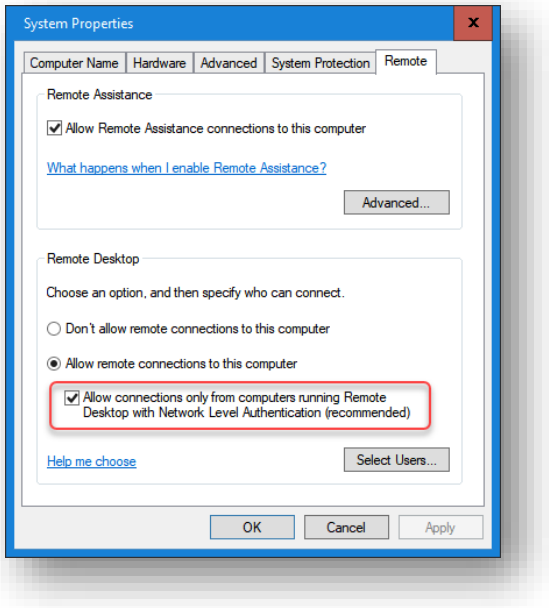
# NETWORK LEVEL AUTHENTICATION STATUS

This agent procedure gets the status of the Windows Network Level Authentication (NLA) setting then documents the result in a Custom Field so you can see its status, report on it, and even create views. This pack consists of five Agent Procedures and this document has two additional sections to show you how to create two Views, and a Report.




Network Level Authentication (NLA) is a feature of Remote Desktop Services (RDP Server) or Remote Desktop Connection (RDP Client) that requires the connecting user to authenticate themselves before a session is established with the server. It is important for organizations to enable network-level authentication (NLA), which will block attackers lacking authentication credentials connecting to RDP.

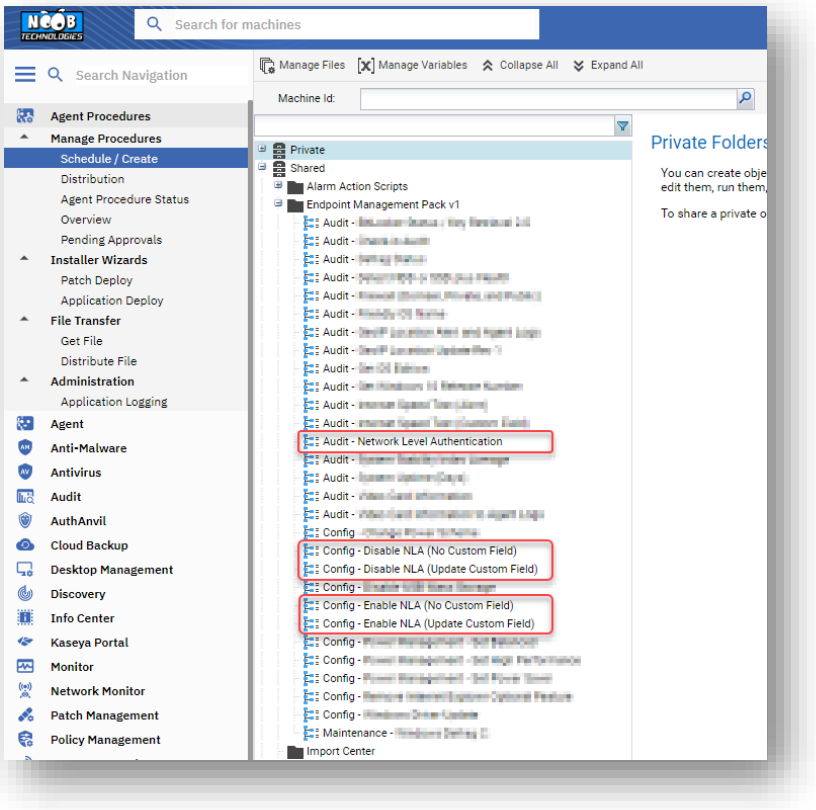
Originally, if a user opened an RDP (remote desktop) session to a server it would load the login screen from the server for the user. This would use up resources on the server and was a potential area for denial of service attacks as well as remote code execution attacks (see BlueKeep). Network Level Authentication delegates the user's credentials from the client through a client-side Security Support Provider and prompts the user to authenticate before establishing a session on the server.

If you have Remote Desktop Protocol (RDP) listening on the internet, Microsoft also strongly encourages you to move the RDP listener behind some type of second factor authentication, such as VPN, SSL Tunnel, or RDP gateway. A solution such as Kaseya's AuthAnvil can also help secure your environment.

# THE AGENT PROCEDURES

This pack consists of the five Agent Procedures listed below:

1. **Audit – Network Level Authentication** – This gets the status and documents the result to a custom field.
2. **Config – Disable NLA (Update Custom Field)** – This disables NLA and changes the custom field status to Disabled.
3. **Config – Disable NLA (No Custom Field)** – This only disables NLA on a Windows Endpoint and doesn't update a custom field. This was created in case if you just want to disable and are not going to use a custom field.
4. **Config – Enable NLA (Update Custom Field)** – This enables NLA and changes the custom field status to Enabled.
5. **Config – Enable NLA (No Custom Field)** – This only enables NLA on a Windows Endpoint and doesn't update a custom field. This was created in case if you just want to disable and are not going to use a custom field.



## IMPORTING THE AGENT PROCEDURES

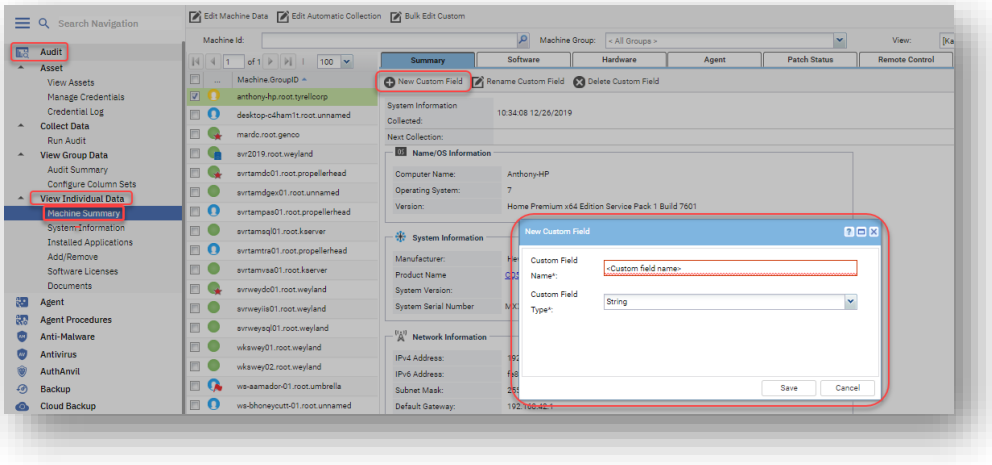
Before importing the XML files, you should create one custom field of type String named as follows:

