3D Tool 2.0 Quick Start Guide

ABOUT THE 3D TOOL

Tenable's 3D Tool is a Windows application that is used to query data from a SecurityCenter 4 server and present it in an interactive visual console to facilitate presentations and security analysis.

Tenable developed the 3D Tool to help communicate different types of information available in SecurityCenter, such as:

- Nessus vulnerability data
- Network topologies
- PVS data, including passively discovered vulnerabilities and new network devices
- Event data discovered and normalized by the Log Correlation Engine (LCE), including intrusion detection, firewall, netflow and syslog data

Many people are "visual learners", preferring to use images, colors and charts to organize information and communicate with others. The 3D Tool provides a mechanism to communicate technical data in visual terms that are easier to understand than written text.

Using three dimensions to visualize network topology is easier than using two dimensions. Most Tenable customers have routing networks that are sufficiently complex enough to clutter any 2D topology map. Using 3D provides a visual display of the network topology and events that is easier to understand and navigate interactively.

The 3D Tool can be applied in a number of different ways depending on the requirements. The typical application is to install it on a desktop in a network that can access the SecurityCenter so the data can be updated. However, once the data is loaded on the 3D Tool desktop, it no longer needs this connectivity. This enables managers and technical staff to examine security data from remote locations.

The 3D Tool is available to all SecurityCenter customers and can be obtained from the Tenable Support Portal. For more information, please refer to the following blog entry or contact Tenable Support.

The 3D Tool is available for all major Windows releases and works on most hardware platforms, although increased memory and multi-CPU configurations will greatly improve performance.

INSTALLING THE 3D TOOL

1. Download the setup executable from the Tenable Support Portal located at: https://support.tenablesecurity.com/support-center/. Confirm the integrity of the installation package by comparing the download md5 checksum with the one listed in the product release notes.
2. Run the installation program, named similar to 3D_Tool_2_x_x_x32.exe.
3. Click "Next" when prompted to install the Tenable 3D Tool v2 on your computer and click on "Install" to begin the installation. The executable will launch the installer, prompt for an installation location and create a "Tenable Network Security" program

group that contains a link to the "3D Tool" application. No manual configuration is performed during the installation process.

4. Once installation is complete, the 3D Tool can be launched via a desktop shortcut or from the "Tenable Network Security" start menu.

CONFIGURING THE 3D TOOL

CONFIGURE SECURITYCENTER QUERIES

Before launching the 3D Tool, one or more custom queries that are used by the 3D Tool must be created on the SecurityCenter to create one or more topologies. The queries can be based on either vulnerability or event data and **must be based on either the "Detailed Vulnerability List" tool for vulnerability data or "List of Events" tool for event data or they will not display in the 3D Tool query dropdown**.

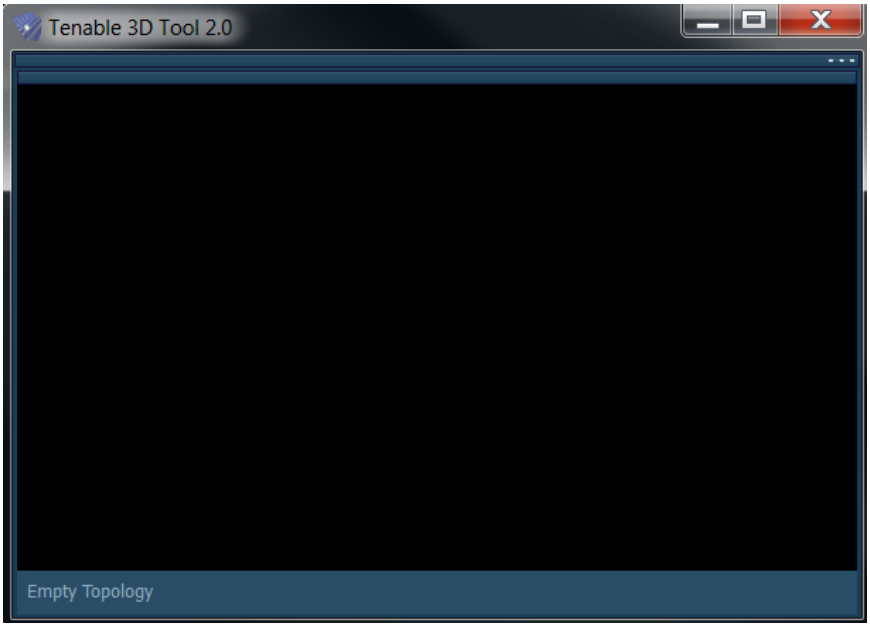
The query type must be "Vulnerability", the analysis tool must be "Detailed Vulnerability List", and there must be results from plugin 10287 (Traceroute).

