



# Tanium Console Quickstart Guide

The Tanium Console Quickstart Guide is intended for administrators who wish to learn how to use the Tanium Console. This document assumes you have a Tanium Console account, and that you have a basic understanding of Tanium platform's purpose in enterprise environments. For more information on the Tanium platform, please visit [www.tanium.com](http://www.tanium.com).

## Table of Contents

### [How to Ask Questions](#)

[How to Retrieve a Single Property](#)

[How to Retrieve a Property on a Subset of Machines using a Filter](#)

[How to Get Multiple Properties with a Filter](#)

[How to Get Multiple Properties with Multiple Filters](#)

[How to Use the "Contains", "Starts With", and "Ends With" Filters](#)

[What Properties Can I Ask About and How do I Create a New One?](#)

[Troubleshooting Your Queries](#)

[Other Sample Questions](#)

[How to Export Data from your Questions](#)

### [How to Author New Sensors](#)

[How to See Existing Sensors](#)

[How to Author New Sensors](#)

[How to Use Your New Sensor](#)

[How to Debug Sensors](#)

### [How to Author Actions](#)

[How to Create a Package](#)

[How to Deploy Actions](#)

[How to Debug Actions](#)

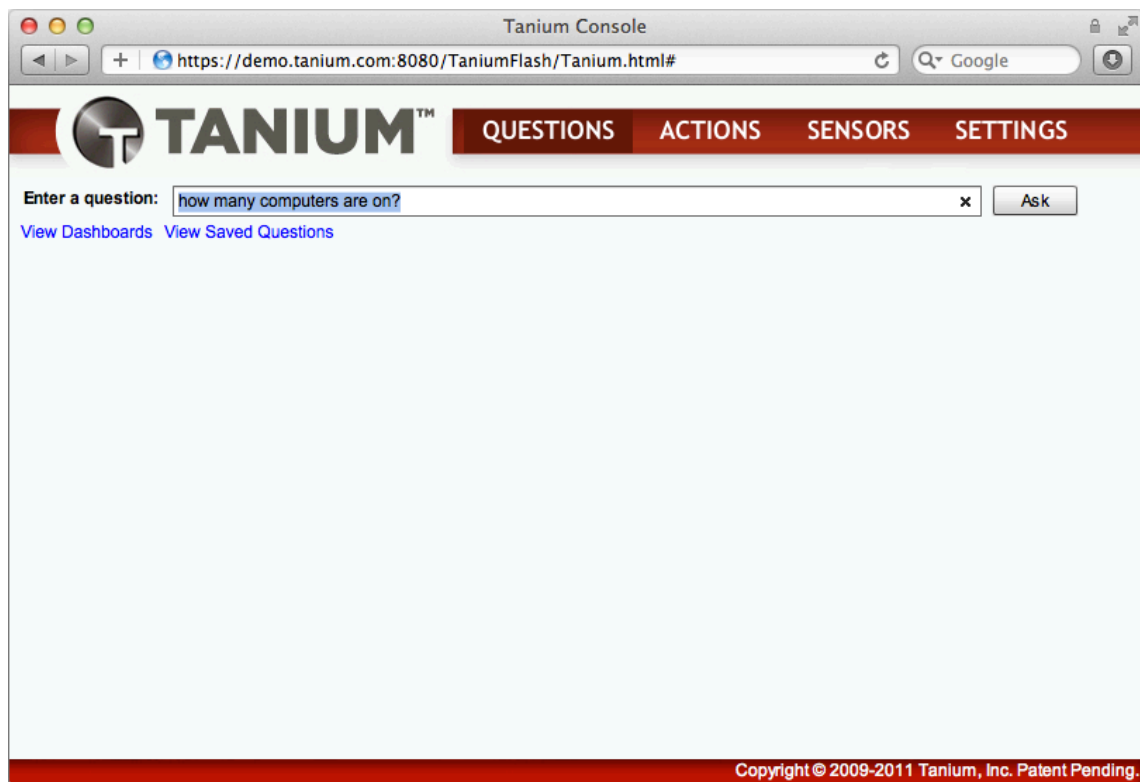
## How to Ask Questions

Tanium is built around a simple question-and-answer interface, which allows you to gather data about the state of the computers in your network. To ask a question, simply click on the Questions tab, and type a question in to the text box. Let's show you a few examples to give you an idea of how its done.

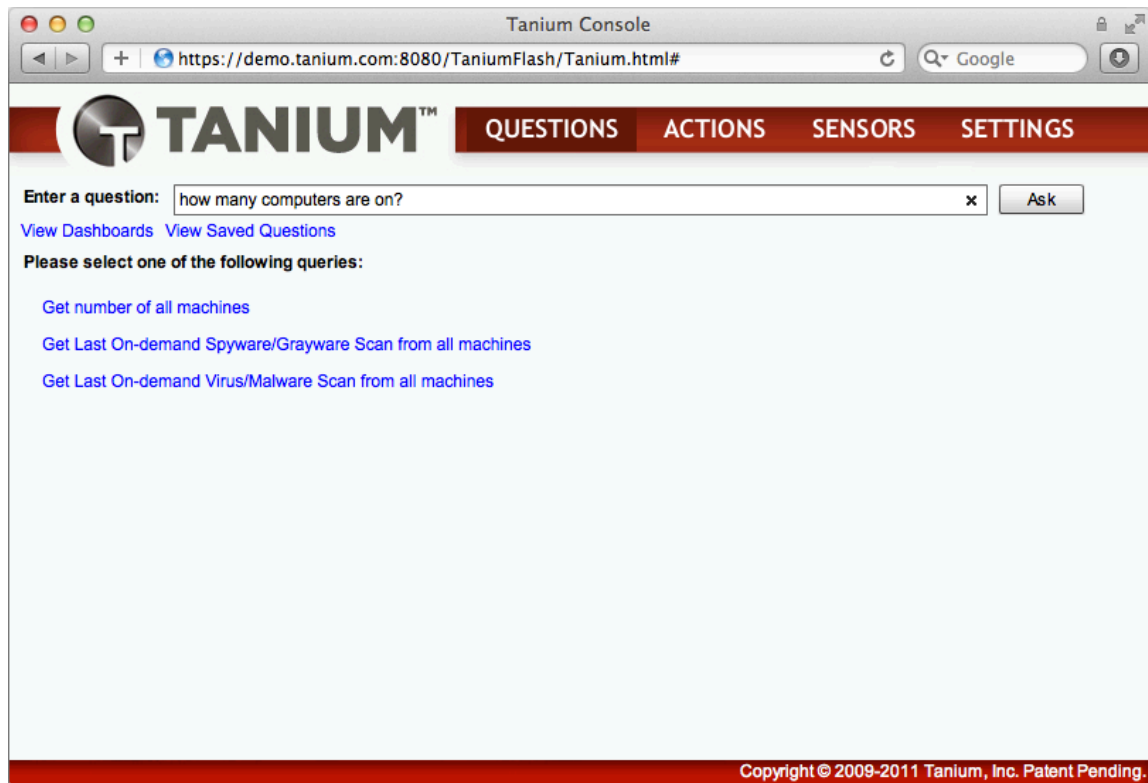
### How to Retrieve a Single Property

The simplest question you can ask in Tanium retrieves a single property that you're interested in from all computers in the network. For example, let's say you wanted to know how many computers are on. To ask that question, type in:

