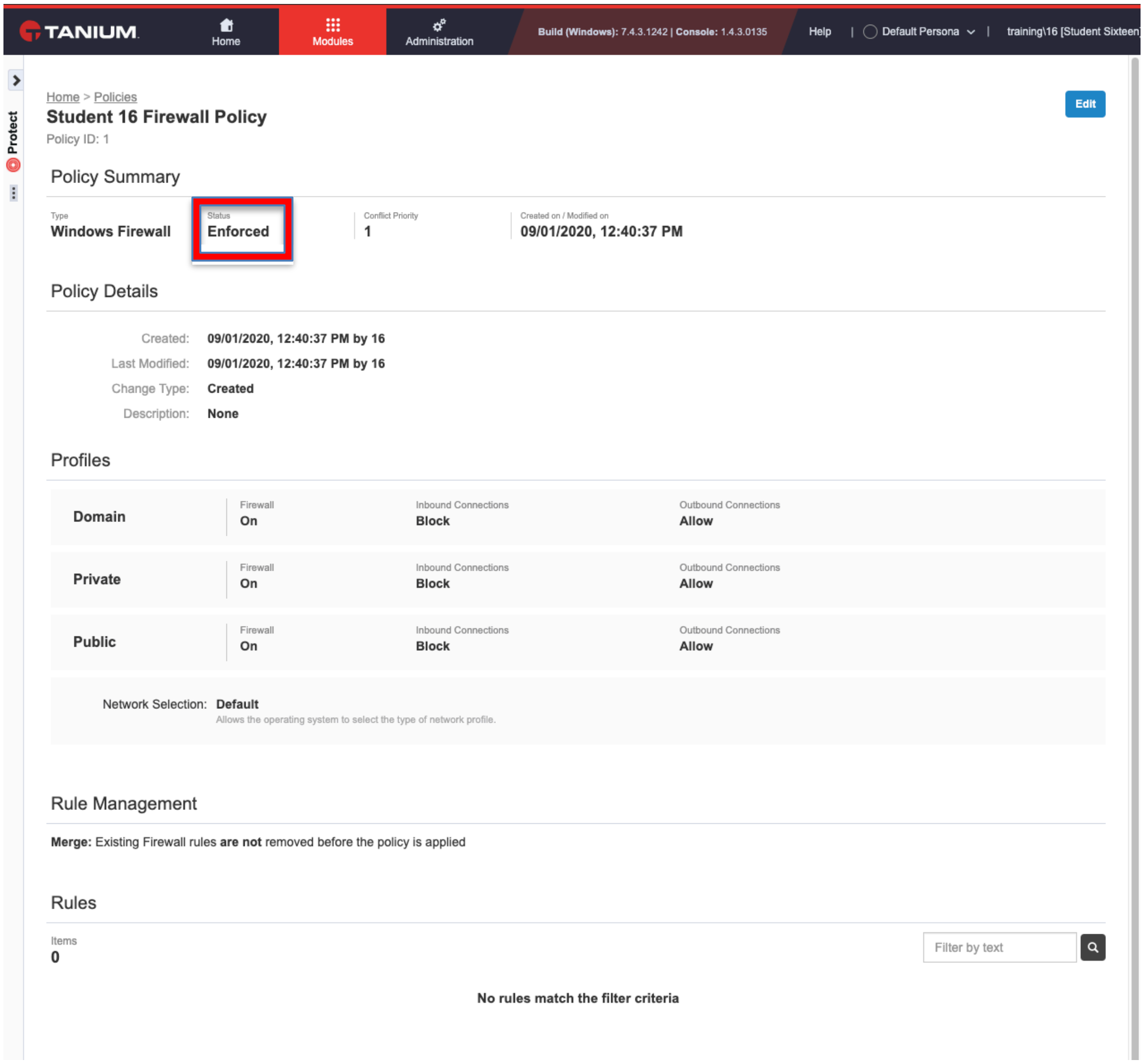
○ Individual Computers

Preview

Targeted Clients Currently Online: 1, 100% Complete

Targeting is determined by each client when the action is issued, so this count does not apply to actions issued in the future.

14. You will again see the summary page, but this time the policy will have a **Status** of **Enforced**.



TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Protect
Edit

Home > Policies

Student 16 Firewall Policy

Policy ID: 1

Policy Summary

Type	Status	Conflict Priority	Created on / Modified on
Windows Firewall	Enforced	1	09/01/2020, 12:40:37 PM

Policy Details

Created: 09/01/2020, 12:40:37 PM by 16
Last Modified: 09/01/2020, 12:40:37 PM by 16
Change Type: Created
Description: None

Profiles

	Firewall	Inbound Connections	Outbound Connections
Domain	On	Block	Allow
Private	On	Block	Allow
Public	On	Block	Allow

Network Selection: Default
Allows the operating system to select the type of network profile.

Rule Management

Merge: Existing Firewall rules **are not** removed before the policy is applied

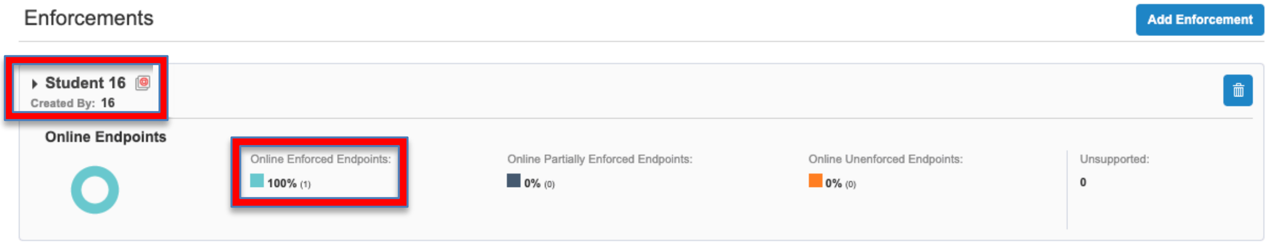
Rules

Items
0

Filter by text

No rules match the filter criteria

At the bottom of the page in the **Enforcements** section, you will see the active enforcements, showing the computer groups enforced and the number of online endpoints with the policy enforced:



Enforcements

Student 16
Created By: 16

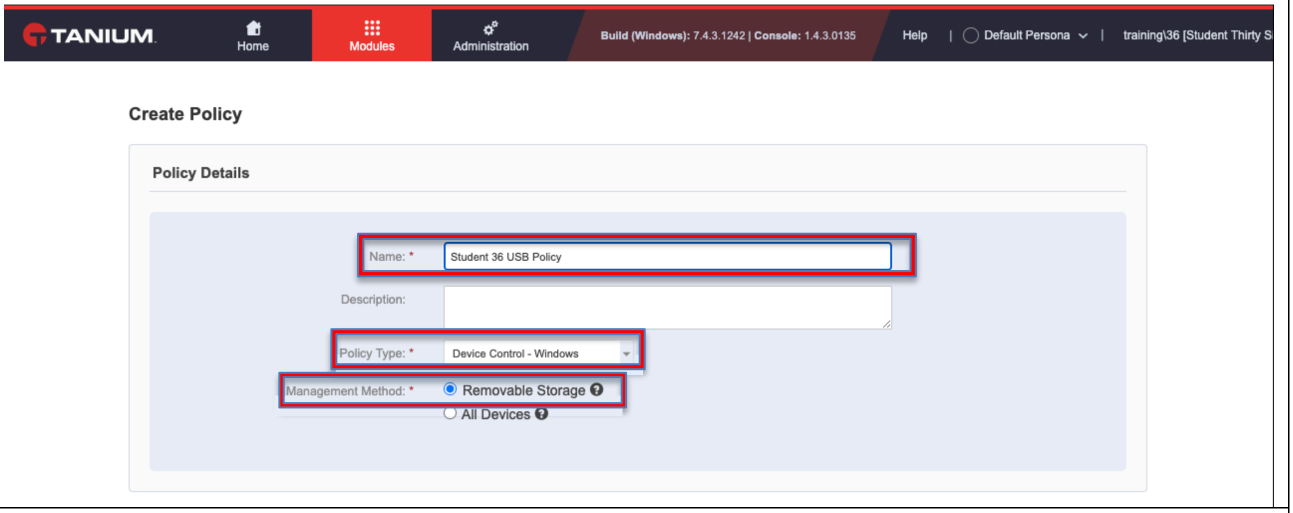
Online Endpoints

Online Enforced Endpoints:	Online Partially Enforced Endpoints:	Online Unenforced Endpoints:	Unsupported:
100% (1)	0% (0)	0% (0)	0

Your policy creation and enforcement are now complete. Continue to step 23 in this lab.

15. **Students 21 – 40**

Name the policy and select *Device Control - Windows* in the **Policy Type** drop-down. Under **Management Method**, select the *Removable Storage* option.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\36 [Student Thirty S

Create Policy

Policy Details

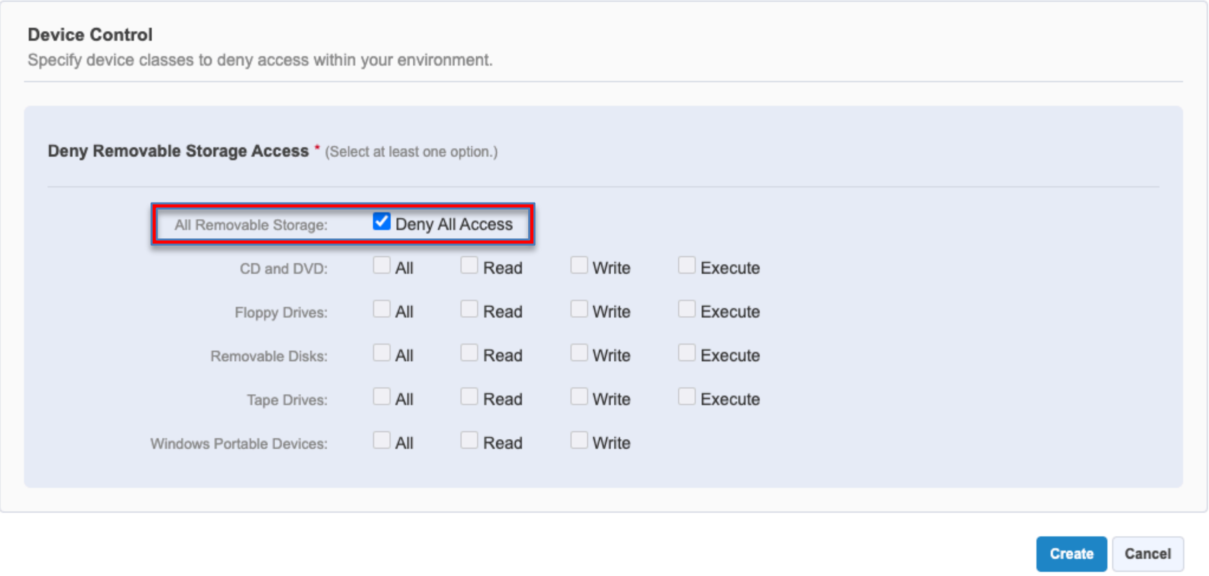
Name: * Student 36 USB Policy

Description:

Policy Type: * Device Control - Windows

Management Method: * ● Removable Storage ○ All Devices

16. In the Device Control options, enable the Deny All Access checkbox against All Removable Storage. Now click **Create**.



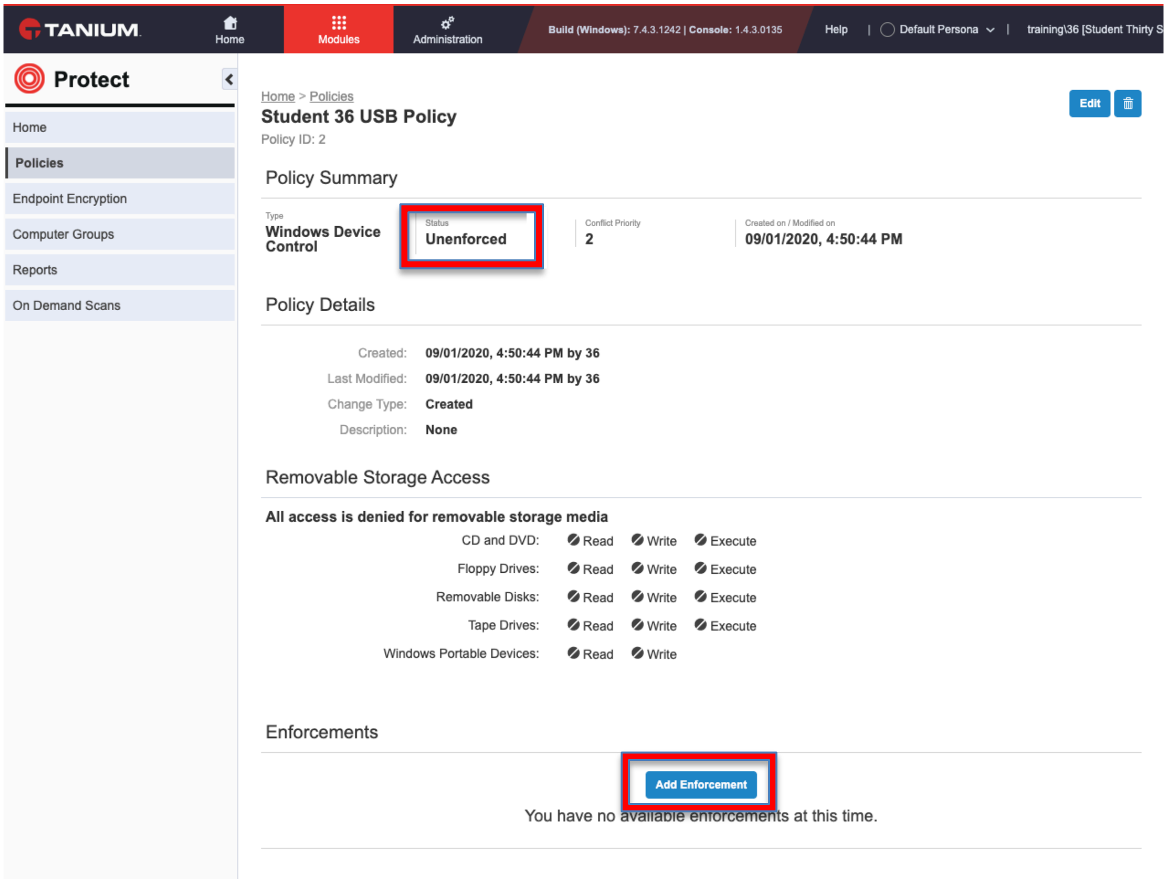
Device Control

Specify device classes to deny access within your environment.

Deny Removable Storage Access * (Select at least one option.)

All Removable Storage:	☑ Deny All Access			
CD and DVD:	□ All	□ Read	□ Write	□ Execute
Floppy Drives:	□ All	□ Read	□ Write	□ Execute
Removable Disks:	□ All	□ Read	□ Write	□ Execute
Tape Drives:	□ All	□ Read	□ Write	□ Execute
Windows Portable Devices:	□ All	□ Read	□ Write	

17. You will now see a summary of your policy. Note that the **Status** shows as **Unenforced**.



Home > Policies

Student 36 USB Policy

Policy ID: 2

Policy Summary

Type	Status	Conflict Priority	Created on / Modified on
Windows Device Control	Unenforced	2	09/01/2020, 4:50:44 PM

Policy Details

Created: 09/01/2020, 4:50:44 PM by 36
Last Modified: 09/01/2020, 4:50:44 PM by 36
Change Type: Created
Description: None

Removable Storage Access

All access is denied for removable storage media

CD and DVD:	⊘ Read	⊘ Write	⊘ Execute
Floppy Drives:	⊘ Read	⊘ Write	⊘ Execute
Removable Disks:	⊘ Read	⊘ Write	⊘ Execute
Tape Drives:	⊘ Read	⊘ Write	⊘ Execute
Windows Portable Devices:	⊘ Read	⊘ Write	

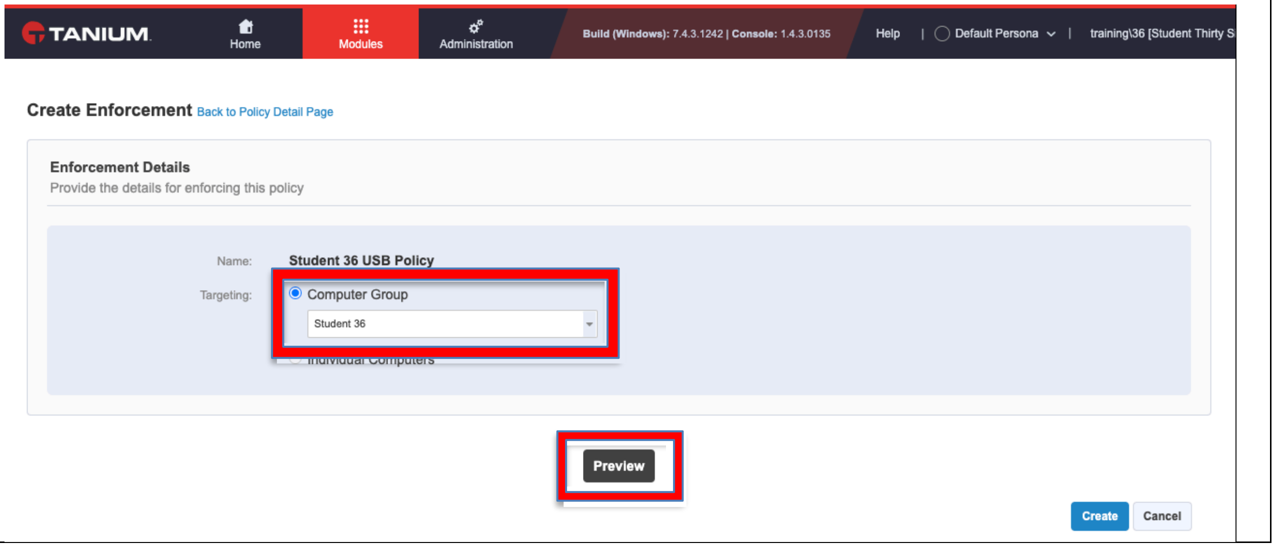
Enforcements

Add Enforcement

You have no available enforcements at this time.

Click on **Add Enforcement**.