**Network_Level_Authentication**

You can create Custom Fields in the Audit module by going to:

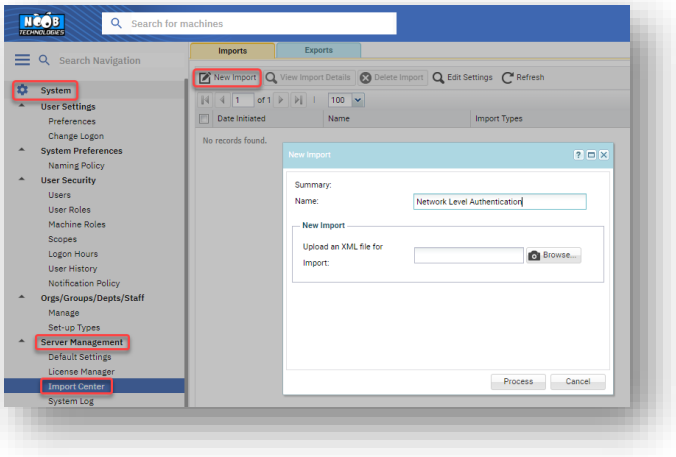
***VSA > Audit > View Individual Data > Machine Summary***

Select any endpoint then click on New Custom Field as seen in the screenshot below.

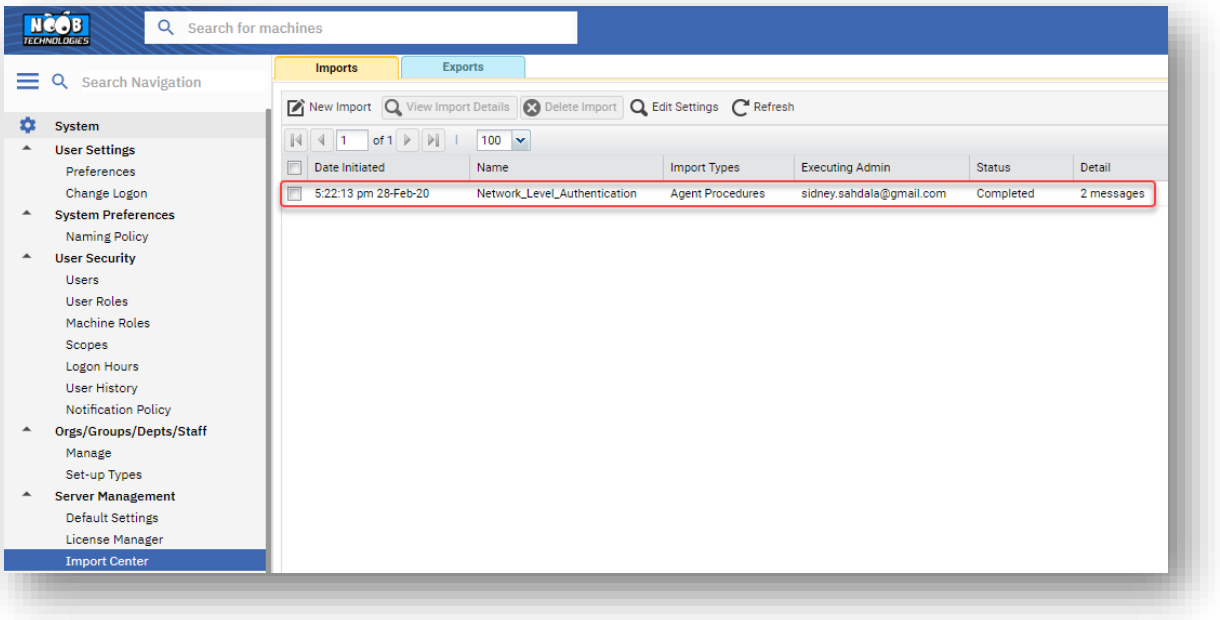



Next, import the XML file. Because we are importing multiple Agent Procedures in one XML file, we will need to use the import center to import the Agent Procedures by going to:

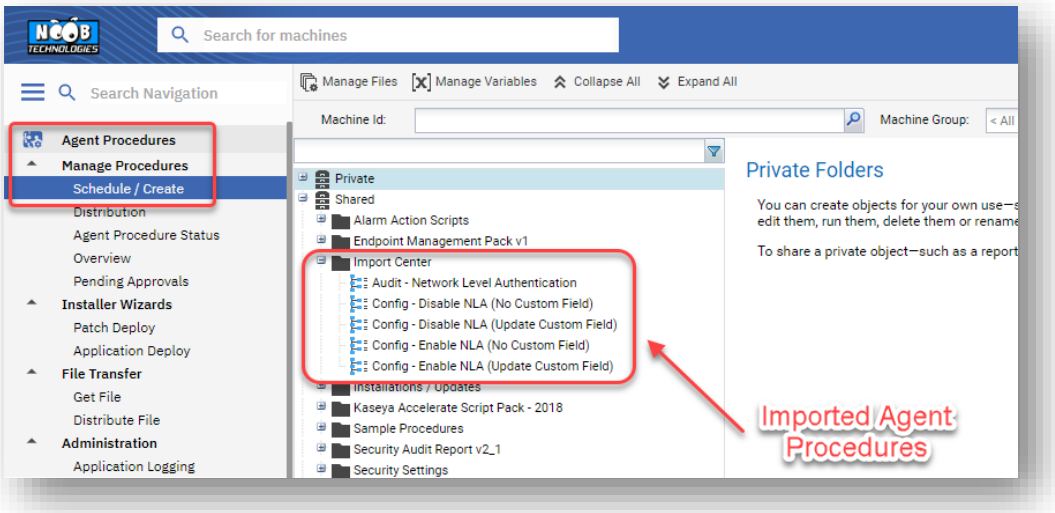
***VSA > System > Server Management > Import Center***



Next, extract the XML file from the downloaded ZIP file and click on the *New Import* button then upload to VSA.