CONFIGURE A NEW TOPOLOGY

Use the steps below to create and configure a new topology view:

1. Launch the 3D Tool interface by double-clicking on the desktop or start menu icon. Once launched, a screen similar to the one below is displayed. The top two configuration panes will automatically hide when not in use and can be displayed by clicking in the 3D Tool window towards the top of the visible area.

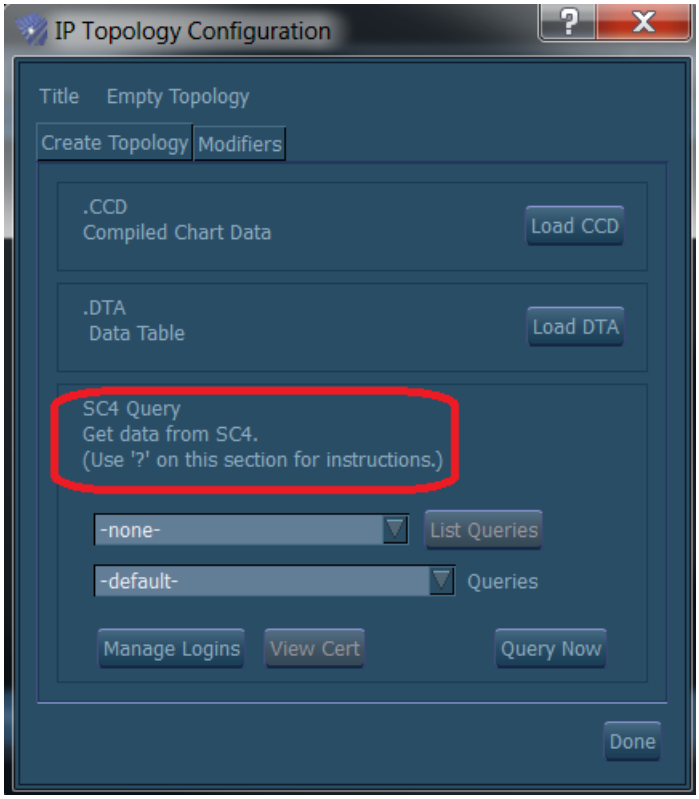
The lower configuration pane contains several elements that can be used to assist with the configuration process. To the right of the configuration gear icon are two icons that determine whether the interface is displayed vertically or horizontally. Choose the display accordingly.



If a layout was previously created, click the arrow icon next to the save icon in the upper pane and choose the layout to use. Otherwise, click the gear icon to start the configuration process.

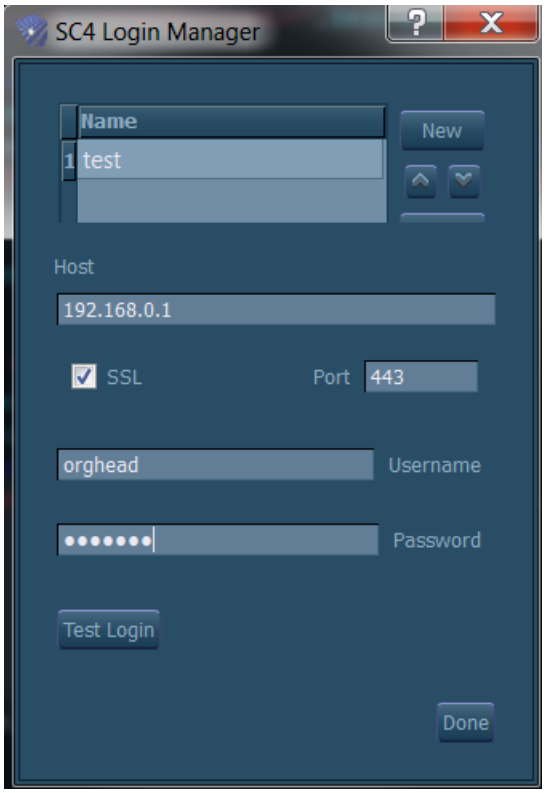
2. Name the topology in the "Title" section as desired.