18. In the **Targeting** section, select **Computer Group** and in the drop-down menu, type in the name or select the computer group associated with your student ID number. Now click **Preview**.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\36 [Student Thirty S
Back to Policy Detail Page
Preview
Create
Cancel

Create Enforcement

Enforcement Details

Provide the details for enforcing this policy

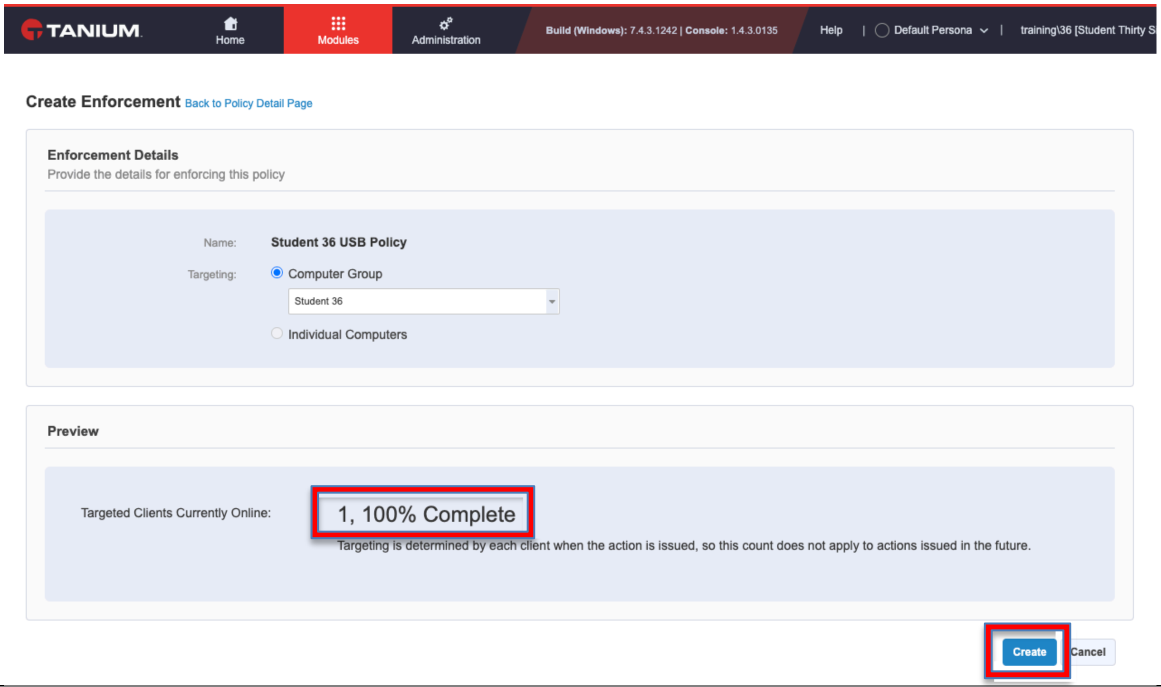
Name: Student 36 USB Policy

Targeting: ● Computer Group

Student 36

○ Individual Computers

19. You will now see how many endpoints your enforcement will apply to. This should only apply to 1 endpoint, which is your lab client which is a member of the computer group you have targeted. Once ready, click on **Create,** then click **Yes** to confirm and create the new enforcement.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\36 [Student Thirty S

Create Enforcement Back to Policy Detail Page

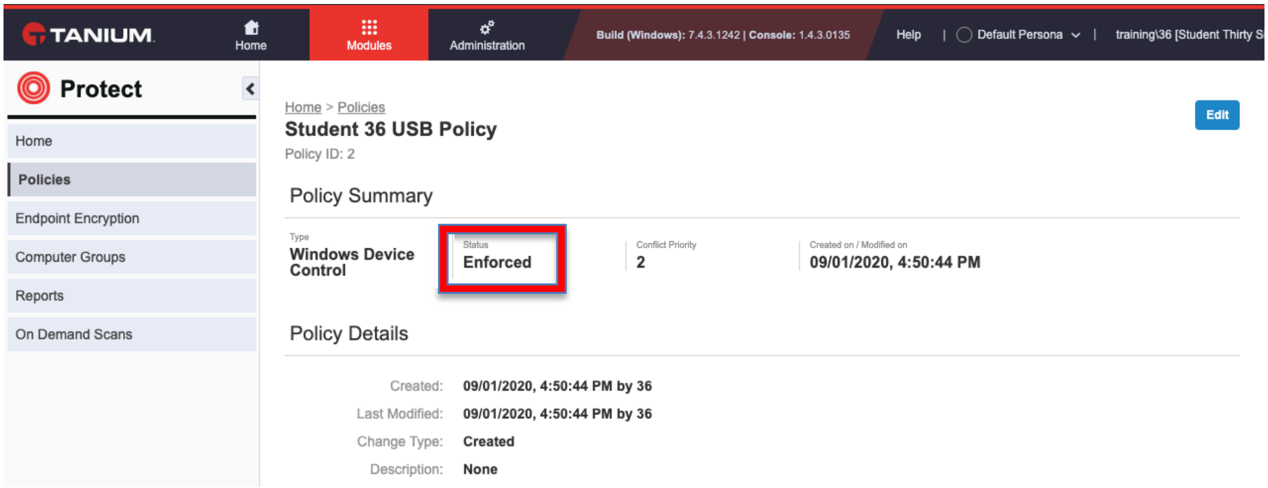
Enforcement Details
Provide the details for enforcing this policy

Name: Student 36 USB Policy
Targeting: ● Computer Group
Student 36
○ Individual Computers

Preview

Targeted Clients Currently Online: 1, 100% Complete
Targeting is determined by each client when the action is issued, so this count does not apply to actions issued in the future.

20. You will now see that your policy is now showing a **Status** of **Enforced**.



Student 36 USB Policy
Policy ID: 2

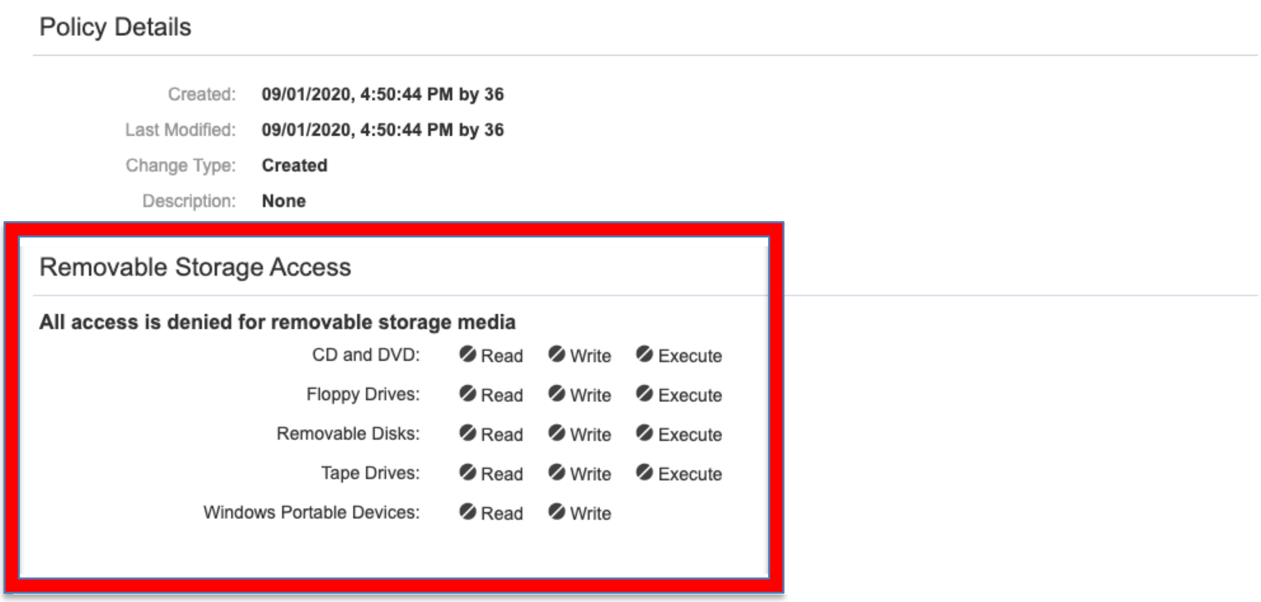
Policy Summary

Type: Windows Device Control
Status: Enforced
Conflict Priority: 2
Created on / Modified on: 09/01/2020, 4:50:44 PM

Policy Details

Created: 09/01/2020, 4:50:44 PM by 36
Last Modified: 09/01/2020, 4:50:44 PM by 36
Change Type: Created
Description: None

21. On the same page, you will also see a summary of the settings configured within the policy



Policy Details

Created: 09/01/2020, 4:50:44 PM by 36

Last Modified: 09/01/2020, 4:50:44 PM by 36

Change Type: Created

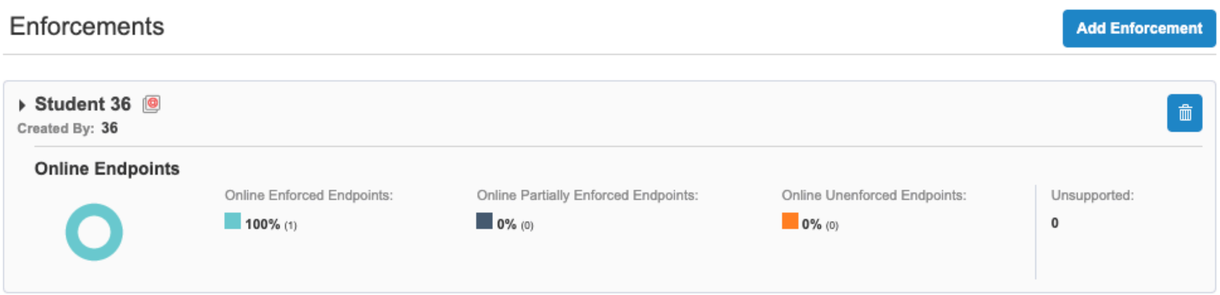
Description: None

Removable Storage Access

All access is denied for removable storage media

CD and DVD:	⊘ Read	⊘ Write	⊘ Execute
Floppy Drives:	⊘ Read	⊘ Write	⊘ Execute
Removable Disks:	⊘ Read	⊘ Write	⊘ Execute
Tape Drives:	⊘ Read	⊘ Write	⊘ Execute
Windows Portable Devices:	⊘ Read	⊘ Write	

22. At the bottom of the page in the **Enforcements** section, you will see the active enforcements, showing the computer groups enforced and the number of online endpoints with the policy enforced:



Student 36

Created By: 36

Online Endpoints

Online Enforced Endpoints: 🟦 100% (1)

Online Partially Enforced Endpoints: ■ 0% (0)

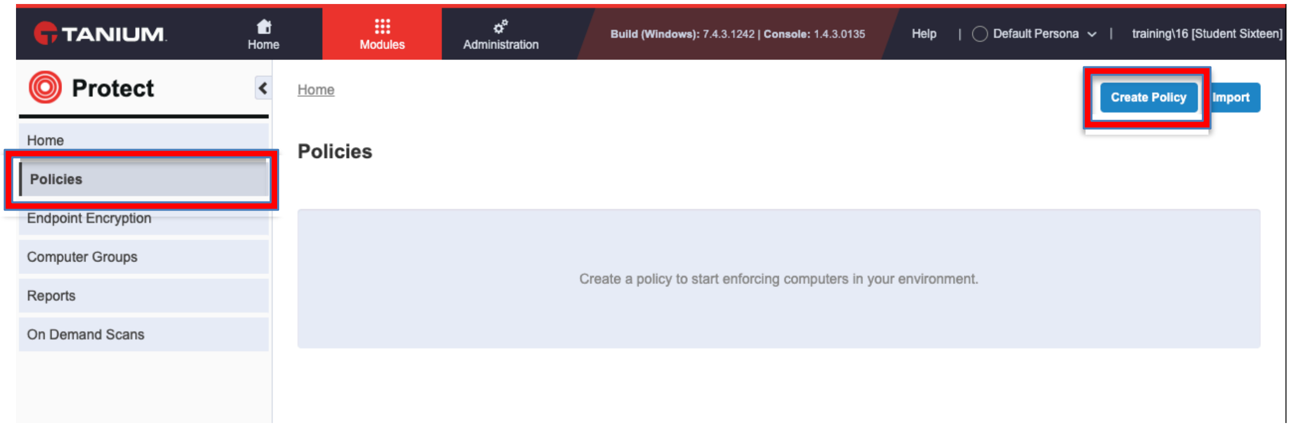
Online Unenforced Endpoints: 🟧 0% (0)

Unsupported: 0

Your policy creation and enforcement are now complete. Continue to step 23 in this lab.

23. We will now create a remediation policy. Let's use a scenario where a particular registry value needs to be present to make an endpoint compliant with corporate security policy. In this example, this value has been deleted and we will use Tanium to ensure the value is restored and the endpoint brought back into compliance.

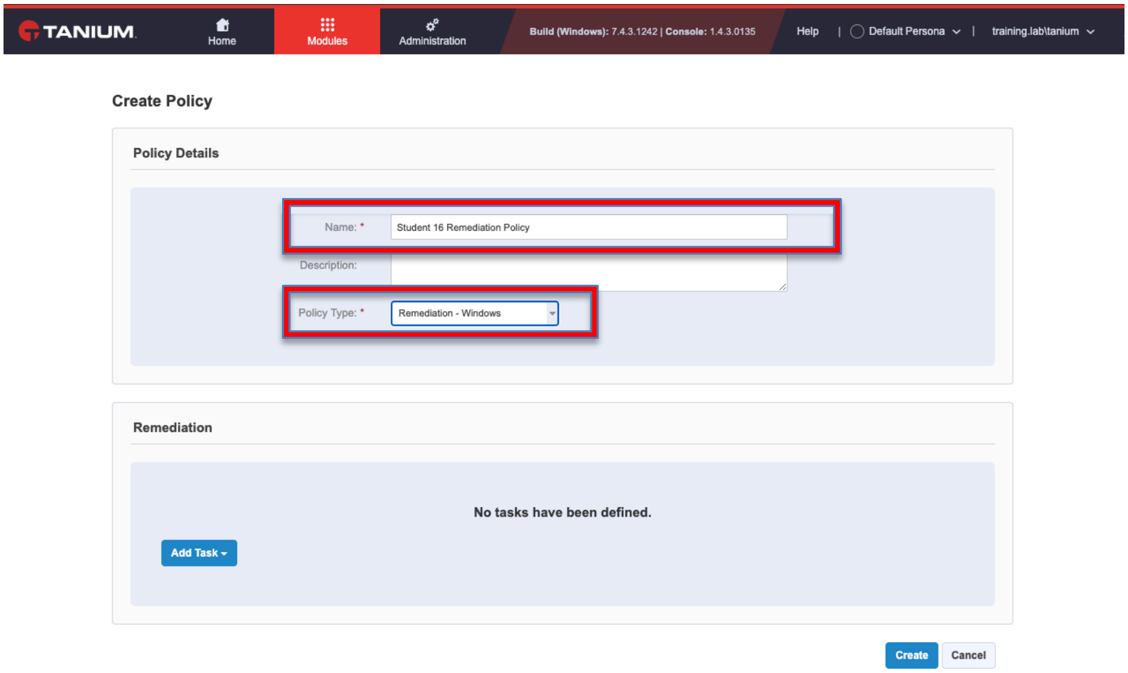
Return to the **Policies** screen using the pop-out menu.



Create a policy to start enforcing computers in your environment.

Once again, click on **Create Policy**.

24. This time name the policy *Student <Student ID Number> Remediation Policy*.



Name: * Student 16 Remediation Policy

Description:

Policy Type: * Remediation - Windows

No tasks have been defined.

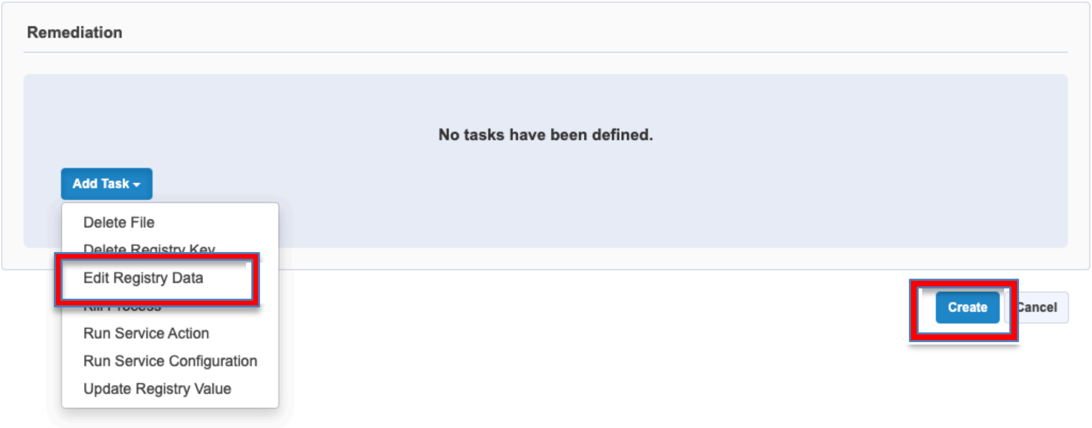
In the **Policy Type** drop-down, select **Remediation – Windows**.

25. In the **Remediation** section, you can define one or more actions which are executed should a remediation policy be applicable. Actions available are:

- Delete File
- Delete Registry Key
- Edit Registry Data
- Kill Process
- Run Service Action
- Run Service Configuration
- Update Registry Value

For example, to combat potential malware, you could have a remediation policy which stops a malicious service, configures it to disable it to prevent it from restarting, and then deletes the file the service is running to remove the malware.

In our scenario, we need to ensure a registry value exists, so we will be using an action which focuses on the registry. In the **Remediation** section, click **Add Task**, then select **Edit Registry Data**.

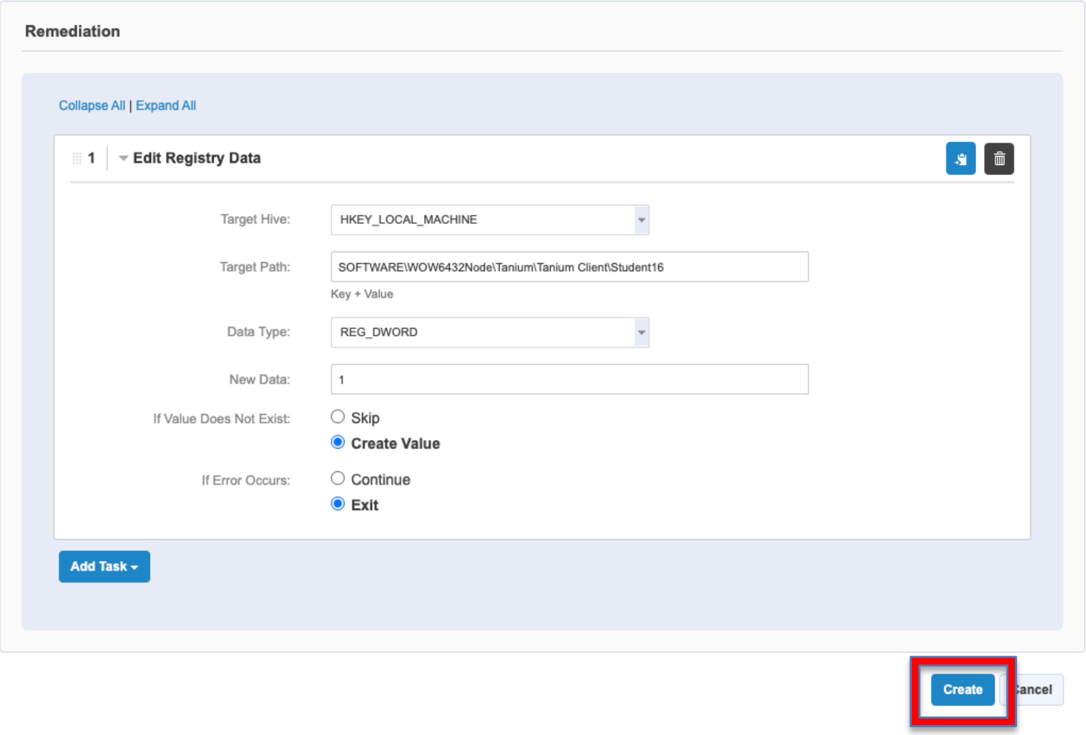

Remediation

No tasks have been defined.