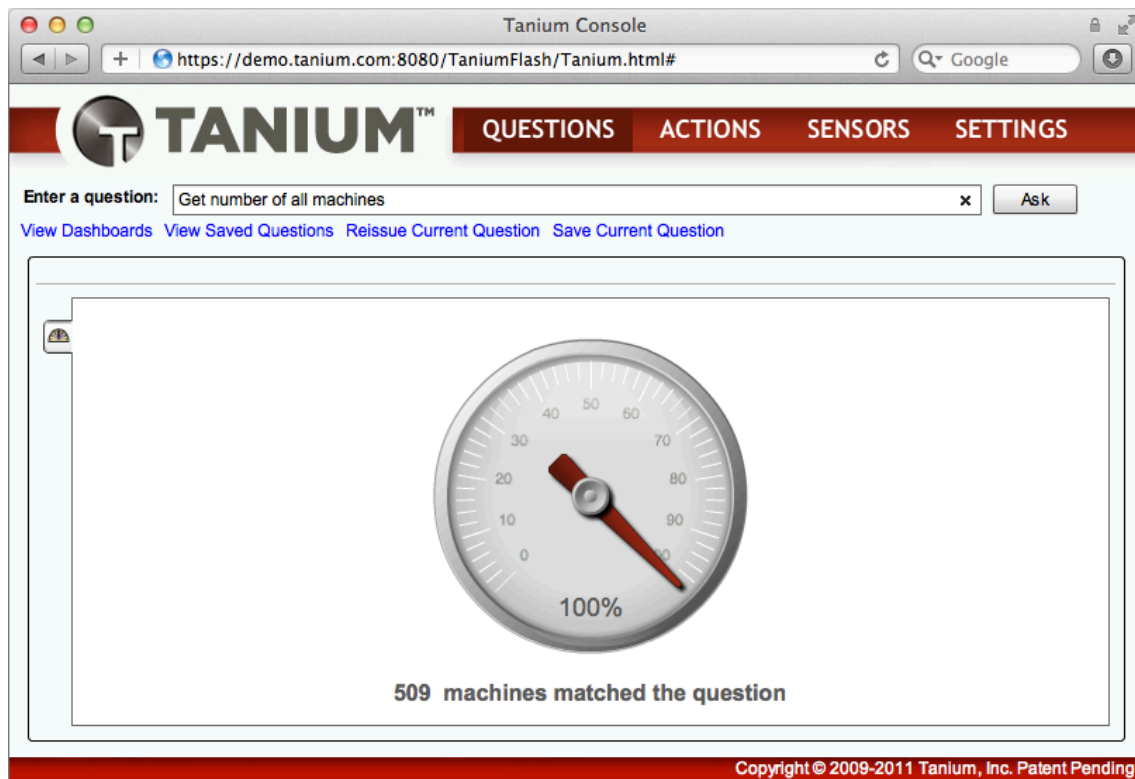
[how many computers are on?](#)



Once you've typed in the question, hit the "Ask" button. That results in a screen that will look like:



When you hit the "Ask" button, Tanium parsed your question to determine what questions that it can answer are most similar to what you were asking. In this case, Tanium only recognizes a few questions that are similar to what you are asking, and presents it to you to in a list. Click the top link, "Get number of all machines", which will present you with a screen similar to this:

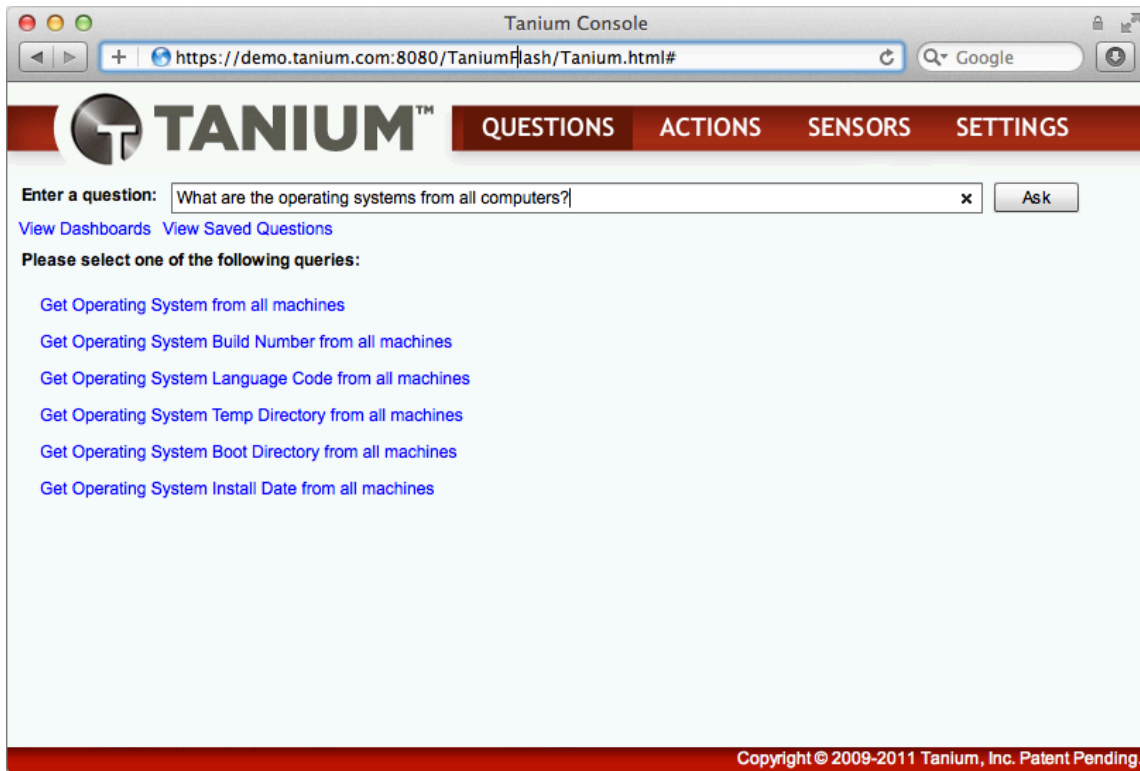


When you ask Tanium for a number, it provides you with a percentage meter that indicates what portion of the machines fit the question. Since we asked for all machines, we see 100%, but if we asked another "number of" question that is filtered (more on that later), it would come back with something less than 100%. Also, note that the above question indicated that there were 509 machines that matched our question, because we have 509 machines that are currently on at the time that the question was asked.

Let's take a look at other questions we can ask. Perhaps you'd like to know not just how many computers are on right now, but also what operating systems they are running. In the question interface, you type in:

[What are the Operating Systems on all computers?](#)

After you hit the Ask button or Enter key, you'll see a screen like:



Again, Tanium presents a number of suggestions that look like the question you asked. It turns out that in this instance the first suggestion is the question you're interested in.