3. On first use,select the SC4 Query section to enter a SecurityCenter login and to gather data.



4. Click the **Manage Logins** command button to enter a SC4 login that will be used to retrieve data. Complete all required fields similar to the screen capture below:

A default login named "Default Login" will already exist. Double-click the name field to create your own login.



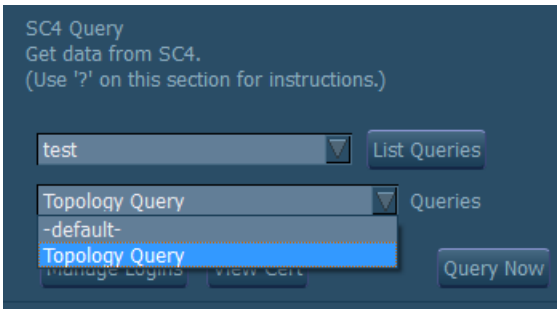
After clicking on "Test Login" for the first time, a certificate warning is displayed. Assuming you trust the remote host, click through the warning to perform the login.

5. Once the test login has been successfully performed, click "Done" to continue. The new login is now listed in the login dropdown box. If at any point you wish to view the certificate of the remote host after performing the first query, click "**View Cert**" to display the certificate of the remote host.

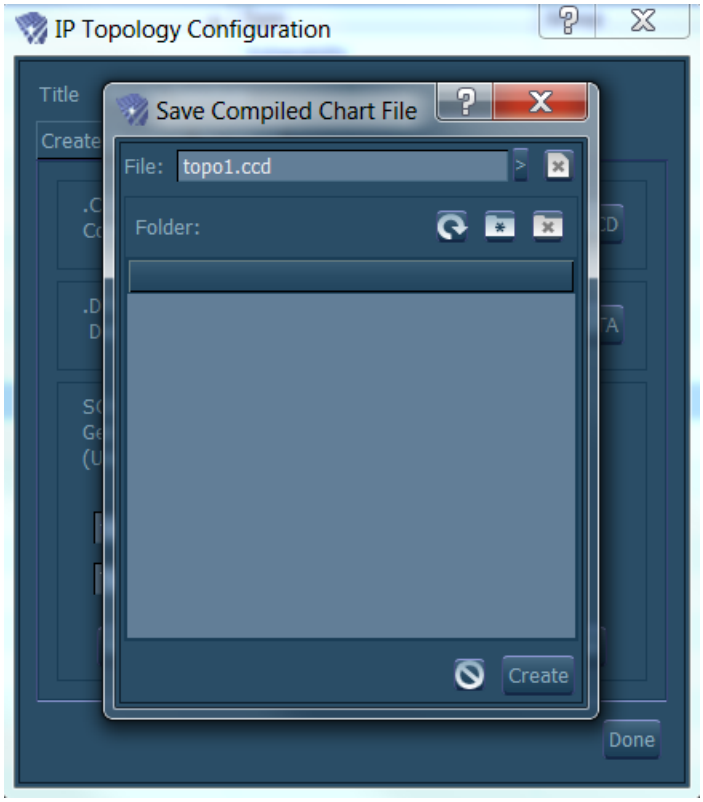
6. Click "**List Queries**" to retrieve a list of available queries from the remote SecurityCenter. The 3D Tool will now log into the SecurityCenter and retrieve a list of available queries.

The query type must be "Vunerability", the analysis tool must be "Detailed Vulnerability List", and there must be results from plugin 10287 (Traceroute).