Configure the new Edit Registry Data entry under Remediation as follows:

- **Target Hive**: HKEY_LOCAL_MACHINE
- **Target Path:** *SOFTWARE\WOW6432Node\Tanium\Tanium Client\Student<ID Number>*
- **Data Type:** *REG_DWORD*
- **New Data:** *1*
- **If Value Does Not Exist:** *Create Value*
- **If Error Occurs:** *Exit*

26. Your remediation action should look similar to that below. Click on **Create**.



Remediation

Collapse All | Expand All

1 Edit Registry Data

Target Hive: HKEY_LOCAL_MACHINE

Target Path: SOFTWARE\WOW6432Node\Tanium\Tanium Client\Student16

Key + Value

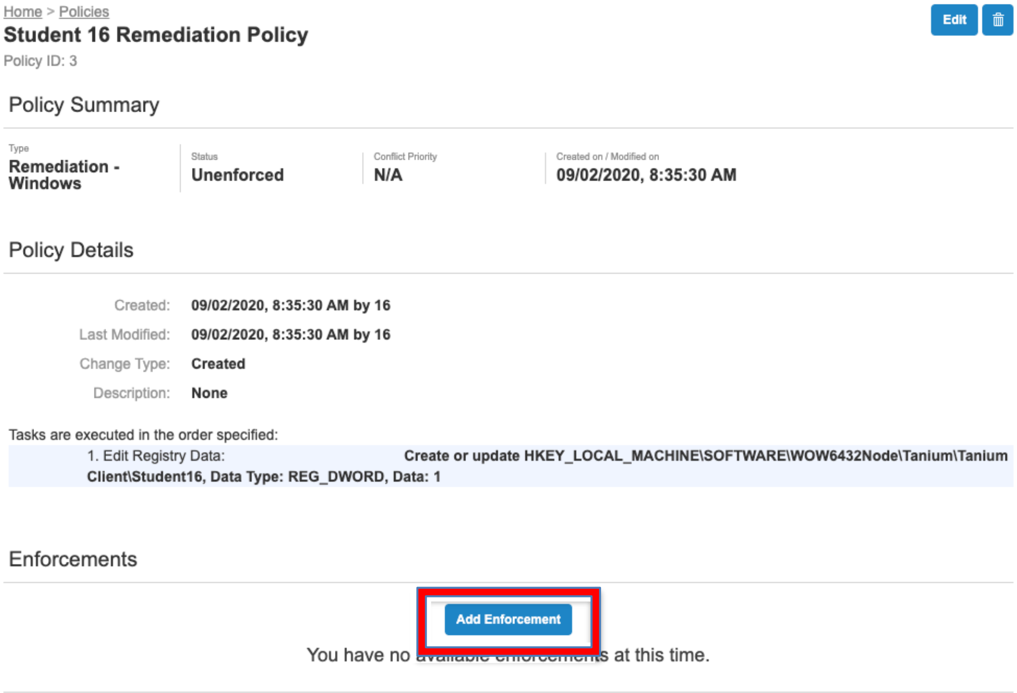
Data Type: REG_DWORD

New Data: 1

If Value Does Not Exist: ○ Skip ● Create Value

If Error Occurs: ○ Continue ● Exit

27. The summary of your policy will appear. Click on **Add Enforcement**.



Home > Policies

Student 16 Remediation Policy

Policy ID: 3

Policy Summary

Type	Status	Conflict Priority	Created on / Modified on
Remediation - Windows	Unenforced	N/A	09/02/2020, 8:35:30 AM

Policy Details

Created: 09/02/2020, 8:35:30 AM by 16

Last Modified: 09/02/2020, 8:35:30 AM by 16

Change Type: Created

Description: None

Tasks are executed in the order specified:

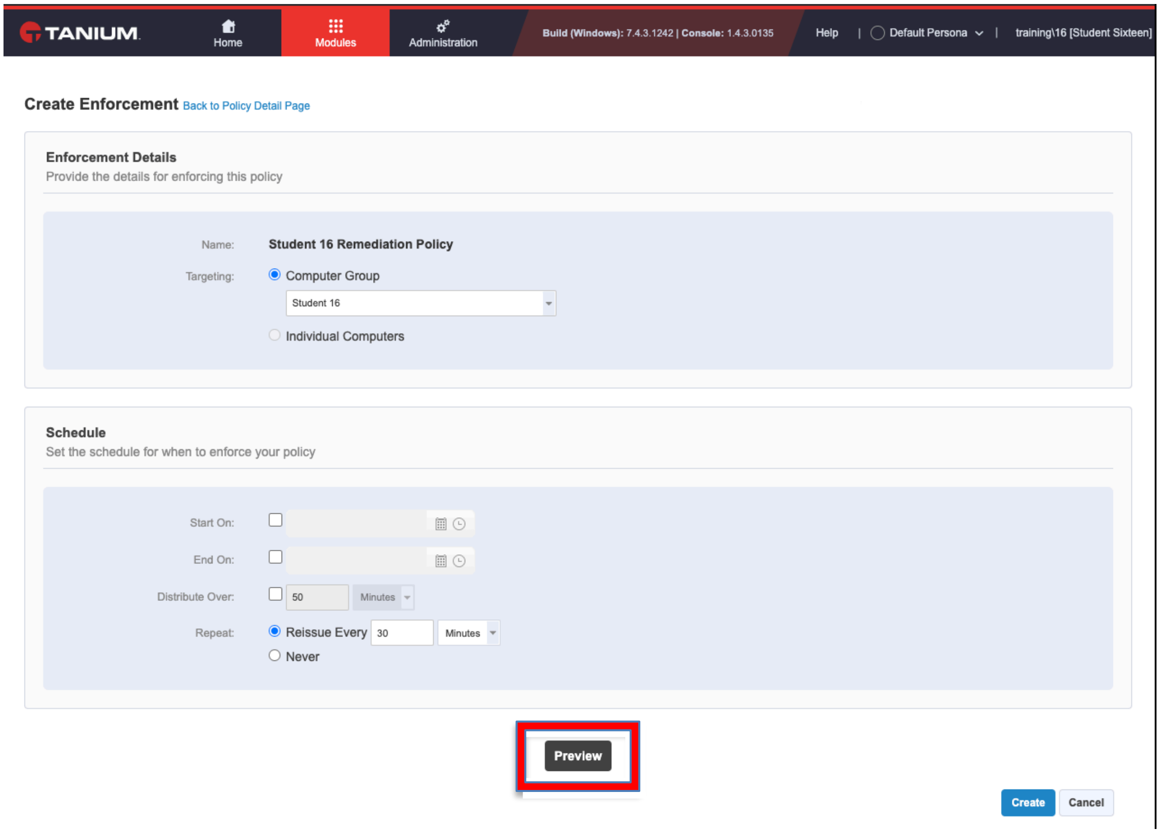
1. Edit Registry Data: Create or update HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Tanium\Tanium Client\Student16, Data Type: REG_DWORD, Data: 1

Enforcements

You have no available enforcements at this time.

28. Select your designated computer group in the **Targeting** drop-down and under **Schedule**, set the following, leaving the other settings as default:

- Uncheck the **Distribute Over** option
- Set **Repeat** to *30 Minutes*


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Preview
Create
Cancel

Create Enforcement Back to Policy Detail Page

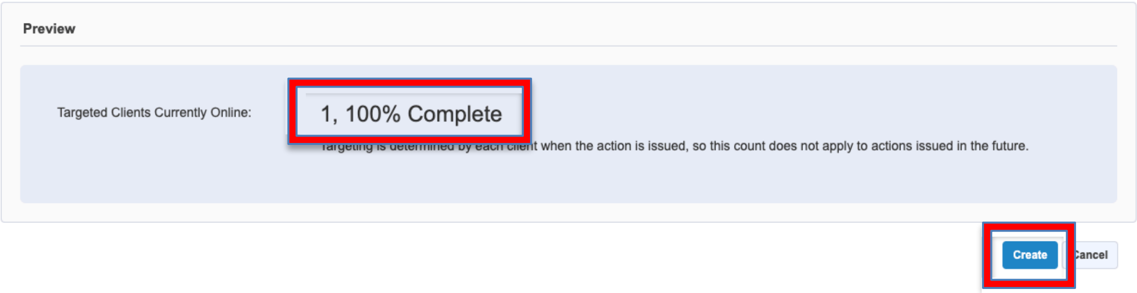
Enforcement Details
Provide the details for enforcing this policy

Name: **Student 16 Remediation Policy**
Targeting: ● Computer Group
Student 16
○ Individual Computers

Schedule
Set the schedule for when to enforce your policy

Start On: □
End On: □
Distribute Over: □ 50 Minutes
Repeat: ● Reissue Every 30 Minutes
○ Never

Click **Preview** to assess how many clients would be affected by this policy.

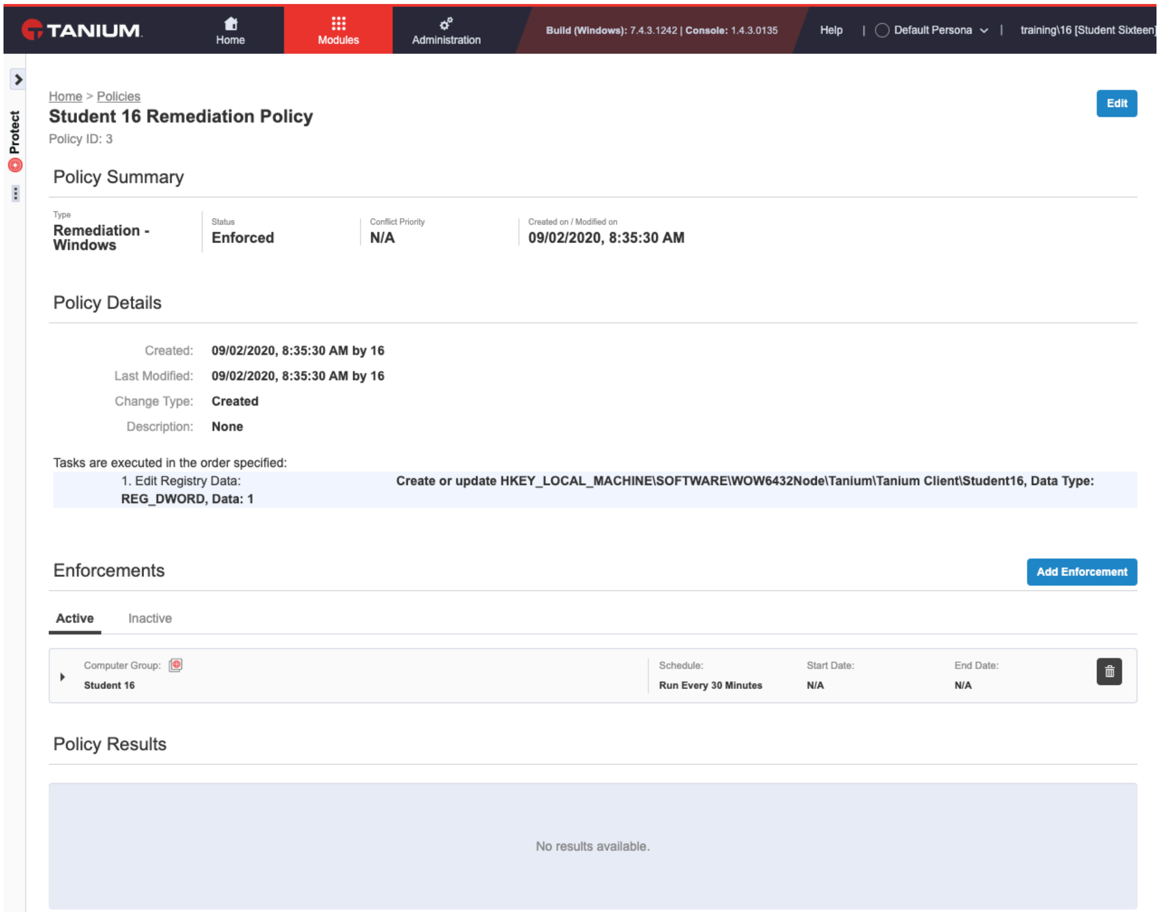


Preview

Targeted Clients Currently Online: 1, 100% Complete
Targeting is determined by each client when the action is issued, so this count does not apply to actions issued in the future.

It should show only one, as only your client in your computer group will be targeted. Once ready to continue, click **Create** and then **Yes** to confirm your changes.

29. The policy summary will now be shown again, this time with active enforcements.



Home > Policies

Student 16 Remediation Policy

Policy ID: 3

Policy Summary

Type	Status	Conflict Priority	Created on / Modified on
Remediation - Windows	Enforced	N/A	09/02/2020, 8:35:30 AM

Policy Details

Created: 09/02/2020, 8:35:30 AM by 16
Last Modified: 09/02/2020, 8:35:30 AM by 16
Change Type: Created
Description: None

Tasks are executed in the order specified:
1. Edit Registry Data: Create or update HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Tanium\Tanium Client\Student16, Data Type: REG_DWORD, Data: 1

Enforcements

Computer Group:	Schedule:	Start Date:	End Date:
Student 16	Run Every 30 Minutes	N/A	N/A

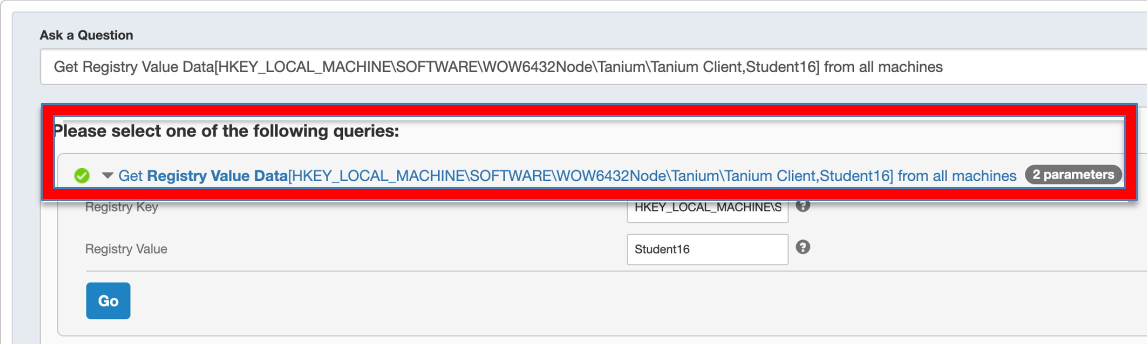
Policy Results

No results available.

30. Click on the Tanium logo top-left to return to the main homepage. In the **Ask a Question** box, issue the following question:

Get Registry Value Data[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Tanium\Tanium Client,Student<Student ID Number>] from all machines

Once the parser finds the correct query, click on the link to issue it.



Get Registry Value Data[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Tanium\Tanium Client,Student16] from all machines

Please select one of the following queries:

Get **Registry Value Data**[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Tanium\Tanium Client,Student16] from all machines

Registry Key: HKEY_LOCAL_MACHINE\S

Registry Value: Student16

	Using a Tanium Sensor, we are able to query the registry key value without the need to have direct access to the endpoint in question. Tanium Protect will monitor the value for the above registry key and remediate any deviation from it quickly. You have now completed lab 8.

Lab 9: Paging Doctor Tanium…

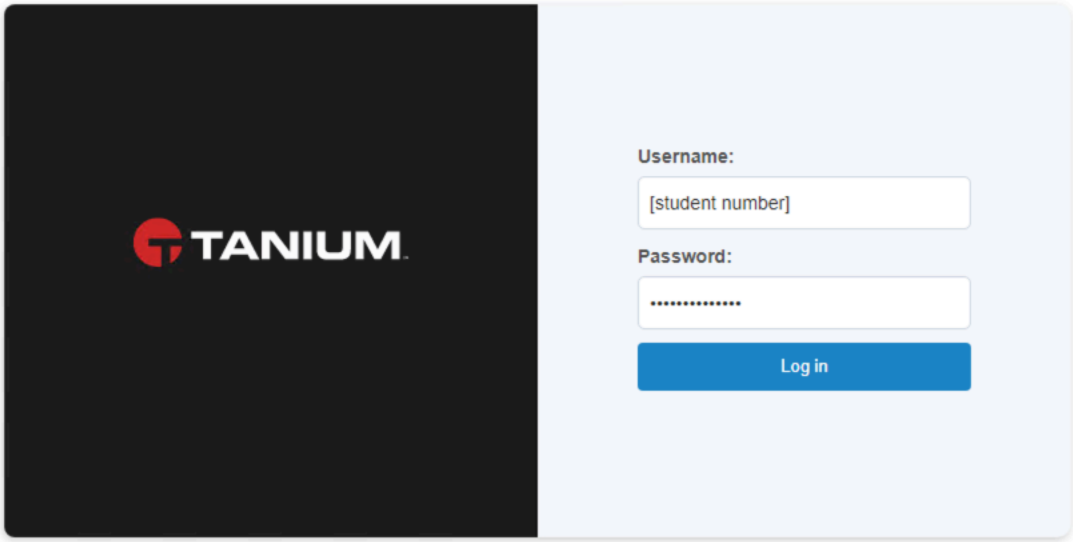
How to use Performance to conduct an ongoing health assessment

Objectives

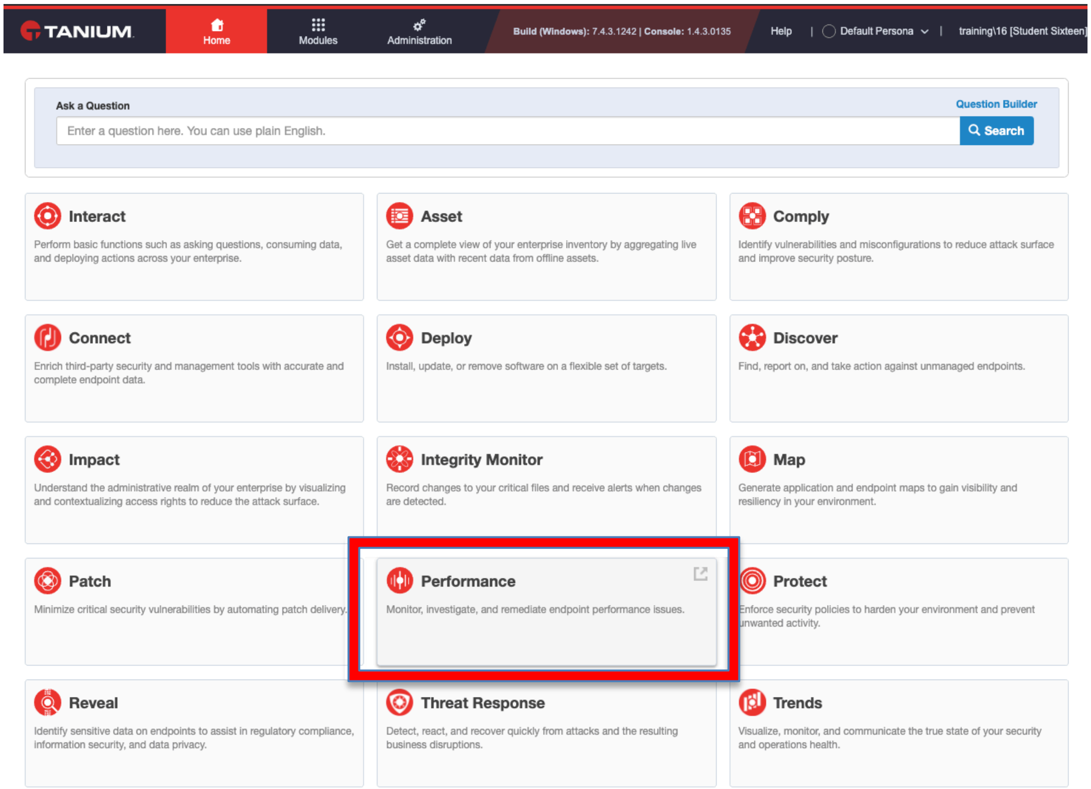
By the end of this lab you will have completed the following objectives:

- Explore enterprise-wide health monitoring
- Interrogate performance of a single client in real time
- Troubleshoot an unreliable application

Lab Steps

1.	Using the URL provided, open the Tanium console and enter your credentials  Username: [student number] Password: ••••••••••••••

2. If you are not already at the homepage, click the **Tanium** logo top-left to return there. Click on the **Performance** “baseball card” to enter the Tanium Performance module workbench.



TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Ask a Question
Question Builder
Enter a question here. You can use plain English.
Search

Interact
Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise.

Asset
Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets.

Comply
Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.

Connect
Enrich third-party security and management tools with accurate and complete endpoint data.

Deploy
Install, update, or remove software on a flexible set of targets.

Discover
Find, report on, and take action against unmanaged endpoints.

Impact
Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface.

Integrity Monitor
Record changes to your critical files and receive alerts when changes are detected.

Map
Generate application and endpoint maps to gain visibility and resiliency in your environment.

Patch
Minimize critical security vulnerabilities by automating patch delivery.

Performance
Monitor, investigate, and remediate endpoint performance issues.

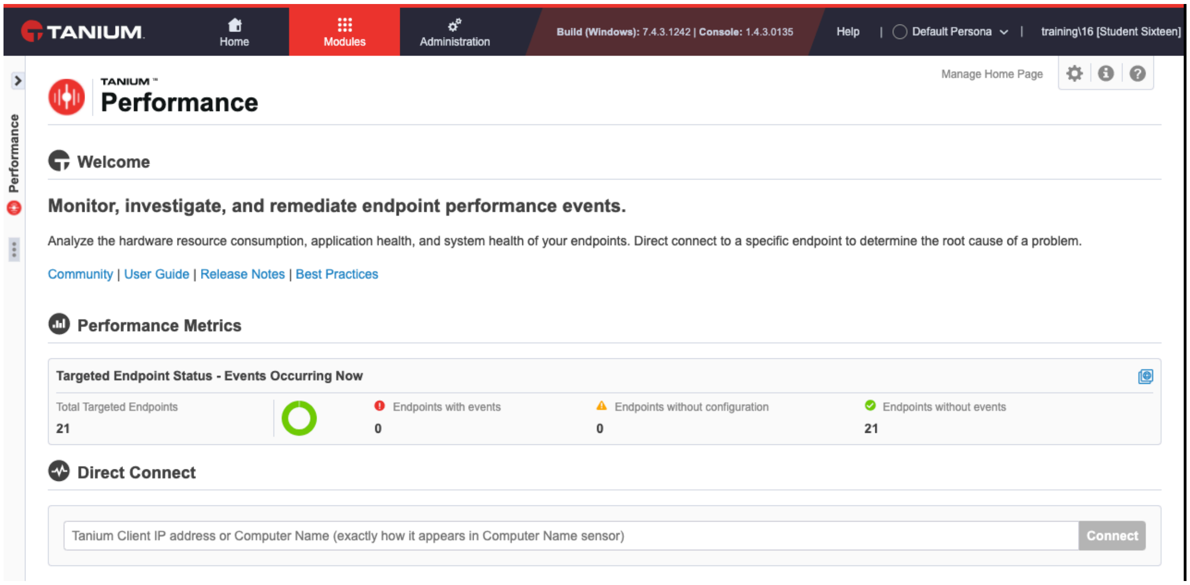
Protect
Enforce security policies to harden your environment and prevent unwanted activity.

Reveal
Identify sensitive data on endpoints to assist in regulatory compliance, information security, and data privacy.

Threat Response
Detect, react, and recover quickly from attacks and the resulting business disruptions.

Trends
Visualize, monitor, and communicate the true state of your security and operations health.

3. Explore the home page. It provides high level metrics on performance events and also allows you to establish direct connection to endpoints, which we will look at in more detail later in this lab.



Performance

Welcome

Monitor, investigate, and remediate endpoint performance events.

Analyze the hardware resource consumption, application health, and system health of your endpoints. Direct connect to a specific endpoint to determine the root cause of a problem.

Community | User Guide | Release Notes | Best Practices

Performance Metrics

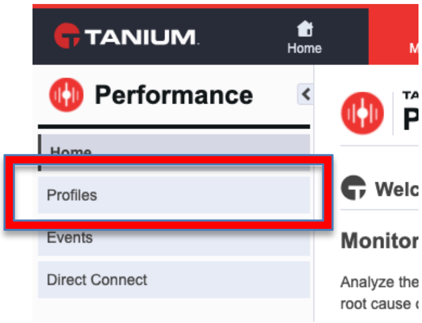
Targeted Endpoint Status - Events Occurring Now

Total Targeted Endpoints	Endpoints with events	Endpoints without configuration	Endpoints without events
21	0	0	21

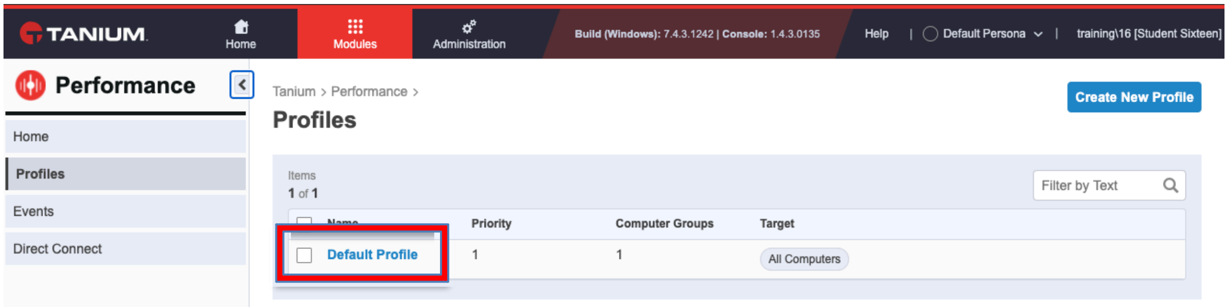
Direct Connect

Tanium Client IP address or Computer Name (exactly how it appears in Computer Name sensor)

4. On the pop-out menu, click on **Profiles**.



Here, you will find the profiles which are configured to specify which events and event types are collected and evaluated on the managed clients. Click on **Default Profile** to open it.



Profiles

Name	Priority	Computer Groups	Target
Default Profile	1	1	All Computers

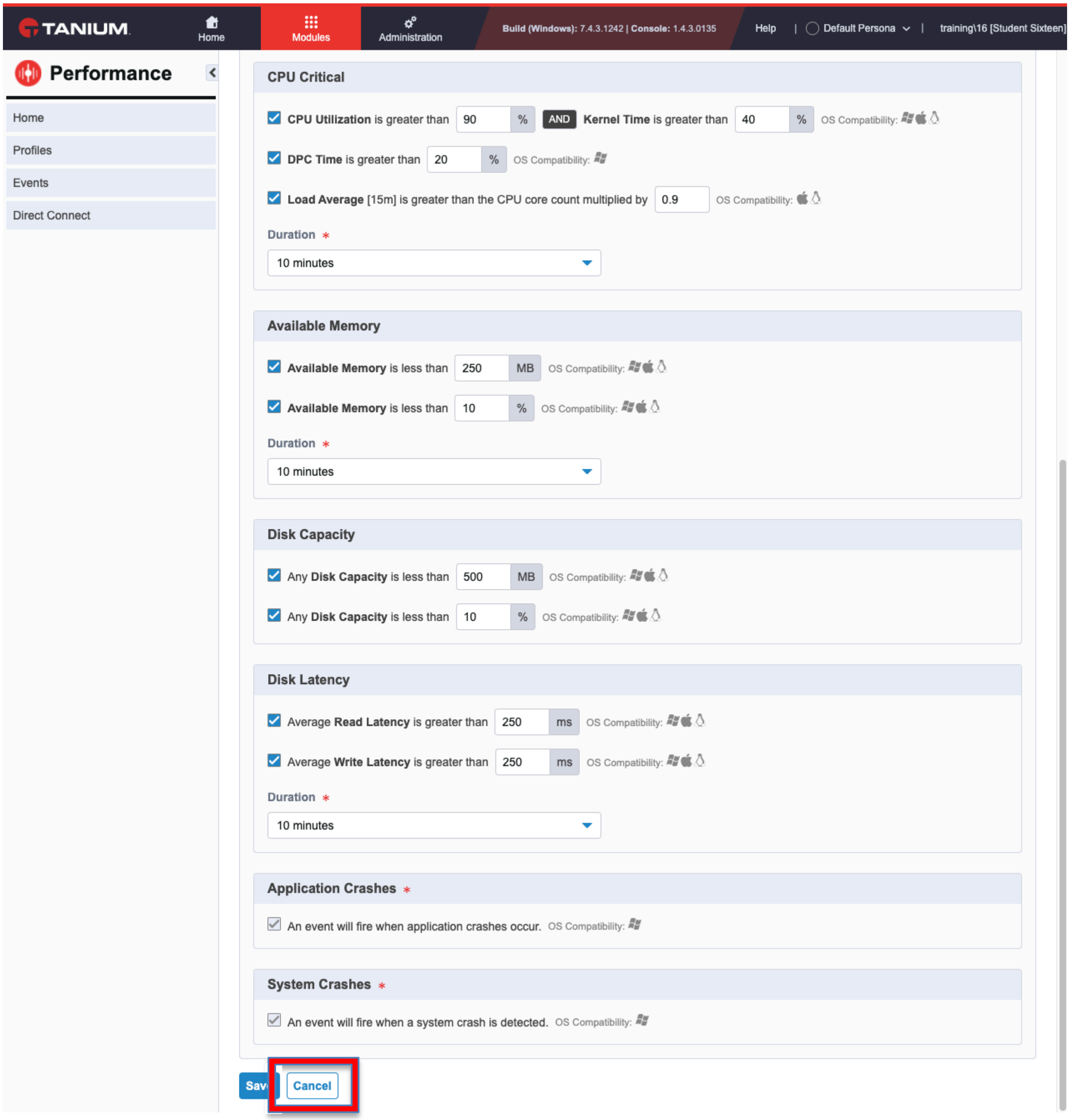
5. Review the profiles configuration. In here you can specify which computer groups will receive this profile, how much performance data is retained, and the retention period of that data.

You can also enable and disable the collection and evaluation of:

- CPU load
- Available Memory
- Disk Capacity
- Disk Latency
- Application Crashes
- System Crashes

Within each of these categories, there are settings which can be adjusted individually to allow you to fine tune your performance baseline which is being measured against.

6. Once you have finished exploring the available configuration settings, click on **Cancel** to exit without making any changes and return you to the **Profiles** page.



CPU Critical

☑ **CPU Utilization** is greater than 90 % AND **Kernel Time** is greater than 40 % OS Compatibility:

☑ **DPC Time** is greater than 20 % OS Compatibility:

☑ **Load Average** [15m] is greater than the CPU core count multiplied by 0.9 OS Compatibility:

Duration *
10 minutes

Available Memory

☑ **Available Memory** is less than 250 MB OS Compatibility:

☑ **Available Memory** is less than 10 % OS Compatibility:

Duration *
10 minutes

Disk Capacity

☑ Any **Disk Capacity** is less than 500 MB OS Compatibility:

☑ Any **Disk Capacity** is less than 10 % OS Compatibility:

Disk Latency

☑ Average **Read Latency** is greater than 250 ms OS Compatibility:

☑ Average **Write Latency** is greater than 250 ms OS Compatibility:

Duration *
10 minutes

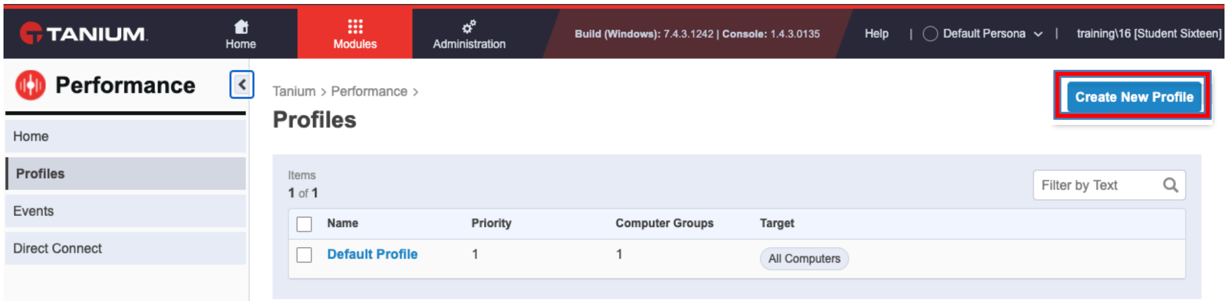
Application Crashes *

☑ An event will fire when application crashes occur. OS Compatibility:

System Crashes *

☑ An event will fire when a system crash is detected. OS Compatibility:

7. Press the **Create New Profile** button to now create your own Performance profile



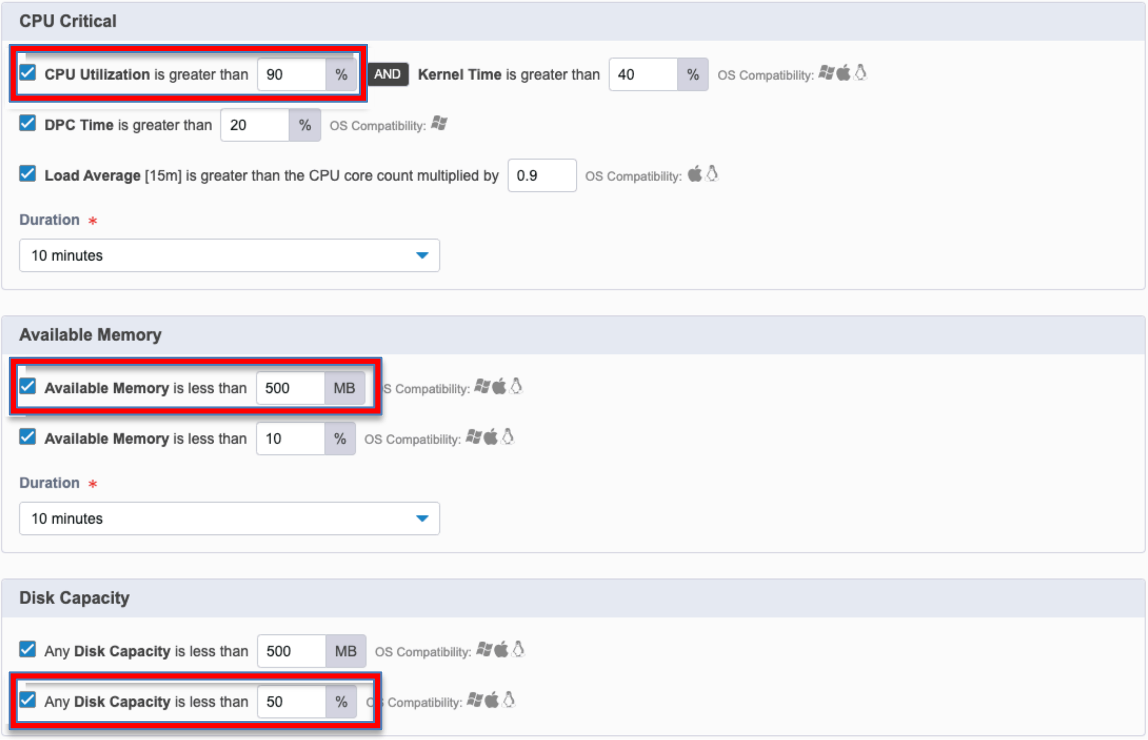
Profiles

Items
1 of 1

Name	Priority	Computer Groups	Target
Default Profile	1	1	All Computers

8. Name your profile *Student <Student ID Number> Performance Profile* and configure the following items, leaving all other options as their defaults:

- **Target**: Select the computer group associated to your student ID number
- **CPU Utilization**: 95%
- **Available Memory is less than**: 500 MB
- **Any Disk Capacity is less than**: 50%



CPU Critical

☑ **CPU Utilization** is greater than 90 % AND **Kernel Time** is greater than 40 % OS Compatibility:

☑ **DPC Time** is greater than 20 % OS Compatibility:

☑ **Load Average** [15m] is greater than the CPU core count multiplied by 0.9 OS Compatibility:

Duration *
10 minutes

Available Memory

☑ **Available Memory** is less than 500 MB OS Compatibility:

☑ **Available Memory** is less than 10 % OS Compatibility:

Duration *
10 minutes

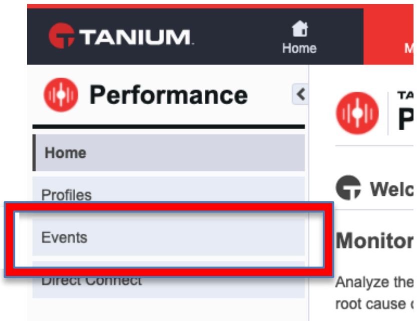
Disk Capacity

☑ Any **Disk Capacity** is less than 500 MB OS Compatibility:

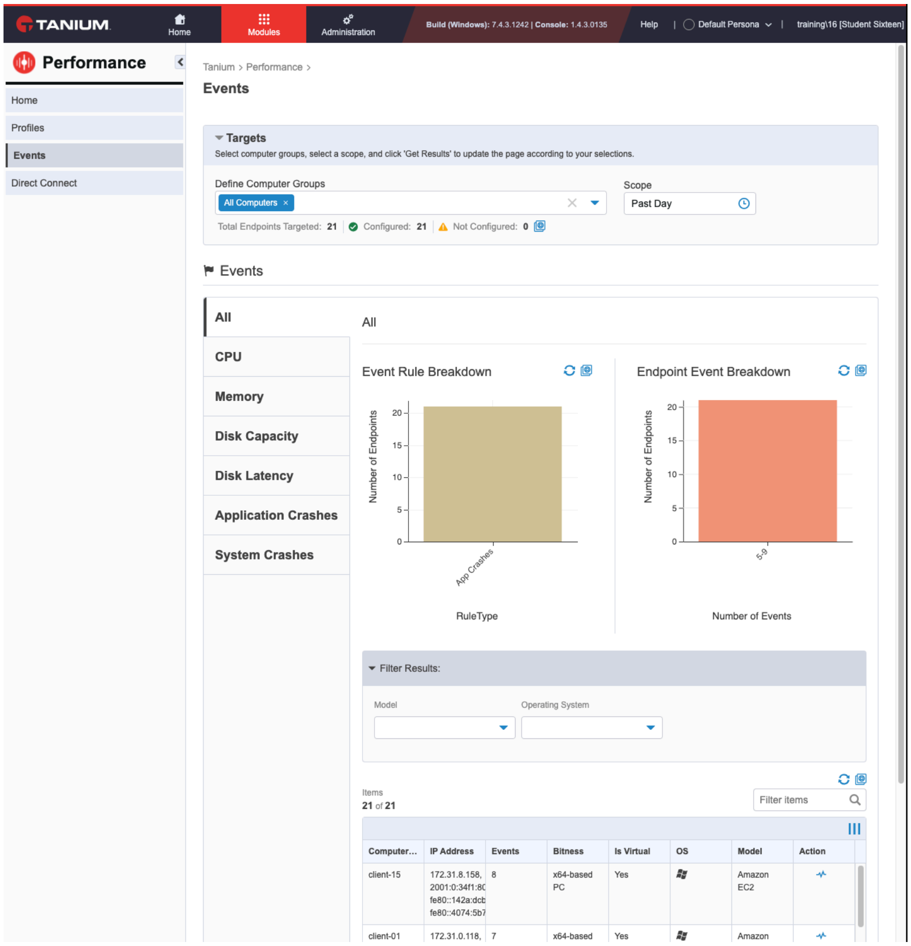
☑ Any **Disk Capacity** is less than 50 % OS Compatibility:

The press **Save**. Your profile will now be saved and deployed to your targeted endpoint.