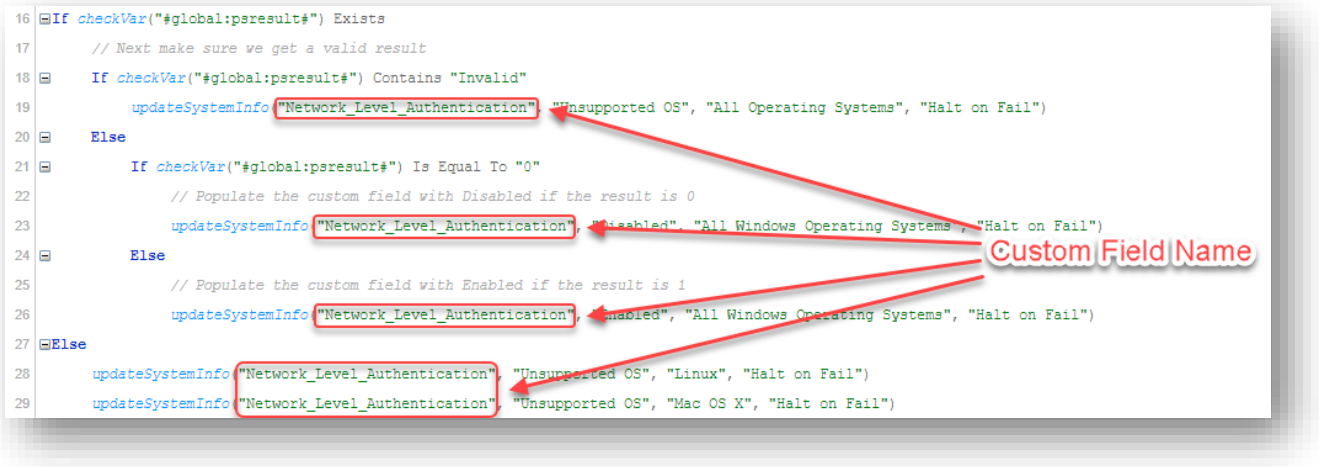



After importing the Agent Procedures, they should be placed in the Shared Folders in the Agent Procedure module in a subfolder called Import Center.




After it has been imported, edit an Agent Procedure and make sure the custom fields are filled in for every 'updateSystemInfo' command in the Agent Procedure. If the first set of commands have it properly filled in, then the rest of the script should also be mapped properly. If it already mapped properly for one Agent Procedure, then it should already be mapped for the other Agent Procedures.

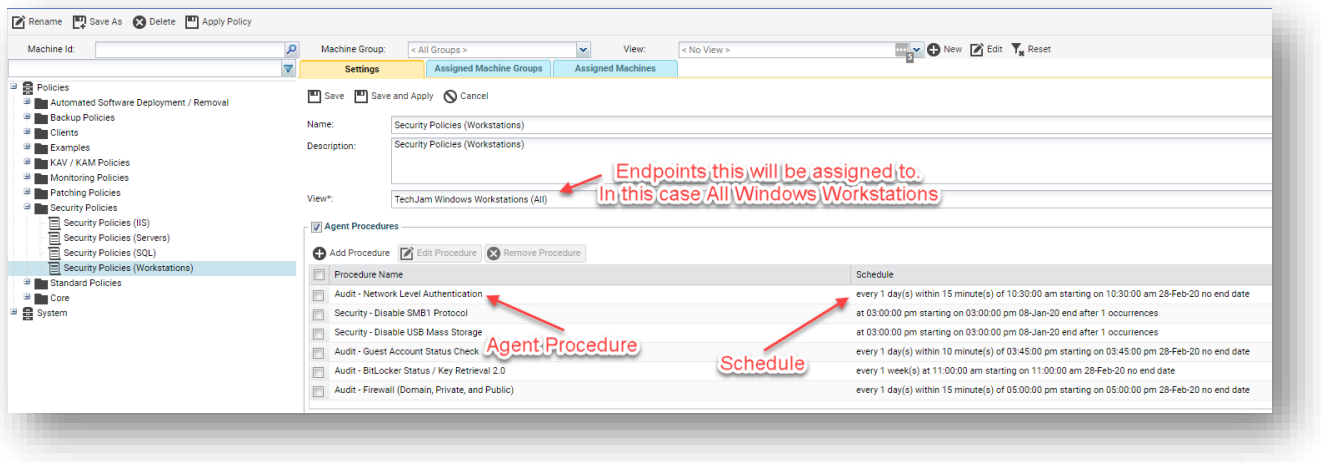
The updateSystemInfo command is the VSA command that puts content in a Custom Field. Below is an example of fields mapping correctly. If your import doesn't show the custom field, then you will have to map the fields manually. This can be easily done by selecting the command then selecting the Custom Field in the drop-down box.



# OTHER VSA MODULES

## *POLICIES*

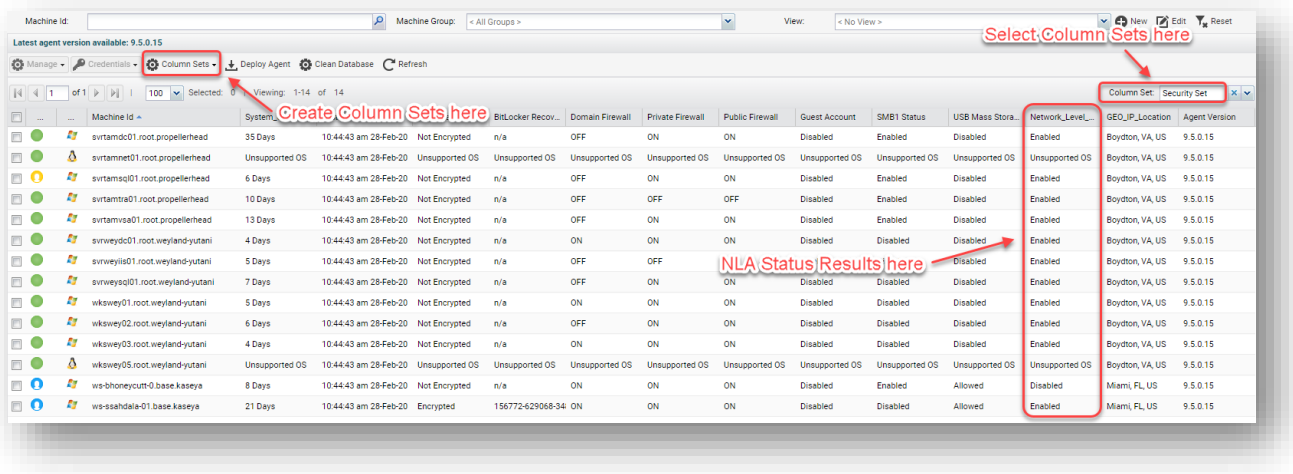
After the Agent Procedures have been properly imported, you just need to run this against your Windows endpoints. You can either run them manually or create a Policy then add the agent procedure to check for NLA to the Policy under a schedule to run however often you want. It may be best to run this weekly to catch any changes to an endpoint. Putting this in a policy to run regularly is the best practice here. Keep in mind that by assigning this to a policy, VSA will assign this to all current endpoints and all future endpoints that the policy applies to. Also, remember that Policies are assigned to a Machine Group (or Organization) and targeted using a View.