7. Once completed, the "Queries" dropdown will appear similar to the following:

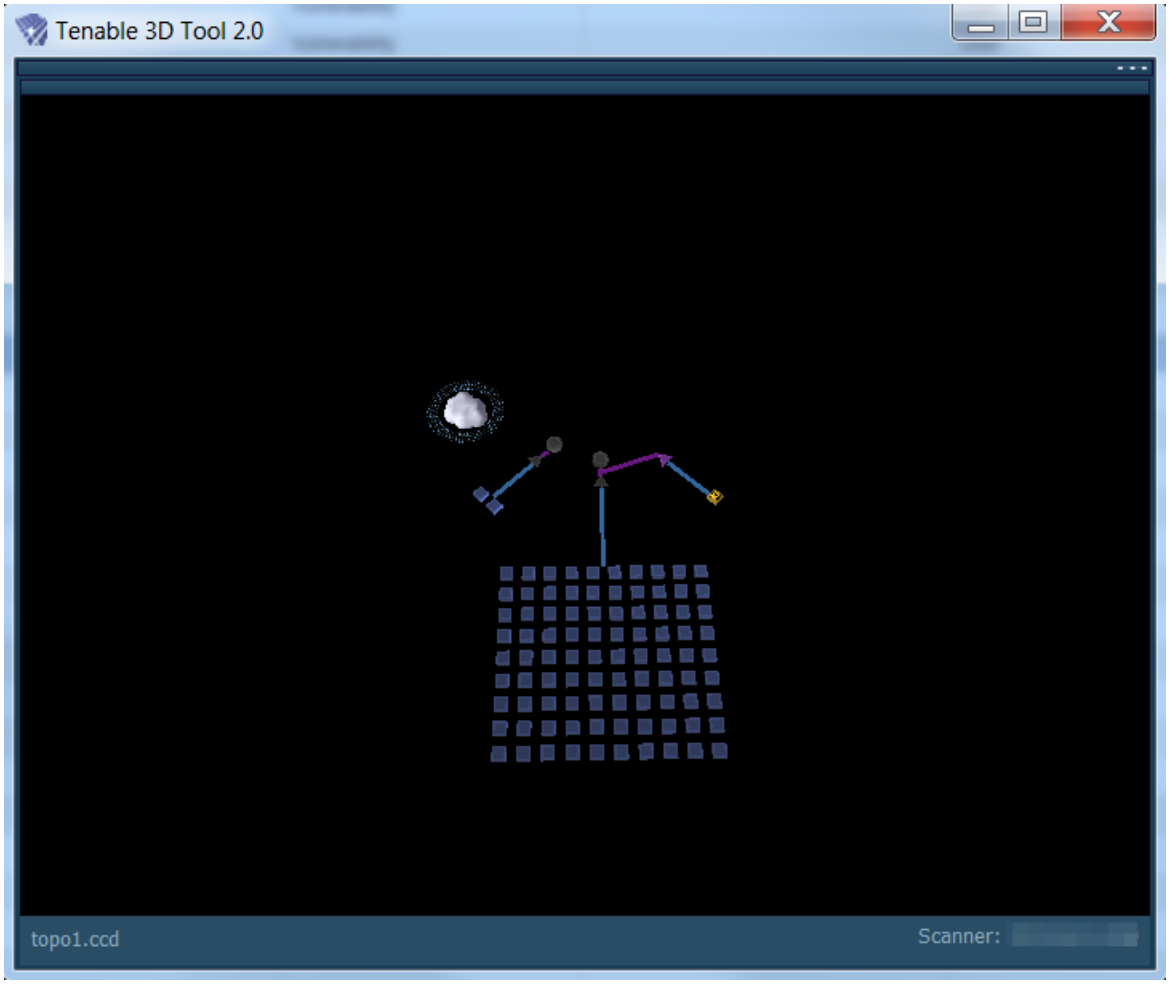


Select the desired query and then click "**Query Now**" to continue. At this point you will be prompted to save a "Compiled Chart File". Enter the desired name for this file that is saved for later reuse and then click "**Create**".



Depending on the number of available records, this process can take a long time to complete.

8. Allow the records to complete processing and populate your new topology. Depending on the number of records, this process can take anywhere from several minutes to over an hour. Allow adequate time for this process to complete. After the data has been retrieved, the topology screen is automatically populated, similar to the screen capture below:



9. Use your mouse's right/left buttons and scroll button to move or rotate the display as desired. In addition, the keyboard arrow buttons can be used to adjust the display.