9. Pop out the menu on the left-hand side again and choose **Events**.



Here you will find detailed information and metrics on the performance events collected. Explore the various graphs, categories and types of events available.



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135

training\16 [Student Sixteen]

Events

Targets

Select computer groups, select a scope, and click 'Get Results' to update the page according to your selections.

Define Computer Groups: All Computers

Scope: Past Day

Total Endpoints Targeted: 21 | Configured: 21 | Not Configured: 0

Events

All

Filter Results:

Model

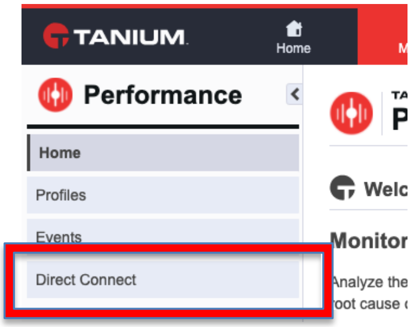
Operating System

Items
21 of 21

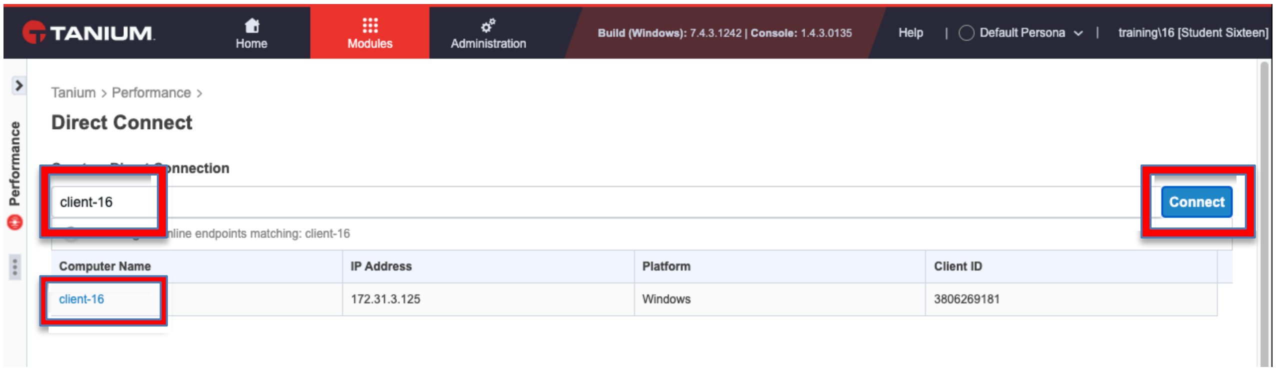
Computer...	IP Address	Events	Bitness	Is Virtual	OS	Model	Action
client-15	172.31.8.158, 2001:0:34f1:80 fe80::142a:dcb fe80::4074:5b7	8	x64-based PC	Yes	⊞	Amazon EC2	∿
client-01	172.31.0.118,	7	x64-based	Yes	⊞	Amazon	∿

Are the results graphs not loading for you? That's because we have not delegated to your 'standard' account the role to view this data. Try again with your administrative persona!

10. Return to the pop-out menu and select **Direct Connect**.

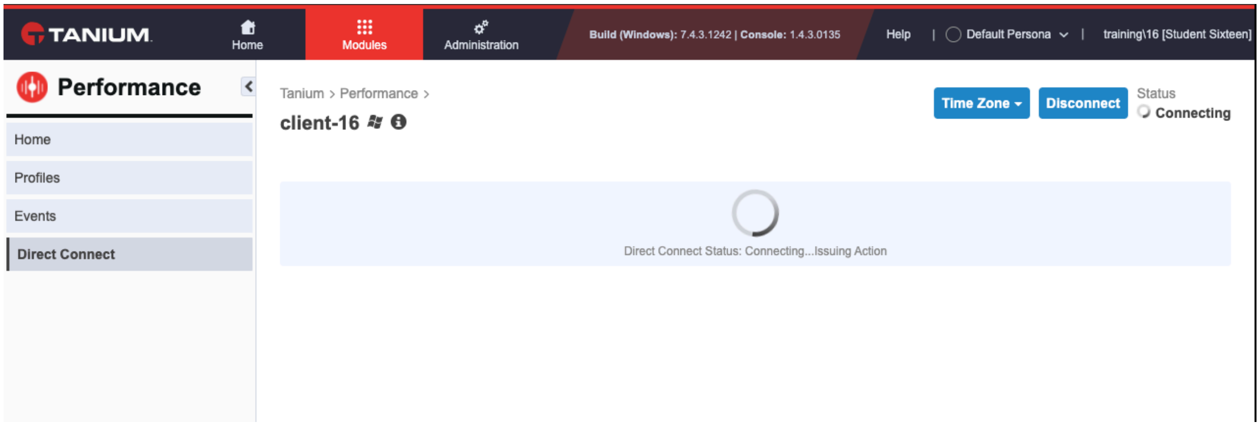


Enter a hostname of *any* lab client and then click on **Connect**. If Direct Connect doesn't immediately attempt a connection, click the link under **Computer Name**. If you don't know the exact name of an endpoint, try just entering *client* into the connection control and press **Connect**. Then you can select an endpoint from the list returned.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Performance
Tanium > Performance >
Direct Connect
Create a Direct Connection
client-16
Connect
Online endpoints matching: client-16

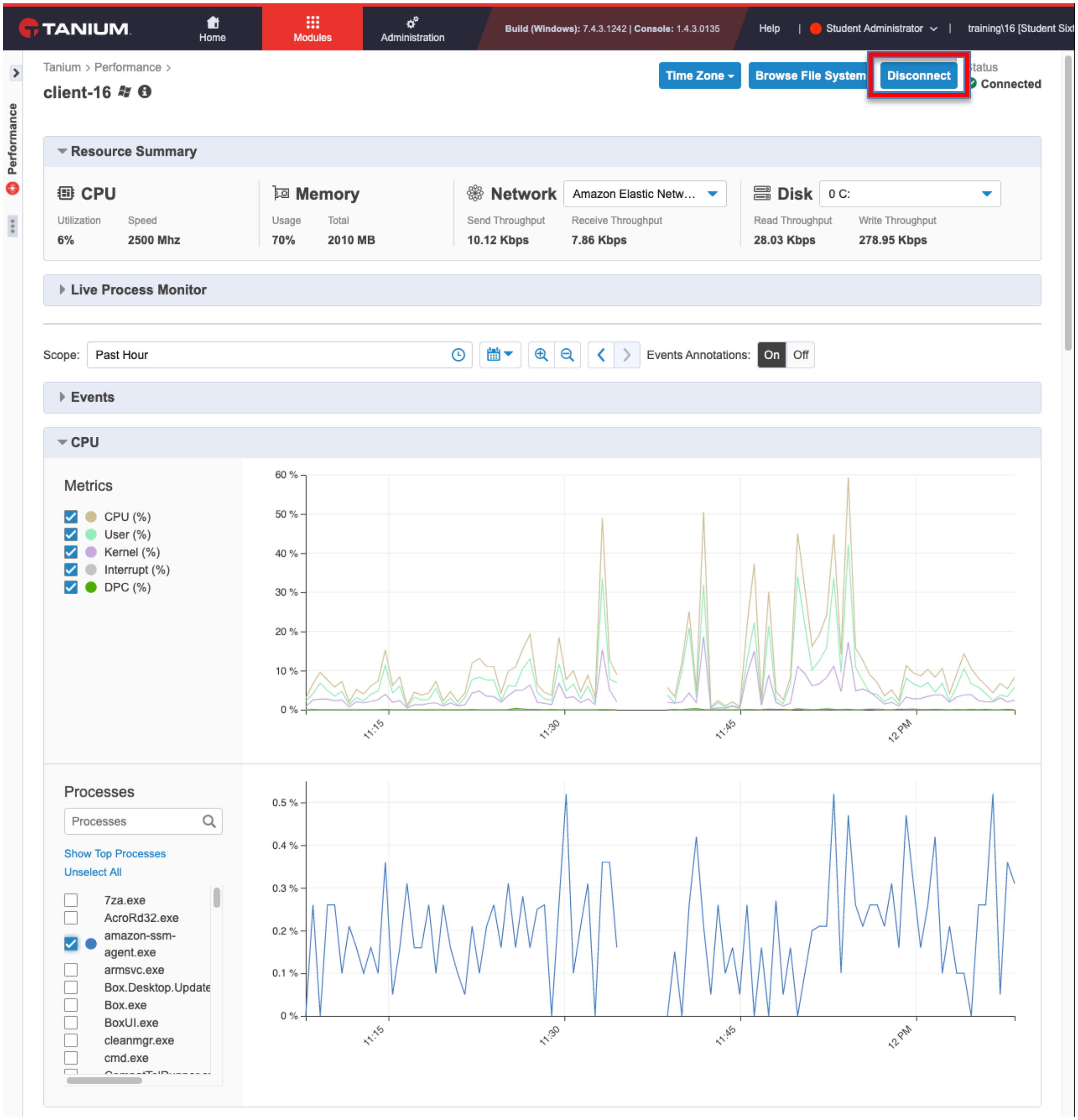
Computer Name	IP Address	Platform	Client ID
client-16	172.31.3.125	Windows	3806269181

An action will now be issued to the specified endpoint requesting a Direct Connect session.



Direct Connect Status: Connecting...Issuing Action

11. Once the session is successfully established, you will begin to see performance data in real time and have the ability to browse the remote file system. You can expand and collapse sections as you choose, just use the small area next to each title.



CPU — Utilization: 6% — Speed: 2500 Mhz

Memory — Usage: 70% — Total: 2010 MB

Network (Amazon Elastic Netw…) — Send Throughput: 10.12 Kbps — Receive Throughput: 7.86 Kbps

Disk (0 C:) — Read Throughput: 28.03 Kbps — Write Throughput: 278.95 Kbps

Scope: Past Hour — Events Annotations: On Off

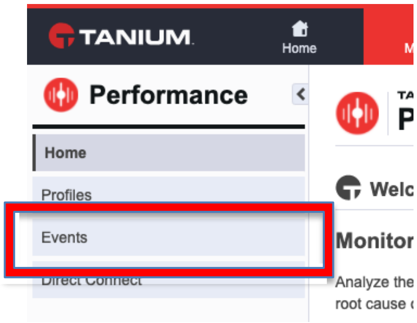
CPU Metrics: ☑ CPU (%) ☑ User (%) ☑ Kernel (%) ☑ Interrupt (%) ☑ DPC (%)

Processes:
- ☐ 7za.exe
- ☐ AcroRd32.exe
- ☑ amazon-ssm-agent.exe
- ☐ armsvc.exe
- ☐ Box.Desktop.Update
- ☐ Box.exe
- ☐ BoxUI.exe
- ☐ cleanmgr.exe
- ☐ cmd.exe

Have a browse around, play with the various options and information to discover how powerful this module is, and then click on **Disconnect** once finished.

12. **The following steps are optional and will not be covered by the instructor. If you have the time then have a go at completing them!**

Once again, pop out the menu on the left-hand side and return to the **Events** page.



Now we have a challenge for you!

There is an application causing issues within the enterprise (hint: *start* from the module home page to view data from all endpoints rather than a specific one).

Using the functionality and information provided here, can you:

❓ Identify the nature of the problem?

❓ Identify the application causing the issue?

❓ Identify one or more endpoints experiencing the issue?

❓ Use Direct Connect to establish how often the issue is occurring and any other data?

Once you have completed the above tasks, let your instructor know and your answers will be reviewed together as a group.

You have completed lab 9.

Lab 10: Charting Your Course

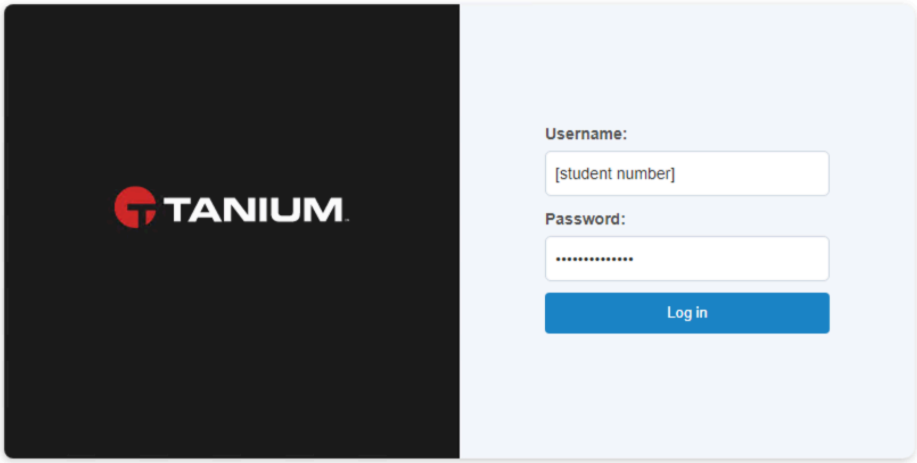
Never underestimate the value of a map.

Objectives

By the end of this lab you will have completed the following objectives:

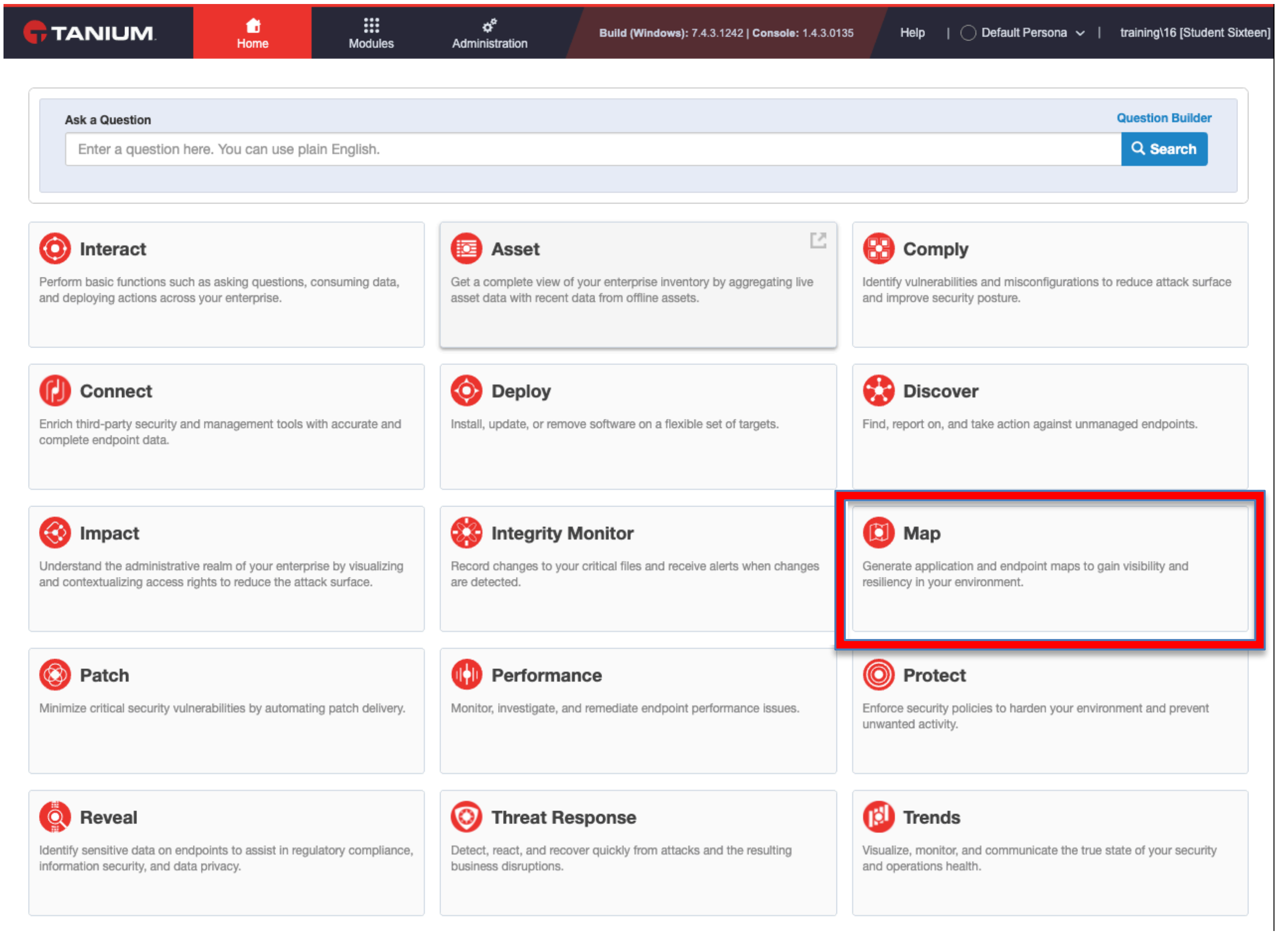
- Created a map of the lab environment.