# AGENT COLUMN SETS

You can also add the Custom Fields to your Manage Agents screen by creating or adding it to your Column Set so you can see the results at a glance.

The following screenshot shows a Column Set called Security Set that shows security settings on the Manage Agents screen.



## *VIEWS*

It may also be useful to create views. Views will allow you to filter a list of endpoints that either have NLA enabled, the desired configuration, or NLA disabled. In addition, when you create a view, you can use it in a policy that would run an Agent Procedure that enables NLA on any endpoints that NLA is disabled, automatically.

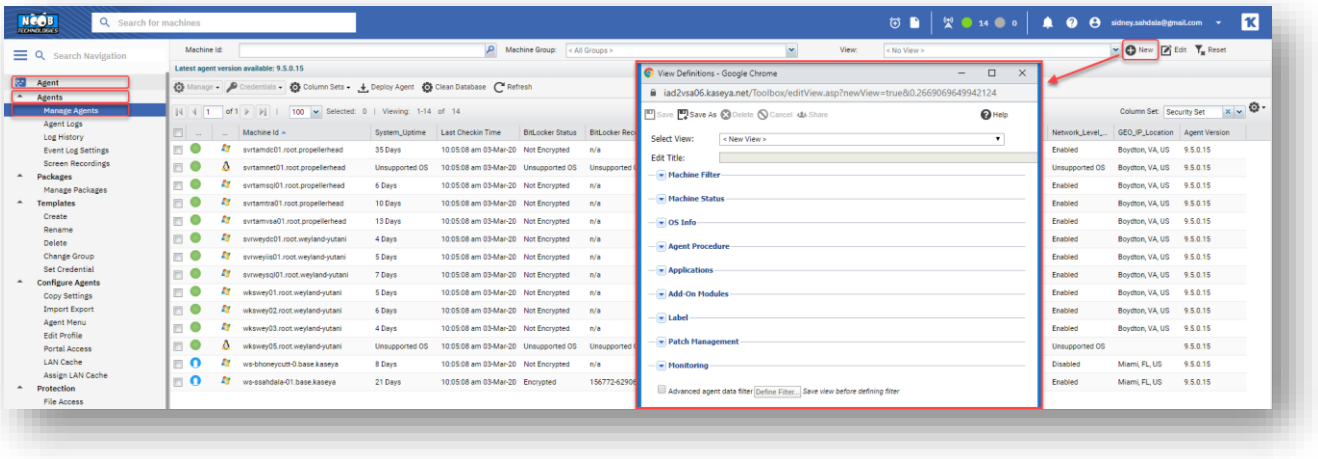
You should create two Views:

1. **Network Level Authentication Disabled** – This shows all endpoints where NLA is disabled.
2. **Network Level Authentication Enabled** – This shows all endpoints where NLA is enabled.

To create a View, go to:

VSA > Agent > Agents > Manage Agents

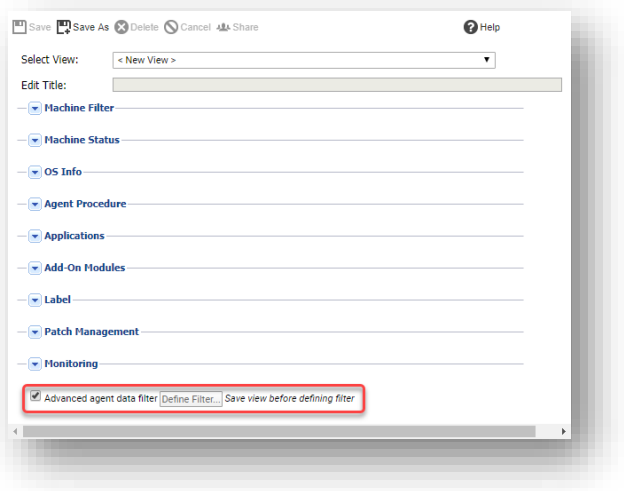
Next, click on New, on the upper right and another browser window should appear as seen below:



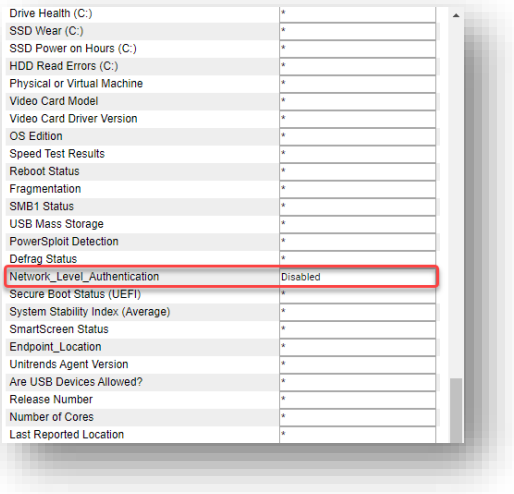

NOTE: You can create a view in any module that shows the View options in the Machine ID / Machine Group / View bar in VSA.

Next, click on Save As in the new window and save two Views called something like **Network Level Authentication Disabled** and **Network Level Authentication Enabled**.

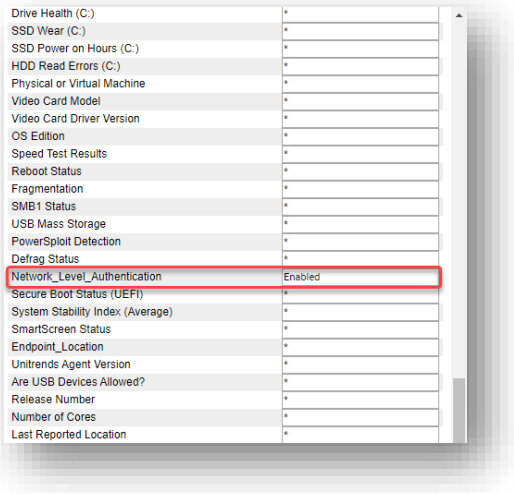
After it has been saved, you can then create an advanced data filter by putting a check mark next to Advanced agent data filter and clicking on **Define Filter**.




A new browser window will appear; scroll down until you find your custom field and enter Disabled in the text box next to the Custom Filed for the **Network Level Authentication Disabled** View and Enabled for the **Network Level Authentication Enabled** View as seen below.