Hitting the first link will show you something like:

The screenshot shows the Tanium Console interface. At the top, there is a navigation bar with the Tanium logo and four tabs: QUESTIONS, ACTIONS, SENSORS, and SETTINGS. Below the navigation bar, there is a search bar with the text "Enter a question:" and a dropdown menu containing "Get Operating System from all machines". To the right of the search bar is an "Ask" button. Below the search bar, there are four links: "View Dashboards", "View Saved Questions", "Reissue Current Question", and "Save Current Question".

The main content area displays a table with the following data:

Operating System	Count
Windows 7 Professional	416
Windows XP Professional	93
Windows Server 2008 R2 Standard	1

At the bottom of the table, there are three links: "Select All", "Copy", and "Export". To the right of the table, it says "3 items". At the bottom of the console, there is a copyright notice: "Copyright © 2009-2011 Tanium, Inc. Patent Pending."

We can see that the results, as well as the counts associated with them, are displayed.

## How to Retrieve a Property on a Subset of Machines using a Filter

The examples given above show you how to get a single property from all computers in the network. However, a common requirement is that you get a piece of data from only computers that meet certain criteria, such as those running a particular application, in a particular region or with a user logged in. You can do that in Tanium by using the separator "of computers" in the question. For example, perhaps you want to know the MAC addresses of only the computers that are currently running Firefox in the environment. If so, you type in:

[What are the mac addresses of computers running firefox.exe?](#)

Note that this question splits into three parts.

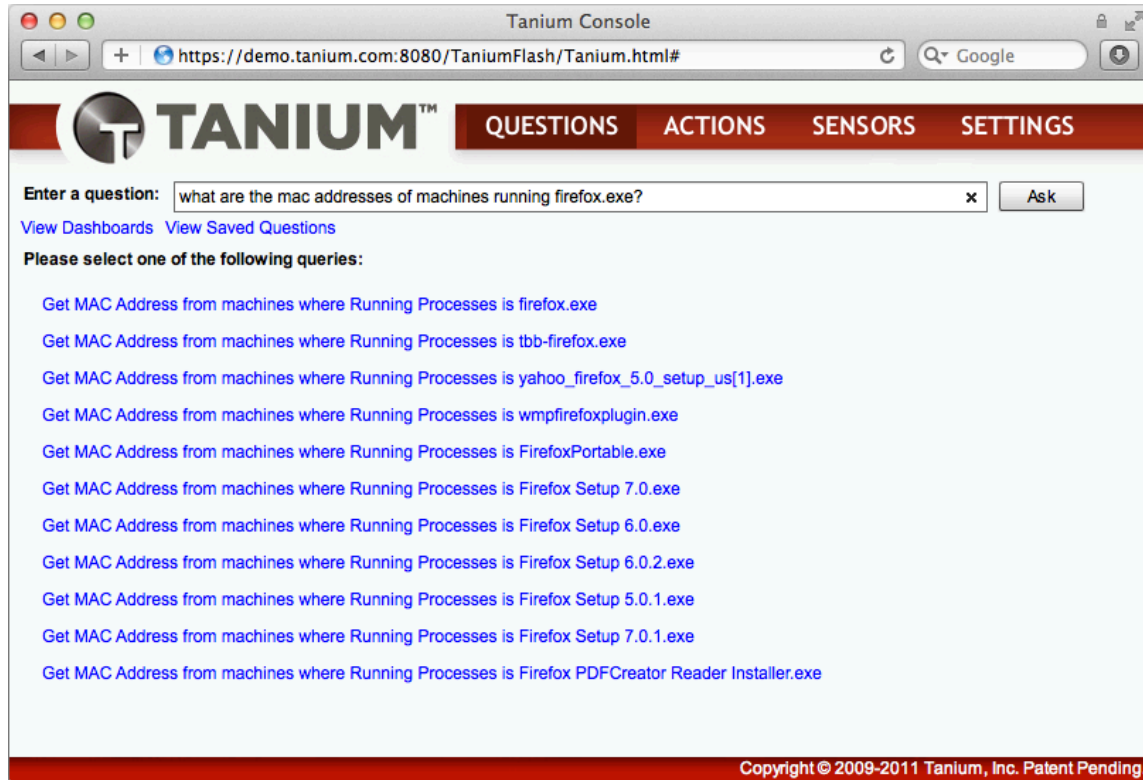
The first part, "[What are the mac addresses](#)", is the *Select*. That describes to Tanium the information you want it to retrieve for you.

The second part, "[of computers](#)", is the *Separator*. The separator allows Tanium to determine where the selects end and the rest of the question begins. There are a number of other separators that Tanium recognizes, such as "on computers where", "on machines that", and so on.

The third part, "[running firefox.exe](#)", is the *Filter*. The filter tells Tanium which computers should answer the question.

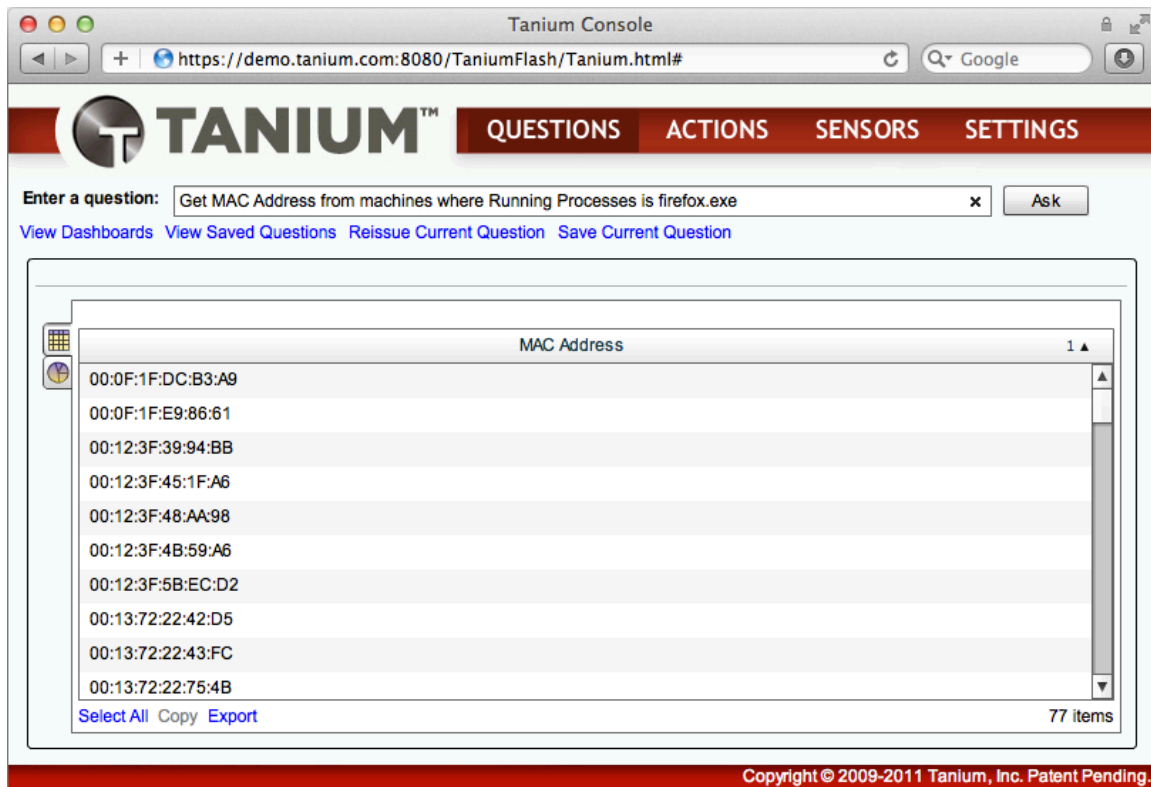
With the question in the box, you hit the "Ask" button.