Lab Steps

1.	Using the URL provided, open the Tanium console and enter your credentials  Username: [student number] Password: •••••••••••••• For this lab you will need the IP address of the Tanium Server and your designated client. This can be obtained by asking your instructor or issuing the following questions in Tanium Interact: *Get computer name and IPv4 Address from all machines* The Tanium server hostname is **TS1.training.lab**. Make a note of its IP address as you will need it a little later.

2. Click on the **Tanium** logo at the top left-hand corner to return you to the home page if you aren’t there already.

You should see the homepage of the Tanium console, displaying the various “baseball cards” for the available modules. From here, click on **Map**.


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Ask a Question
Question Builder
Enter a question here. You can use plain English.
Search

Interact
Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise.

Asset
Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets.

Comply
Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.

Connect
Enrich third-party security and management tools with accurate and complete endpoint data.

Deploy
Install, update, or remove software on a flexible set of targets.

Discover
Find, report on, and take action against unmanaged endpoints.

Impact
Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface.

Integrity Monitor
Record changes to your critical files and receive alerts when changes are detected.

Map
Generate application and endpoint maps to gain visibility and resiliency in your environment.

Patch
Minimize critical security vulnerabilities by automating patch delivery.

Performance
Monitor, investigate, and remediate endpoint performance issues.

Protect
Enforce security policies to harden your environment and prevent unwanted activity.

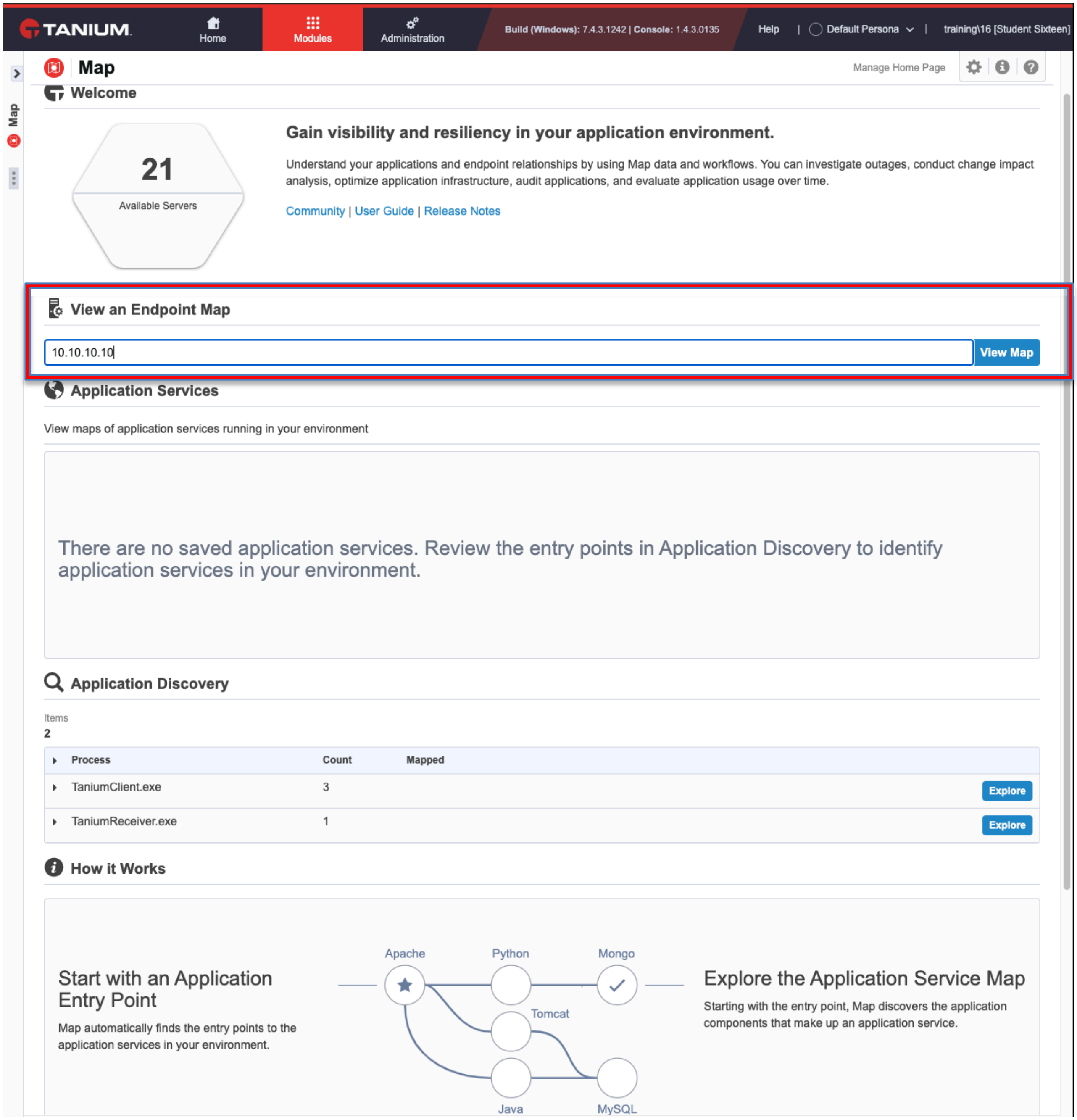
Reveal
Identify sensitive data on endpoints to assist in regulatory compliance, information security, and data privacy.

Threat Response
Detect, react, and recover quickly from attacks and the resulting business disruptions.

Trends
Visualize, monitor, and communicate the true state of your security and operations health.

This will now take you to the Map workbench.

3. You will now see the **Map** workbench homepage. Enter the IP Address of the Tanium Server, which you obtained earlier, into the field under **View an Endpoint Map**.



TANIUM | Home | Modules | Administration | **Build (Windows):** 7.4.3.1242 | **Console:** 1.4.3.0135 | Help | Default Persona | training\16 [Student Sixteen]

Map — Manage Home Page

Welcome

21

Available Servers

Gain visibility and resiliency in your application environment.

Understand your applications and endpoint relationships by using Map data and workflows. You can investigate outages, conduct change impact analysis, optimize application infrastructure, audit applications, and evaluate application usage over time.

Community | User Guide | Release Notes

View an Endpoint Map

10.10.10.10 — View Map

Application Services

View maps of application services running in your environment

There are no saved application services. Review the entry points in Application Discovery to identify application services in your environment.

Application Discovery

Items

2

Process	Count	Mapped	
TaniumClient.exe	3		Explore
TaniumReceiver.exe	1		Explore

How it Works

Start with an Application Entry Point

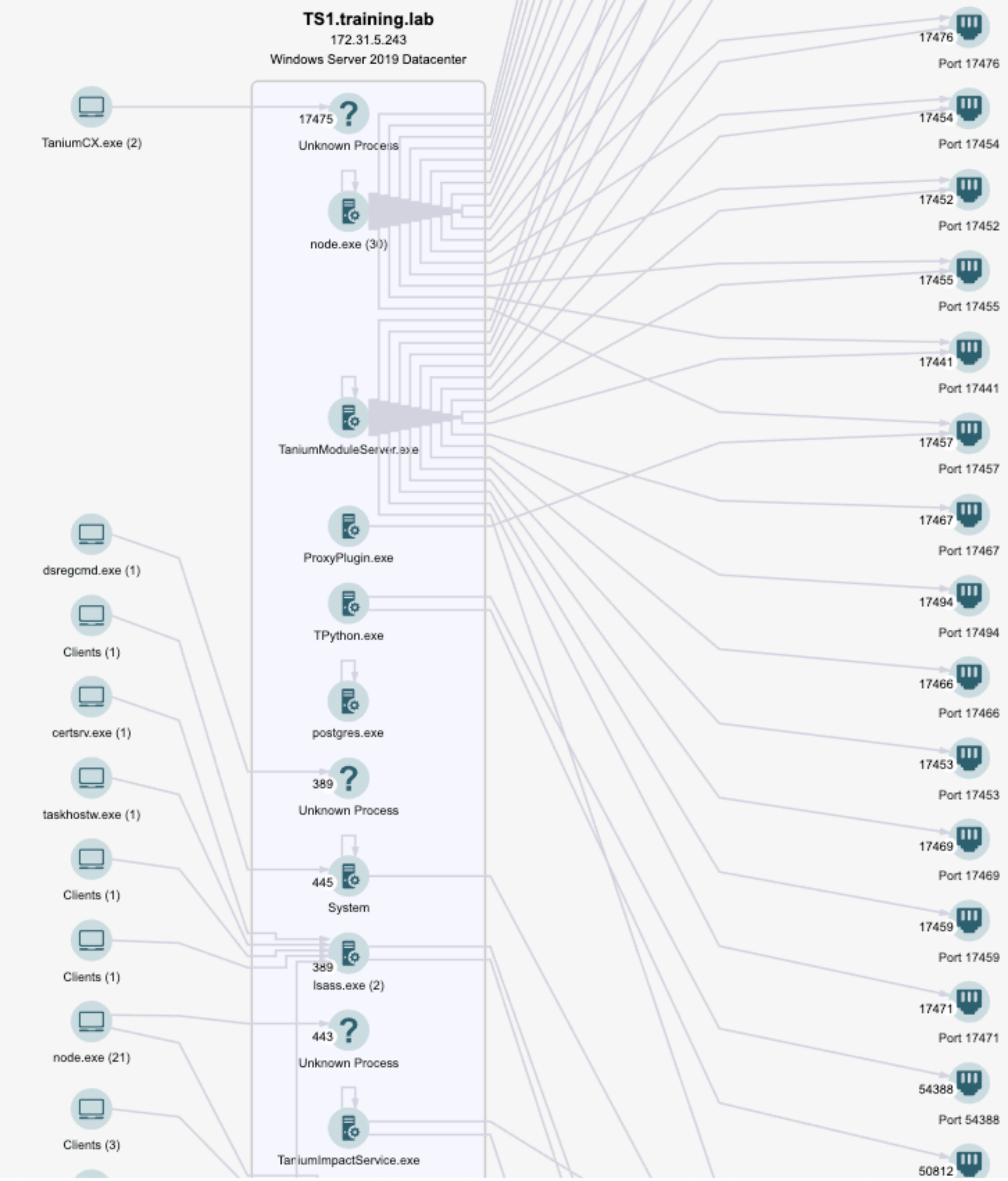
Map automatically finds the entry points to the application services in your environment.

Explore the Application Service Map

Starting with the entry point, Map discovers the application components that make up an application service.

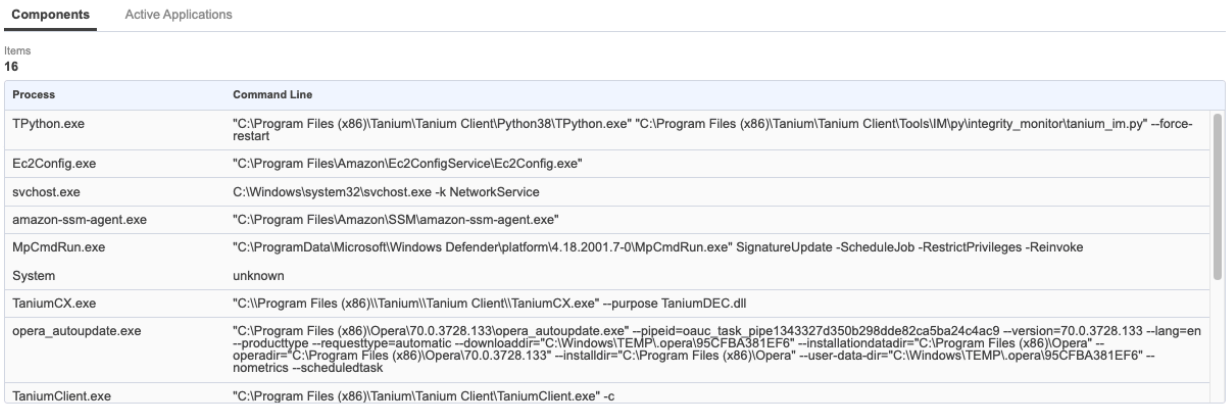
Click on **View Map** to begin generating the map.

4. Tanium Map will now interrogate the recorder data on that endpoint to establish, among other things, which services are running, which ports are open, where the endpoint is connecting to and which endpoints are connecting to it. Note that numbers in brackets indicate the number of connections active.



Your map will likely be much bigger than the one displayed above!

5. At the bottom of the map, additional contextual information can be found depending on which element of the map you are looking at. You can select elements from the map to change the focus for the **Component Details** section.

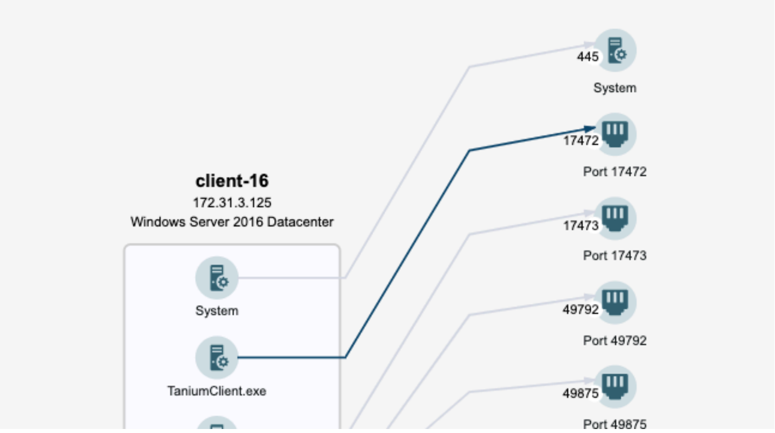


Components Active Applications

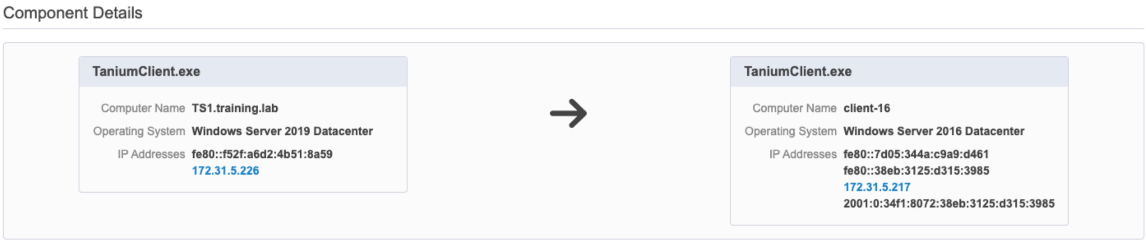
Items
16

Process	Command Line
TPython.exe	"C:\Program Files (x86)\Tanium\Tanium Client\Python38\TPython.exe" "C:\Program Files (x86)\Tanium\Tanium Client\Tools\IM\py\integrity_monitor\tanium_im.py" --force-restart
Ec2Config.exe	"C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe"
svchost.exe	C:\Windows\system32\svchost.exe -k NetworkService
amazon-ssm-agent.exe	"C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"
MpCmdRun.exe	"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2001.7-0\MpCmdRun.exe" SignatureUpdate -ScheduleJob -RestrictPrivileges -Reinvoke
System	unknown
TaniumCX.exe	"C:\\Program Files (x86)\\Tanium\\Tanium Client\\TaniumCX.exe" --purpose TaniumDEC.dll
opera_autoupdate.exe	"C:\Program Files (x86)\Opera\70.0.3728.133\opera_autoupdate.exe" --pipeid=oauc_task_pipe1343327d350b298dde82ca5ba24c4ac9 --version=70.0.3728.133 --lang=en --producttype --requesttype=automatic --downloaddir="C:\Windows\TEMP\.opera\95CFBA381EF6" --installationdatadir="C:\Program Files (x86)\Opera" --operadir="C:\Program Files (x86)\Opera\70.0.3728.133" --installdir="C:\Program Files (x86)\Opera" --user-data-dir="C:\Windows\TEMP\.opera\95CFBA381EF6" --nometrics --scheduledtask
TaniumClient.exe	"C:\Program Files (x86)\Tanium\Tanium Client\TaniumClient.exe" -c

6. Click on the **TaniumClient.exe** connection line on the map as shown below (your own line may be in a different location to that shown here). It will highlight in **blue**:



You will then see the details of that connection, showing the destination IP of the connection, and other vital information.



Component Details

TaniumClient.exe

Computer Name **TS1.training.lab**
Operating System **Windows Server 2019 Datacenter**
IP Addresses **fe80::f52f:a6d2:4b51:8a59**
172.31.5.226

→

TaniumClient.exe

Computer Name **client-16**
Operating System **Windows Server 2016 Datacenter**
IP Addresses **fe80::7d05:344a:c9a9:d461**
fe80::38eb:3125:d315:3985
172.31.5.217
2001:0:34f1:8072:38eb:3125:d315:3985

You have now completed lab 10.

Lab 11: Making It Look Pretty

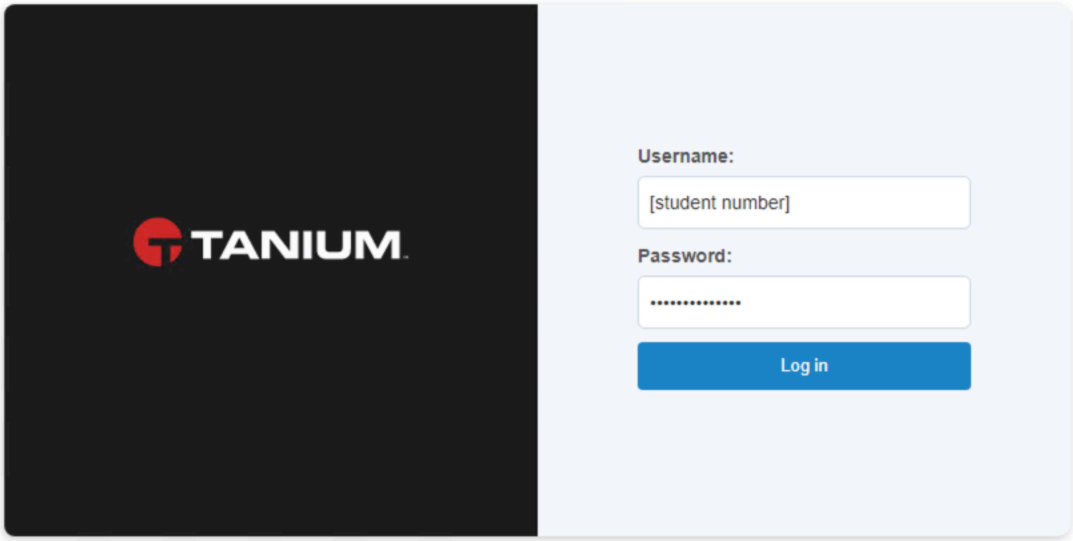
It’s time to put it all together and create some visuals.