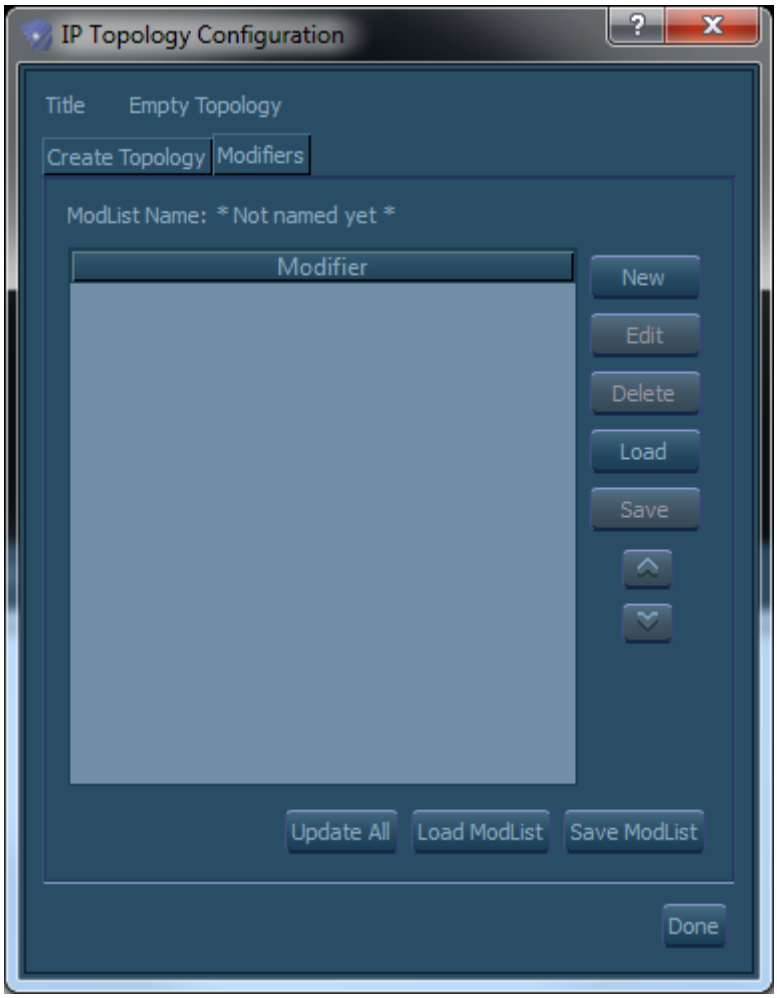
Load a Saved Topology

Click the radio button titled "Load one of these already compiled data sets." and use the dropdown to select the compiled data set. Then click "**Done**" to continue.