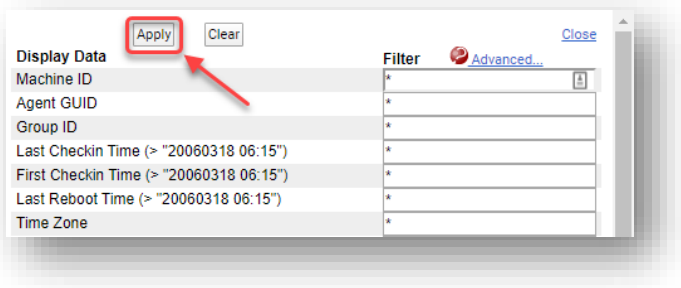

Network Level Authentication Disabled



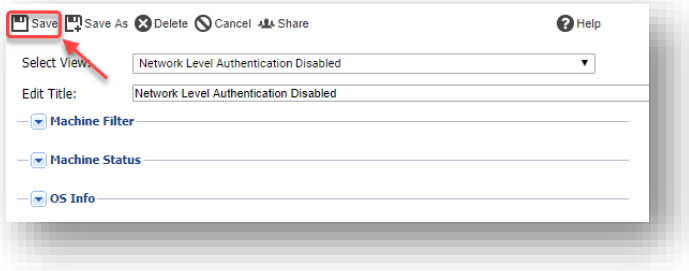

Network Level Authentication Enabled

REMEMBER: You can create Views on any of your Custom Fields in the advanced data filter.

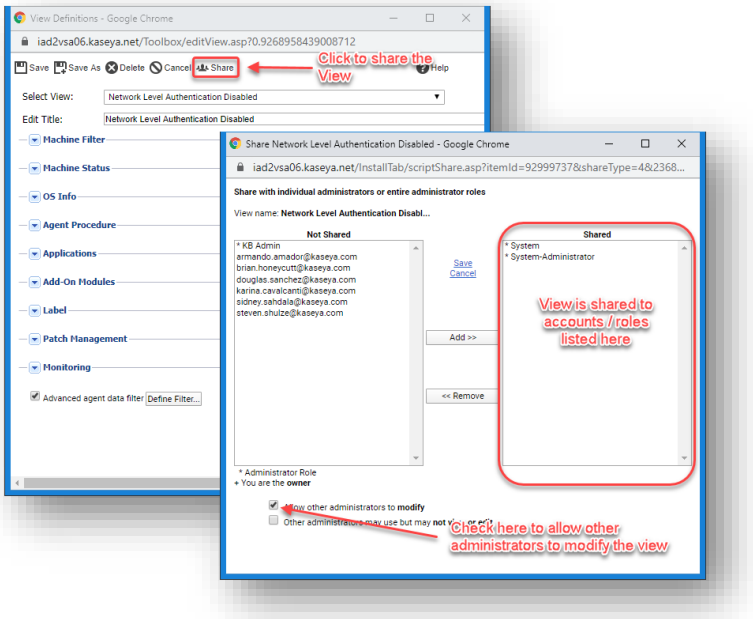
After you enter the information above in the Custom Field, be sure to scroll to the top of the page and click on Apply.




Then save the View once again to commit the changes and the view is ready to use.




Once saved, the Views will appear in your Views drop-down; you may want to share it with other administrators as well so they can use it.



## INFO CENTER

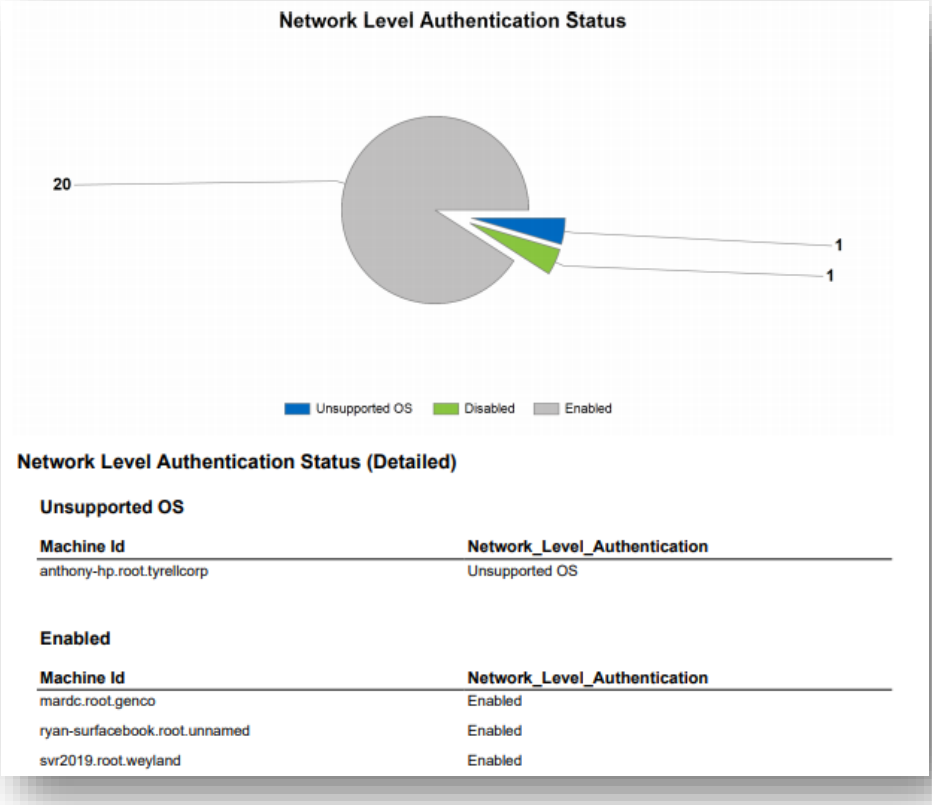
Now that you have a Custom Field you can use it in your reports in Info Center. This will be a simple report, but the goal of this section is to introduce you to VSA reporting concepts.

1. How to report on custom fields
2. How to make a pie chart
3. Using Grouping
4. Using Filters

Go to the Reports section of Info Center module in VSA by going to:

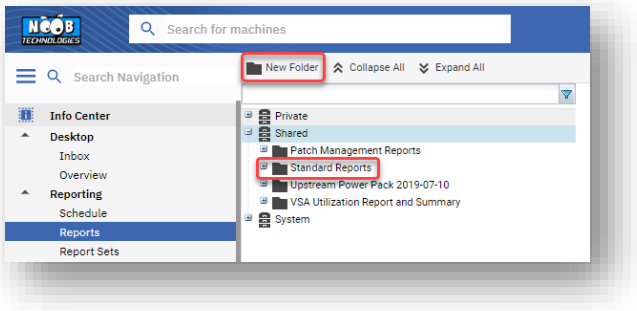
**VSA > Info Center > Reporting > Reports**

Below is a sample of a report that we will build. It shows the status of NLA in a pie chart and a table.