As you've seen before, Tanium uses its parser to interpret the question and presents to you only queries that it knows how to ask and which questions look as close as possible to the question you typed in. So in this case, Tanium will present a list of questions similar to the ones below:



Note that Tanium's parser knows which characteristics are present in your network and presents the ones that make the most sense based on the question you're asking. You'll notice that the first option "Get MAC Address from machines where Running Processes is firefox.exe" is indeed what you're looking for. You'll also notice that the parser knew that you meant "Running Processes" when you said "running". In fact, aside from the separator that was described above, there aren't rules on how you write questions which means you can start using Tanium without learning a bunch of exact syntax first.

So to get your answers, you click the link of the question you meant to ask. Tanium will communicate the question to the computers in the network that you have management rights on, and retrieve the answers. You can watch the progress spinner in the upper right hand corner that indicates what % of machines have responded. Generally within seconds, you'll have a page that looks like:



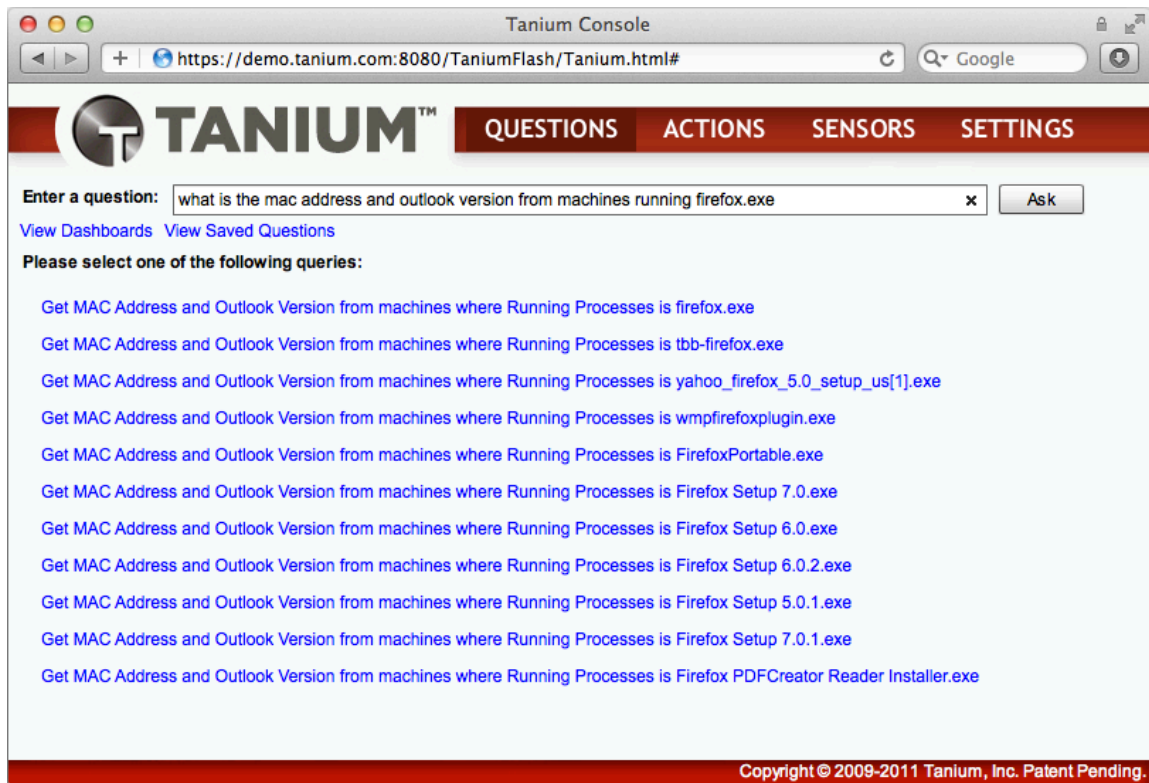
## How to Get Multiple Properties with a Filter

Tanium can easily be instructed to return multiple properties from each computer answering instead of just a single property. For example, let's say that you didn't just want to know the MAC addresses from each computer answering, but instead you wanted to know both the MAC addresses and the Outlook version in the same answer set. Just add the second property to the *Select* using an "and" between the first and second property you want to retrieve:

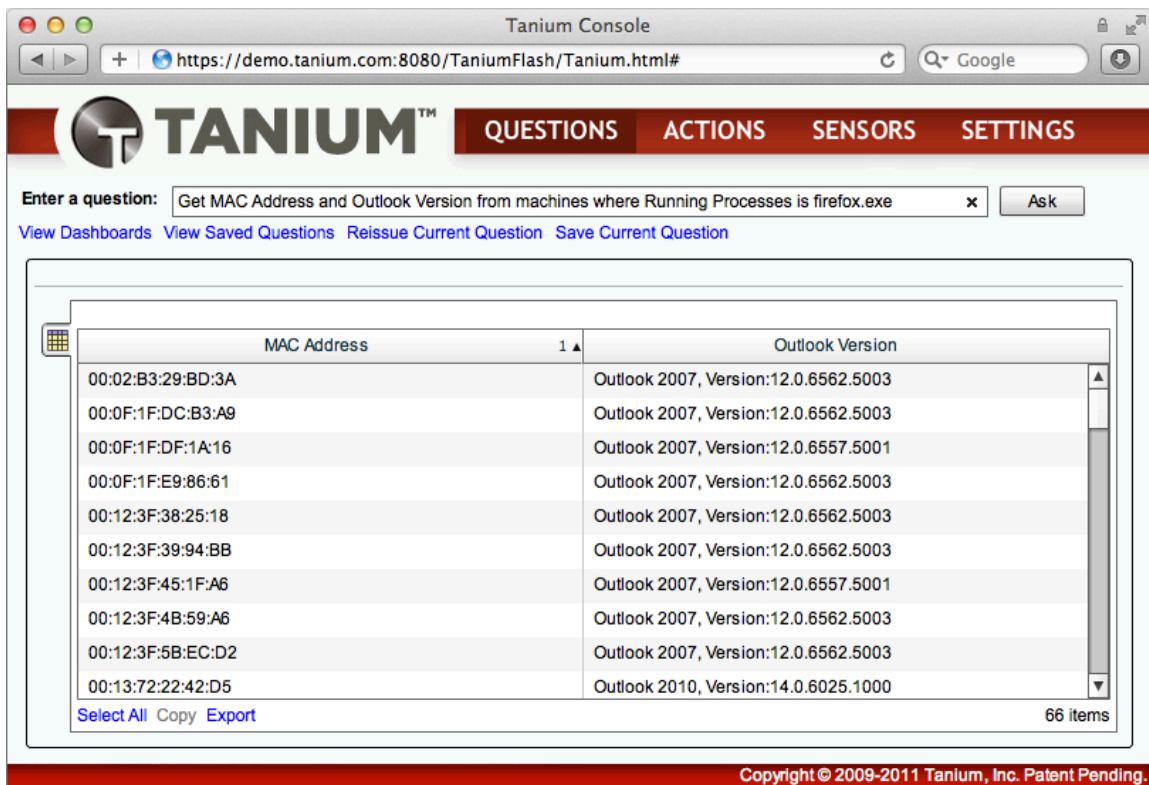
[What is the mac address and outlook version from machines running firefox.exe](#)