Adding a New Modifier

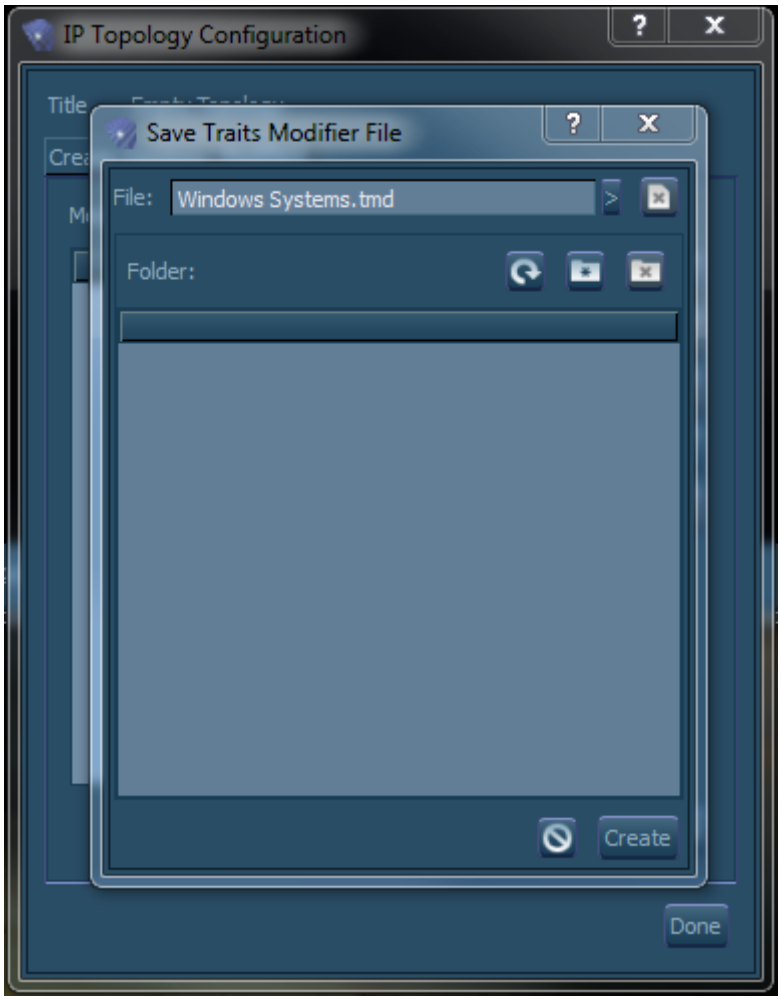
Modifiers are options that can be applied to specialize or modify the topology display based on your unique needs. **Host**, **connection** and **count** display attributes can be modified using this tool. Use the steps below to add a modifier.

1. Click the "Modifiers" button at the top of the topology configuration screen below the title bar. A screen similar to the one below is displayed:



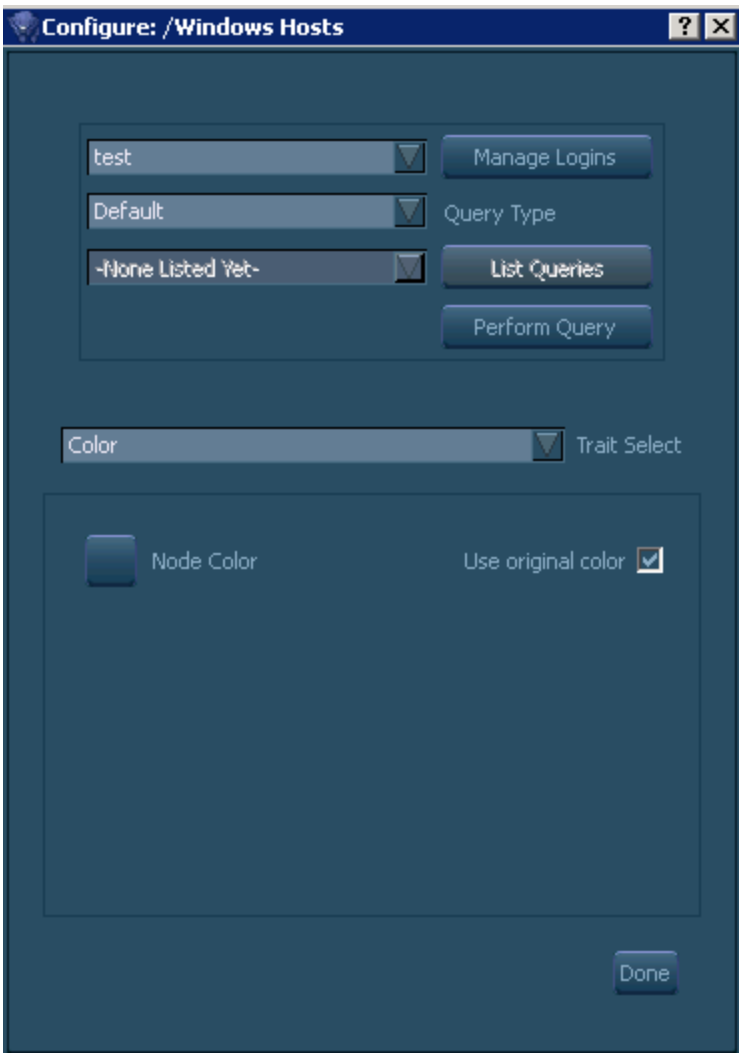
2. Click "**New**" to add a new modifier.There are three available modifier types: "**Node Traits List**", "**Connections List**" and "**Counts List**". The "Node Traits List" modifier allows you to adjust host attributes such as color, shape, icon and vertical offset. The "Connections List" modifier visually displays connections using lines of varying height and source/destination color for contrast. The "Counts List" modifier displays counts of vulnerability and/or events per host with a vertical bar.