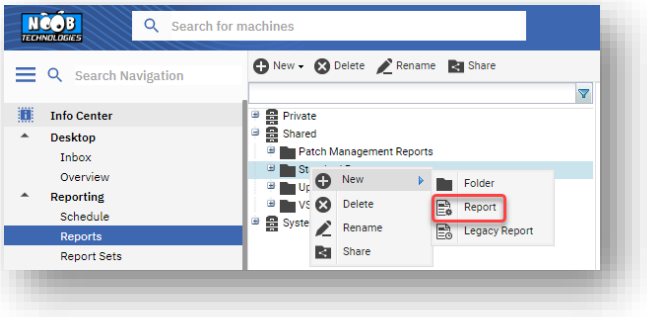


## Step 1 – Create a new Report

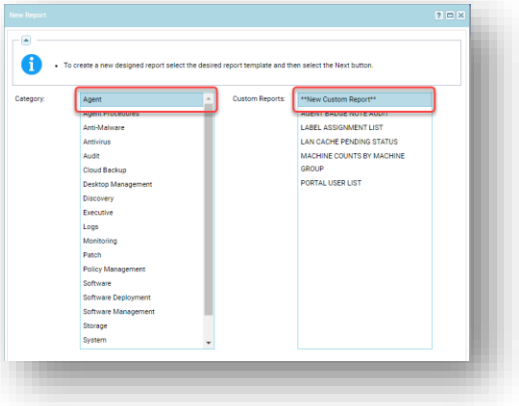
In the Reports section, select the Shared folder and create a new Folder called Standard Reports.




Right Click on the folder and click on **New > Report**.



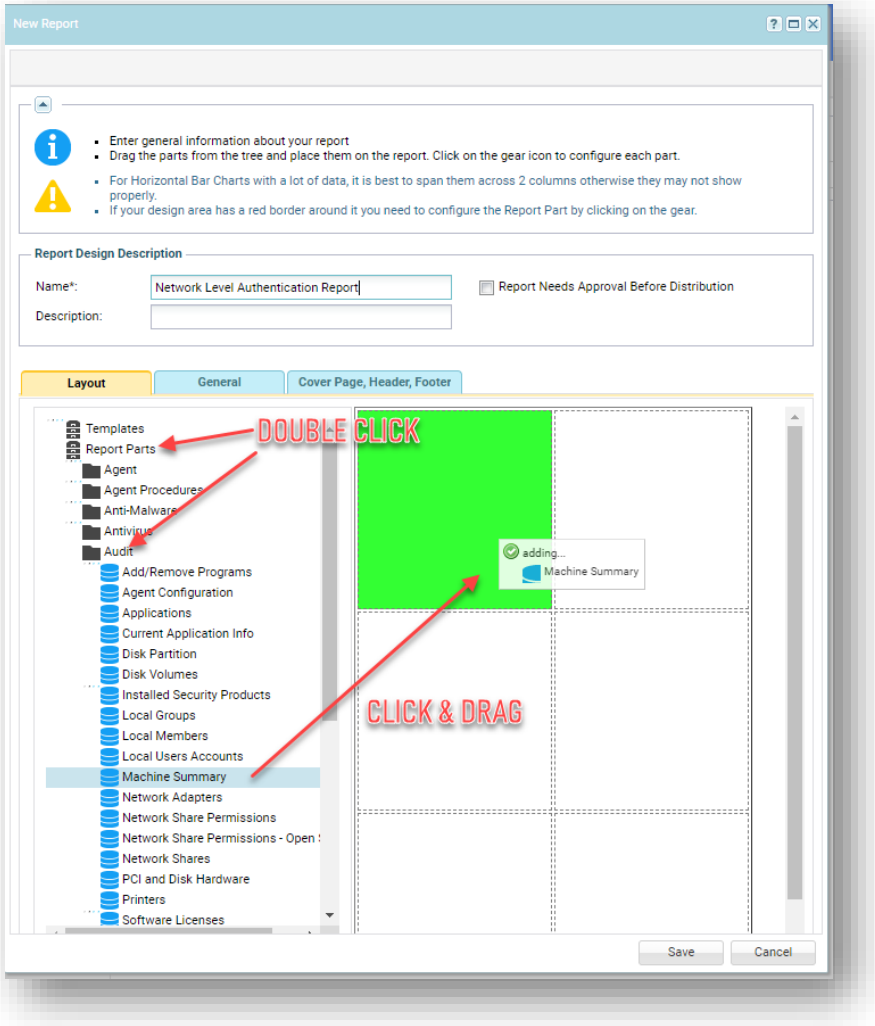

In the next screen you can categorize the report. You can select any category on the left, select **New Custom Report** on the right, then press Next.



## Step 2 – Add and Configure Report Parts

On the next screen, add a report part that will let you report on Custom fields.
Custom Fields can be reported on using the **Machine Summary** Report Part.

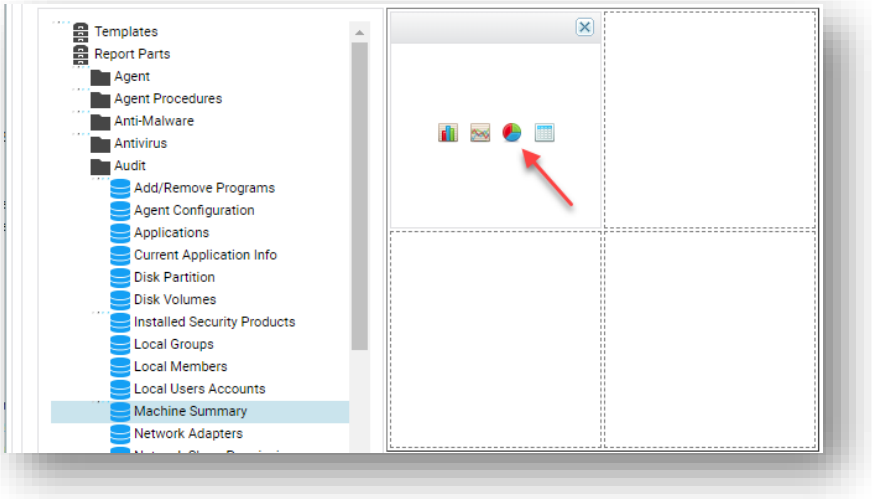
First, give the report a Name. We will call this report Network Level Authentication Report.



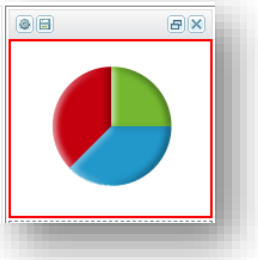

Next, add the Report Part to your Report by:

1. Double-clicking on the Report Parts Folders on the left.
2. Double-clicking on the Audit Folder.
3. Click and Drag the Machine Summary Report Part to the grid on the right.