You'll note that I added an "and" after "mac address" and then named the second property I wanted to retrieve before the separator "[from computers that](#)".

Clicking the Ask button will give you:



Hit the top link, and you'll get a list like:



You can ask for more than two properties as well. Just add another "and" and name the next

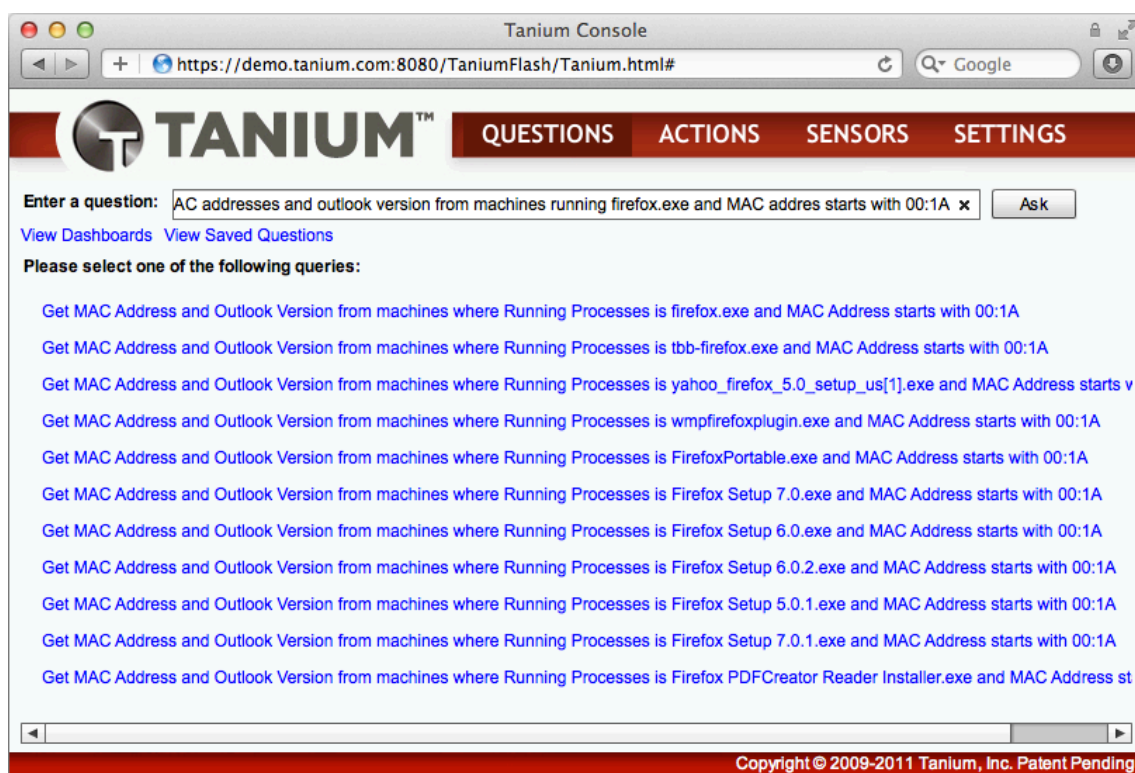
property you want, all before the separator. Each piece of information you ask for (such as MAC Address and Outlook Version in the example above) will simply show up as another column of data.

## How to Get Multiple Properties with Multiple Filters

You can use "and" and "or" to extend the Filter as well to change which computers are asked for answers. For example, if you wanted to know the mac addresses and outlook versions of computers that are running firefox.exe **and** mac address starts with 00:1A, you could type in:

MAC addresses and outlook version from machines running firefox.exe and MAC address starts with 00:1A

which gives us:



You can notice in the above example that MAC Address was misspelled with only 1 's'. The Tanium parser is still smart enough to overcome most spelling mistakes.

The top option results in:

The screenshot shows the Tanium Console interface. At the top, there's a navigation bar with 'TANIMUM' logo and tabs for 'QUESTIONS', 'ACTIONS', 'SENSORS', and 'SETTINGS'. Below the navigation bar, there's a search bar with the text 'Enter a question: Get MAC Address and Outlook Version from machines where Running Processes is firefox.exe and MA x'. Below the search bar, there are links for 'View Dashboards', 'View Saved Questions', 'Reissue Current Question', and 'Save Current Question'. The main content area displays a table with two columns: 'MAC Address' and 'Outlook Version'. The table contains 16 rows of data. The MAC addresses all start with '00:1A:A0'. The Outlook versions are either 'Outlook 2007, Version:12.0.6562.5003' or 'Outlook 2010, Version:14.0.4760.1000'. At the bottom of the table, there are links for 'Select All', 'Copy', and 'Export', and a count of '16 items'. A copyright notice 'Copyright © 2009-2011 Tanium, Inc. Patent Pending.' is visible at the bottom of the interface.

MAC Address	Outlook Version
00:1A:A0:A4:AD:8B	Outlook 2007, Version:12.0.6562.5003
00:1A:A0:A5:91:78	Outlook 2010, Version:14.0.4760.1000
00:1A:A0:A6:60:4F	Outlook 2010, Version:14.0.6025.1000
00:1A:A0:A6:65:59	Outlook 2007, Version:12.0.6562.5003
00:1A:A0:A6:68:B9	Outlook 2010, Version:14.0.4760.1000
00:1A:A0:A6:6E:8E	Outlook 2010, Version:14.0.4760.1000
00:1A:A0:A8:6F:A7	Outlook 2010, Version:14.0.6025.1000
00:1A:A0:A8:98:DB	Outlook 2010, Version:14.0.6025.1000
00:1A:A0:A8:A3:56	Outlook 2007, Version:12.0.6562.5003
00:1A:A0:A8:A4:BB	Outlook 2007, Version:12.0.6562.5003

Here you can notice that the MAC addresses only start with "00:1A".