   After selecting the desired modifier type, you are prompted to save a file that will contain the modifier definitions. Enter the desired name of this file and then click "**Create**":



3. Highlight the modifier in the list and click "Edit" and then "Configure" to add attributes.

4. A screen similar to the following is displayed:

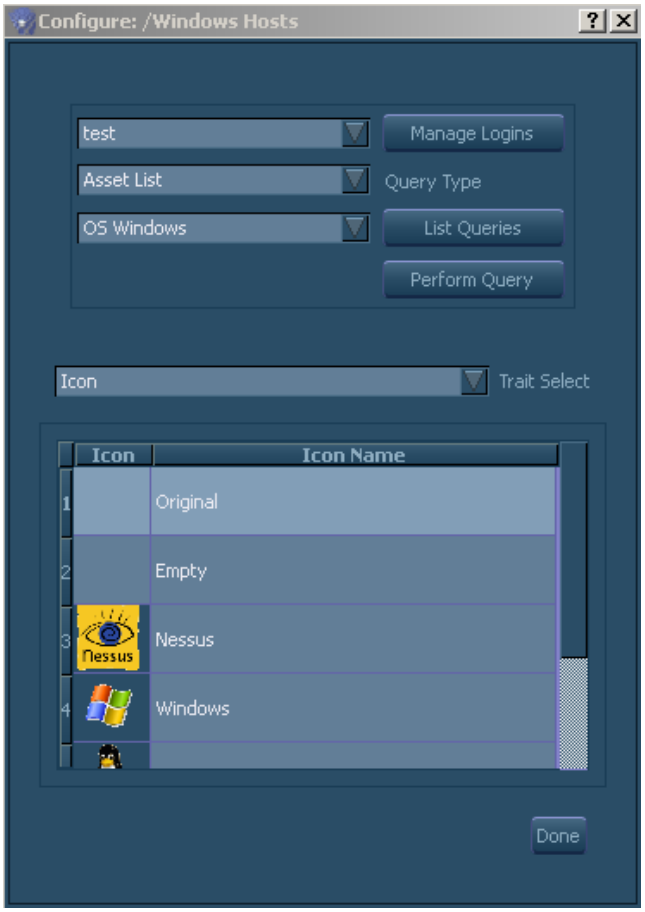


5. Use the login created during the initial topology creation.

6. Under "Query Type" choose "Asset List".

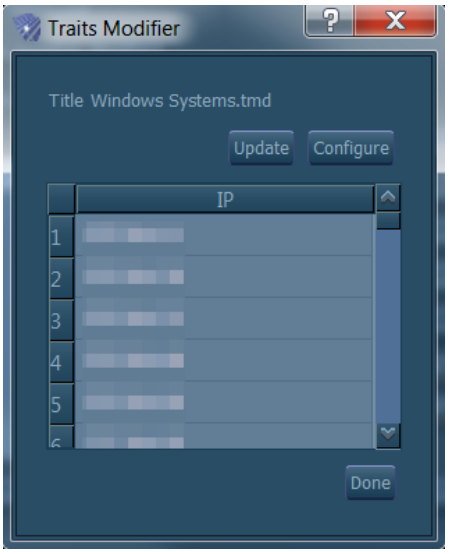
7. Choose "**List Queries**" and then select the desired query. In our case, the query name was "OS Windows". Then click "**Perform Query**" to pull the assets that match this query on the remote SecurityCenter. After clicking "Perform Query", you will be prompted to choose from a repository on the remote host that contains the desired host data. Either select "Use all repositories", or individually select the desired repository.

8. For "Trait Select" choose "Icon" and then choose the default Windows icon.

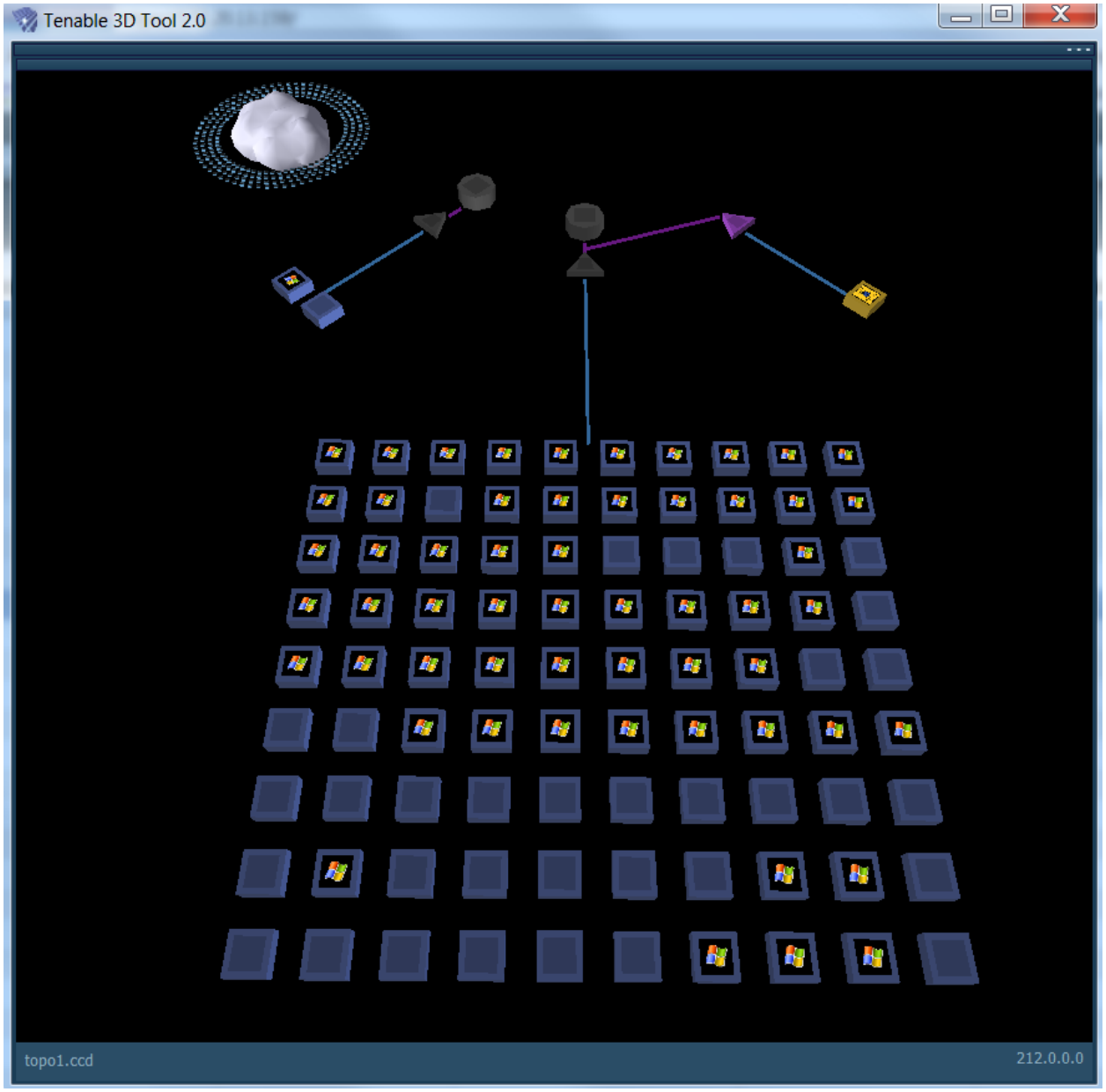


9. Click "**Done**" and a list of affected hosts is displayed.

In addition to the display list, existing modifier lists can be updated by clicking on "Update" as shown in the screen capture below.



10. Click "**Done**".



This is just a small sampling of what the Tenable 3D Tool v2 is capable of accomplishing. For a more information about this tool, please refer to the 3D Tool User Guide.

ABOUT TENABLE NETWORK SECURITY

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.

Tenable Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com