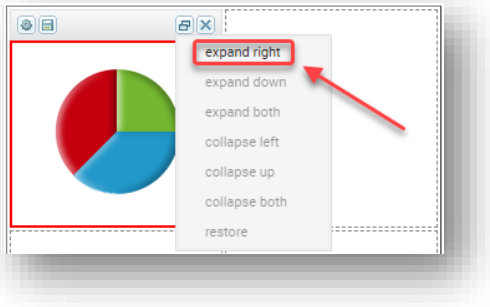
Next, click on the icon that shows the way you want to represent the data. In this case we will choose Pie Chart.



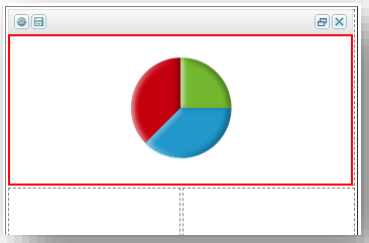

After you selected the Pie Chart, the Report Part should then look like this:



You may want to expand the Report Part to take the entire width of the page so click on the  icon on the top right then select Expand Right.

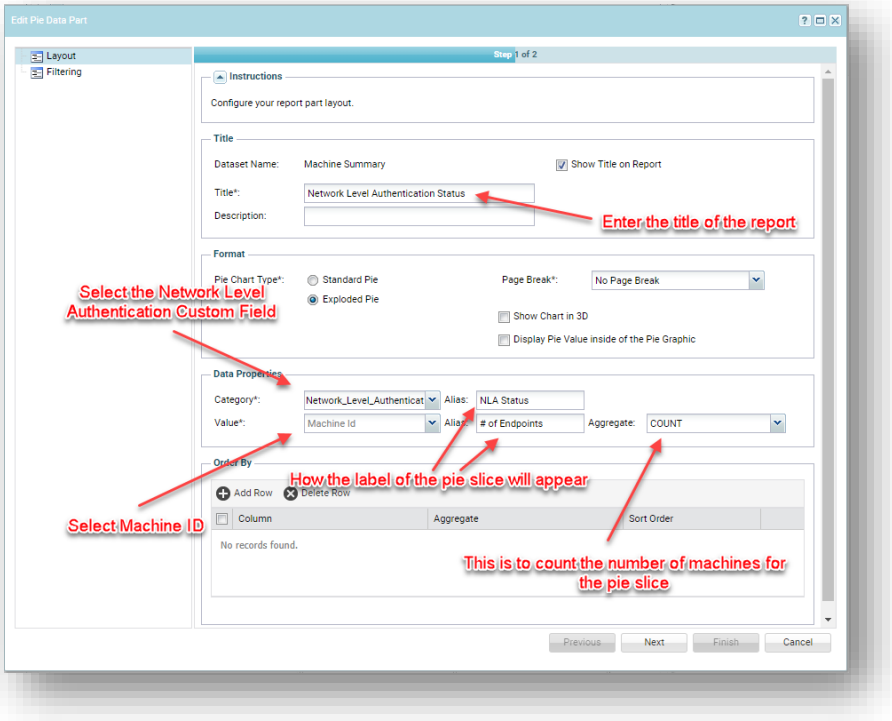


Your report layout should now look like this:



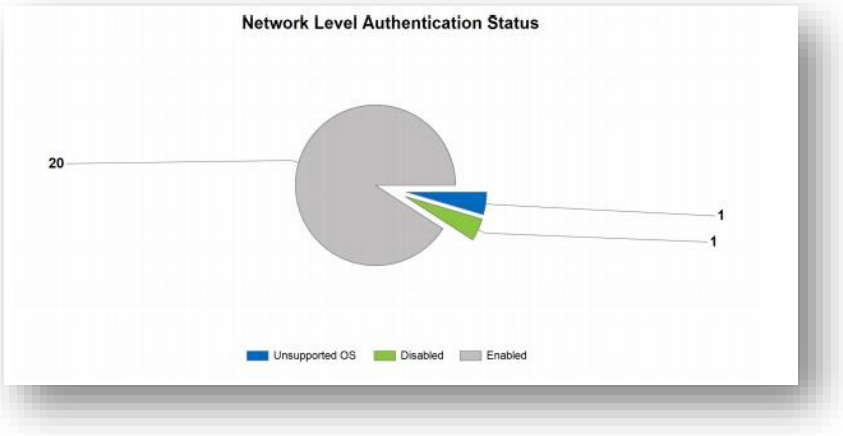
Double-Click on the Pie Chart and make the following changes to the repot part settings:

1. **Title**: Network Level Authentication Status
2. **Category**: Network_Level_Authentication
3. **Alias**: NLA Status
4. **Value**: Machine Id
5. **Alias**: # of Endpoints
6. **Aggregate**: COUNT




Click on Next then Click on Finish.

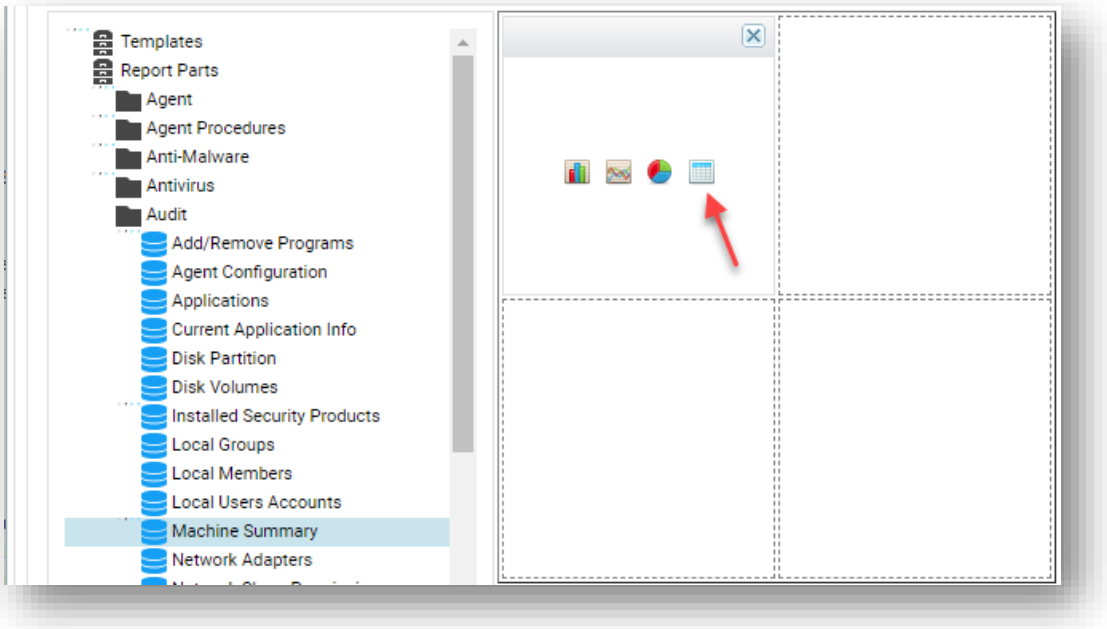
If you run the report, it should show something like this:



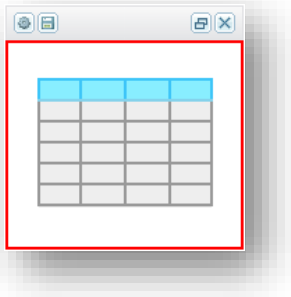

Next, we want to create a table with the details so you can see exactly which endpoints either have NLA Enabled, NLA Disabled, or does not support NLA.