Objectives

By the end of this lab you will have completed the following objectives:

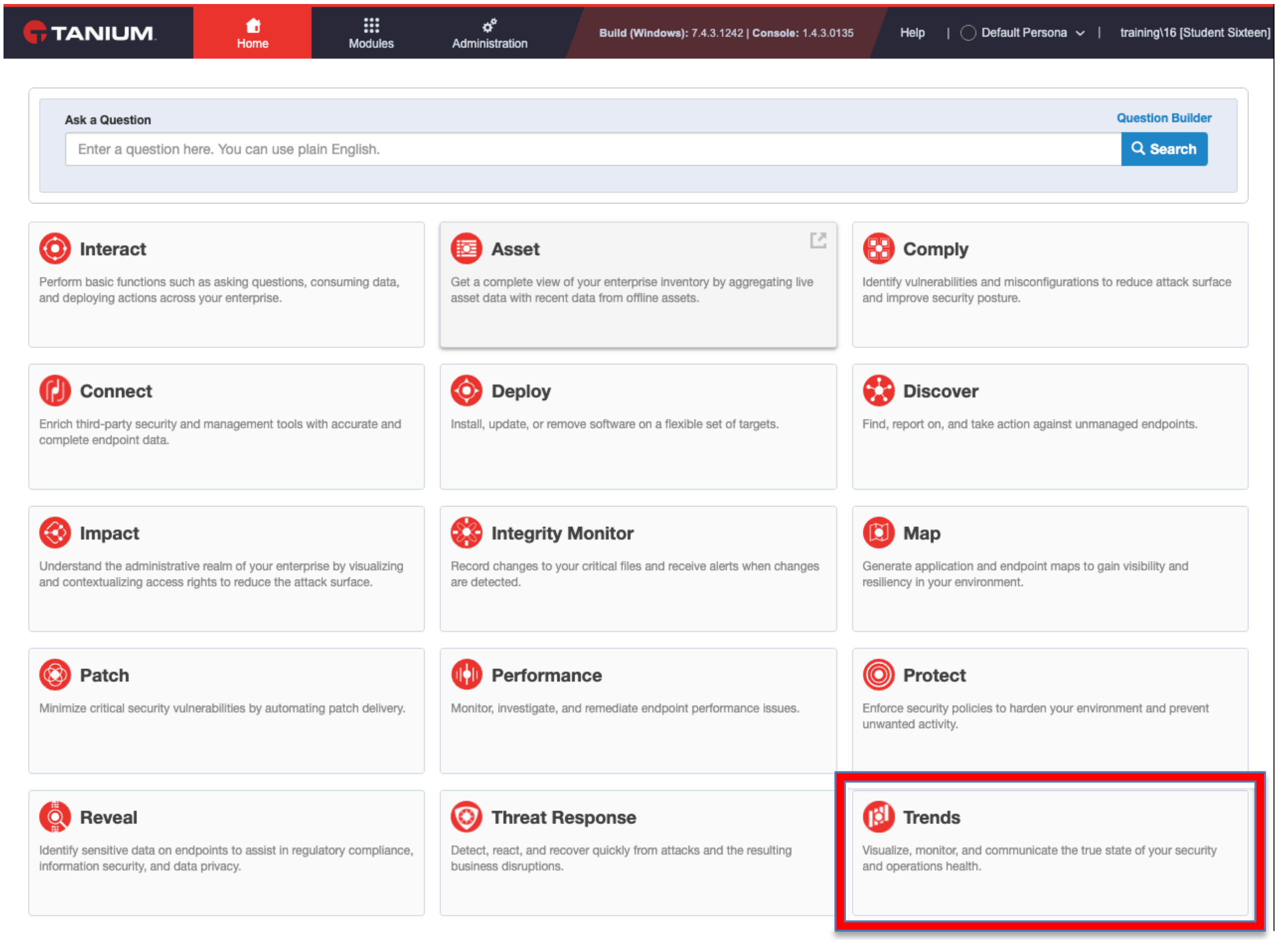
- Build custom IT Operations dashboard that reflects information from all the lessons learnt today

Lab Steps

1.	Using the URL provided, open the Tanium console and enter your credentials  Username: [student number] Password: ••••••••••••••

2. Click on the **Tanium** logo at the top left-hand corner to return you to the home page if you aren't there already.

You should see the homepage of the Tanium console, displaying the various "baseball cards" for the available modules. From here, click on **Trends**.



TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Ask a Question
Question Builder
Enter a question here. You can use plain English.
Search

Interact
Perform basic functions such as asking questions, consuming data, and deploying actions across your enterprise.

Asset
Get a complete view of your enterprise inventory by aggregating live asset data with recent data from offline assets.

Comply
Identify vulnerabilities and misconfigurations to reduce attack surface and improve security posture.

Connect
Enrich third-party security and management tools with accurate and complete endpoint data.

Deploy
Install, update, or remove software on a flexible set of targets.

Discover
Find, report on, and take action against unmanaged endpoints.

Impact
Understand the administrative realm of your enterprise by visualizing and contextualizing access rights to reduce the attack surface.

Integrity Monitor
Record changes to your critical files and receive alerts when changes are detected.

Map
Generate application and endpoint maps to gain visibility and resiliency in your environment.

Patch
Minimize critical security vulnerabilities by automating patch delivery.

Performance
Monitor, investigate, and remediate endpoint performance issues.

Protect
Enforce security policies to harden your environment and prevent unwanted activity.

Reveal
Identify sensitive data on endpoints to assist in regulatory compliance, information security, and data privacy.

Threat Response
Detect, react, and recover quickly from attacks and the resulting business disruptions.

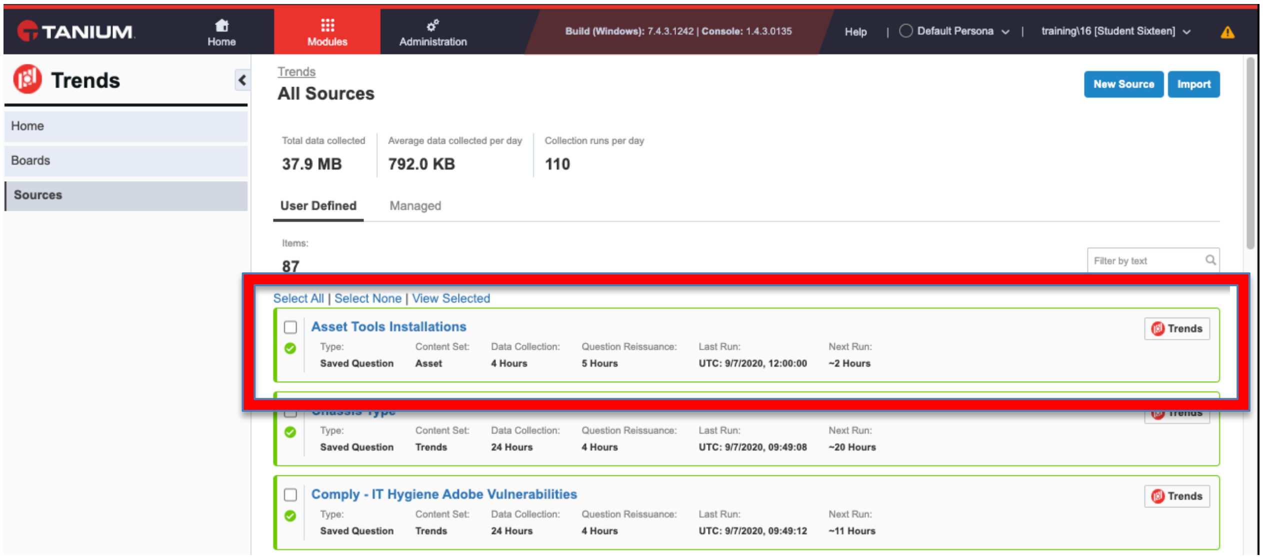
Trends
Visualize, monitor, and communicate the true state of your security and operations health.

This will now take you to the Trends workbench.

Explore the workbench to review the information available and how it is represented visually in the form of graphs and charts.

3. Trends operates using three core object types:

- **Sources** – These define which data points are collected



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135 | Default Persona | training\16 [Student Sixteen]

Trends
All Sources

Total data collected	Average data collected per day	Collection runs per day
37.9 MB	792.0 KB	110

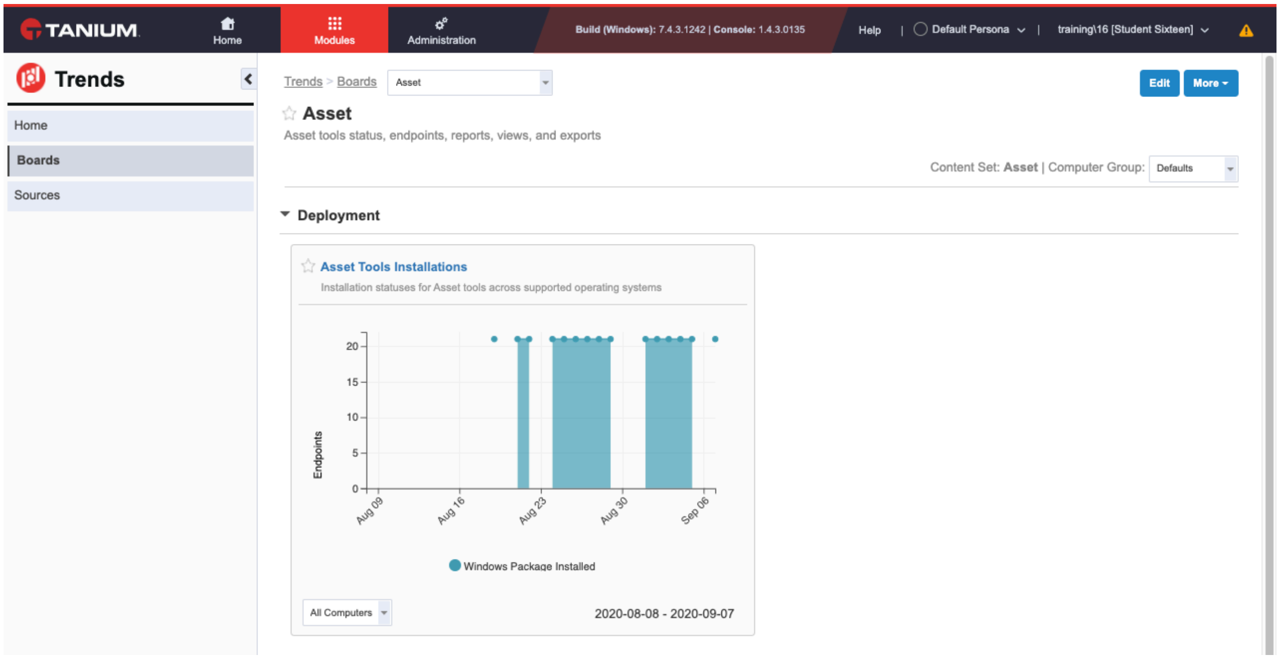
User Defined | Managed

Items:
87

Select All | Select None | View Selected

Name	Type:	Content Set:	Data Collection:	Question Reissuance:	Last Run:	Next Run:
Asset Tools Installations	Saved Question	Asset	4 Hours	5 Hours	UTC: 9/7/2020, 12:00:00	~2 Hours
Chassis Type	Saved Question	Trends	24 Hours	4 Hours	UTC: 9/7/2020, 09:49:08	~20 Hours
Comply - IT Hygiene Adobe Vulnerabilities	Saved Question	Trends	24 Hours	4 Hours	UTC: 9/7/2020, 09:49:12	~11 Hours

- **Boards** – These collate panels and can be used to group and organise related panels, such as those relevant to a specific module.



Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135 | Default Persona | training\16 [Student Sixteen]

Trends > Boards | Asset

Asset
Asset tools status, endpoints, reports, views, and exports

Content Set: **Asset** | Computer Group: Defaults

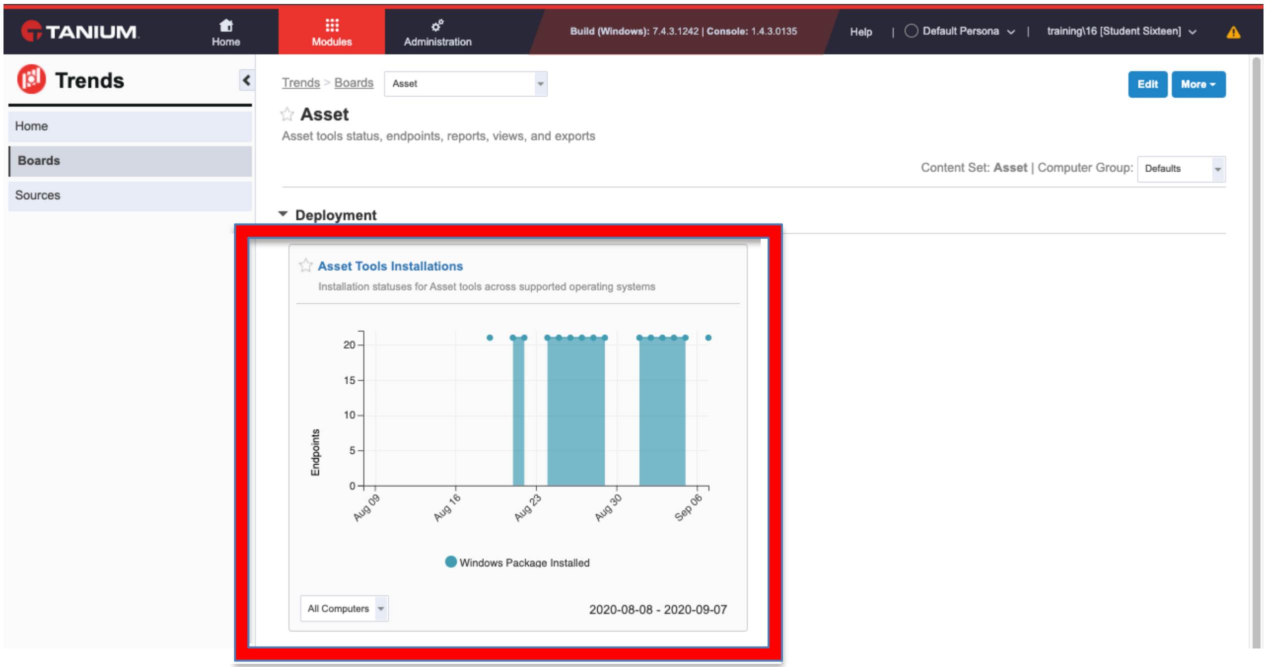
Deployment

Asset Tools Installations
Installation statuses for Asset tools across supported operating systems

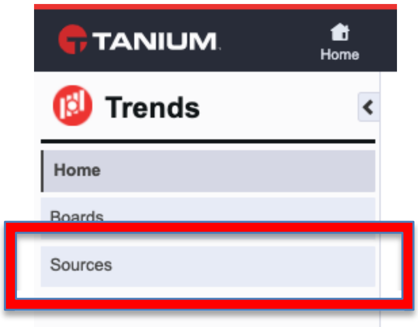
● Windows Package Installed

2020-08-08 - 2020-09-07

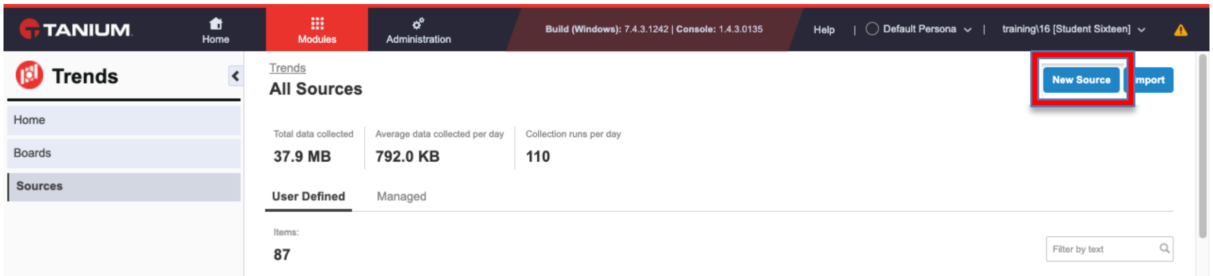
- **Panels** – These are used to visualise the data made available by the sources


TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Trends
Home
Boards
Sources
Trends > Boards
Asset
Edit
More
Asset
Asset tools status, endpoints, reports, views, and exports
Content Set: Asset | Computer Group: Defaults
Deployment
Asset Tools Installations
Installation statuses for Asset tools across supported operating systems
20
15
10
5
0
Endpoints
Aug 09
Aug 16
Aug 23
Aug 30
Sep 06
Windows Package Installed
All Computers
2020-08-08 - 2020-09-07

4. Click on **Sources** on the pop-out menu on the left-hand side.

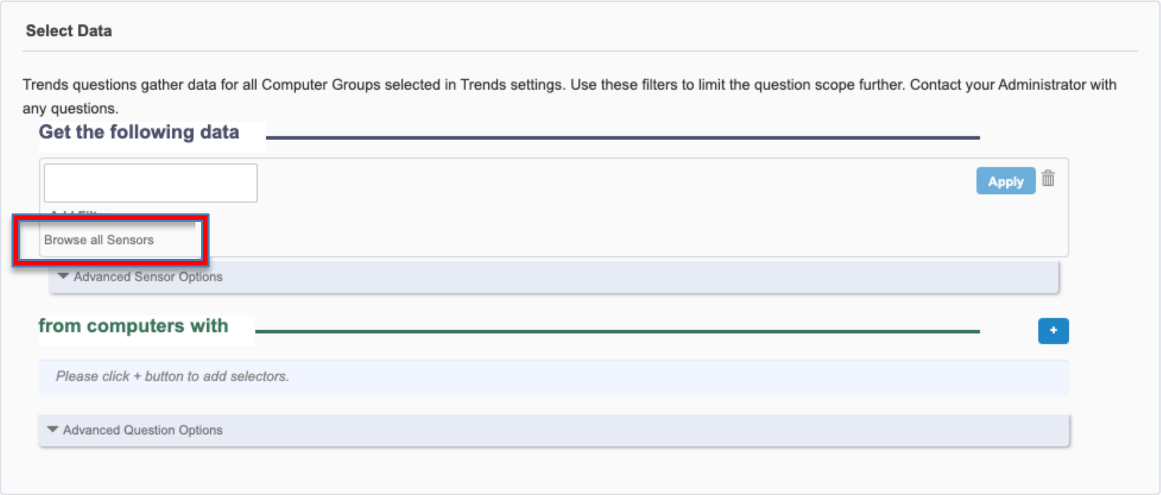


5. Click on the **New Source** button.

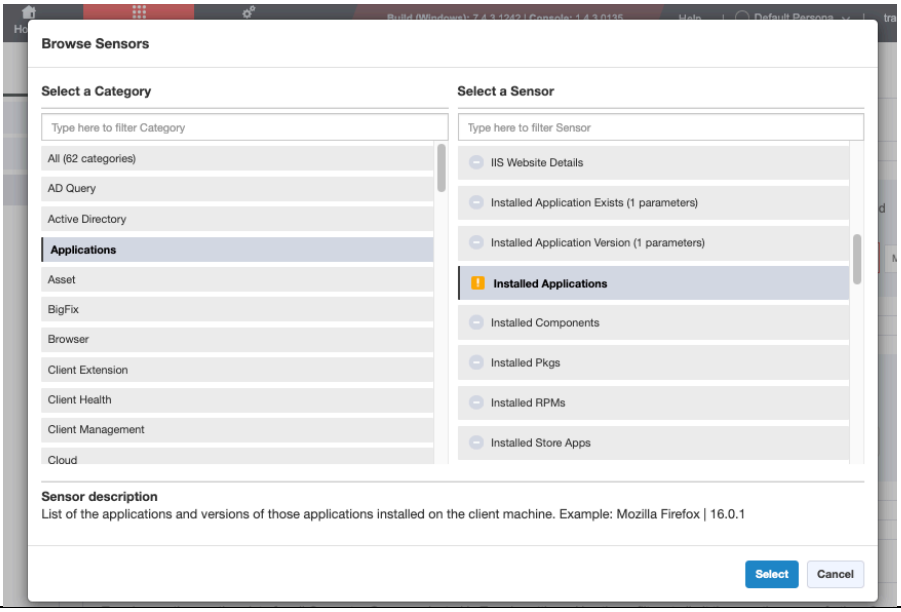
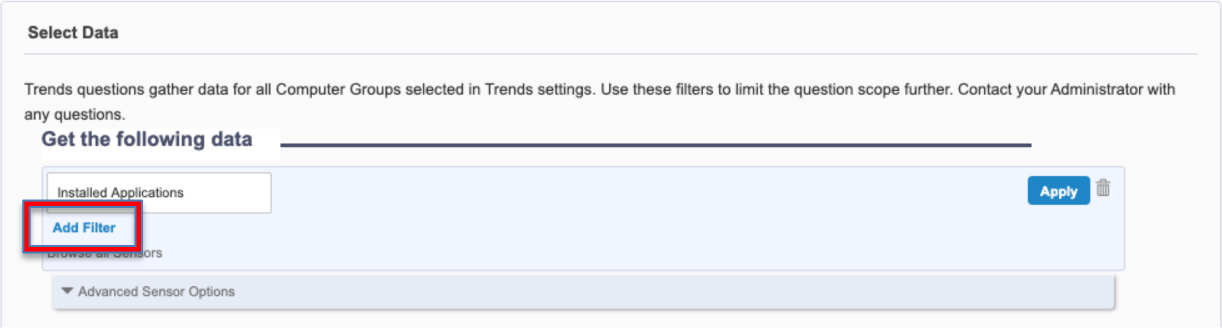


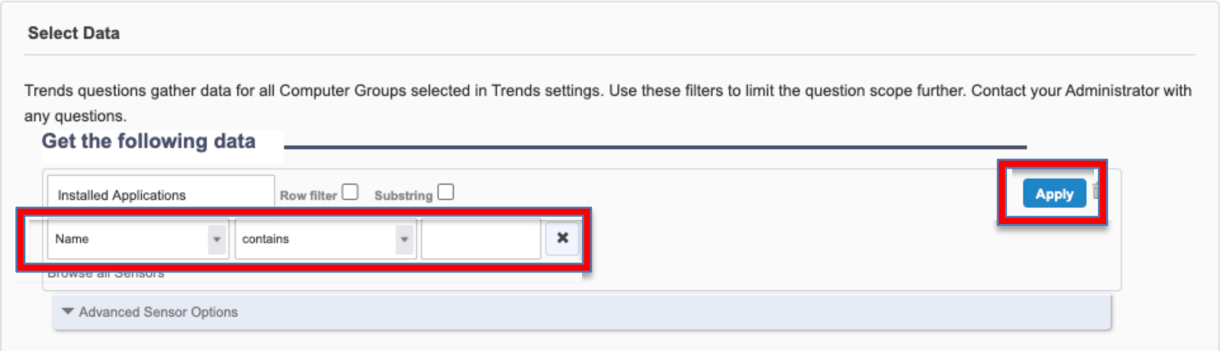
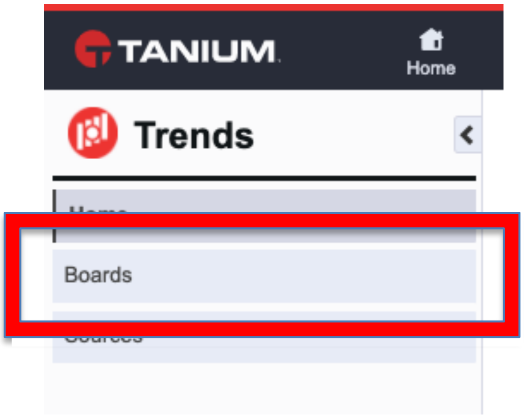
Set the **Name** of the new source as *Student <Student ID Number> - Source*
Set the **Question Reissue** to *30 Minutes*

In the **Select Data** section, click the plus symbol for **Get the Following Data** and then on **Browse all Sensors.**

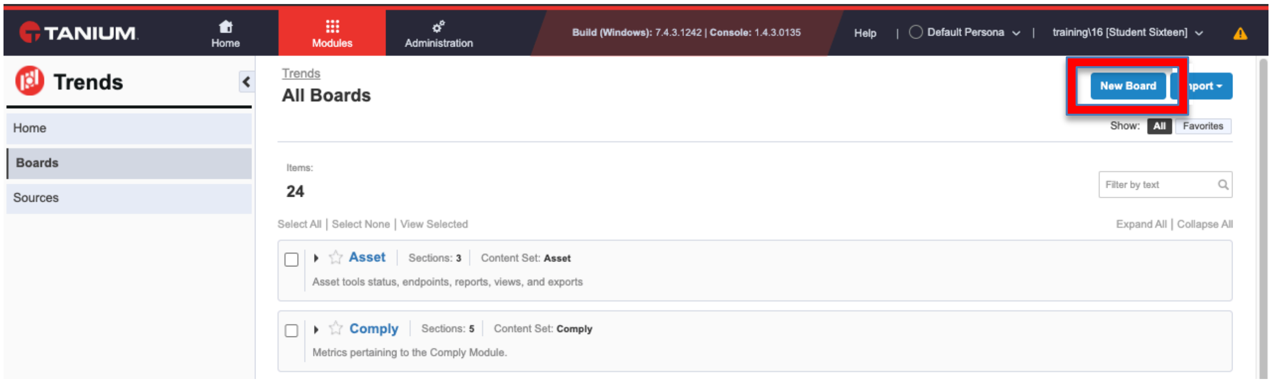


Trends questions gather data for all Computer Groups selected in Trends settings. Use these filters to limit the question scope further. Contact your Administrator with any questions.

6.	You will now be able to browse for the sensor, the results or which, will be your data source. Select *Applications* from the **Select a Category** column and *Installed Applications* from the **Select a Sensor** column. Click on **Select**.  Browse Sensors Select a Category Type here to filter Category All (62 categories) AD Query Active Directory Applications Asset BigFix Browser Client Extension Client Health Client Management Cloud Select a Sensor Type here to filter Sensor IIS Website Details Installed Application Exists (1 parameters) Installed Application Version (1 parameters) Installed Applications Installed Components Installed Pkgs Installed RPMs Installed Store Apps Sensor description List of the applications and versions of those applications installed on the client machine. Example: Mozilla Firefox | 16.0.1 Select Cancel
7.	Your chosen sensor will now be selected. Click on Add Filter.  Select Data Trends questions gather data for all Computer Groups selected in Trends settings. Use these filters to limit the question scope further. Contact your Administrator with any questions. Get the following data Installed Applications Add Filter Browse all Sensors Apply Advanced Sensor Options

8.	Ensure that the column selected in the filter is *Name* and that the condition is set to *Contains*. Enter the word *adobe* in as the value so that it appears similar to that shown below:  **Select Data** Trends questions gather data for all Computer Groups selected in Trends settings. Use these filters to limit the question scope further. Contact your Administrator with any questions. Get the following data Installed Applications Row filter □ Substring □ Apply Name contains ✖ Browse all Sensors Advanced Sensor Options Then click **Apply**. You will now see a preview of the results. Once ready to proceed, click on **Create** to create your new data source.
9.	From the pop-out menu, click on **Boards**. 

10. Click on **New Board**.

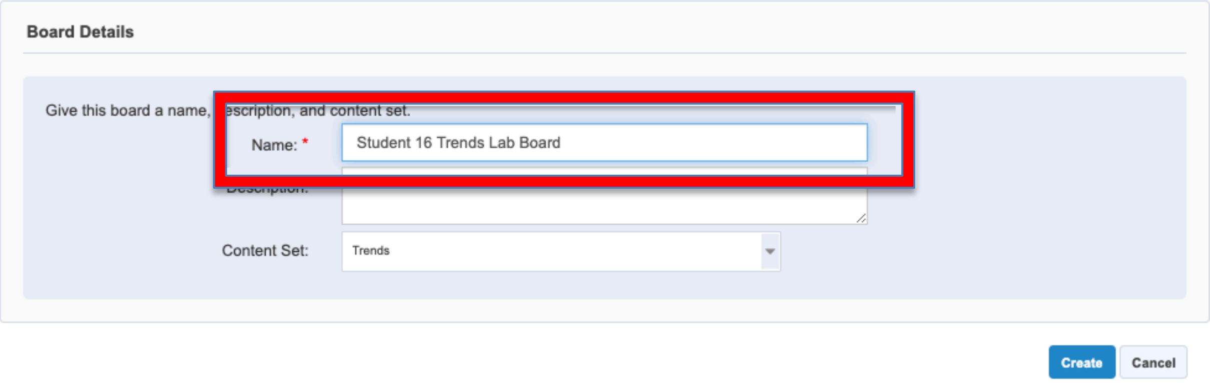

TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Trends
Home
Boards
Sources
Trends
All Boards
New Board
Import
Show: All Favorites
Filter by text
Select All | Select None | View Selected
Expand All | Collapse All

Items: 24

Asset | Sections: 3 | Content Set: Asset
Asset tools status, endpoints, reports, views, and exports

Comply | Sections: 5 | Content Set: Comply
Metrics pertaining to the Comply Module.

Enter *Student <Student ID Number> Trends Lab Board* into the **Name** field. Click on **Create**.



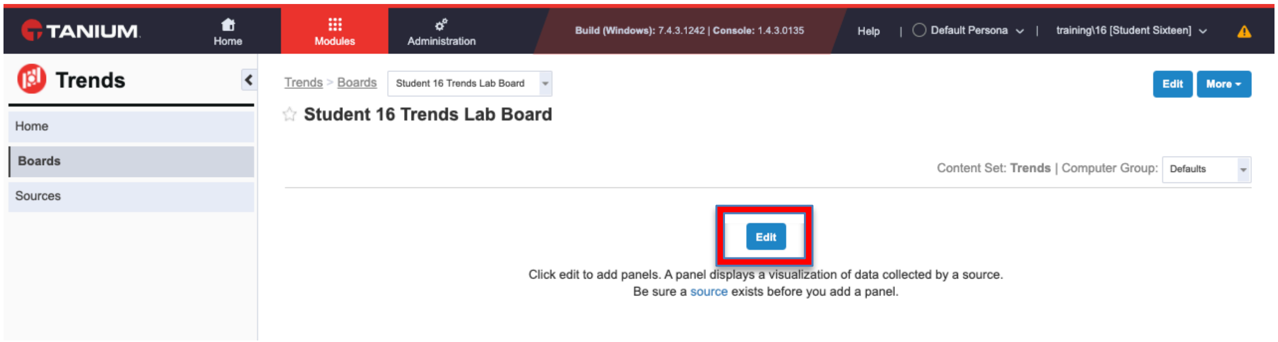
Give this board a name, description, and content set.

Name: * Student 16 Trends Lab Board

Description:

Content Set: Trends

11. You will be returned to the list of Trends boards. Locate your new board and click on it to open it, and then click the **Edit** button.

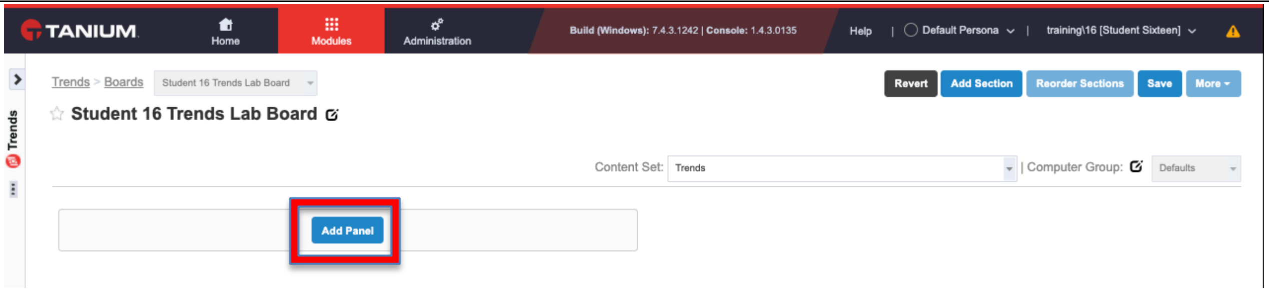

TANIUM
Home
Modules
Administration
Build (Windows): 7.4.3.1242 | Console: 1.4.3.0135
Help
Default Persona
training\16 [Student Sixteen]
Trends
Home
Boards
Sources
Trends > Boards > Student 16 Trends Lab Board
Edit
More
Edit

Student 16 Trends Lab Board

Content Set: Trends | Computer Group: Defaults

Click edit to add panels. A panel displays a visualization of data collected by a source.
Be sure a source exists before you add a panel.

Click on **Add Panel** to allow you to add a panel to your Trends board.

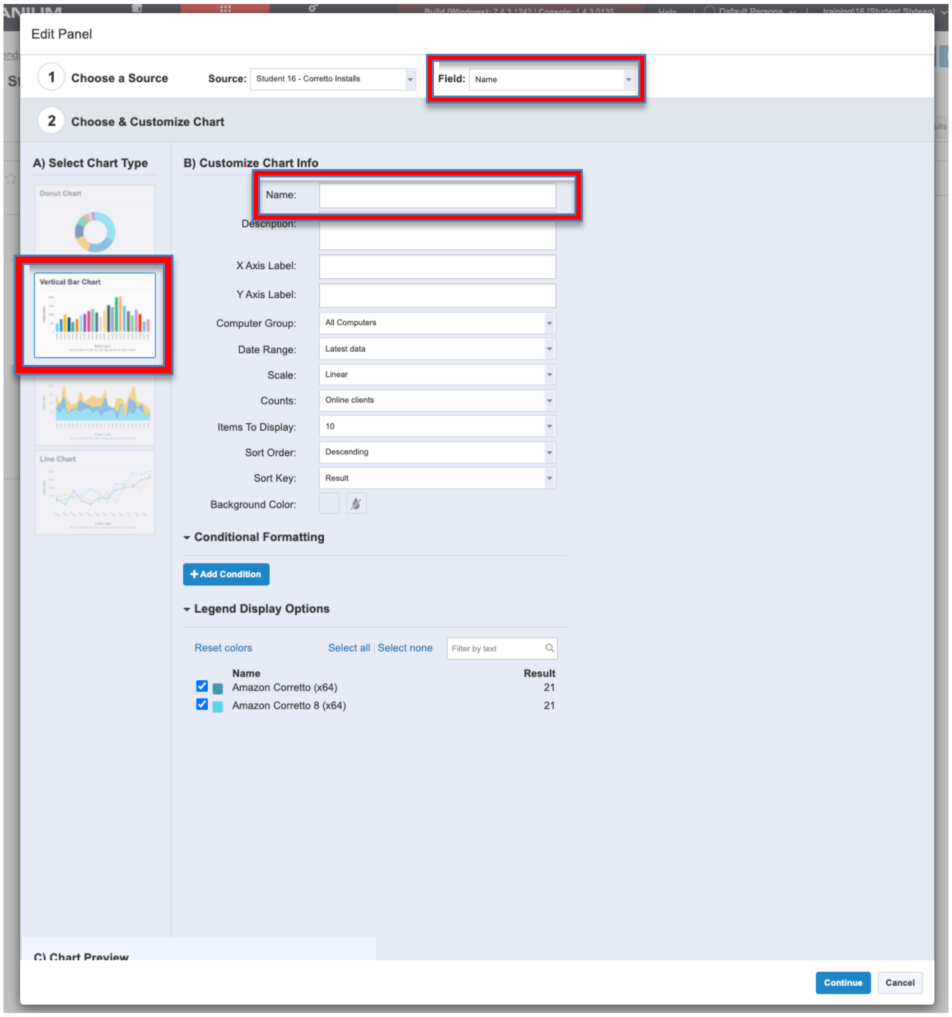


Student 16 Trends Lab Board

Content Set: Trends | Computer Group: Defaults

In the **Source** drop-down, filter using the word *student* to find the data source you created earlier and then select it.

12. Name your chart *Adobe Versions* and then select the *Vertical Bar Chart* under **Select Chart Type**. Investigate the various other options available, especially the ability to select which field of data to visualise but leave settings as default. Once happy with your selection, click on **Continue**.



Edit Panel

1 Choose a Source — Source: Student 16 - Corretto Installs — Field: Name

2 Choose & Customize Chart

Name:
Description:
X Axis Label:
Y Axis Label:
Computer Group: All Computers
Date Range: Latest data
Scale: Linear
Counts: Online clients
Items To Display: 10
Sort Order: Descending
Sort Key: Result
Background Color:

	Name	Result
☑	Amazon Corretto (x64)	21
☑	Amazon Corretto 8 (x64)	21

13. Boards can also be split into multiple sections in order to aid the organisation of panels into related categories or topics. Use the **Add Section** button to create a new section in your board.

Click on **Save** to add the panel and commit the changes to your new board. In the event of the need to regress any unwanted changes, clicking **Revert** will undo any changes back to the boards previously saved state.

14.

Final Challenge

Using everything you have learned so far in this lab, can you create a Trends board which features the following characteristics?

- Named *Student <Student ID Number> Challenge Board*
- A separate section reflecting examples of data from each of the first 10 labs in this course
- **At least** one trends panel per section which relates to each lab you have completed throughout this course. This could be based on existing sources which are already available or new sources which you may have to create from the many sensors available.
- Some suggested data points, relevant to each lab are:
    - Lab 1 –Tanium Client Versions.
    - Lab 2 – Questions / Sensors
    - Lab 3 – Discover Scan Metrics showing the duration of endpoint scans
    - Lab 4 – Successful Tanium Client Management installs over time
    - Lab 5 – Asset SQL Server details
    - Lab 6 – Patch deployment results
    - Lab 7 – Mean time to Deploy
    - Lab 8 – Protect Windows Firewall Rules (by Group)
    - Lab 9 – Performance event category match counts
    - Lab 10 – Map endpoint connections

Once you have completed this lab, log out of the console. You have now completed this lab and also the course; Congratulations!