## How to Use the "Contains", "Starts With", and "Ends With" Filters

Tanium's parser gives you the flexibility to do string comparisons as well as the equality checks we've seen so far. To do that, you can use comparisons like "starts with", "contains", and "ends with" in the filter expressions, which give you a lot of flexibility in your questions. Some examples include:

- [number of computers with ip addresses that contain 192](#)
- [What is the current CPU utilization of the computers with an installed hotfix that contains KB929399](#)

You can also use those comparisons to narrow down the results in the select. For example:

- [What are the application event log entries that contain Exception on computers in the Americas region](#)
- [What are the running services that start with SQL on computers with names that do not contain SQL](#)

Try out a few combinations to get the hang of it.

## What Properties Can I Ask About and How do I Create a New One?

The properties you can ask about are what Tanium calls "Sensors". To learn more about Sensors and how to author new ones, take a look at the "[Sensor Authoring](#)" section of this document.

## Troubleshooting Your Queries

There are only a few rules in Tanium's parser. The first rule is that the thing you want to collect, e.g. the "computer names" in the question "[what are the computer names on computers in the Finance OU and running excel](#)", must come first in the question. If you are trying to ask questions with the order reversed (e.g. "on the computers running excel, tell me the computer names"), you might want to try reversing that.

Second, Tanium's parser requires that the things you're asking for, such as the "computer name" in the example above, be separated from the rest of the question by something like "on computers that" or "where" or "from computers which". So while the question "bios versions video card contains Nvidia" won't work well, "[bios versions of computers with a video card that contains Nvidia](#)" will.

Third, if you have something that you're looking for that contains multiple words, e.g. "Microsoft Office", putting it in quotes will help the parser know that you mean to have those words considered together. For example:

[What are the computer names of computers with installed applications that contain "Microsoft Office"](#)

Finally, if you aren't getting the result you want, try to be more specific about the data you're asking for. "[mac addresses of computers with xp](#)" might not get you what you want, but "[mac addresses of computers running the operating system Windows XP](#)" almost certainly will.

## Other Sample Questions

Here are a few examples of some questions that customers of ours have found very useful:

- [What are the Running Applications on computers that have a running service name containing SQL](#)
- [What are the computer names and users on computers where a network accessed drive is \\EMAIL\IPC\\$](#)
- [What are the operating systems of computers that have an "HP LaserJet 4000" printer installed](#)
- [What are the ip addresses and mac addresses of computers where symantec viruses found contains sasfis](#)
- [What are the time zone settings for computers in the "New York" Region](#)
- [What are the stopped services on the computer with the computer name QX394B](#)
- [What are the computer names and user names of computers that have USB Storage Devices attached and have a "Patient Data" Security Level](#)
- [What are the BIOS Release Dates and BIOS versions from computers that are the Model](#)

## "Optiplex 745"

Note that a few of the questions above have Sensors that have been defined by those customers to suit their particular environment such as the "Regions" of computers, or their "Data Security Level" that you would need to have defined in your environment appropriately for those questions to work for you as well.

### **How to Export Data from your Questions**

There are three ways to get the data out of Tanium:

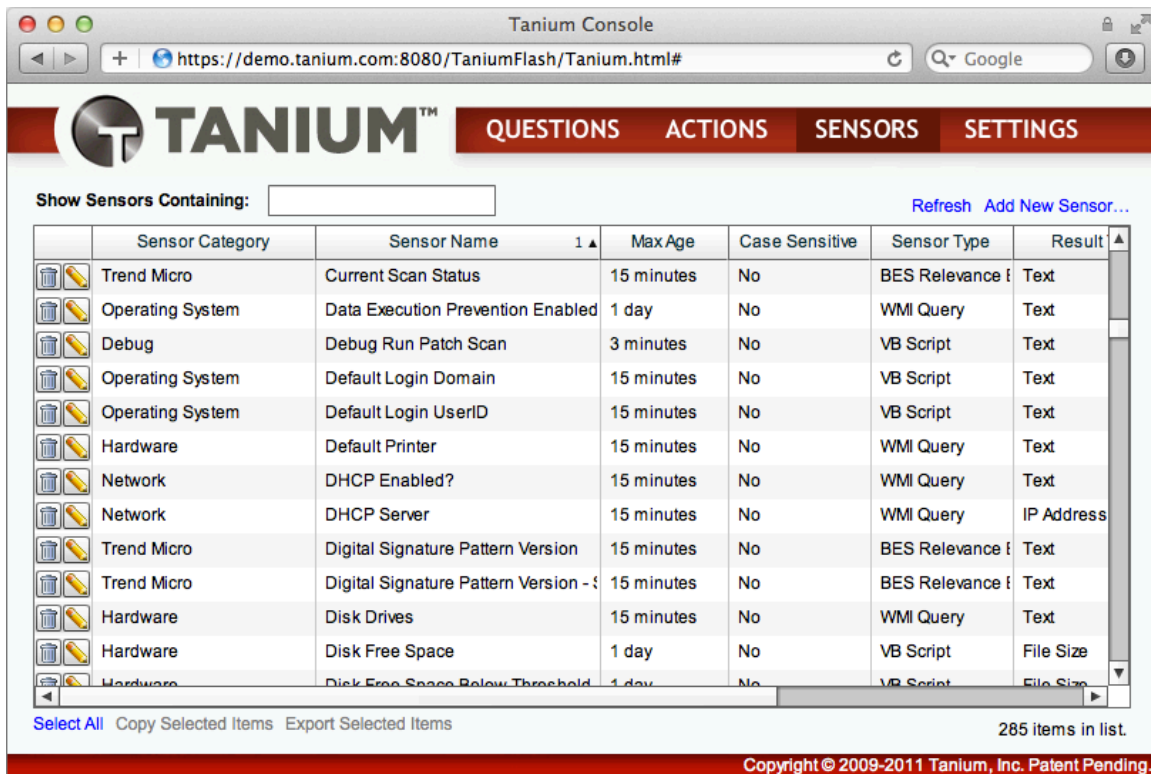
1. You can copy and paste answers out of the UI by selecting the ones you want and hitting the Copy link below any list.
2. You can highlight the rows of data you want and Export them to a comma delimited file that is readable in Microsoft Excel and other spreadsheet applications.
3. There are a number of APIs on the Tanium Server that allow for data to be extracted in SOAP format for consumption by other processes. Ask your organization's Tanium contact for more details.

## How to Author New Sensors

Tanium recognizes the "nouns" in your questions based on the Sensors that are defined in the environment. Tanium ships with hundreds of Sensors that allow it to identify the state of the hardware, software, and network of the computers in the enterprise.

## How to See Existing Sensors

To see which Sensors are currently defined, click the Sensors tab at the top of the Console:



	Sensor Category	Sensor Name	Max Age	Case Sensitive	Sensor Type	Result
	Trend Micro	Current Scan Status	15 minutes	No	BES Relevance	Text
	Operating System	Data Execution Prevention Enabled	1 day	No	WMI Query	Text
	Debug	Debug Run Patch Scan	3 minutes	No	VB Script	Text
	Operating System	Default Login Domain	15 minutes	No	VB Script	Text
	Operating System	Default Login UserID	15 minutes	No	VB Script	Text
	Hardware	Default Printer	15 minutes	No	WMI Query	Text
	Network	DHCP Enabled?	15 minutes	No	WMI Query	Text
	Network	DHCP Server	15 minutes	No	WMI Query	IP Address
	Trend Micro	Digital Signature Pattern Version	15 minutes	No	BES Relevance	Text
	Trend Micro	Digital Signature Pattern Version - S	15 minutes	No	BES Relevance	Text
	Hardware	Disk Drives	15 minutes	No	WMI Query	Text
	Hardware	Disk Free Space	1 day	No	VB Script	File Size
	Hardware	Disk Free Space Below Threshold	1 day	No	VB Script	File Size

Note that you will need Sensor Read and/or Sensor Write privileges on your Tanium account to view and edit Sensors on the Sensors tab.

## How to Author New Sensors

In addition to the Sensors Tanium ships with, Sensor Authors in your environment can dynamically add Sensors to monitor properties on the computers in your network. New Sensors can be defined in a variety of languages, including WMI, VBScript, Powershell, BigFix Relevance, Shell Script, or a number of other interpreters that are resident on the computers you wish to monitor. For example, this allows you to extend Tanium to use VBScript to parse the contents of an internally developed log file and return specific results from it within seconds, or alternatively to monitor particular performance counters through WMI and return a real time view of that counter from particular machines across the

environment.

To add a new Sensor, simply click the "Add New Sensor..." link on the Sensors tab. You'll be presented with a number of fields to enter:

The screenshot shows the "Add New Sensor" dialog box. The "Sensor Name" field contains "New Sensor". The "Sensor Category" field contains "Miscellaneous". The "Sensor Type" dropdown menu is open, showing options: "WMI Query", "BES Relevance Expression" (highlighted), "VB Script", "PowerShell Script", and "Unix Shell". The "Results Type" dropdown menu is also open. The "Query/Expression" text area contains the text "if true then "Yes" else "No"". Below the text area is a section for "Advanced Options" with a right-pointing arrow. At the bottom, there is a section for "When answering questions, ensure results are newer than:" with a value of "15" and a unit of "Minutes". There are two checkboxes: "Ignore case in result values" (checked) and "Exclude result values when parsing questions" (unchecked). An "OK" button is located at the bottom center.

First, you'll need to Name your sensor, and provide a Category for the Sensor. Next, you'll want to select the scripting interface that the Sensor will use to execute on the Tanium Clients. The Sensor Type drop-down in your environment may only contain a subset of the scripting types that are listed above, and in fact there are a number of other options, such as Perl or Python, which can be accessed by extending the Tanium platform if those interpreters are commonly deployed on your Tanium Clients - in those cases, your Tanium support contact can provide scripting connectors to allow you to access other interpreters as desired. Note as well that you can simply "frame" any script within another script for execution - for example, by using VBScript to write out Javascript, and calling the appropriate interpreter from VBScript.

Once you've selected the scripting language that you wish to use, enter the script in the Query/Expression section. Note that in some scripting types, you will need to follow a convention to specify what results are returned for the Sensor when it is executed. The Tanium Client will return standard output for each Sensor Type. For example, in VBScript, any results that are returned using the "Wscript.Echo" VBScript command will be shown as Sensor results:

**Add New Sensor**

Sensor Name:  Sensor Type:

Sensor Category:  Results Type:

Query/Expression:

Advanced Options

When answering questions, ensure results are newer than:

Ignore case in result values

Exclude result values when parsing questions

OK

For other Sensor Types, you will need to output the results that you would like to retrieve to standard out. For instance, if you are using the “UNIX Shell” type, a simple “echo test” would output the word “test”.

Finally, in the field marked "When answering questions, ensure results are newer than:", select the amount of time that answers should be maintained before re-evaluating the Sensor. This effectively sets the maximum "age" of the answers that you can see in the Console when asking a new question. If you have a Sensor that is retrieving a very time critical piece of data you may want to set this very aggressively - for example, if you are concerned that a worm is spreading through your environment, you might want to set this to 1 minute, whereas if you are trying to check a very static piece of data such as the number of drives on your computers, you may be willing to set this to 1 hour or even longer.

Once you hit the OK button to save the Sensor, the Sensor will be automatically propagated out to all Clients in the environment.

## How to Use Your New Sensor

To view the results of a Sensor you've defined, go to the Questions tab, and ask a question about it. For example, if you define a Sensor named "My Echo Test", you can ask a question like "My Echo Test from all machines" to test your sensor:

The screenshot shows the Tanium Console interface. At the top, there is a navigation bar with the Tanium logo and four tabs: QUESTIONS, ACTIONS, SENSORS, and SETTINGS. Below the navigation bar, there is a search bar with the text "Enter a question:" and a text input field containing "Get My Echo Test from all machines". To the right of the input field is a small "x" icon and an "Ask" button. Below the search bar, there are four links: "View Dashboards", "View Saved Questions", "Reissue Current Question", and "Save Current Question".

The main content area displays a table with the following data:

My Echo Test	Count
Hello world!	472

At the bottom of the table, there are three links: "Select All", "Copy", and "Export". In the bottom right corner of the table area, it says "1 item". At the very bottom of the page, there is a red footer bar with the text "Copyright © 2009-2011 Tanium, Inc. Patent Pending."

## How to Debug Sensors

When developing Sensors, the best way to ensure that they work is to first test locally on one of the machines that you will be deploying to. For instance, if you are developing a VBScript-based sensor, you should test it with "cscript my-new-sensor.vbs" at a Command Line in Windows, where the Sensor script is in the file "my-new-sensors.vbs". If it doesn't work locally, it will not work in the Tanium environment.

If you continue to have difficulty getting your Sensors to output expected results, you may want to enable "Error Results" so you can see any problems that are coming back from interpreting your Sensor. Go to Settings -> Preferences, and make sure the "Hide Error Results from Saved Questions" checkbox is unchecked. If there are any programmatic errors with your Sensor definition, they may show up once you reissue the question (whether they show depends on the Sensor Type and how errors are interpreted).

## How to Author Actions

Once Tanium is used to find machines that are suffering from an issue or require a change, the system can be quickly used to make changes on those computers using the Tanium Actions capabilities. Actions require that a Package be defined by a Console user with Action Write privileges. The Package is associated with a Saved Question, and at that point it is available to be executed by Console Users with Action execution privileges in Tanium.

### How to Create a Package

To begin Package definition, go to the Actions->Packages tab, and click "Add New Package". A Package requires you to enter a few parameters. First, you'll need to name the Package. The Command should be entered exactly as you would enter it into the command line if you were executing the action on the local computer. So, for example, if you wished to kill the Firefox application, you could use the command "taskkill", with the appropriate command line arguments, just as you would from the Windows command line:

#### **taskkill /F /IM firefox.exe**

If the command that you wish to execute requires files (e.g. a patch or Antivirus update), you will want to attach those files to the action. Files may either be specified through a URL, or from the local filesystem. The command will be run with all attached files in its same path - as such, if you wanted to run a VBScript in the Package, for example, you could attach the file "test.vbs" to the Package, and for the command, place something like:

#### **cscript test.vbs**

The screenshot shows the 'Add New Package' dialog box. It contains the following fields and controls:

- Package Name:** My Test Package
- Command:** cscript test.vbs
- Command Timeout After:** 1 Minutes
- Files:** A list containing 'test.vbs'. Below the list, there are input fields for 'File Name' (test.vbs), 'SHA-256', and 'Size' (130.00bytes (130 bytes)).
- Buttons:** 'Add Local Files...', 'Add URL', 'OK', and 'Cancel'.
- Source Sensors:**  Require specific sensors

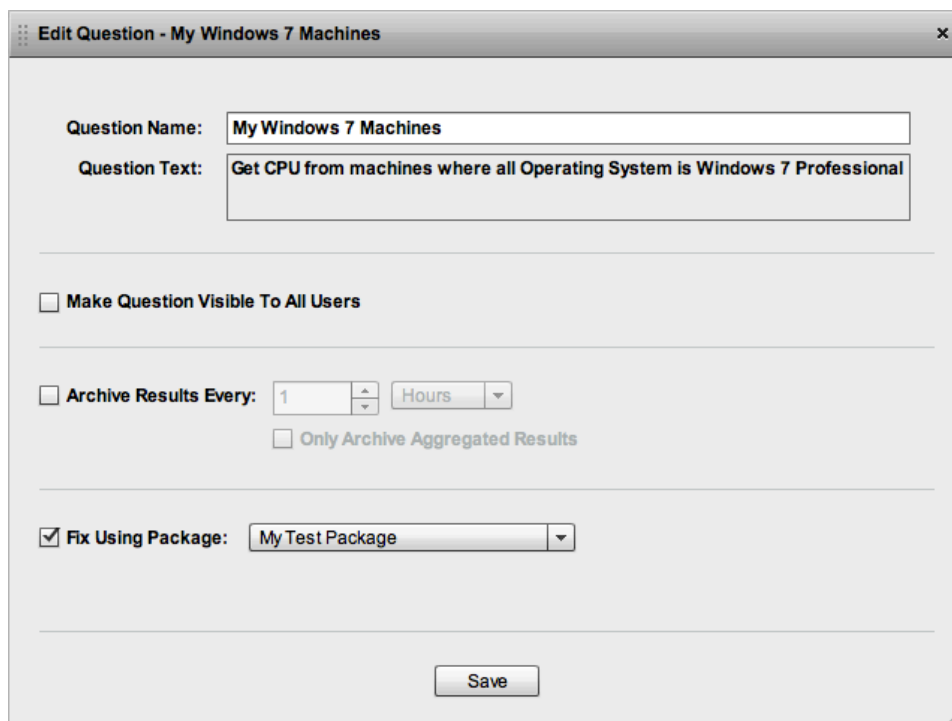
Similarly, MSIs, executables, and entire folder contents can be attached and called with the appropriate

command line arguments.

If you wish to be very secure, you can specify a pre-calculated SHA256 hash for the files that you are uploading to Tanium for distribution. If you do not specify a SHA256, one will be calculated automatically by the Console, and all Clients will check that SHA256 hash before they accept the file for execution.

## How to Deploy Actions

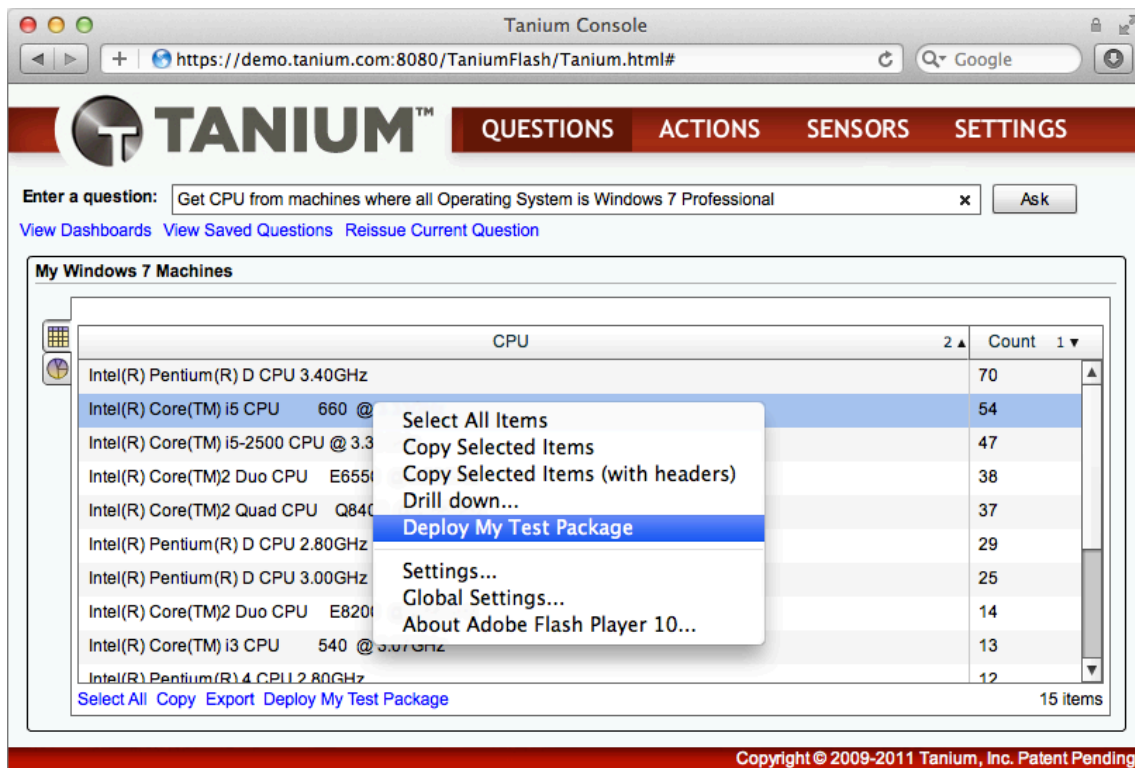
Once you have a Package specified, you can associate it with a Saved Question by editing the Saved Question definition, and checking the "Fix using Package" checkbox, with the appropriate Package selected in the dropdown:



The screenshot shows a dialog box titled "Edit Question - My Windows 7 Machines". It contains the following fields and options:

- Question Name:** My Windows 7 Machines
- Question Text:** Get CPU from machines where all Operating System is Windows 7 Professional
- Make Question Visible To All Users
- Archive Results Every: 1 Hours
- Only Archive Aggregated Results
- Fix Using Package: My Test Package
- Save** button

At that point, any Console users with Action execution privileges will be able to see a context menu option and link at the bottom of the Saved Question, allowing them to execute the Package against any set of computers that respond to the Saved Question:



## How to Debug Actions

To debug actions, it is often effective to copy all of the expected files to a folder on the computer, open a command prompt on the computer with administrative privileges, and run the Command as specified in the Package. At that point, you can interactively review the failure that is occurring. You can also browse to a Tanium Client that executed the action, and open the "Tanium Client\Downloads\Action\_xxx" file in the filesystem, which contains the log that the Tanium client generated for the Action. Note that xxx will correspond with the Action ID, which can be found in the Actions->Action History tab.