Add the next Report Part to your Report just like you did with the Pie Chart by Clicking and Dragging the same Machine Summary Report Part to the grid on the right report grid.

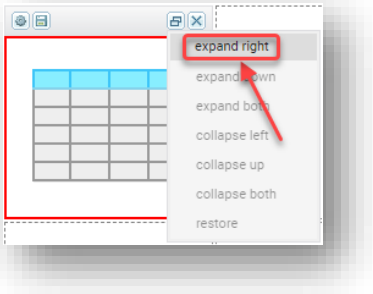
Next, click on the icon that shows the way you want to represent the data. In this case we will choose the Table so we can list the details.



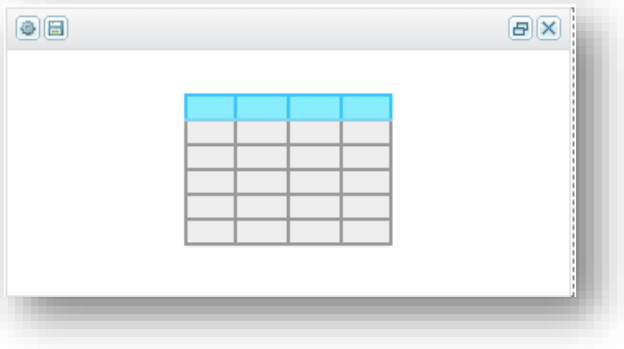
After you selected the Table, the Report Part should then look like this:



You may want to expand the Report Part to take the entire width of the page so click on the  icon on the top right then select Expand Right.



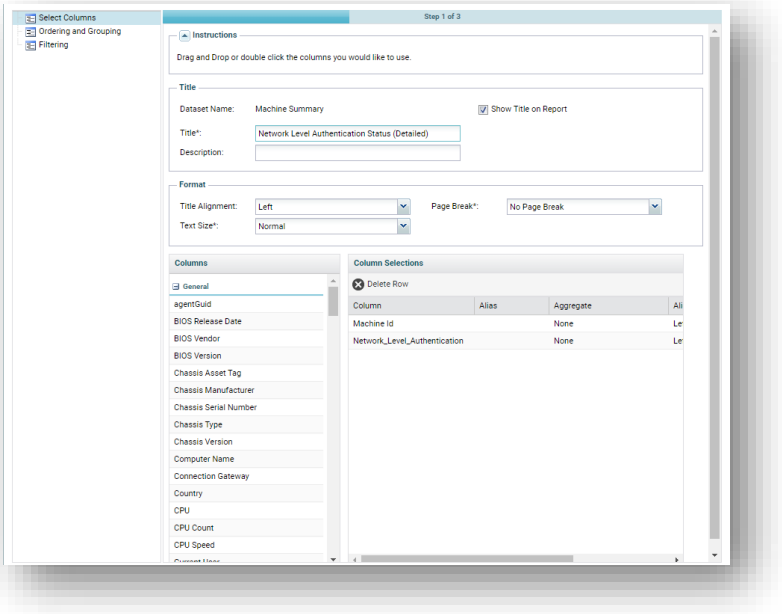

Your report layout should now look like this:



Double-Click on the Pie Chart and make the following changes to the repot part settings:

1. **Title**: Network Level Authentication Status (Detailed)
2. **Column Selections**:
    a. Machine Id
    b. Network_Level_Authentication

Your Report Part should look similar to the screenshot below:

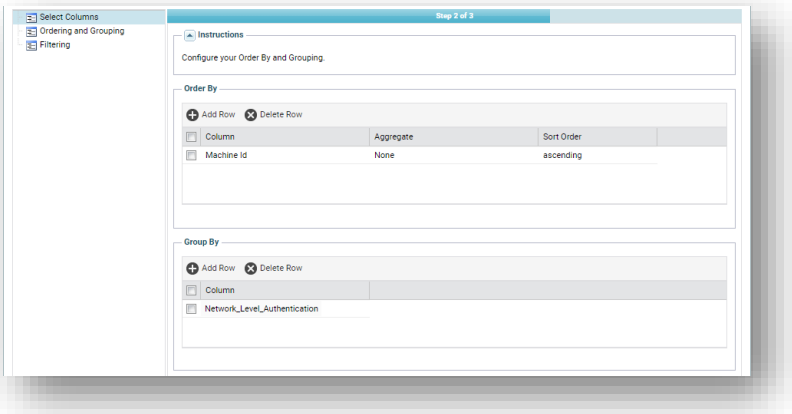



Click Next.

On the following page add the following:

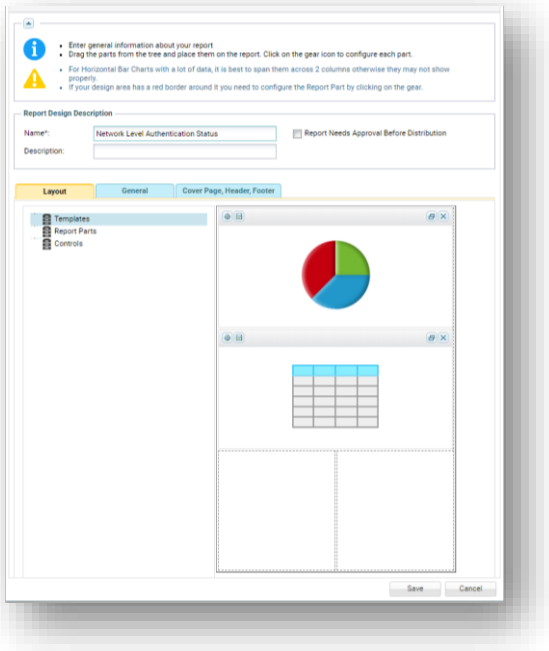
1. Under, **Order by**, add a row then:
    a. **Column**: Machine Id
    b. **Sort Order**: Ascending
2. Under, **Group by**, add a row then select **Network_Level_Authentication** (the custom field you created)

Doing this will list all the Machine Id's in alphabetical order and group the machines based on the content of the custom field called Network_Level_Authentication.



Click on Next then on the following page just click on Finish.

Your Report screen should look like this.




Click on Save then Run the Report. Your report should look similar to this: