Dashboard User Guide

Nanoheal Dashboard Version 6 for AVIRA

Contents

Nanoheal by HFN 7
Last Updated: 5-July-2017 7
What is Nanoheal? 8
What is Dashboard? 9
Sign Up Flow 10
Nanoheal Provisioning 10
Provisioning Entities and Their Relationships 10
How to Sign up 10
How to register a new reseller/customer? 11
How to create a customer for the first time? 13
Trial Flow 25
NH Pre-Requisites 27
Minimum System Requirements 27
Application exception list in Anti-virus software installed in the managed device 27
EXE file information: 27
DLL File information: 27
Files to be whitelisted from temp location: 28
Firewall/Proxy unblock 28
Download-Install flow 29
My Account Page 33
Account Details 34
Order Details 35
Customer Details 35
Getting started with Dashboard 36
Sign In 36
Understanding Dashboard Layout 38
Dashboard Data 39
Home Page Statistics 41
Sites 42
Compliance 42
Compliance Trend 46
Notifications 48
Notification Status 49
Notes 50

Fixing Notification 51
Using Troubleshooting Notification Fix 52
Notification Alert 54
Notification View 56
Notification Export 57
Notification Trend 58
Resolutions – Proactive (Audit & Schedule) 59
Resolutions Status: 61
Resolutions – Predictive 63
Event Information 65
Event Detail 66
Events Export 67
Event Filter Search 67
Asset Information 69
1. Basic Info 70
2. System Info 71
3. Software Info 71
4. Patch Info 72
5. Resource View 72
6. Network Info 73
Export 74
Asset Analytics Report 74
Asset Query Execution 75
Asset Report Download 76
Asset Analytics Delete 77
Asset Analytics Refresh 77
Deployment 78
Steps 79
Deployment 81
Deployment Audit 84
Manage Customers 85
Add OTC 89
Add a Customer 90
Update OTC 95
Add Avira Subscription 97

Edit Customer 98
Revoke & Remove 101
Customer Details 102
Export AVIRA details 103
Disable Customer 105
Services 106
Avira configuration: 107
System Scanner 108
Real Time Protection 112
Web Protection 116
Mail Protection 119
Device Protection 124
Threat Categories 126
Advanced Protection 127
Password 129
Security 130
Scheduler 132
Avira Configuration Audit 141
Nanoheal Configurations 145
Problem Automation 145
Application Monitoring 146
Network & Printers 146
Operating System 147
Device Management 148
Maintenance 148
Intrusion Protection 149
Antivirus Management 149
Resource Utilization 150
Device Policies 150
Network Policies 151
Files, Folders & Peripherals 152
Others 152
System Management 153
Patch Management 153
Software Distribution 154

Provisioning & Metering 154
Software Update 155
Proactive Resolution 155
NH Configuration Audit 156
Troubleshooting 157
Users 166
Add New User 167
Edit User 169
Delete User 170
Export 170
User Roles 171
Groups 174
Add New Group 174
Rebuild Group 177
View Details 179
Export Group Detail 180
Export Group List 181
Delete group 181
Insights 183
Incident Trend 184
Compliance Trend 185
1. Add New Report 188
2. Add New Section 191
3. Edit 192
4. View Section 193
5. View 194
6. Download 197
7. Delete Report Files 198
8. Delete Report 198
9. Run Now 199
10. Refresh 199
Annexure 200
Software Distribution 200
FTP/CDN Configuration 202
View Software Details 204

Add Package 205
Nanoheal Repository 207
Vendor Repository 208
Edit Package 208
Configure Configuration for Vendor Repository 210
- File 212
- Software Name 212
- Registry 212
Distribute Configuration for Nanoheal Repository 216
Configuration Post Validation for Nanoheal Repository 216
Edit Configuration 216
Distribute Package 217
Delete Package 218
View Software Distribution 218
Export 219
Software Update 220
Add 221
Edit 223
Details 224
Versions 225

Nanoheal by HFN

Copyright 2016-17 © HFN, Inc. All Rights Reserved.

Nanoheal, HFN and its logos are registered trademarks of HFN Inc. in United States and other countries. Other brands and logos may be claimed by other organizations and individuals.

HFN does not warrant that this document is error free and retains the right to make changes to this document or any other related documentation at any time without notice. HFN does not assume any obligation to update the information contained in this document. This document is provided "AS IS" and without any guaranty, warranty, or license, express or implied, including but not limited to: fitness for a particular purpose, merchantability, non-infringement of intellectual property, or other rights of any third party.

Last Updated: 5-July-2017

S.no	Date	Prepared by	Reviewed by	Version
1	30th November 2016	Wasif	Divya	1.1
2	29th January 2017	Divya	Abhishray	1.2
3	30th January 2017	Abhishray	Divya	1.3
4	07th March 2017	Abhishray	Divya	1.4
5	12th April 2017	Priyanka Kanak	Priyanka Saha	1.5
5	5th July 2017	Priyanka Kanak	Wasif	1.6

What is Nanoheal?

Nanoheal is a powerful end point management solution which combines enterprise system management, proactive & auto heal incident resolution capabilities and enterprise mobility management in a cloud delivery model.

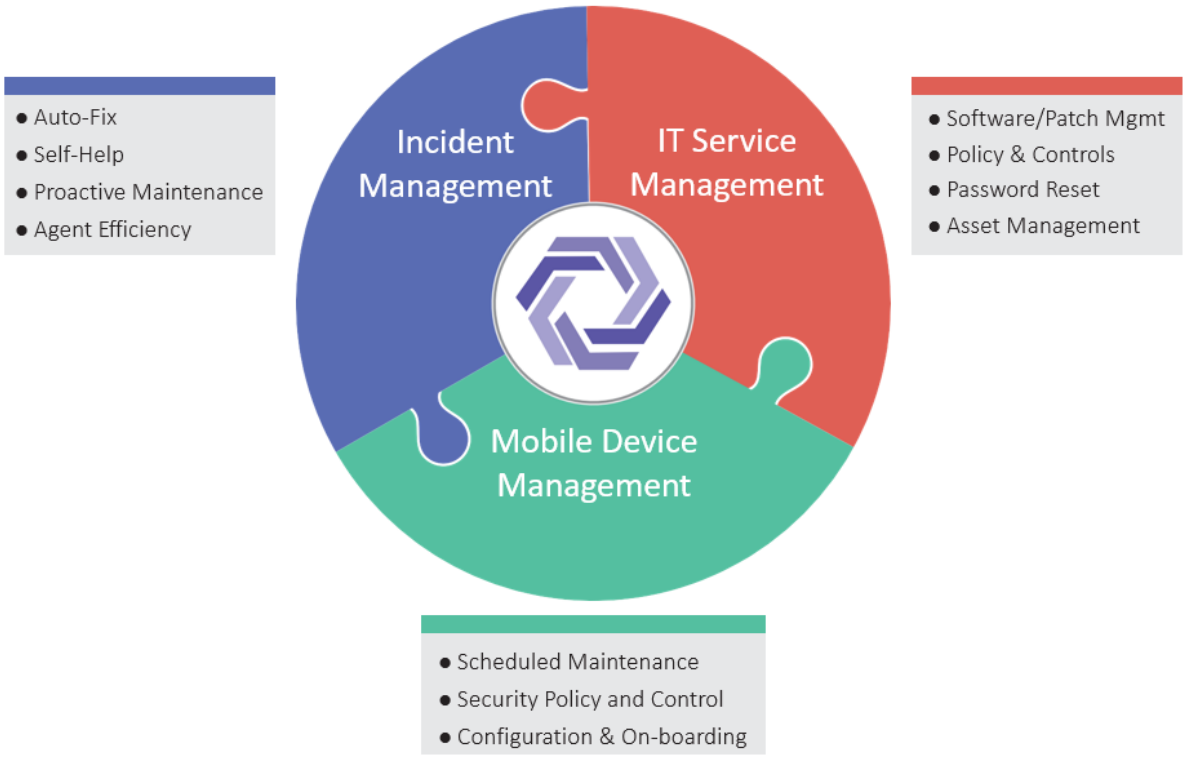


Figure 1 Nanoheal Components

Nanoheal enables Enterprise IT Teams, Managed Service Providers and OEMs to move their and their customer environments from reactive support model to proactive and self-healing model.

More information about Nanoheal features, technology and support philosophy visit www.nanoheal.com.

What is Dashboard?

The Dashboard/Console is the server component of Nanoheal that allows a user to view information and enables them to manage configurations centrally.

The Nanoheal Dashboard lets a user manage and access information about the systems they have under management, in an intuitive and straightforward manner.

The high-level feature list of the Nanoheal Dashboard is as follows. The table shows the AVIRA – NH Console and the NH Specific Feature –

Area/Module	Default AVIRA-NH Console	NH Specific Feature
Dashboard Landing page and functionalities	YES	NO
Side Panel	YES	NO
Dashboard - Sites	YES	NO
Dashboard - Compliance[AVIRA Specific]	YES	NO
Dashboard - Notification[AVIRA Specific]	YES	NO
Dashboard - Resolutions[AVIRA Specific]	YES	NO
Dashboard - Compliance[NH Specific]	NO	YES
Dashboard - Notification[NH Specific]	NO	YES
Dashboard - Resolutions[NH Specific]	NO	YES
Manage - Services - Avira Configuration	YES	NO
Manage - Services - Nanoheal Configuration	NO	YES
Manage - Troubleshooting - PC Tune Up	NO	YES
Manage - Troubleshooting - Hardware Fixit and Troubleshooters	NO	YES
Manage - Troubleshooting - Software Fixit and Troubleshooters	NO	YES
Manage - Troubleshooting - Enterprise App Store	NO	YES
Manage - Troubleshooting - Run as Administrator	NO	YES
Manage - Troubleshooting - Avira Antivirus	YES	NO
Manage - Users	YES	NO
Manage - Groups	YES	NO
Insights - Services Insights[AVIRA Specific]	YES	NO
Insights - Services Insights[NH Specific]	NO	YES
Insights - Sales Insights	NO	YES

Sign Up Flow

Nanoheal Provisioning

Nanoheal allows individual users, SMBs, Enterprises and MSPs to manage their environments and associated services. Many enterprises and MSPs have multiple partners who provide IT support to SMBs. Nanoheal's enterprise provisioning system allows Enterprises and Service Providers to manage their customers through an amazingly easy to use web module.

Provisioning Entities and Their Relationships

To use Nanoheal's provisioning system efficiently, the user will need to understand the following terms and their relationships.

Resellers or Service Providers: A Reseller is a company that partners with a manufacturer [AVIRA] or producer to market and sell the manufacturer's products, services, or technologies. Resellers may be distributors, vendors, retailers, consultants, systems integrators (SI), technology deployment consultancies, value-added resellers (VARs) and other such organizations.

Reseller has provision to create following:

- Admin - who would manage their OR their customer's devices
- Customer - who would manage their devices by themselves

Reseller or Customer as an **Admin**: Resellers as Admin manage devices of their customers directly and Customers as Admin manage their own devices.

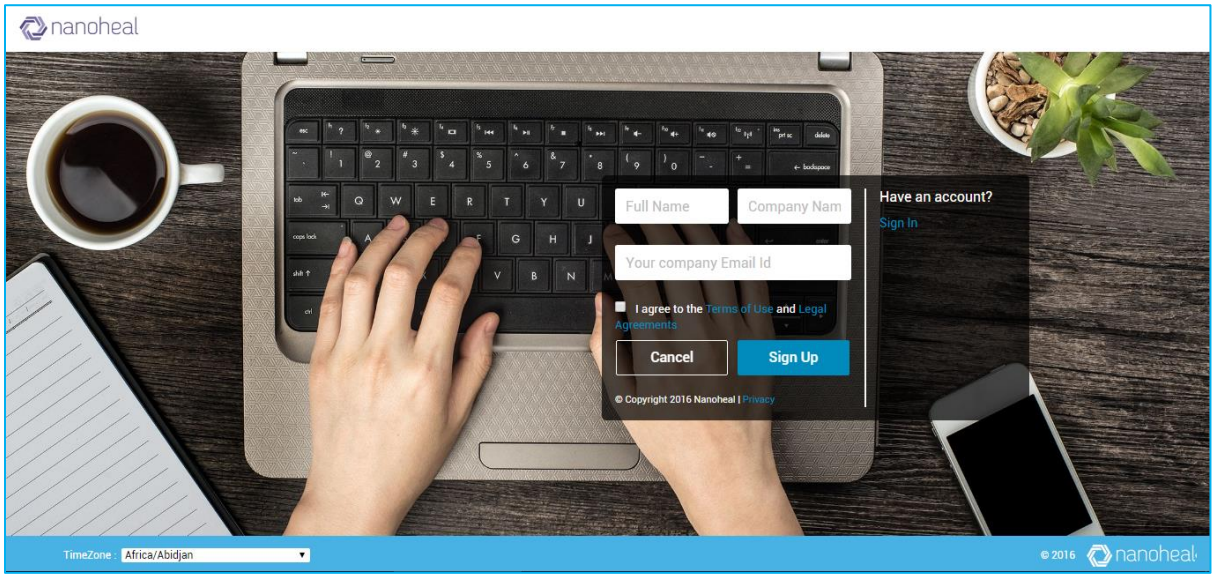
Customer: A customer is an organization, whose IT (End Point Devices) environment is supported using Nanoheal product and associated services.

How to Sign up

In order to Sign up, the user needs access the following link and choose "Create Account"
https://commandcenter.nanoheal.com/Dashboard

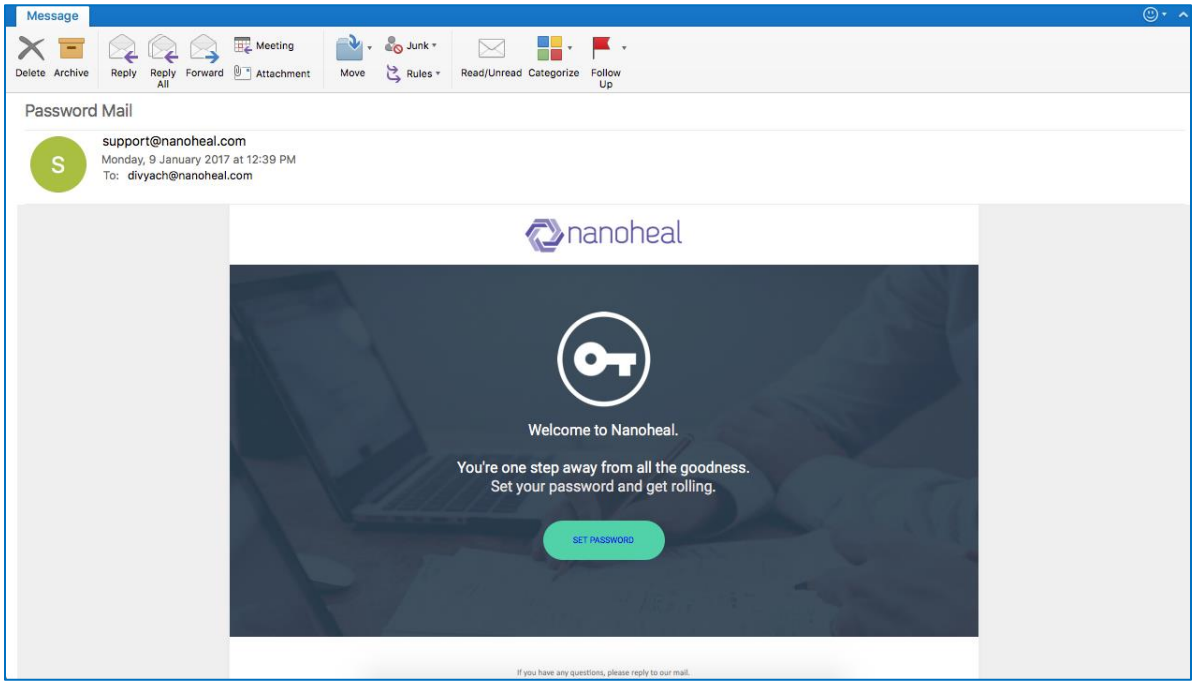
How to register a new reseller/customer?

a. The user needs to navigate to the link provided for the account creation, and enter the basic details in the space provided. The details required are:
    i) First Name - It does not accept special characters.
    ii) Company Name
    iii) Email ID

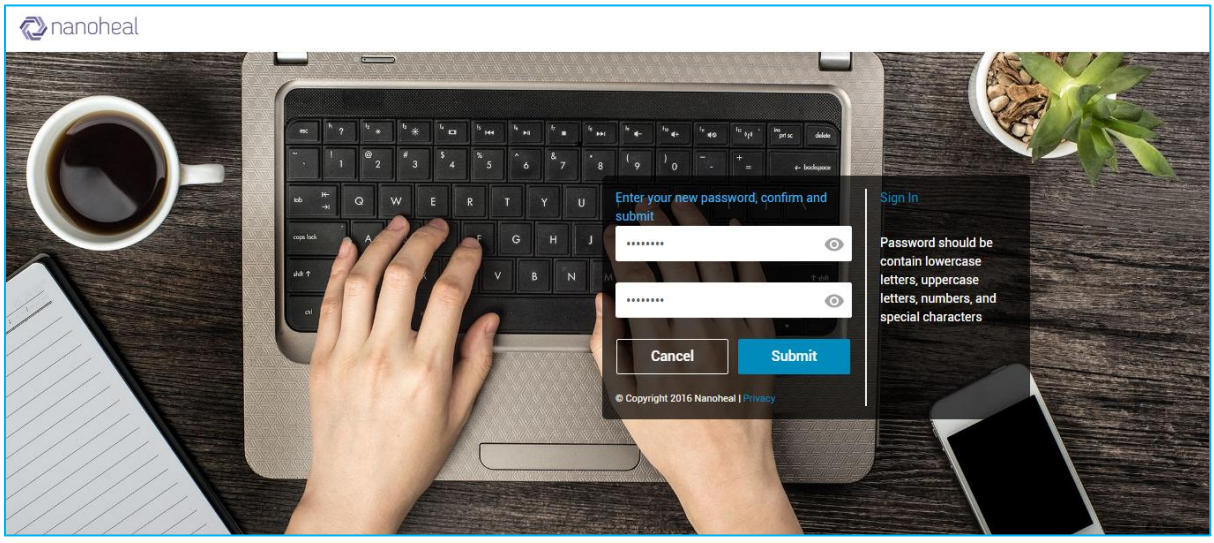


a. The user should Accept the T&C and click on "Sign Up"
b. The user will receive a confirmation email. With an option to set their password. If the email is not found in the inbox, the user may need to check their email filter settings and Junk folder.

    As shown below:



a. The password must adhere to the following rules:
    i) Has at least one capital case letter
    ii) Has at least one numerical character
    iii) Has at least one special character
    iv) Password is at least 8 or more characters' long



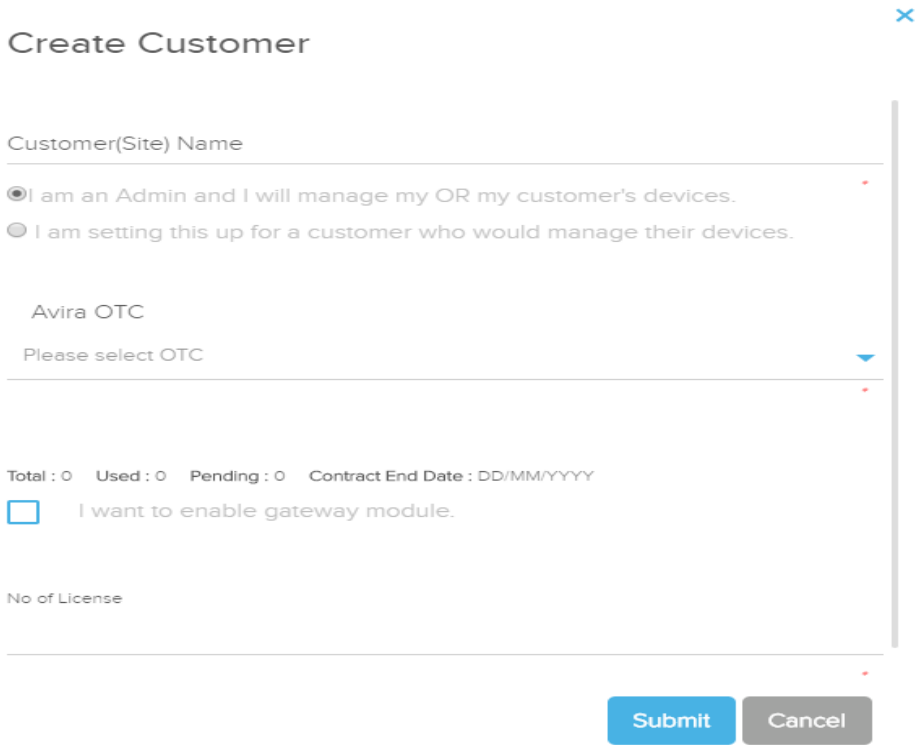
a. Once the password is set, the user should proceed to sign in.
b. Once logged-in, a popup prompts to create a customer

There are two radio buttons to select from:

- I am an Admin and I will manage my OR my customer's devices – *This option would enable a Reseller to manage multiple customers and their devices.*

Additionally, the same option would enable the IT Admin of a company/customer to manage their own devices

- I am setting this up for a customer who would manage their devices – *This option enables a Reseller to create login and site for customers who would manage their devices but need the Reseller to help setup the Dashboard.*
  Limitation: Upon using this option – the customer would not be able to create new sites by themselves. They would need to contact the Reseller for the same.



How to create a customer for the first time?

When a user logs into the dashboard for the first time, he is greeted with a popup that prompts him to create a "Customer" as shown above.

Illustration: A Reseller can select - "I am an Admin and I will manage my OR my customer's devices", and add OTC. Reseller can view the site they created and have full access to my account page. On the contrary, if he selects, "I am setting this up for a customer who would manage their devices" and adds OTC, then when the customer login after setting password, he will see the site in right pane and does not have full access to my account page.

Please follow the following steps to add a new customer/site.

1. I am an Admin and I will manage my OR my customer's devices:

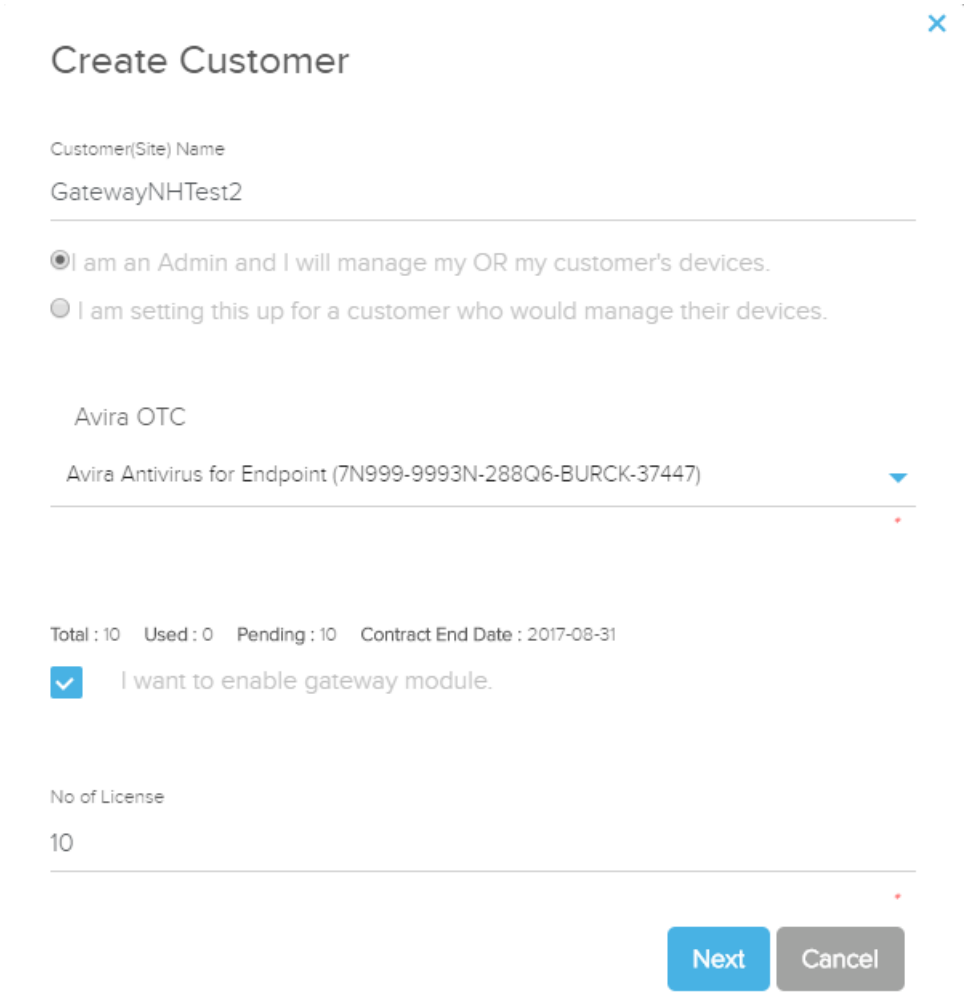
   i) The user will see a popup as shown below, wherein he has to enter:

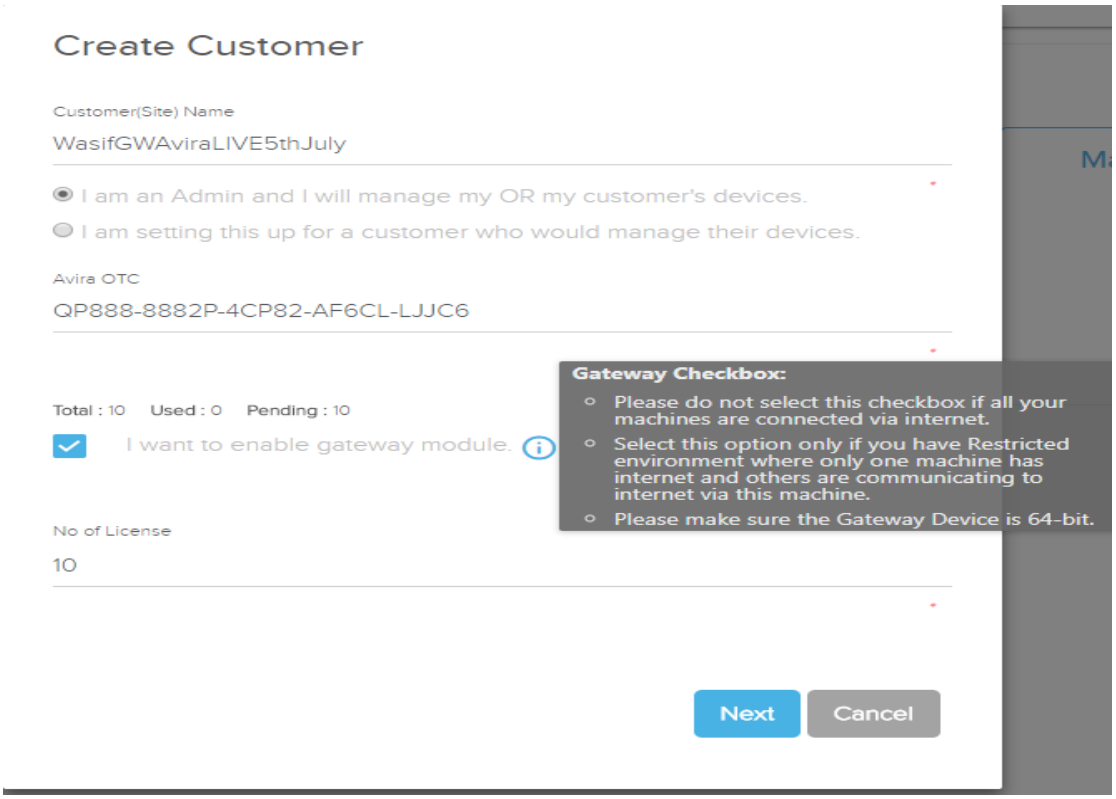
      i. OTC
      ii. Number of Licenses to use

   ii) Enter the number of devices he wants to install the software on

   iii) Select the checkbox of gateway option if you want to enable gateway module.

   iv) Click on "Verify" to verify the OTC and "Submit" to goto next page.





Gateway Module: If gateway module is enabled, machine in the same network will not need internet connection to install nanoheal. User has to make a machine in the network as gateway machine and all other machine will install client from gateway machine.

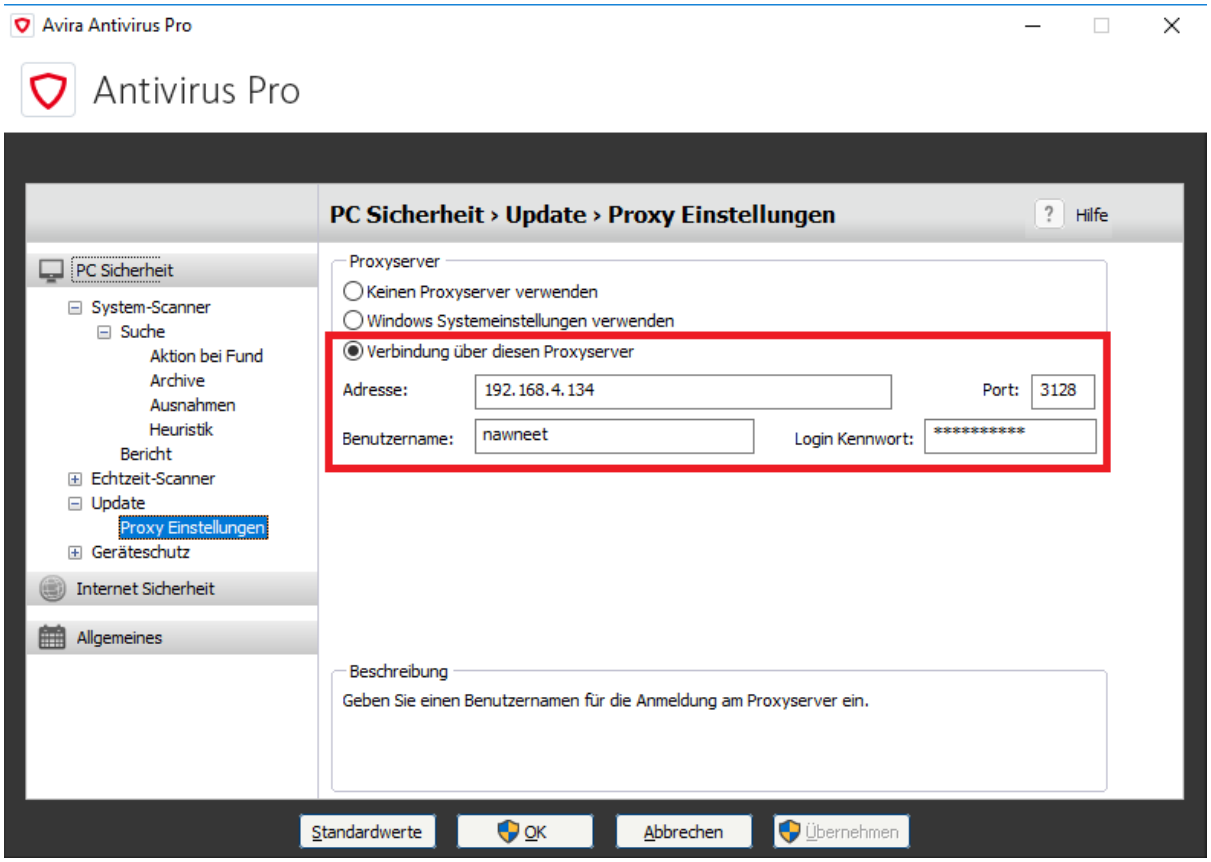
We are using Squid Proxy software for setting the proxy details in gateway machine which would take care of the entire communication. Squid would get installed before nanoheal installation i.e As soon as customer double clicks on the nanoheal exe, it will first download Squid and install it, then customer will get Nanoheal UI for installation. Generally it takes 5-6 minutes for installing squid(depends on internet speed) and then Nanoheal UI will come asking customer to install.

Prerequisite for Gateway Model:

1. Gateway machine should have minimum of 2GB RAM.
2. Gateway machine should be a 64-bit machine.
3. Firewall should be turned off on the sub-machines.
4. Gateway machine and sub -machines should be in the same **domain**/network.
5. There should not be pre-installed Squid software (If installed, Squid should be uninstalled and all concerned directories from C: drive should be manually deleted.)
6. Gateway machine should be a windows machine.

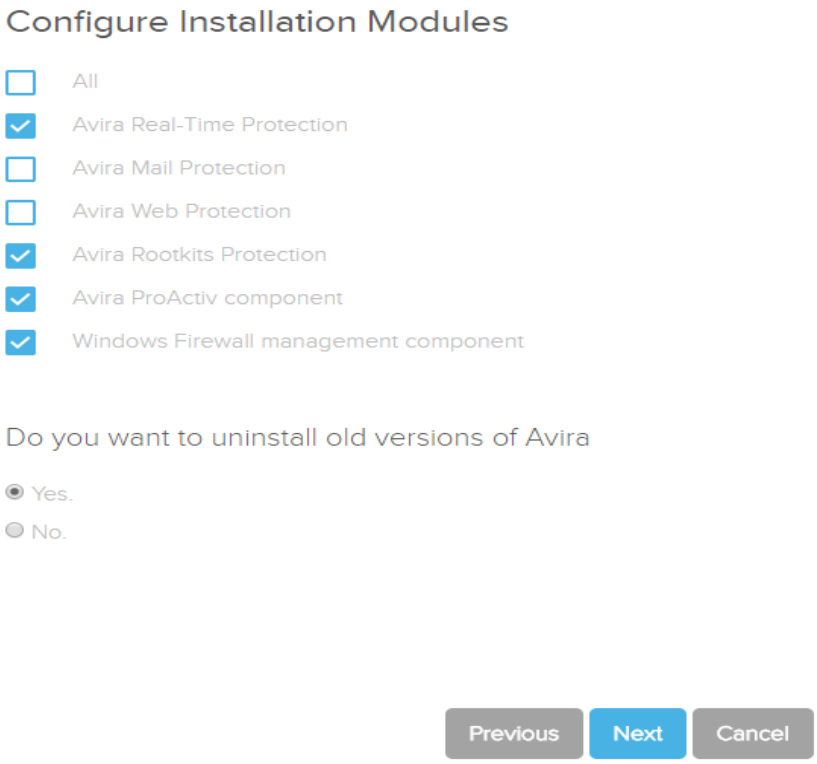
7. Squid service need to be added in start-up during booting.
8. Gateway machine should have admin rights to install Squid.

When deployment happens from gateway machine to sub-machines/endpoints, proxy details will get set under 'Update and proxy settings' in Avira UI in sub-machines also as shown below:

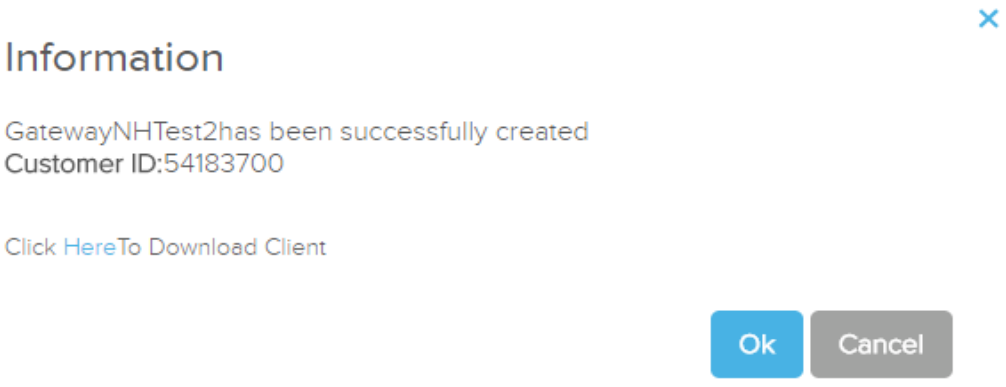


Note: This feature works only for the machines which are in the same network/domain. Squid software use 3128 port no. as default port for gateway communication.

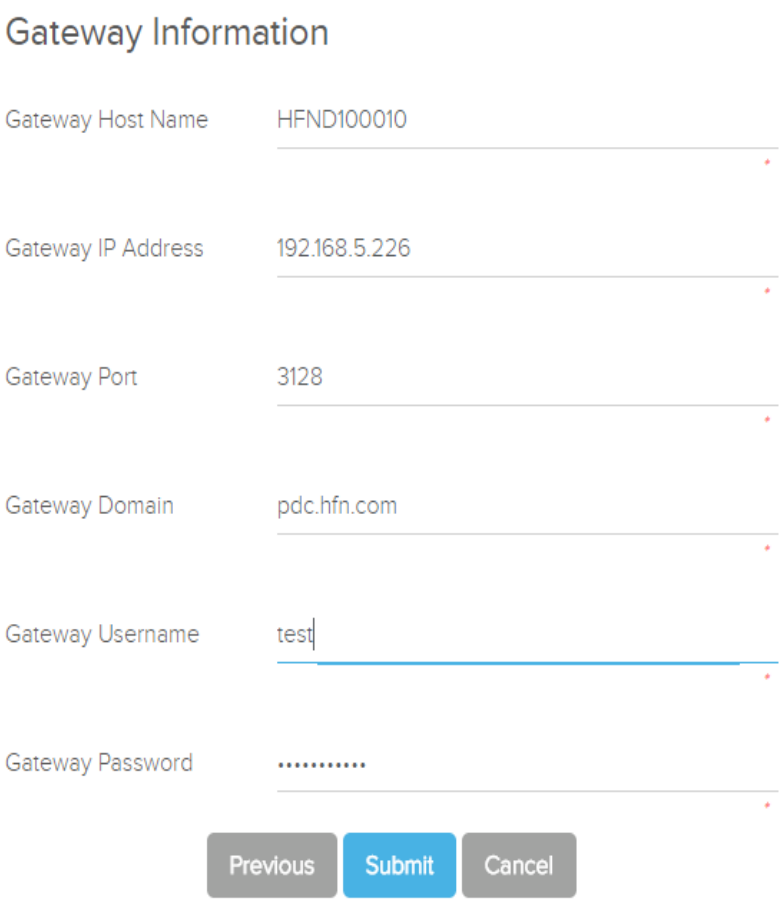
After the OTC gets verified, User will get the popup to select which modules to install by default with Avira and option to uninstall older version of Avira as shown below:



Click on Next will ask for gateway machine details if gateway option is enabled, if not it will directly create the customer and will give the download URL to download the client as shown below:



If gateway module is enabled:

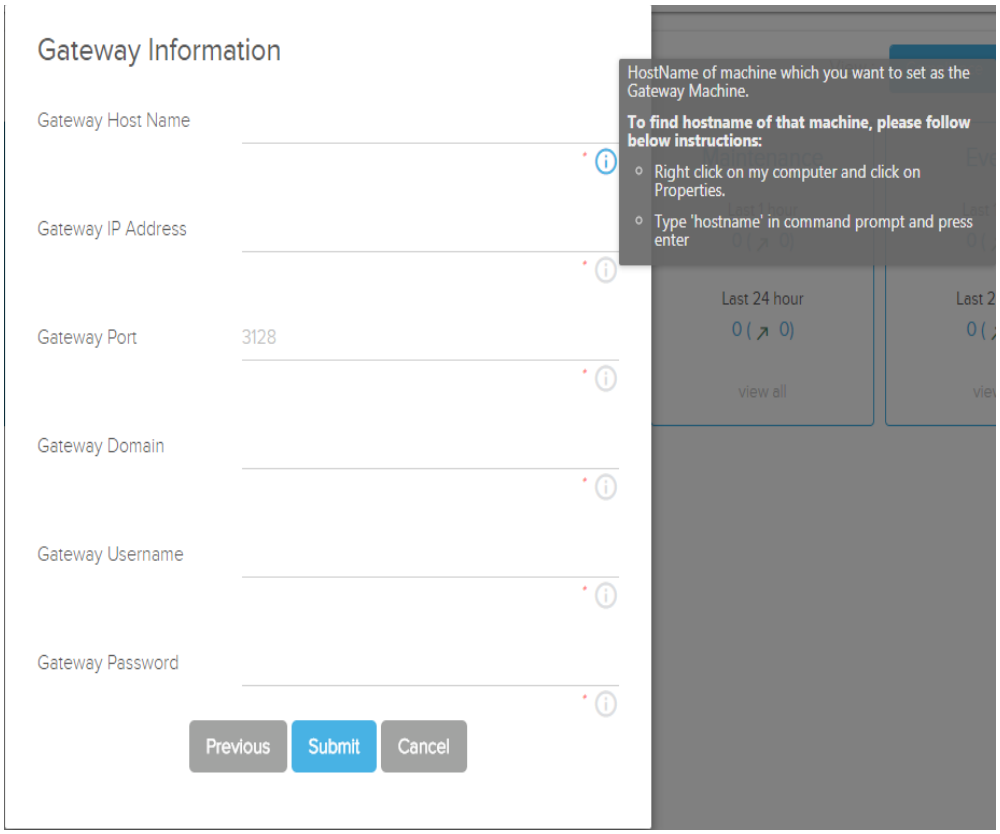


Gateway Information details:

1. HostName: HostName of machine which you wants to set as the Gateway Machine. To find hostname of that machine, please follow below instructions:

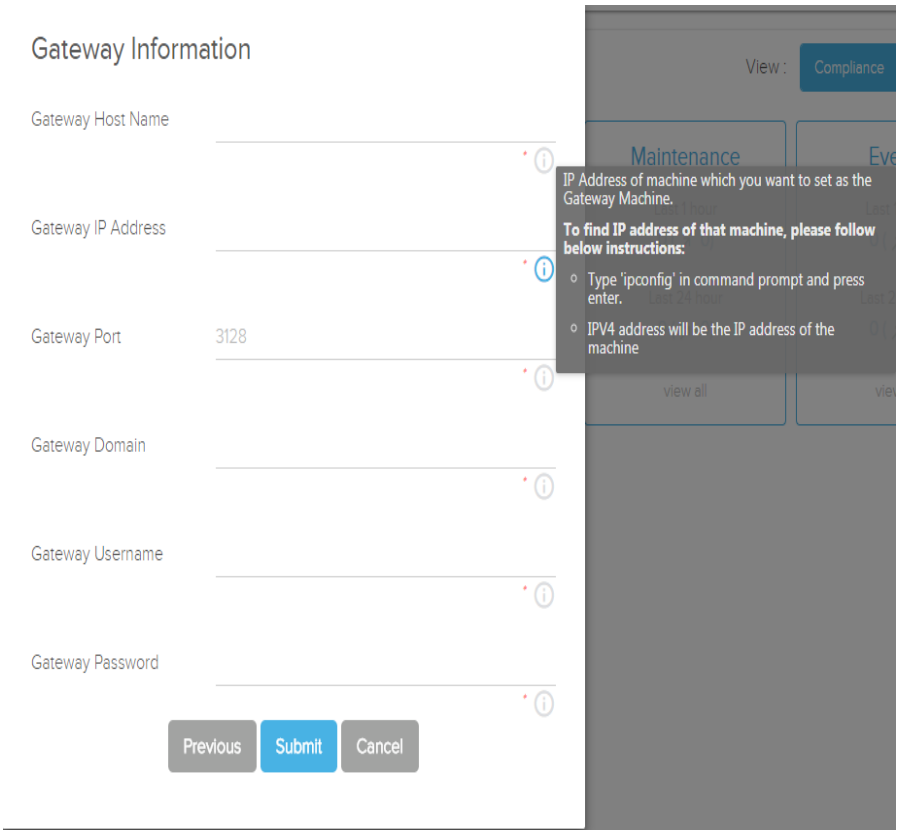
    a. Right click on my computer, name will be the hostname of the machine

    b. Type 'hostname' in command prompt and press enter

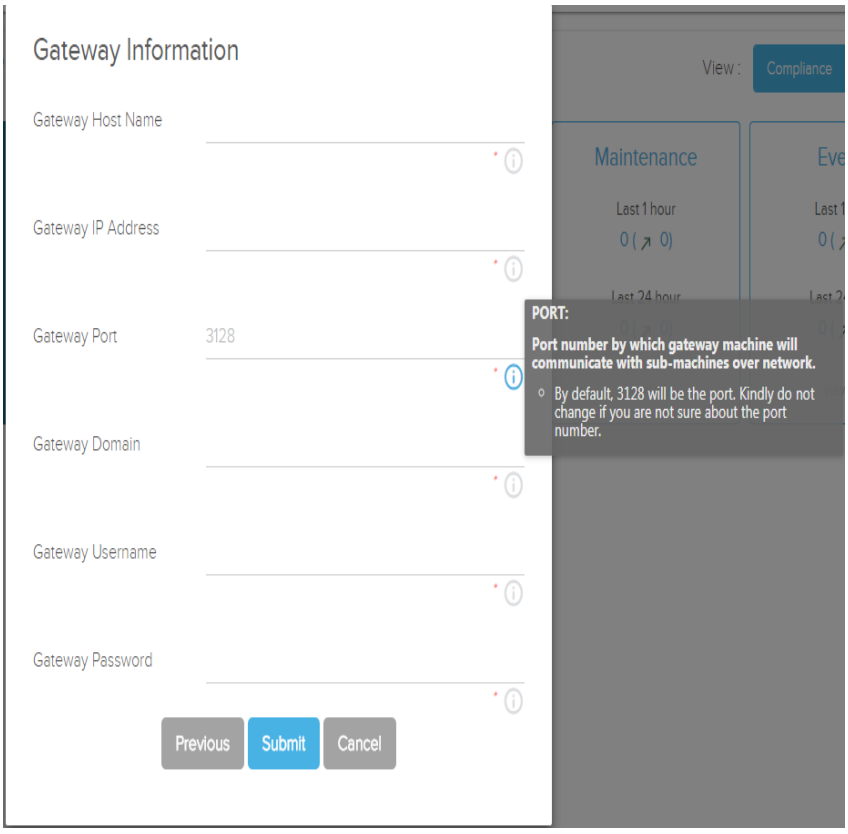


2. IP Address: IP Address of machine which you wants to set as the Gateway Machine. To Find IP address of that machine, please follow below instructions:

    1. Type 'ipconfig' in command prompt and press enter. IPV4 address will be the IP address of the machine

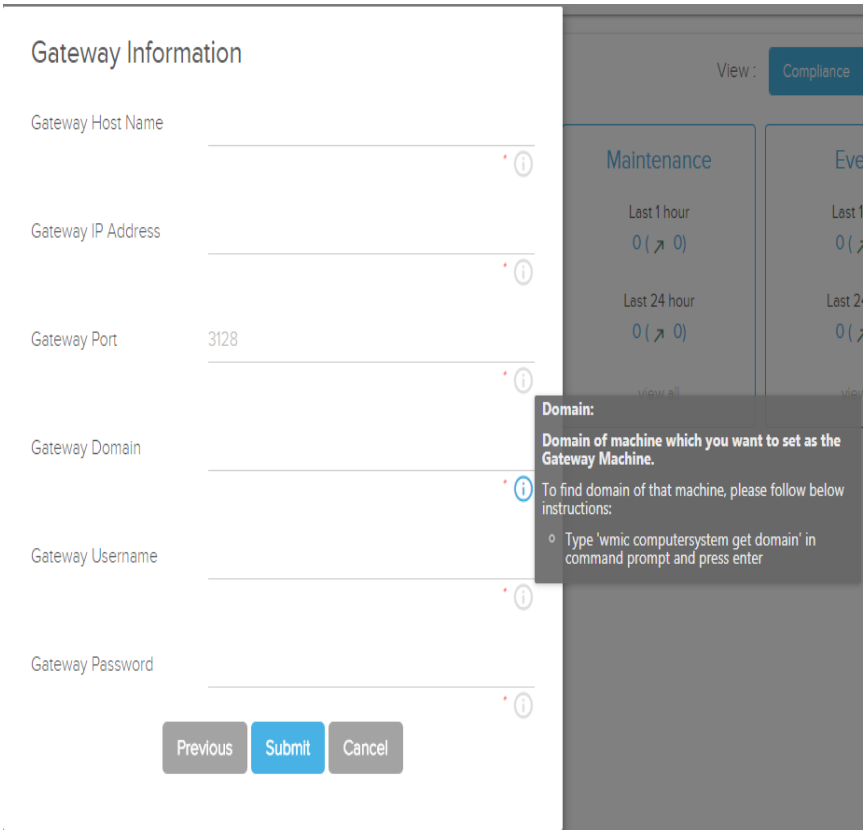


3. PORT: Port number by which gateway machine will communicate with sub-machines over network. By default, 3128 will be the port. Kindly do not change if you are not sure about the port number.

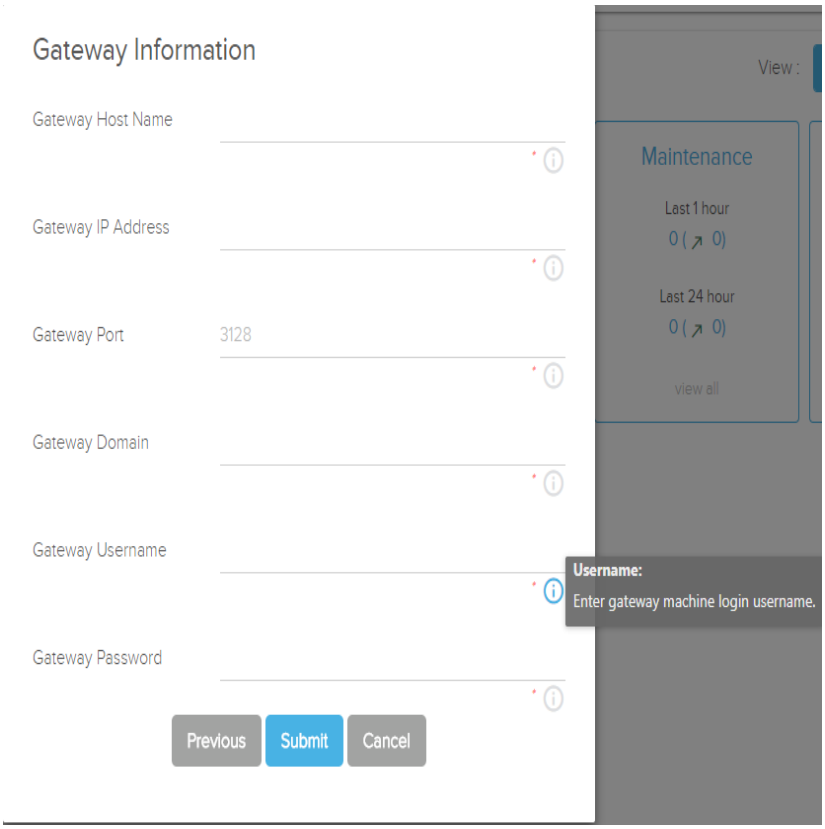


4. Domain: Domain of machine which you wants to set as the Gateway Machine. To find domain of that machine, please follow below instructions:

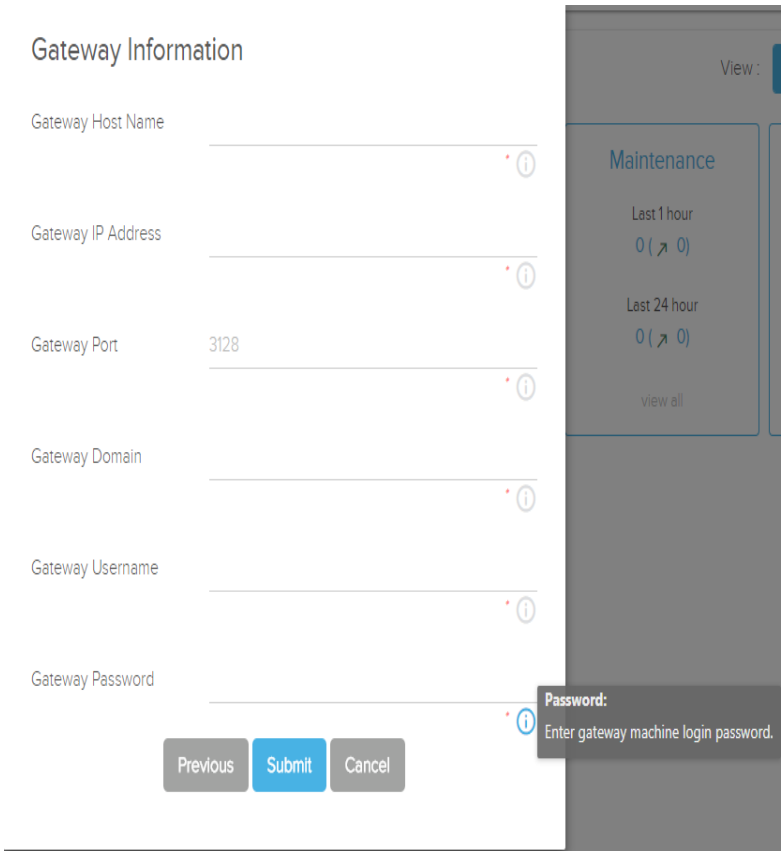
   1. Type 'wmic computersystem get domain' in command prompt and press enter



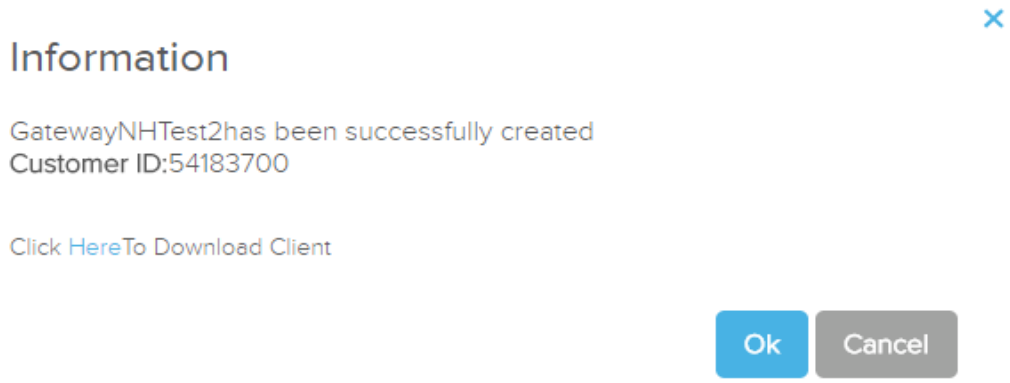
5. Username: Enter gateway machine login username.



6. Password: Enter gateway machine login password.

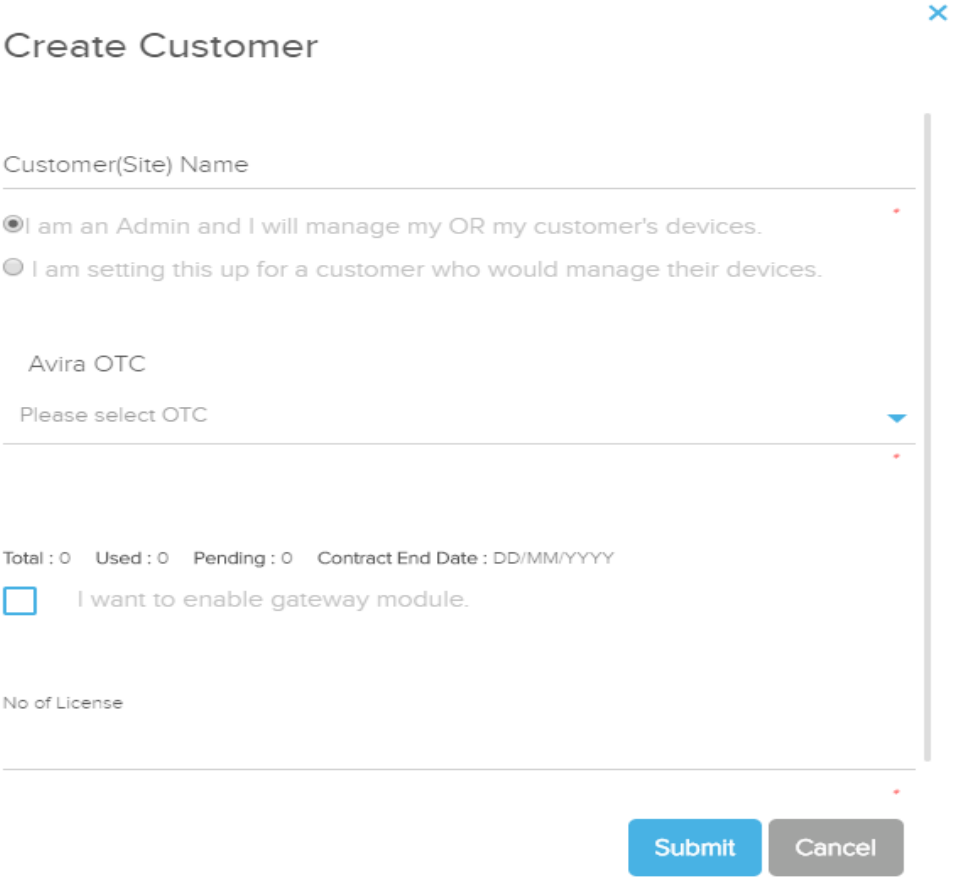


Then it will generate the download URL as shown below:

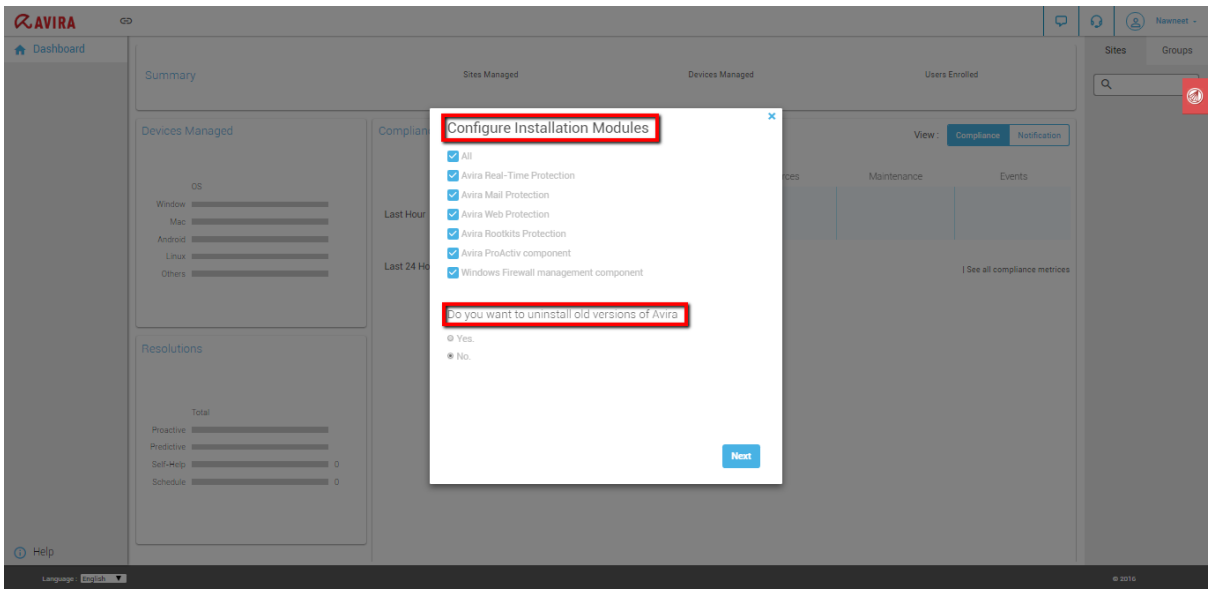


Customer has to use the above download link to download and install client in the **gateway machine only**. Once client is installed, Customer has to use deployment feature to install client on other machines of the same network which are not having internet.

2. I am setting this up for a customer who would manage their devices
    a. The user will see a popup as shown below, wherein he has to enter:
        i. First Name of the customer
        ii. Last Name of the customer
        iii. Email of the customer



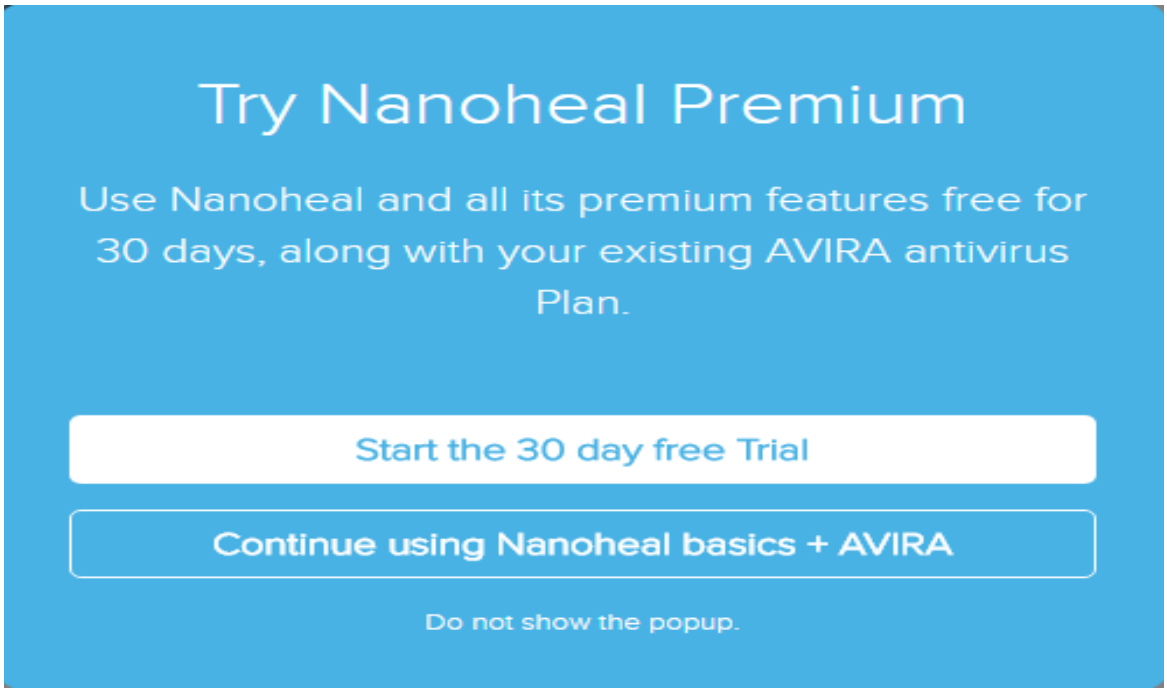
b. Click on "Verify" to verify the OTC and then popup will come to select Avira modules to be installed as shown below:



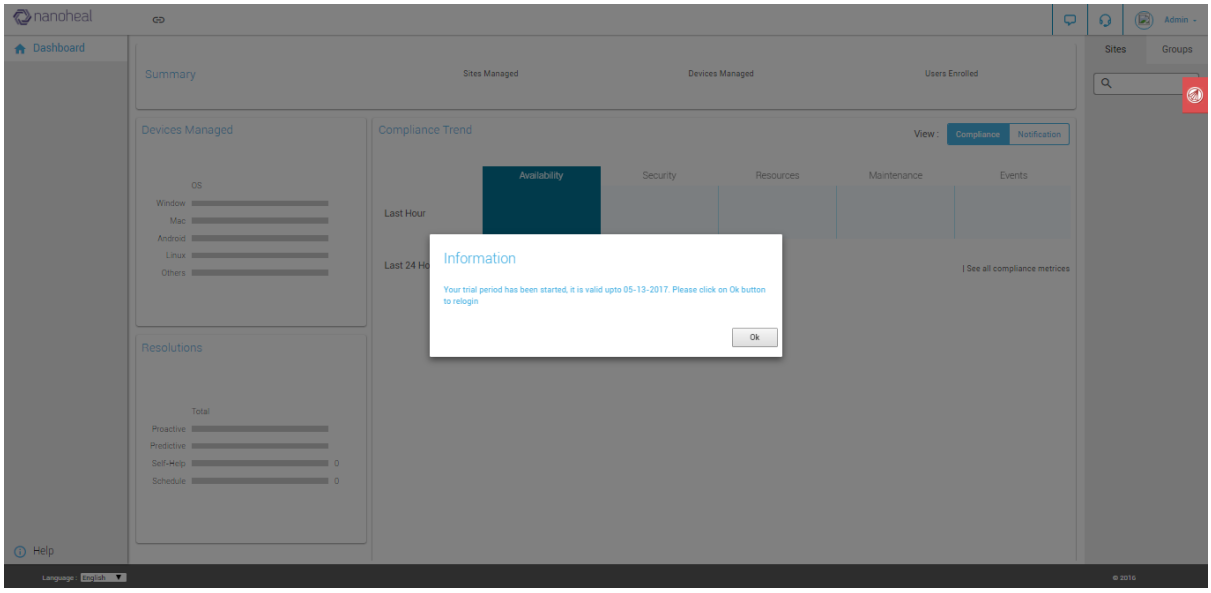
c. Click on next will send the download URL link and reset password link to the given customer mail id.

Trial Flow

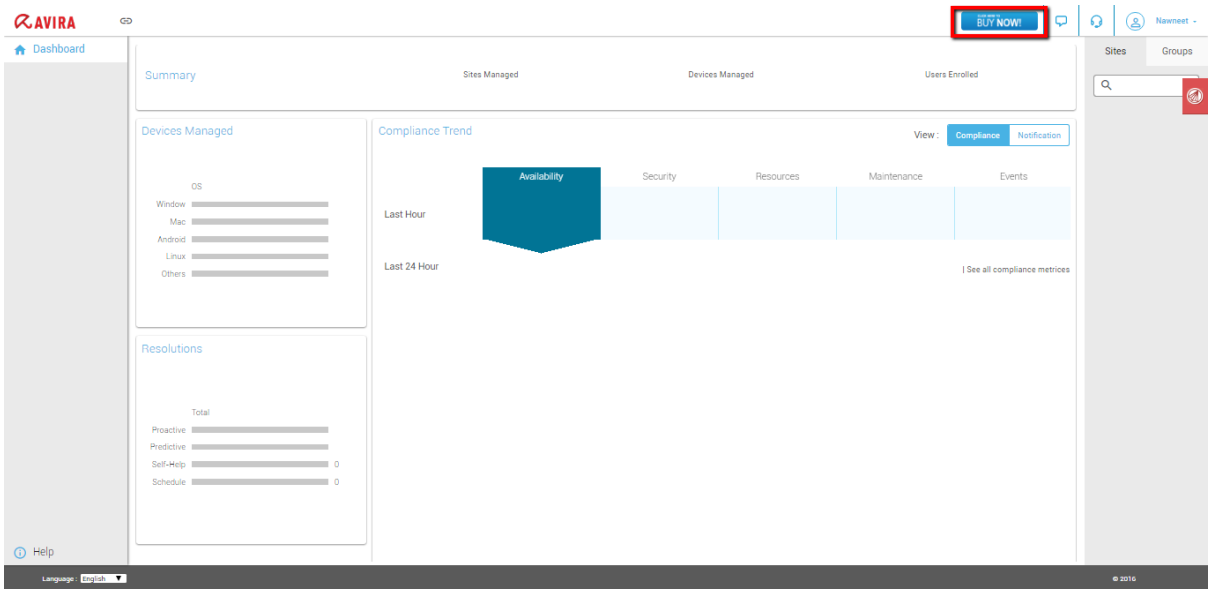
Once the customer has been created, trial flow pop up shows up on the screen and it Let's the resellers use Nanoheal and its features free for 30 days as shown below:



Upon the click of *Start the 30 days Trial*, an Information dialog comes up as shown below:

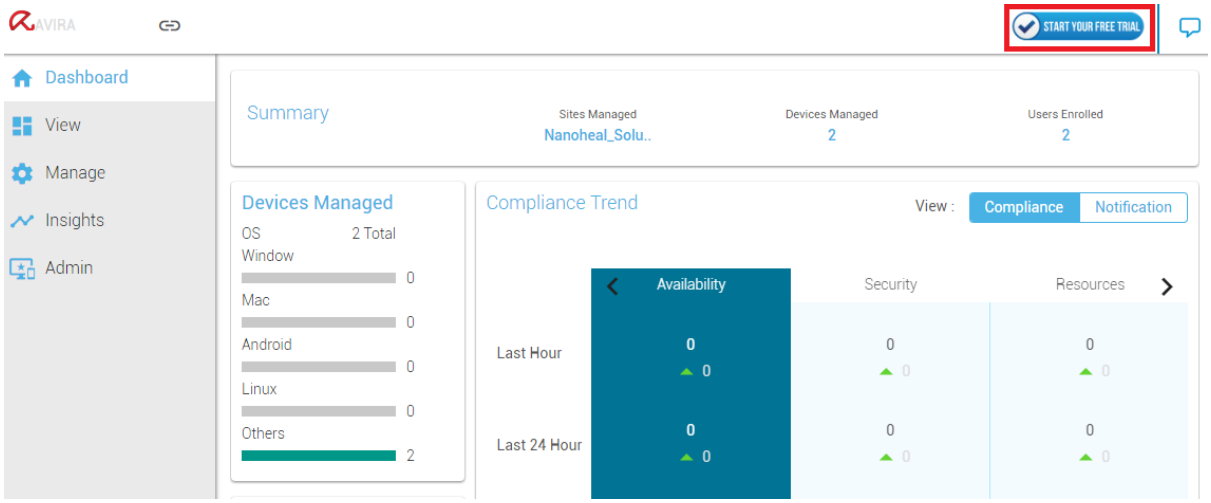


During trial flow period, customer can also buy the product anytime by clicking on *Buy Now* button available on the top as shown below:



Click on buy now will redirect to "https://nanoheal.com/contact/" page where customer can drop a request and nanoheal sales team will contact them for further processing.

If the customer selects "*Do not show this popup*" option, then Start your trial flow option will come at the top of the home page as shown in the diagram below



NH Pre-Requisites

The following requirements must be met before deploying Nanoheal in an environment:

Minimum System Requirements

Windows (Laptops/Desktops)

- 1 GB of RAM , 333 MHz CPU or greater
- 30 MB of free disk space
- Network Interface Card (NIC) or modem
- Windows XP, Vista, Win 7, Win 8, Win 8.1, Win 10

Application exception list in Anti-virus software installed in the managed device

- C:\Program Files\Nanoheal - This folder needs to be excluded from AV application.
- Also, the below mentioned files are to be added into SONAR and Runtime exception:

EXE file information:

- C:\Program files\Nanoheal\Client\capp.exe
- C:\Program files\Nanoheal\Client\cust.exe
- C:\Program files\Nanoheal\Client\cutil.exe
- C:\Program files\Nanoheal\Client\dmidecode.exe
- C:\Program files\Nanoheal\Client\downloader.exe
- C:\Program files\Nanoheal\Client\intfr.exe
- C:\Program files\Nanoheal\Client\MessageBox.exe
- C:\Program files\Nanoheal\Client\progressBar.exe
- C:\Program files\Nanoheal\Client\provwrap.exe
- C:\Program files\Nanoheal\Client\RealtimeProtection.exe
- C:\Program files\Nanoheal\Client\rerun.exe
- C:\Program files\Nanoheal\Client\srtct.exe
- C:\Program files\Nanoheal\Client\srvc.exe
- C:\Program files\Nanoheal\Client\32bit\capp.exe

DLL File information:

- C:\Program files\Nanoheal\Client\bdardrv.dll
- C:\Program files\Nanoheal\Client\bdquar.dll
- C:\Program files\Nanoheal\Client\BDUpdateServiceCom.dll
- C:\Program files\Nanoheal\Client\gzfltum.dll

- C:\Program files\Nanoheal\Client\libeay32.dll
- C:\Program files\Nanoheal\Client\NanohealPasswordReset.dll
- C:\Program files\Nanoheal\Client\NanohealPasswordResetXp.dll
- C:\Program files\Nanoheal\Client\nfapi.dll
- C:\Program files\Nanoheal\Client\nfapinet.dll
- C:\Program files\Nanoheal\Client\PcaFilterApi.dll
- C:\Program files\Nanoheal\Client\pfapinet.dll
- C:\Program files\Nanoheal\Client\ProtocolFilters.dll
- C:\Program files\Nanoheal\Client\scan.dll
- C:\Program files\Nanoheal\Client\sqlite3.dll
- C:\Program files\Nanoheal\Client\sqlite64.dll
- C:\Program files\Nanoheal\Client\ssleay32.dll
- C:\Program files\Nanoheal\Client\trig.dll
- C:\Program files\Nanoheal\Client\trig00.dll
- C:\Program files\Nanoheal\Client\trig000.dll
- C:\Program files\Nanoheal\Client\trufos.dll
- C:\Program files\Nanoheal\Client\32bit\trig00.dll
- C:\Program files\Nanoheal\Client\i386\nwapi.dll

Files to be whitelisted from temp location:

C:\Users*\AppData\Local\Temp:

- Downloader.tmp
- inst64.tmp
- inst32.tmp

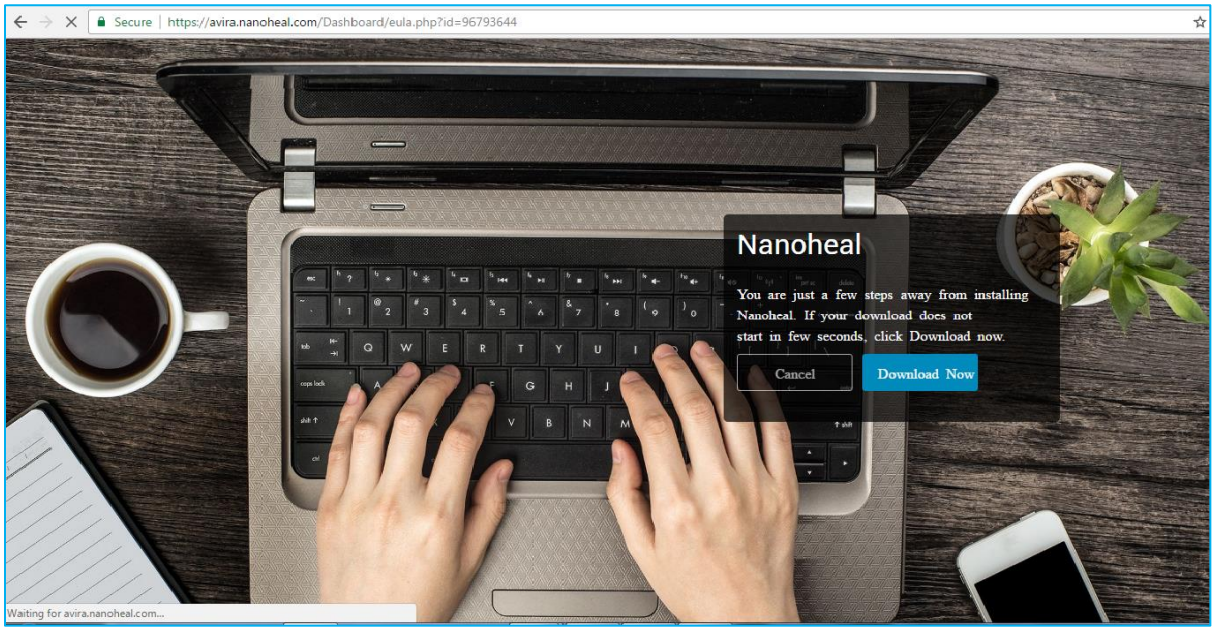
Firewall/Proxy unblock

URLs to be whitelisted

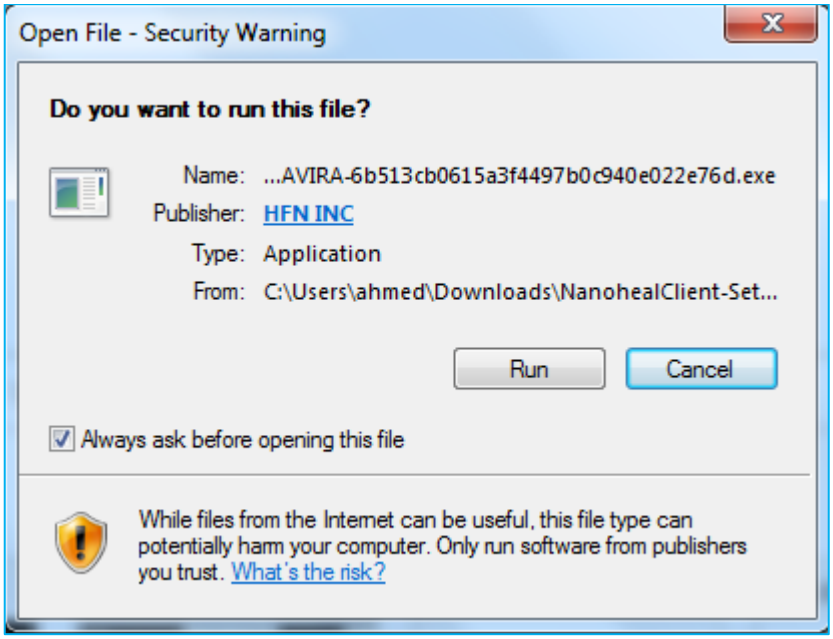
- *. nanoheal.*
- Ports to be whitelisted for the URL *nanoheal.*
- 443 (For secured software agent–server communication)
- 80 (for regular access)
- Nanoheal certificate and content from Nanoheal URLs needs to be allowed under the target environment.

Download-Install flow

The download URL would download and install the Nanoheal and the AVIRA clients. The following series of screens would appear upon clicking the URL:

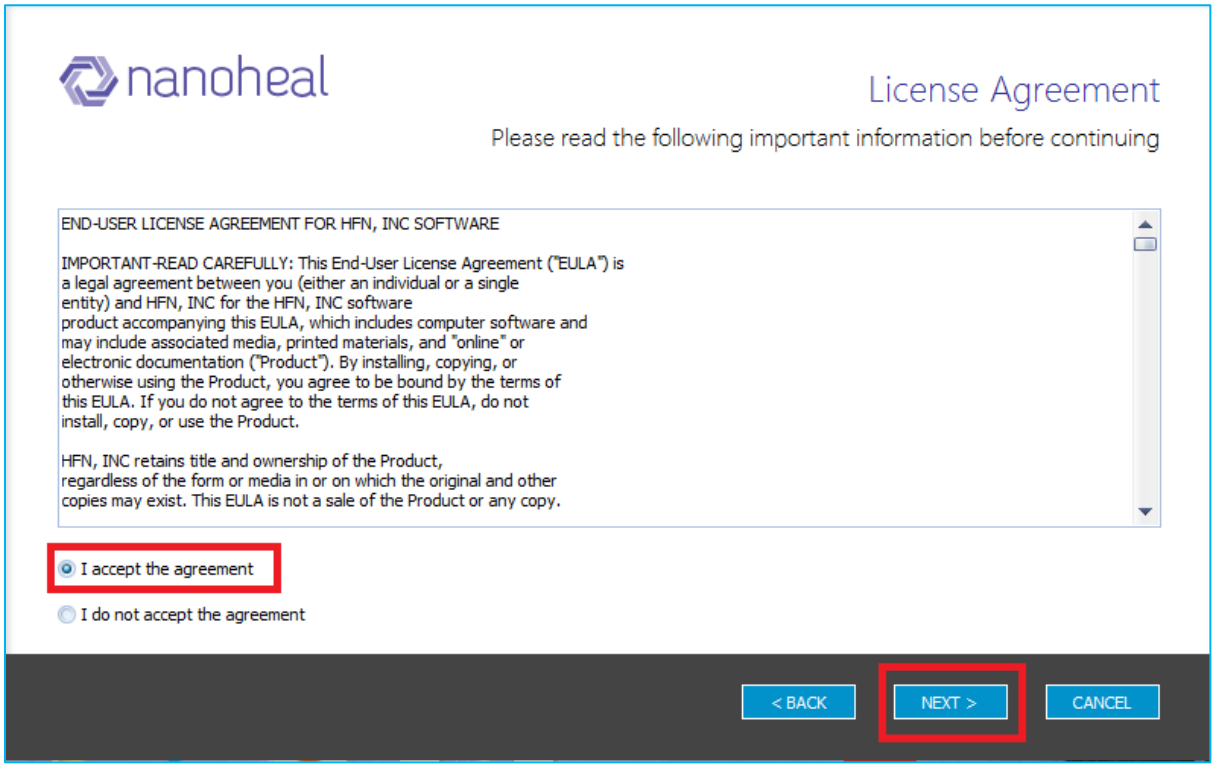


The following screen would appear once Nanoheal download is complete and you double click on downloaded exe to install.

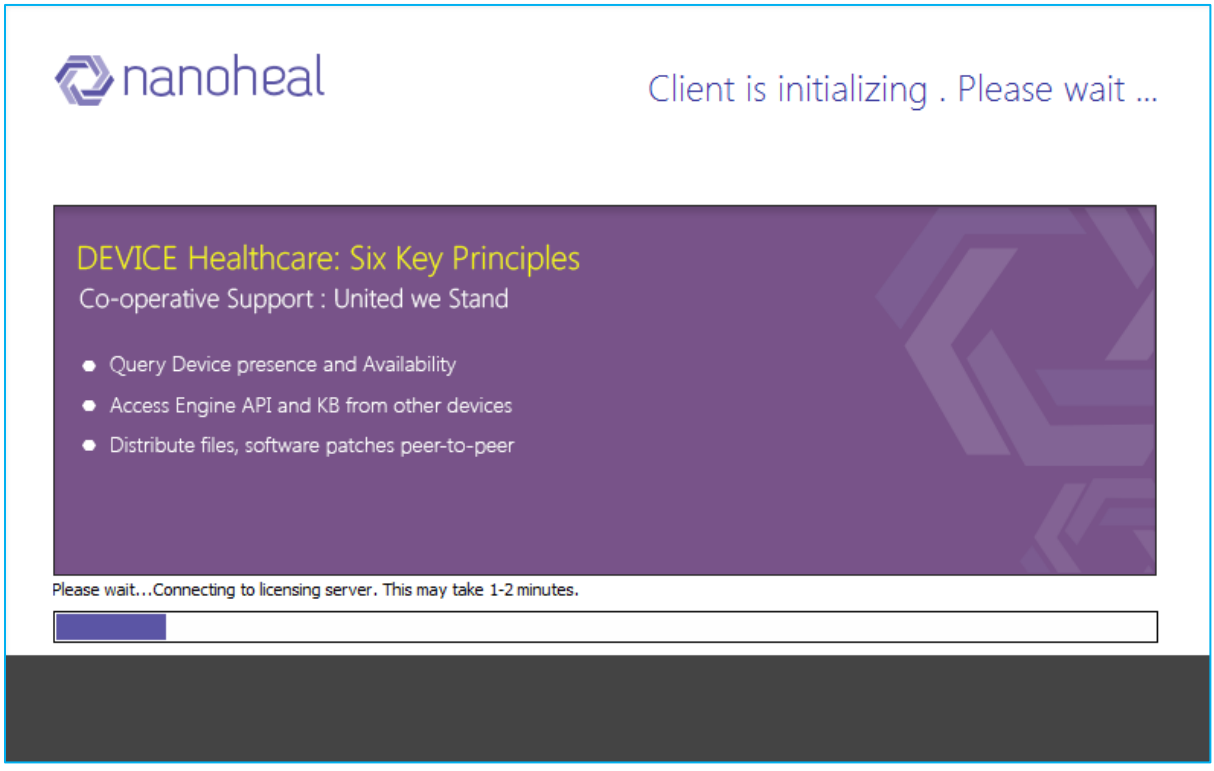


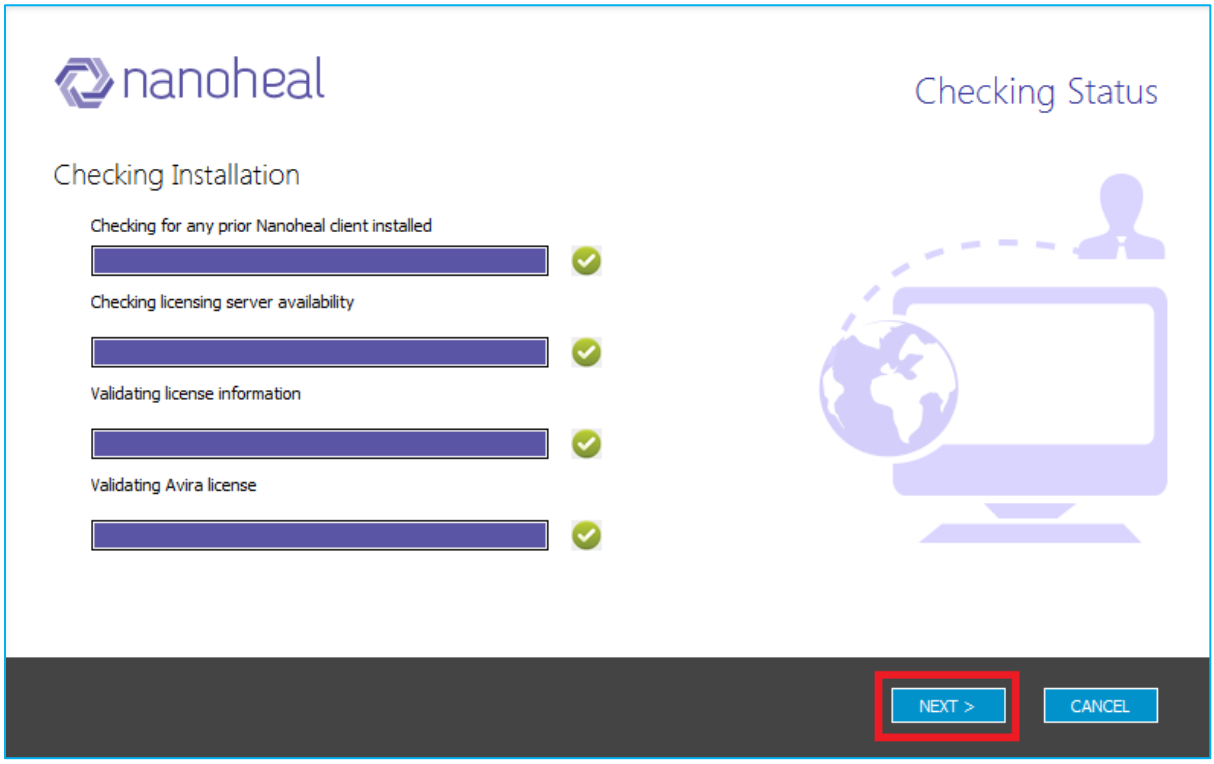
The above screen might take 4-5 minutes of time to come if it is a gateway machine as Squid Software will get downloaded and installed first and then nanoheal installation will get triggered.

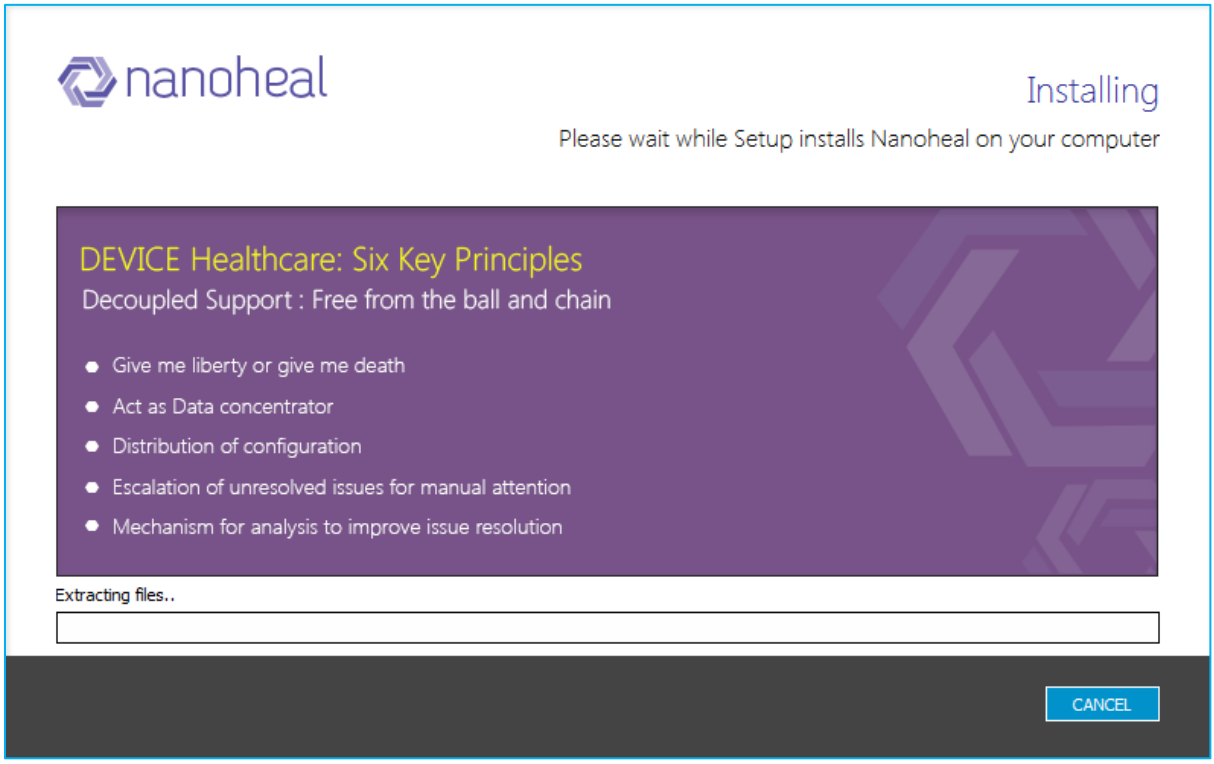
The user would need to accept the agreement at this stage:



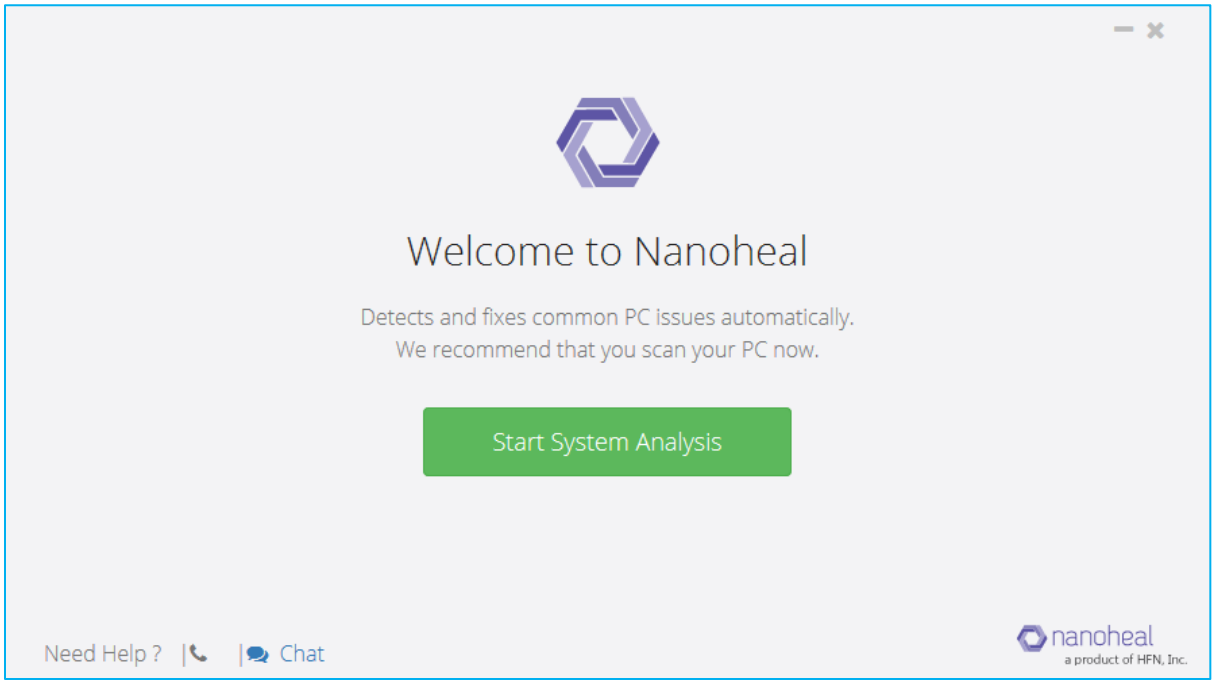
The following two screens would indicate that the installation is under process:







A complete and successful installation would result in the following screen:

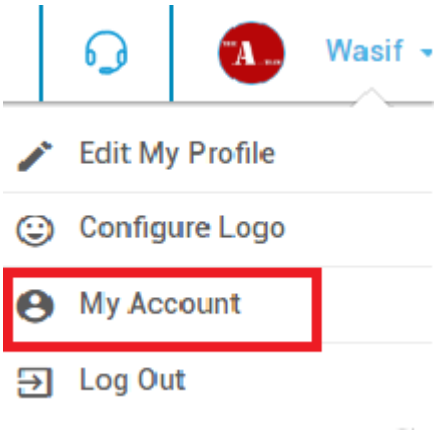


My Account Page

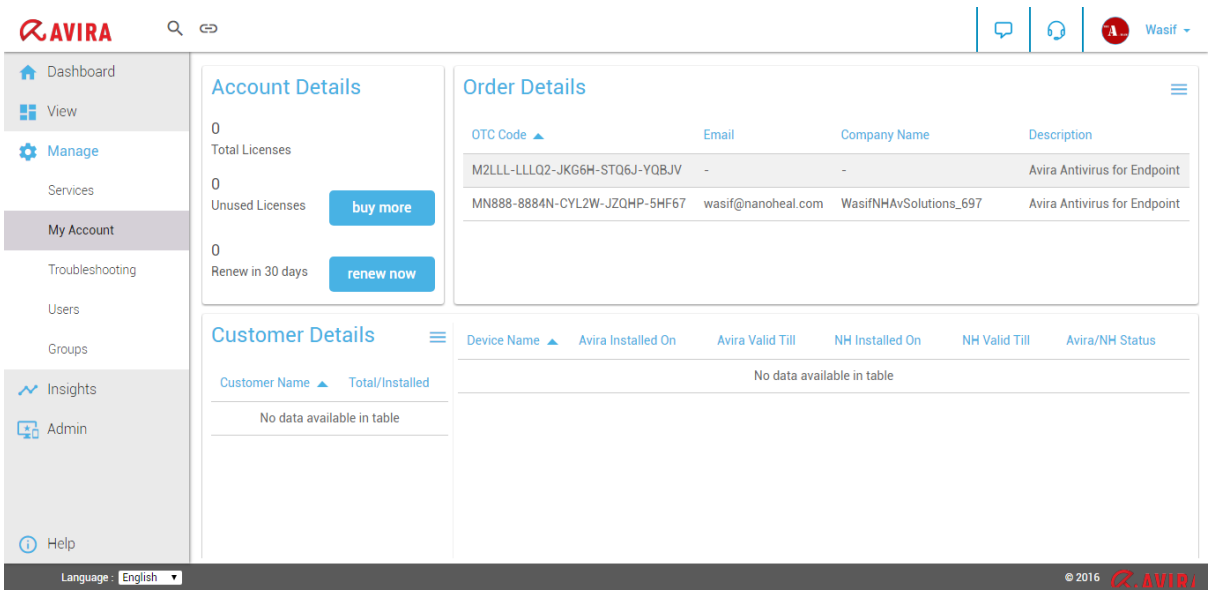
The My Account page depicts the following:

1. Account Details
2. Order Details
3. Customer Details

2. In order to navigate to the My Account Page, the user would need to click on the Account Name at the top right corner and select "My Account" from the drop down menu:



Upon selecting "My Account", the My Account page would appear, as shown here.

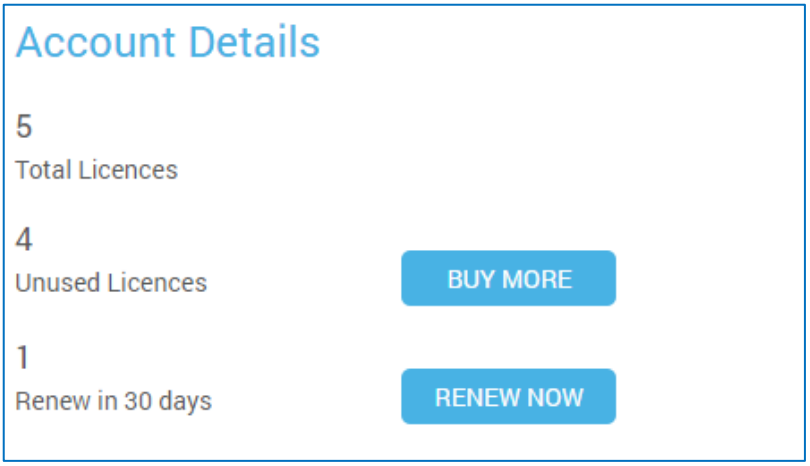


Account Details

The Account Details section of My Account Page shows the following information:

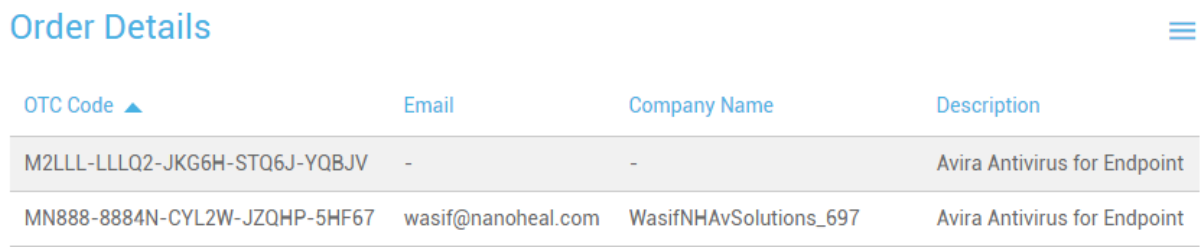
- Total Licenses
- Unused Licenses
- Renew in 30 Days

The user can buy additional NH licenses by clicking on the "Buy More" button and renew by clicking on "Renew Now" button:



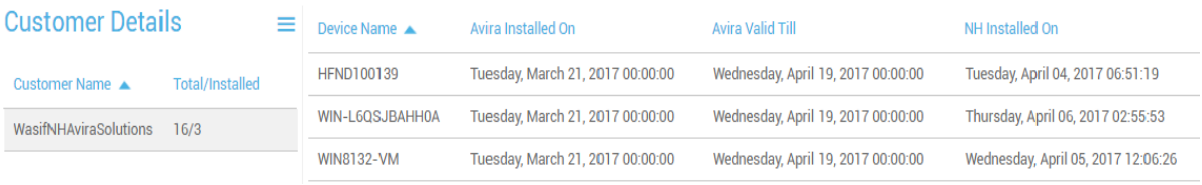
Order Details

The Order details section of My Account Page shows information about the OTC Code, Email Address, Company Name, Description and Licenses

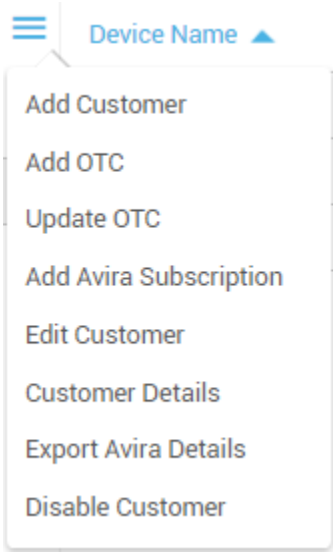


Customer Details

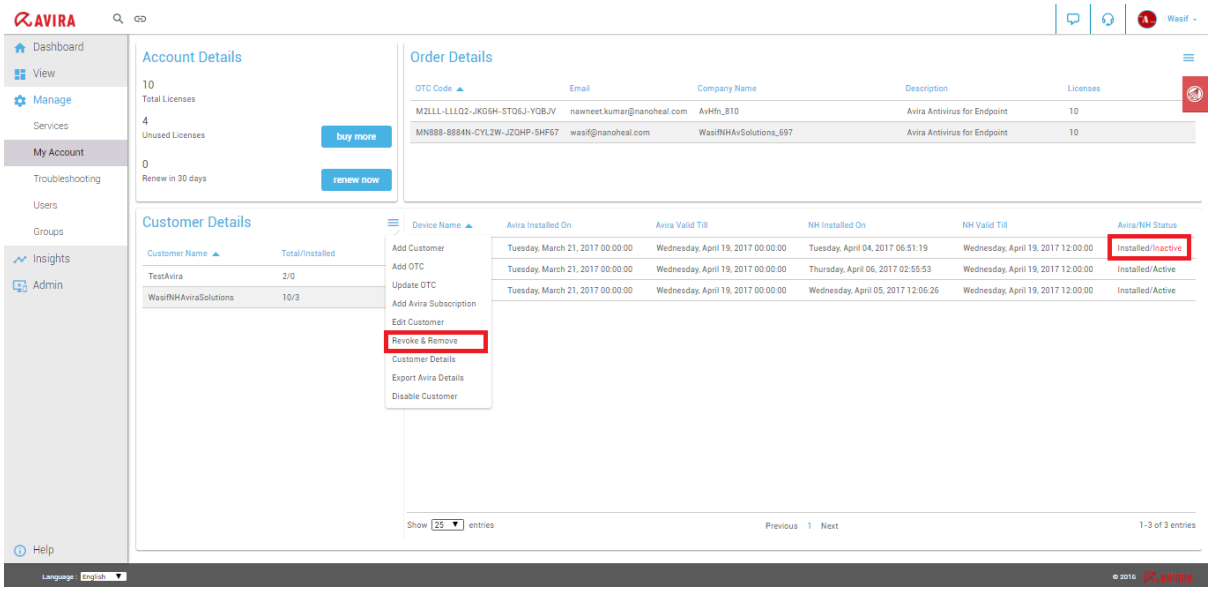
The Customer Details section of My Account Page shows information about Customer Name, Total/Installed, Device Name, Avira Installed on[date], Avira Valid Till and NH installed date.



Customer Details also has the following options:



If there is any machine where nanoheal has been uninstalled and the machine status changes to inactive, then customer will get an option to revoke and remove those machines in customer details section as shown below:



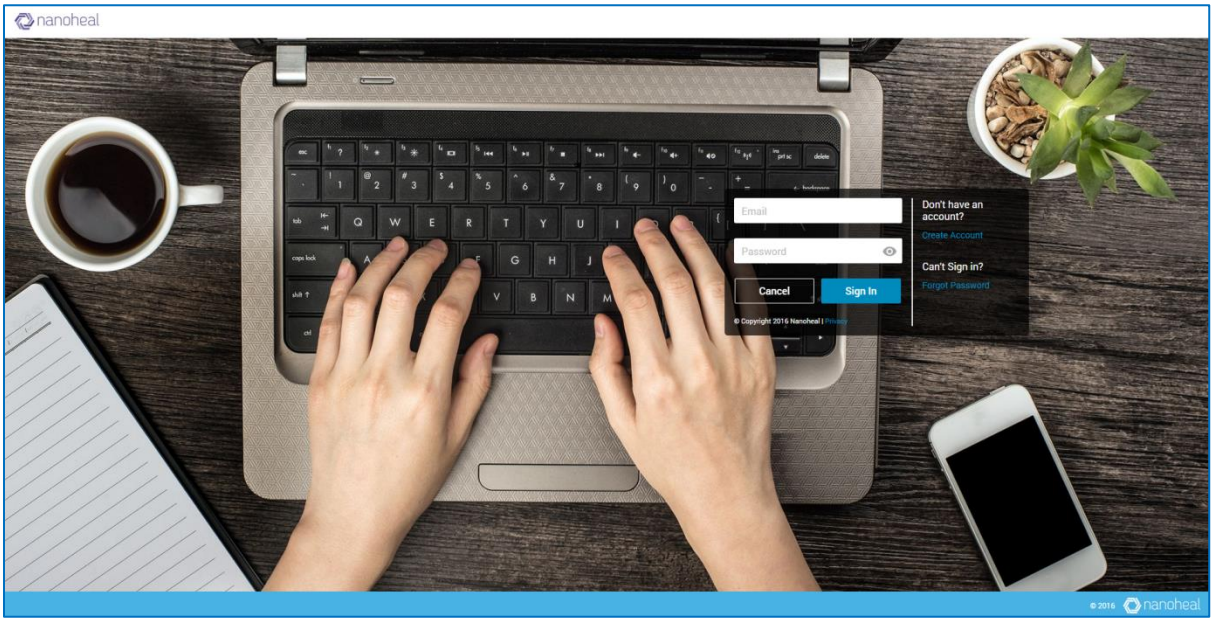
These options have been further explained under – "Manage a Customer"

Getting started with Dashboard

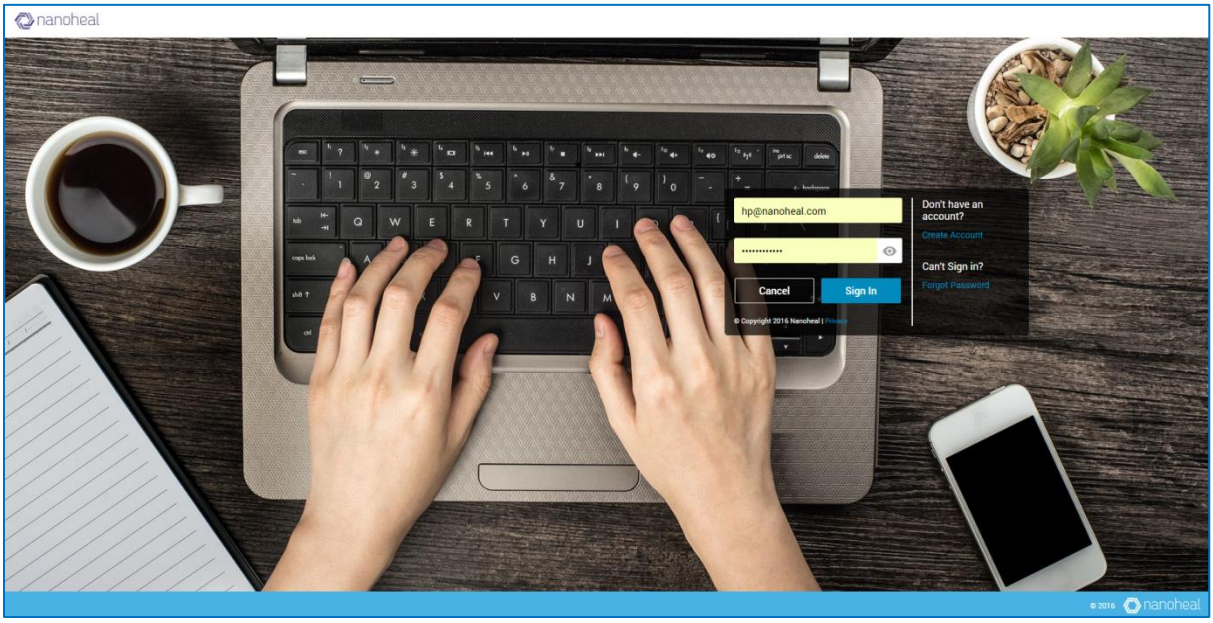
Sign In

The following steps need to be followed to Sign in to Dashboard.

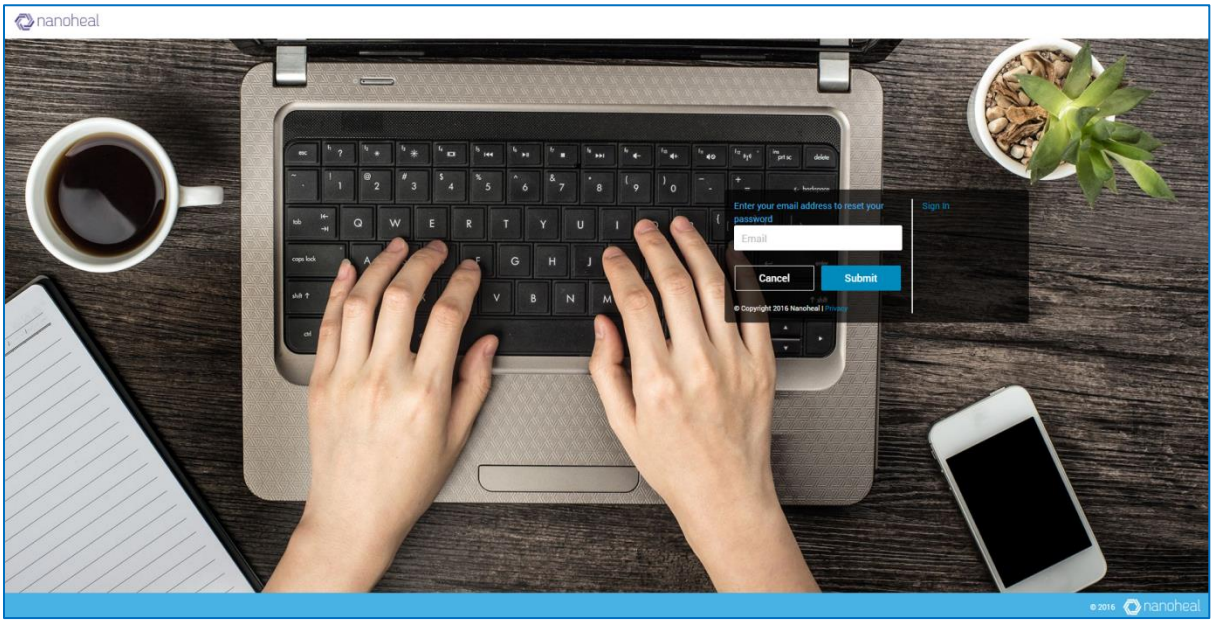
1. User needs to click on the link provided to access a page that looks similar to the one shown below:



2. Enter the sign in credentials and click on sign in.



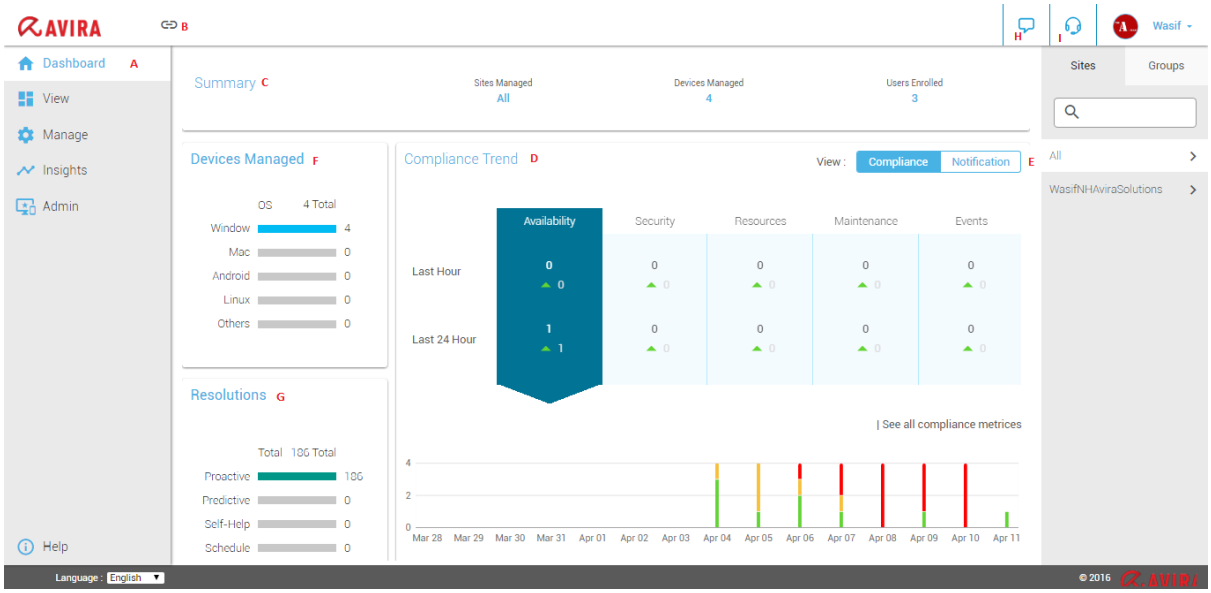
3. If the user has forgotten their password, they can retrieve it by clicking on "Forgot Password" link and entering their email address to get the password reset link by email.



Understanding Dashboard Layout

Dashboard landing page, which is also referred to as the Dashboard Home page in this manual provides a brief overview on the Summary (Sites/Devices Managed), Compliance, Notifications, Resolutions.

Home page of dashboard has been divided into 9 portions as shown in the screenshot below.



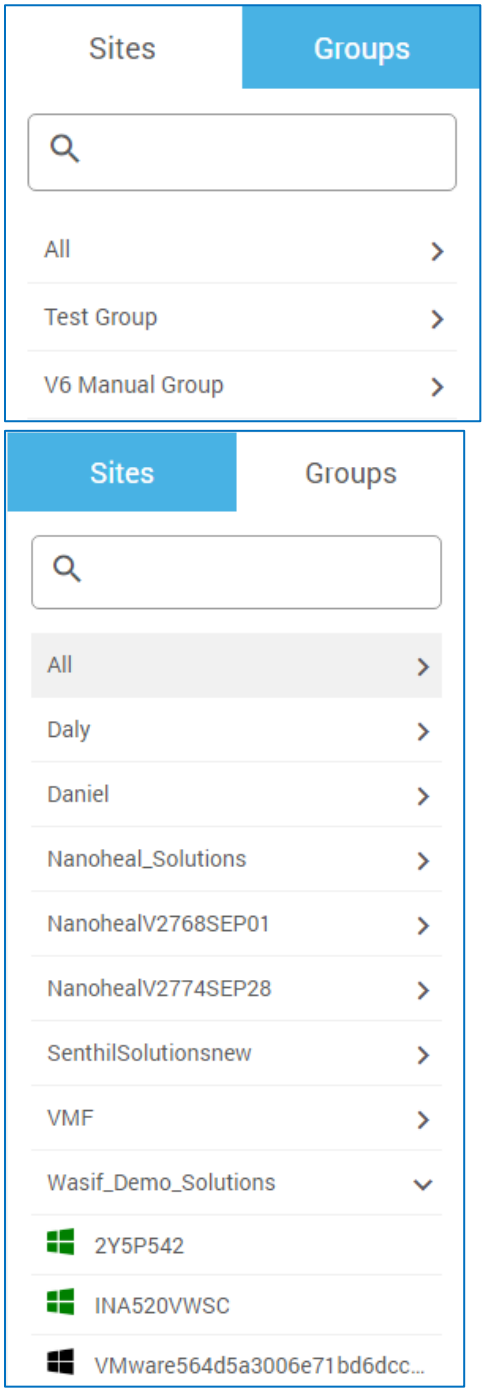
The Home Page consists of -

- **A - Left Pane (Module list)** – Left Pane is available at the left side of all pages across Dashboard. This will display all the modules available on the Dashboard and click on each module will display its corresponding sub modules.
- **B – Breadcrumb Links** – Following Breadcrumb links are available: Event Information, Asset Information, Deployment, Manage Customers
- **C – Summary** – This will display the count of total number of sites managed &attached to the server, Current selected All/Site/Machine/Group Name, Total number of Devices Managed & Total number of Users Enrolled.
- **D & E – Compliance & Notification Trend** – In this, we would be creating compliance rules for end point devices, which they should adhere to at all times. These rules can be for end point system hardening, availability or for maintenance & up keep. The help topics in this section describe how to navigate and access various options. Section I is for toggling between Compliance Trend and Notification Trend.
- **F – Devices Managed** – This will display the individual count of machines across all OS namely Windows, Android, MAC, iOS & Linux.
- **G – Resolutions** – This will display the count of Predictive & Proactive Resolutions.
- **H - Chat** - This will redirect you to nanoheal chat site.
- **I - Support** - This will redirect to nanoheal support.

Dashboard Data

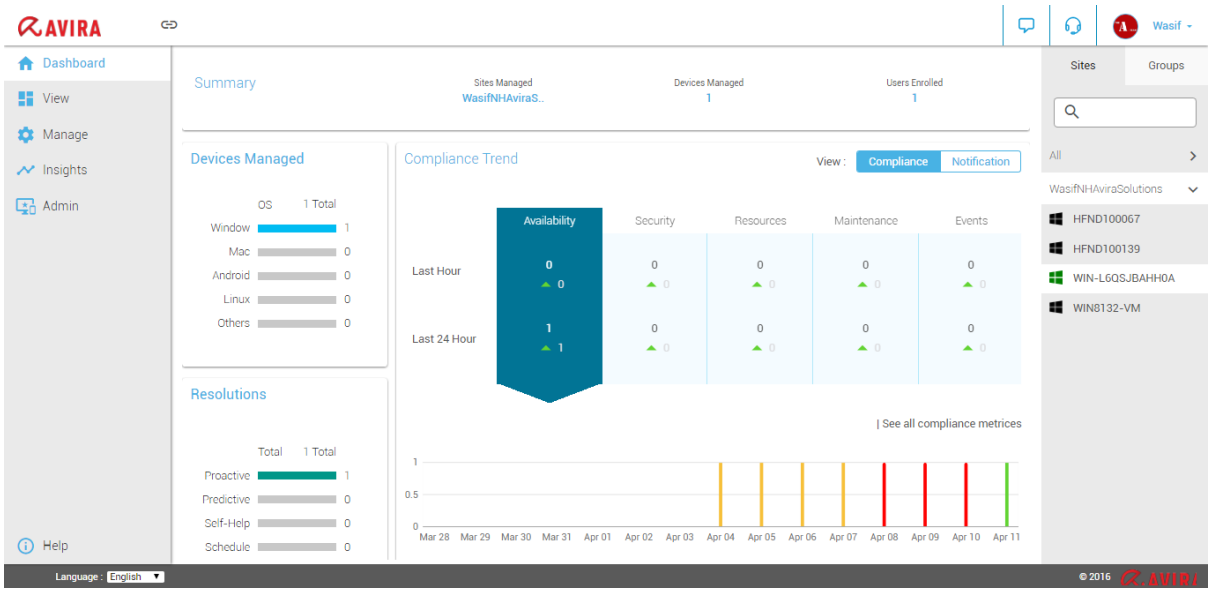
On the top right corner of almost all pages in Dashboard, we have the "**Site Pane**" which will allow the user to perform any dashboard operations at overall level or site level or machine level or group level. Once the user selects an appropriate option, the entire data on the Nanoheal Dashboard gets drilled down based on that option.

For instance, if user selects one site on the Search screen- the Dashboard data will be shown for that site. Click on "Sites" and it will display list of sites along with "**All"** option. Here "**All"** option will show the data for all sites in Dashboard. *However, the user cannot take "actions" at the "All" level*. Upon clicking a Site Name, the list of machines attached to that site will be displayed. Upon clicking "Group", the list of groups gets displayed. Choosing appropriate options will load Dashboard data based on that. Images below show a snapshot on how to drill-down to site / machine level.

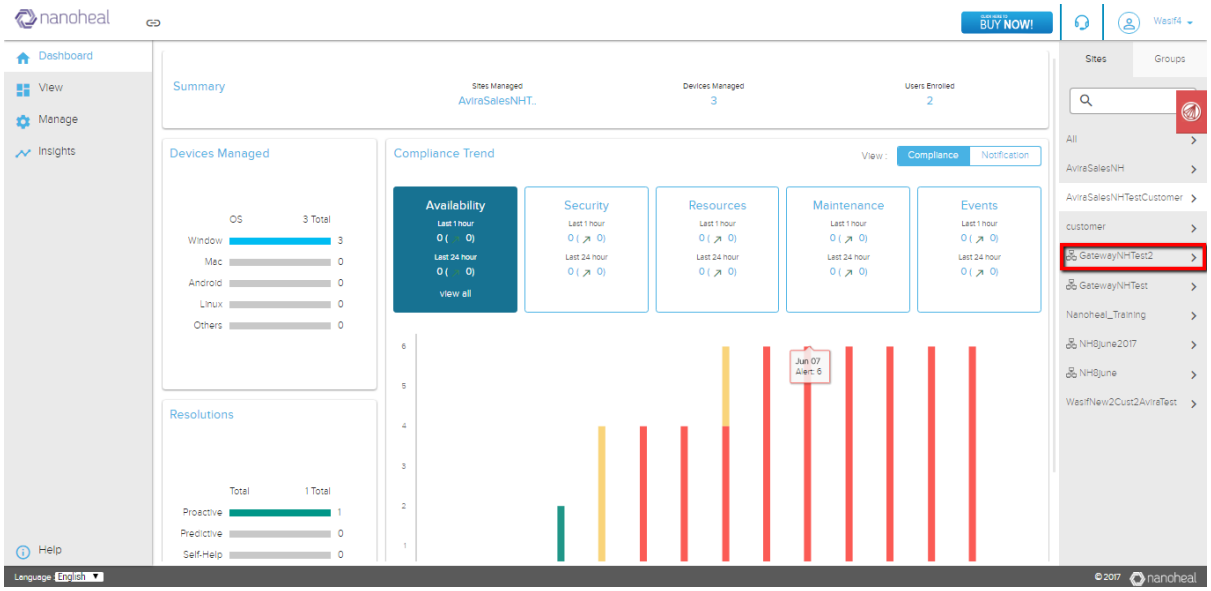


As shown in the screenshot below, based on user selection (machine level / site level / group level / all level in Sites or Groups), corresponding data would be shown only for those machines.

For instance, if user selected one machine in Search, then entire dashboard data (Notification, Stats, graph etc.) will be shown only for that particular machine.



If there is any gateway machine in any site then an icon will get displayed in-front of the site name as shown below:



The icon before the site name means that atleast one machine in the site is a gateway machine.

Home Page Statistics

The statistics about the total devices (machines) managed under a given site by Nanoheal, issues reported by them and the resolution status are shown here.

Per-All/ Site/ Group/ Machine level statistics related to following items would be displayed:

1. Compliance % for Availability, Maintenance, Events, Security & Resources
2. Notification Count of total number of notification along with %. (Priority 1, Priority 2, Priority 3, Priority 4, Priority 5)
3. Total number of Devices Managed.
4. Total number of Resolutions (Predictive & Predictive)

Instead of the site, if user selects all / machine / group, then the above data gets loaded based on machine / group level.

Sites

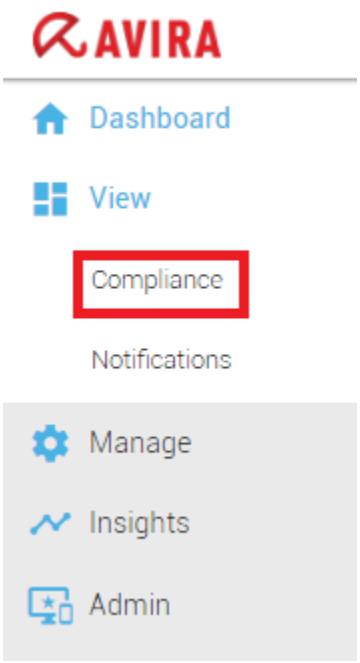
A site is a location (physical or logical) with which a user wants to associate their endpoints, which are managed using Nanoheal. Site can be Country, City or a Building, depending upon the way the user would want to classify the endpoints.

This module will list out the number of machines available in a particular site / group. It will show the number of machines based on the OS. Like Windows, Android, Linux and MAC.

Compliance

The Compliance section is used to set a compliance baseline and to handle any compliance variances.

The Compliance section can be accessed through the left panel as shown below



Compliance is classified into 5 sections. Each of these sections have rules which should be met to deem a device, compliant. Examples of these rules are given next to each of the sections.

1. Availability
2. Security
3. Maintenance
4. Resources
5. Events

1. Availability
   EG-Under availability, a **Machine is compliant if:** Nanoheal has reported at-least once in the last 4 hours

2. Security
   EG-Under security, a **Machine is compliant if:** Anti-virus definition update was attempted 0 times in the last 60 minutes

3. Maintenance
   EG-Under maintenance, a **Machine is compliant if:** The disk defragmenter was run at-least once in the last 30 days and there is no other antivirus program on the computer other than "Windows Defender", etc.

4. Resources
   EG-Under resources, a **Machine is compliant if:** Free space on OS Drive (disk drive on which the OS is installed) is more than 30% of total space and there are no media files (.mp3, .wav, .avi, .mpeg, .3gp, .mp4) of size more than 500 MB

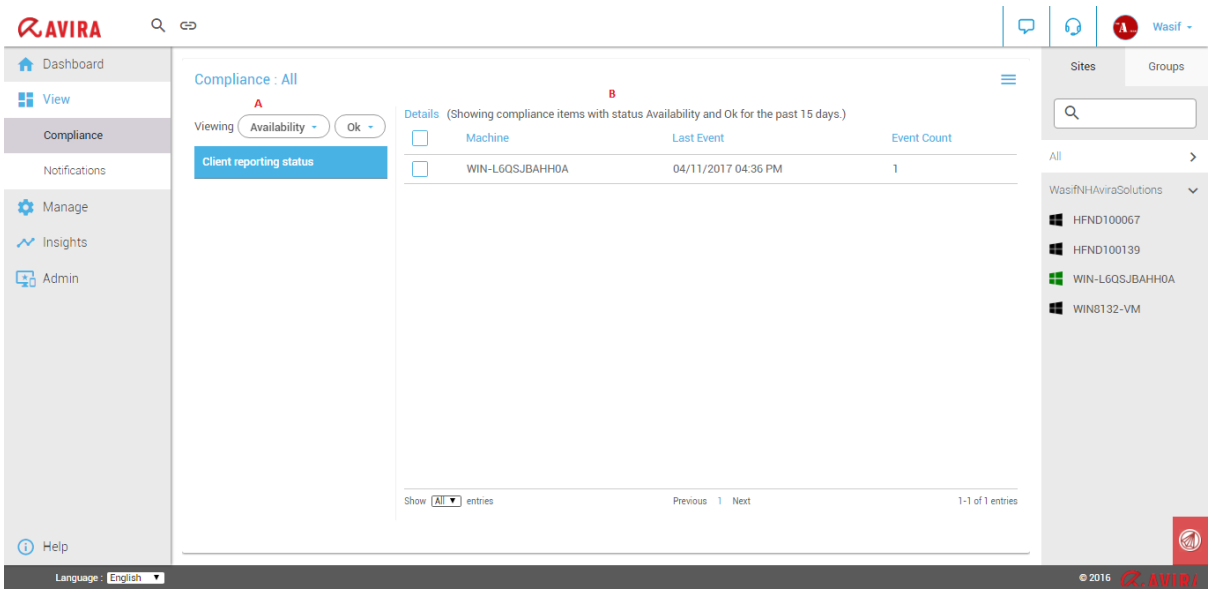
5. Events
   EG-Under Events, we say that a "**Machine is compliant if:**" The system was Shut down or Restarted in the last 15 days

As mentioned above, there could be one or many criteria to be met to deem a machine complaint.

NOTE: Please contact the Nanoheal Team to add new Compliance criteria

To navigate to the compliance screen, the user can click on - **Dashboard** > **Compliance** on the left pane.

As shown below:



A Compliance Criteria, B Compliance Data for the selected criterion

The Compliance screen is split into 2 parts: The Compliance Items on the left & the corresponding Compliance on the right.

By Default, the 1st criterion will be selected as shown in the screenshot above.

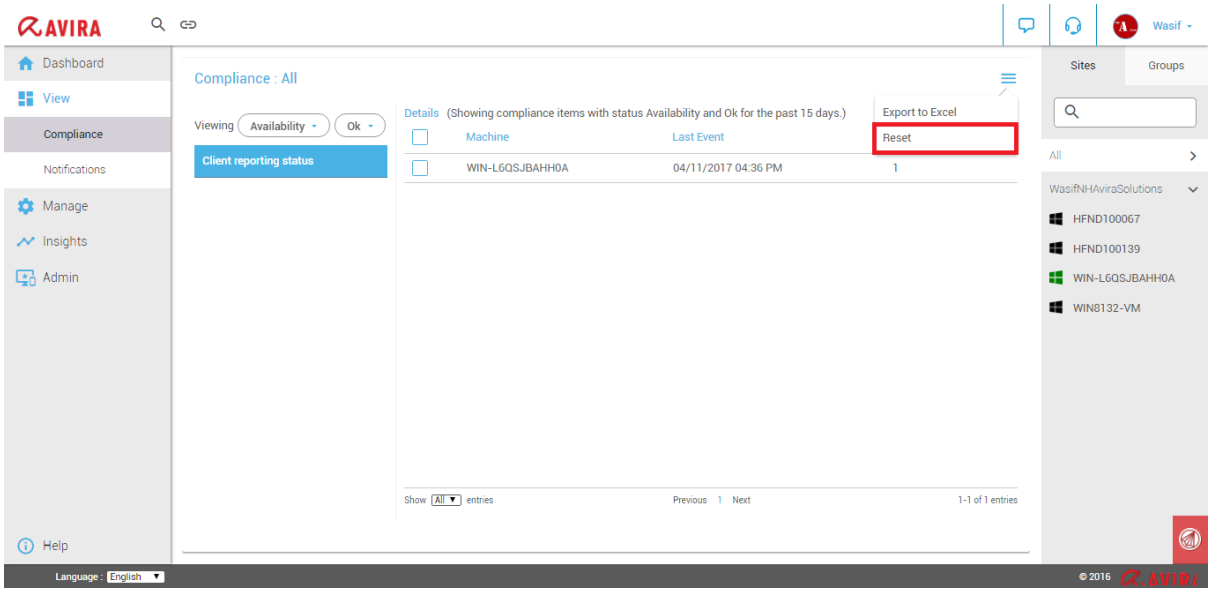
Each Compliance category falls under "Warning" / "Alert" / "Ok" buckets.

As explained above, the Compliance screen will show the data (if available) across all the 5 service categories. Namely - Availability, Security, Resources, Maintenance & Event. Data would be displayed under relevant categories like - "OK" / "Warning" / "Alert". Count for each category will be seen at the top left corner of each tab of "OK" / "Warning" / "Alert". Count will be prefixed with these tab items as shown above.

As shown in the screenshot above, left hand side shows different categories & criteria name. For example - "Client reporting status", etc. The right hand side shows relevant details of the selected/highlighted category:

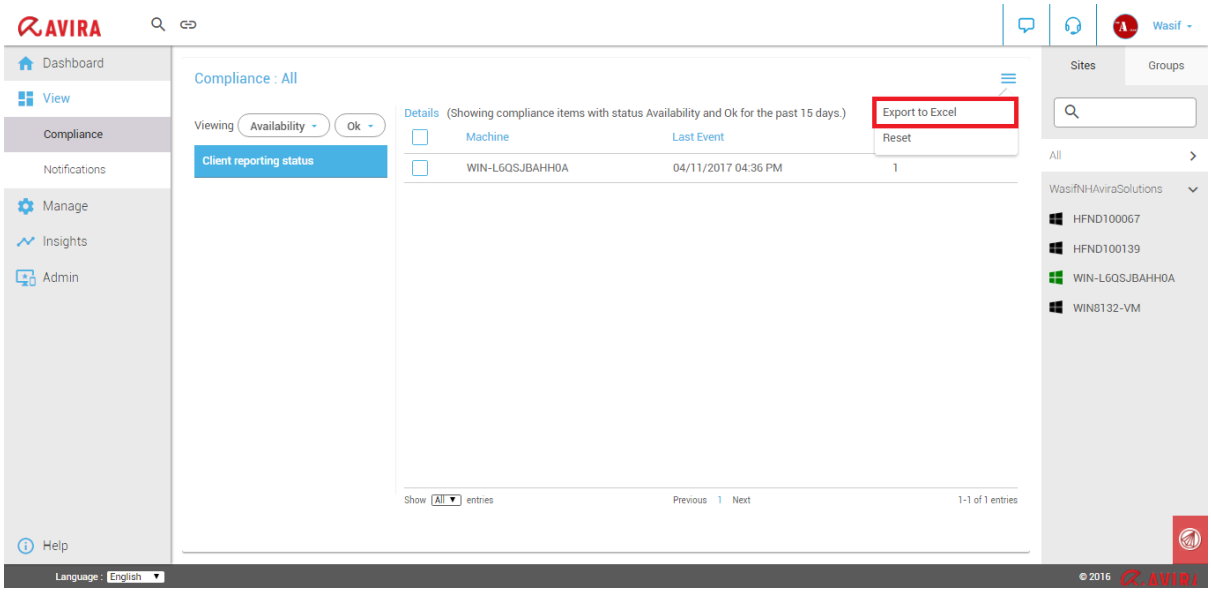
- **Machine**: Machine name
- **Last Event**: Latest event time
- **Event Count**: Number of events available

If a user has already reviewed an issue, knows how to fix it and does not want this item to be shown on the list, they can delete the record by clicking the option, "**Reset**". The user can find the reset link under the Breadcrumb drop-down menu on the top right corner. An example is shown below:



Please note: Grid data would be shown for 1 day.

The user can also export the compliance data in xls format as shown below:

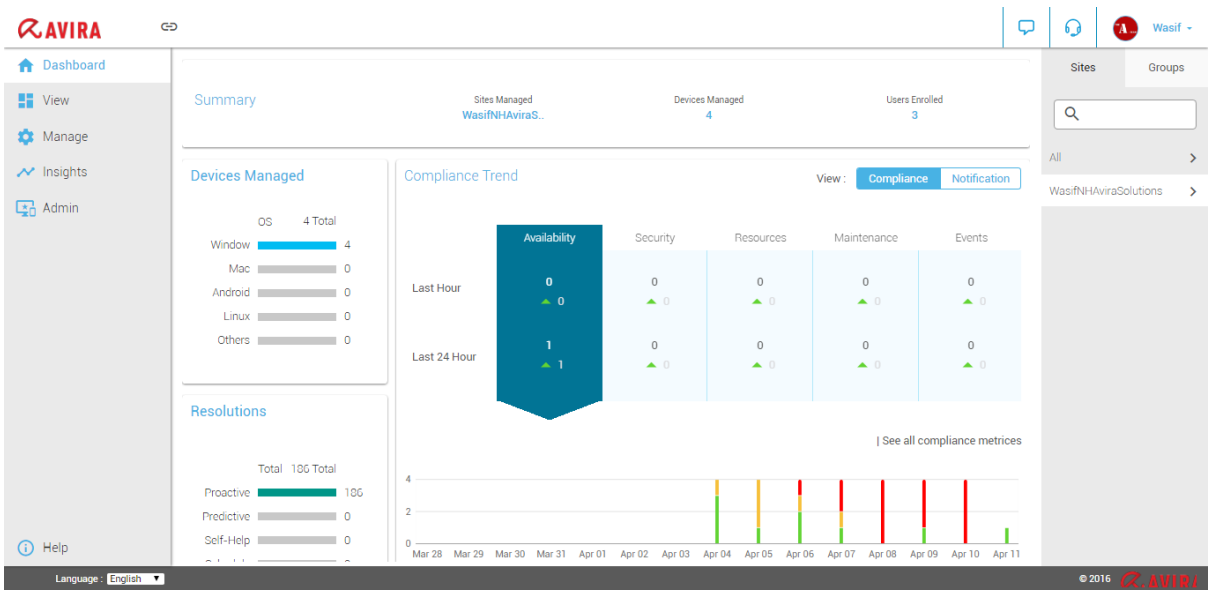


The downloaded report will have data like below:

	A	B	C
1	**Showing compliance items with status Availability and Ok for the past 15 days**		
2	Machine	Last Event	Event Count
3	WIN-L6QSJBAHH0A	04/11/2017 04:36 PM	1
4			

Compliance Trend

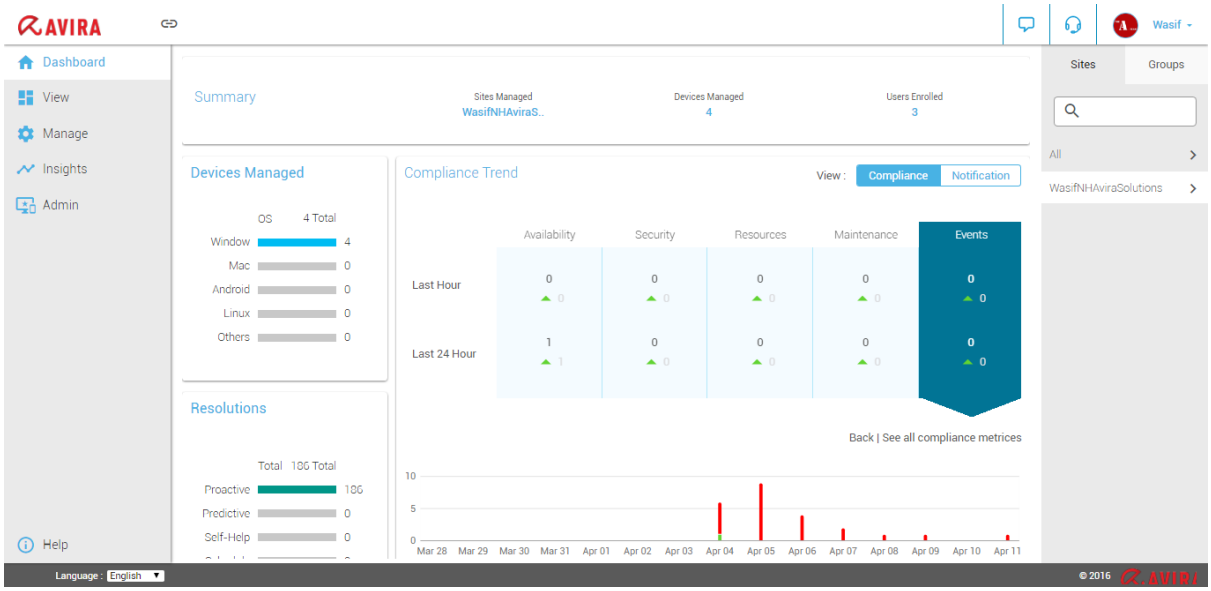
The Compliance Trend Graph data on the home page would be shown for 15 days:



As shown in the screenshot above, the Compliance Trend will be shown for the Last Hour & the Last 24 hours,

The user can also see the Trend graph for the last 15 days which shows the number of Ok/Warning/Alert items count per day.

If the user needs to view detailed compliance trend - they can click on any Compliance item, and the detailed trend will be shows as seen below:



The user can also see all the compliance matrices, by clicking on 'See all compliance metrics' link as shown above. This will navigate to the Compliance Page.

Notifications

Notifications are created based on the event filter. Hence, it is mandatory that there should already be a filter for notifications to be created. As the name only indicates, "Notification" means, notifying the user about an event occurrence.

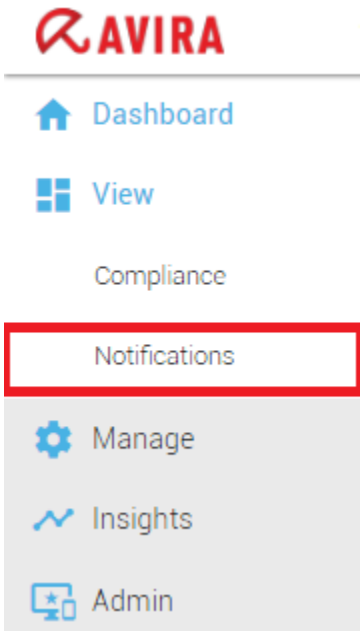
Dashboard has 5 notification priorities ranging from P1 to P5. These are placed under Critical, Major and Minor categories. Critical notifications are of the highest priority and minor are of the lowest.

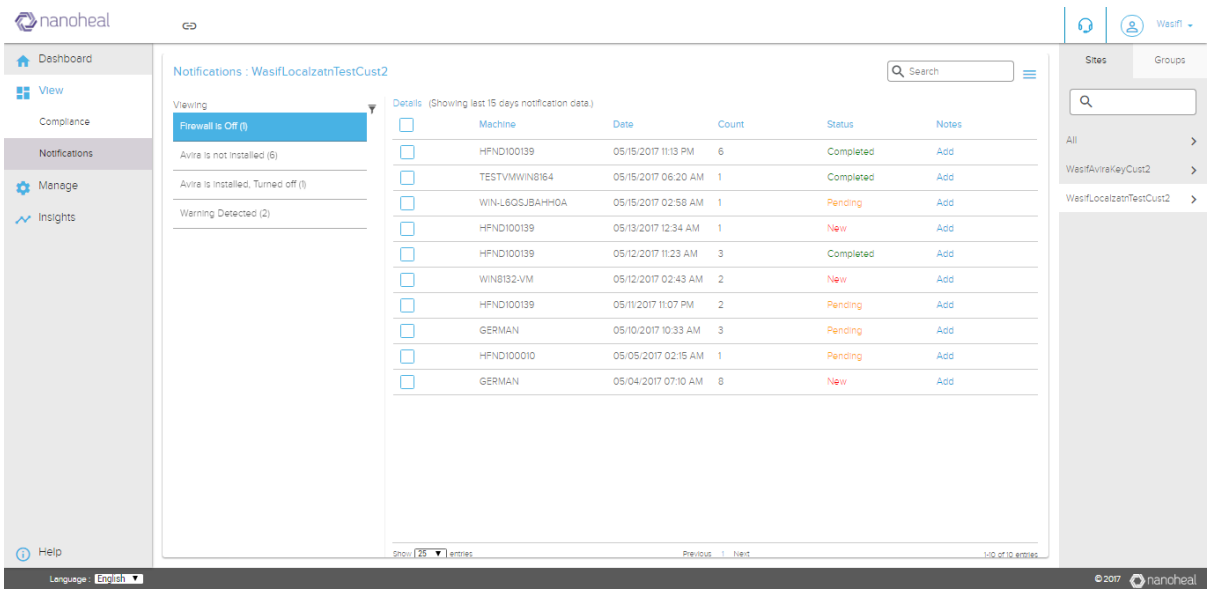
- Critical category includes Notifications with Priorities P1 and P2
- Major category includes Notifications with Priorities P3 and P4
- Minor category includes Notifications with Priorities P5

This module would hold and show important notifications about:

- # of machines with Avira
- # Malware infections
- # Other Warnings
- Etc.

Users can navigate to the Notifications page by clicking on the Notifications link from the left panel as shown below:





The Notifications Page is divided into two, with the notification categories on to the left and the corresponding device data shown to the right. (Device data is shown for the past 15 Days). A user can segregate through and view only the list of Critical, Major or Minor Notifications by using the 'All' drop-down. When "All" is selected it will show a compilation of Critical, Major and Minor notification data.

- All category includes Notifications with P1 to P3
- Critical category includes Notifications with priority P1 and P2
- Major category includes Notifications with priority P3

On the right side of the Notifications page a table with the following information is displayed.

- Machine – shows the Machine Name
- Date – shows the Date & Time on which the Notification is generated
- Count – shows the number of events count being generated for a notification
- Status – Three kinds: Pending, Actioned & Completed
- Notes – Users can add notes to any of the notification entries using the- Add link

Notification Status

- New - List of notifications for which no action has been taken yet

- Pending– List of notifications on which action has been pushed but the action has not run yet or the action pushed is from

- Completed- A list of notifications for which the action has been taken using:

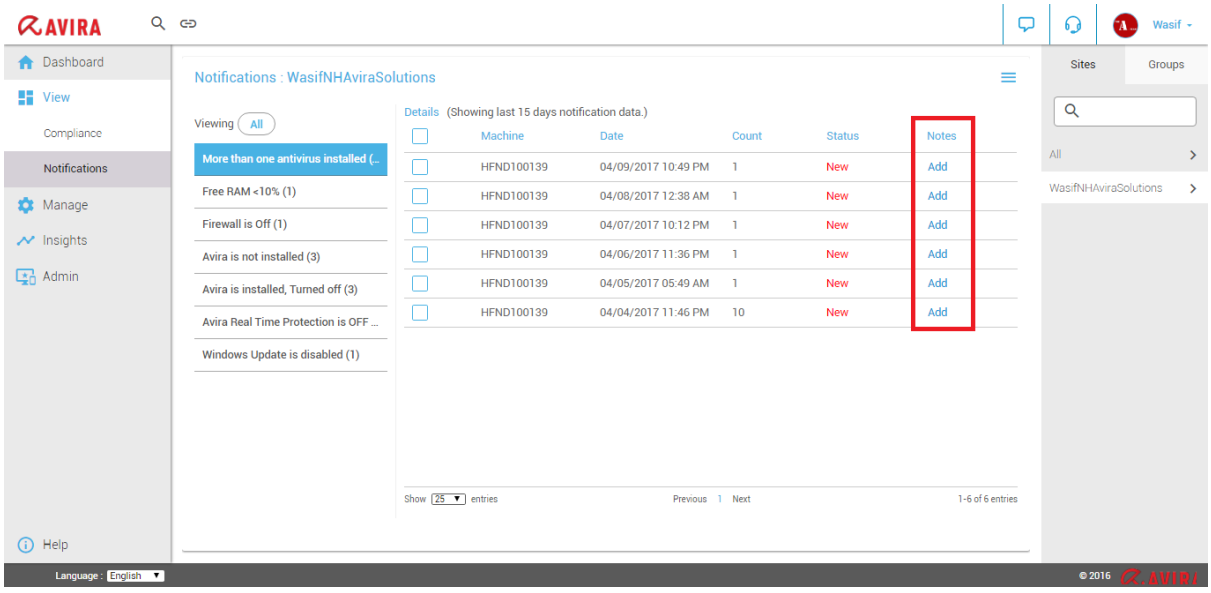
  a) 'Fix' from the drop-down menu on the Notifications page from Troubleshooters.

  b) 'Other Actions' from the drop-down menu on Notifications page

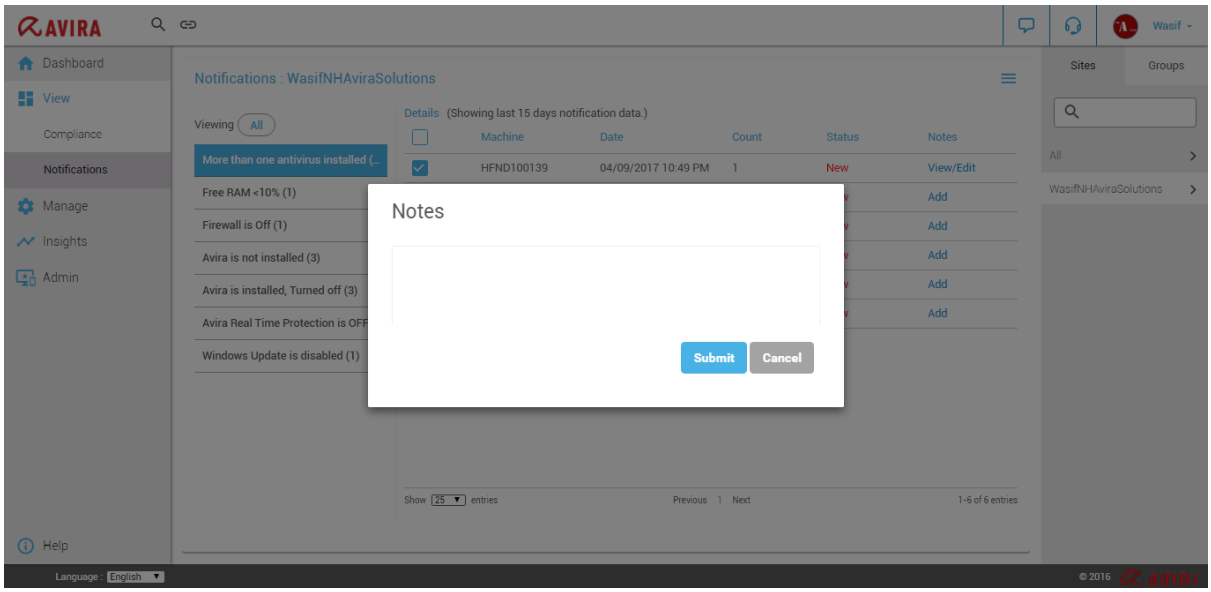
Events that can prove critical to the end user's environment and need to be resolved on a priority - the same can be notified to the persons of interest specified during notification creation via an email. These can also be published as a notification on the Notification Console.

Notes

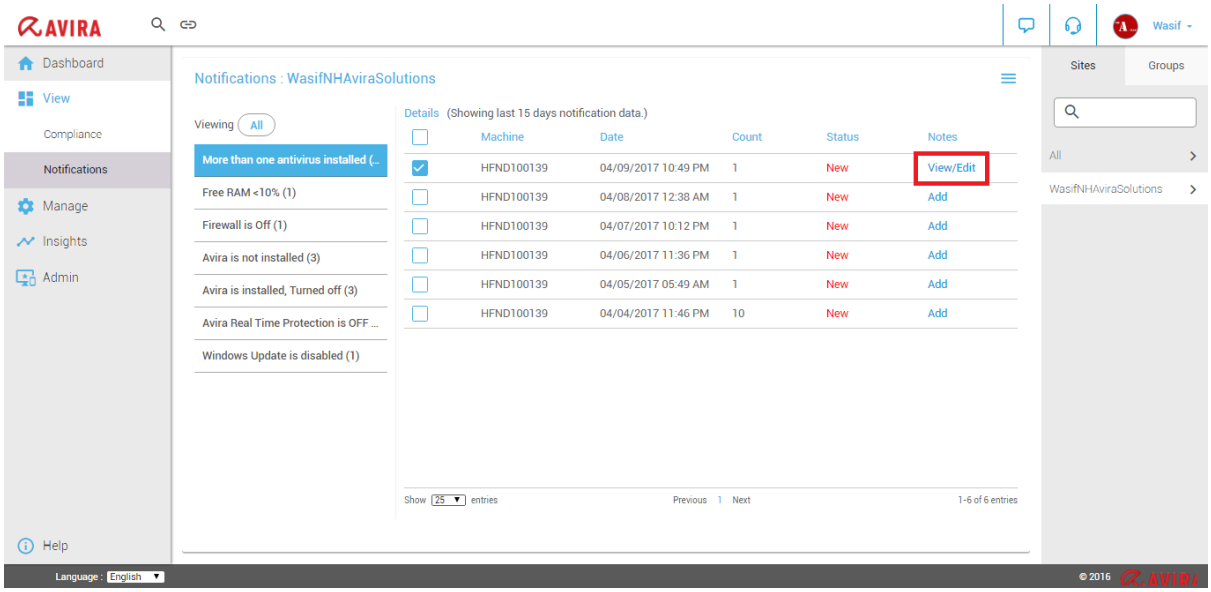
Users can Add/Edit/Update/Delete the Notes assigned to individual notifications. In order to add Notes to a particular notification, users must go to the Notifications Page, select the notification on left and click on 'Add' link under Notes for that particular notification. An example is shown below:



Add Notes pop-up shows up, where in the user can enter the notification notes & click on Submit to add notes. An example is shown below:



Once the notes are added successfully, View/Edit option will come as shown below. In order to edit notification notes, the user should select a notification which already has notes & click on the edit icon. In order to view notes, the user should click on view



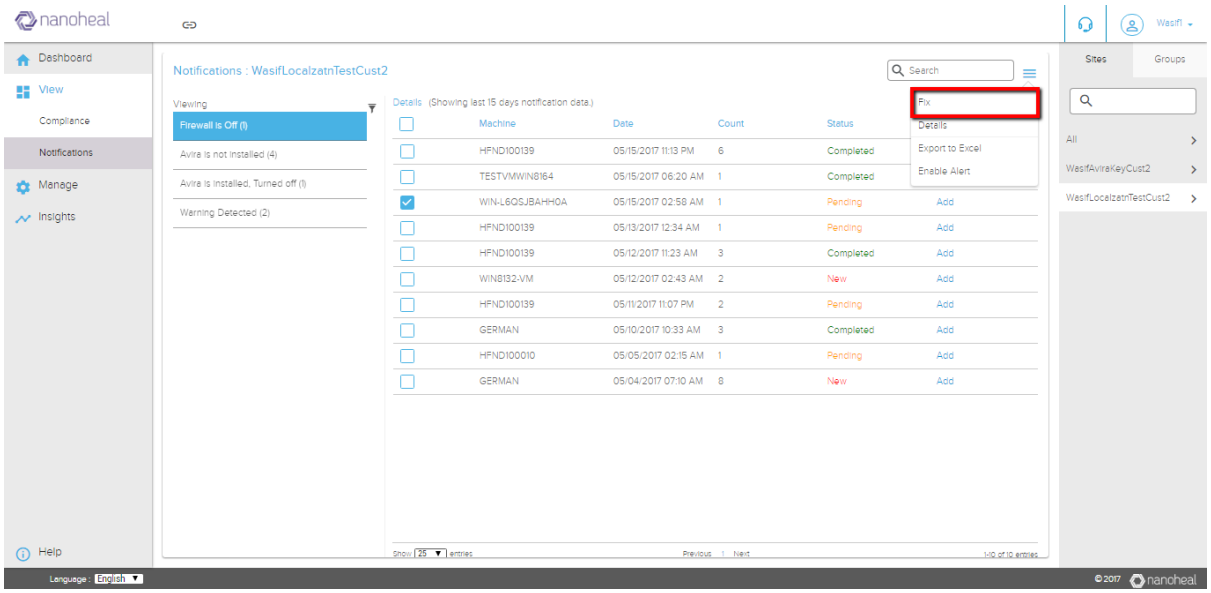
Fixing Notification

Notifications can be fixed using "Troubleshooting" or "Others Actions"

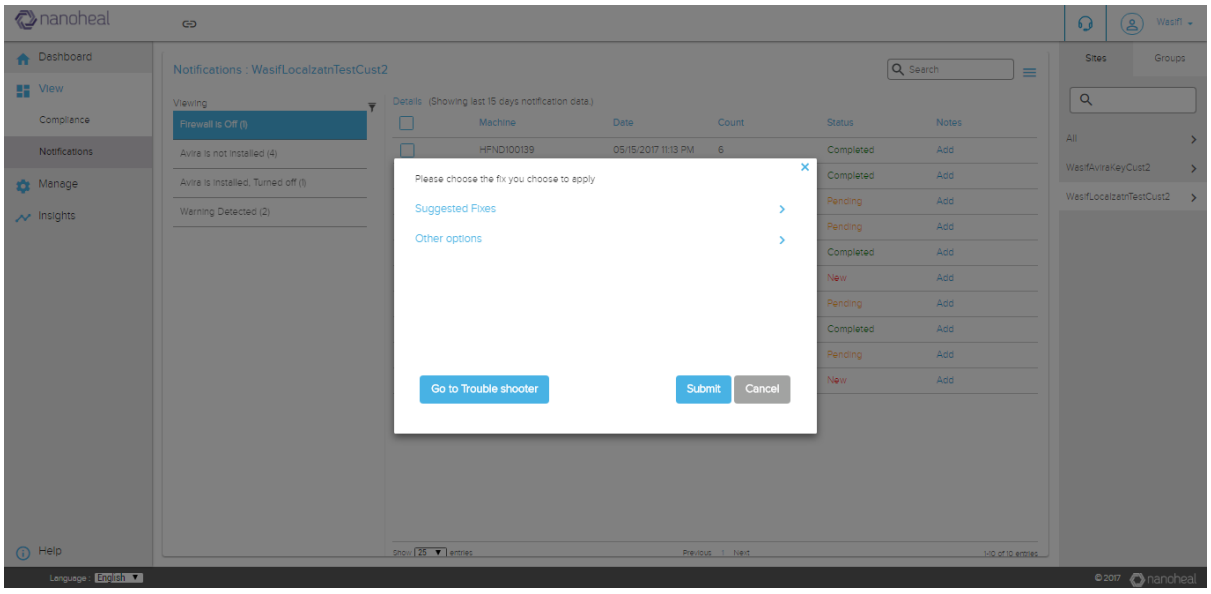
When any particular notification is actioned from the "Others List", count gets decremented from "Pending" and gets incremented to "Action". Similarly, when any Notification is fixed by triggering a profile from "Troubleshooting", the "Fixed" count gets incremented by 1 from "Pending".

Using Troubleshooting Notification Fix

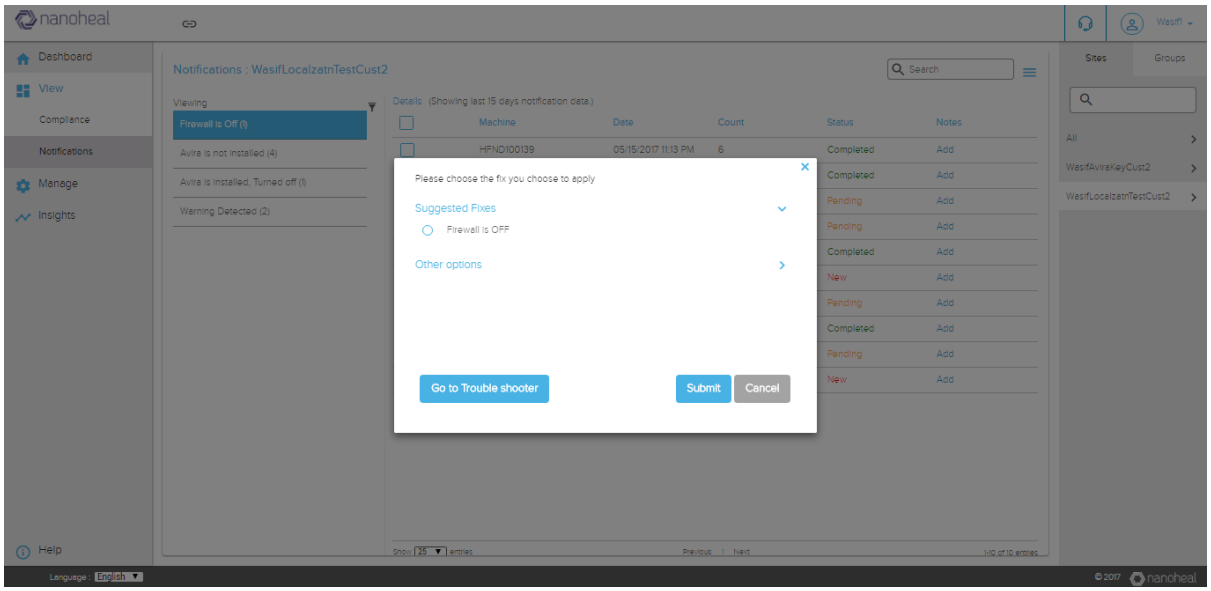
To fix a notification by triggering the troubleshooting tools, the user should select the particular notification from the left and select the records for which action need to be taken (on the right) and click on menu. Select Fix from the drop-down menu as shown in the example below:



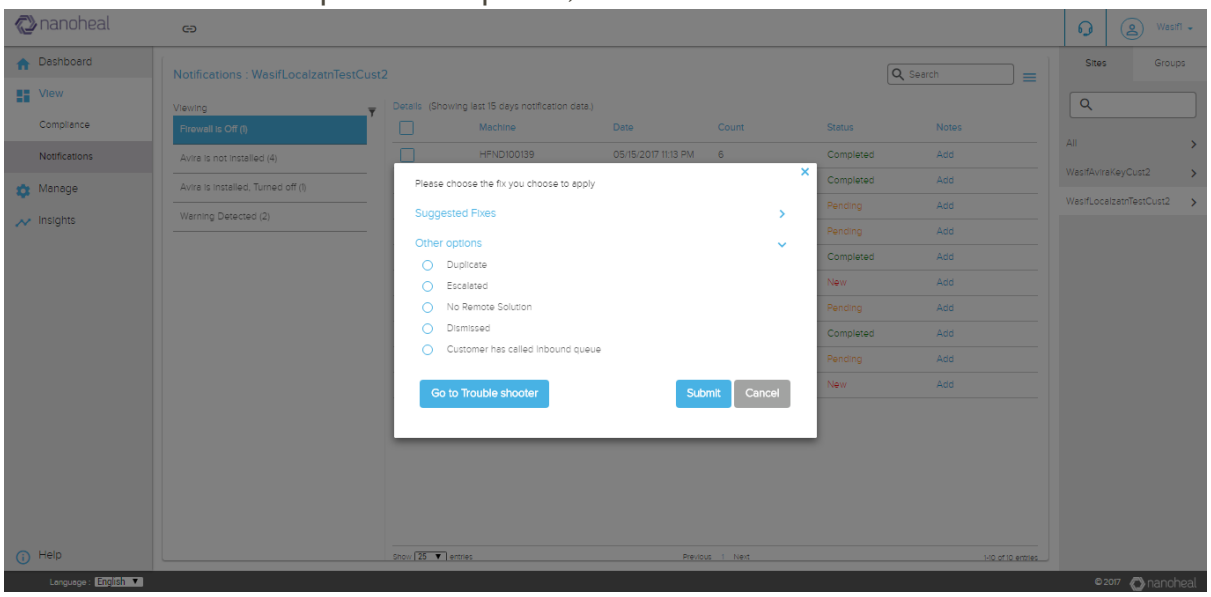
Once the user clicks on "Fix" he/she will be redirected to the below page:



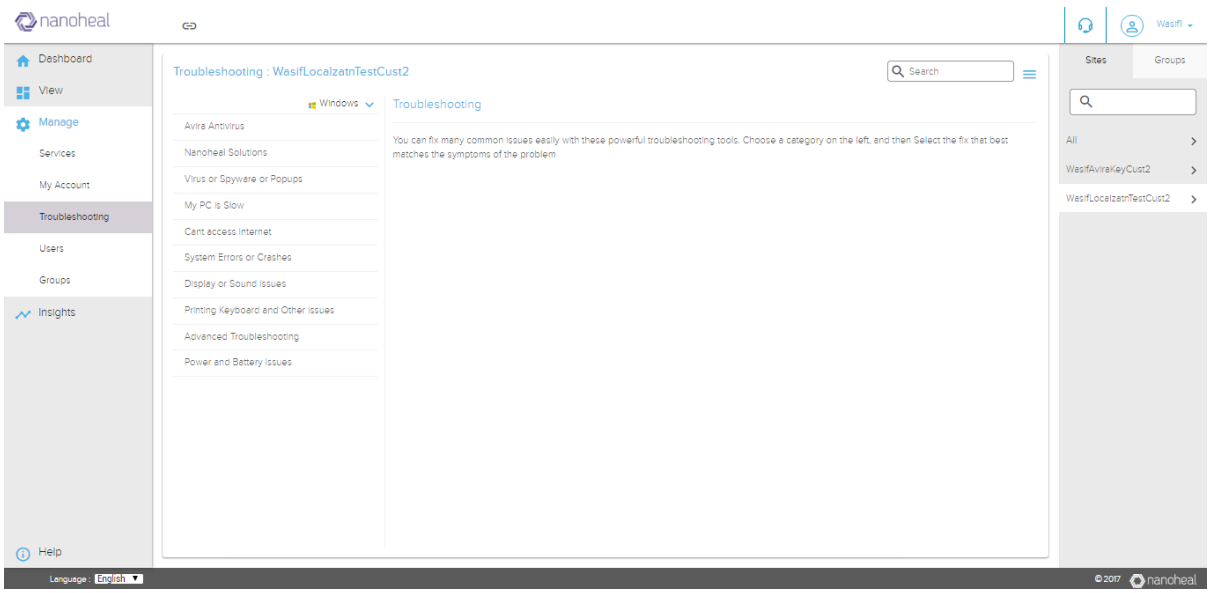
Suggested fix will show the needed action to be taken for that particular notification. For ex: for firewall turned Off notification, suggested fix shown is:



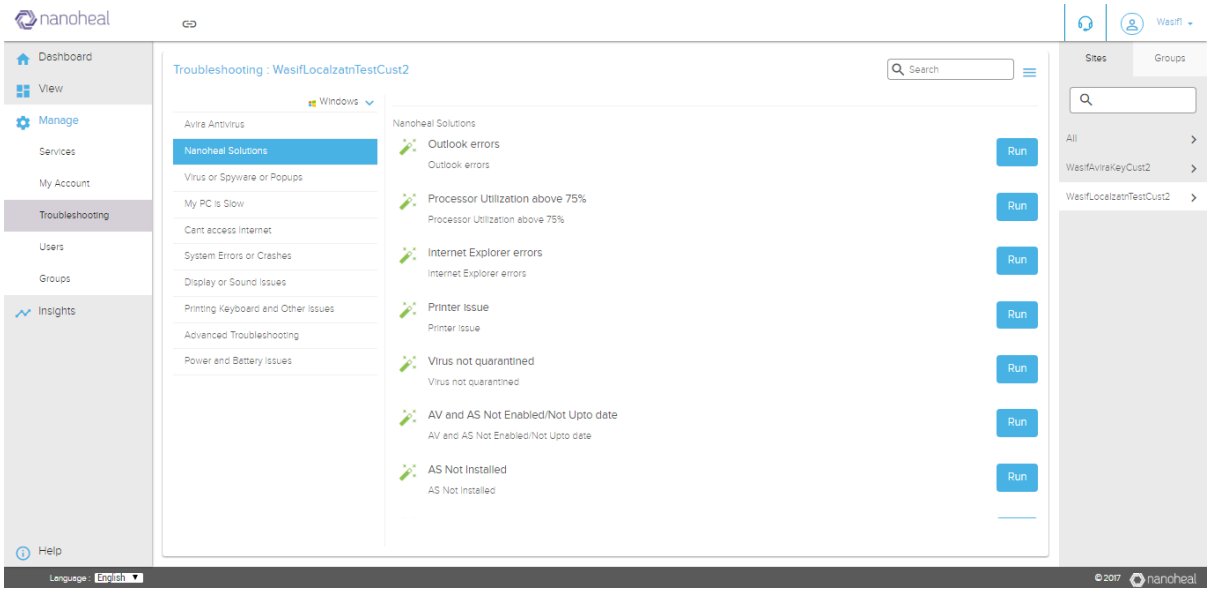
Other action will have option like duplicate,escalated etc as shown below:



Click on "Goto Troubleshooter" will take to the troubleshooting page as shown below:



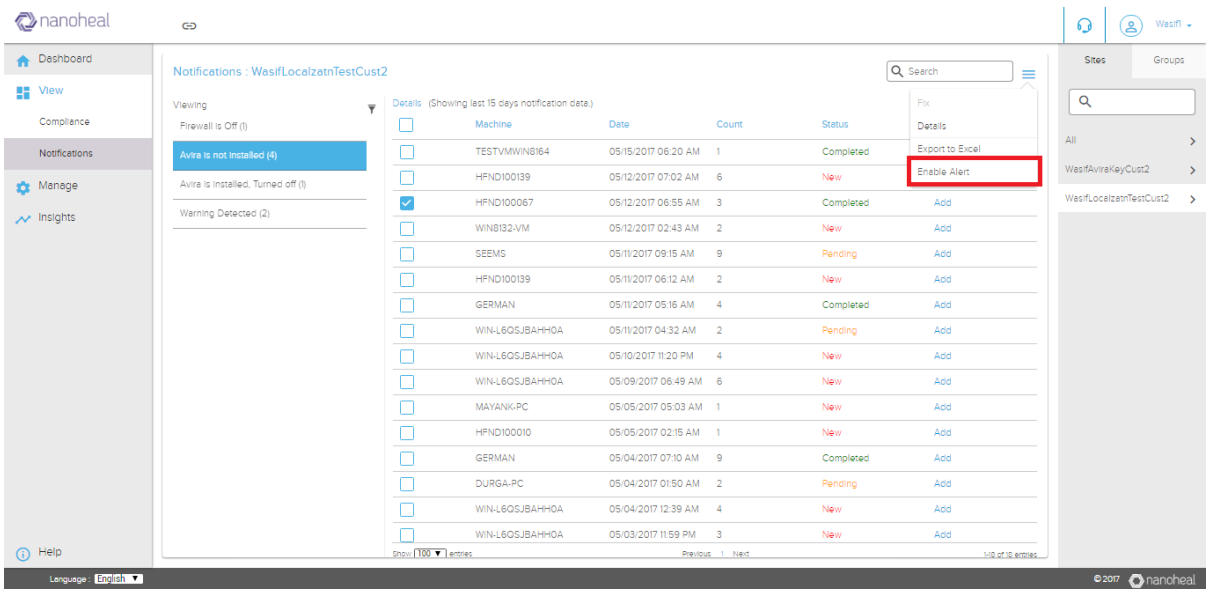
In order to fix the issue, select the relevant troubleshooting tool from the left and click on "Run this Repair". An example is shown below:



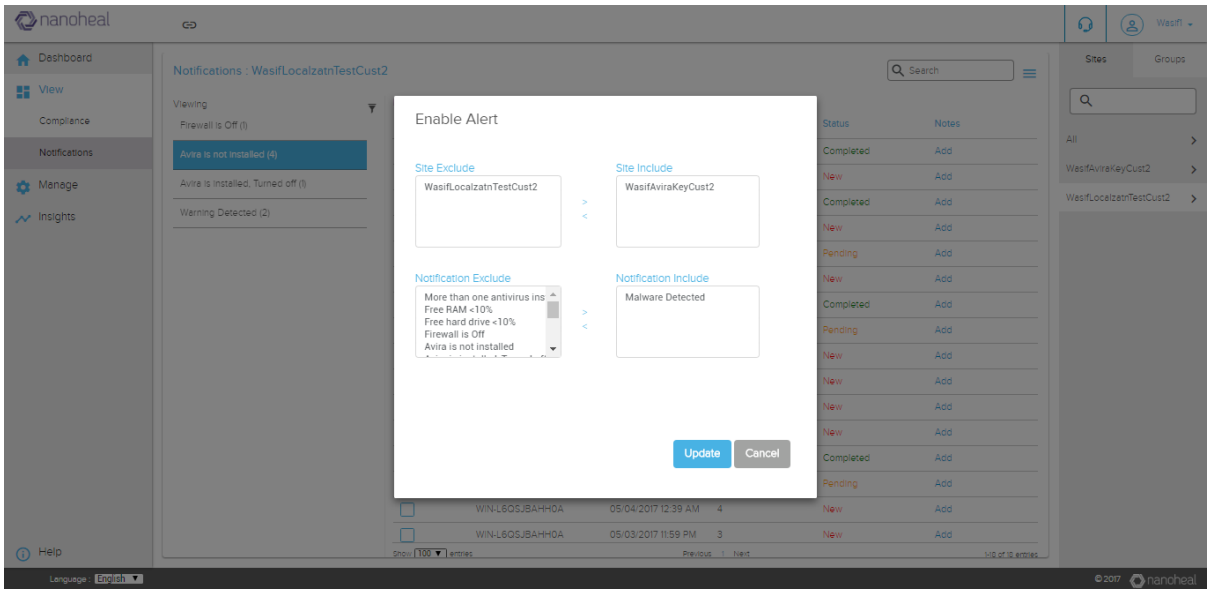
Please note that the device needs to be online for the solution to be pushed immediately. Else the solution is pushed the next time the device comes online.

Notification Alert

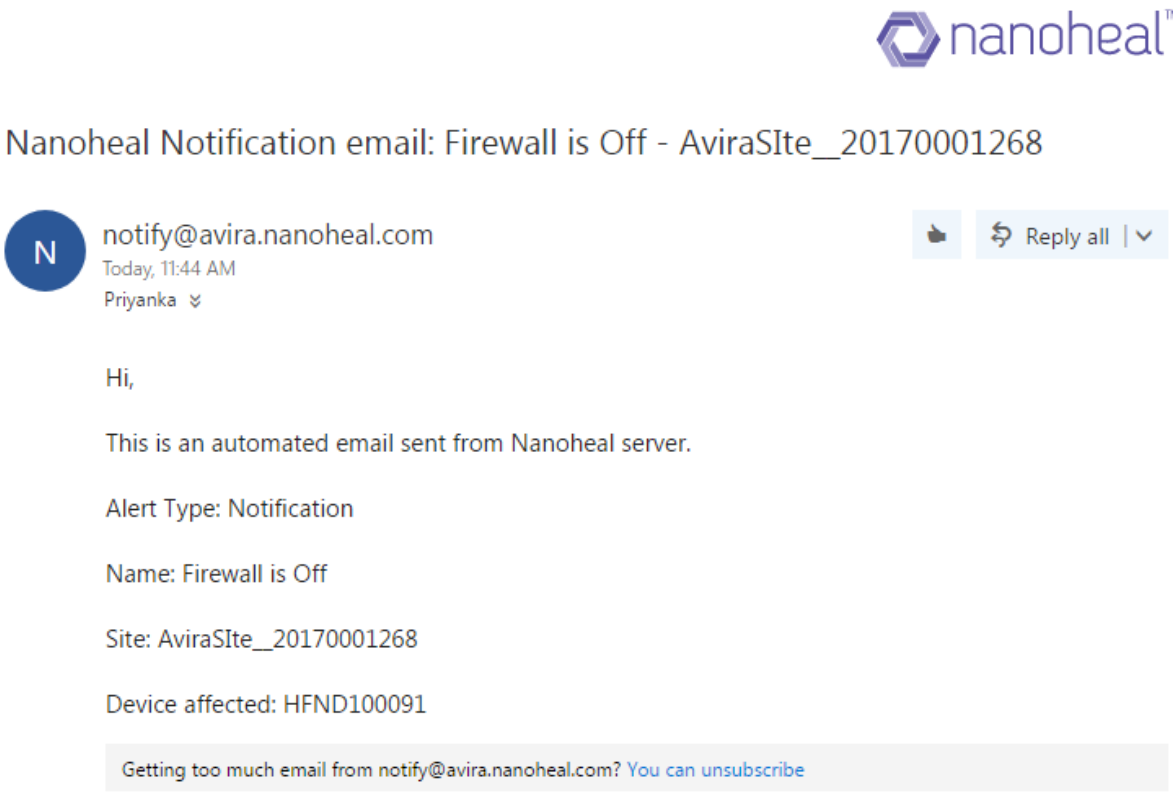
This feature will help user to get notification alert on their mail id. User can configure alert by going to menu icon and clicking on "Enable Alert" as shown below:



Clicking on enable alert will give the following window asking user to configure site and notification:

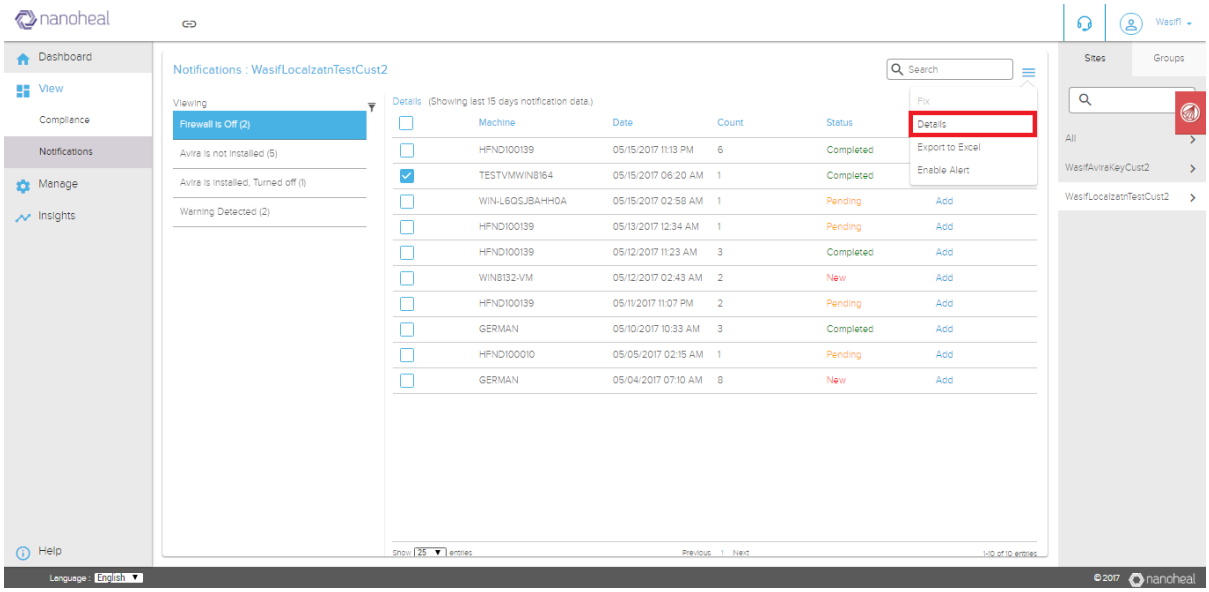


Click on update will create alert and mail will be sent to that particular user on whose login alert has been configured as shown below:

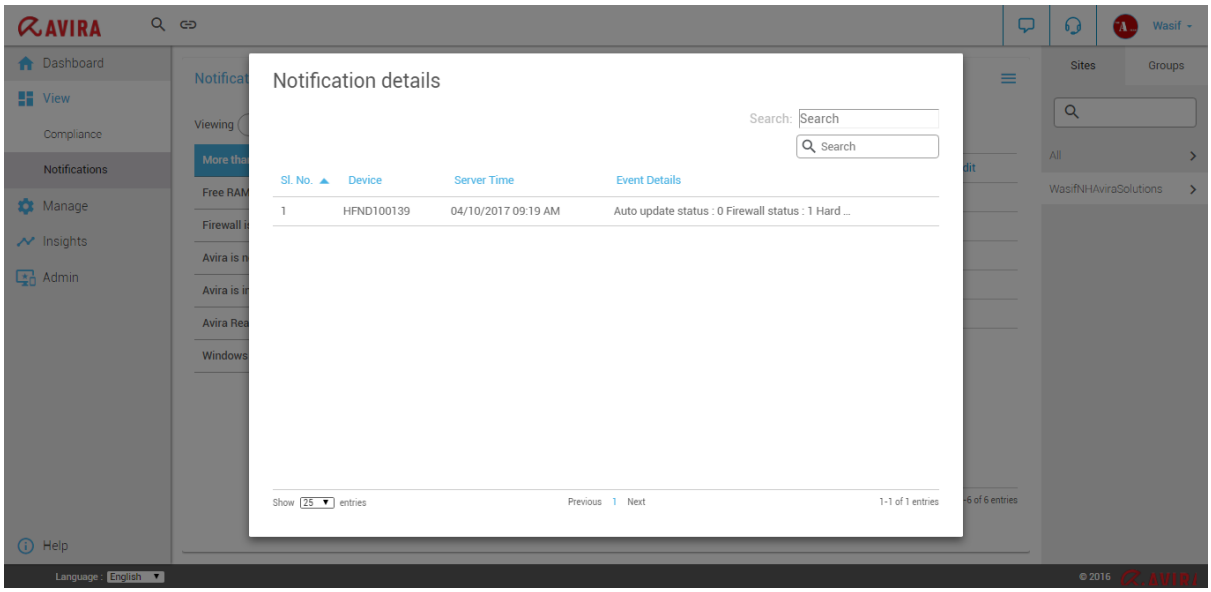


Notification View

To see the notification details, the user needs to select the notification and select 'Details' from the drop-down menu. An example is shown below:

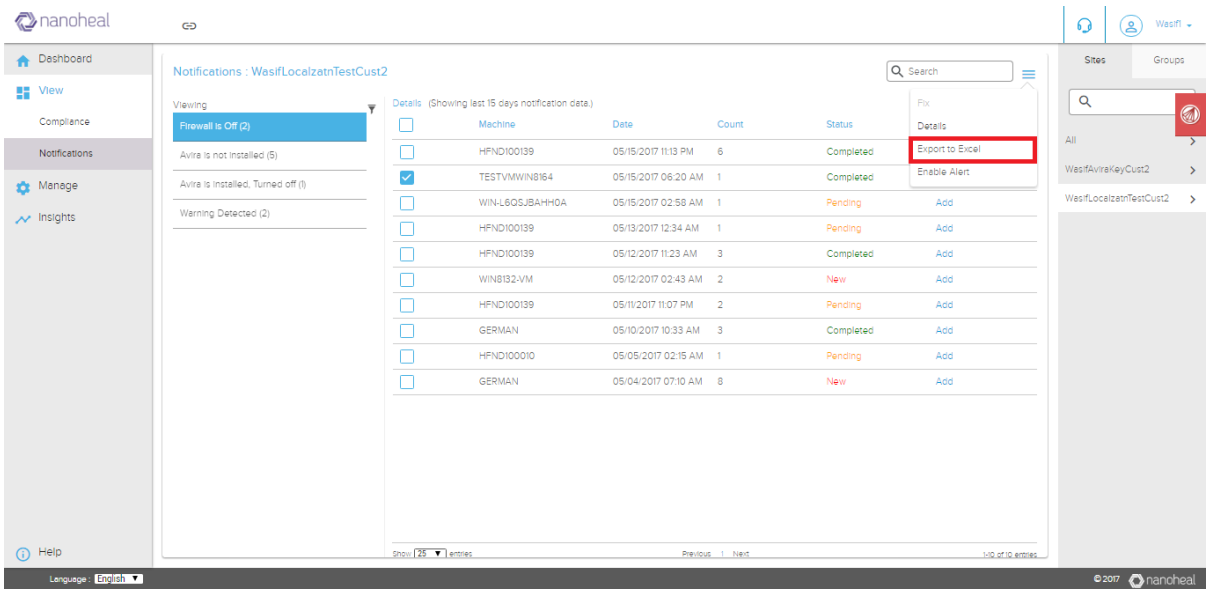


A pop-up displays the notification details as shown below.

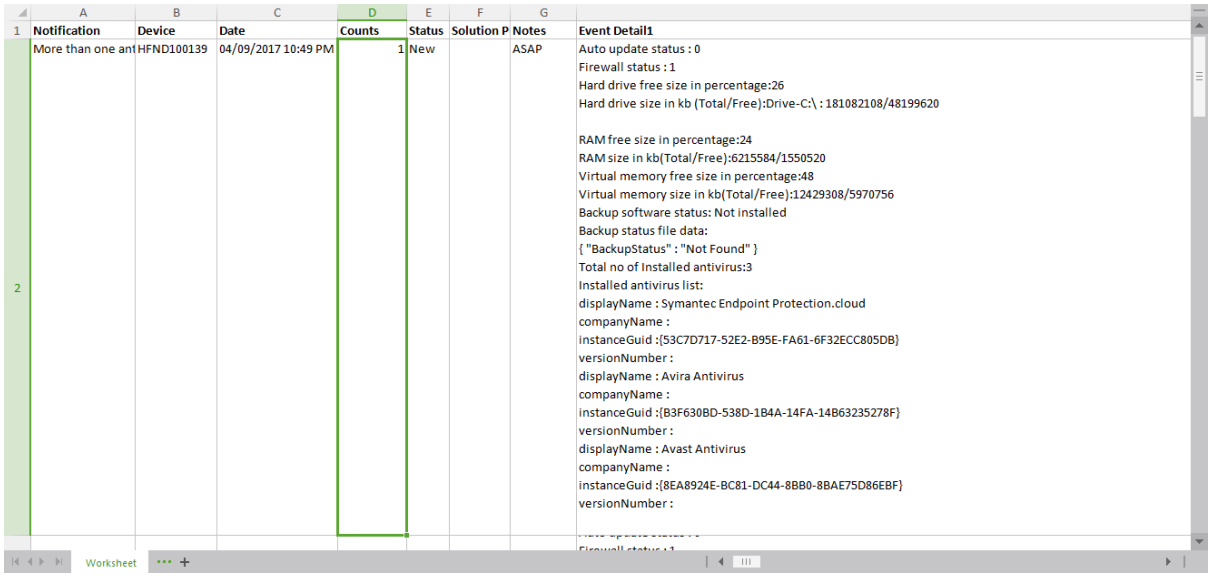


Notification Export

Users can export all the notifications data to an .xls file by clicking on "Export to Excel" under the drop-down menu options. An example is shown below:



An example of the .xls file thus generated is given below:



	A	B	C	D	E	F	G	
1	Notification	Device	Date	Counts	Status	Solution P	Notes	Event Detail1
2	More than one ant	HFND100139	04/09/2017 10:49 PM	1	New		ASAP	Auto update status : 0 Firewall status : 1 Hard drive free size in percentage:26 Hard drive size in kb (Total/Free):Drive-C:\ : 181082108/48199620 RAM free size in percentage:24 RAM size in kb(Total/Free):6215584/1550520 Virtual memory free size in percentage:48 Virtual memory size in kb(Total/Free):12429308/5970756 Backup software status: Not installed Backup status file data: { "BackupStatus" : "Not Found" } Total no of Installed antivirus:3 Installed antivirus list: displayName : Symantec Endpoint Protection.cloud companyName : instanceGuid :{53C7D717-52E2-B95E-FA61-6F32ECC805DB} versionNumber : displayName : Avira Antivirus companyName : instanceGuid :{B3F630BD-538D-1B4A-14FA-14B63235278F} versionNumber : displayName : Avast Antivirus companyName : instanceGuid :{8EA8924E-BC81-DC44-8BB0-8BAE75D86EBF} versionNumber :

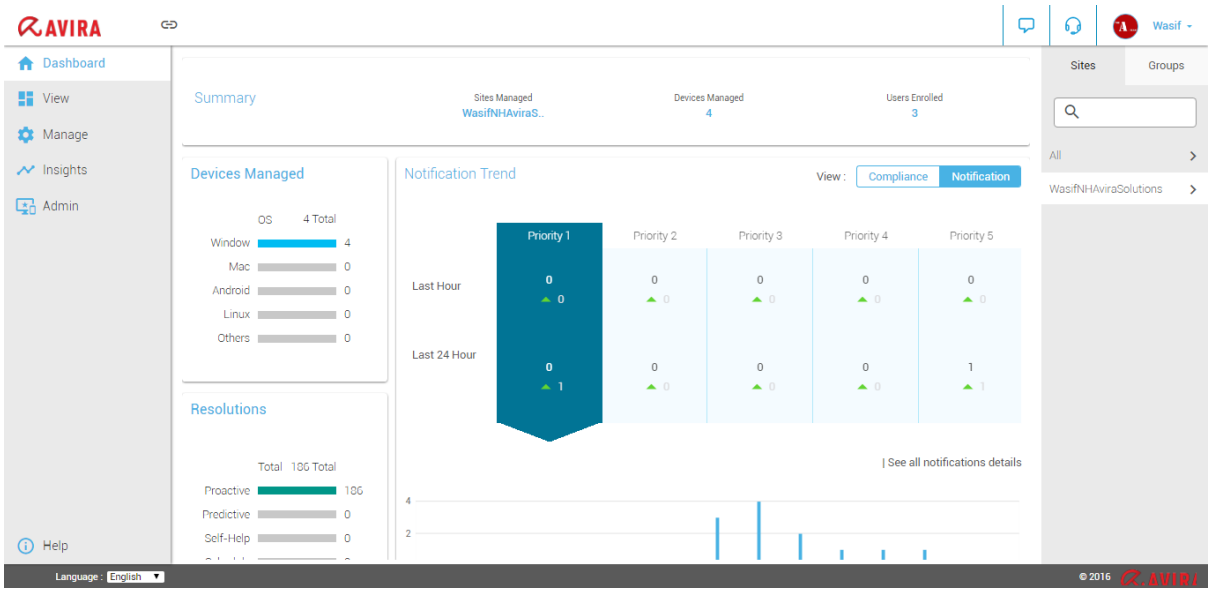
Worksheet

Notification Summary" on the right side of the Dashboard Home Page displays the following:

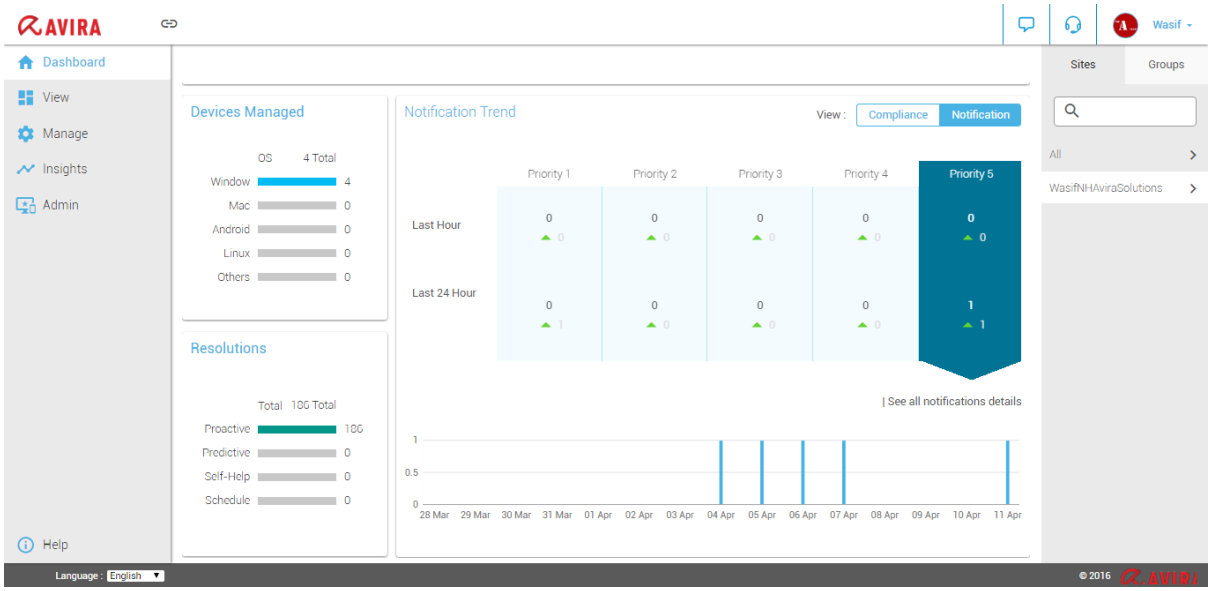
- All the Notifications for a particular site / machine / group. This is the Count of Priority1 + Priority2 + Priority3
- Priority 1 to Priority 3 Notifications Count
- Notifications % which is calculated as (Individual Notification Count / All Notifications Count) X 100

Notification Trend

We can view the Notification trend from the Home Page by clicking on the Toggle icon for Notifications in the Compliance trend section. Once the Toggle icon is clicked, the Notification Trend will be shown as seen below.



If the user needs to view detailed notification trend, then clicking on any Notification Priority item would display detailed trend as shown below.

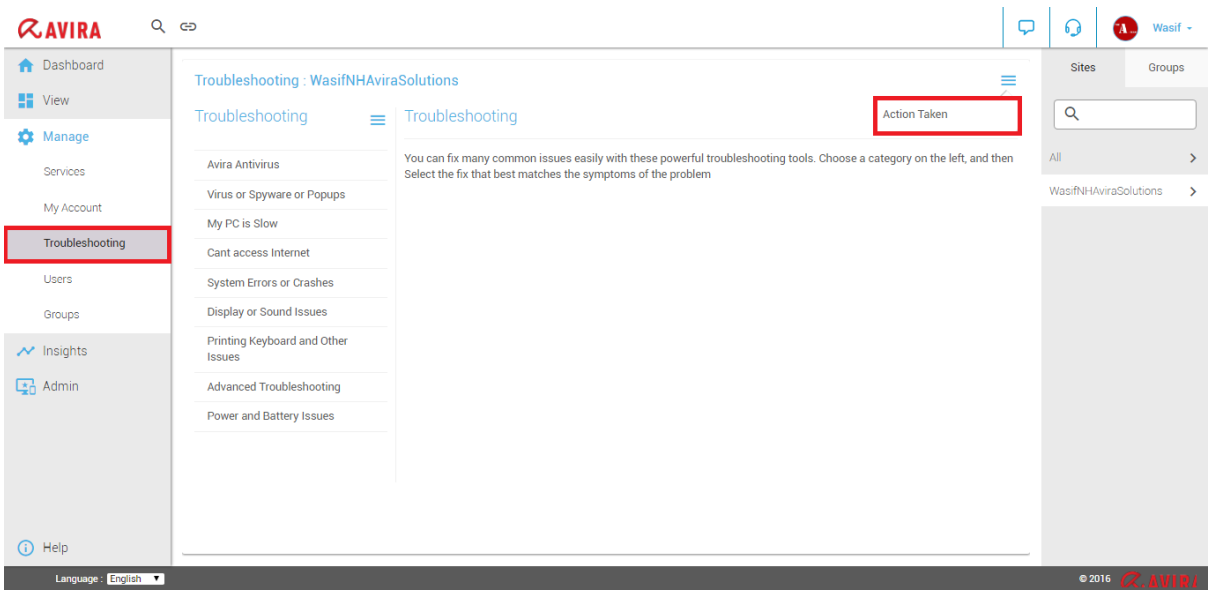


The user can also see all notifications, by clicking on 'See all notifications' link as shown above. This will navigate to Notifications Page.

Resolutions – Proactive (Audit & Schedule)

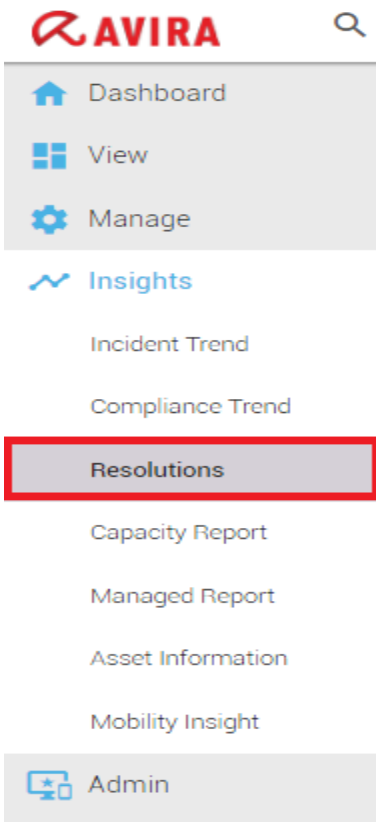
A user can get to the page titled Resolutions in 2 ways:

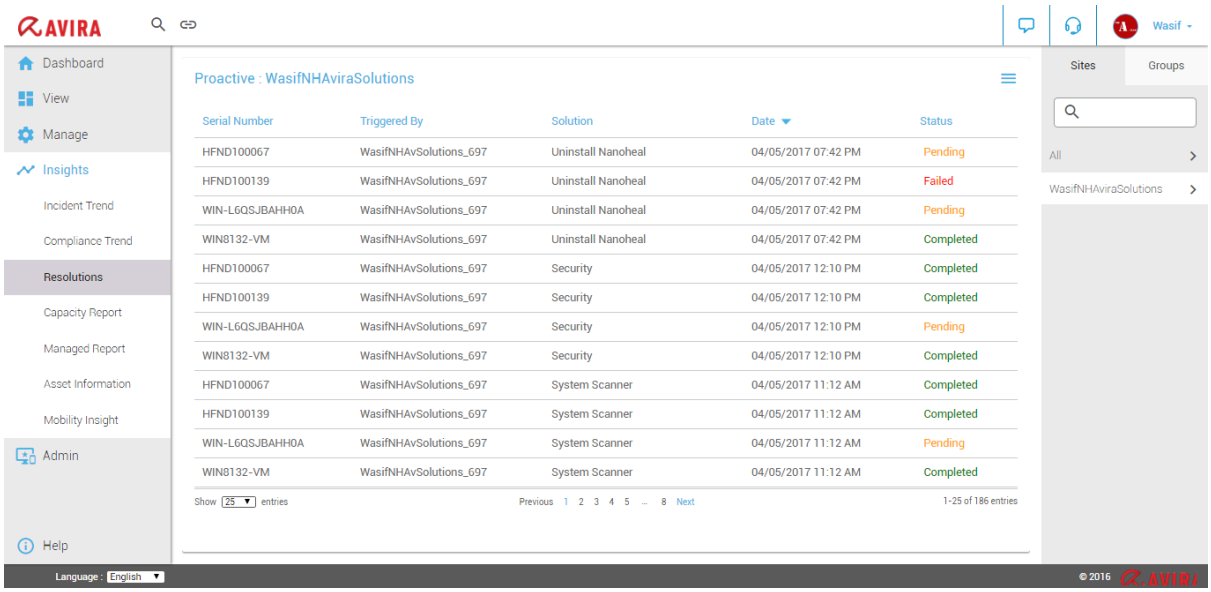
1. From **Manage > Troubleshooting** - Using **Menu > Action taken**



From the Left panel, **Insights > Resolutions**

As shown below:





A sample '**Resolutions'** screen is shown above.

Resolutions screen provides details of who has triggered the solution, Site or Machine Group where a resolution has been pushed, and the date on which the resolution was triggered.

All items on this screen will be in one of these 3 states- Completed, Pending, or Failed.

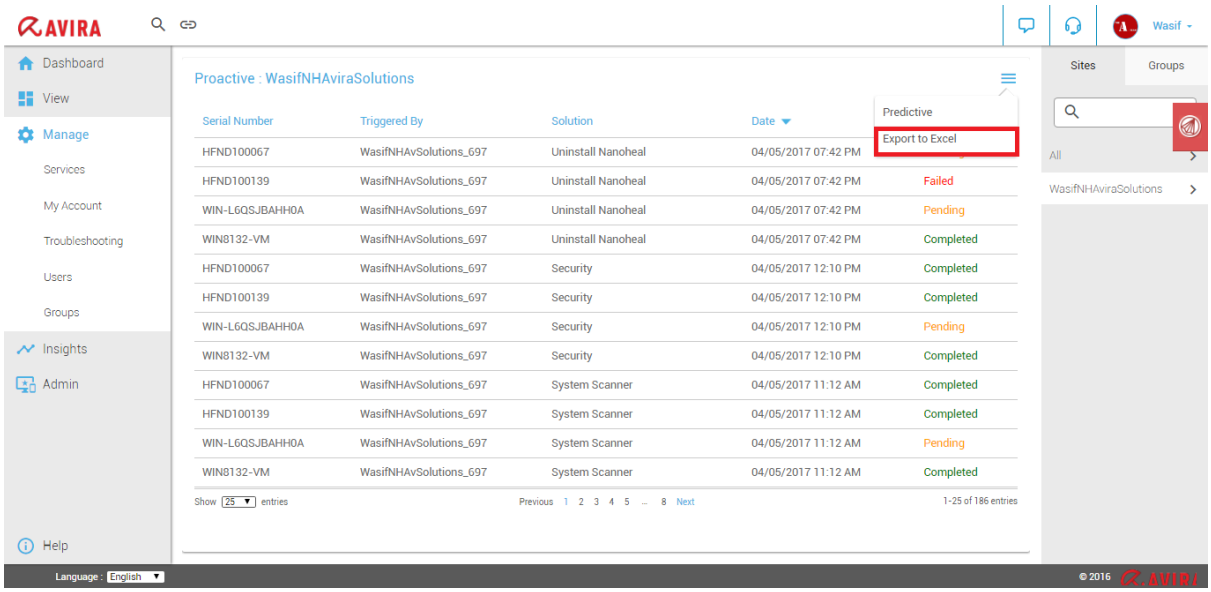
Resolutions Status:

1. Completed: Once the triggered resolution from Troubleshooting is successfully executed on the machine, the status is updated to "Completed".

2. Pending: If a triggered resolution has not reached the machine either because the machine is offline or if another triggered resolution is under execution – the status would appear as "Pending".

3. Failed: If a triggered solution has failed to execute on the machine, the Resolution status will be updated as "Failed".

A user can also export this data to a .xls file by using the Export to Excel link under the drop-down menu as shown below:



An example of the xls file is shown below:

	A	B	C	D	E	F	G	H
1	Serial Number	Triggered By	Type	Solution	Date	OS	Status	
2	HFND100139	ResolvIT_03	Troubleshooting	Turn off RTP	03/13/2017 09:30 AM	Windows7Professional64-bit	Completed	
3	HFND100139	ResolvIT_03	Troubleshooting	Turn on RTP	03/13/2017 09:31 AM	Windows7Professional64-bit	Completed	
4	HFND100139	ResolvIT_03	Troubleshooting	Start-up Optimization	03/13/2017 09:42 AM	Windows7Professional64-bit	Completed	
5	HFND100139	ResolvIT_03	Troubleshooting	Reliability Monitor	03/13/2017 11:01 AM	Windows7Professional64-bit	Completed	
6	HFND100139	ResolvIT_03	Troubleshooting	One Drive	03/13/2017 11:02 AM	Windows7Professional64-bit	Completed	
7	HFND100139	ResolvIT_03	Notification	Turn on RTP	03/13/2017 11:16 AM	Windows7Professional64-bit	Completed	
8	HFND100139	ResolvIT_03	Notification	Turn off RTP	03/13/2017 11:21 AM	Windows7Professional64-bit	Completed	
9	HFND100139	ResolvIT_03	Notification	Turn on RTP	03/13/2017 11:35 AM	Windows7Professional64-bit	Completed	
10	HFND100139	ResolvIT_03	Troubleshooting	Quick Scan	03/13/2017 11:38 AM	Windows7Professional64-bit	Completed	
11	HFND100139	ResolvIT_03	Troubleshooting	Process Scan	03/13/2017 11:52 AM	Windows7Professional64-bit	Completed	
12	HFND100139	ResolvIT_03	Troubleshooting	Turn off RTP	03/13/2017 11:55 AM	Windows7Professional64-bit	Completed	
13	HFND100139	ResolvIT_03	Troubleshooting	Turn on RTP	03/13/2017 11:55 AM	Windows7Professional64-bit	Completed	
14	HFND100139	WasifAviraUAT1_448	Notification	Reliability Monitor	03/14/2017 01:06 PM	Windows7Professional64-bit	Completed	
15	HFND100139	WasifAviraUAT1_448	Troubleshooting	Quick Scan	03/14/2017 01:09 PM	Windows7Professional64-bit	Completed	
16	HFND100139	WasifAviraUAT1_448	Troubleshooting	Process Scan	03/14/2017 01:12 PM	Windows7Professional64-bit	Completed	
17	HFND100139	WasifAviraUAT1_448	Troubleshooting	Get last fullscan date	03/14/2017 01:22 PM	Windows7Professional64-bit	Completed	
18	HFND100139	WasifAviraUAT1_448	Troubleshooting	Turn off RTP	03/14/2017 01:22 PM	Windows7Professional64-bit	Completed	
19	HFND100139	WasifAviraUAT1_448	Troubleshooting	Turn on RTP	03/14/2017 01:23 PM	Windows7Professional64-bit	Completed	
20	HFND100139	WasifAviraUAT1_448	Troubleshooting	Quick Scan	03/14/2017 04:25 PM	Windows7Professional64-bit	Failed	
21	HFND100139	WasifAviraUAT1_448	Notification	Start-up Optimization	03/14/2017 05:34 PM	Windows7Professional64-bit	Completed	
22	HFND100067	WasifAviraDemo	Troubleshooting	Quick Scan	03/16/2017 01:03 PM	Windows7Professional64-bit	Completed	
23	HFND100139	WasifAviraDemo	Troubleshooting	Quick Scan	03/16/2017 01:03 PM	Windows7Professional64-bit	Completed	
24	HFND100067	WasifAviraDemo	Troubleshooting	Full Scan	03/16/2017 01:03 PM	Windows7Professional64-bit	Completed	
25	HFND100139	WasifAviraDemo	Troubleshooting	Full Scan	03/16/2017 01:03 PM	Windows7Professional64-bit	Failed	
26	HFND100067	WasifAviraDemo	Troubleshooting	Removable disks scan	03/16/2017 01:03 PM	Windows7Professional64-bit	Completed	
27	HFND100139	WasifAviraDemo	Troubleshooting	Removable disks scan	03/16/2017 01:03 PM	Windows7Professional64-bit	Completed	
28	HFND100067	WasifAviraDemo	Troubleshooting	Process Scan	03/16/2017 01:03 PM	Windows7Professional64-bit	Completed	
29	HFND100139	WasifAviraDemo	Troubleshooting	Process Scan	03/16/2017 01:03 PM	Windows7Professional64-bit	Completed	

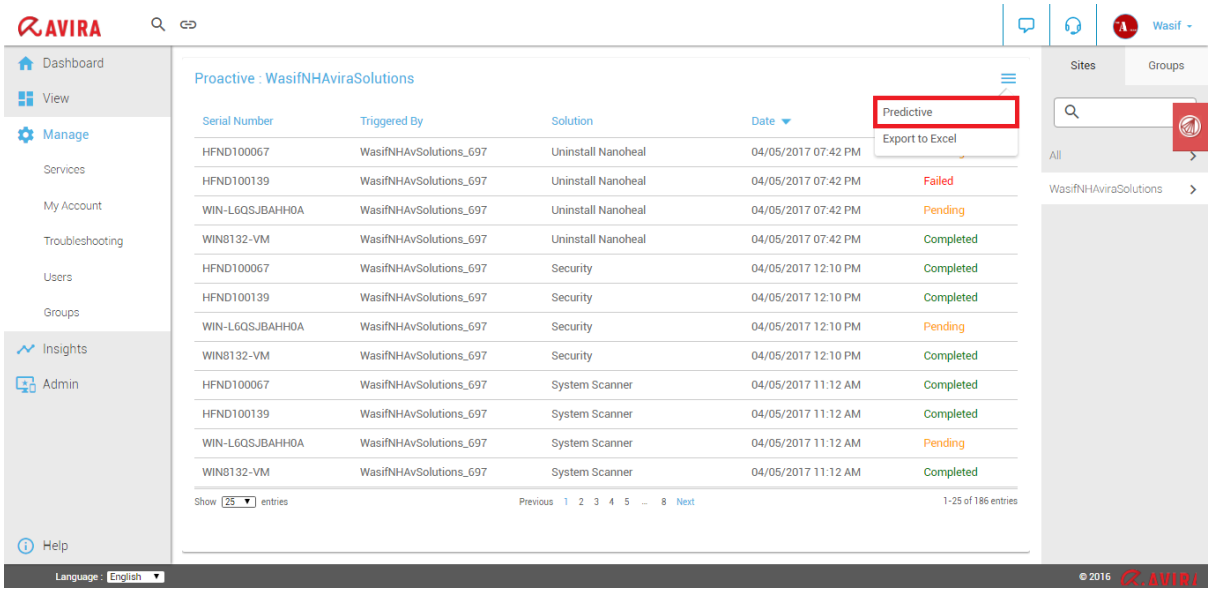
Worksheet

The "Type" column indicates whether the Resolution was pushed from the Troubleshooting or the Notifications screen.

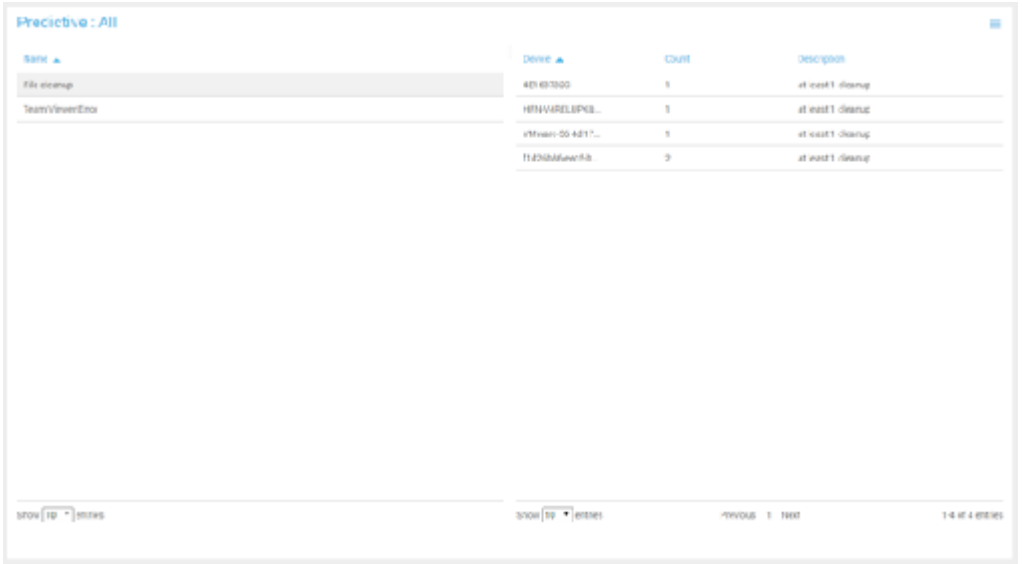
Resolutions – Predictive

Predictive resolutions differentiate Nanoheal from its competitors. In simple terms, Predictive resolutions or Auto heal resolutions means that Nanoheal is Capable of fixing issues in real-time as and when they occur.

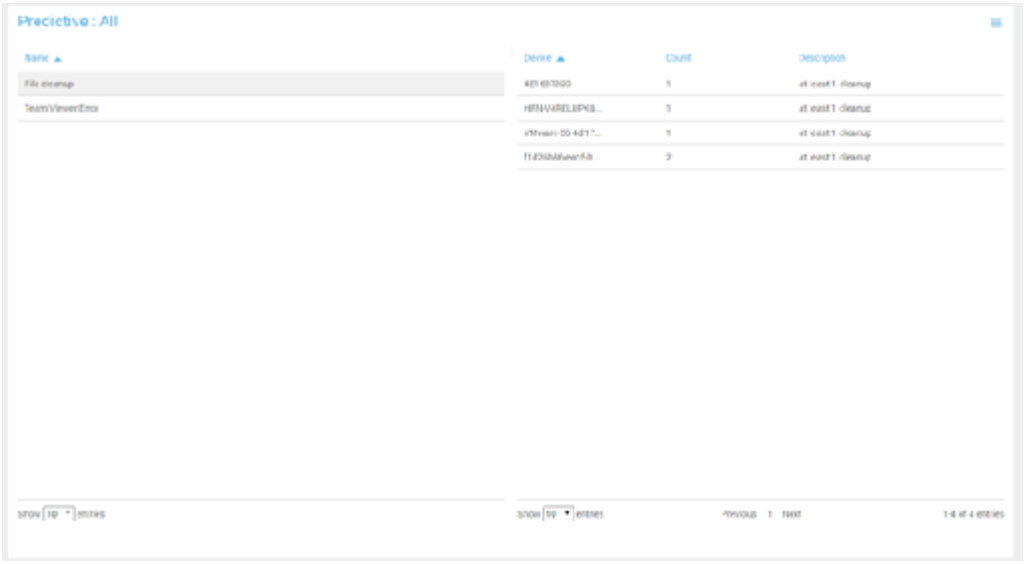
The user can view Resolutions details from the Dashboard > Resolutions menu > Predictive as shown below.



Upon clicking "Predictive" from the Resolutions menu, the following page will be shown.



Predictive will have data related to Autoheal, file clean up, intrusion protection registry rejection, start-up registry item data rejection, some apps like Team Viewer crashed etc. As the name Suggests, we predict few related changes happening to machine and generate data for the same. We have a DART 77 (Windows Logs Changes Detected) which when enabled will capture all logs that is captured by Windows Event Viewer. Hence, using this, we can get to know what is happening on the machine and action them as required.

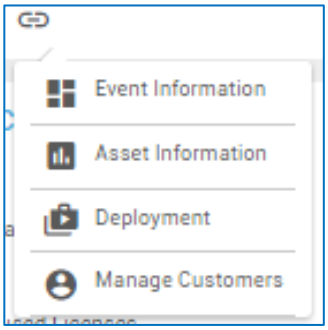


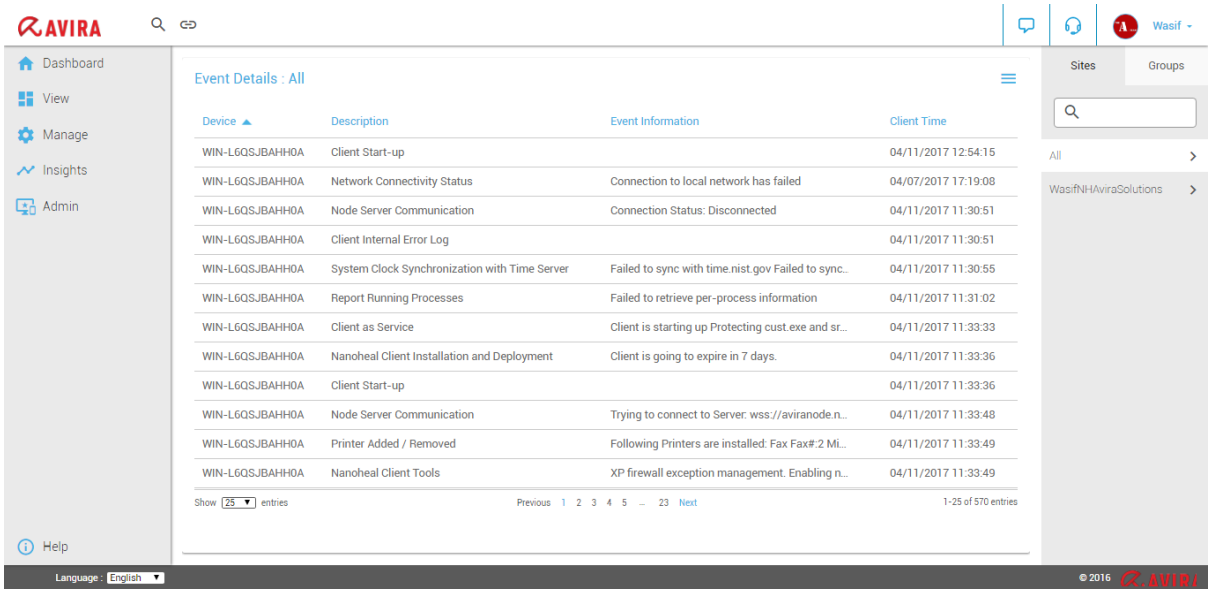
The screenshot above shows file clean-up data.

Event Information

1. Events are the actions that are performed on a machine when a DART gets executed. It provides details of execution time, results after execution, etc.
2. A DART is a mechanism to perform set of defined actions on a given machine.
3. For instance, when DART 77 (Windows Event Log Detected) runs, it logs all Windows events. When DART 189 (File Download Filtering) runs, it blocks the list of file types that have been specified by the user.
4. Easy tracking down of the events helps the end user to understand the problem. After successful analysis, the appropriate resolution can be applied to the machine.
5. Events that are captured are not only related to OS but also outside OS through its own event logging mechanism.
6. End User can track down the events occurring on a machine on a real-time basis.
7. Events can be analyzed for a group of machines or a given site or multiple sites.

In order to navigate to the Events Page, the user has to click on the breadcrumb link on the top left corner and then click on the Event Information as shown below:

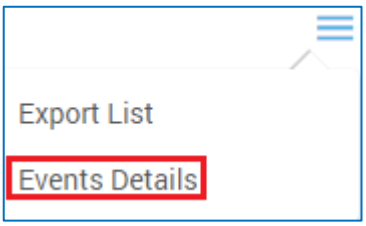




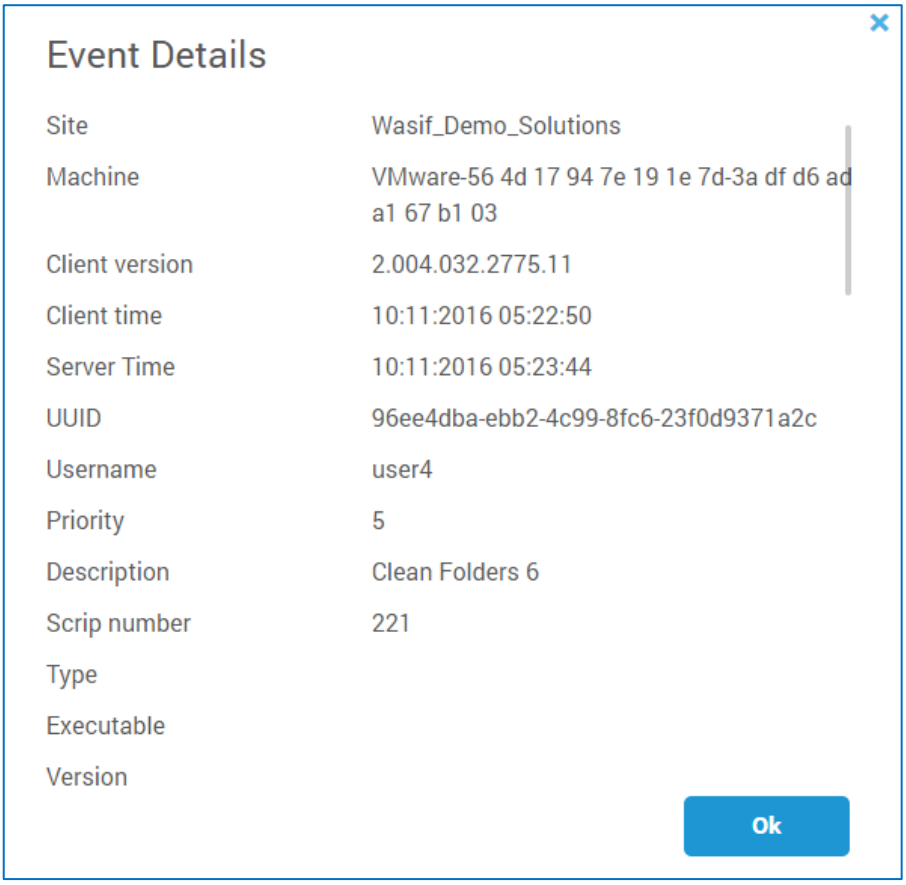
As shown in the screen above, every event record provides information about machines on which it occurred, time at which it occurred, corresponding DART that was executed, brief description about execution. For more details, user has to click on "Events Details" link available at the right-side menu.

Event Detail

The user can view the event details by selecting any event record and clicking on the top right menu and selecting the Events Details link as shown below.

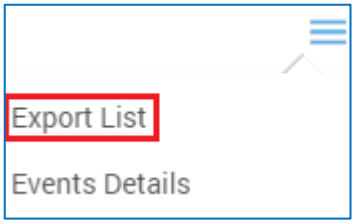


Upon clicking the Events Details link, Event Detail pop appears, showing all the event details as shown in the screenshot below:



Events Export

The user can also export all the events data that has been displayed on the page into excel for future reference. In order to export, click on the "Export List" link available on the top right side menu icon on the same page as shown below.

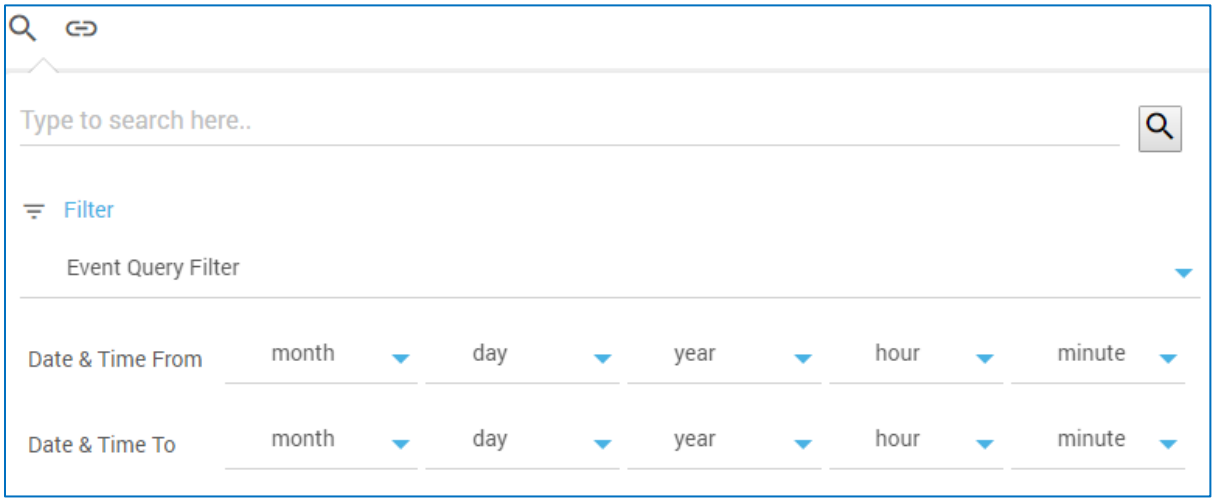


Upon clicking "Export List", it will export the data to .xls format.

	A	B	C	D	E
1	**Description**	**Event Information**	**Executable**	**Client Time**	**Server Time**
2	Scrip Configuration Update	Client is synchronized		2016-11-10 02:47:57	2016-11-10 02:49:34
3	Process Completion Detected		WMIC.exe	2016-11-10 02:48:40	2016-11-10 02:49:38
4	System Survey	Completed data collection		2016-11-10 02:47:44	2016-11-10 02:49:41
5	Machine list management	Reporting machine list. See field text4.		2016-11-10 02:48:44	2016-11-10 02:49:44
6	Microsoft Update Management	Scrip state: execute software update The Scrip is not currently performing a repeat software update install cycle		2016-11-10 02:47:56	2016-11-10 02:49:48
7	Process Completion Detected		WMIC.exe	2016-11-10 02:48:54	2016-11-10 02:49:51
8	Send Queued Asset Logs	Asset synchronization with server is done		2016-11-10 02:48:42	2016-11-10 02:49:57
9	Process Completion Detected		WMIC.exe	2016-11-10 02:49:02	2016-11-10 02:50:00
10	Scrip Configuration Update	Client is synchronized		2016-11-10 02:48:40	2016-11-10 02:50:04
11	Process Completion Detected		WMIC.exe	2016-11-10 02:49:50	2016-11-10 02:50:09
12	Process Completion Detected		WMIC.exe	2016-11-10 02:50:04	2016-11-10 02:50:13
13	Process Completion Detected		wpsupdate.exe	2016-11-10 02:53:00	2016-11-10 02:53:05
14	Physical Disk Statistics	mSec Sampling period: 30000 Drive: 0 C: E: D: Percent busy time: 0 Reads per second: 0 Writes per second: 1 Average queue length: 0 Drive: _Total Percent busy time: 0 Reads per second: 0 Writes per second: 1 Average queue length: 0		2016-11-10 02:58:37	2016-11-10 02:58:42
15	Process Completion Detected		WMIC.exe	2016-11-10 03:00:11	2016-11-10 03:00:16
16	Process Completion Detected		WMIC.exe	2016-11-10 03:00:18	2016-11-10 03:00:24
17	Process Completion Detected		WMIC.exe	2016-11-10 03:04:20	2016-11-10 03:04:26
18	Process Completion Detected		UI0Detect.exe	2016-11-10 02:47:56	2016-11-10 02:48:50
19	Software patch (User mode with thread)	HTTPError or FTP server not ready.		2016-11-10 02:47:56	2016-11-10 02:48:54
20	Process Completion Detected		regsvr32.exe	2016-11-10 02:47:58	2016-11-10 02:48:57
21	Process Completion Detected		WMIC.exe	2016-11-10 02:48:00	2016-11-10 02:49:03

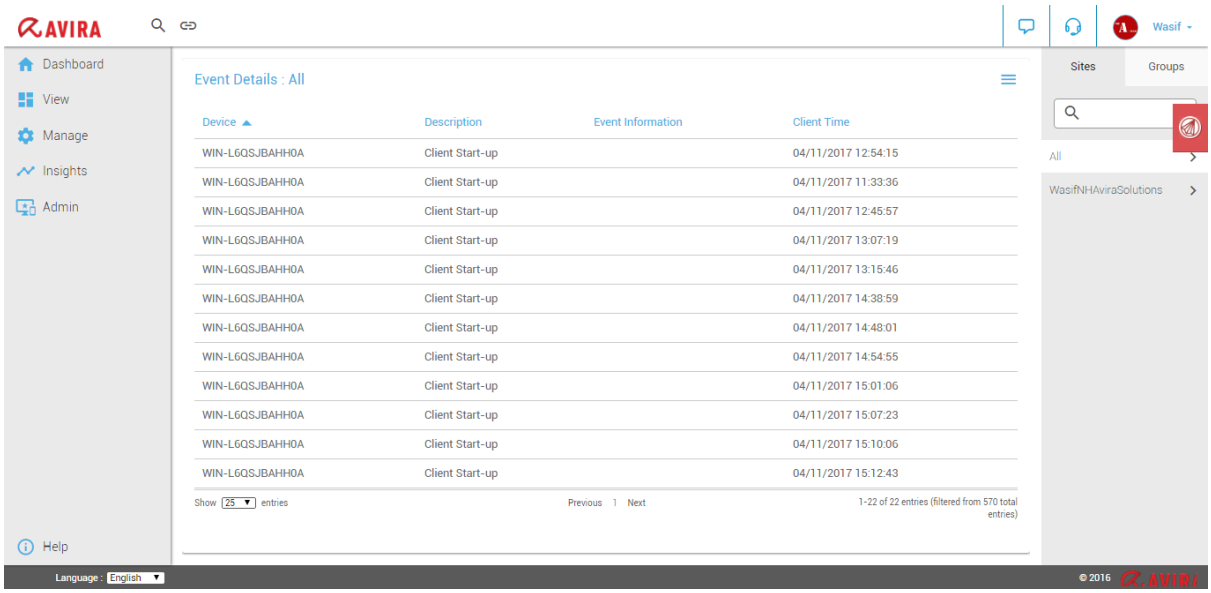
Event Filter Search

The user also has an option to search for events based on different criteria. Like search based on Event Filters / search based on different date ranges etc. In order to perform this activity, the user has to click on lens icon which is available at the top left corner of the screen.



As shown in the screenshot above, event search criteria pop-up opens up. The user can search events based on the following:

- **Event Query Filter**: Search events based on event filters. Event Filter is nothing but events of interest
- **Date & Time From, Date & Time to:** Search events between two dates. Enter the desired date and time range and click the lens icon



Asset Information

1. Assets provide software and hardware related information of a particular machine

2. End user can study the asset details and use the data for Efficient Asset Auditing, IT inventory management, etc. for the machines

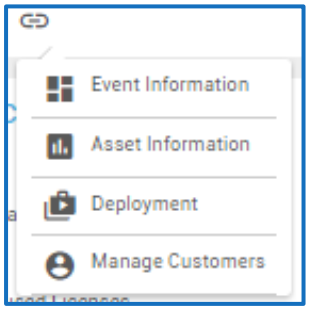
3. All the Asset details get captured for every machine that starts reporting to the dashboard

4. Having all the asset details captured helps the user to logically group the machines on the basis of any asset data in an organized and comprehensive way

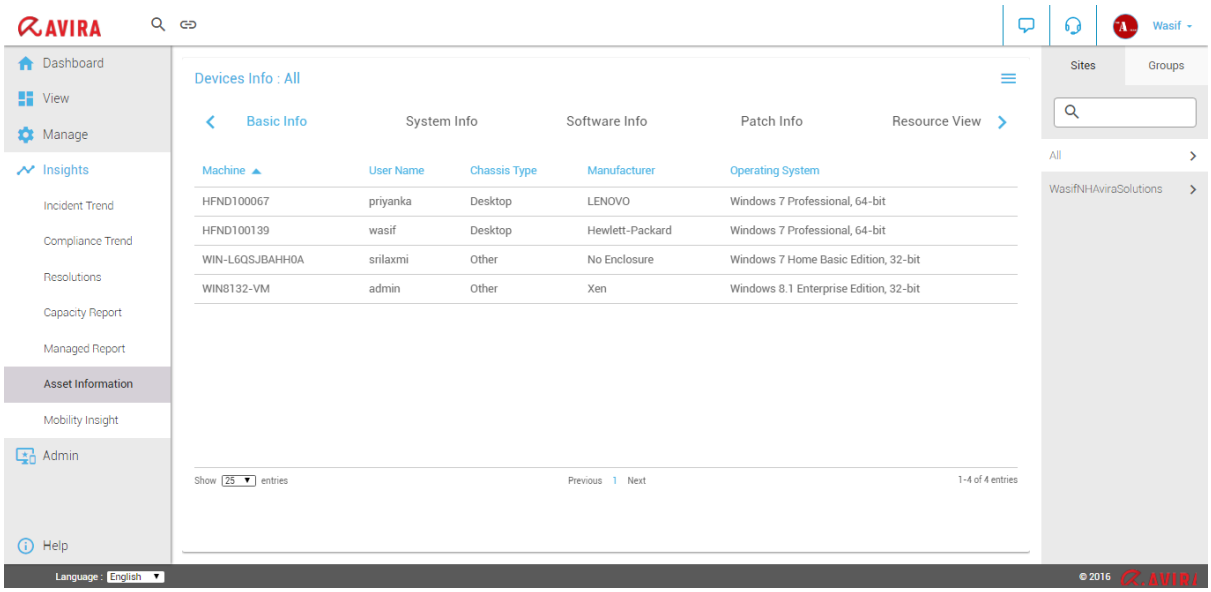
5. The changes introduced across the assets can be managed through logging them and generating reports which can be scheduled either to be mailed to the relevant person or it can be published on the information portal on the server

User can view asset information by two ways:

1. User would need to click on the breadcrumb link and then click on Asset Information as shown below:



2. User can go to insights>Asset information



The following information is displayed:

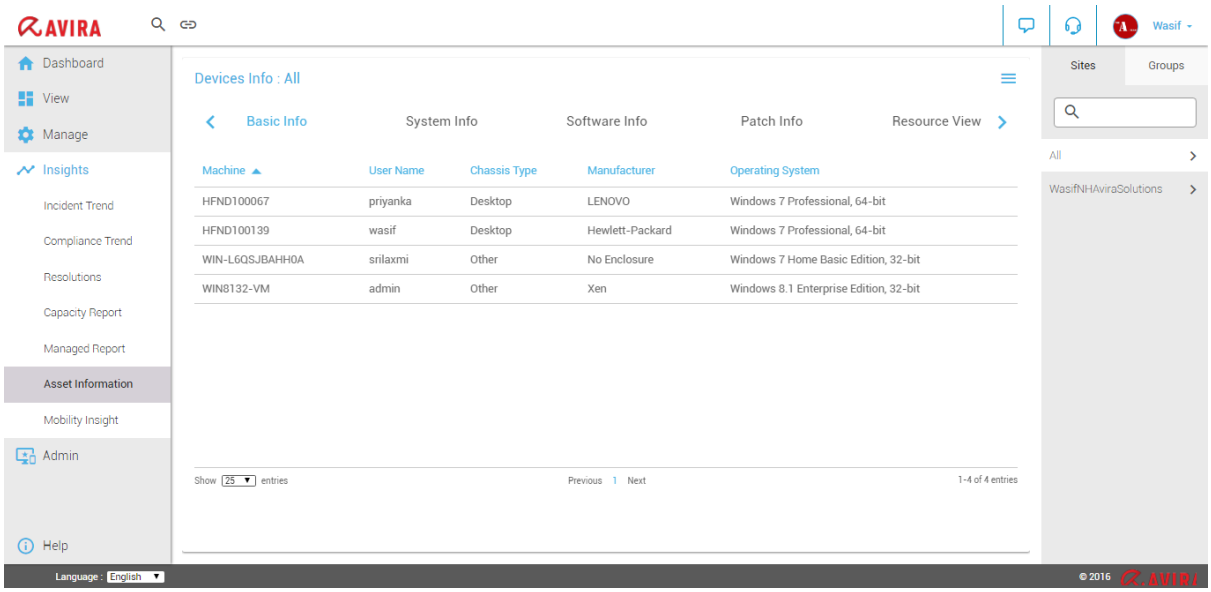
- Basic information of the machines
- System information of the machine
- Software Information of the machines
- Patch Information of the machines
- Resource view of the machines
- Network Information of the machines

The Asset Information page has 5 Tabs:

1. Basic Info

The module opens up with the "Basic Info" screen. As shown below, the grid data has following information:

- Machine: Machine name for which data is being shown
- User Name: Username of that machine
- Chassis Type: Chassis Type of the machine
- Manufacturer: Name of the manufacturer
- Operating System: Operating System of machine

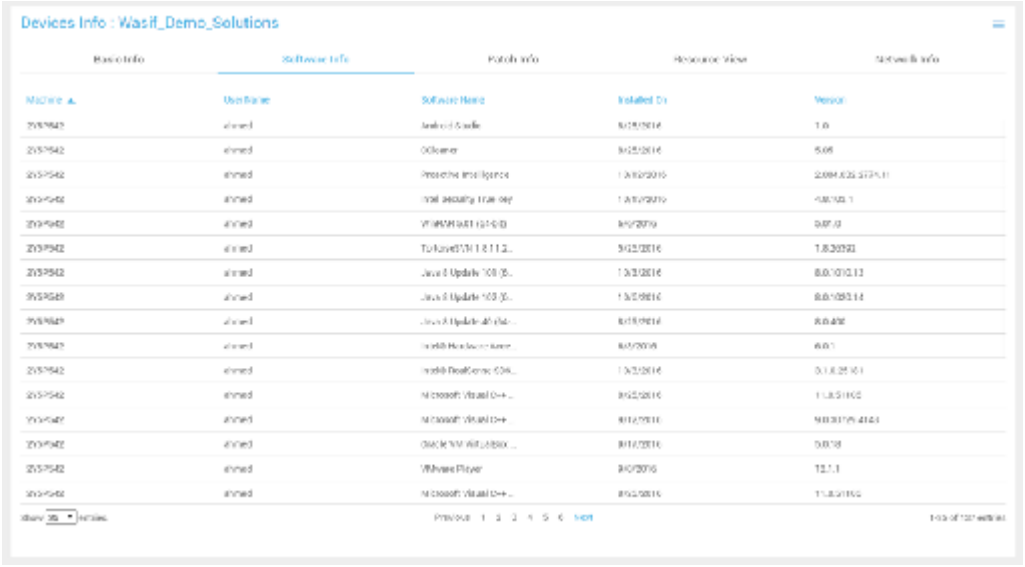


2. System Info

The System Information tab will show details about system:

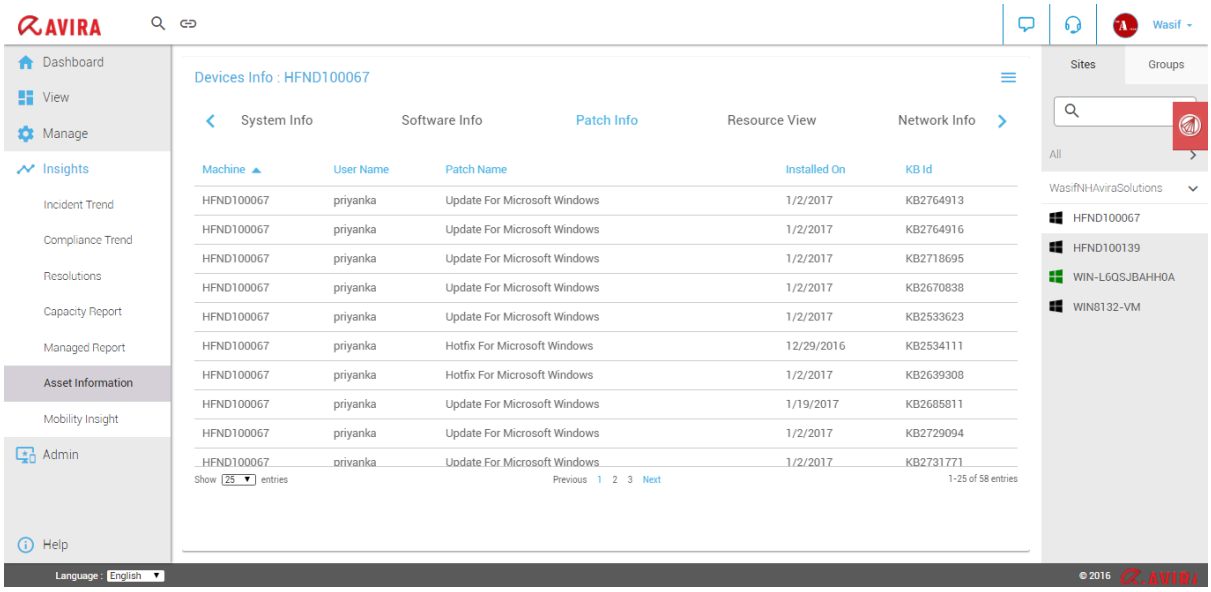
3. Software Info

The Software Information tab will show the list of software installed:



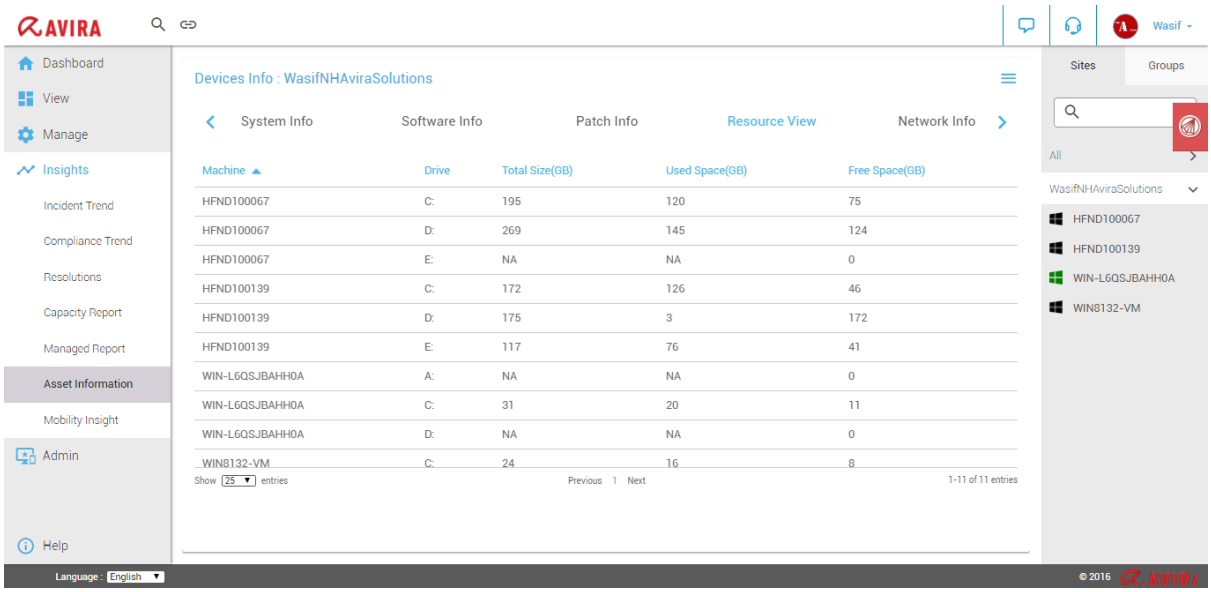
4. Patch Info

The Patch Information tab will show the list of Microsoft Patches installed:



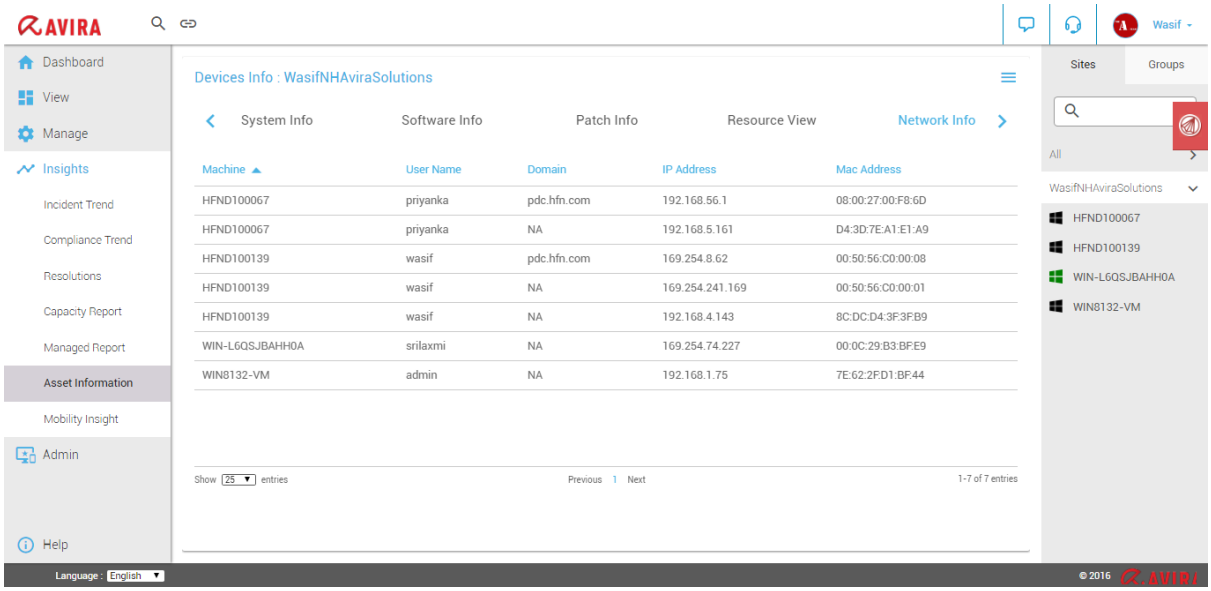
5. Resource View

The Resource View tab will list all the machine Drives along with Total Size (GB), Used Space (GB) and Free Space (GB) as shown below:



6. Network Info

The Network Info tab will list all network related information of the machine:

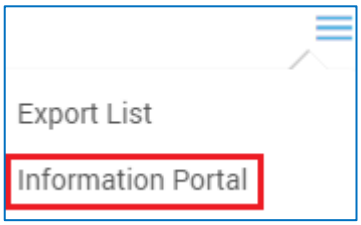


Export

The "Export List" option available under the menu at the top right which can export the screen data on to an xls file.

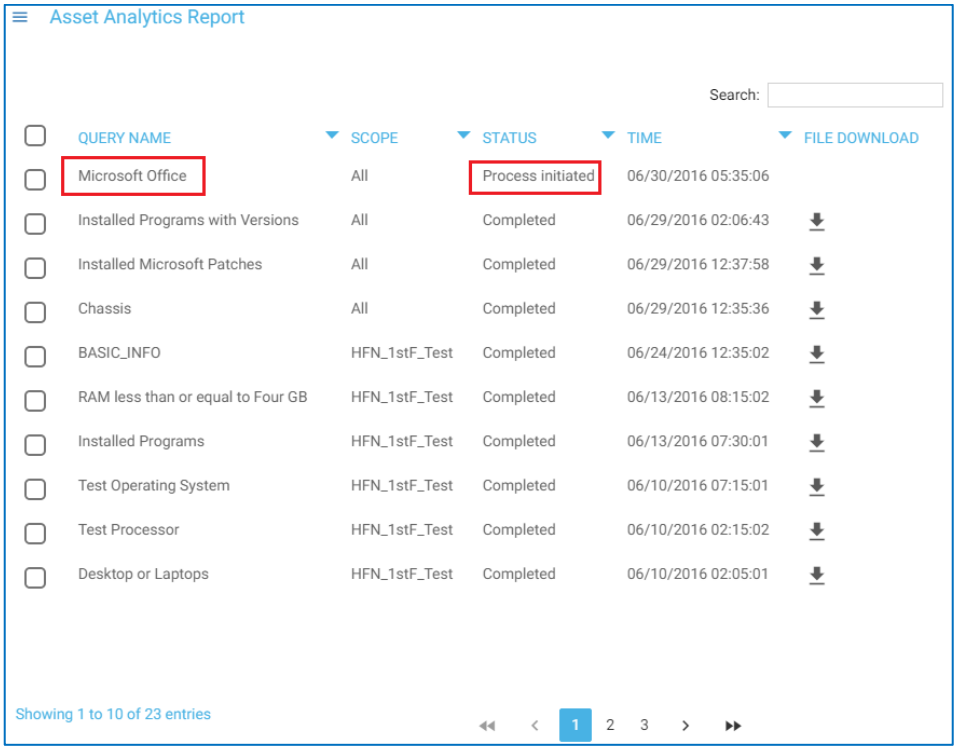
Asset Analytics Report

The Asset Analytics Report provides an analysis of the asset components. This option is available on the Asset Information page menu as 'Information Portal' as shown below.



In order to navigate to the Asset Analytics Report pop up, the user needs to click on breadcrumb link and then click on asset information. Then click on menu icon and click on "Information Portal" link as shown above.

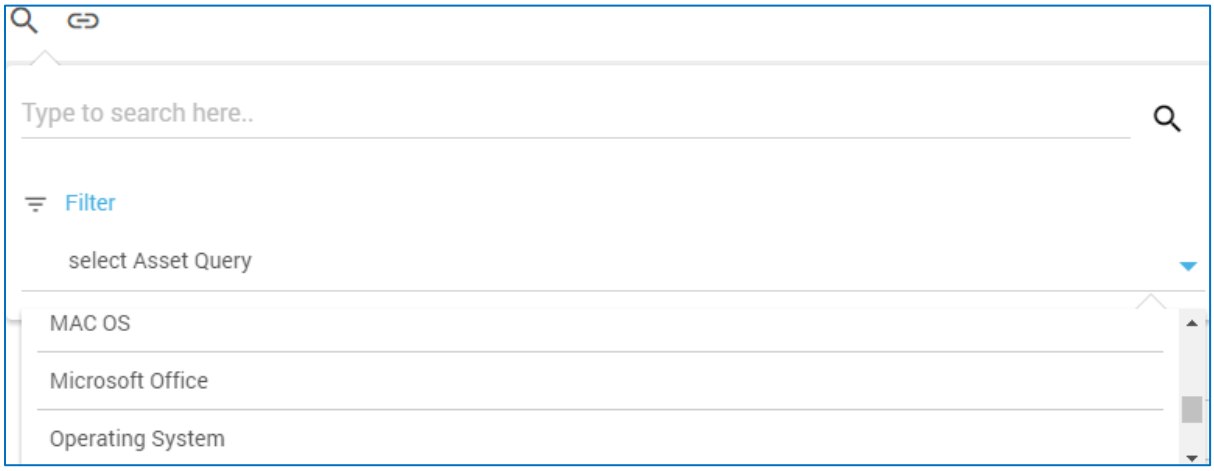
Once Information portal link is clicked, the Asset Analytics Report pop up will be shown as below.



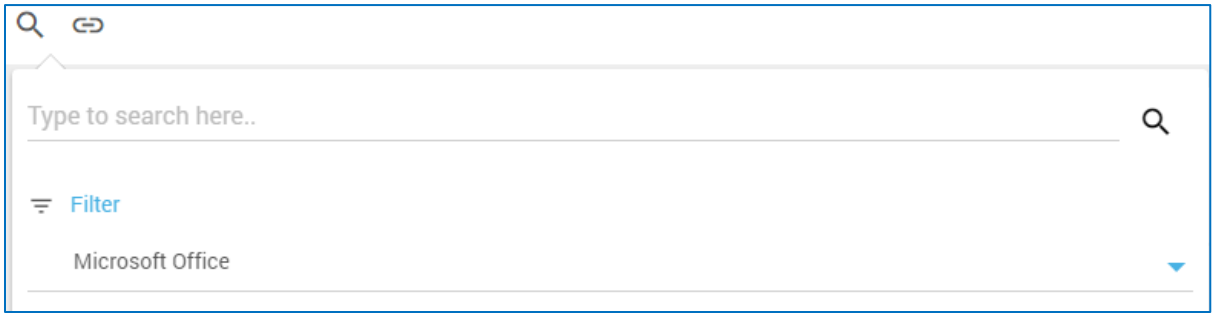
Asset Query Execution

In order to generate an Asset Analytics Report, the user needs to execute Asset Queries.

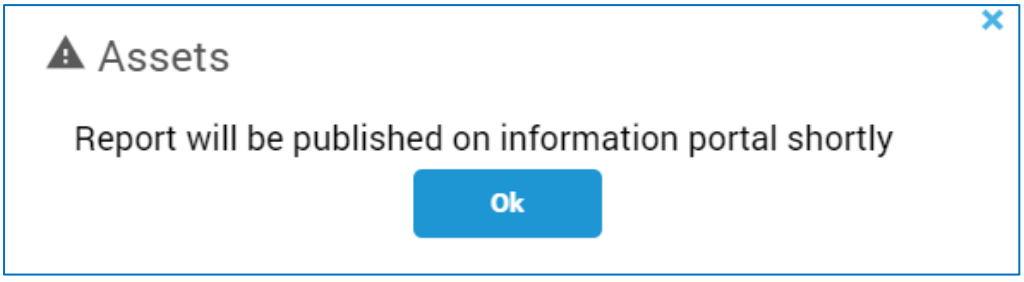
This can be done by clicking on Search icon >>Asset Radio button>> asset query from drop down >>search icon. These steps would post the report to the information portal.



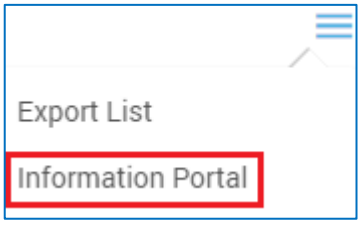
As shown in the screenshot above, there are inbuilt asset queries which when executed will provide output based on the purpose it serves.

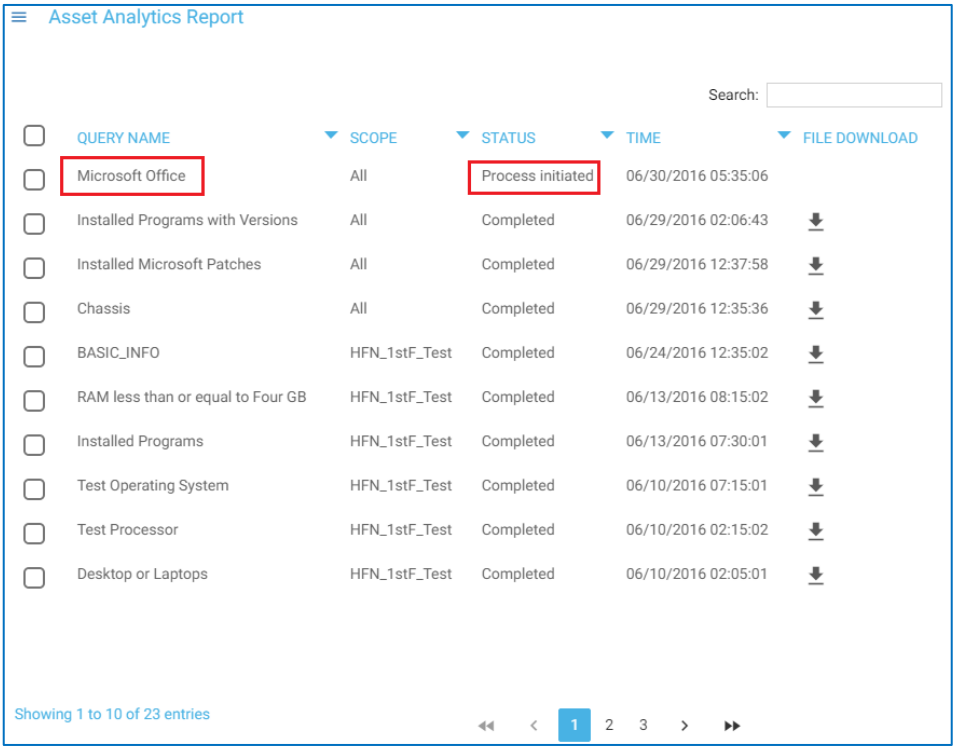


After the user clicks on the search icon on right side as shown in the screenshot above – the report will be posted on to the information portal and an alert will be displayed.



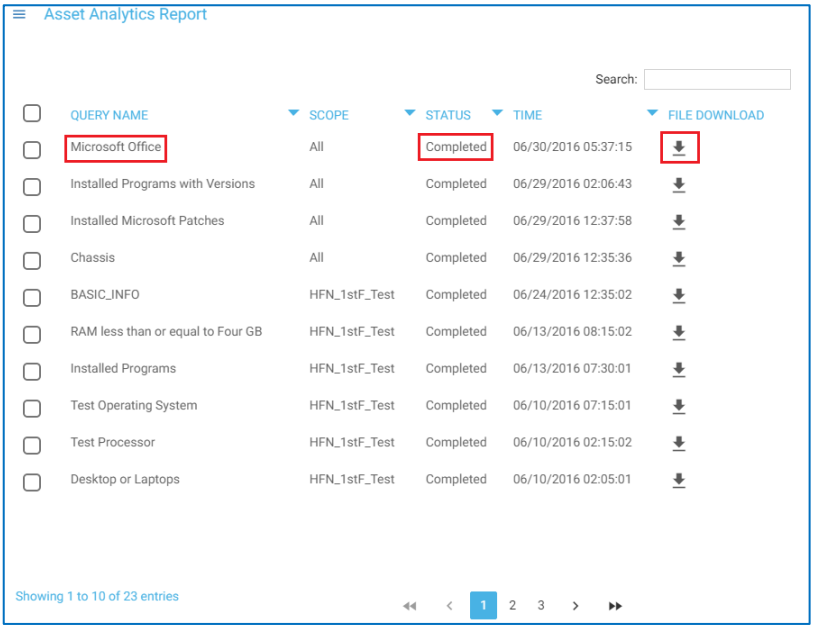
The user can now click on 'Information Portal' from right menu as shown in the screenshot below to get to the report





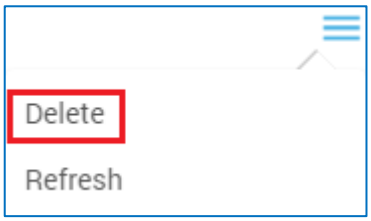
Asset Report Download

Once query is completed, it is shown as "Process Completed" with a download button to download the query output on to an xls file.



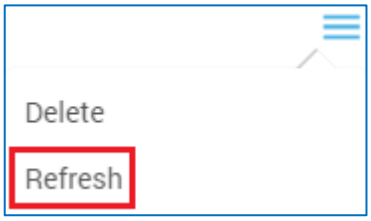
Asset Analytics Delete

The option to delete is available on the right menu icon as shown in screenshot below.



Asset Analytics Refresh

We can also refresh the Asset Analytics Report window by clicking on Refresh link available under left menu as shown in the screenshot below.



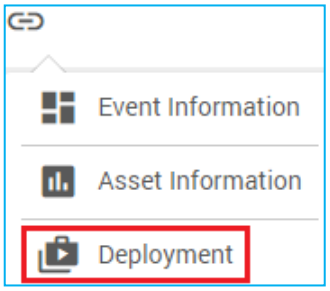
Deployment

Deployment is used to install the Nanoheal and AVIRA Clients on multiple systems at once.

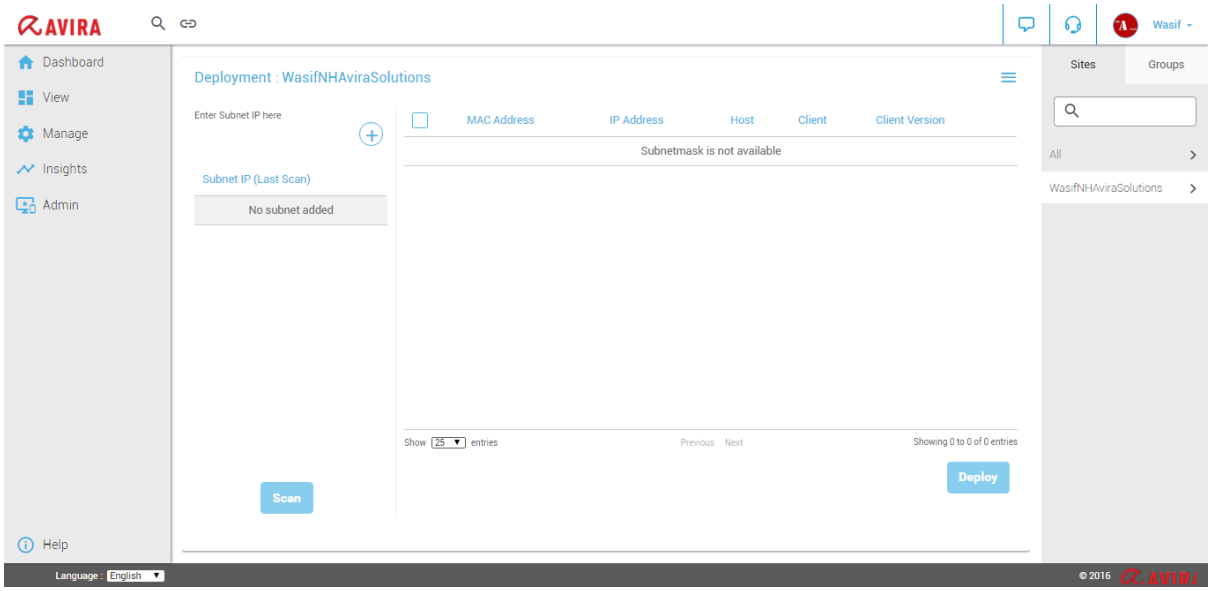
Please refer to the section – NH Pre-Requisites to understand the needs and ensure readiness towards deployment.

Please do note that Nanoheal Client Network Deployment will not work on sub-nets that do not have all the devices under the same domain. Nanoheal Client Network Deployment works only if the machines are in a domain.

To perform Deployment, navigate to the bread crumb icon at the top left corner of the page and click on Deployment, as shown below.



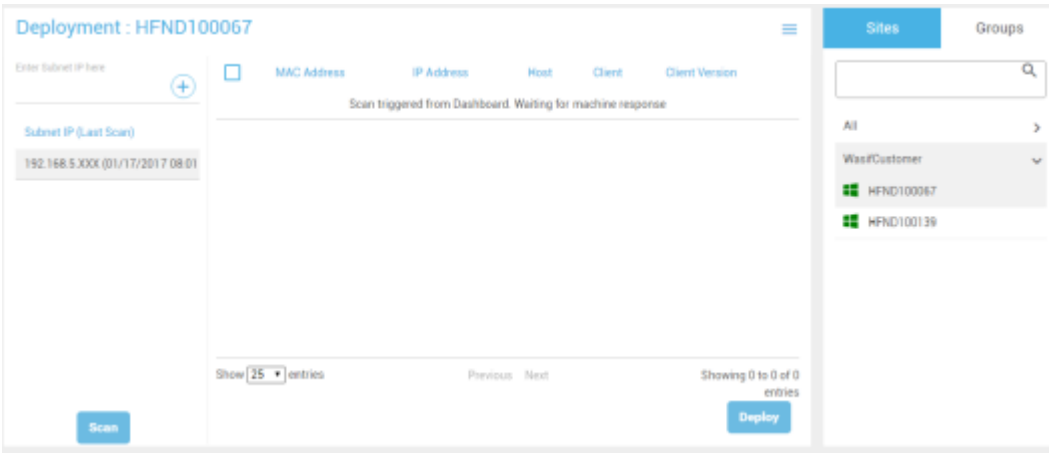
Deployment looks similar to the image shown below:



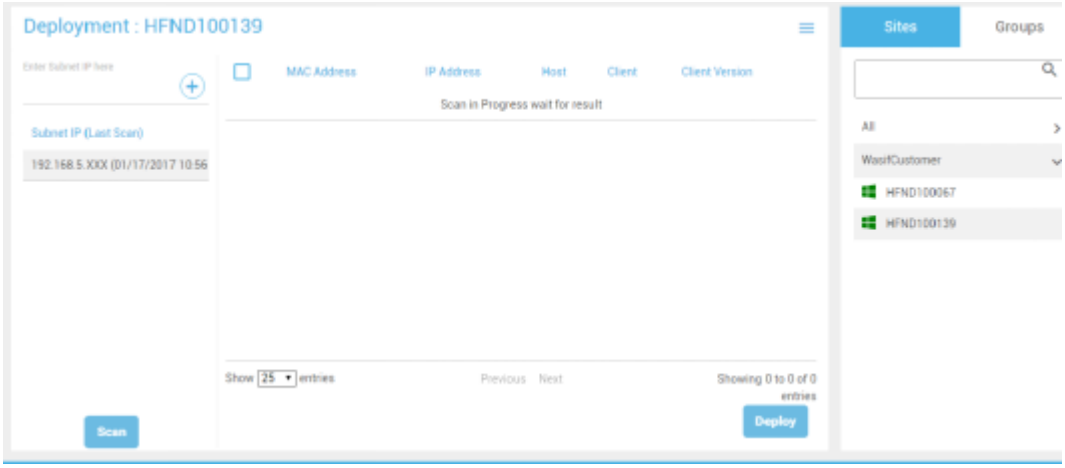
Steps

1. Enter the Subnet IP in the space provided, and click on icon..

2. Select the IP from the left pane and a corresponding machine from the right, and click on Scan. Please note that the machine must be 'Online' for scanning. Once the scan is initiated the dashboard screen would look similar to the one shown below:

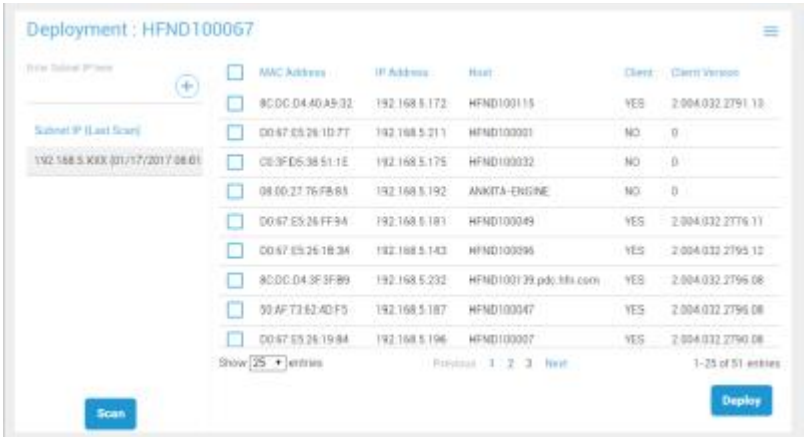


3. Refresh the page to get the status of the scan.

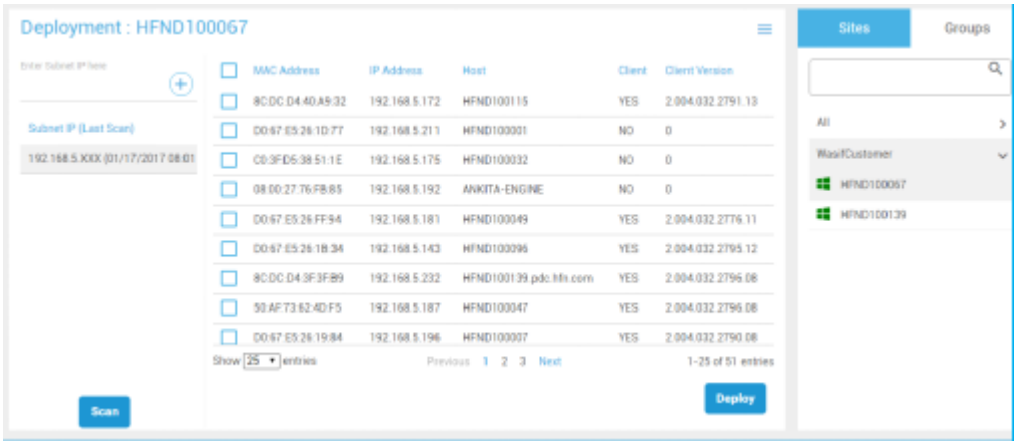


4. Once the scan is completed, select the IP from the left hand side and the corresponding data is populated on to the right. Table on the right shows information related to the selected Subnet IP. The table has following details :

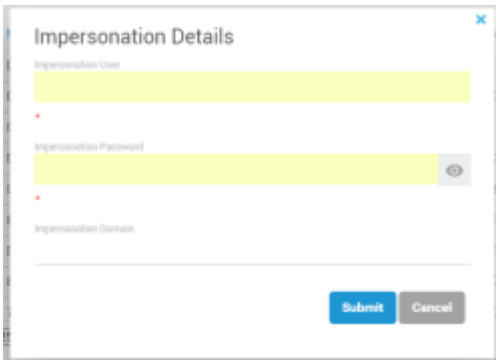
    a. MAC Address
    b. IP Address
    c. Host
    d. Client installation status
    e. Client Version.



5. Before deploying, set impersonation credential by navigating to the menu icon on the top right corner and by selecting impersonation settings. A sample is shown below:

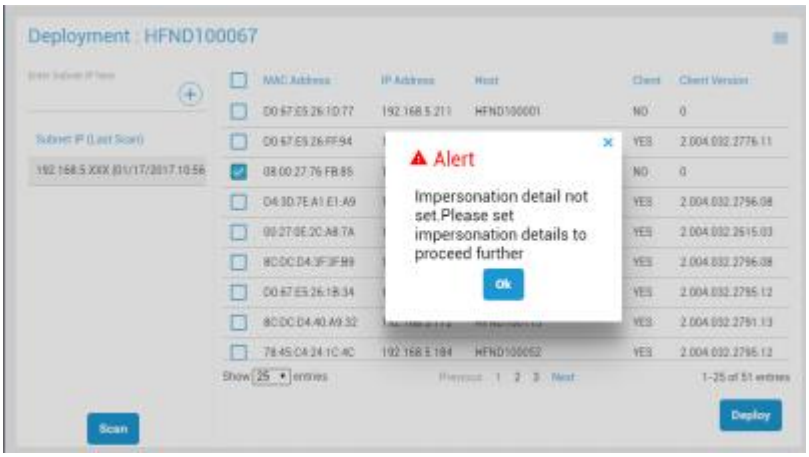


6. Enter appropriate values in the required fields. The values asked for, are:
    a. Impersonation user name
    b. Password
    c. Domain on which deployment is set to happen



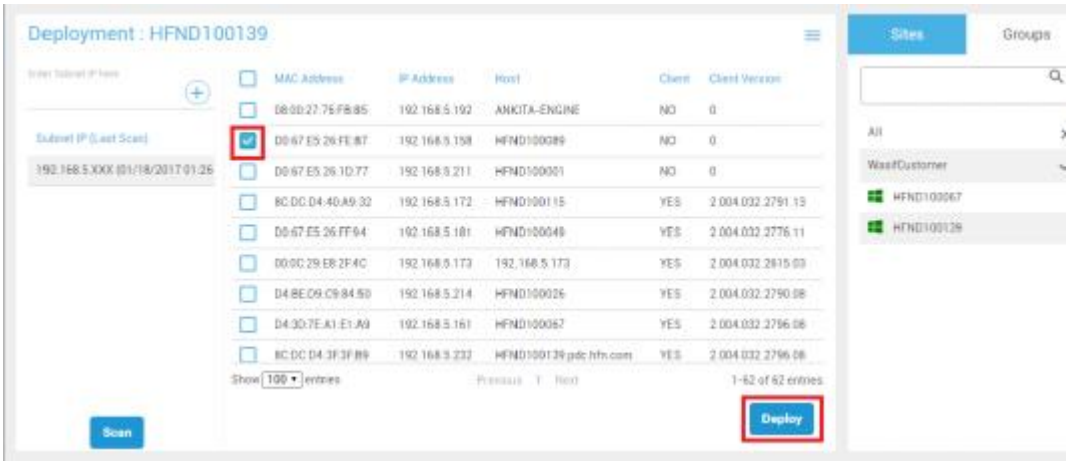
7. Submit the impersonation data and proceed with deployment to install the client on all the machines that are reachable.

Note: If impersonation has not been set and if a user tries to deploy the client on to the machines they will receive an alert stating the same. An example is shown below:

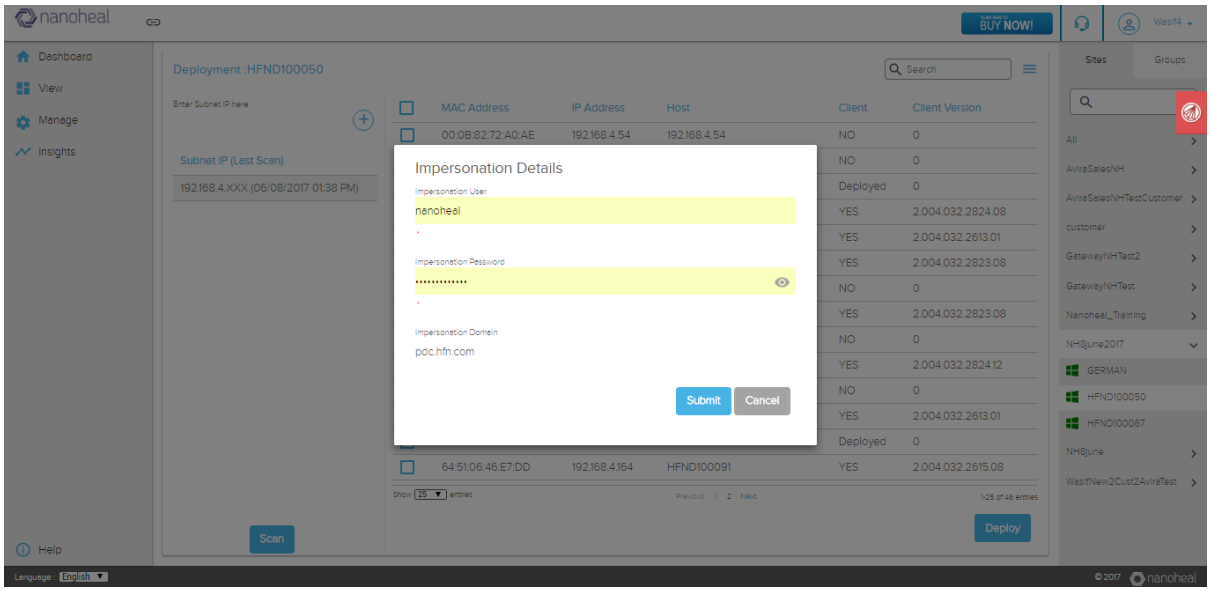


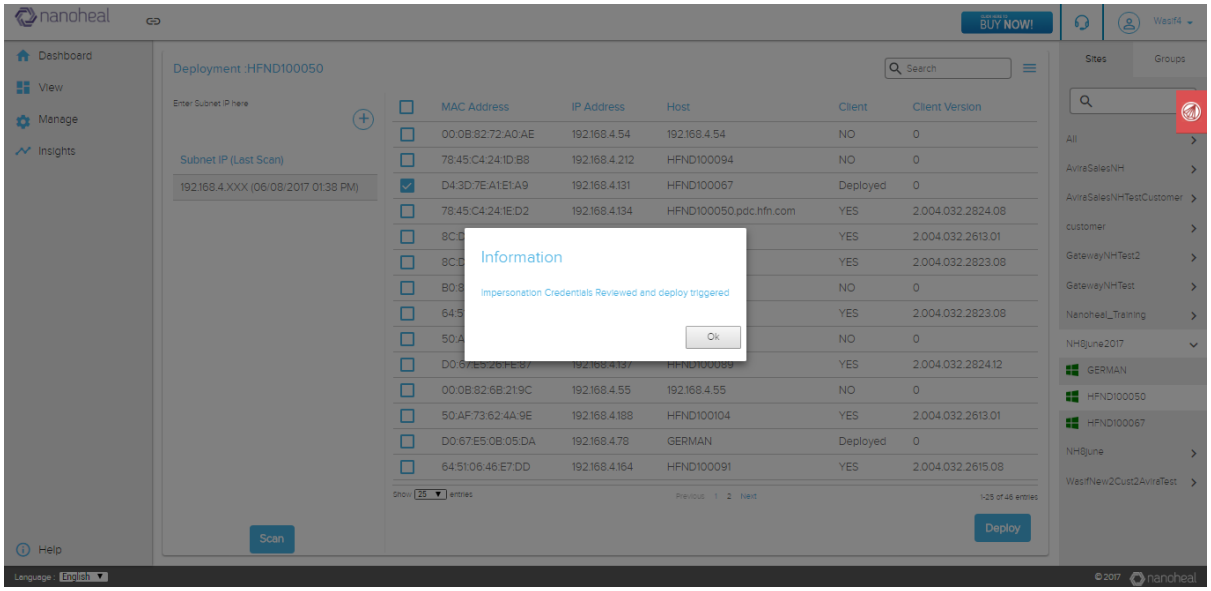
Deployment

1. Select the check box corresponding to the machines that have the column named "Client" set to a 'NO' & Client Version set to '0'.

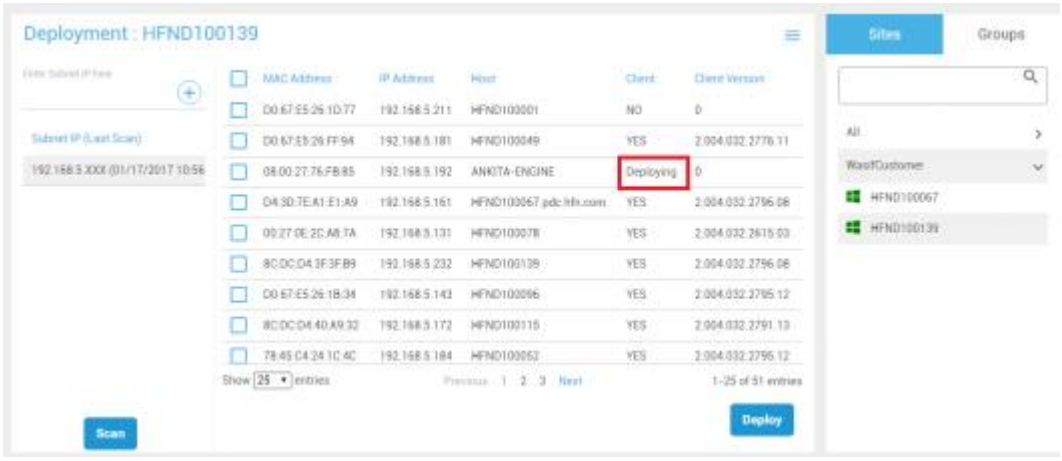


2. Click on the Deploy button to deploy the client on to the selected machines. It will review the impersonation credential provided as shown below:

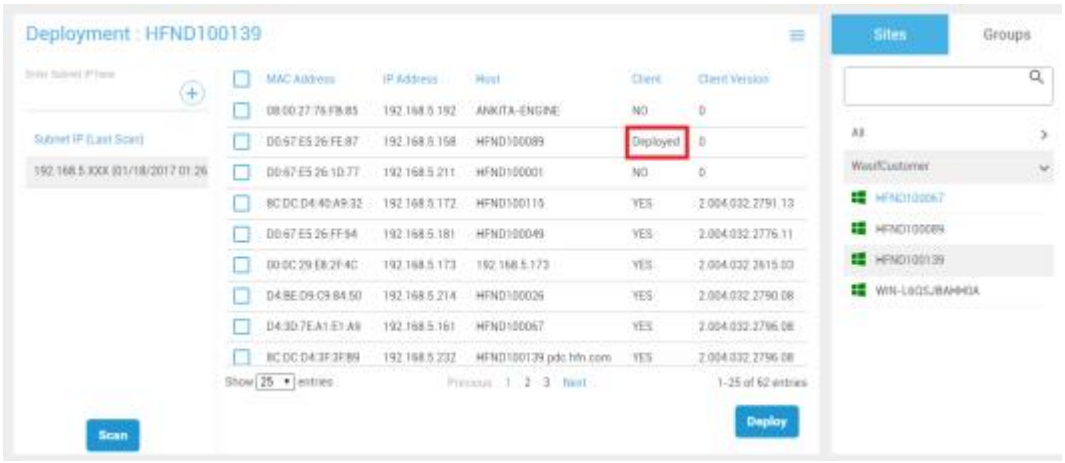




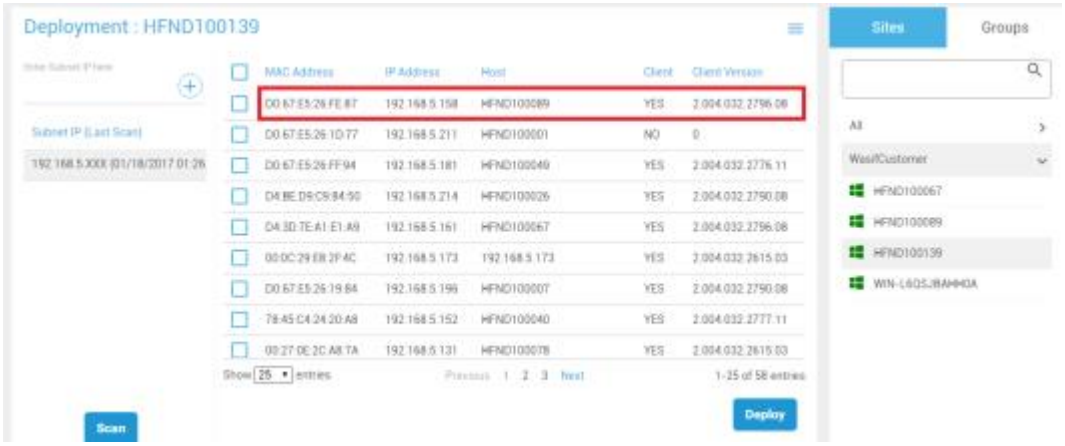
The status under the "client" column should change to "deploying" at this stage as shown below:



3. Once the client has been successfully deployed, the status will change from 'deploying' to 'Deployed'. Please note - the page must be refreshed for this change to reflect onto the table.

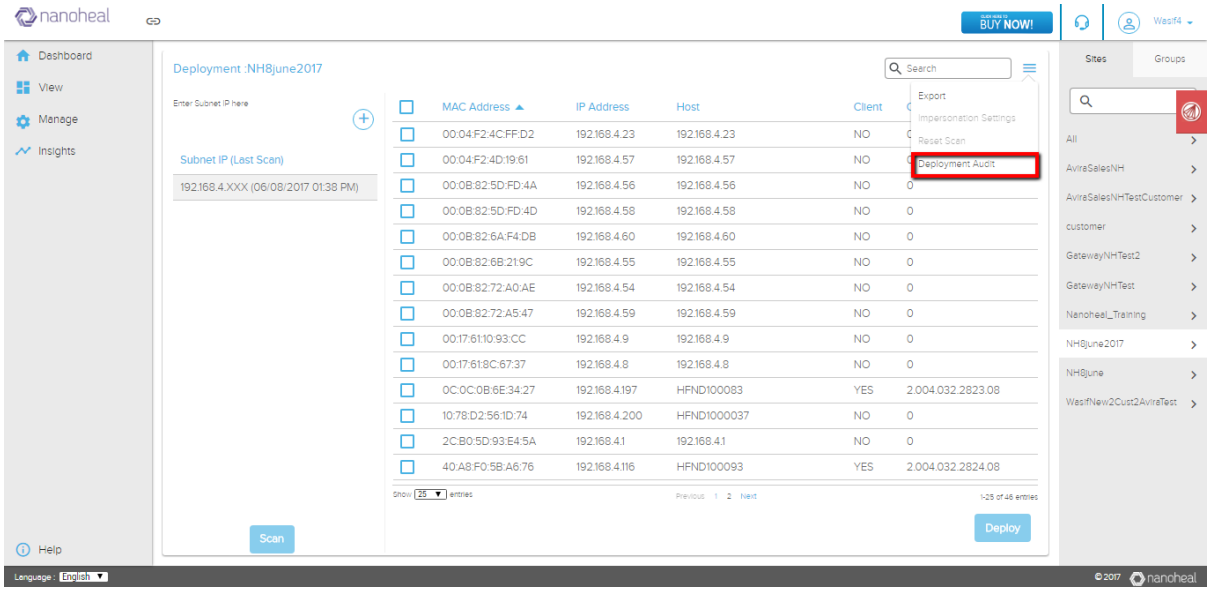


4. Once the installation is completed successfully, scan the subnet again to see that the client has been successfully installed, and to see the corresponding client version updated on the table.

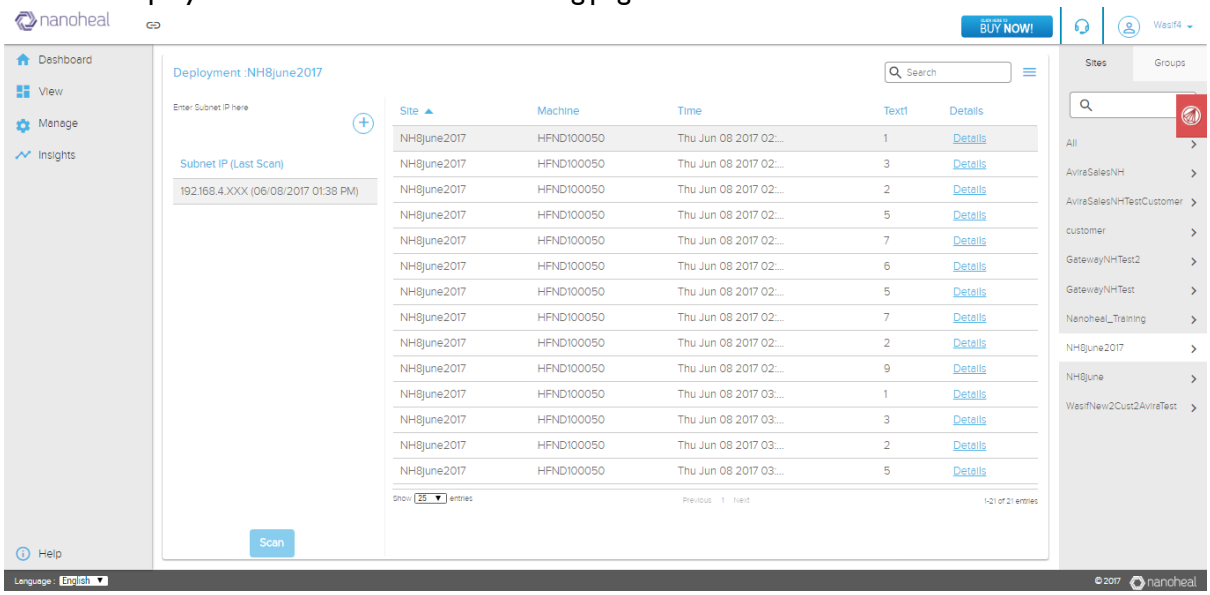


Deployment Audit

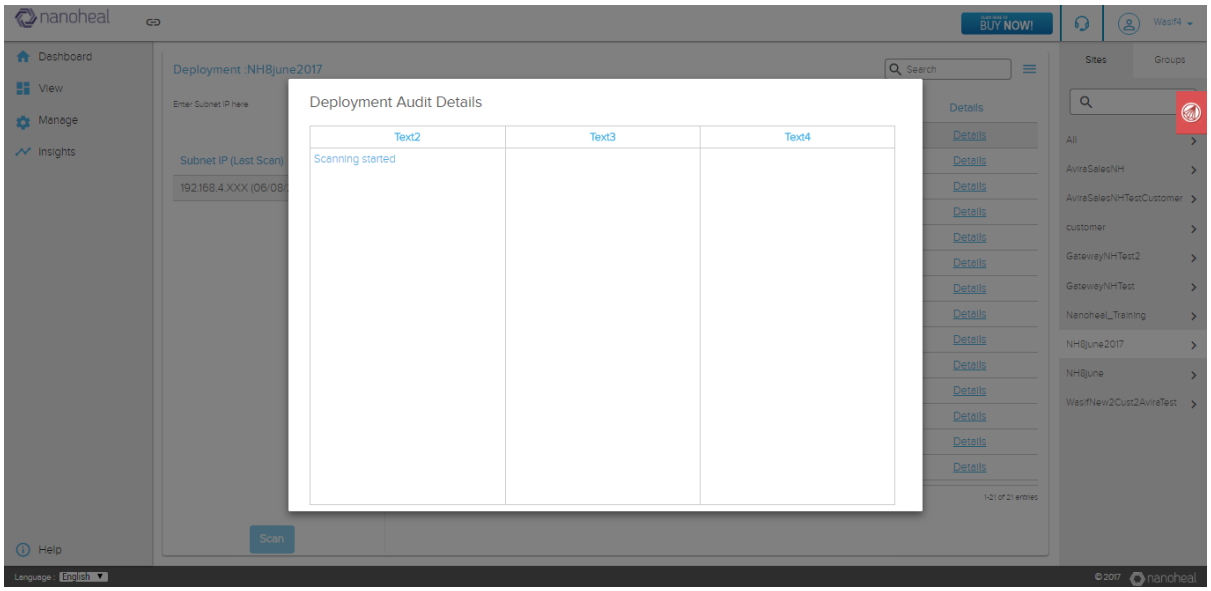
Customer can also view and export Deployment Audit data by following below steps:



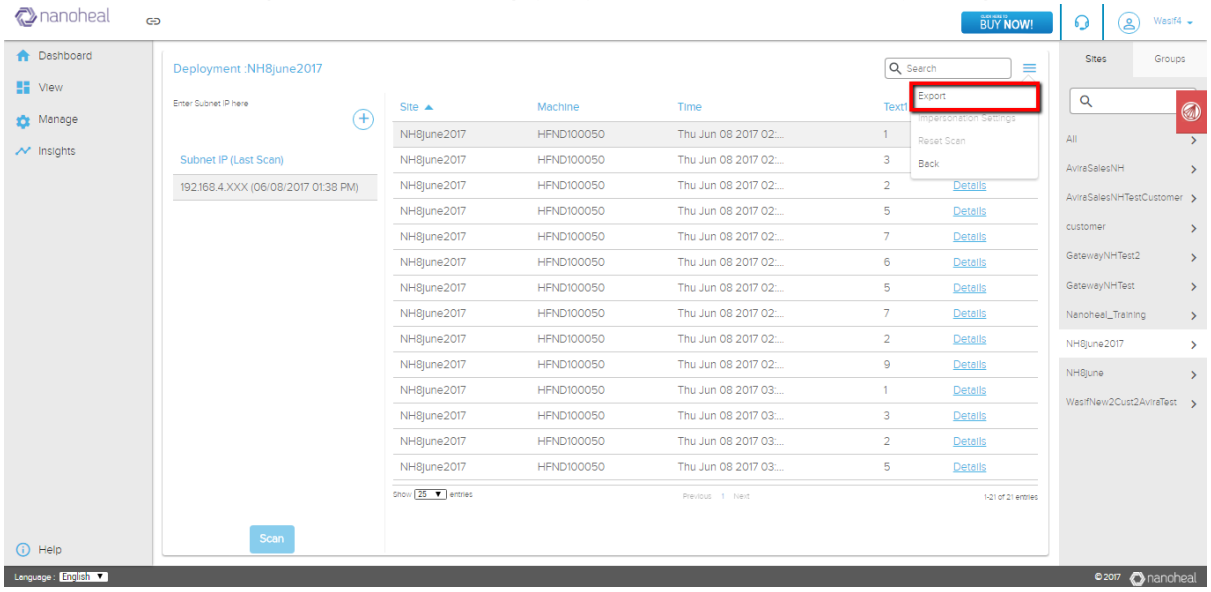
Click on Deployment audit will take to following page:



Click on details will show the information of deployment on that particular machine:



Customer can also export the audit data by going to menu icon and clicking on export:



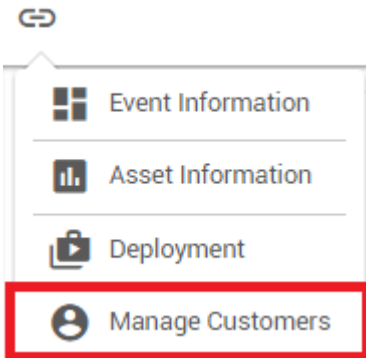
Data will get downloaded in .xls file as shown below:

	A	B	C	D	E	F	G
1	Host	Site	Mac Address	IP Address	Client Available	Client Version	Last Scan
2	192.168.4.54	NH8june2017__20170001638	00:0B:82:72:A0:AE	192.168.4.54	NO	0	06/08/2017 12:57 PM
3	HFND100067	NH8june2017__20170001638	D4:3D:7E:A1:E1:A9	192.168.4.131	Deployed	0	06/08/2017 12:57 PM
4	HFND100081	NH8june2017__20170001638	64:51:06:47:2E:2C	192.168.4.155	YES	2.004.032.2823.08	06/08/2017 12:57 PM
5	HFND100050.pdc.hfn.c	NH8june2017__20170001638	78:45:C4:24:1E:D2	192.168.4.134	YES	2.004.032.2824.08	06/08/2017 12:57 PM
6	HFND100139	NH8june2017__20170001638	8C:DC:D4:3F:3F:B9	192.168.4.143	YES	2.004.032.2823.08	06/08/2017 12:57 PM

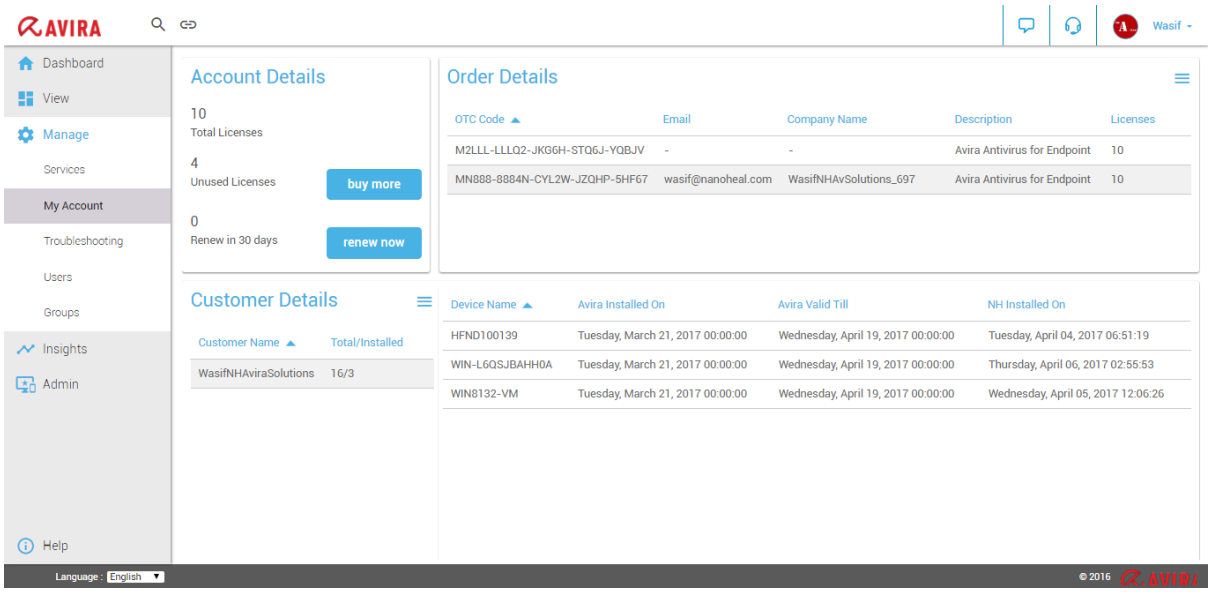
Manage Customers

Please follow the following steps to manage a customer:

Navigate to the "Manage customer" from the quick links on the top left corner.



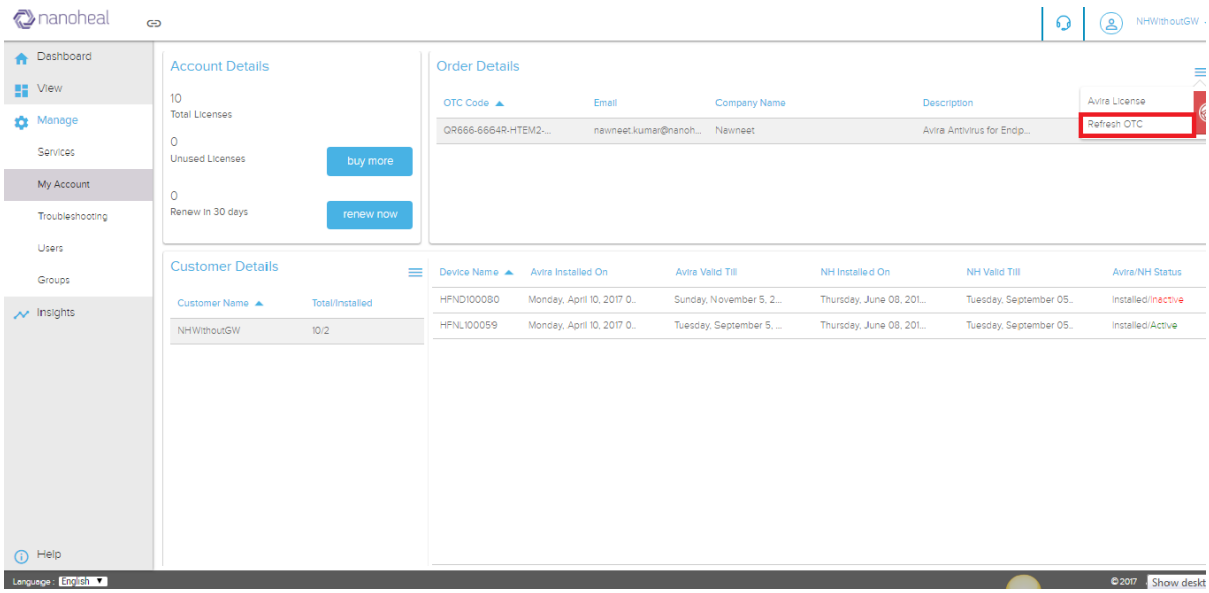
The user can manage existing customers; add new OTCs and customers from here.



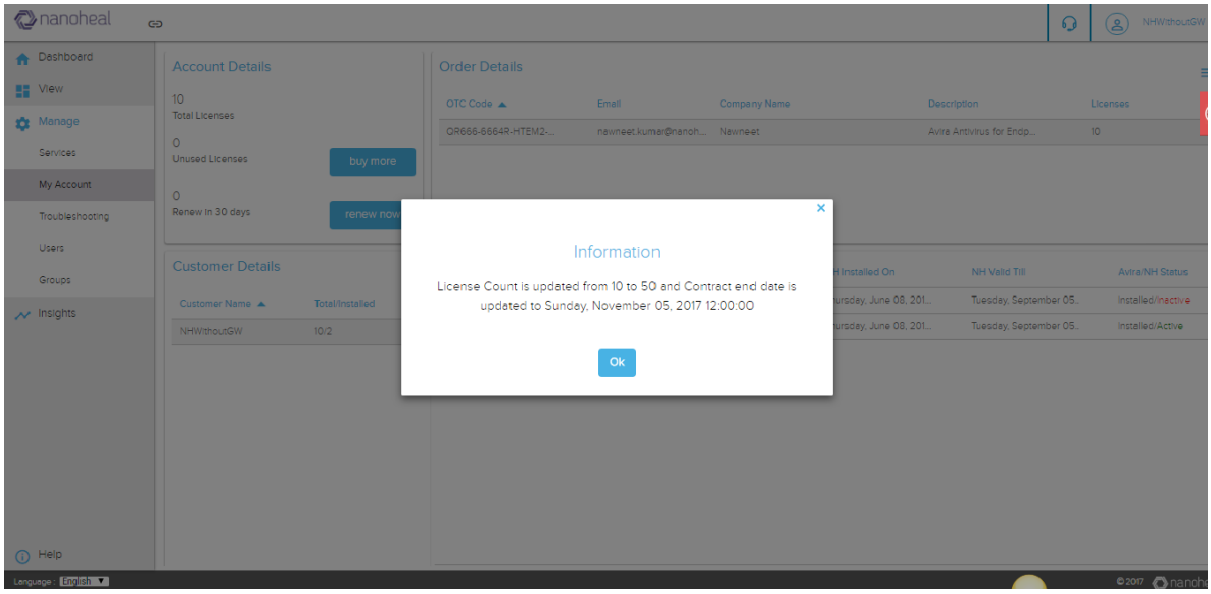
Refresh OTC

If there is any change in license data of any OTC, those changes will be reflected on server by doing refresh OTC. Select the OTC and click on refresh OTC under order details menu iconsssssssssss. It will refresh the data of that particular OTC.

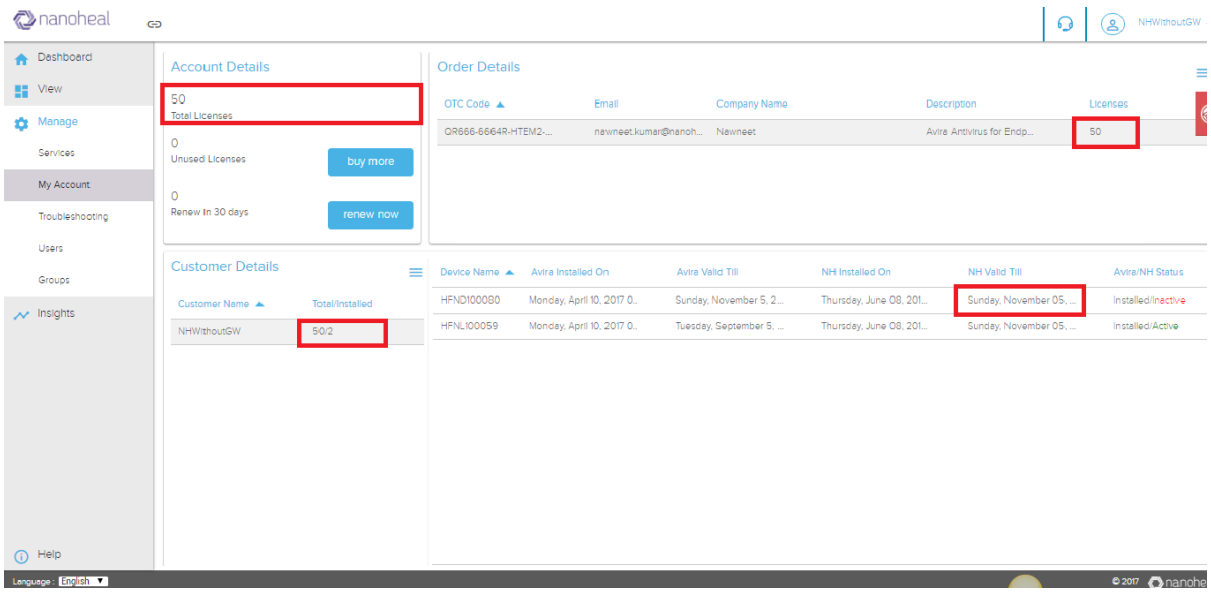
Customer can refresh OTC as shown below:



Click on Refresh OTC will give the following alert msg box with the details of data which has been changed:

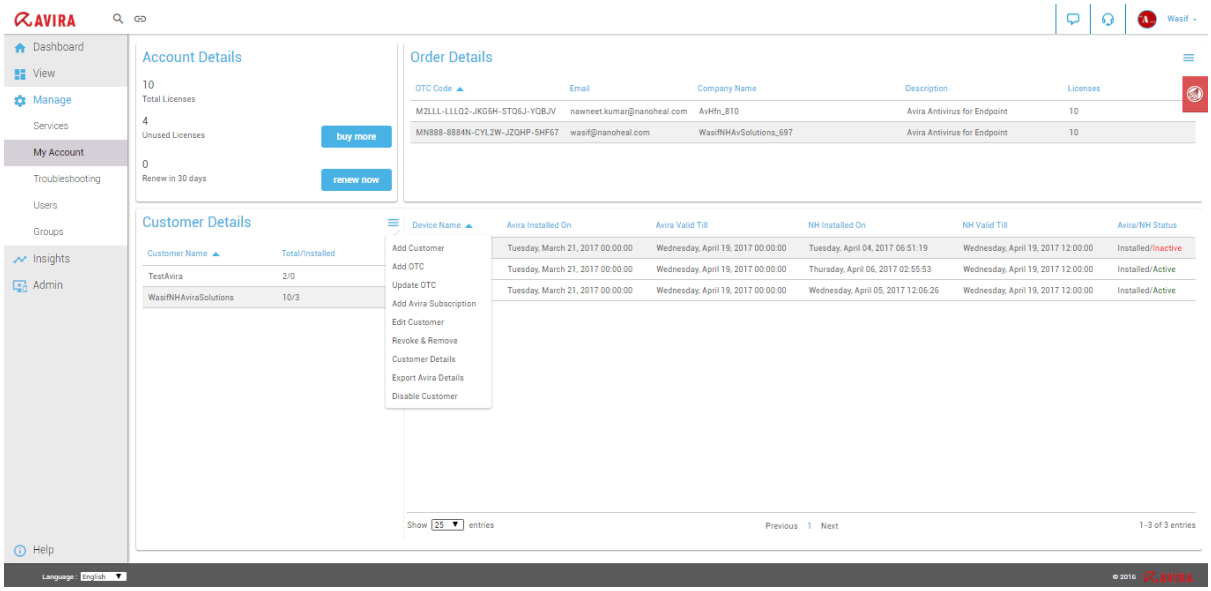


Click on OK will refresh the page and customer can see the updated data on dashboard as shown below:



A click on the hamburger menu next to "Customer details" would show the following options.

a. Add customer
b. Add OTC
c. Update OTC
d. Add Avira Subscription
e. Edit Customer
f. Customer Details
g. Export Avira Details
h. Disable Customer
i. Revoke & Remove



Add OTC

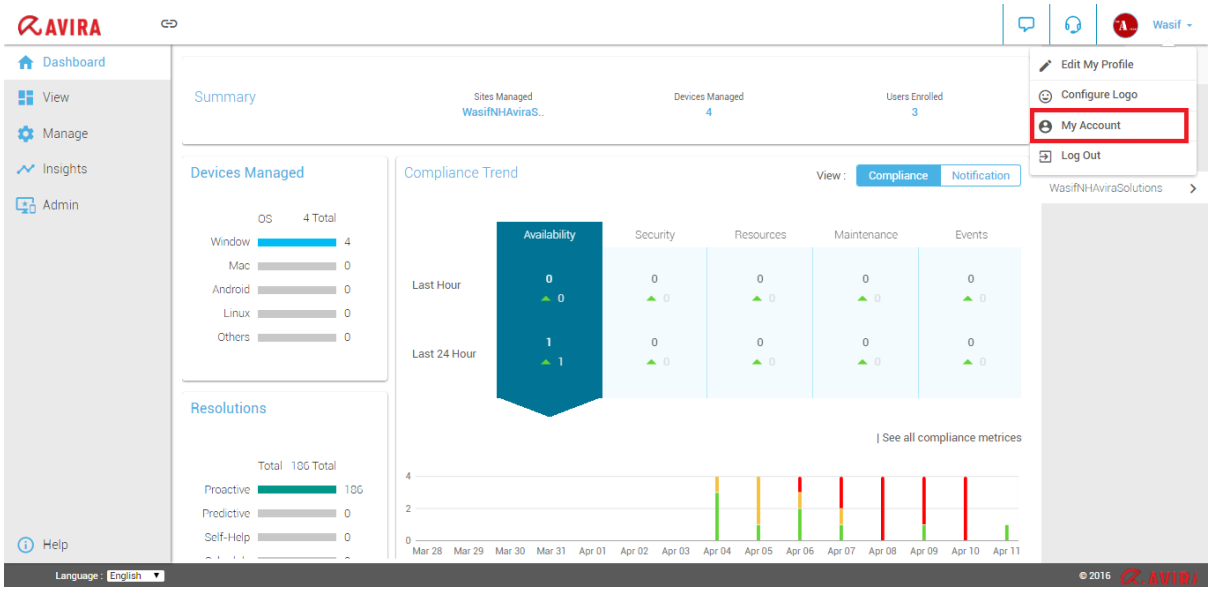
Please follow the following steps to add a new OTC.

NOTE: This would always be the first step towards adding new licenses.

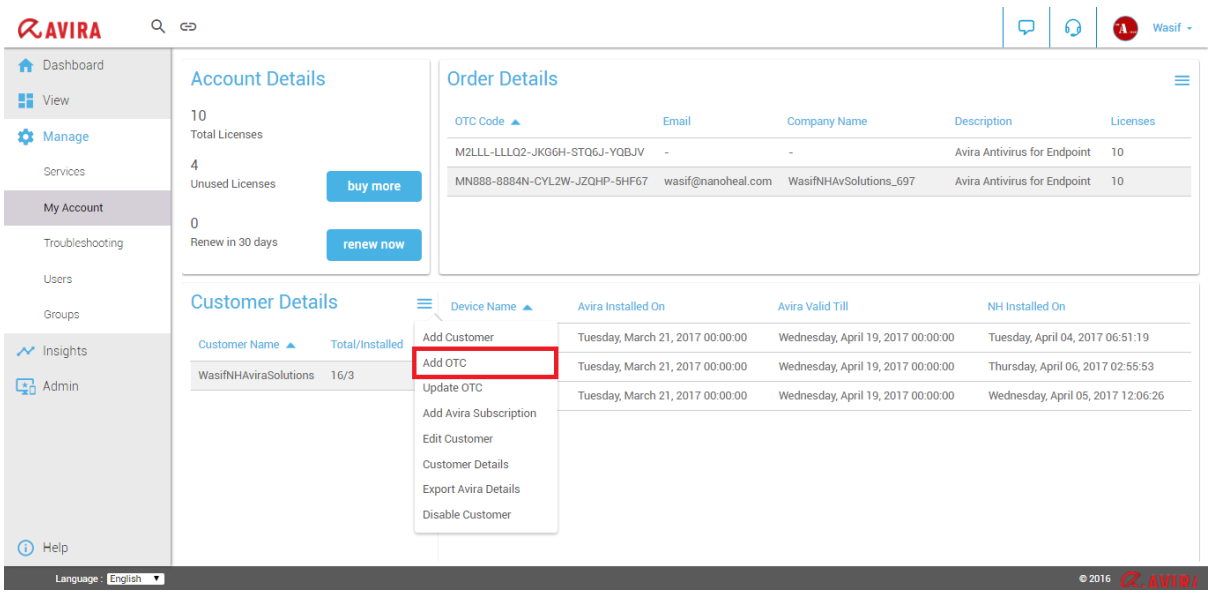
i.e.

- Users **must** add new OTC/s before adding a New Customer
- Users **must** add new OTC/s before adding new Avira Subscriptions to existing customers

The user would need to navigate to the top right corner of the dashboard > click on the user name > Click on "My Account".
OR select "Manage Customers" from the Quick Link at the top left



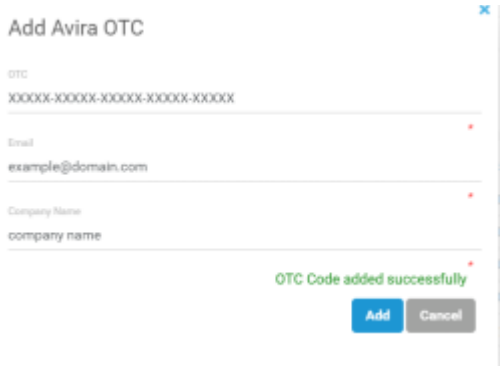
Click on the hamburger menu next to "Customer details" and click on "Add OTC".



Enter the following details in the popup box.

- OTC code
- Email
- Company name

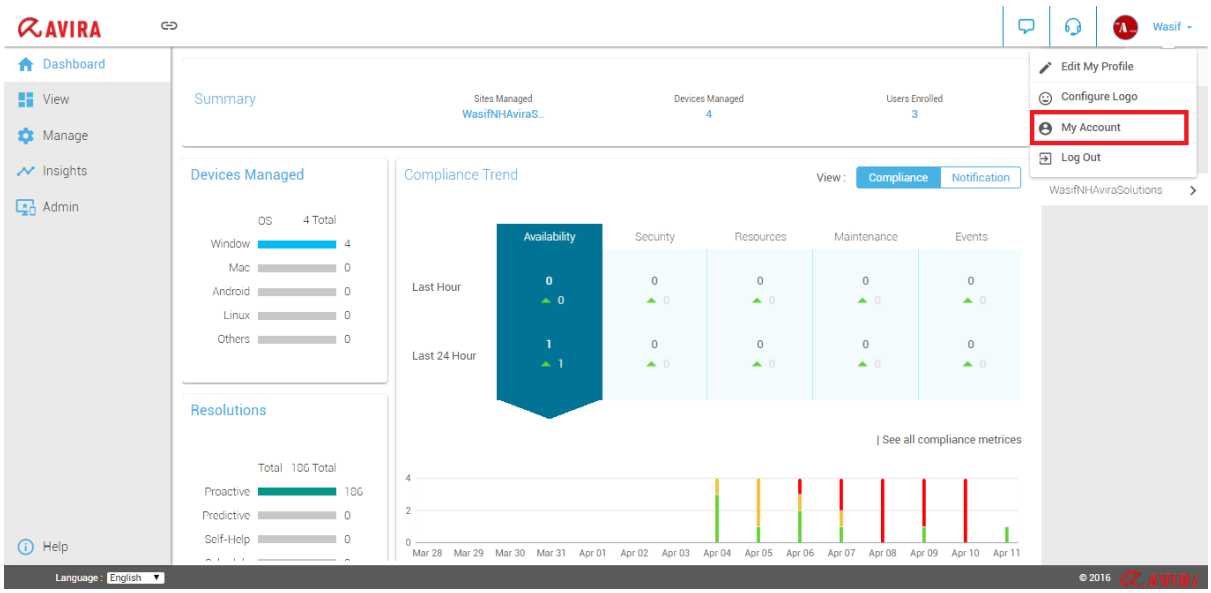
Click on “Add” to add the OTC code.



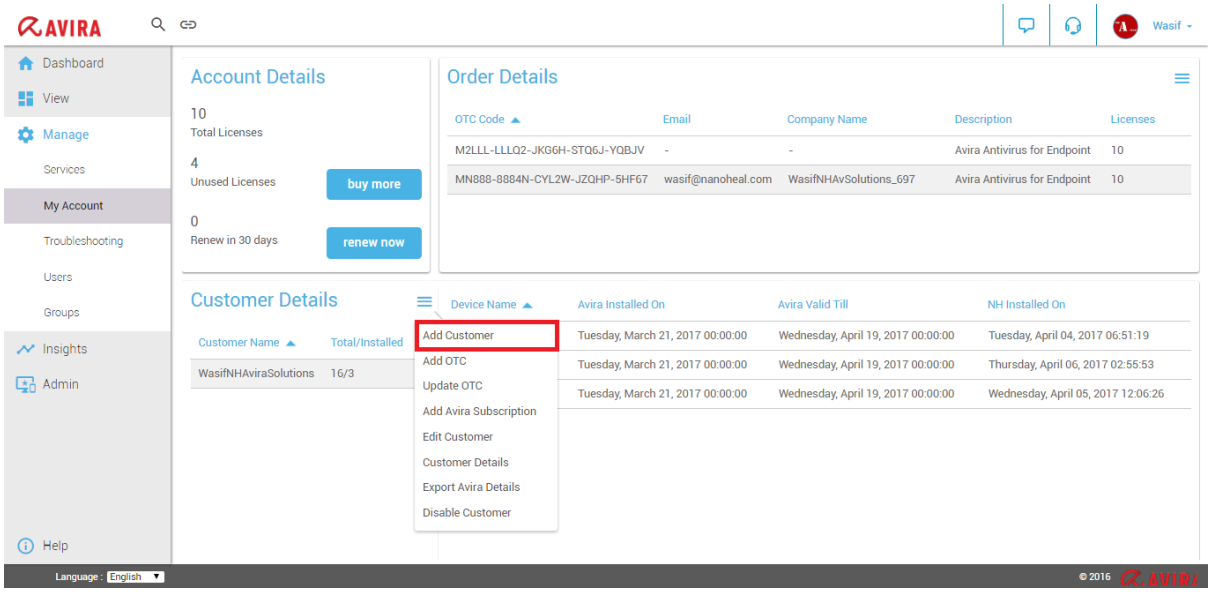
Add a Customer

Please follow the following steps to add a new customer/site.

Navigate to the top right corner of the dashboard and click on the user name, and Click on "My Account".



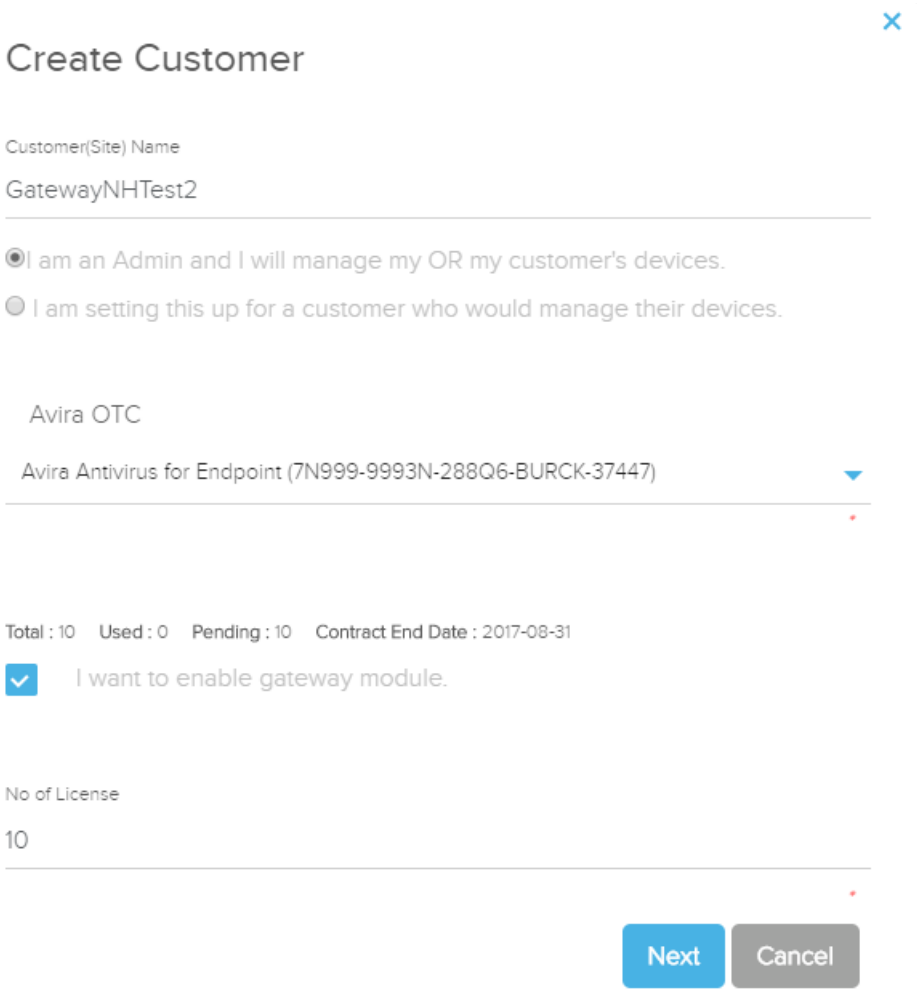
Click on the hamburger menu next to "Customer details" and click on "Add Customer".



Enter the following details in the popup box.

- Site/Customer name
- OTC

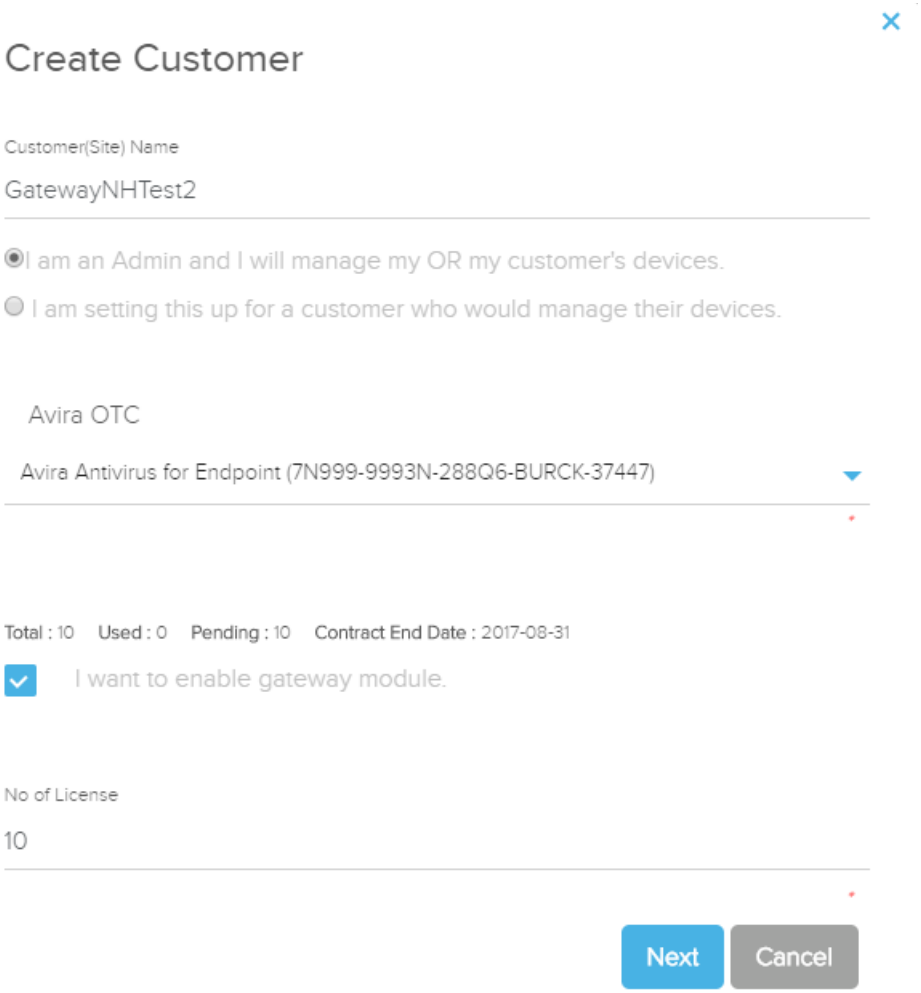
- Number of License

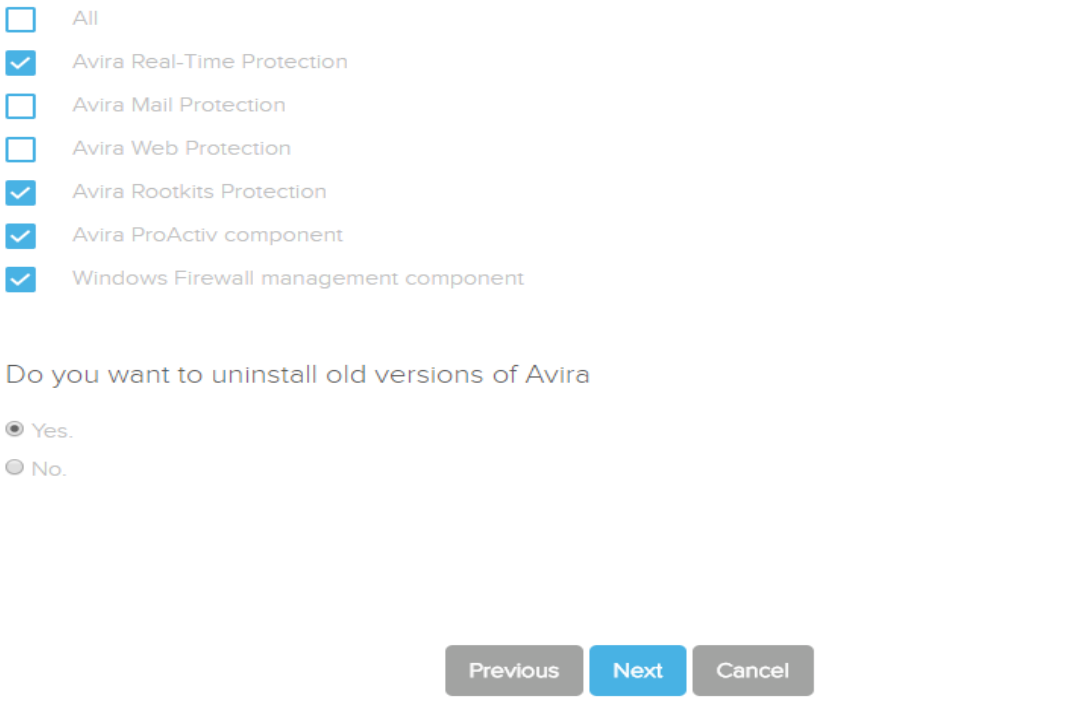


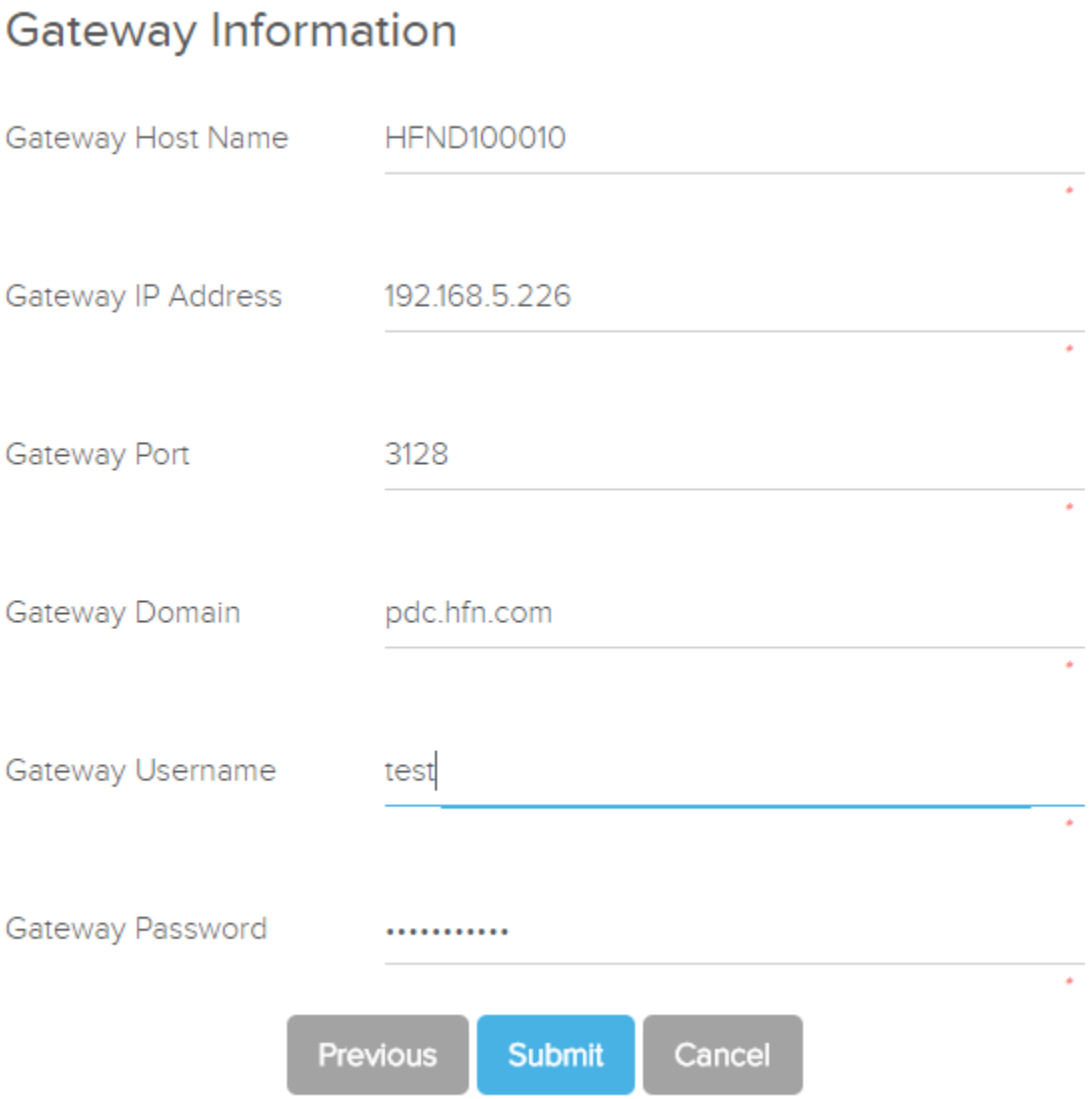
1. Choose an OTC from the dropdown
   i) Enter the site name and select OTC from drop down list. Depending on the OTC chosen, the user will get to see the
      (1) Total number of licenses
      (2) Used licenses
      (3) Number of pending licenses
      (4) Contract End date
      (5) Gateway Module

   ii) Click on submit to continue.

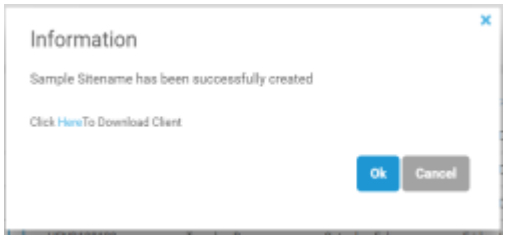
   As shown below:


Create Customer
Customer(Site) Name
GatewayNHTest2
I am an Admin and I will manage my OR my customer's devices.
I am setting this up for a customer who would manage their devices.
Avira OTC
Avira Antivirus for Endpoint (7N999-9993N-288Q6-BURCK-37447)
Total : 10 Used : 0 Pending : 10 Contract End Date : 2017-08-31
I want to enable gateway module.
No of License
10
Next
Cancel


Configure Installation Modules
All
Avira Real-Time Protection
Avira Mail Protection
Avira Web Protection
Avira Rootkits Protection
Avira ProActiv component
Windows Firewall management component
Do you want to uninstall old versions of Avira
Yes.
No.
Previous
Next
Cancel



iii) Click on "here" to download the client.

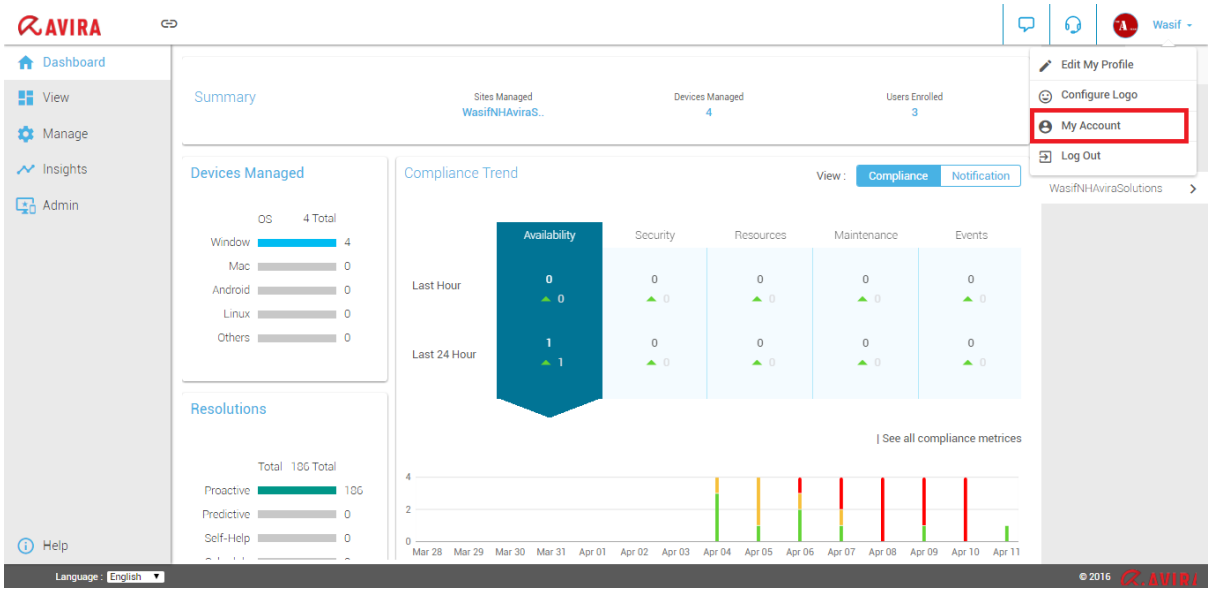


If the user selects the second checkbox I.e. customer, then download link and password reset link will be shared on mail given during the customer creation.

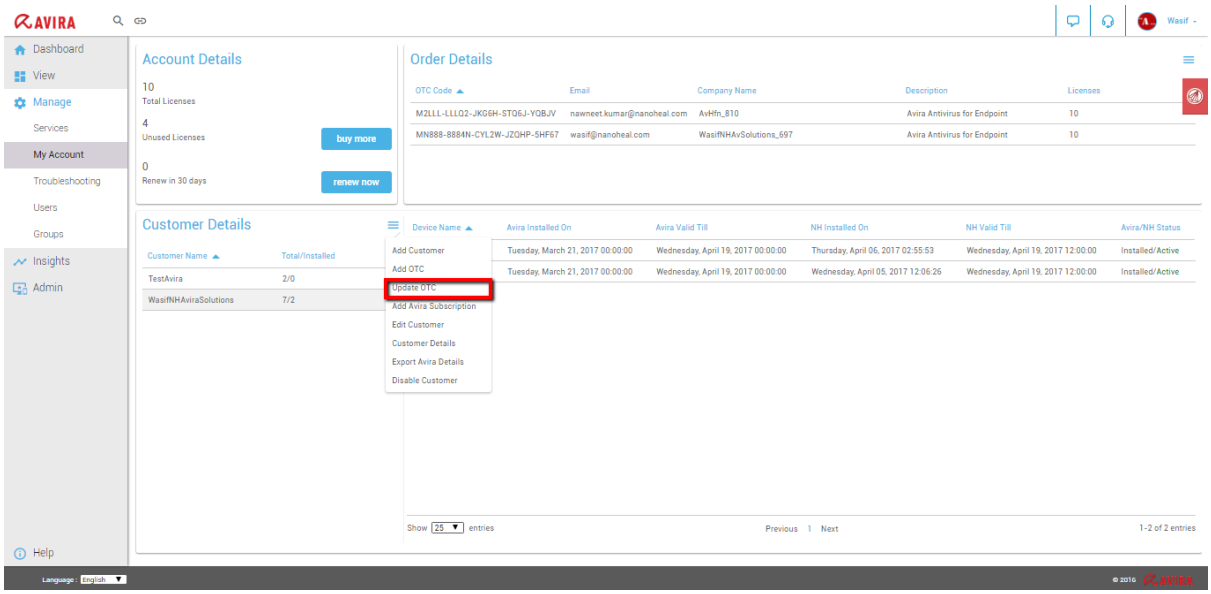
Update OTC

This feature helps users to change the attached OTC for any customer at any time. Please follow the following steps to change OTC:

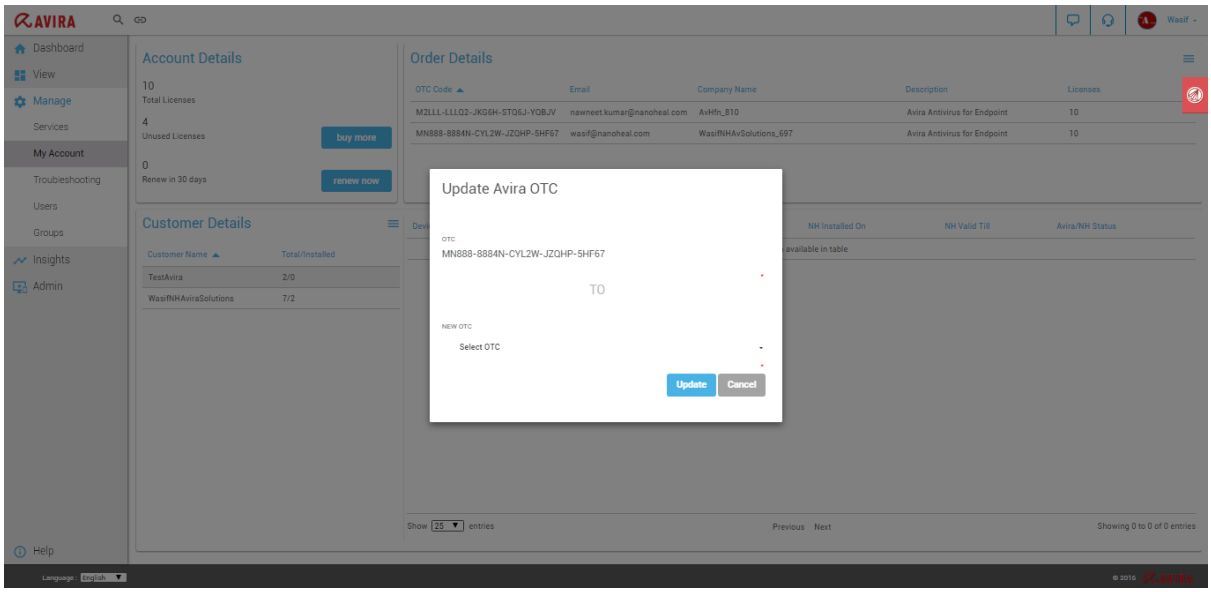
Navigate to my account page as shown below:



Click on the hamburger menu next to "Customer details" and click on "Update OTC"



Select the new OTC which needs to be attached to that particular customer:

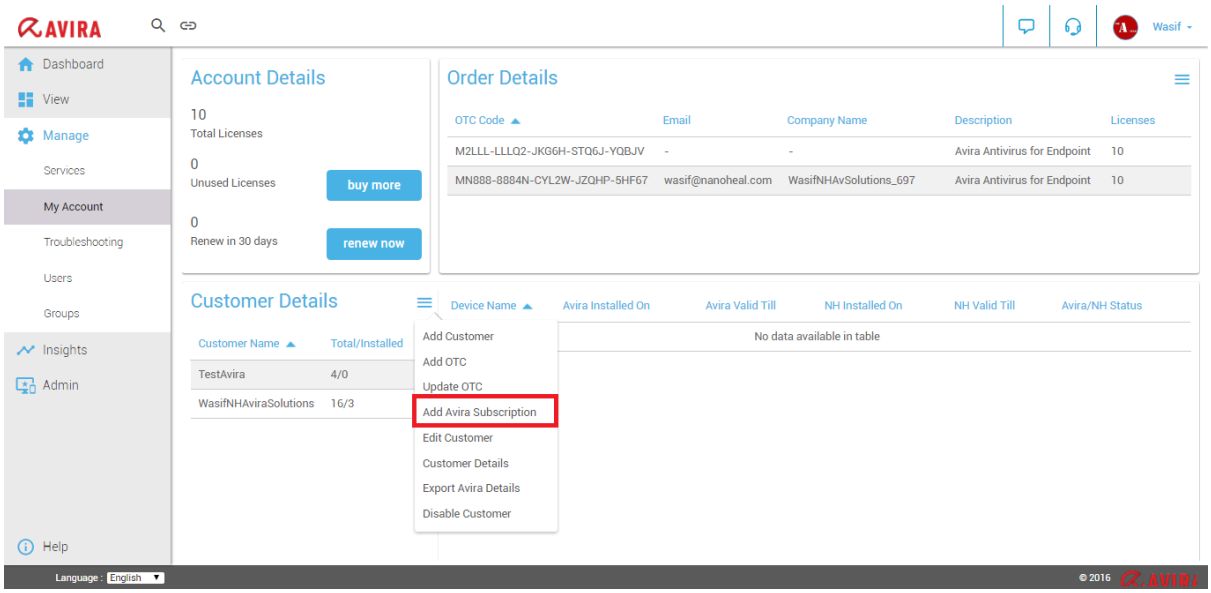


NOTE: User needs to add the OTC first by using "Add OTC" option so that the particular OTC comes in the dropdown list of "Update OTC" option. Update OTC changes will be applied/reflected only after client restart.

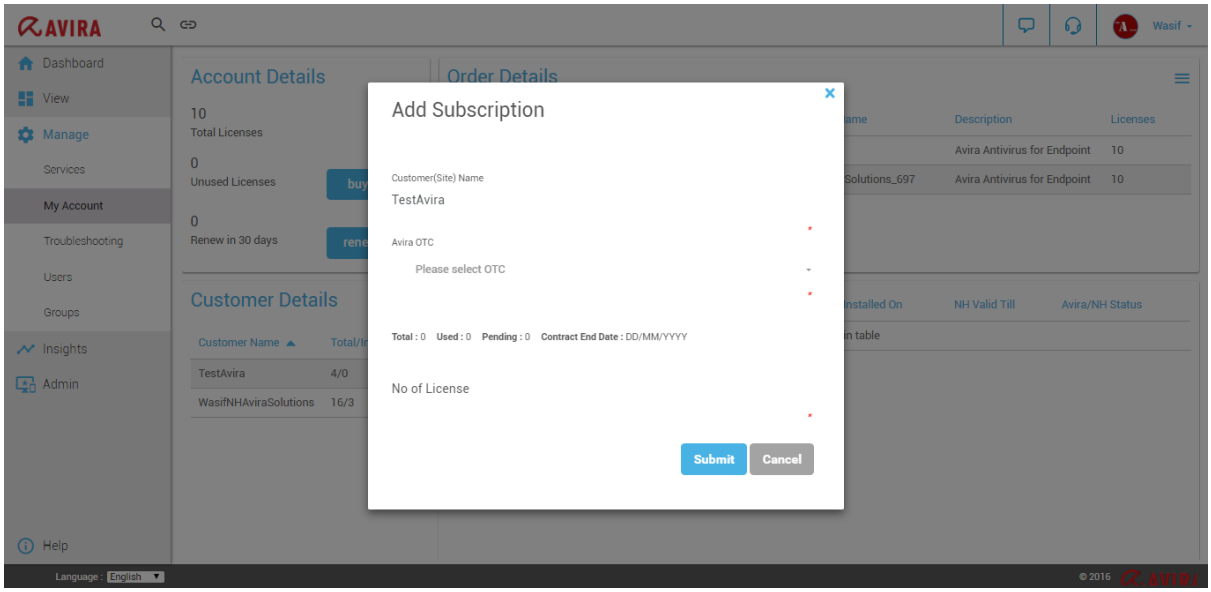
Add Avira Subscription

Users would need to Add Avira Subscription to assign OTCs to an existing customer/site This can be achieved by:

I. Highlighting the Customer/Site Name under the "Customer Details" section
II. Selecting "Add Avira Subscription" from the hamburger menu



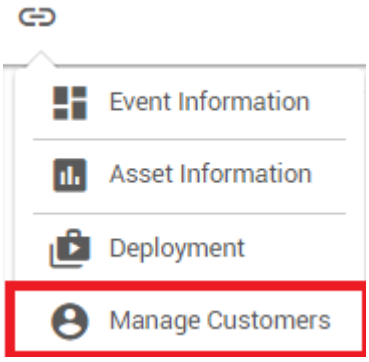
And filling the form below:



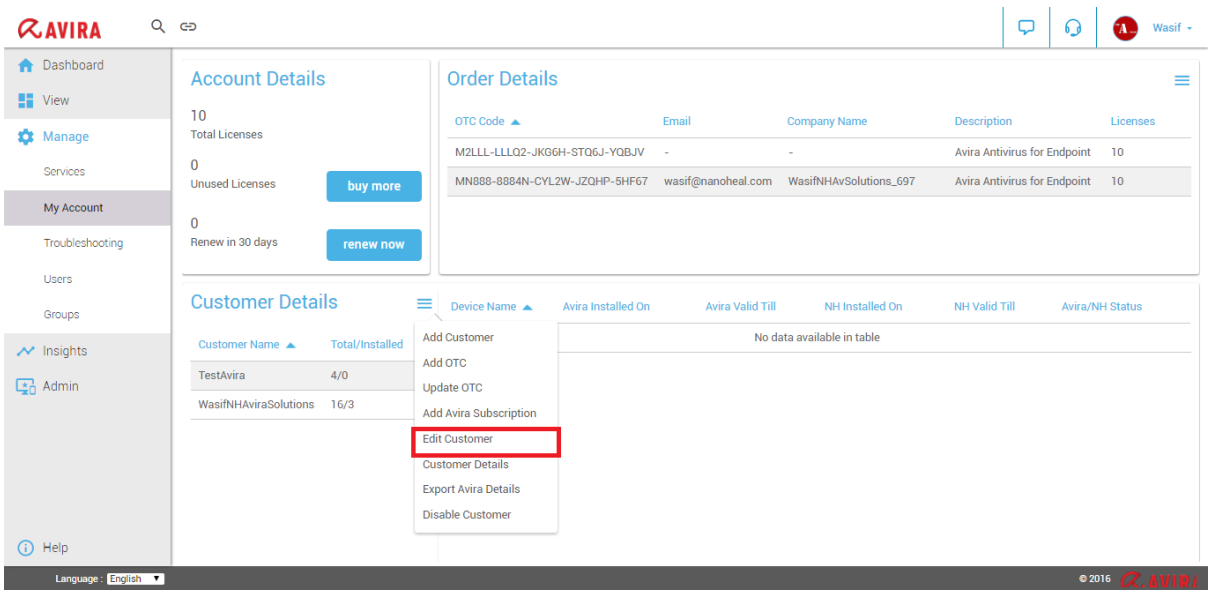
Edit Customer

Please follow the following steps to edit a customer:

Navigate to the "Manage customer" from the quick links on the top left corner.

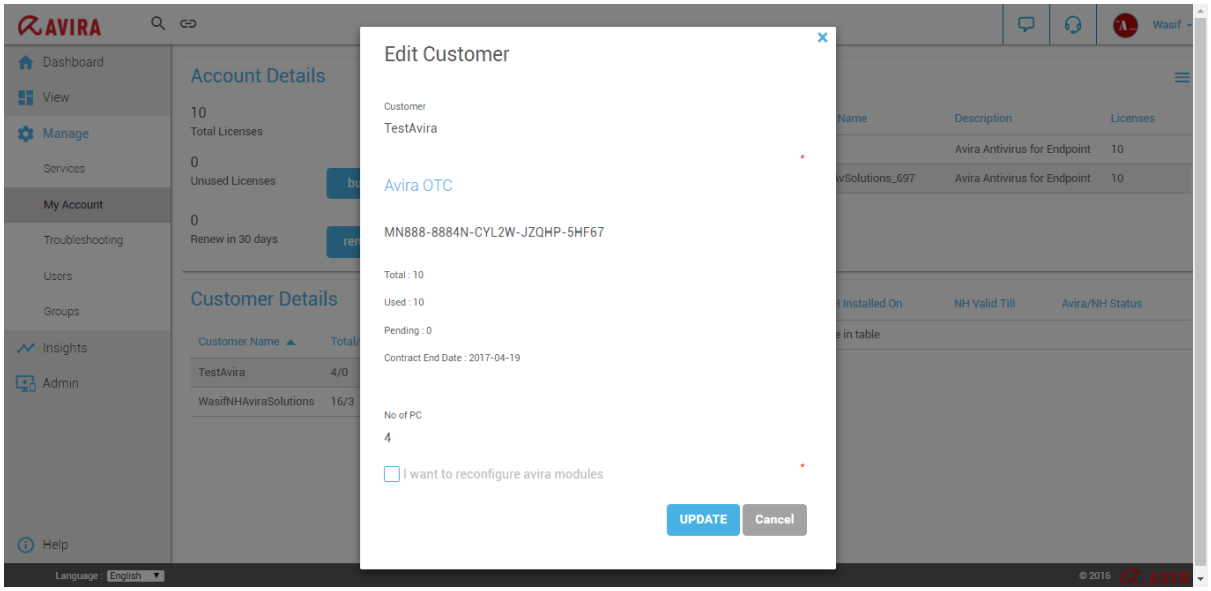


You will see a page similar to the one shown below. Click on the hamburger menu next to "Customer details" and click on "Edit Customer".

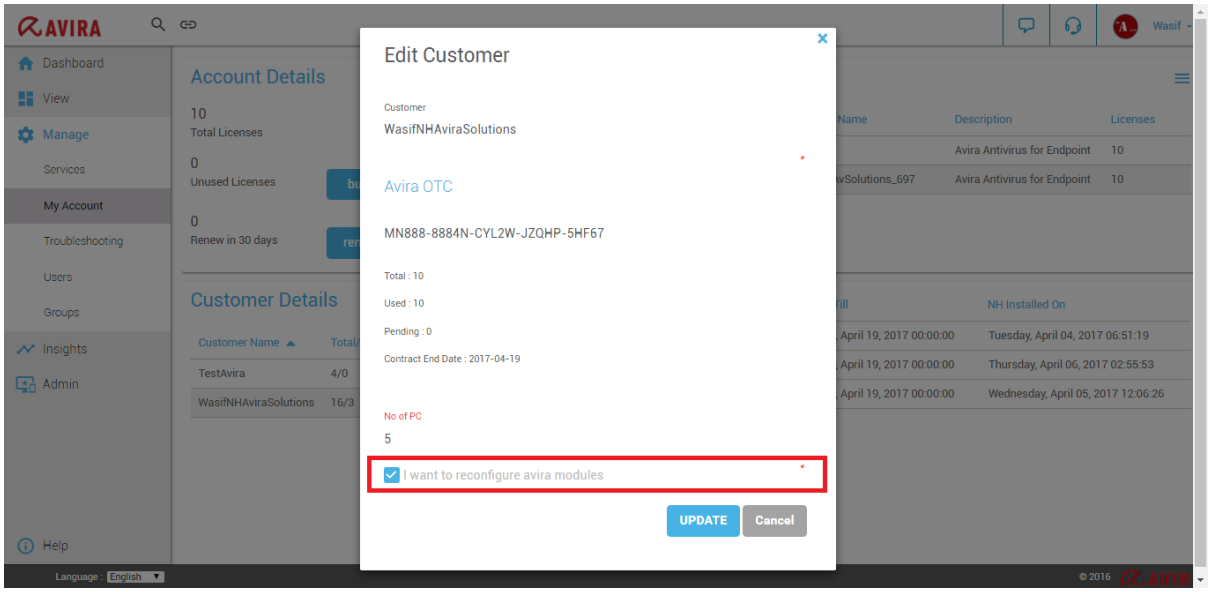


Edit the details and click on update to update the details.

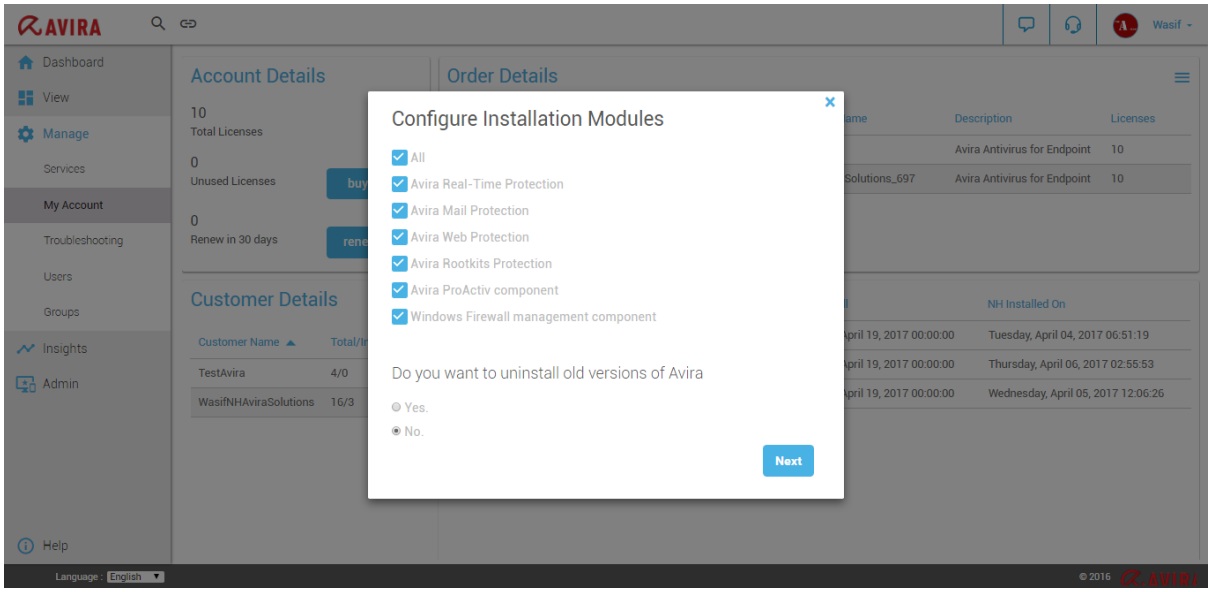
The OTC code and no of PC cannot be changed at this point. However, the Site name can be updated.



The user can configure what needs to be installed by default with Avira as shown below:

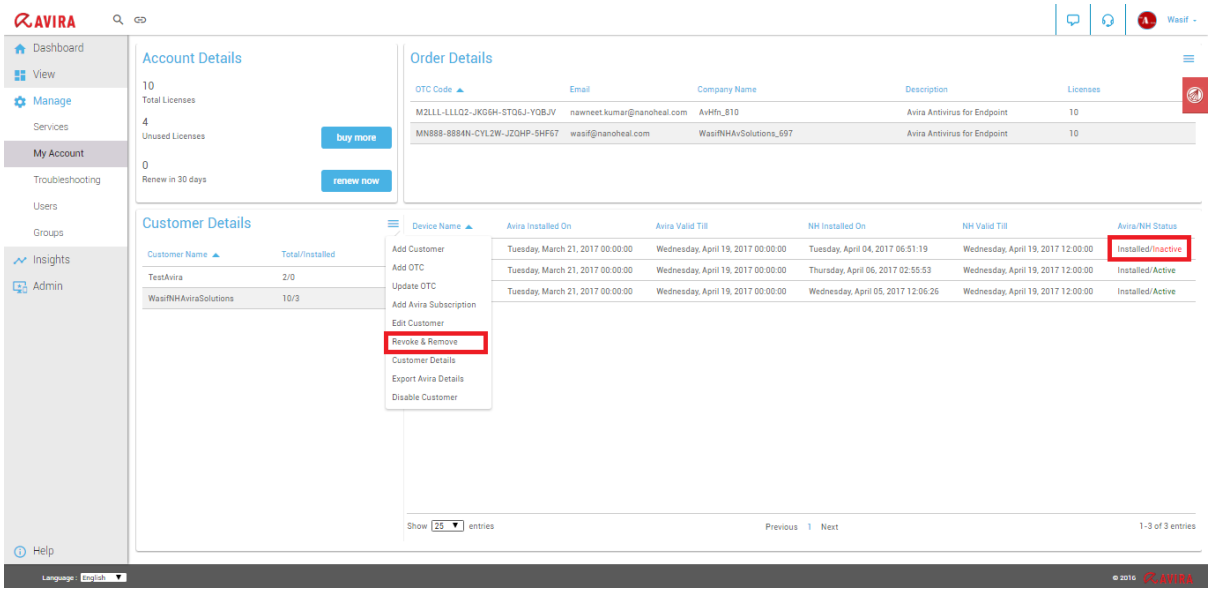


Click on update, the next page will give user the option to select which modules to install and whether user want to uninstall older version of Avira as shown below:

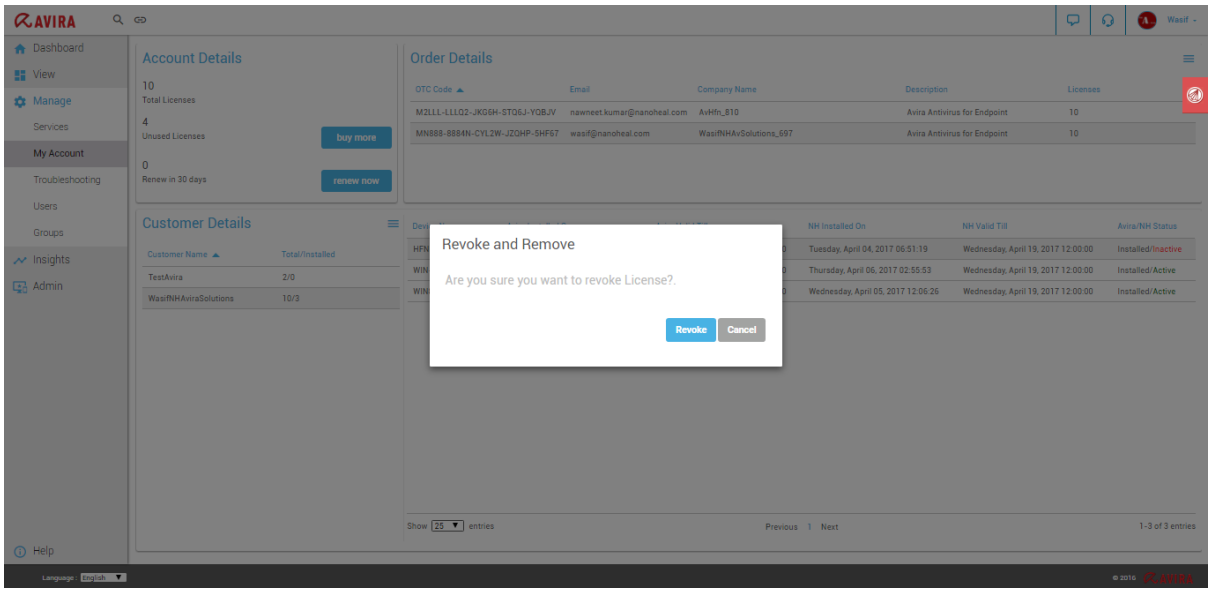


Revoke & Remove

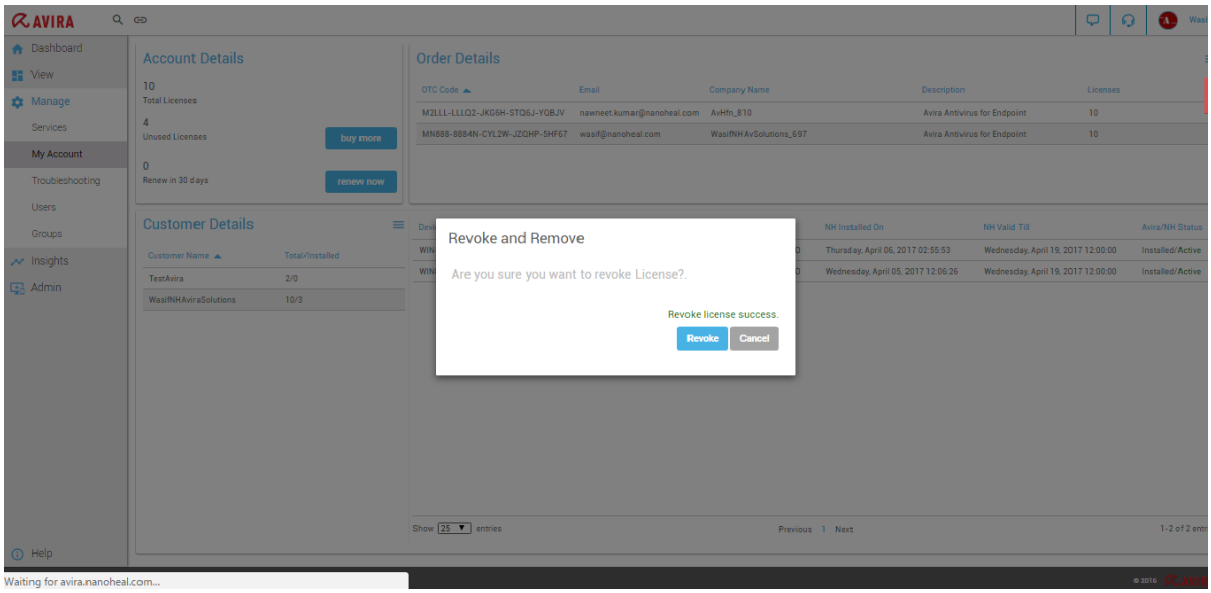
Revoke and remove option will appear only when there are machines where nanoheal has been uninstalled and NH status has been changed to Inactive.



Select the machine whose status is inactive and then click on revoke & remove. Following screen will come asking whether you want to revoke the license:



Click on revoke will revoke the license and installed count will decrease by 1. Following message will come asking customer to confirm:

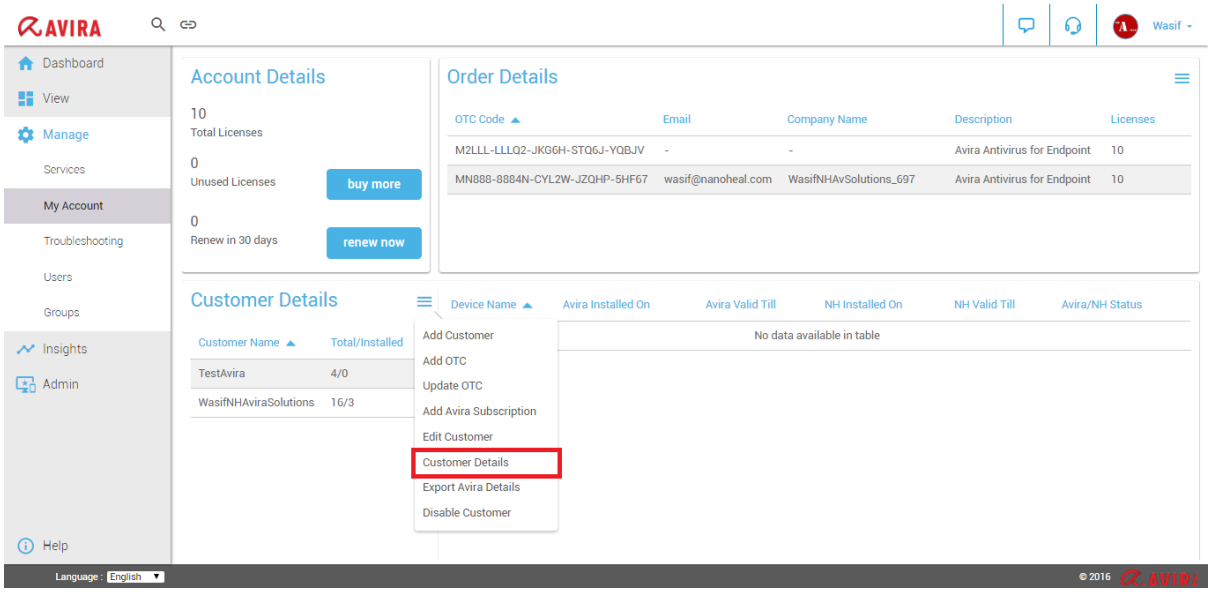


Customer Details

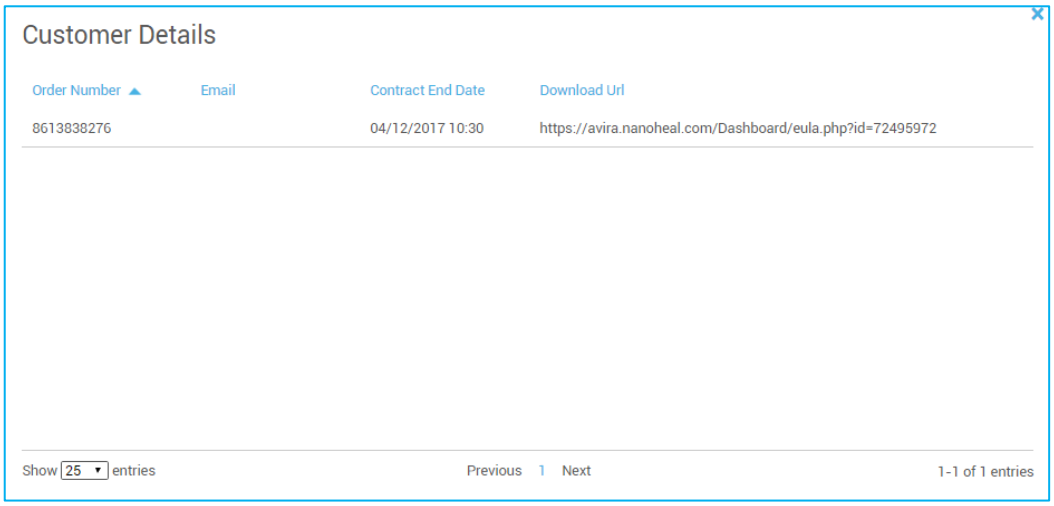
Please follow the following steps to check a particular customer's details:

Highlight a customer under the section, Customer details.

Choose the option to view "Customer Details" from the drop down menu:



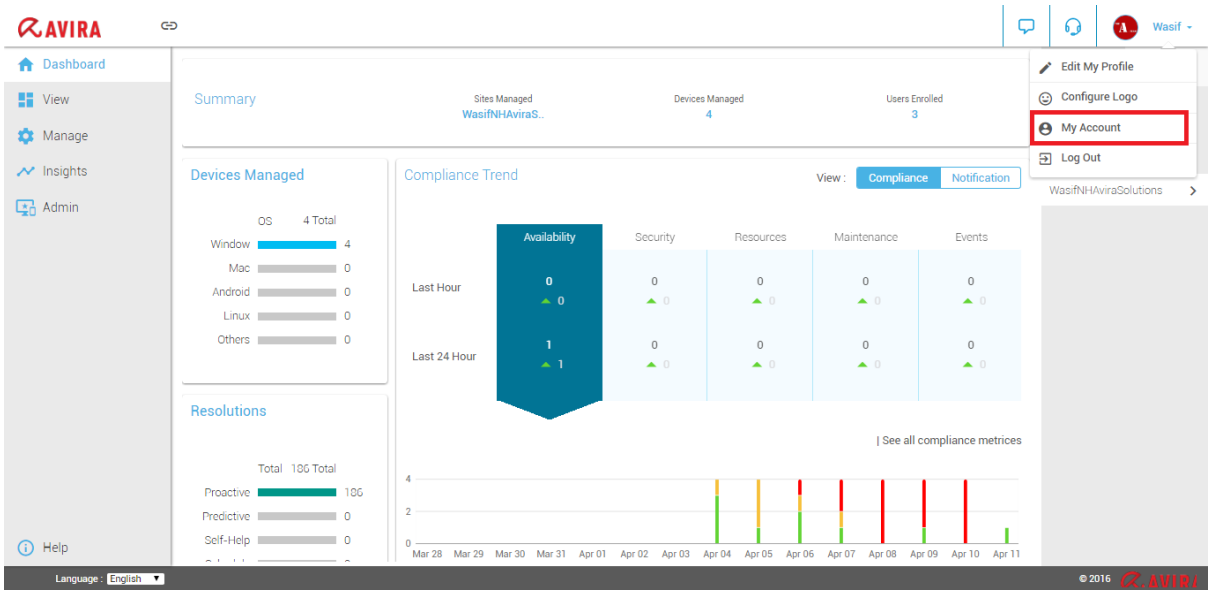
The details would appear in the following format:



Export AVIRA details

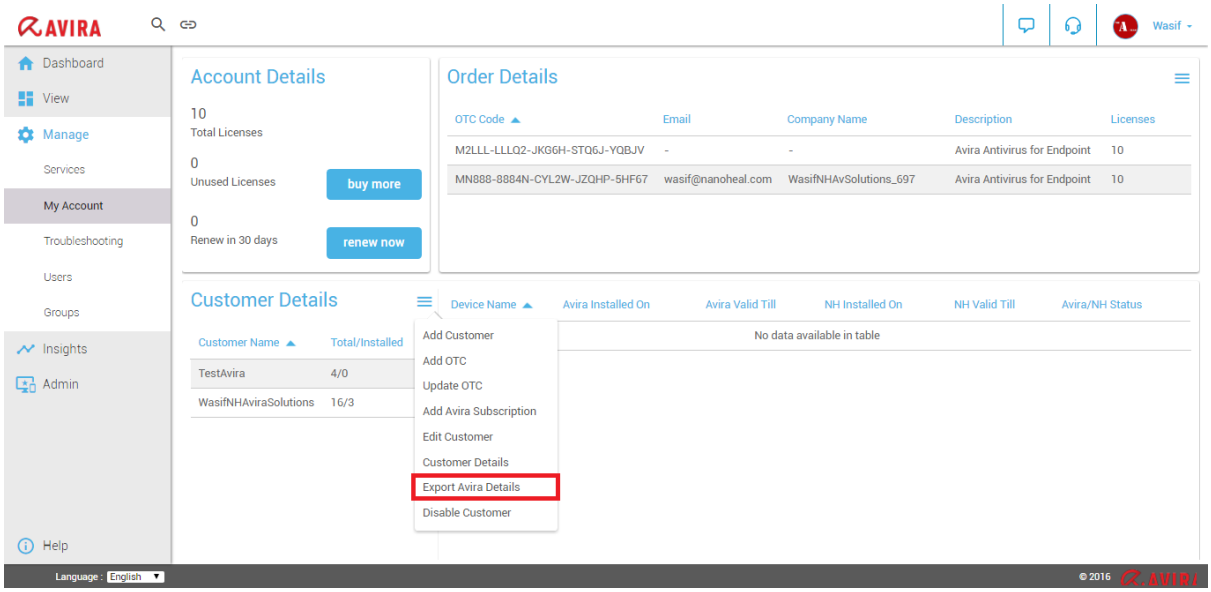
Please follow the following steps see AVIRA details:

Navigate to the "My account" from the top right corner of your Dashboard.



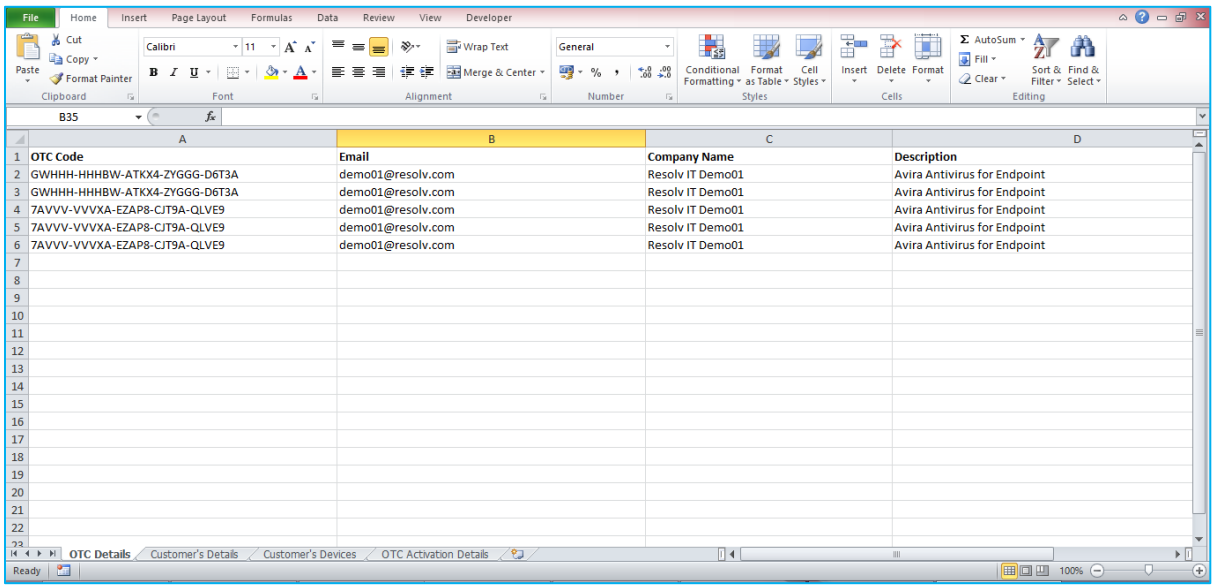
Click on the hamburger menu next to "Customer details" and click on "Export Avira Details".

As shown below:



Details are downloaded in the form of an excel workbook. The workbook will have 4 sheets that contain details about:

i) OTCs
ii) Customers/Sites
iii) Customer's Devices
iv) OTC Activation

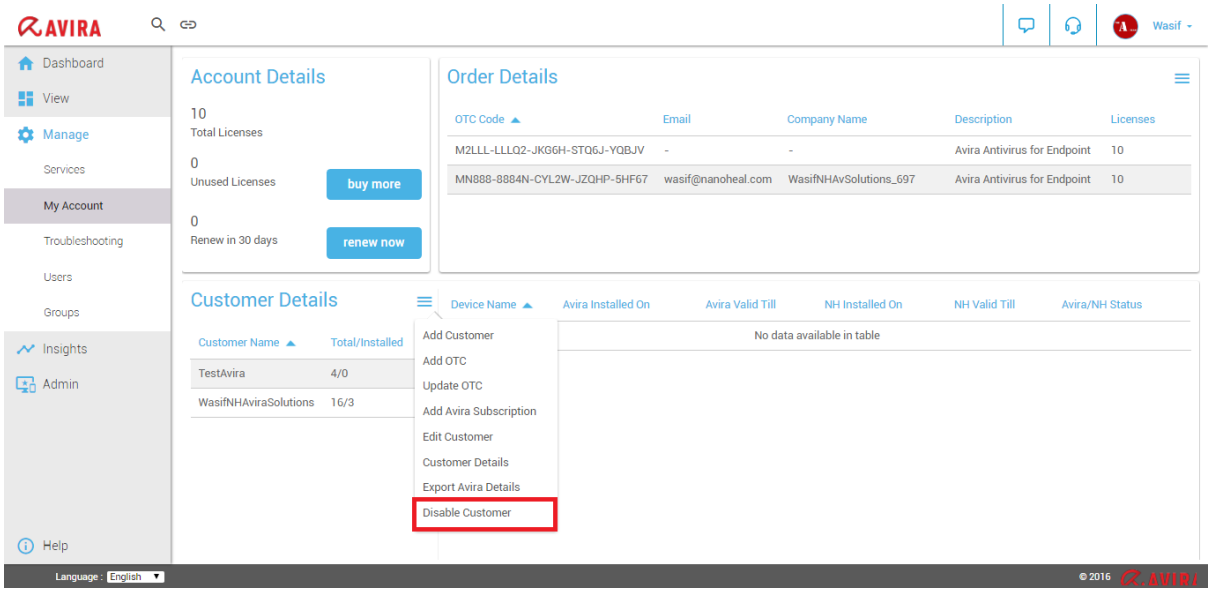


	A	B	C	D
1	OTC Code	Email	Company Name	Description
2	GWHHH-HHHBW-ATKX4-ZYGGG-D6T3A	demo01@resolv.com	Resolv IT Demo01	Avira Antivirus for Endpoint
3	GWHHH-HHHBW-ATKX4-ZYGGG-D6T3A	demo01@resolv.com	Resolv IT Demo01	Avira Antivirus for Endpoint
4	7AVVV-VVVXA-EZAP8-CJT9A-QLVE9	demo01@resolv.com	Resolv IT Demo01	Avira Antivirus for Endpoint
5	7AVVV-VVVXA-EZAP8-CJT9A-QLVE9	demo01@resolv.com	Resolv IT Demo01	Avira Antivirus for Endpoint
6	7AVVV-VVVXA-EZAP8-CJT9A-QLVE9	demo01@resolv.com	Resolv IT Demo01	Avira Antivirus for Endpoint

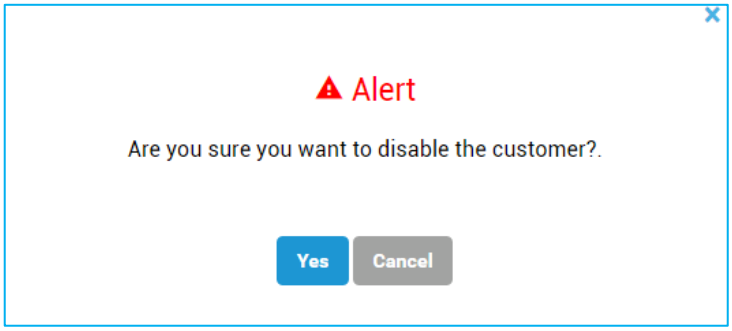
Disable Customer

The user may follow the following steps to disable a customer:

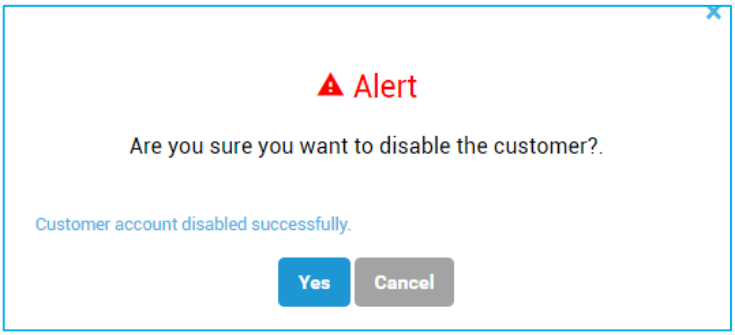
Select the option, "Disable Customer" from the drop down menu.



Click, "Yes" on the Pop Up box to confirm:



A confirmation text appears thereafter:



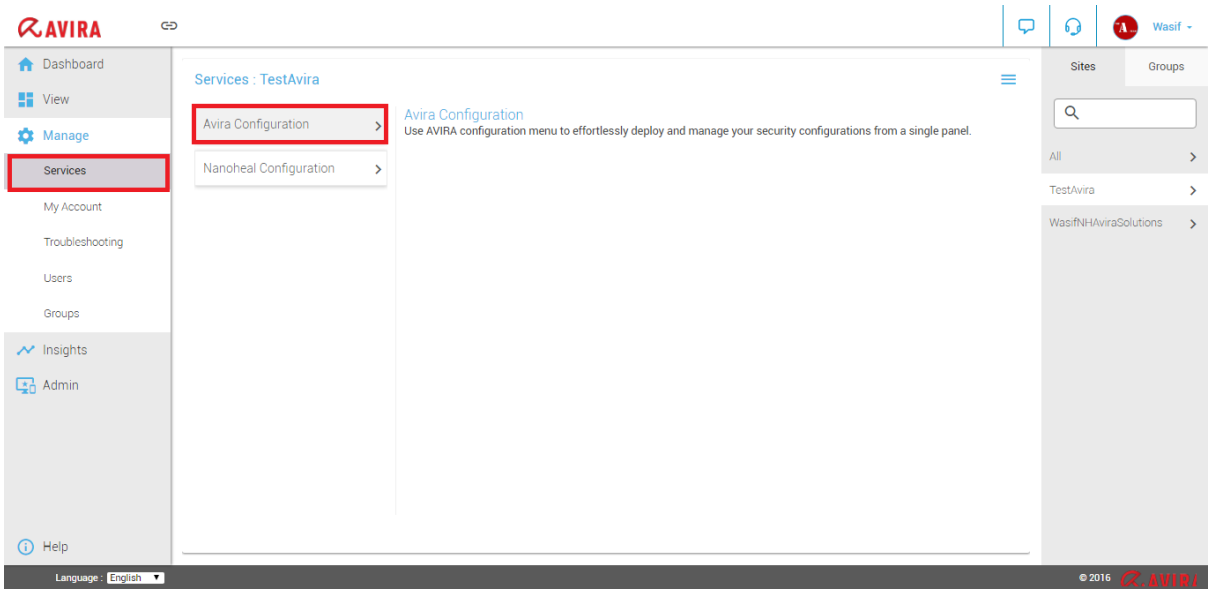
The same dropdown menu option would let the user "Enable" a disabled customer.

Services

1. The Knowledge base for a machine can be reviewed and updated at any point of time.

2. The required changes can be applied to the knowledge base instantly and the updated knowledge base can be propagated across a site or a group of machines or a single machine.

3. This can be done using the "Services" screen which is available on the home page (Under "Manage" in left pane) as shown below.



Services section is divided into two parts:

- Avira Configuration- Using this segment – the user can deploy and manage the security configurations from a single panel for Avira.
- Nanoheal Configuration- Using this segment – the user can push device policies and configurations to all managed devices through a unified panel.

Avira configuration:

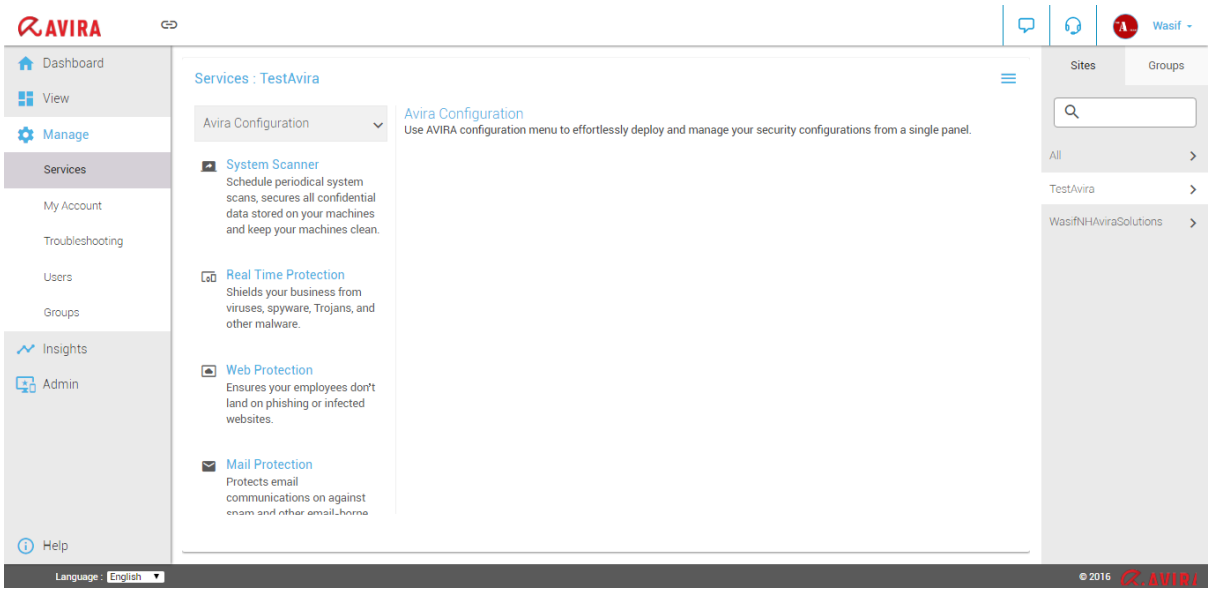
This section is divided into 9 parts:

It must be noted that this module follows a hierarchy. As shown below:

1. Site
2. Group
3. Machine

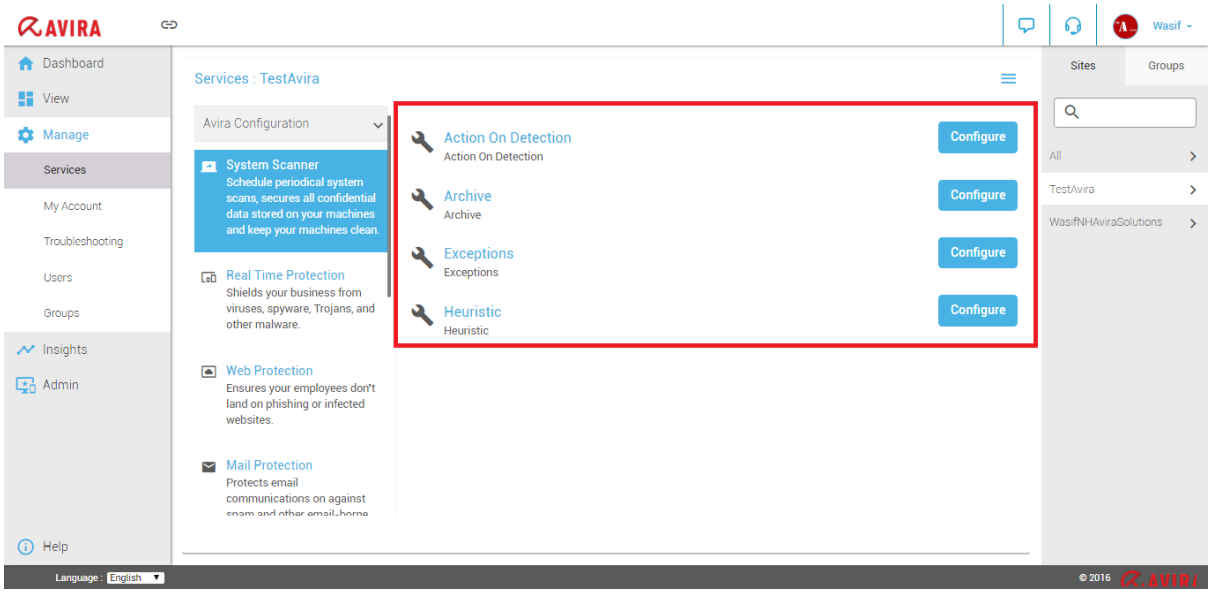
i.e. - A configuration pushed at the Machine level will be overwritten by a configuration pushed at the group level. A configuration pushed at a group level will be overwritten with the configuration pushed at the site level.
Additionally, each submodule within the Configuration Module of the Dashboard/console would show the same configuration on machine level. I.e. The configuration last pushed at a site level would show at the site level and at machine level, the configuration last pushed at a group level would show at the group level and at machine level, the configuration last pushed at a machine level would show at the machine level.
The configuration pushed at site level will reach by default to the freshly installed machine. User does not have to push the configuration again after installing client.

- System Scanner
- Real Time Protection
- Web protection
- Mail Protection
- Update and Proxy Settings
- Device protection
- Threat Categories
- Advanced Protection
- Password
- Security
- Scheduler



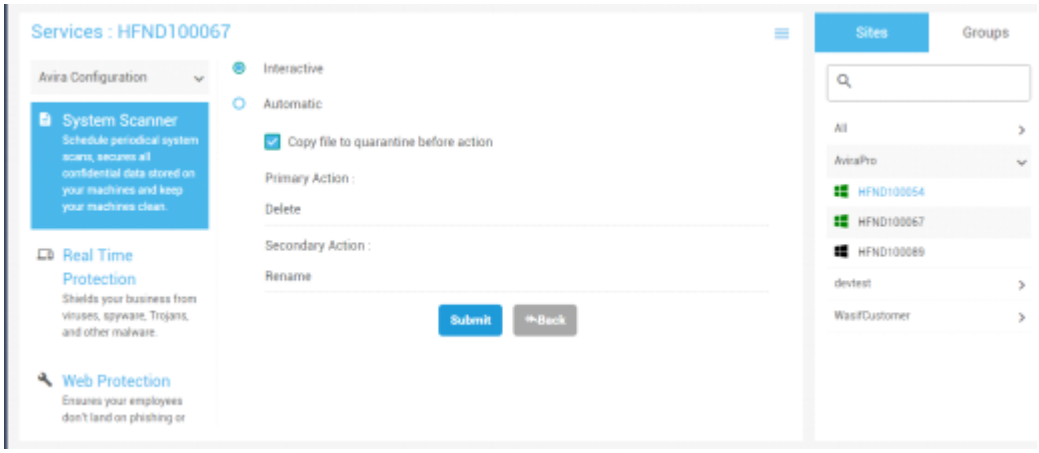
System Scanner

This section is sub divided into - Action on Detection, Archive, Exceptions and Heuristic, as shown below:

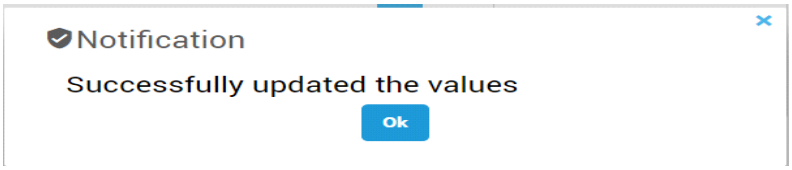


1.1 Action on Detection: This option helps a user to push configurations for scenarios when a virus is detected during a scan:

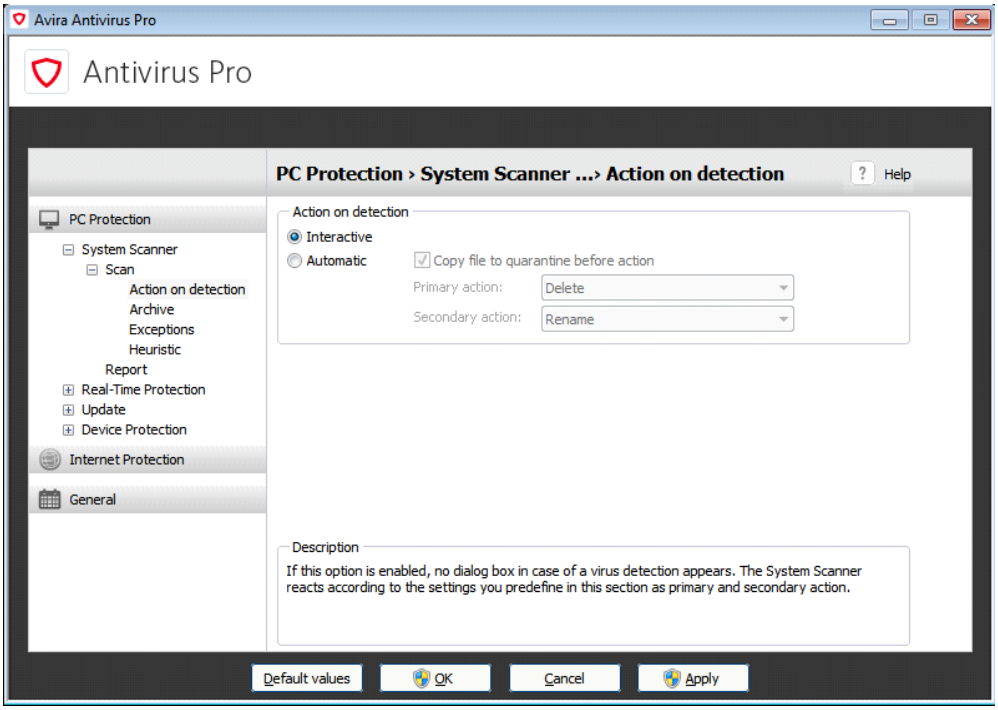
As shown below:



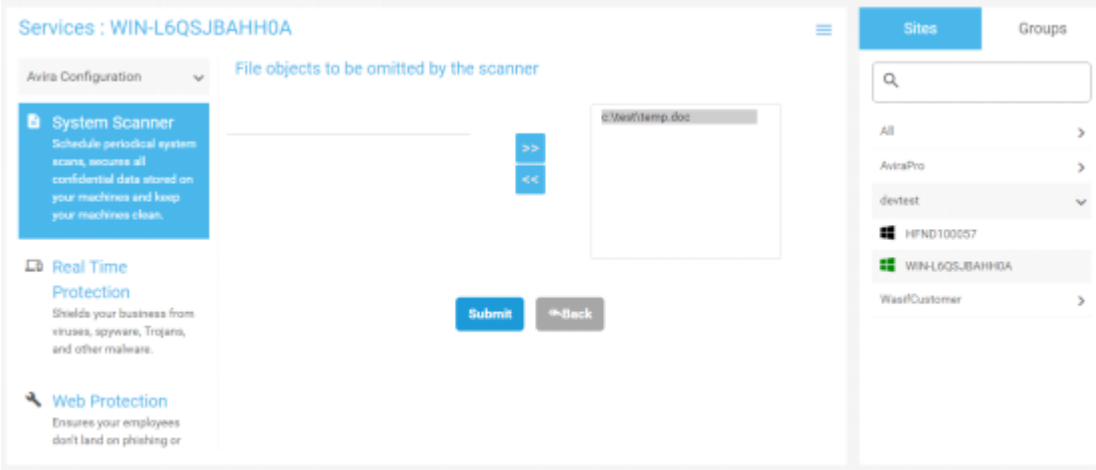
When configurations are pushed from the server, the following message box appears:



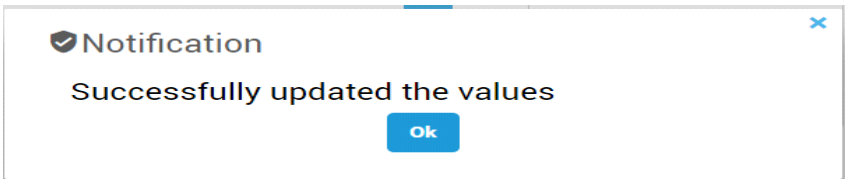
And the values are set on the Avira UI as shown below:



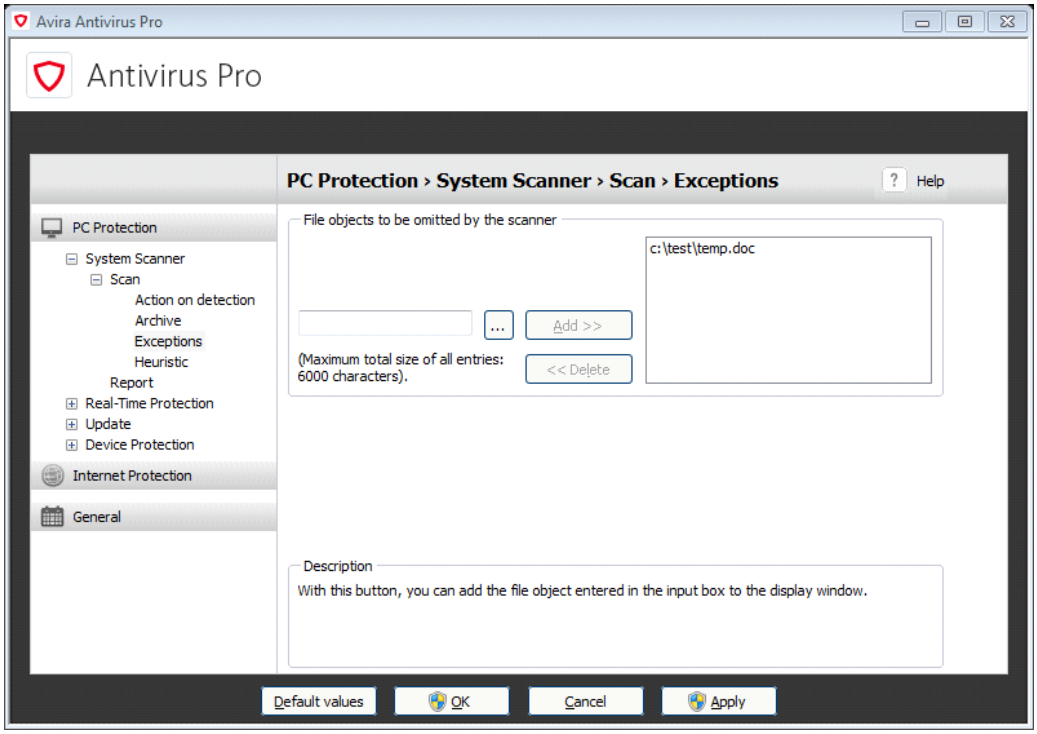
1.2 Exceptions: This option helps a user to include the path of the file/s that need/s to be exempted from a scan.



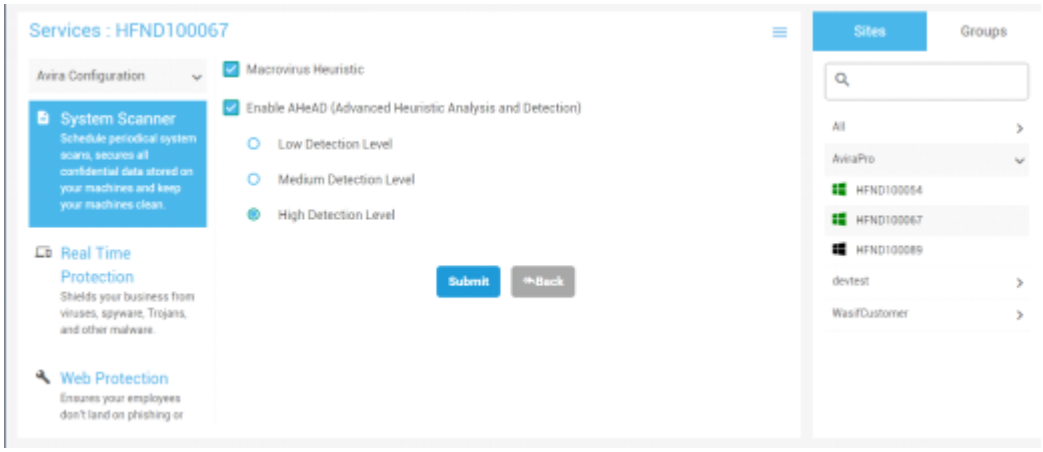
Once pushed, the following notification appears to indicate a successful execution:



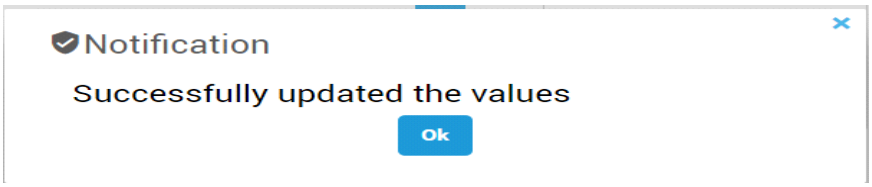
And the values are set on the Avira UI as shown below:



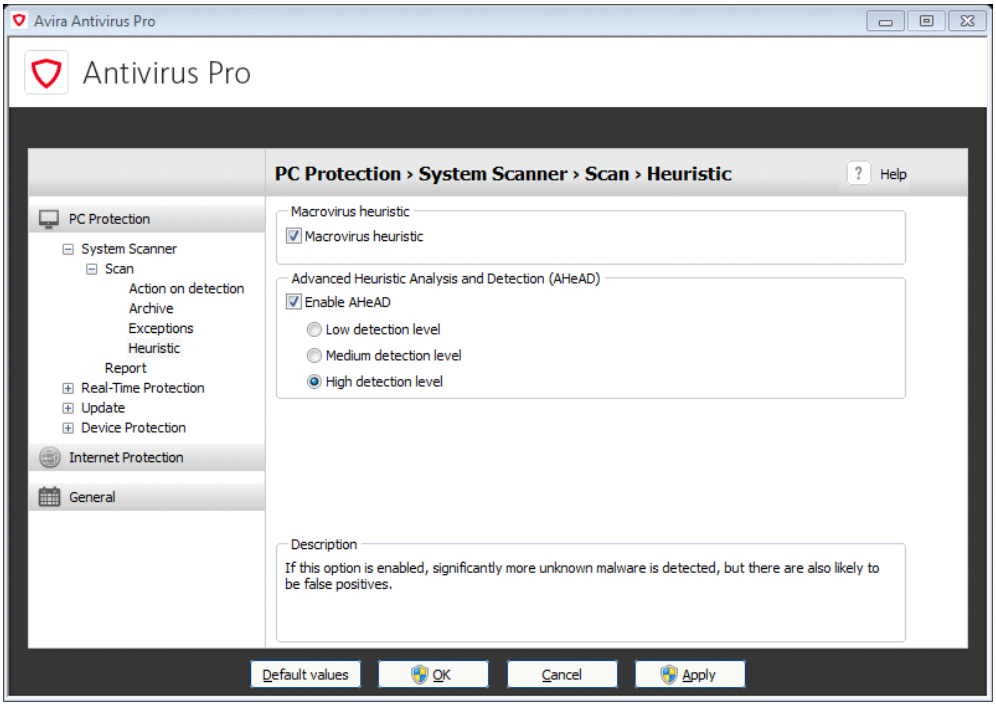
1.3 Heuristic: This option helps in defining the level of detection in Avira:



Once pushed, the following notification appears to indicate a successful execution:

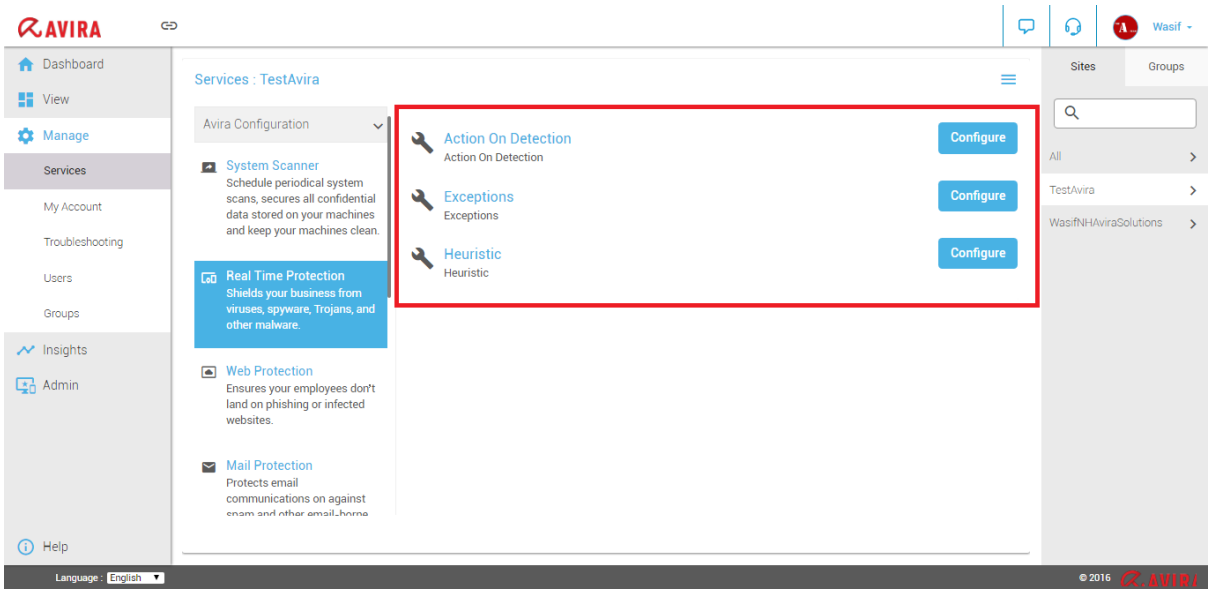


And the values are set on the Avira UI as shown below:

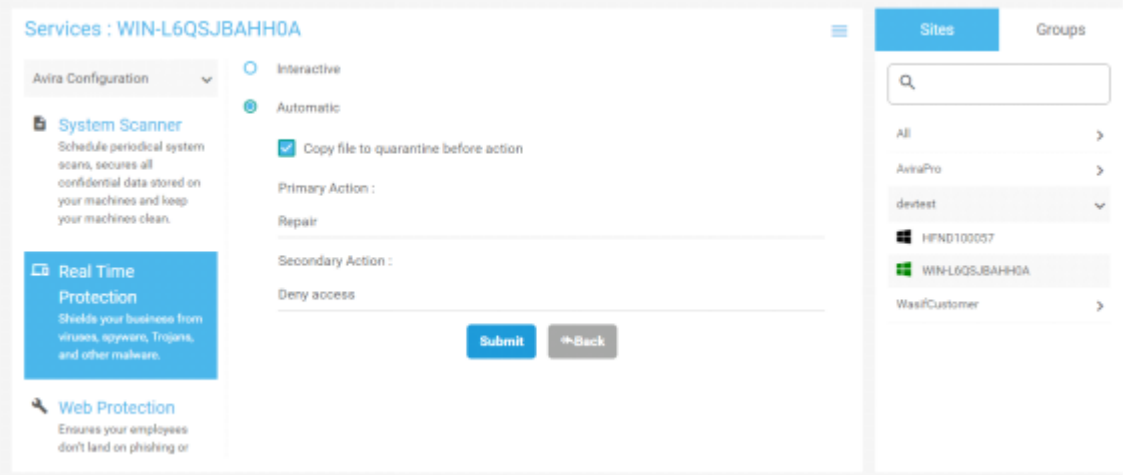


Real Time Protection

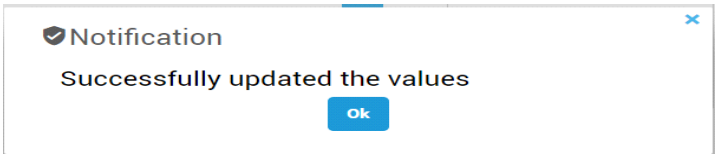
This section is sub divided into Action on Detection, Exceptions and heuristic as shown below:



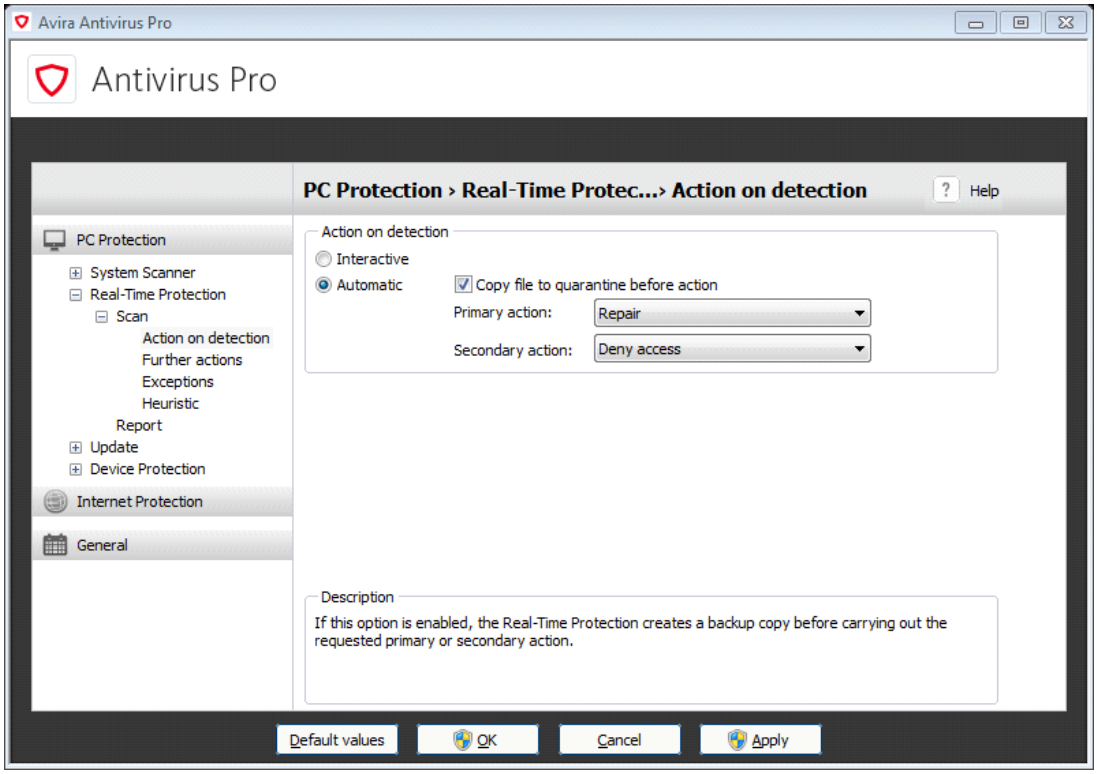
2.1 Action on Detection: This options helps a user to set configurations in scenarios when a defected file is detected.



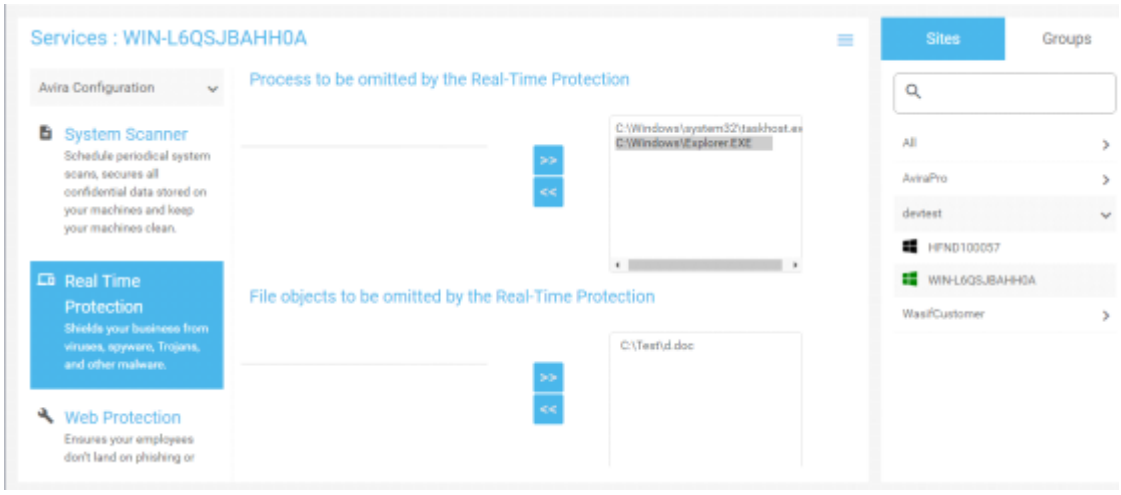
Once pushed, the following notification appears to indicate a successful execution:



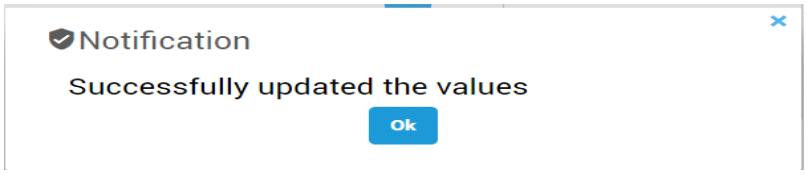
And the values are set on the Avira UI as shown below:



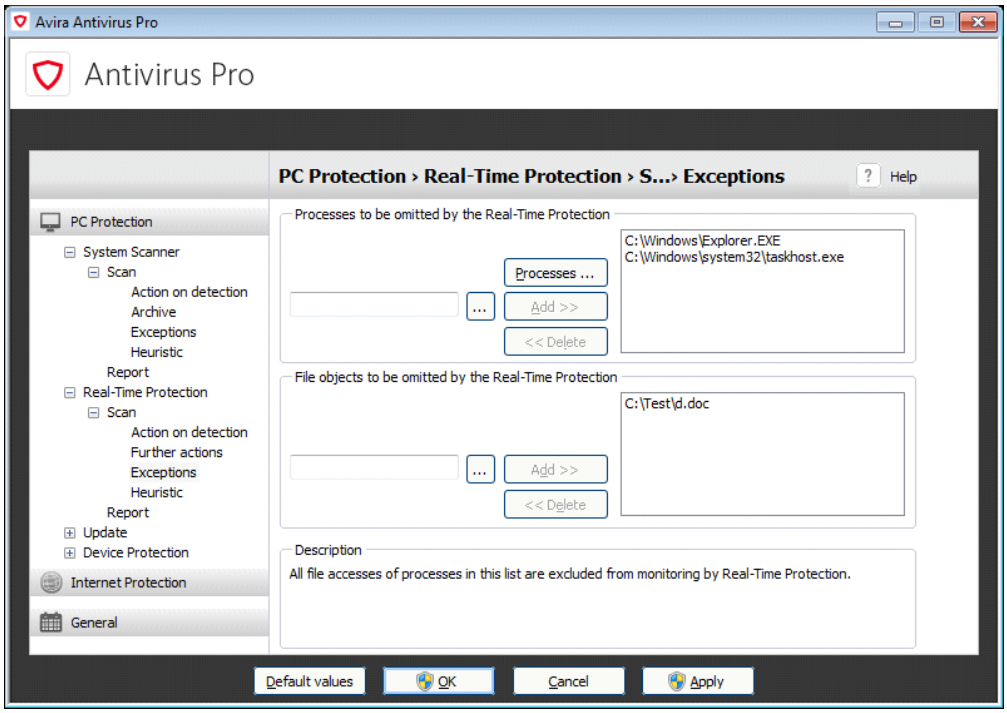
2.2 Exceptions: This option lets a user add process and files as exceptions when RTP is on.



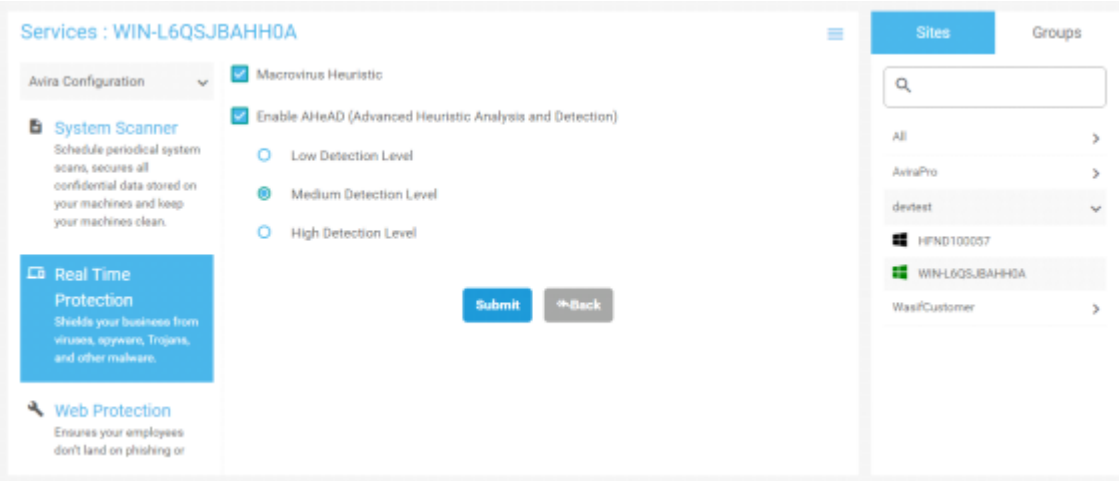
Once pushed, the following notification appears to indicate a successful execution:



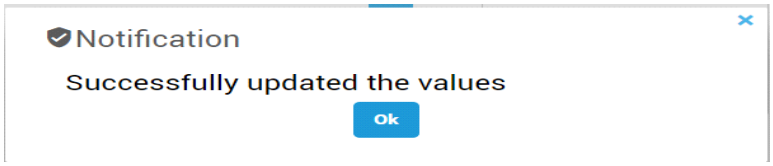
And the values are set on the Avira UI as shown below:



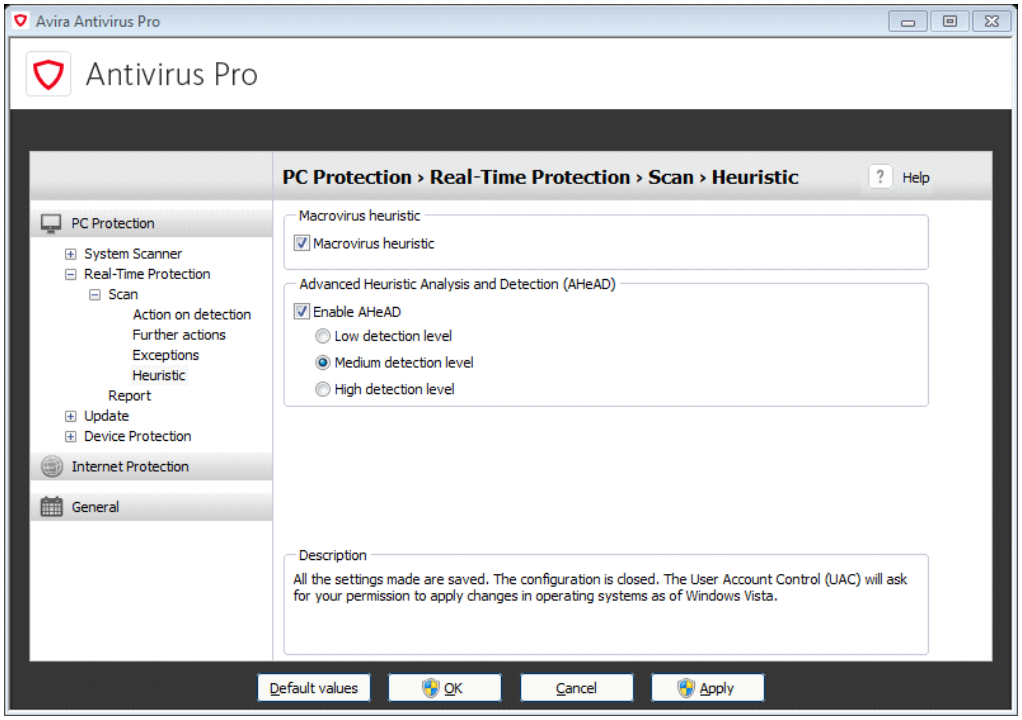
2.3 Heuristic: Following options can be set using the Heuristic section.



Once pushed, the following notification appears to indicate a successful execution:

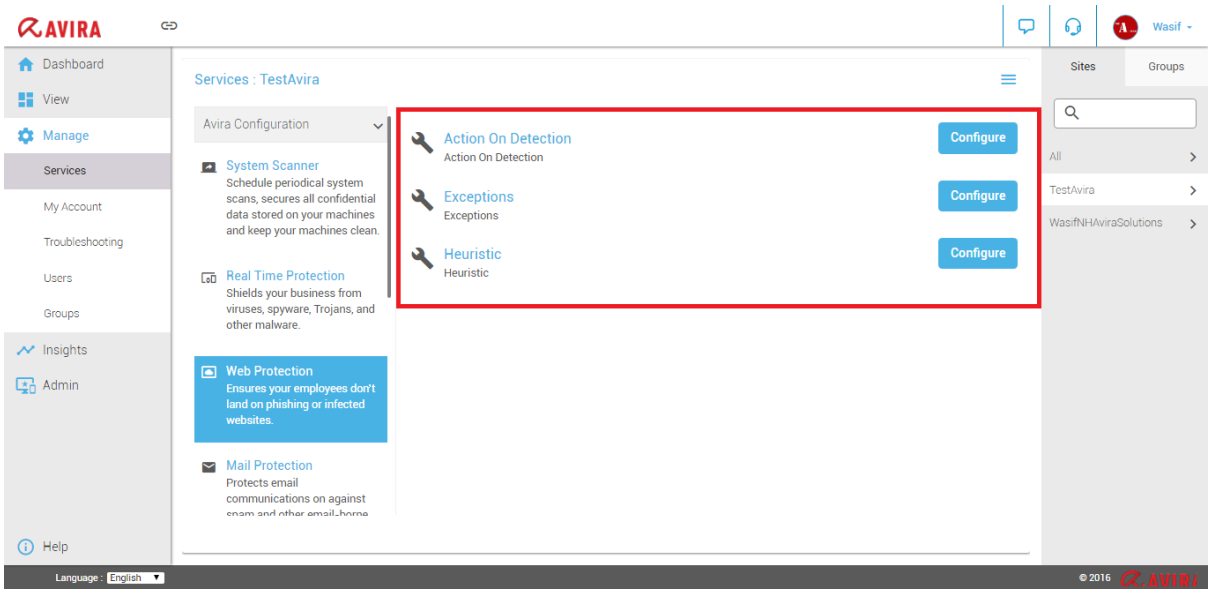


And the values are set on the Avira UI as shown below:

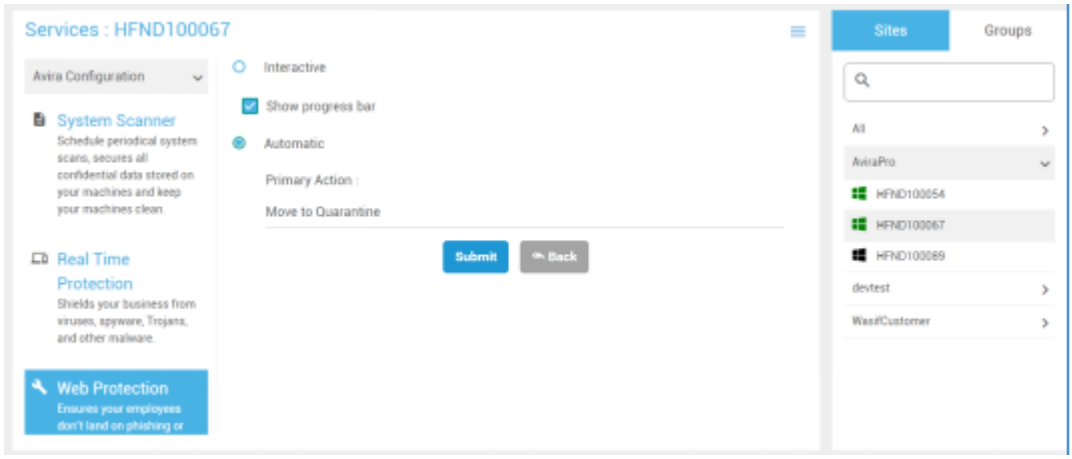


Web Protection

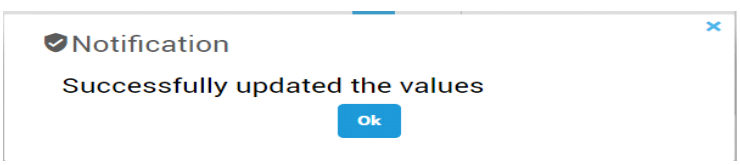
This section is divided into - Action on Detection, Exceptions and Heuristic as shown below:



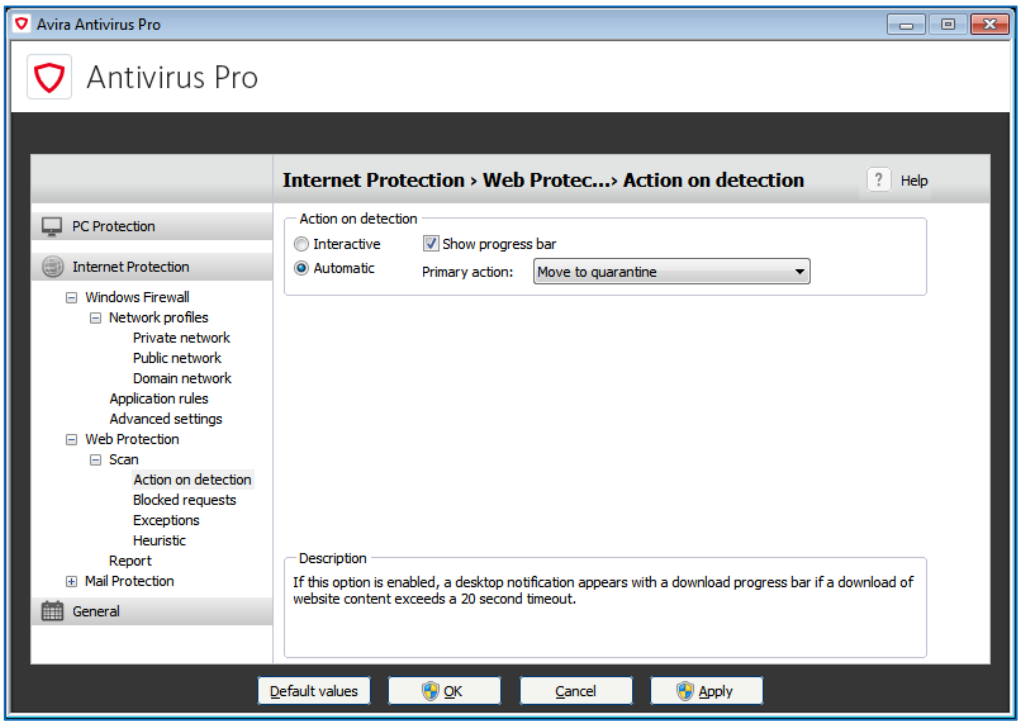
3.1Action On Detection: This option helps a user set configuration for defects detected during web browsing.



Once pushed, the following notification appears to indicate a successful execution:

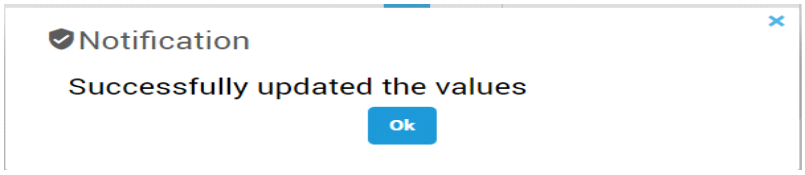


And the values are set on the Avira UI as shown below:

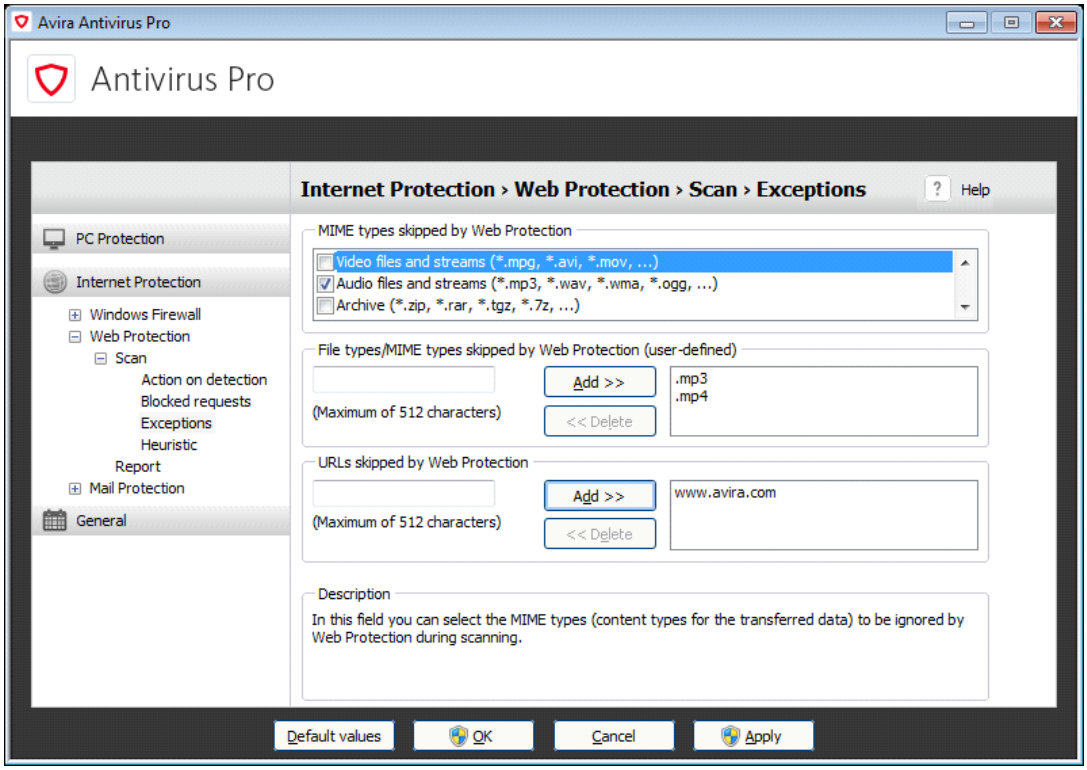


3.2 Exceptions: This option helps add file types and URLs as exceptions:

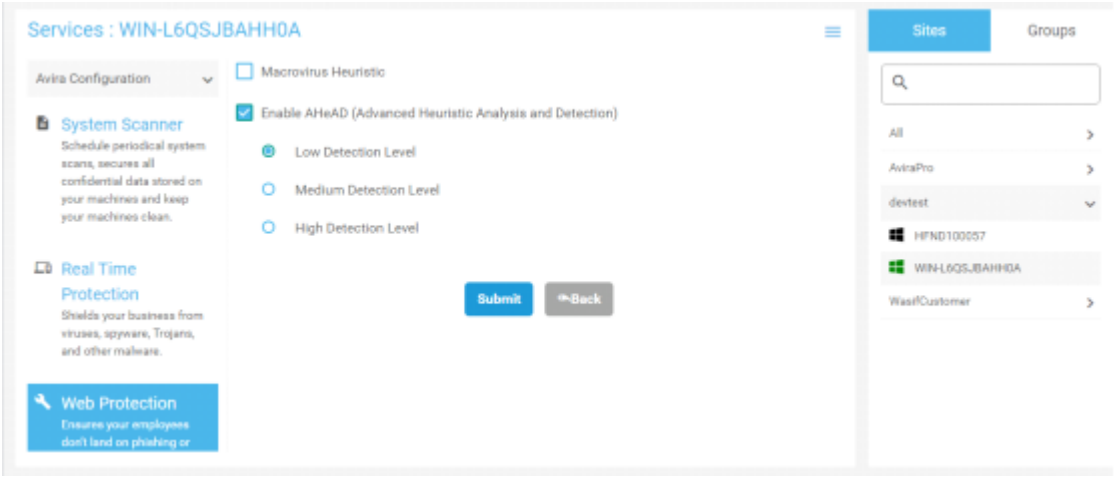
Once pushed, the following notification appears to indicate a successful execution:



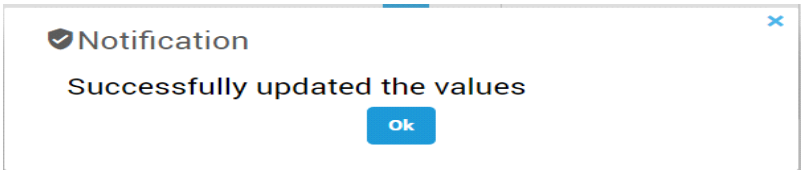
And the values are set on the Avira UI as shown below:



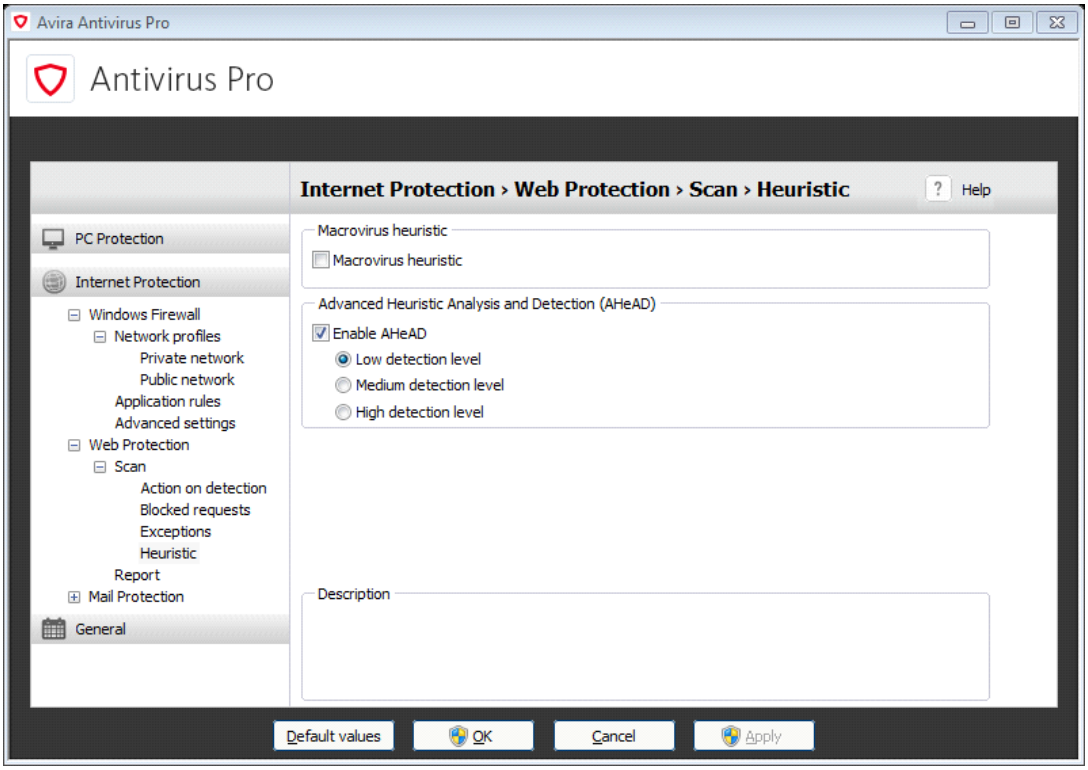
3.3 Heuristic: Following configurations can be set using the Heuristic section:



Once pushed, the following notification appears to indicate a successful execution:

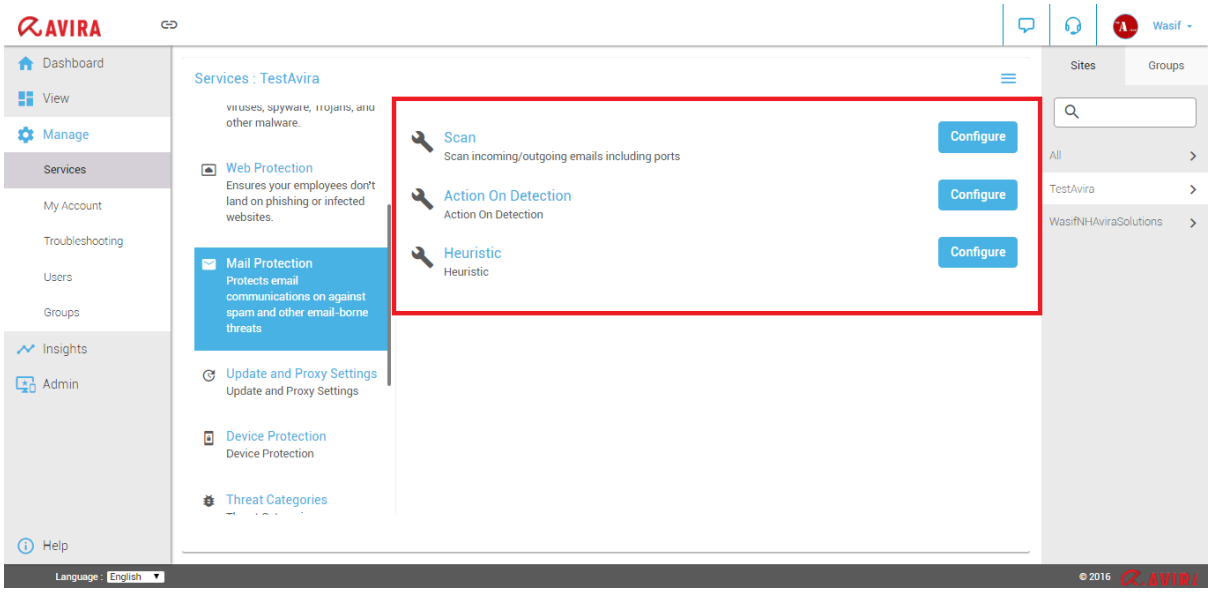


And the value will get set on Avira UI as shown below:

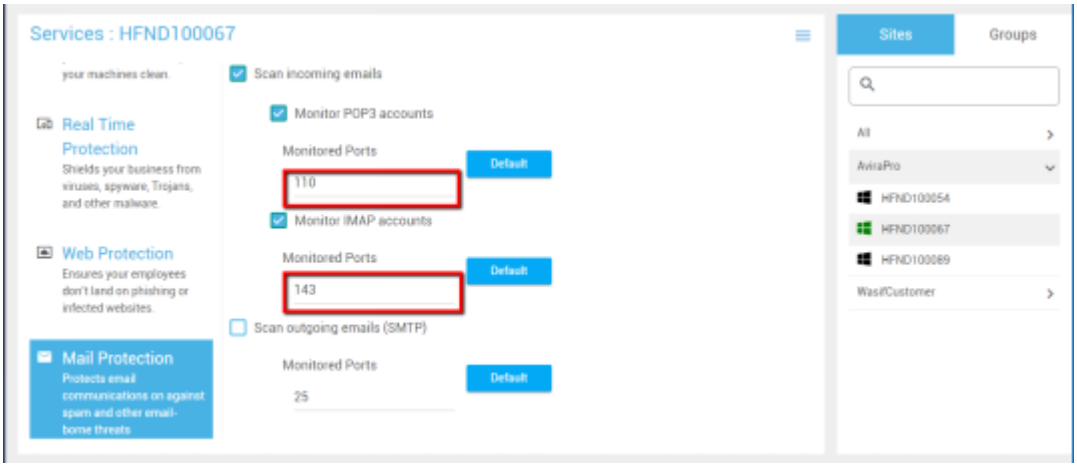


Mail Protection

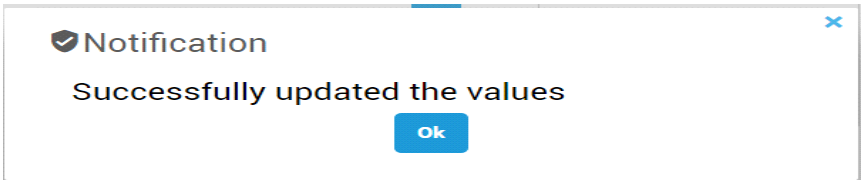
This section is divided into Scan, Action on Detection and Heuristic, as shown below:



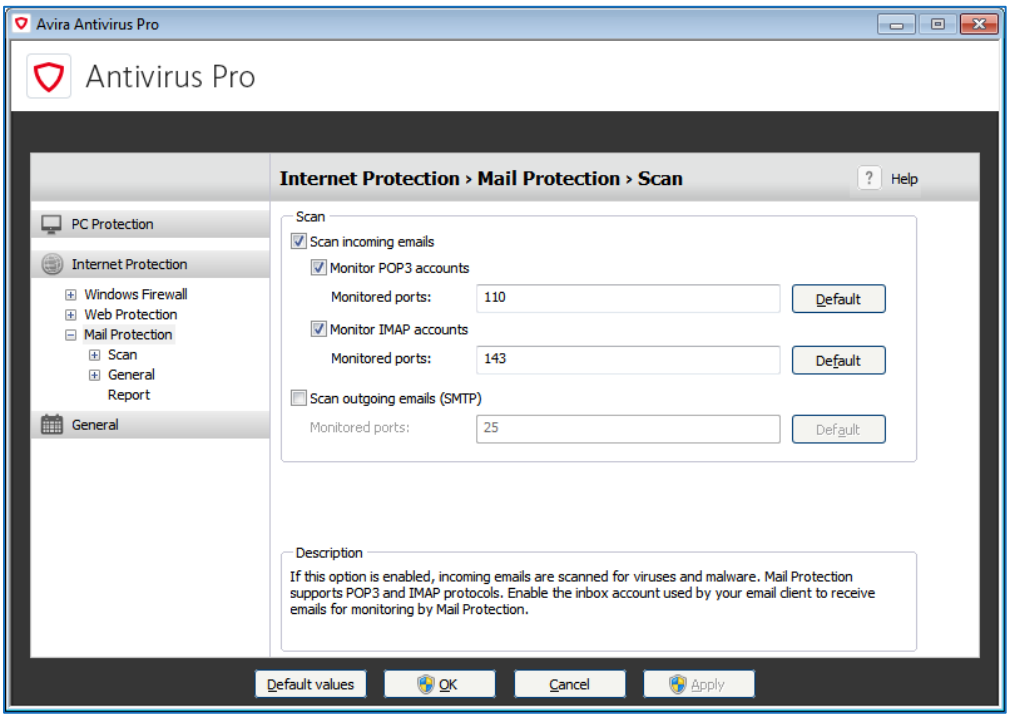
4.1Scan: This option helps in scanning specific ports:



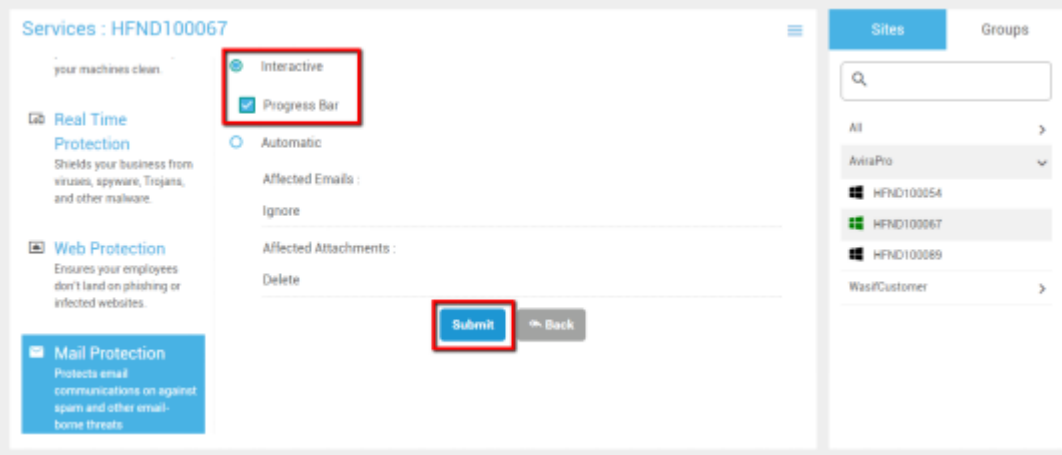
Once pushed, the following notification appears to indicate a successful execution:



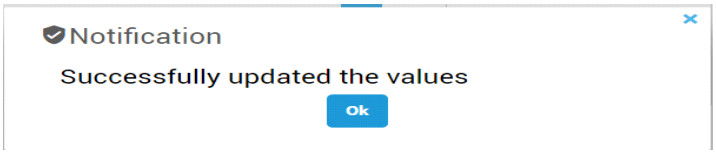
And the value will get set on Avira UI as shown below:



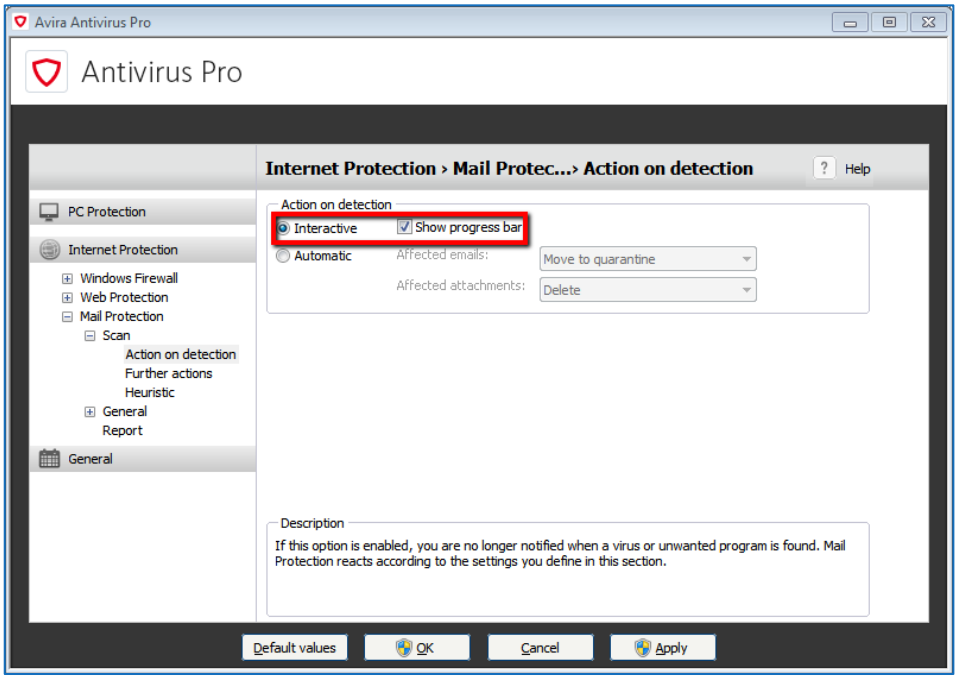
4.2Action On Detection: This enables a user to select what needs to be done when defects are detected in mails, as shown below:



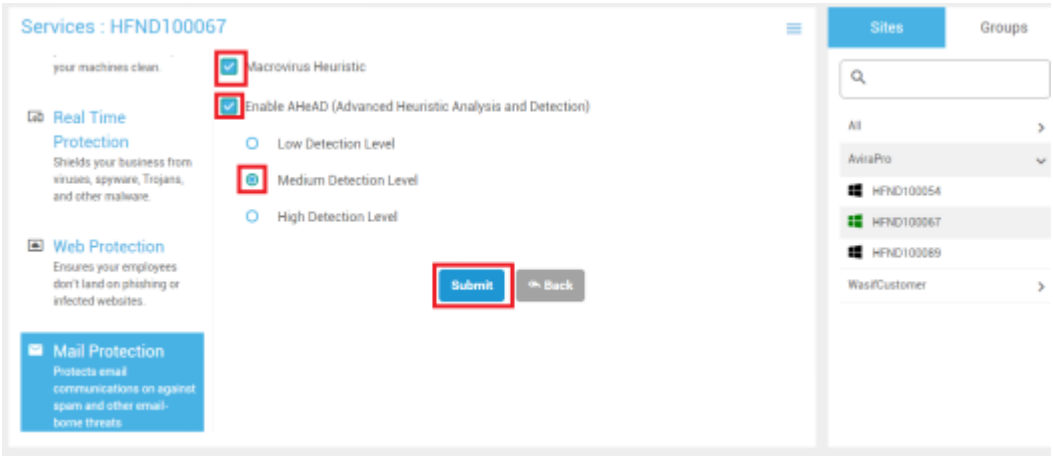
Once pushed, the following notification appears to indicate a successful execution:



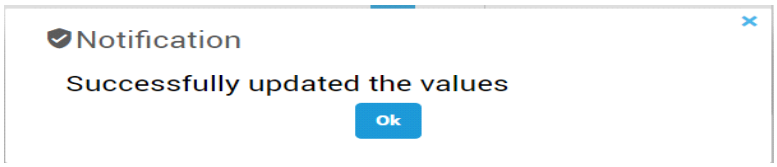
And the value will get set on Avira UI as shown below:



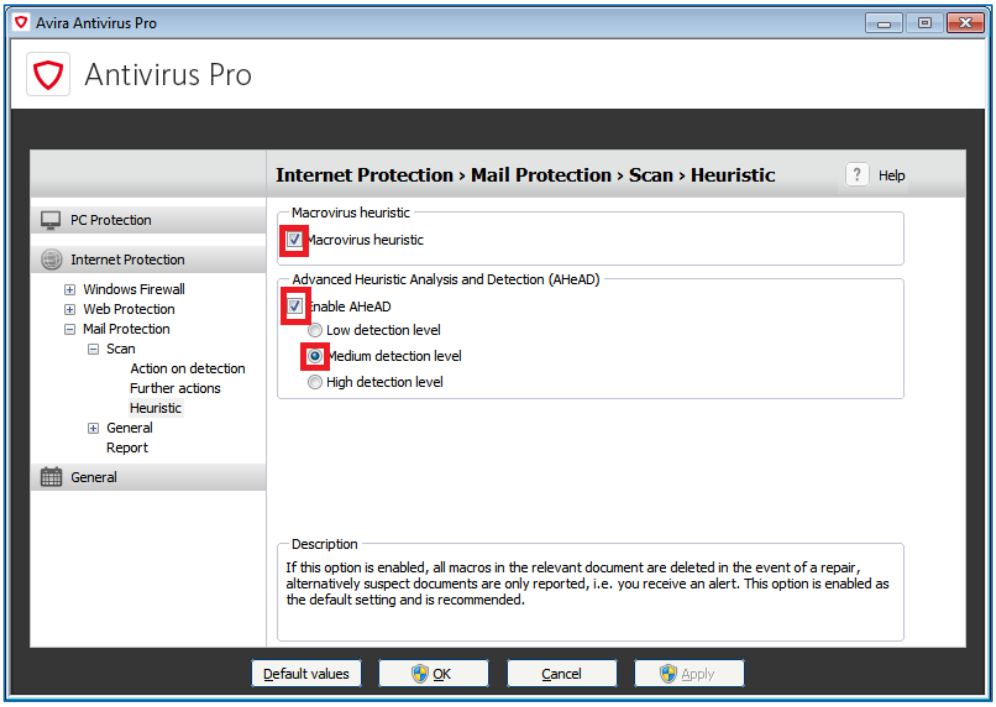
4.3Heuristic: The following configurations can be set using the heuristic feature:



Once pushed, the following notification appears to indicate a successful execution:

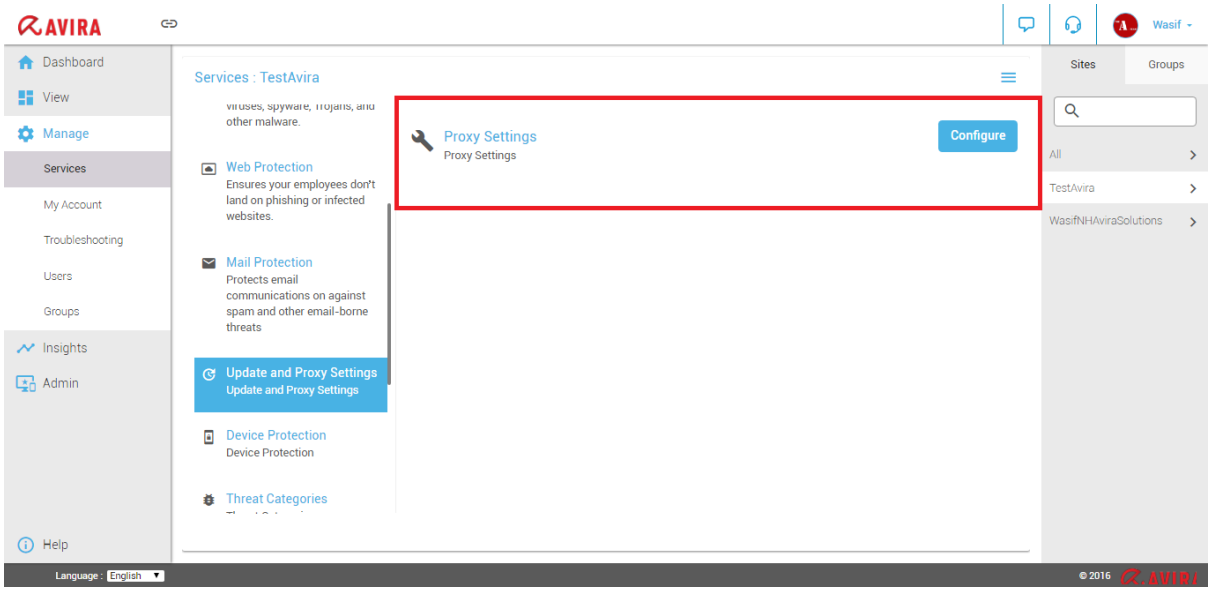


And the value will get set on Avira UI as shown below:

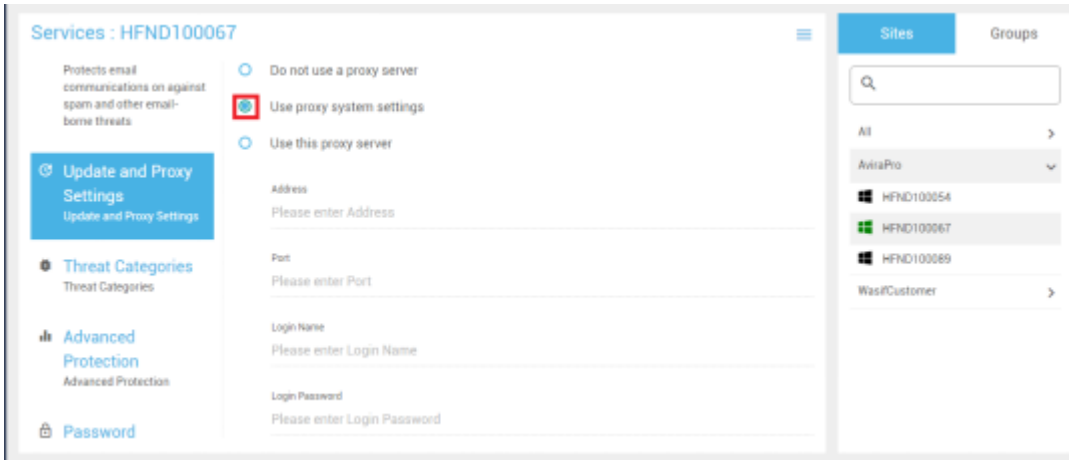


5. Update And Proxy Settings

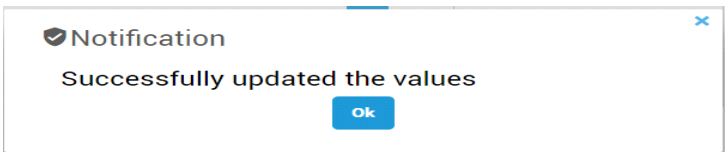
This feature helps a user configure proxy settings as shown below:



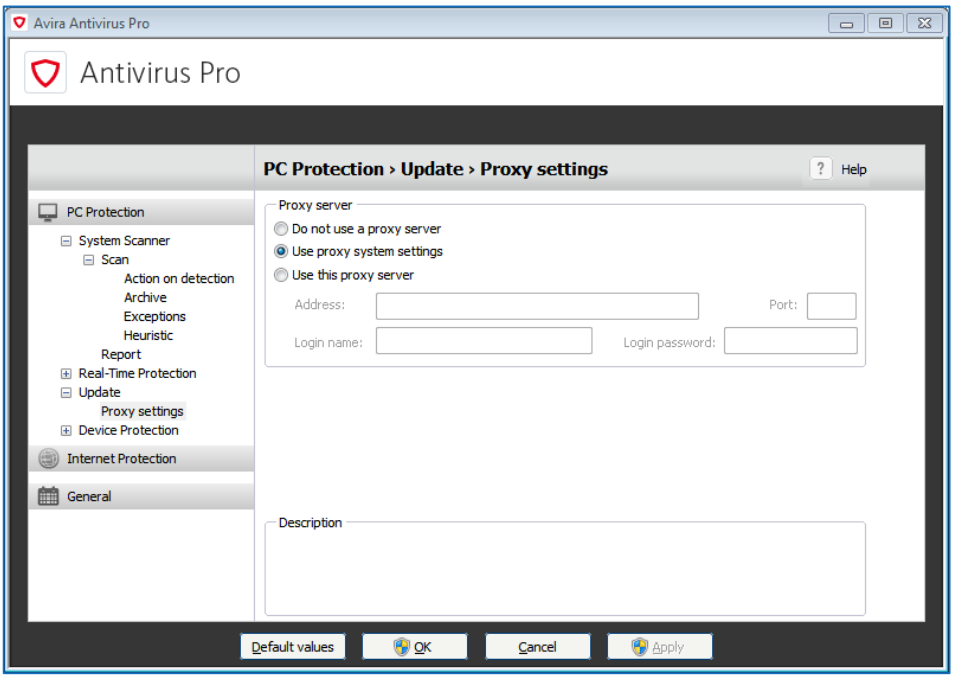
The following screen is displayed upon clicking “Configure”



Once pushed, the following notification appears to indicate a successful execution:

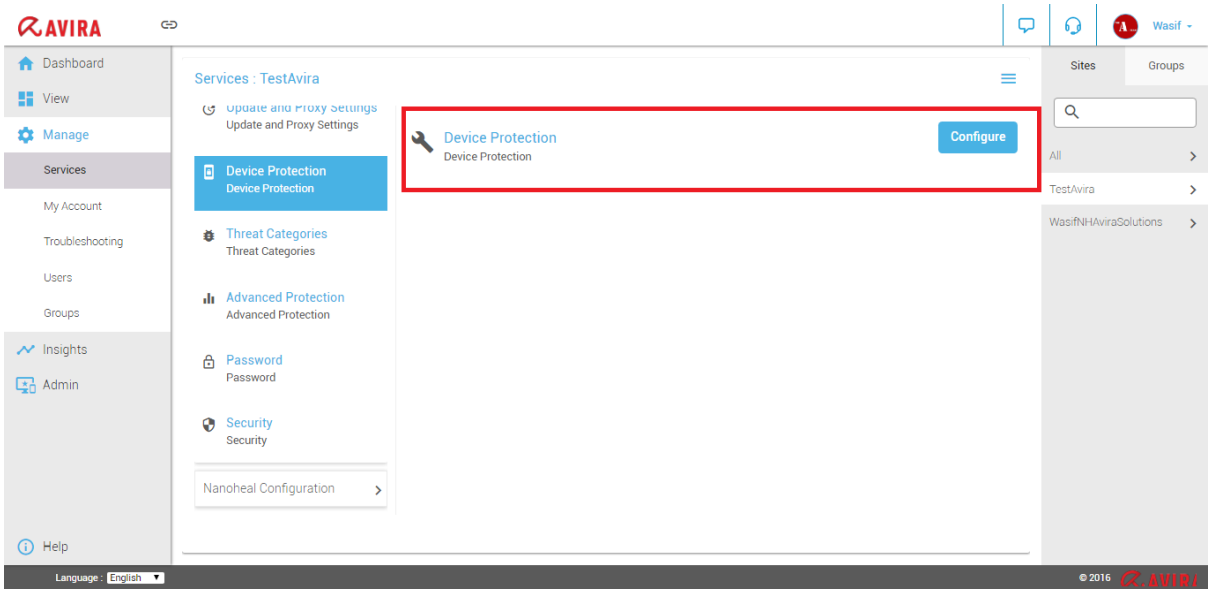


And the value will get set on Avira UI as shown below:

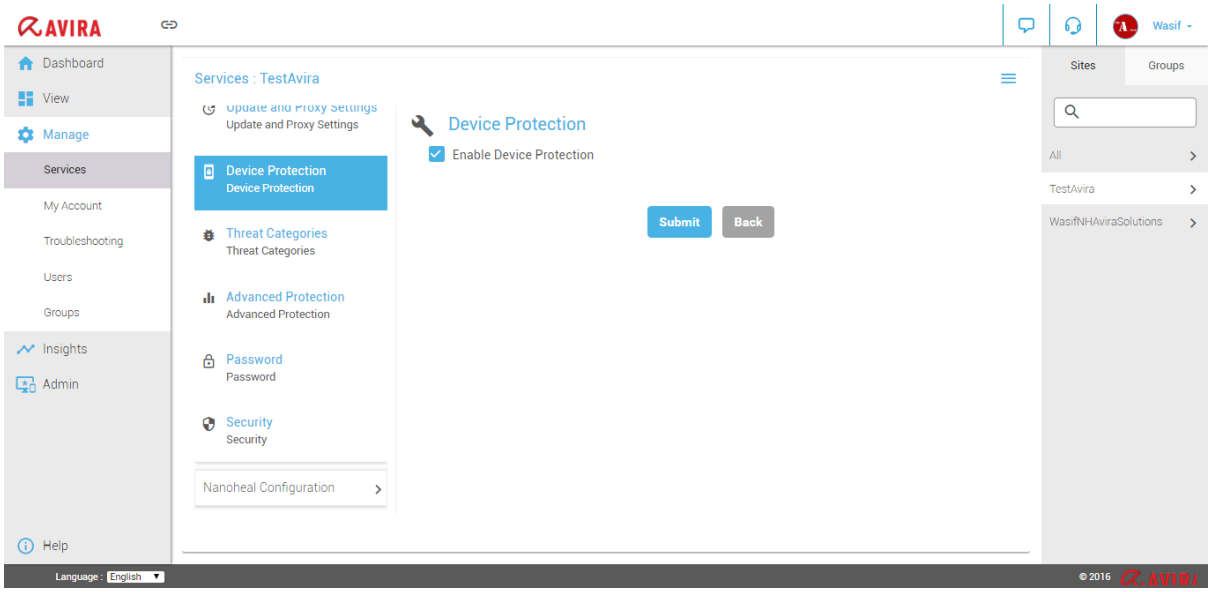


Device Protection

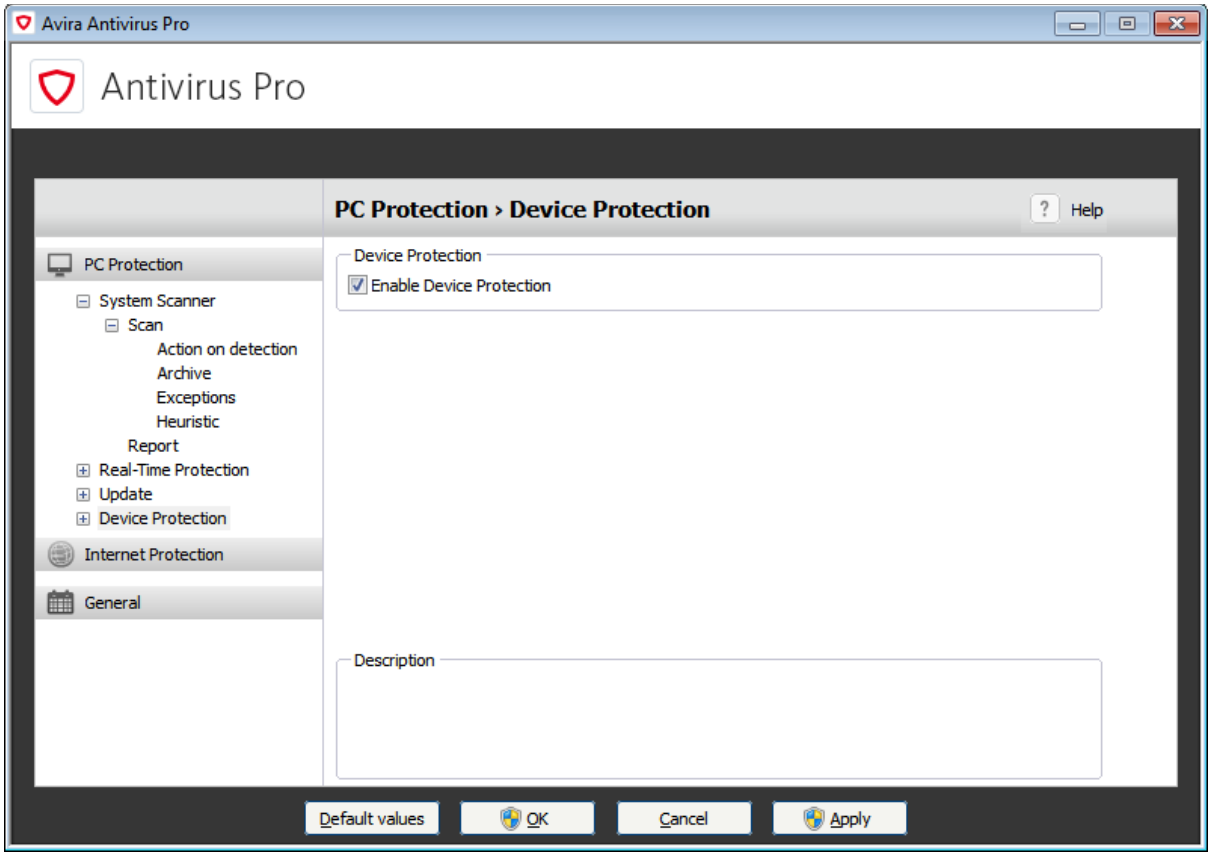
This feature helps a user configure device protection:



The following screen is displayed upon clicking “Configure”

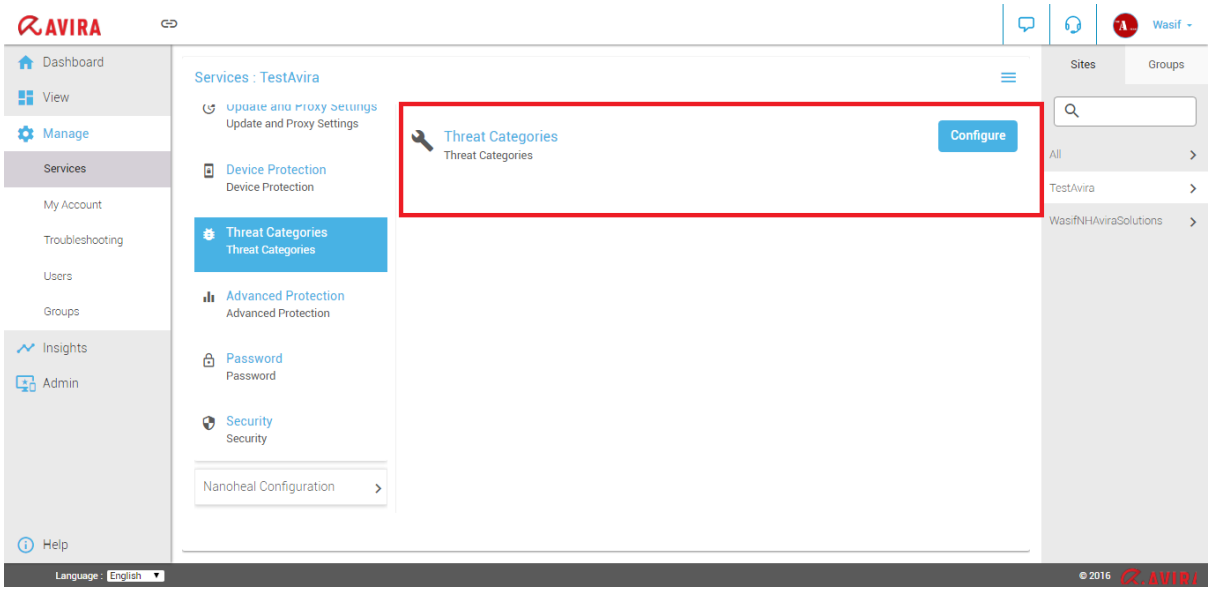


And the value will get set on Avira UI as shown below:

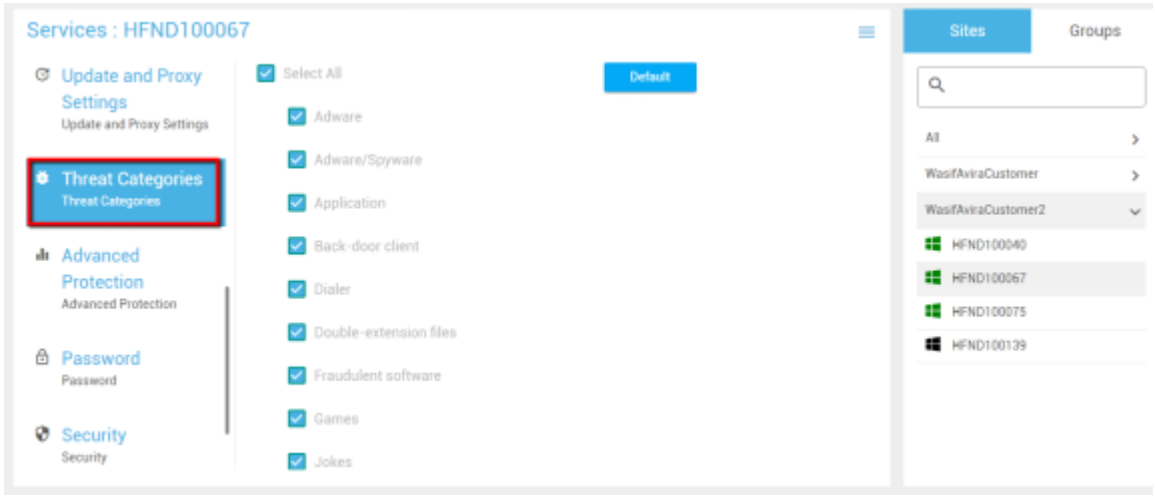


Threat Categories

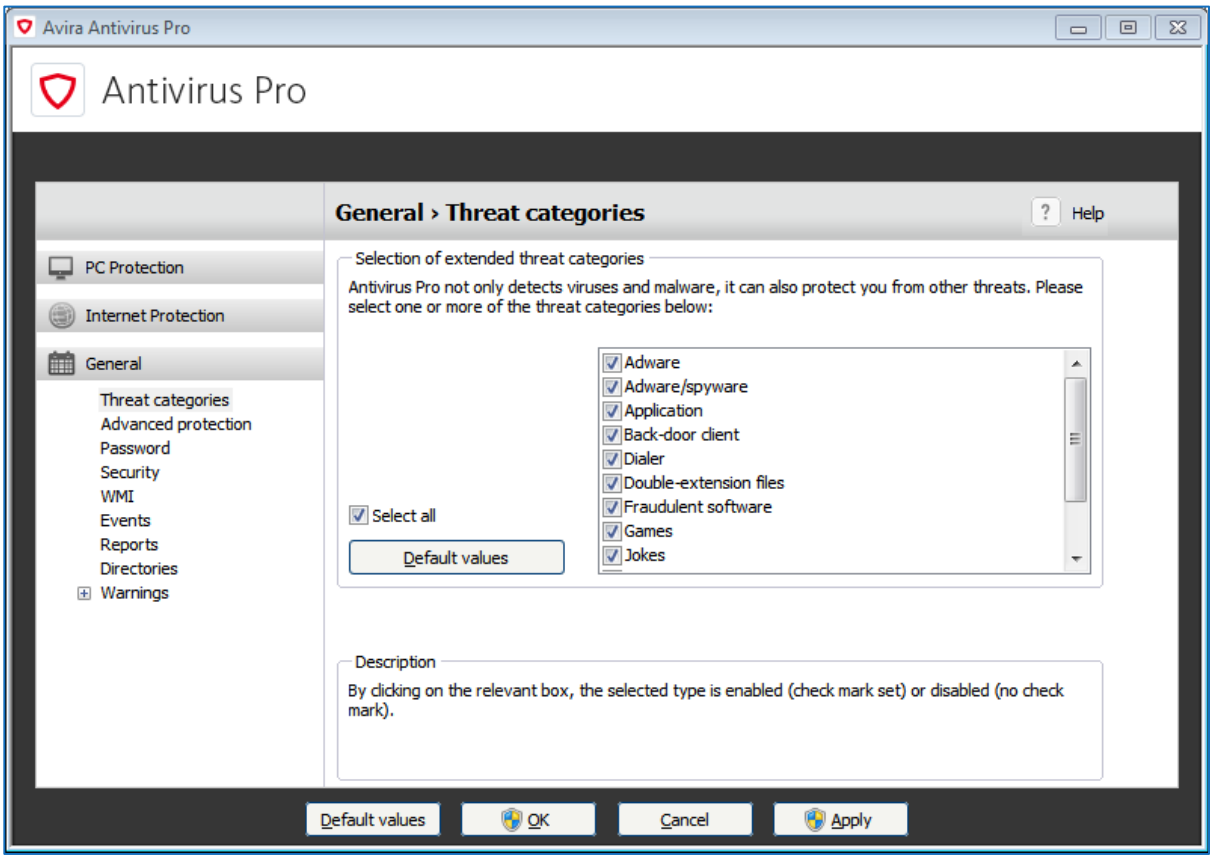
This feature helps a user configure the threat categories:



The following screen is displayed upon clicking “Configure”

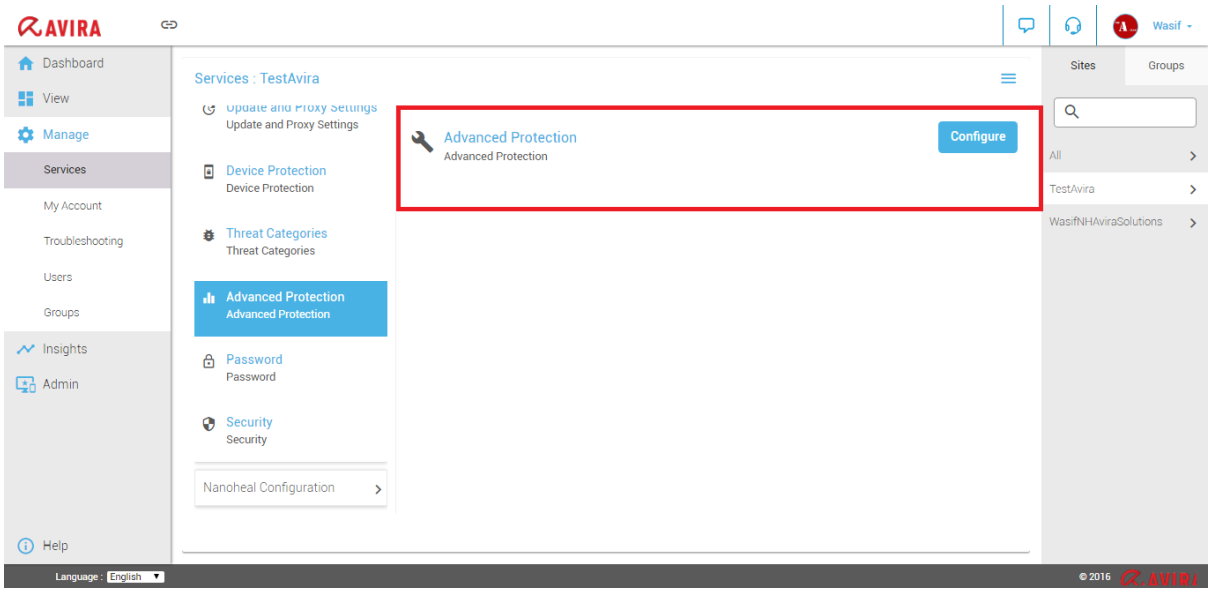


And the value will get set on Avira UI as shown below:

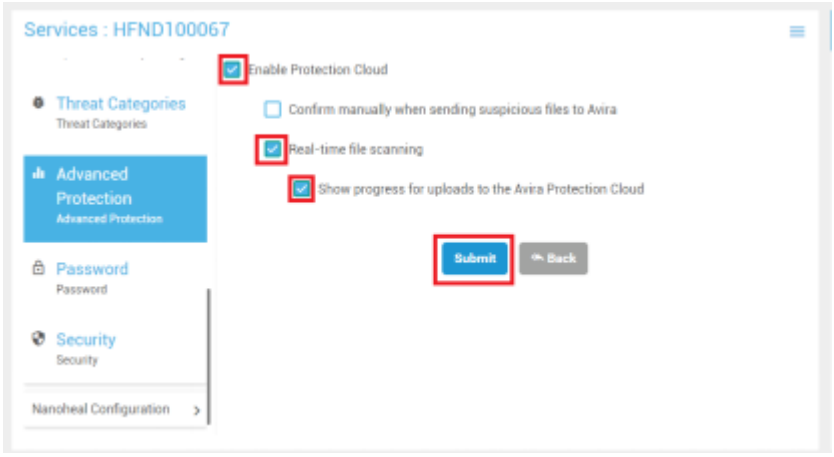


Advanced Protection

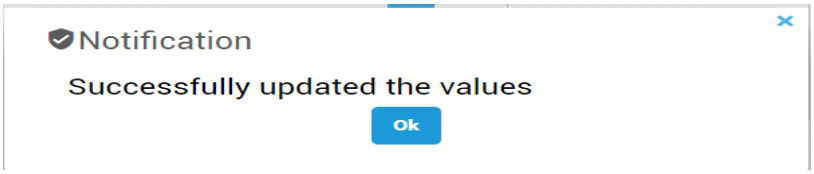
This feature helps a user configure advance protection options as shown below:



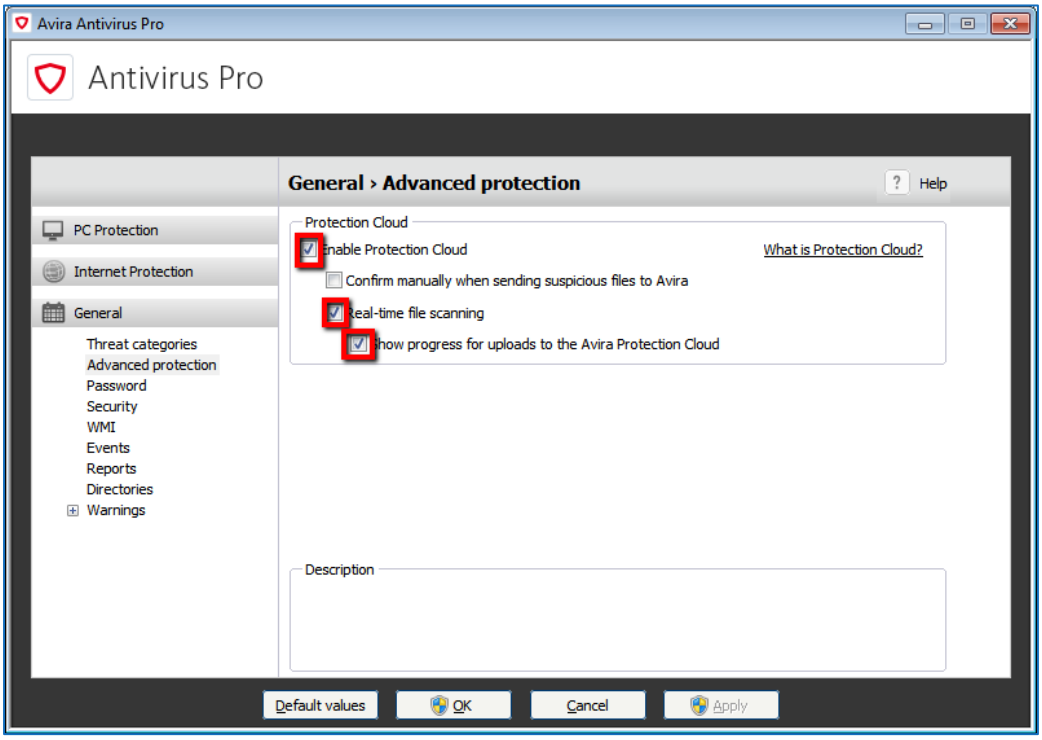
The following screen appears upon clicking "Configure"



Once pushed, the following notification appears to indicate a successful execution:

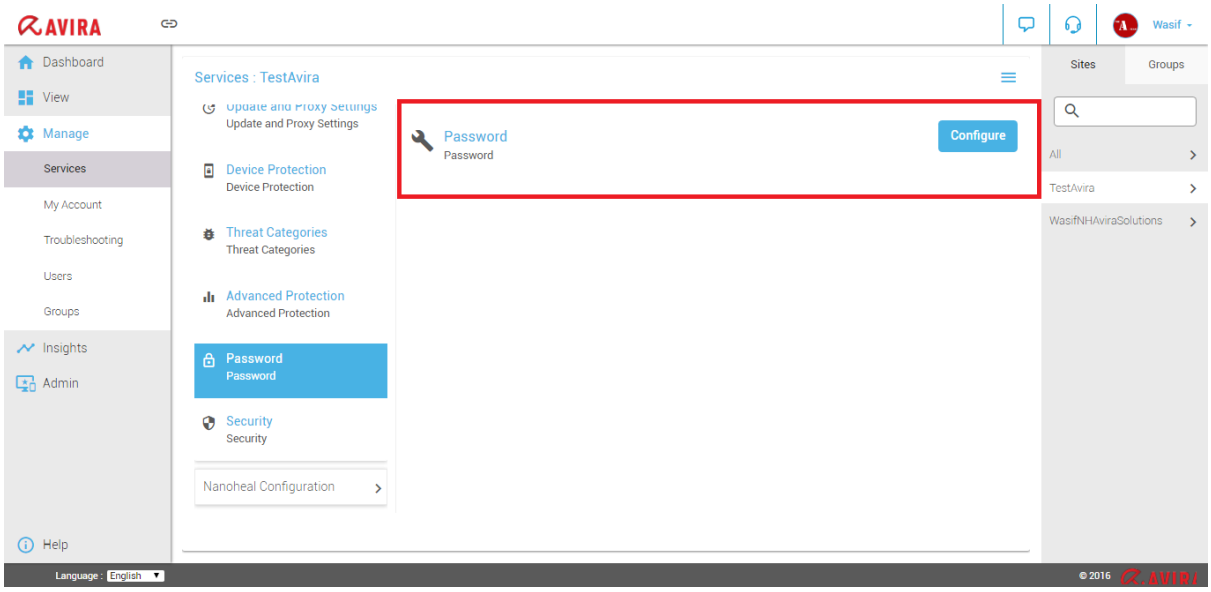


And the value will get set on Avira UI as shown below:



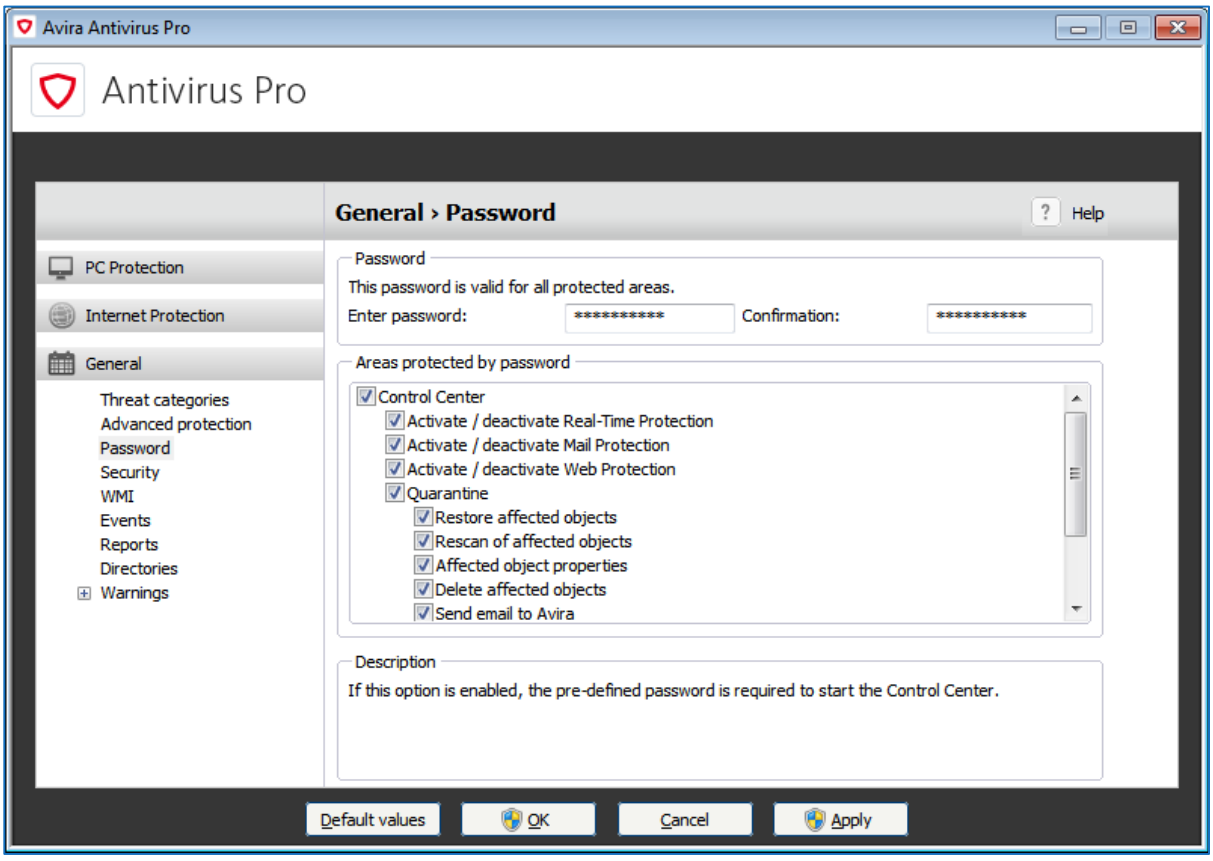
Password

This feature helps the user configure a password for the AVIRA modules:



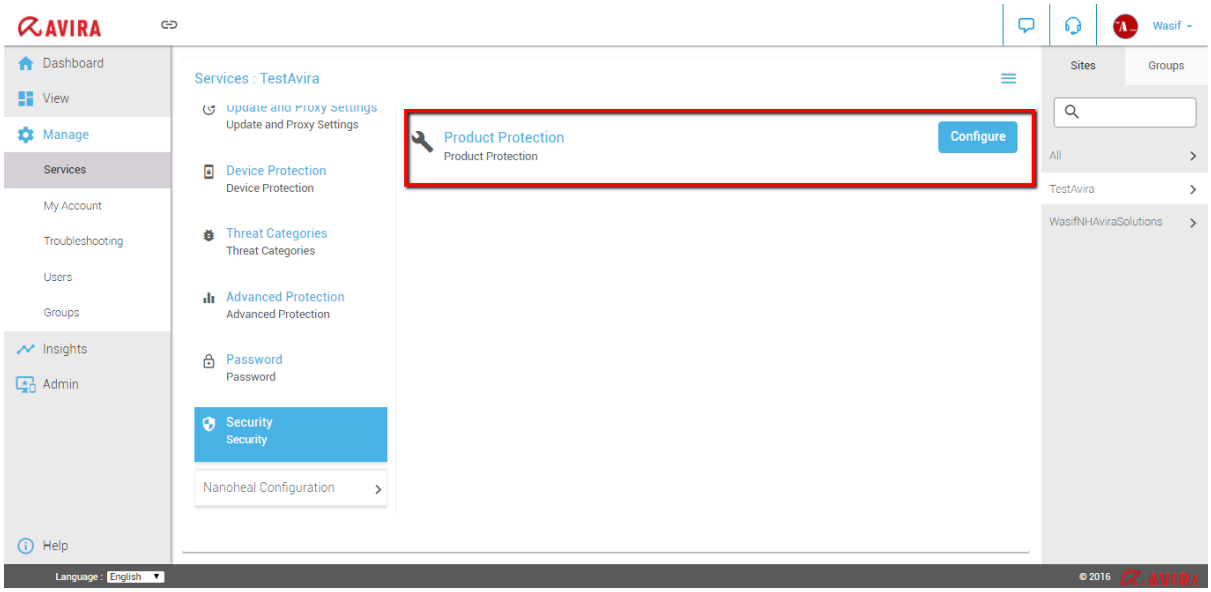
The following screen appears upon clocking "Configure". The user must select the desired categories to be protected using a password.

And the value will get set on Avira UI as shown below:



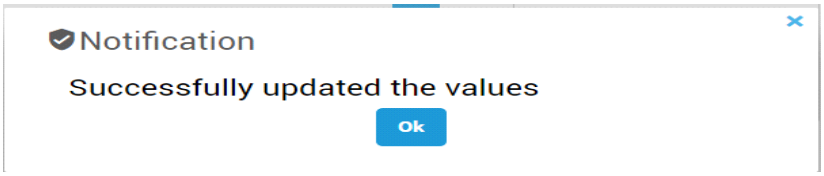
Security

This feature helps the user configure security options as shown below:

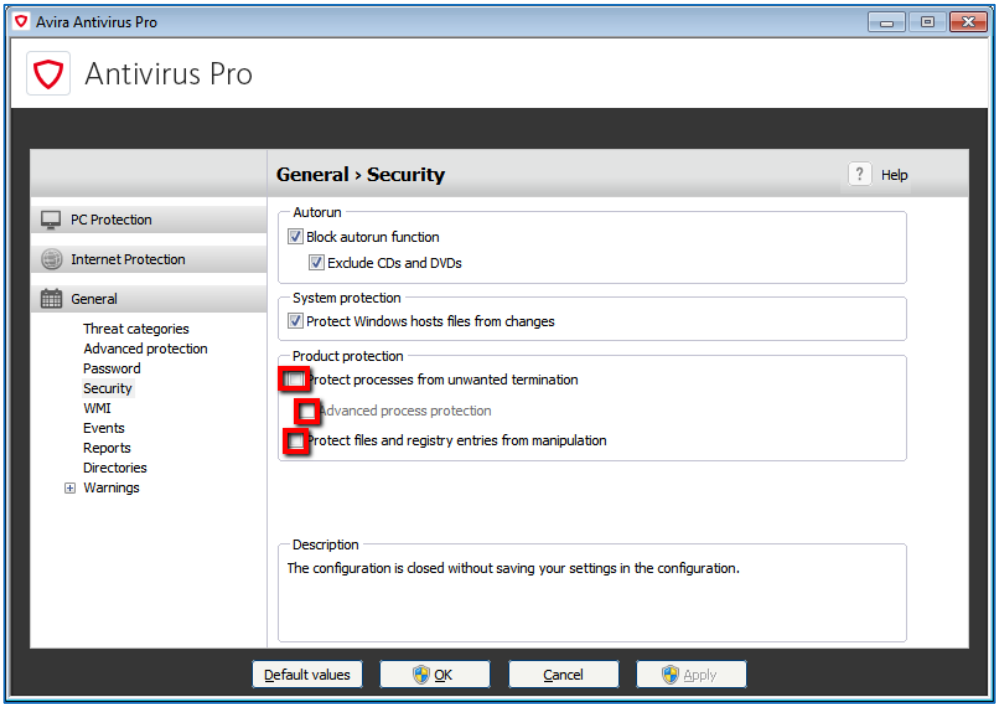


The following screen appears upon clicking “Configure”

Once pushed, the following notification appears to indicate a successful execution:



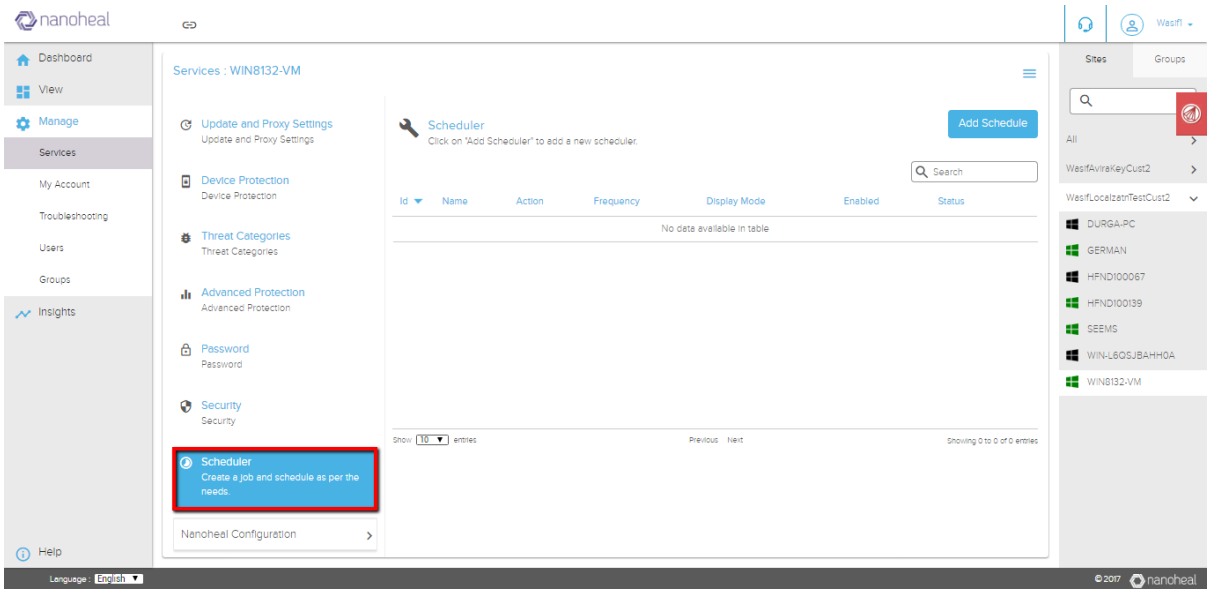
And the value will get set on Avira UI as shown below:



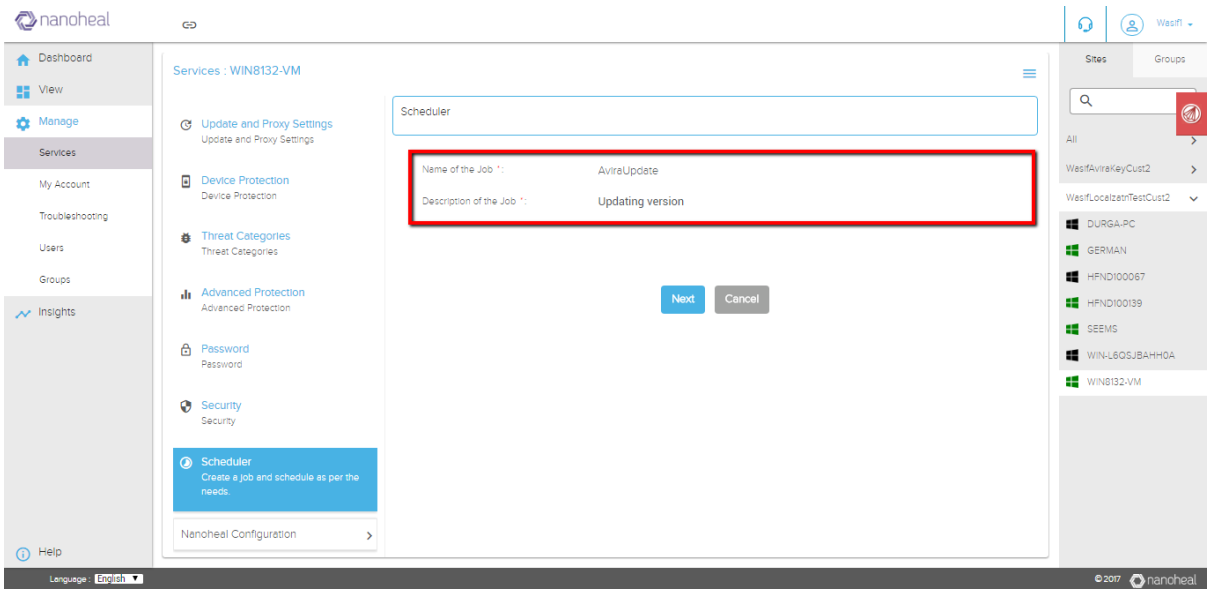
Scheduler

This feature helps user to schedule scan and update functionality on daily,weekly,hourly basis.

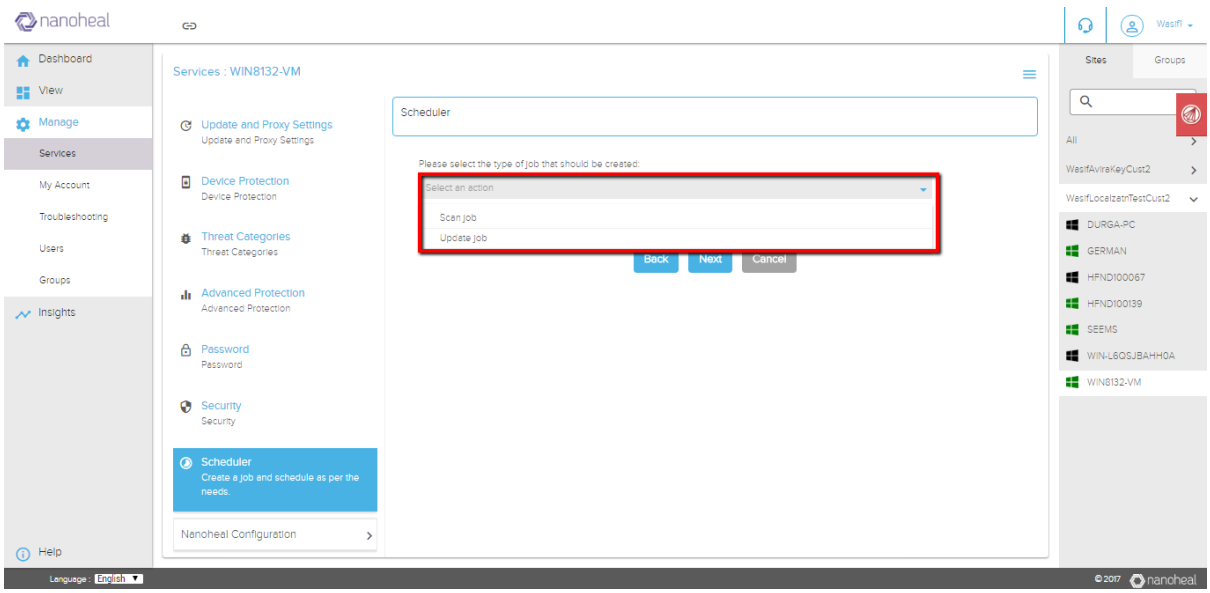
On click of scheduler following screen will come up:



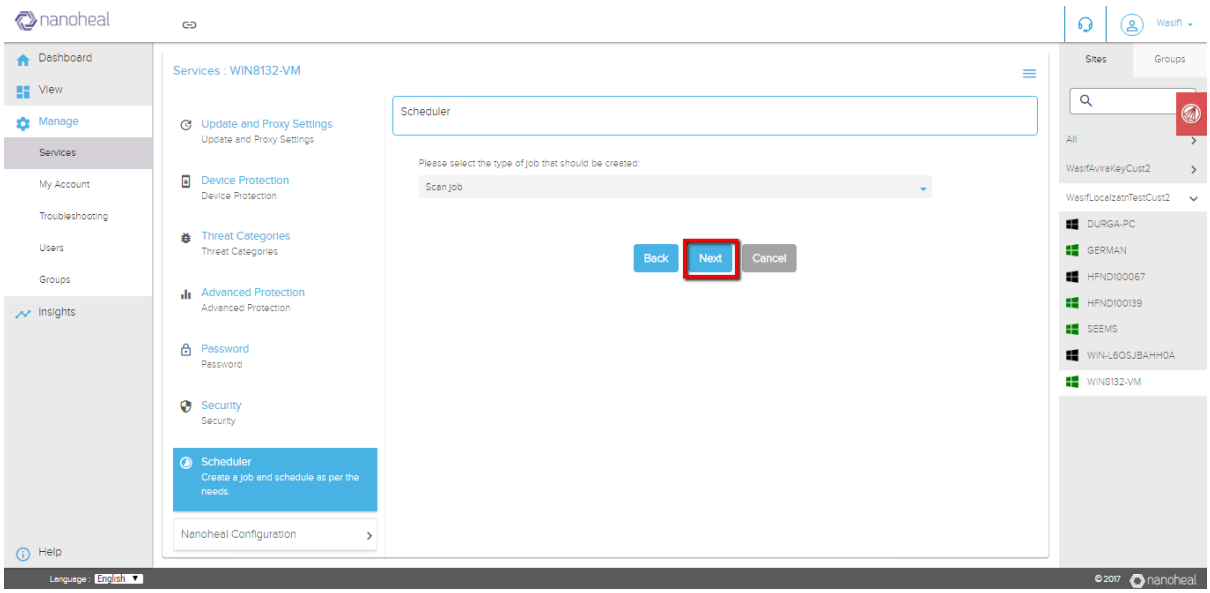
User has to click on "add schedule" to schedule a job and has to enter name of job and description as shown below:

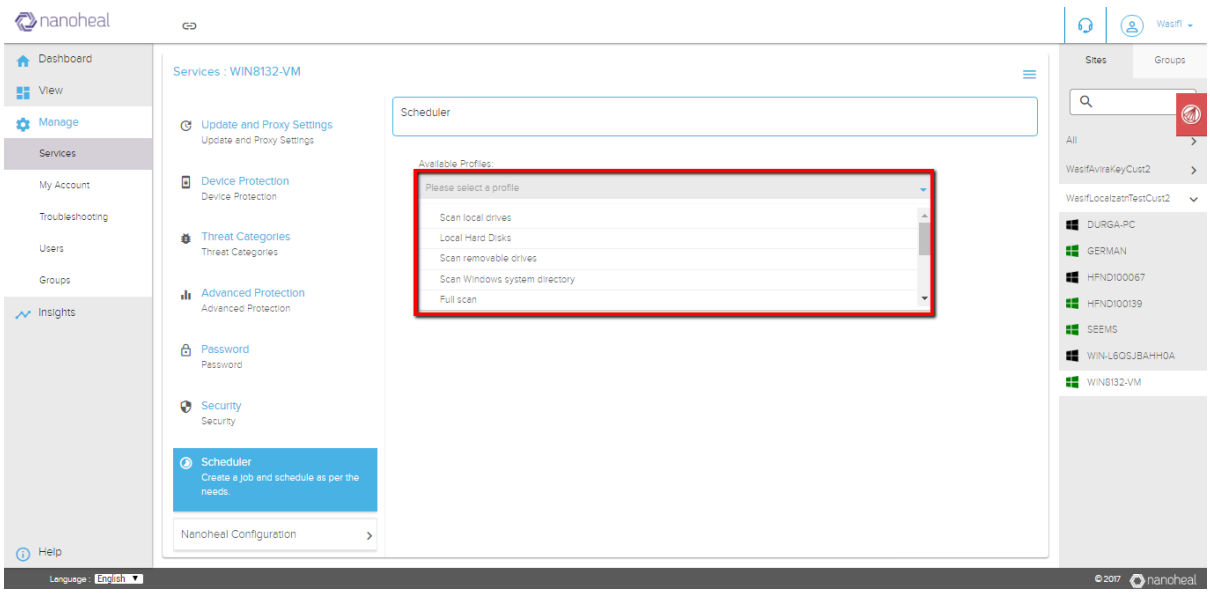


Click on Next will give user option to select whether they want to schedule scan or update as shown below:



Scan: If user proceed to schedule scan, on the next page he will be prompted with the option of different types of scan as shown below:





I) Scan local drives: It will scan only the local drives on the schedule run.

II) Local Hard Disk: It will scan only the local hard disk.

III) Scan Removable drives: It will scan only the removable drives.

IV) Scan Windows System Directory: It will scan only the system directory.

V) Full scan: It will scan the whole system.

VI) Quick Scan: It will do a quick scan.

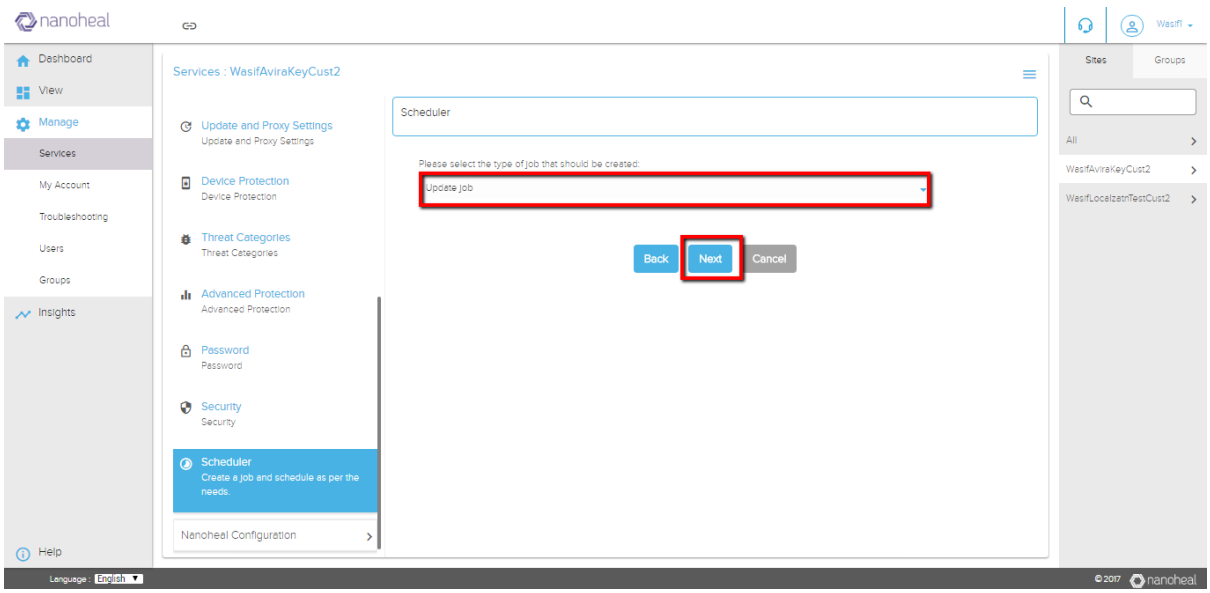
VII) Scan my documents: It will scan only My Documents folder.

VIII) Scan Active processes: It will scan only the active processes.

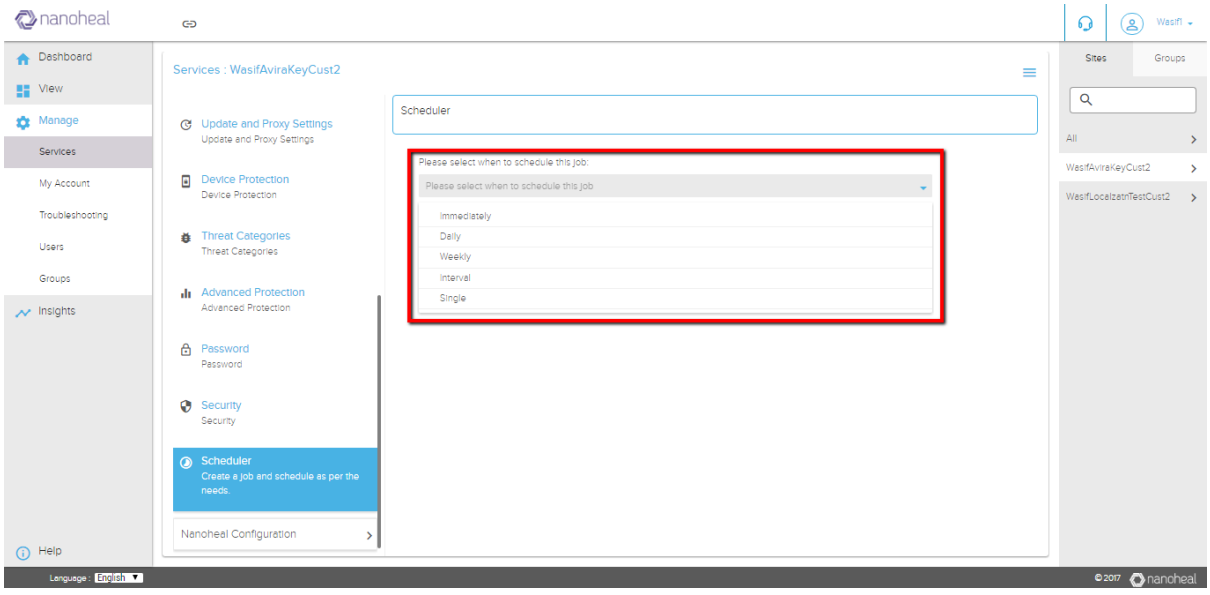
IX) Scan for rootkits: It will scan only to search for rootkits.

X) Custom scan: It will do scan of configured location only.

Update : This feature will help user to schedule Avira Update as shown below:

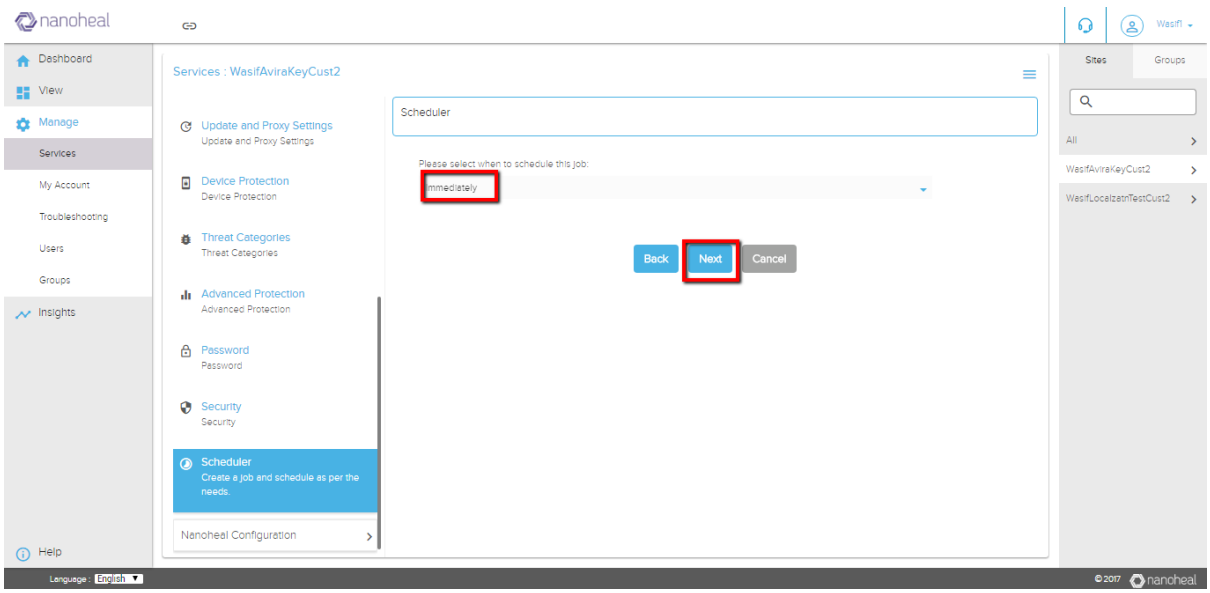


Selecting any type of scan or Update option and clicking on next will give user the option to schedule the job as shown below:

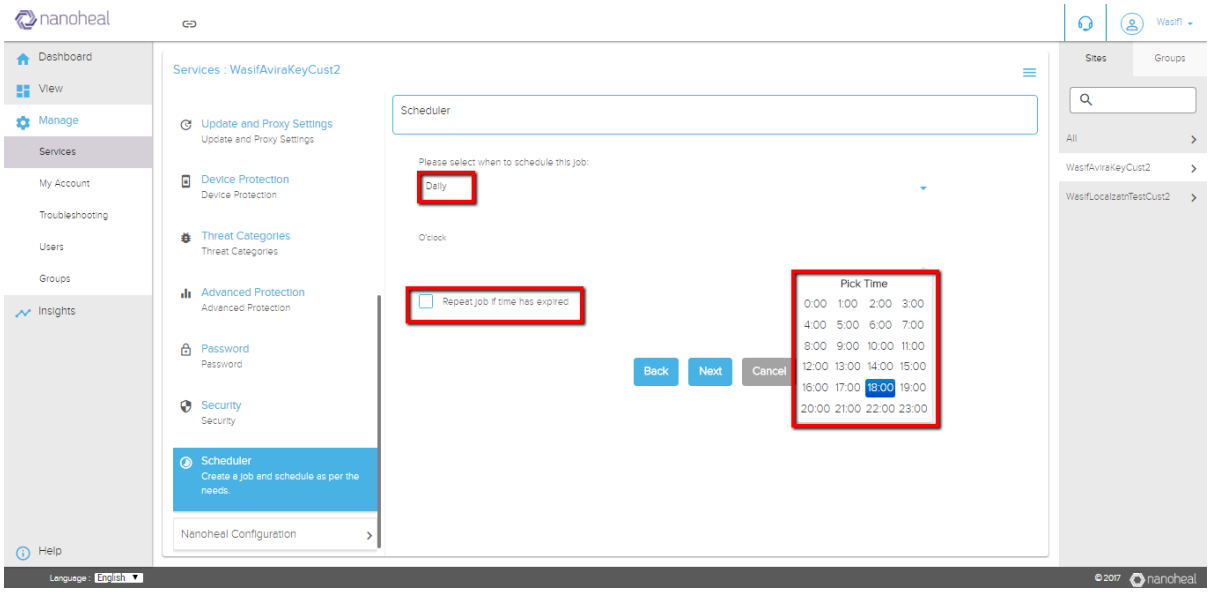


User can schedule the job in following formats:

I) Immediately: It will trigger the selected option I.e scan/Update immediately once the config reaches to machine.

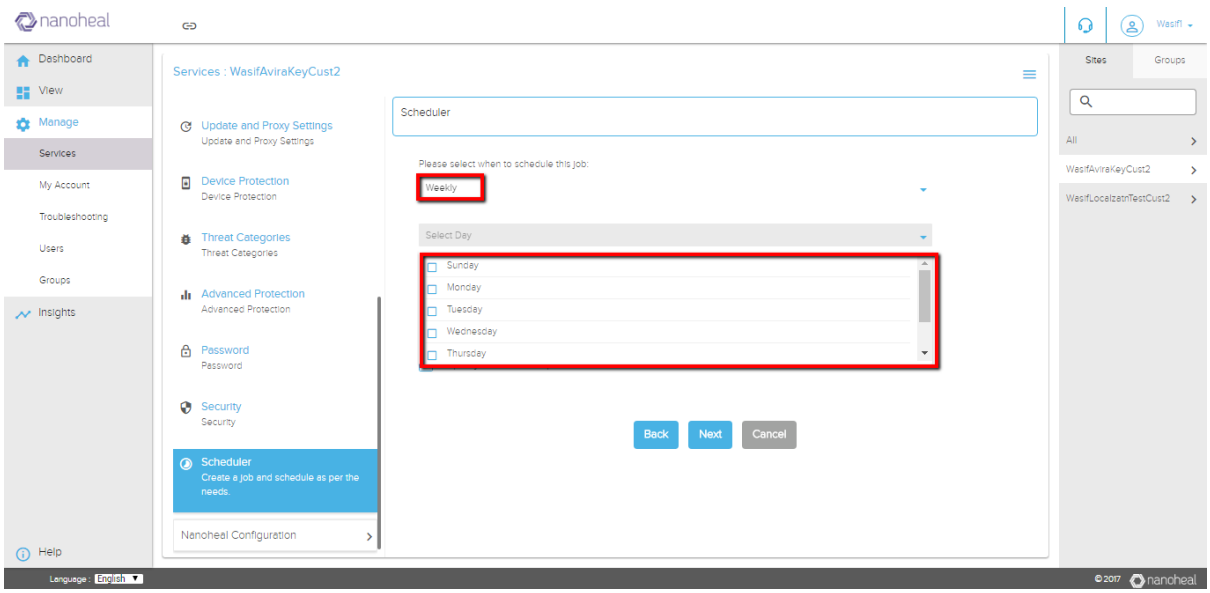


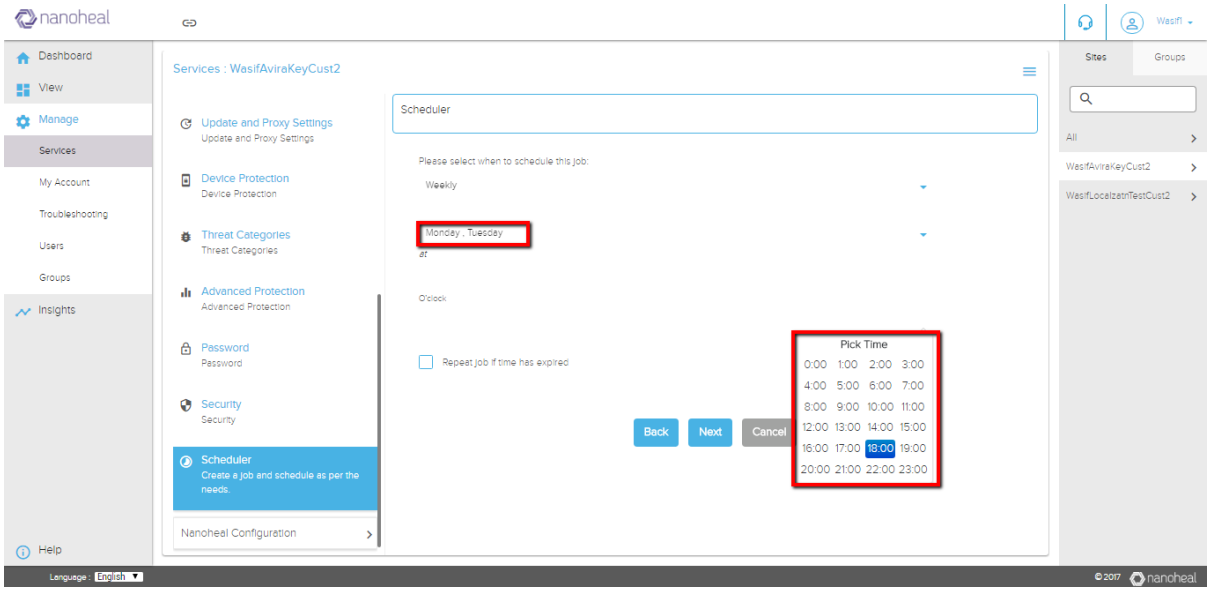
II) Daily: It will give user further option to pick a time on which the task will run and what to be done if the schedule is missed.



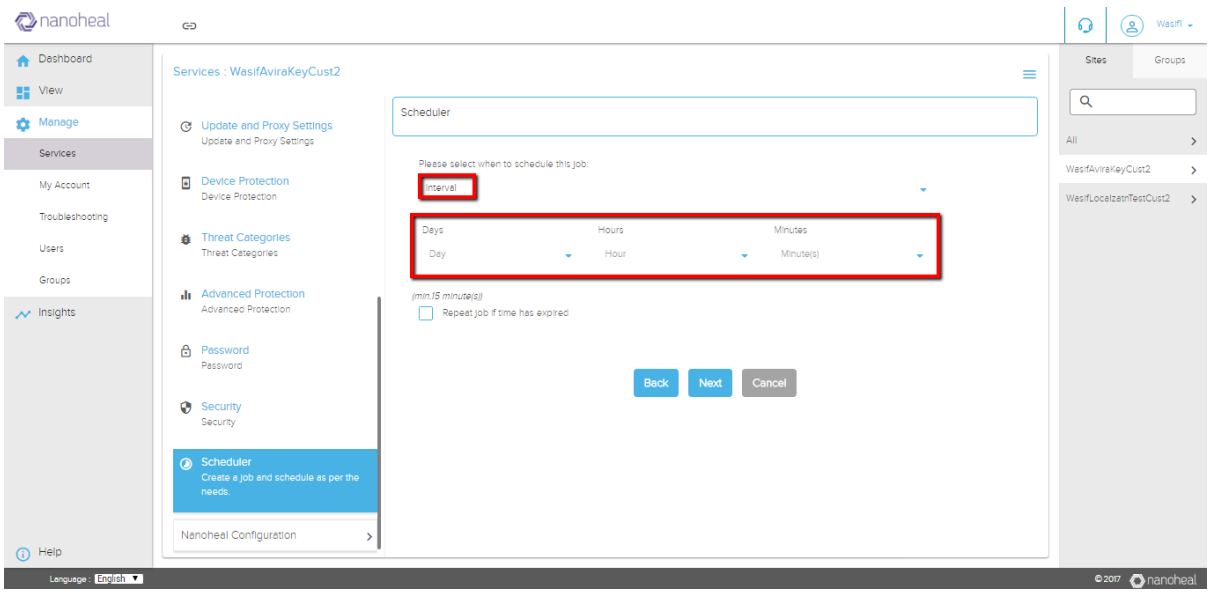
If the scheduled time is missed and 'Repeat job if time has expired' option is checked, it will execute the task immediately whenever the nanoheal service is up after schedule miss.

III) Weekly: By this, user can schedule the task on weekly basis(day and time) as shown below:



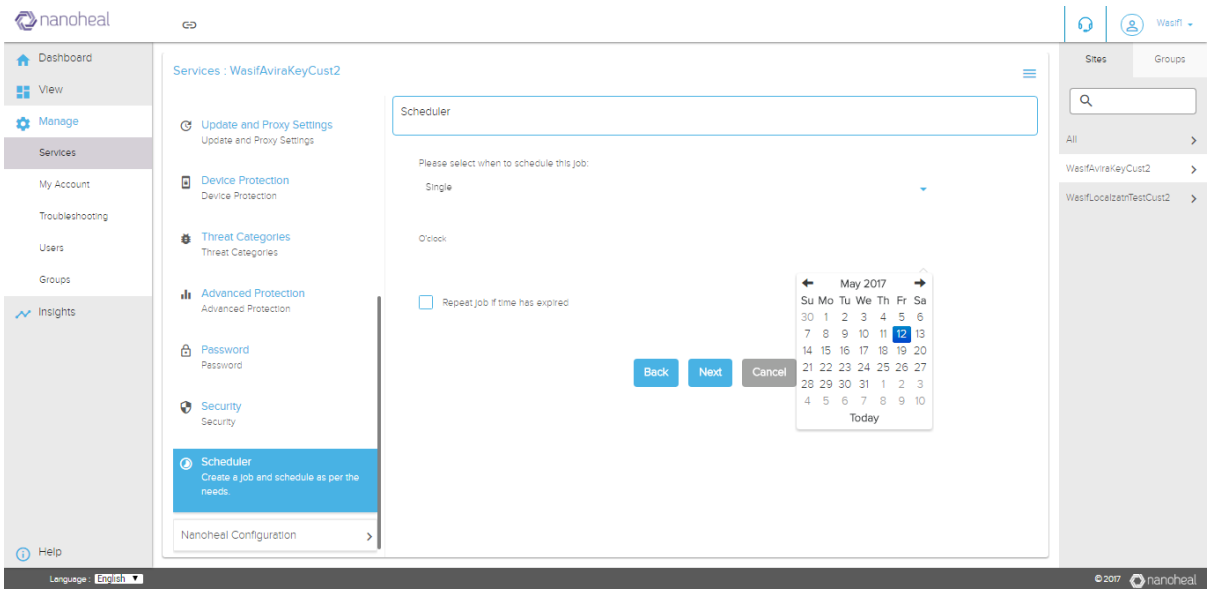


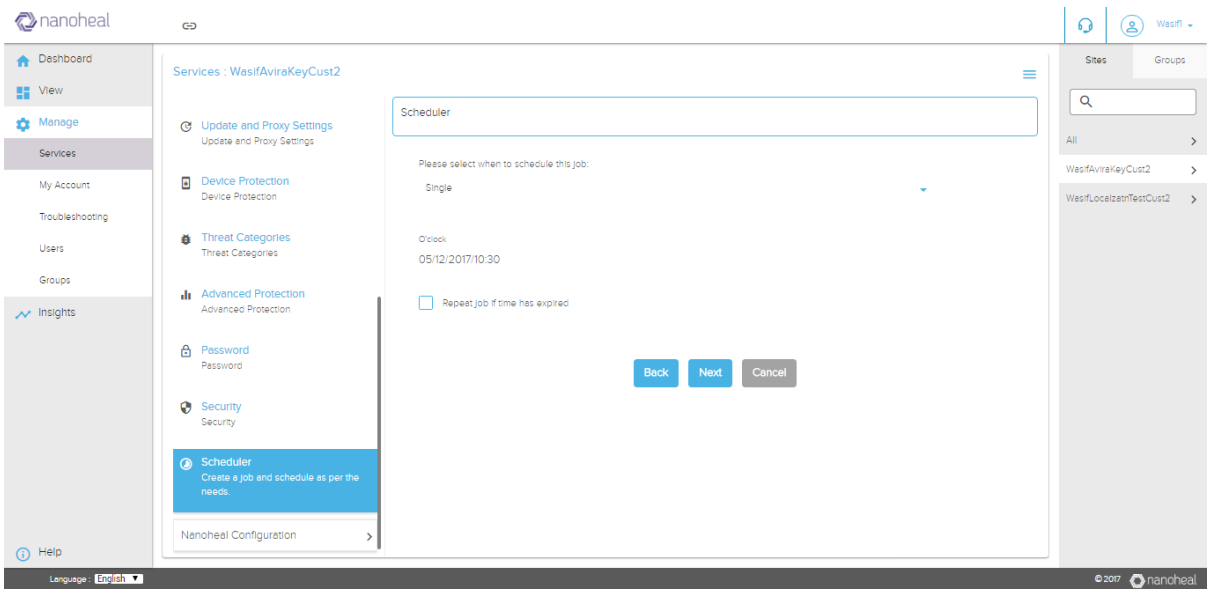
IV) Interval: This option will perform the task after the configured interval.



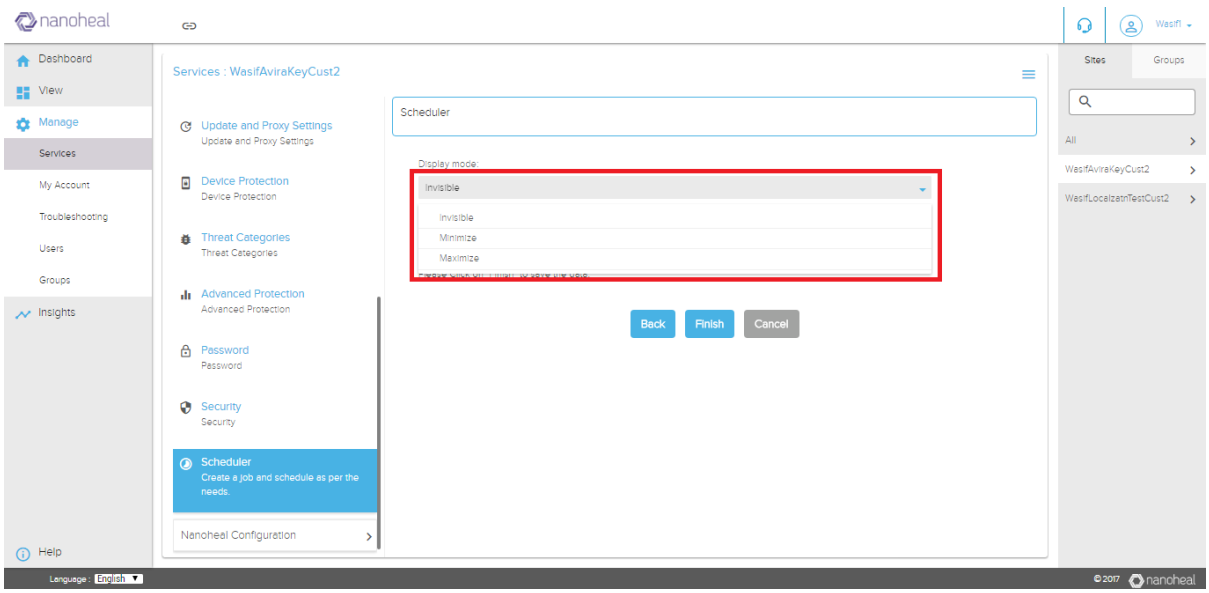
NOTE: The interval should be minimum of 15 minutes.

V) Single: This option will perform the task only on the configured day and time as shown below:





Now after scheduling the time, click on next will ask user how they want to perform the task and whether the want to shut down the system after task is done as shown below:

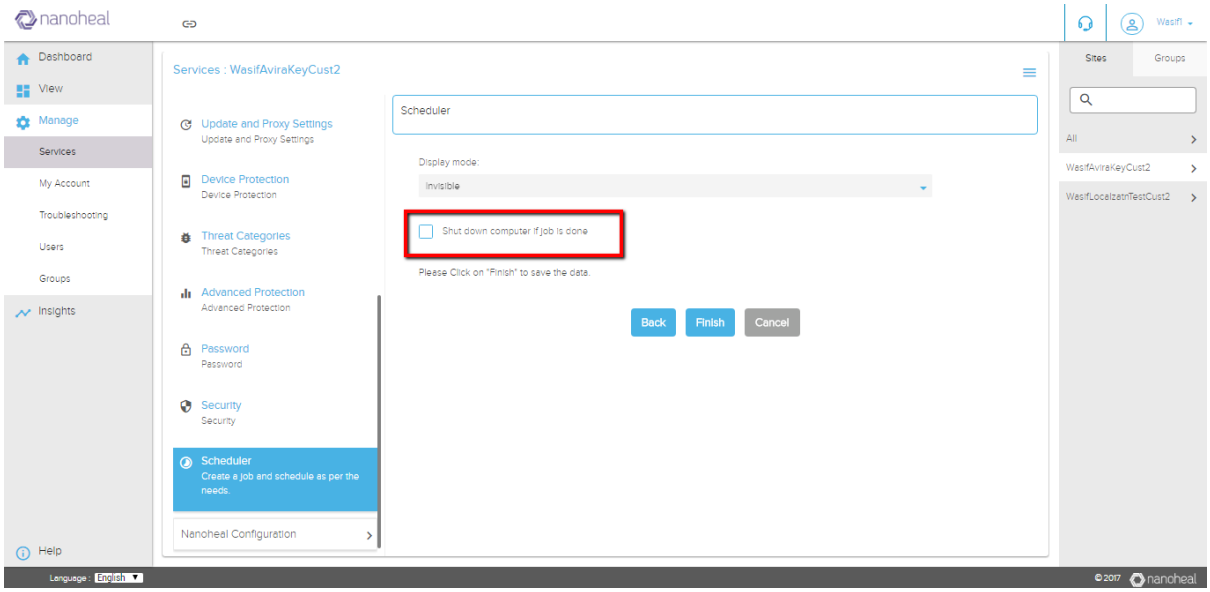


I) Invisible: It will perform the task in background.

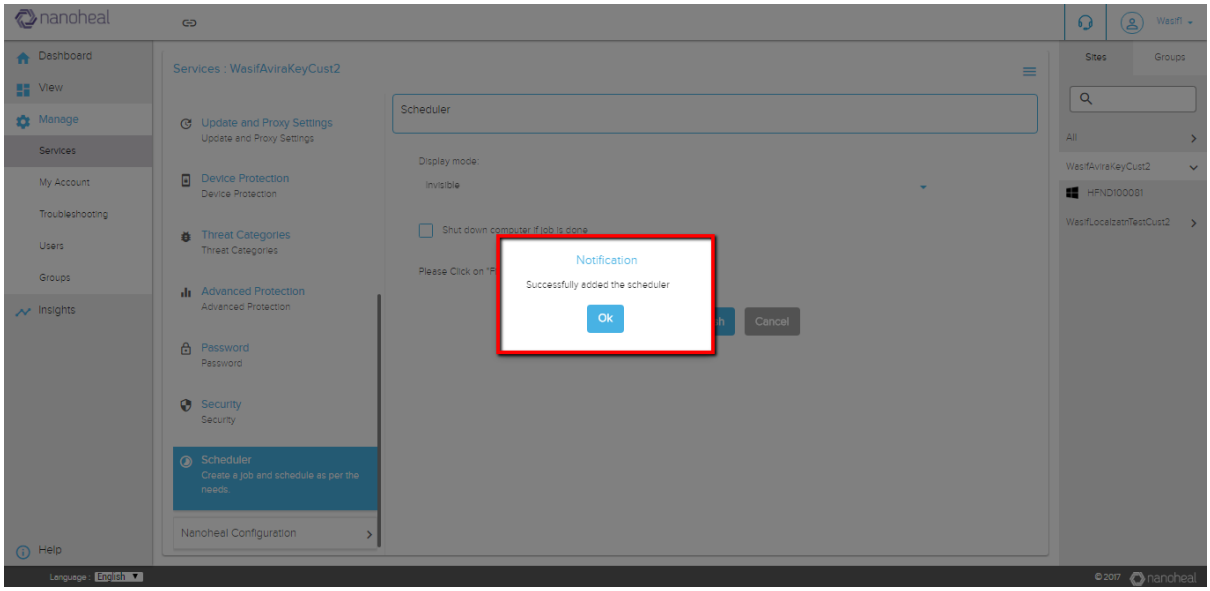
II) Minimize: It will minimize the avira UI while performing the task.

III) Maximize: Avira UI will be visible to the user.

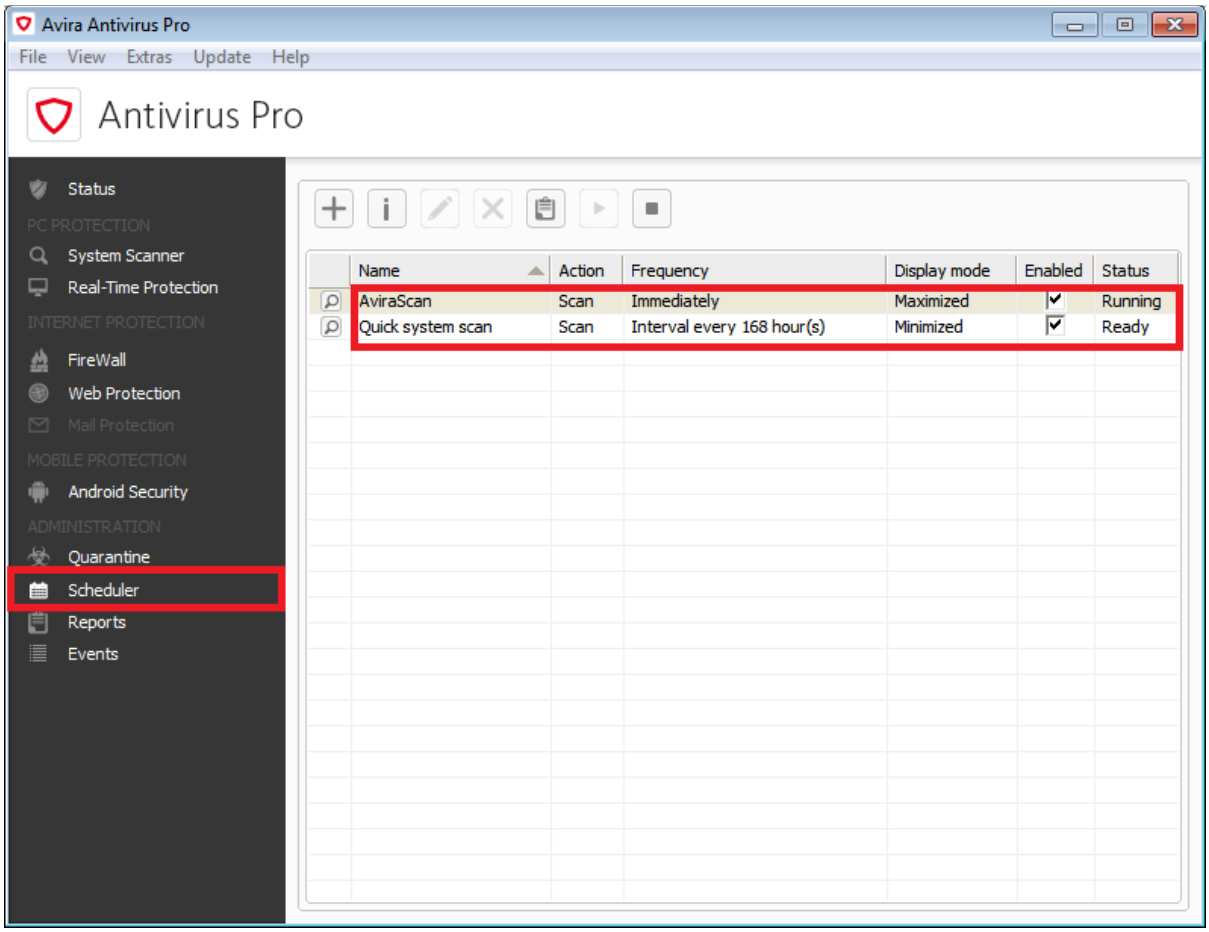
If "Shut down computer if job is done" option is selected as shown below, it will shut down the system after job is completed.



Click on finish will schedule the job and below message will come on the screen:

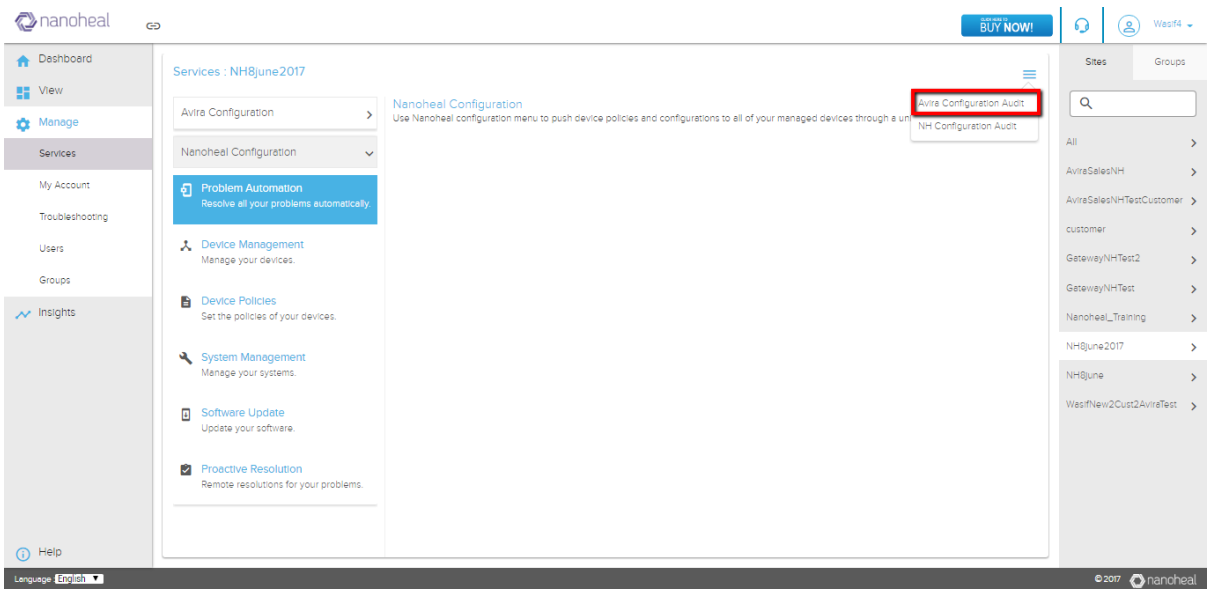


Now going to Avira UI and clicking on scheduler will show the scheduled task for that machine as below:



Avira Configuration Audit

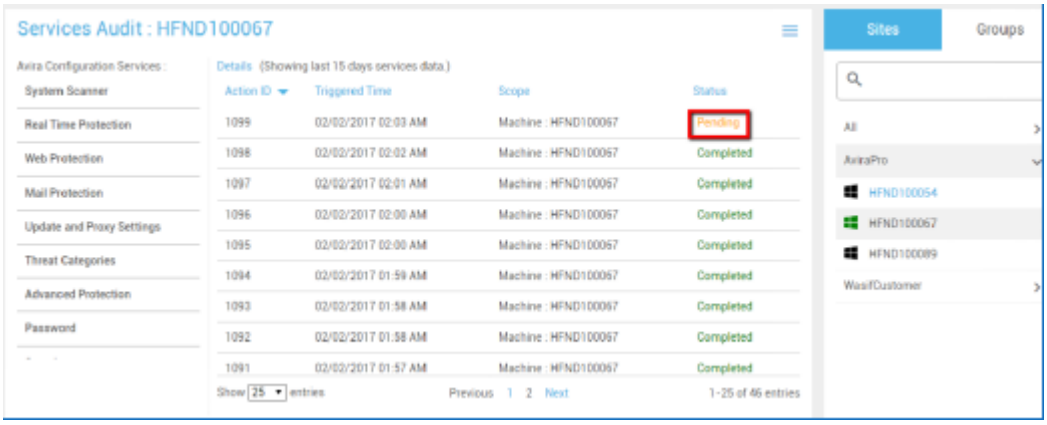
Audit: A user can find out the status of a configuration push by clicking on the Menu drop-down at the top right corner and navigate to "**Audit**", as shown below:



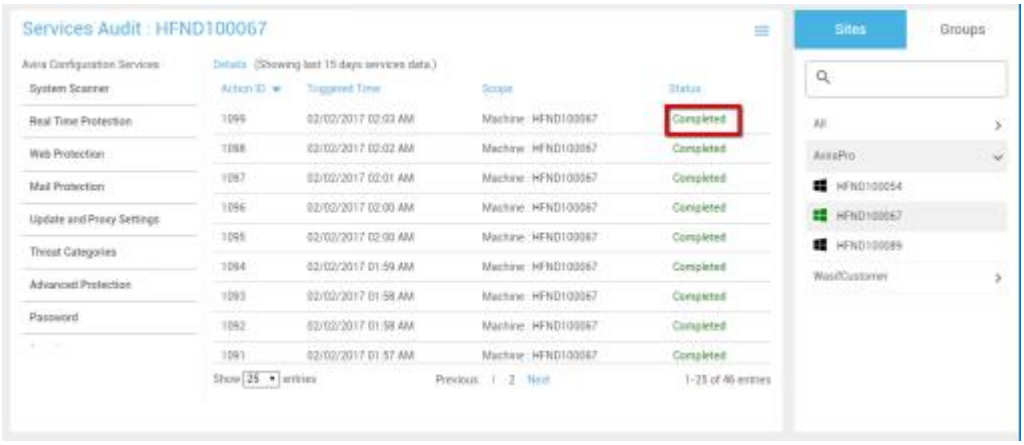
Once a triggered configuration is successfully executed on the machine, its status is updated as "Completed". If the triggered configuration has not reached the machine either because it is offline or because of another configuration push under execution, the second push would be in "Pending" state. If the push has failed to execute, the push status is updated as "Failed".

For example, once a configuration is pushed. As shown below:

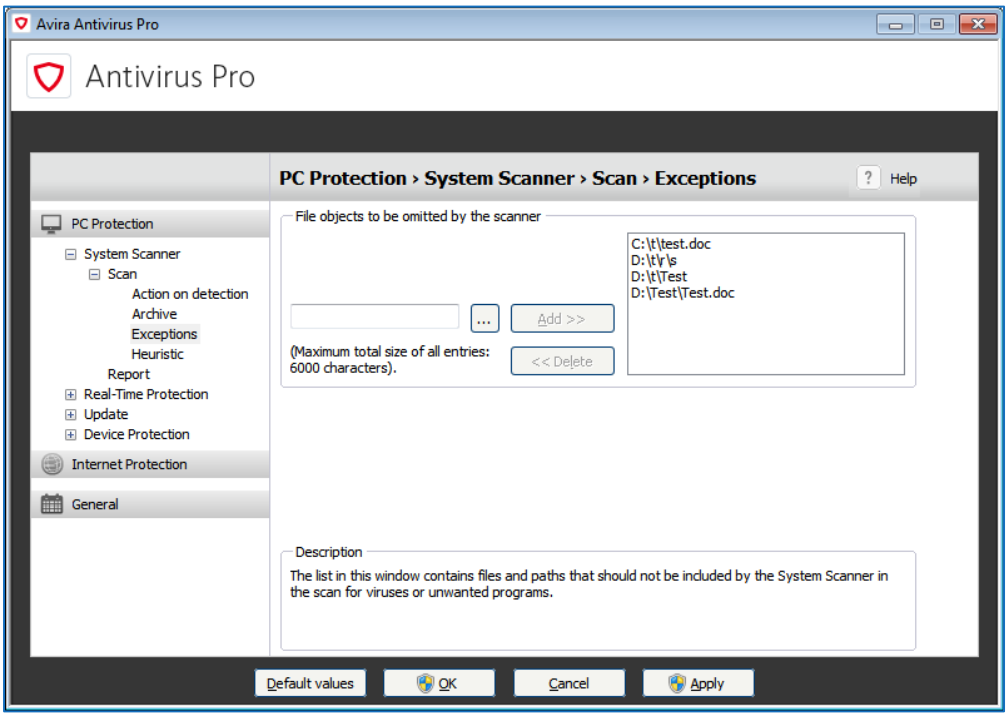
The Services Audit screen shows the status as "Pending" if the configuration has not reached the machine yet.



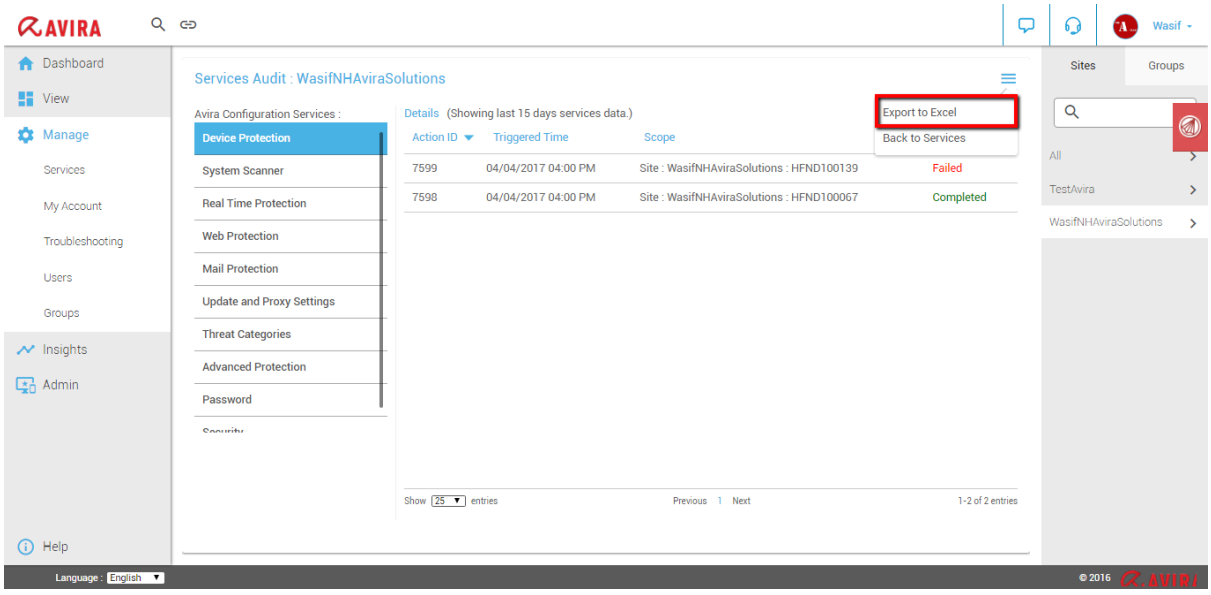
Once the configuration reaches the machine, the status is updated as “Completed”



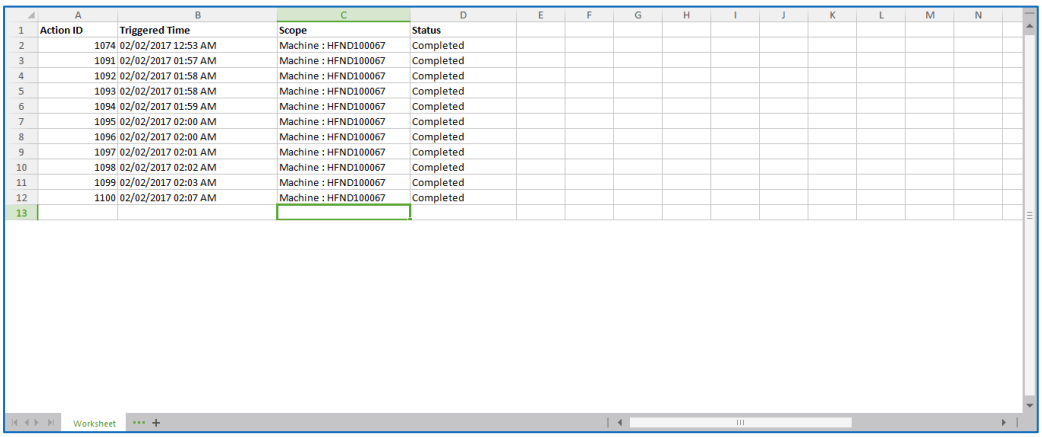
When the status is updated as “Completed”, it means the configuration has reached the machine.



The user can choose to export the audit data by navigating to the Menu at the top-right corner and selecting the option, "Export to Excel":

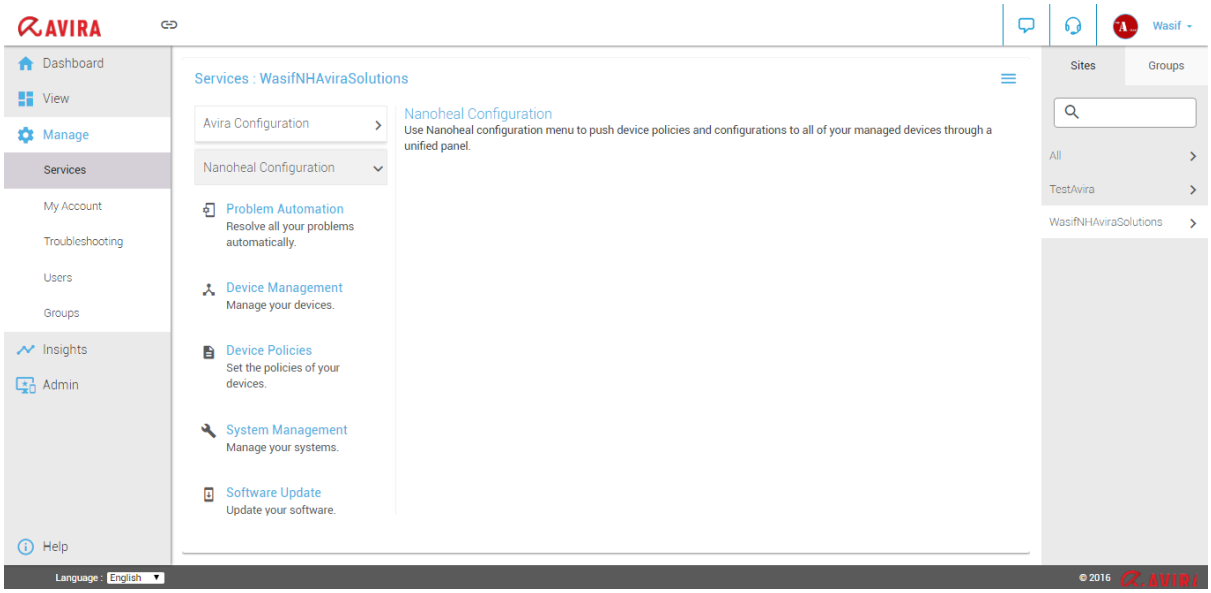


The exported data appears in a format similar to the one below:



Action ID	Triggered Time	Scope	Status
1074	02/02/2017 12:53 AM	Machine : HFND100067	Completed
1091	02/02/2017 01:57 AM	Machine : HFND100067	Completed
1092	02/02/2017 01:58 AM	Machine : HFND100067	Completed
1093	02/02/2017 01:58 AM	Machine : HFND100067	Completed
1094	02/02/2017 01:59 AM	Machine : HFND100067	Completed
1095	02/02/2017 02:00 AM	Machine : HFND100067	Completed
1096	02/02/2017 02:00 AM	Machine : HFND100067	Completed
1097	02/02/2017 02:01 AM	Machine : HFND100067	Completed
1098	02/02/2017 02:02 AM	Machine : HFND100067	Completed
1099	02/02/2017 02:03 AM	Machine : HFND100067	Completed
1100	02/02/2017 02:07 AM	Machine : HFND100067	Completed

Nanoheal Configurations

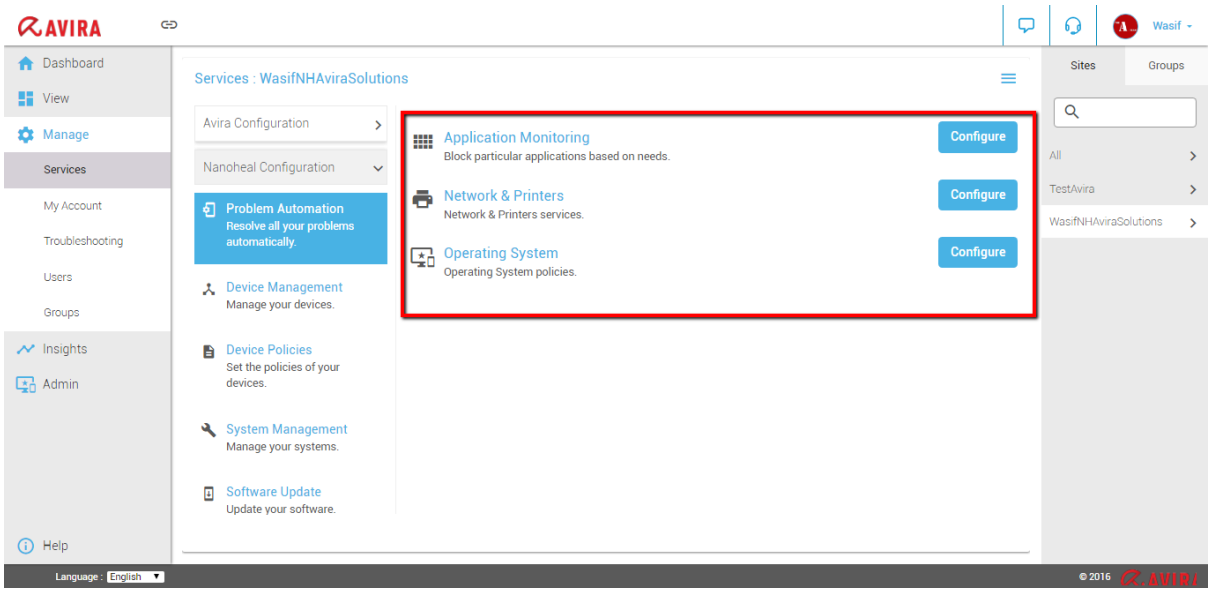


Nanoheal Services is divided into 6 sections.

1. Problem Automation
2. Device Management
3. Device Policies
4. System Management
5. Software Update
6. Proactive Resolution

Problem Automation

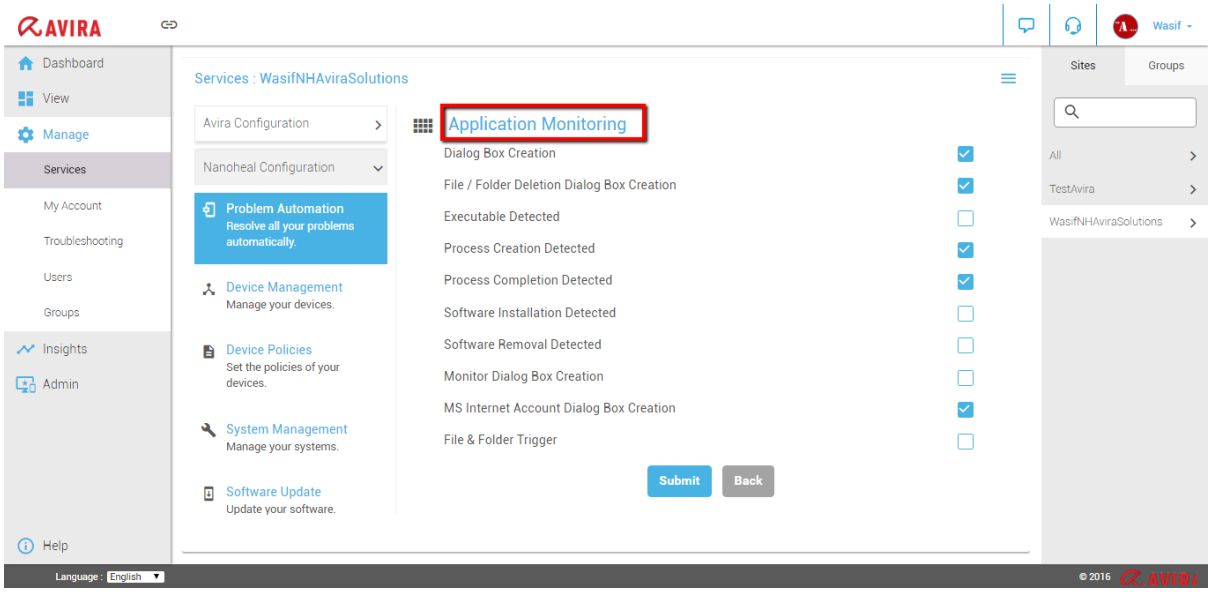
Problem Automation section has sub sections namely - Application Monitoring, Network Printers, and Operating System as shown in screenshot below.



In each sub section, the user can configure policies by clicking on Configure button.

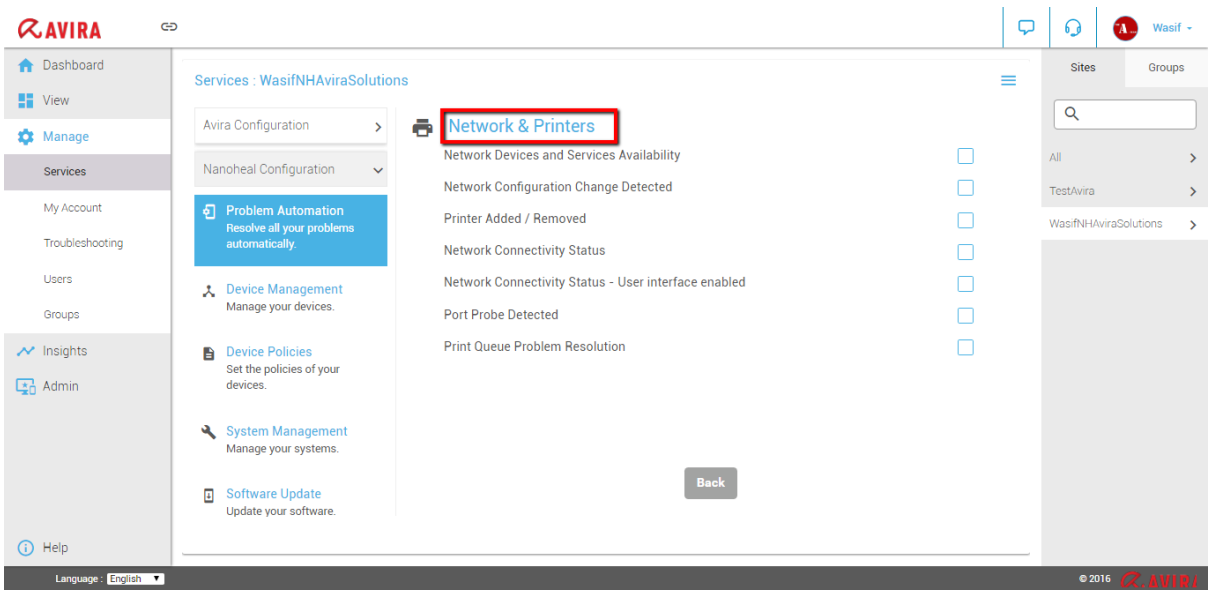
Application Monitoring

In the Application Monitoring Services, the user can configure following Policies as shown in the screenshot below.



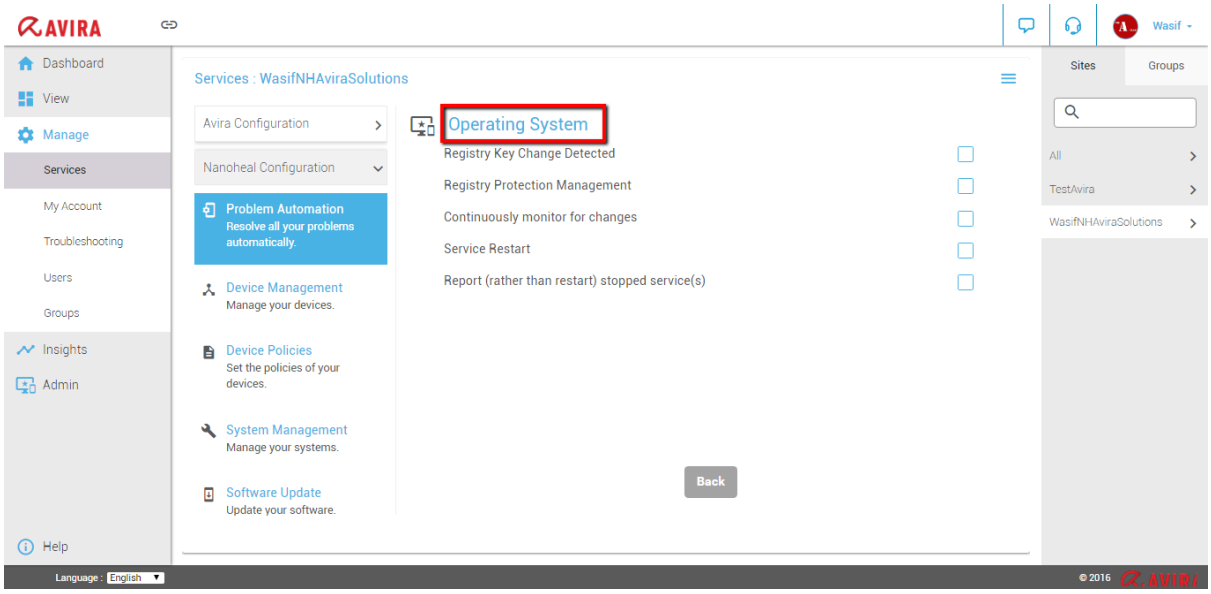
Network & Printers

In Network & Printers Services, the user can configure following Policies as shown in the screenshot below.



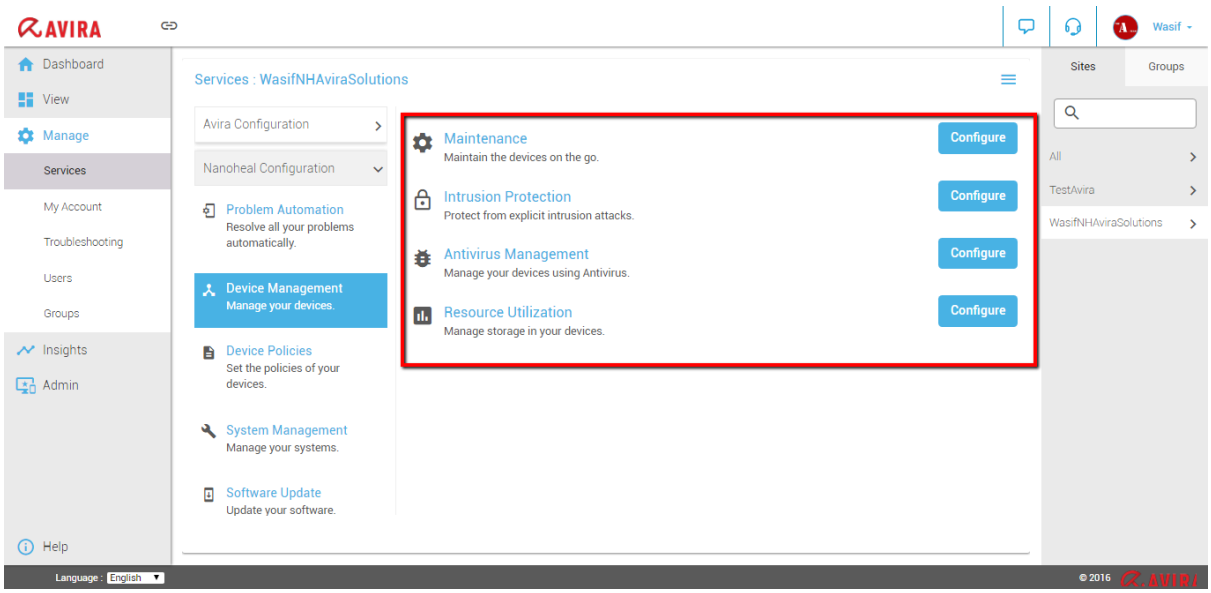
Operating System

In Operating System Services, the user can configure following Policies as shown in the screenshot below.



Device Management

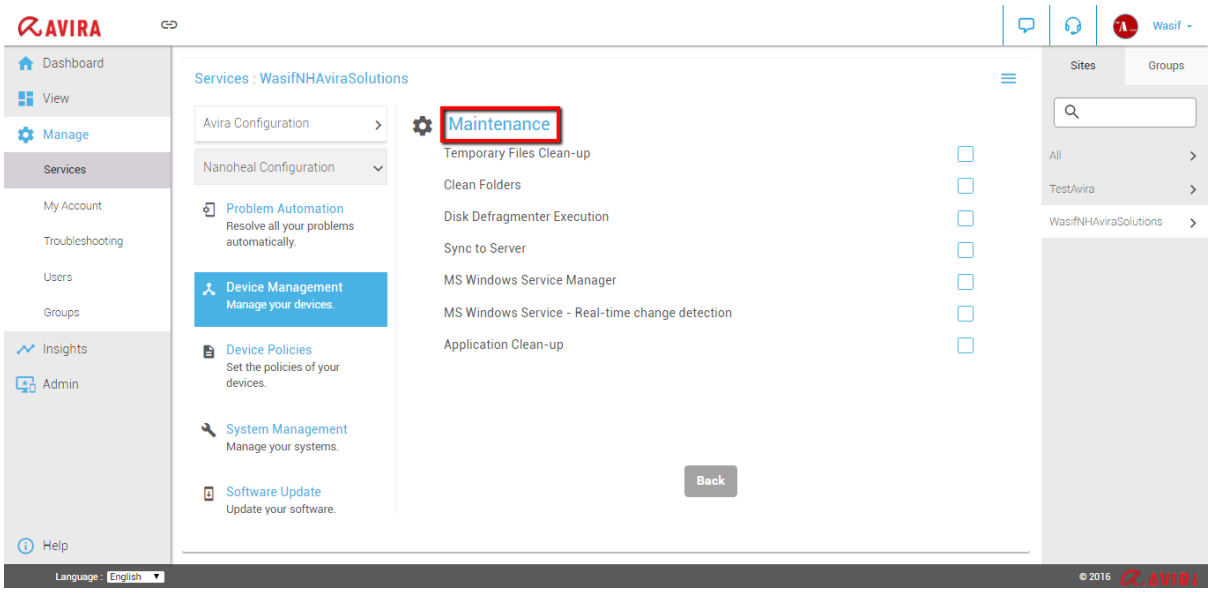
Device Management section in turn has sub sections namely - Maintenance, Intrusion Protection, Anti-virus Management, and Resource Utilization as shown in the screenshot below.



In each sub section, the user can configure policies by clicking on Configure.

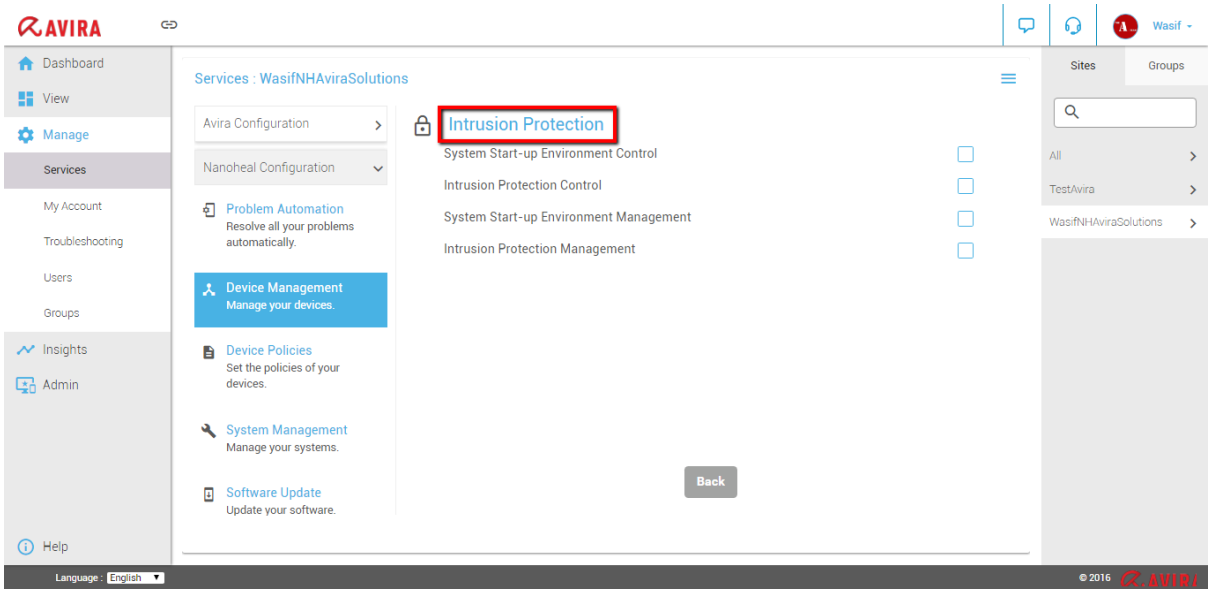
Maintenance

In Maintenance Services, the user can configure following Policies as shown in the screenshot below.



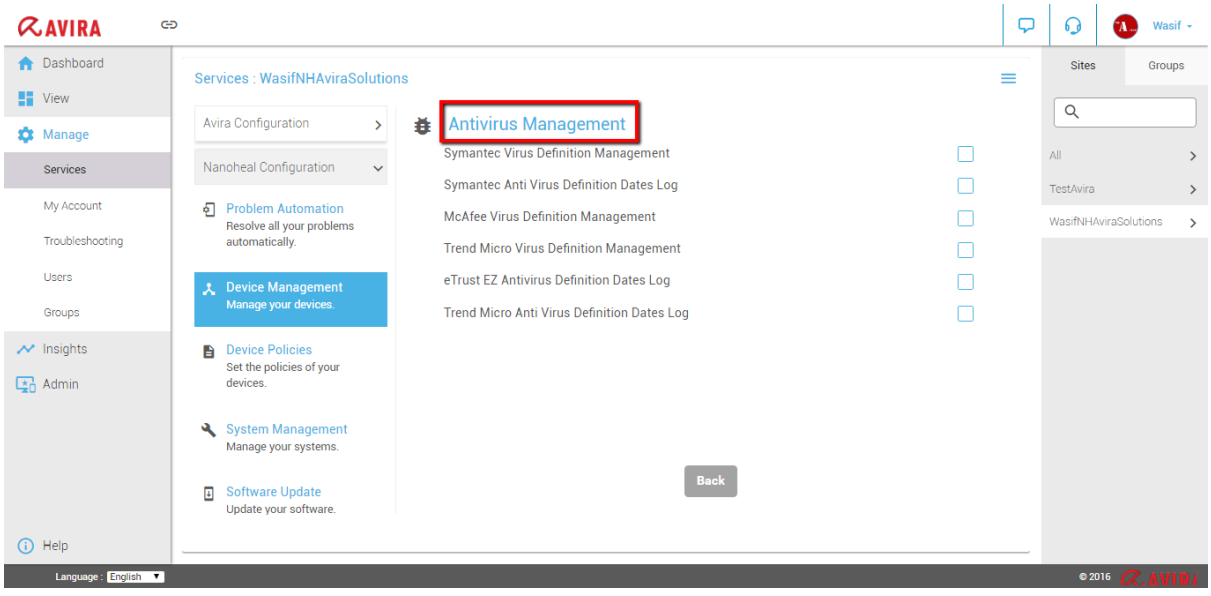
Intrusion Protection

In Intrusion Protection Services, the user can configure following Policies as shown in the screenshot below.



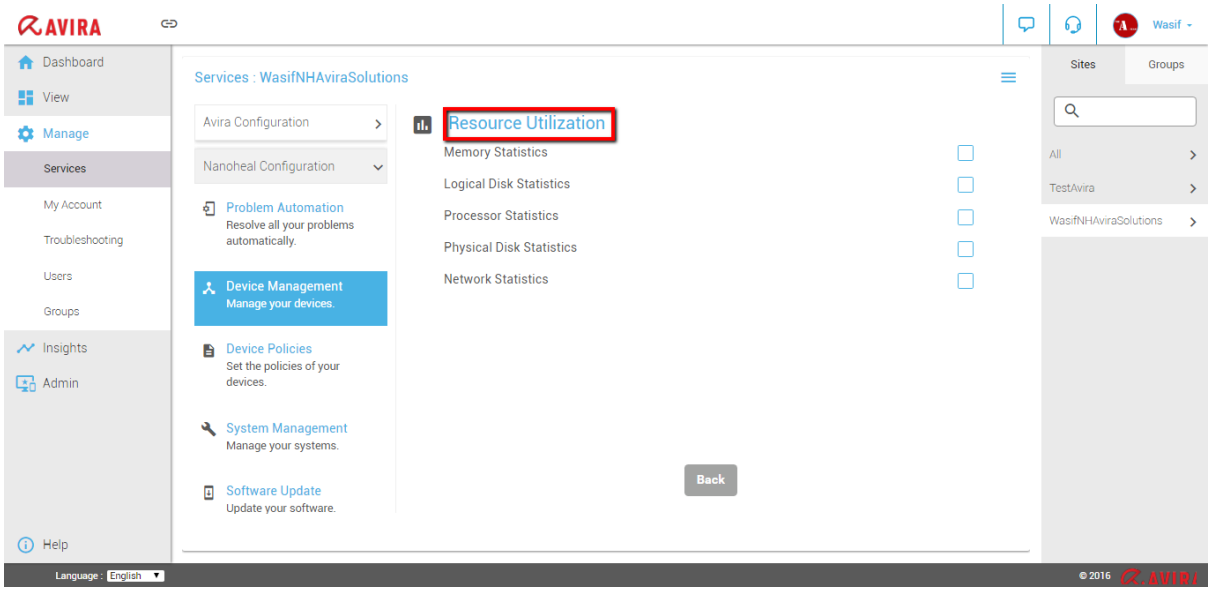
Antivirus Management

In Antivirus Management Services, the user can configure following Policies as shown in the screenshot below



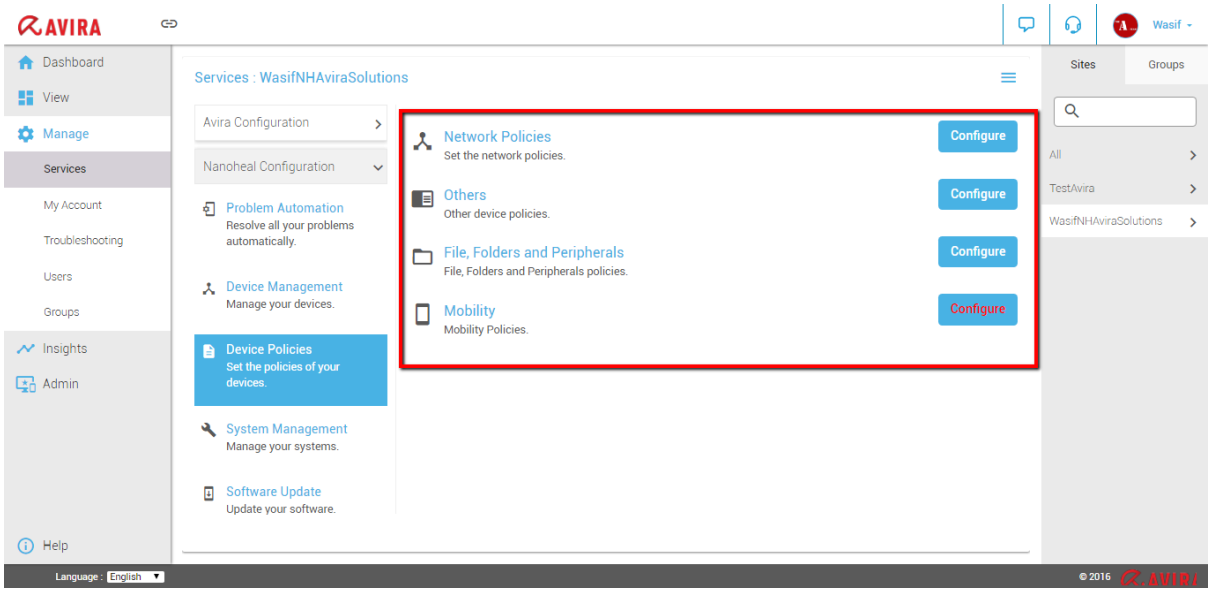
Resource Utilization

In Resource Utilization Services, the user can configure following Policies as shown in the screenshot below



Device Policies

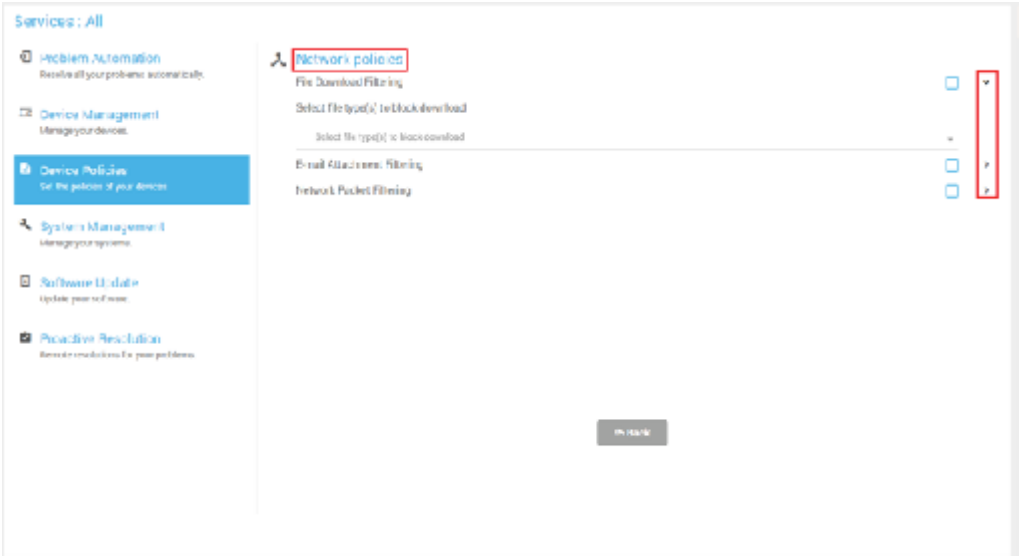
Device Policies section in turn has Sub Sections Namely Network Policies, Mobility, Files, Folders & Peripherals and Others as shown in the screenshot below.



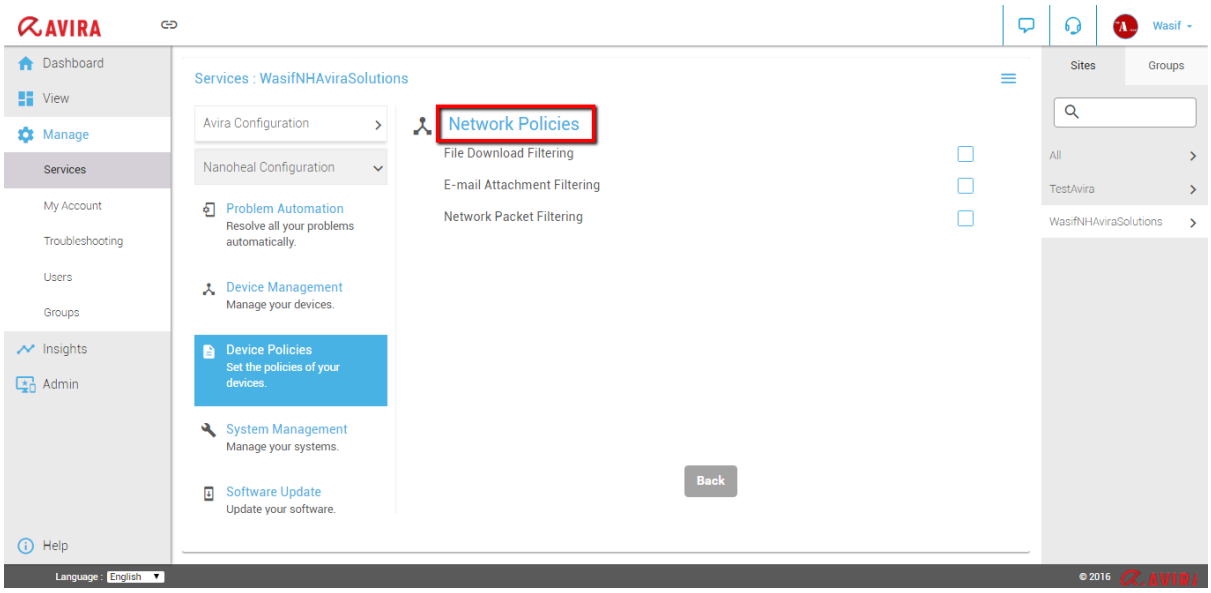
In each sub section, user can configure the policies by clicking on Configure button.

Network Policies

In Network Policies Services, user can configure following Policies as shown in the screenshot below.

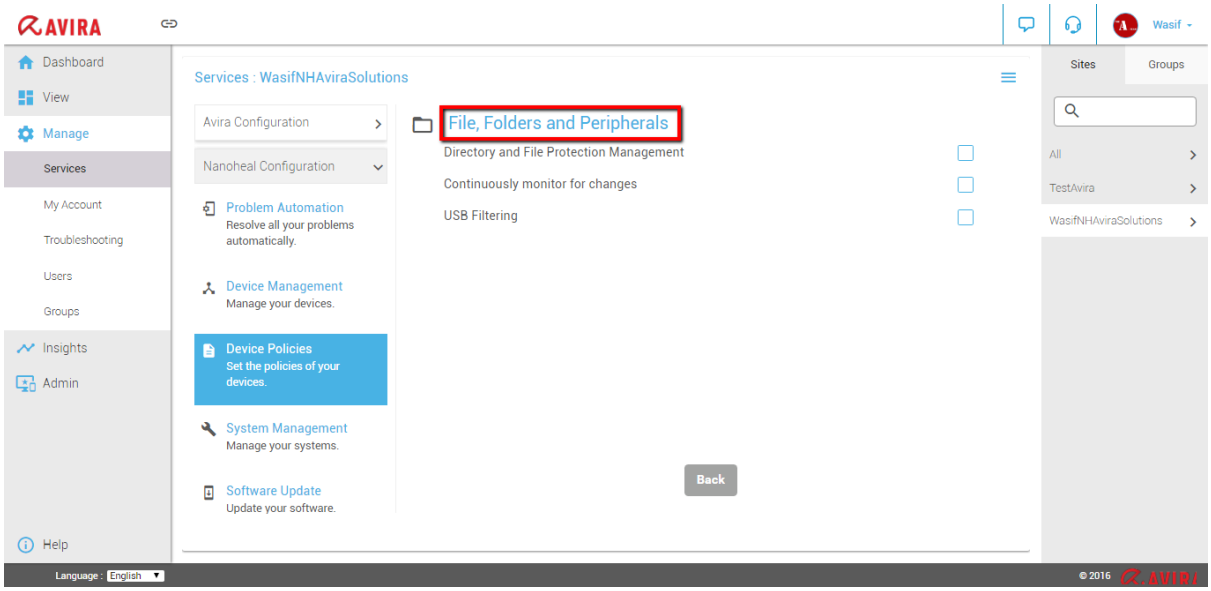


Note: Only the Nanoheal Admin will be able to the Advance configuration option. Users other than admin won't see the Advance Configuration option as shown in the screenshot below.



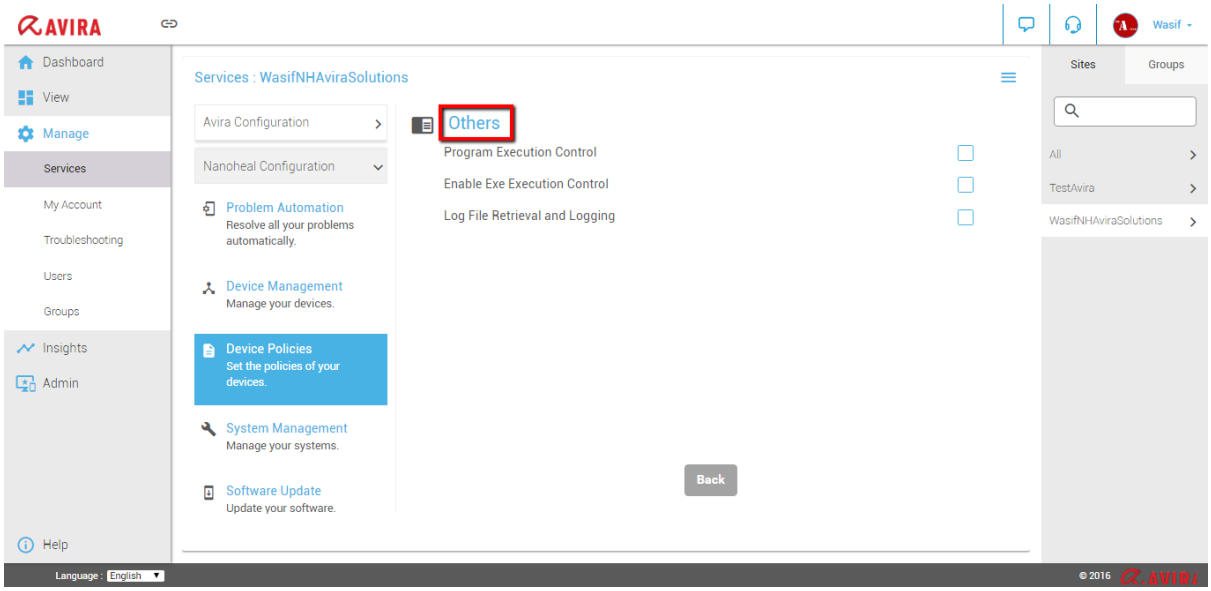
Files, Folders & Peripherals

In the Files, Folders & Peripherals Services, the user can configure following Policies as shown in the screenshot below.



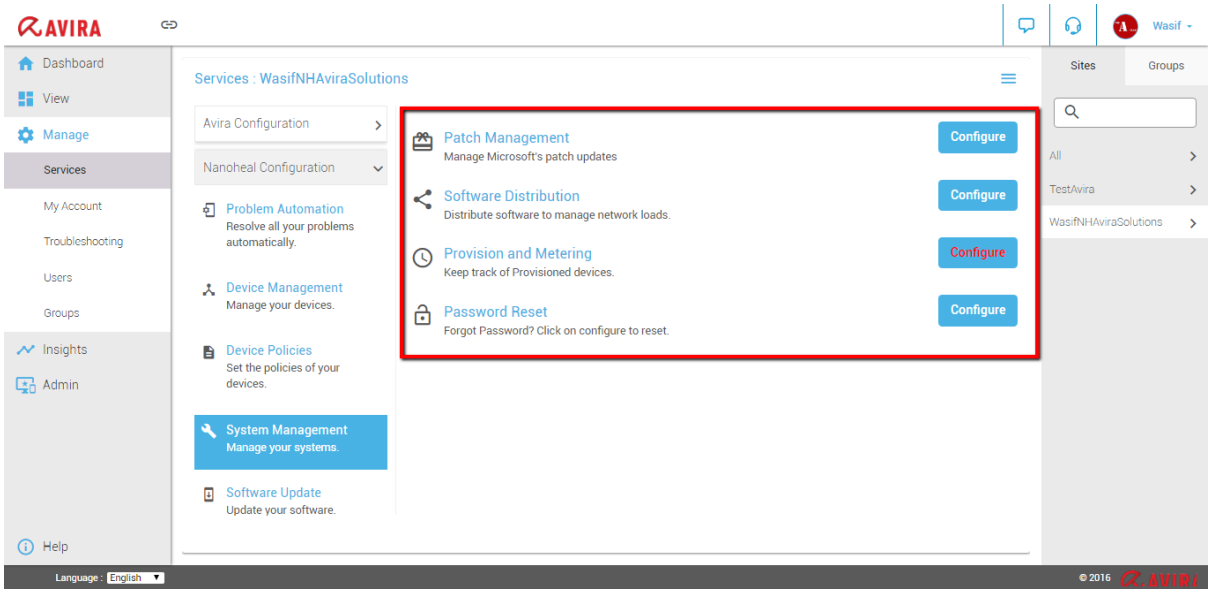
Others

In the Others Services, the user can configure following Policies as shown in the screenshot below.



System Management

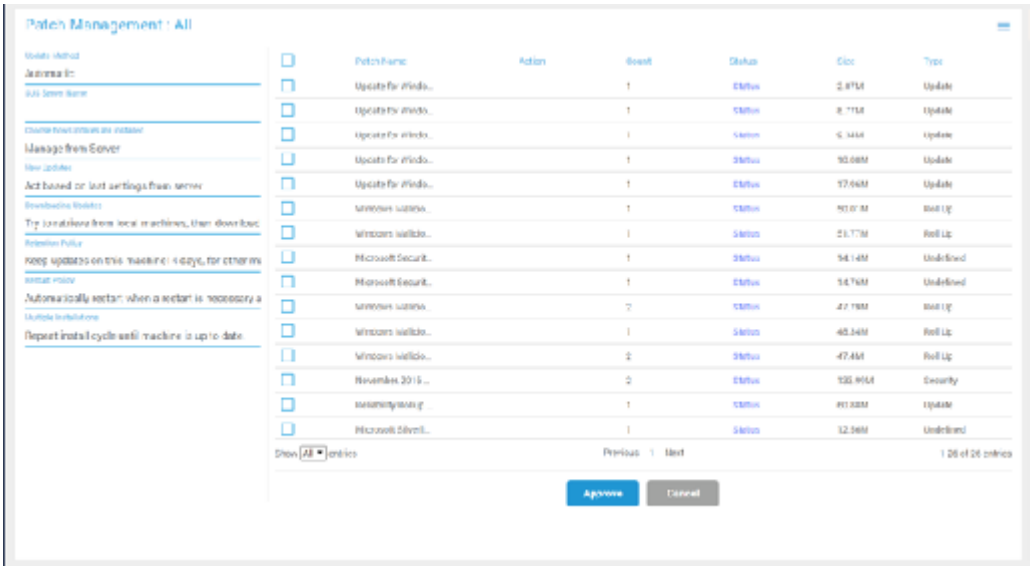
System Management section has sub sections. Namely - Patch Management, Software Distribution, Provisioning & Metering and Password Reset as shown here.



In each sub section, the user can configure the policies by clicking on the "Configure" button.

Patch Management

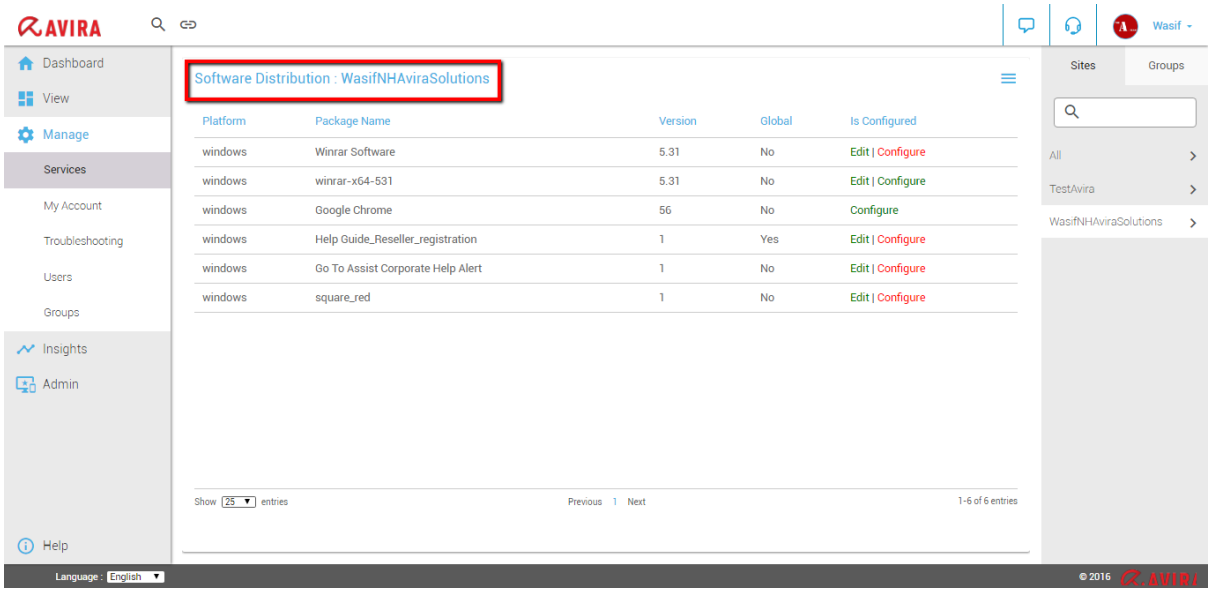
In the Patch Management section, the user can Manage Microsoft's patch updates. Upon clicking the Configure Button, the Patch Management screen will be displayed as shown here.



Patch Management will be explained in detail in further sections. Click here to know more.

Software Distribution

In the Software Distribution section, the user can distribute software to manage network loads. Upon clicking the Configure Button – the Software Distribution screen will be displayed as shown below.



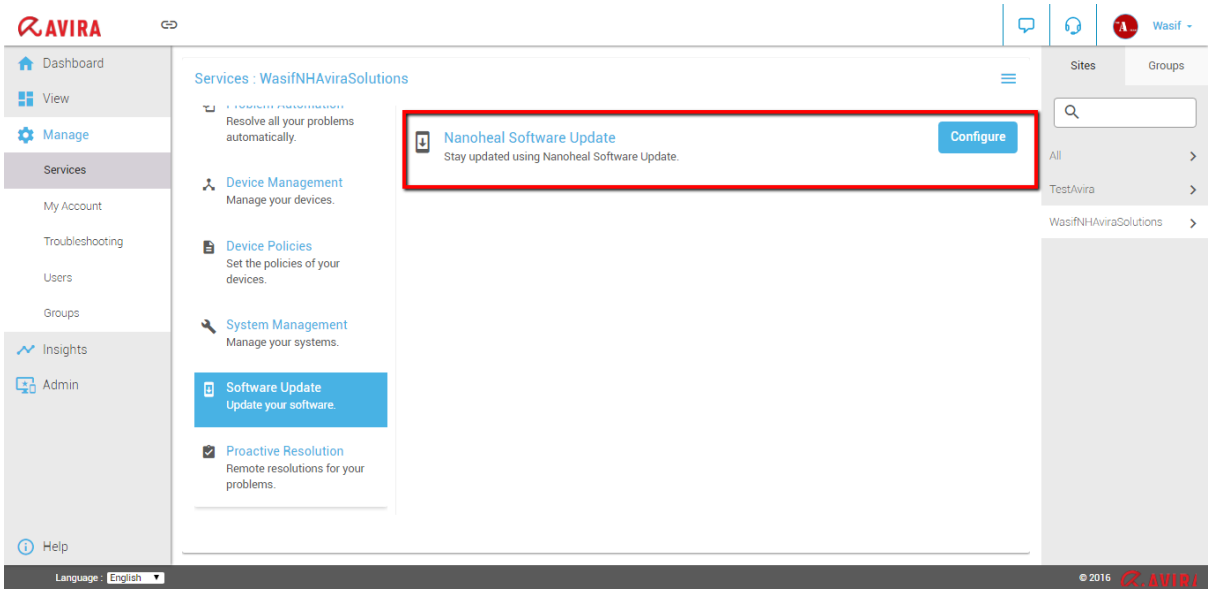
Click Here to know more information about Software Distribution.

Provisioning & Metering

In the Provisioning & Metering section the user can Keep track of the Provisioned devices, upon clicking the Configure Button, the Provisioning & Metering screen will be displayed.

Software Update

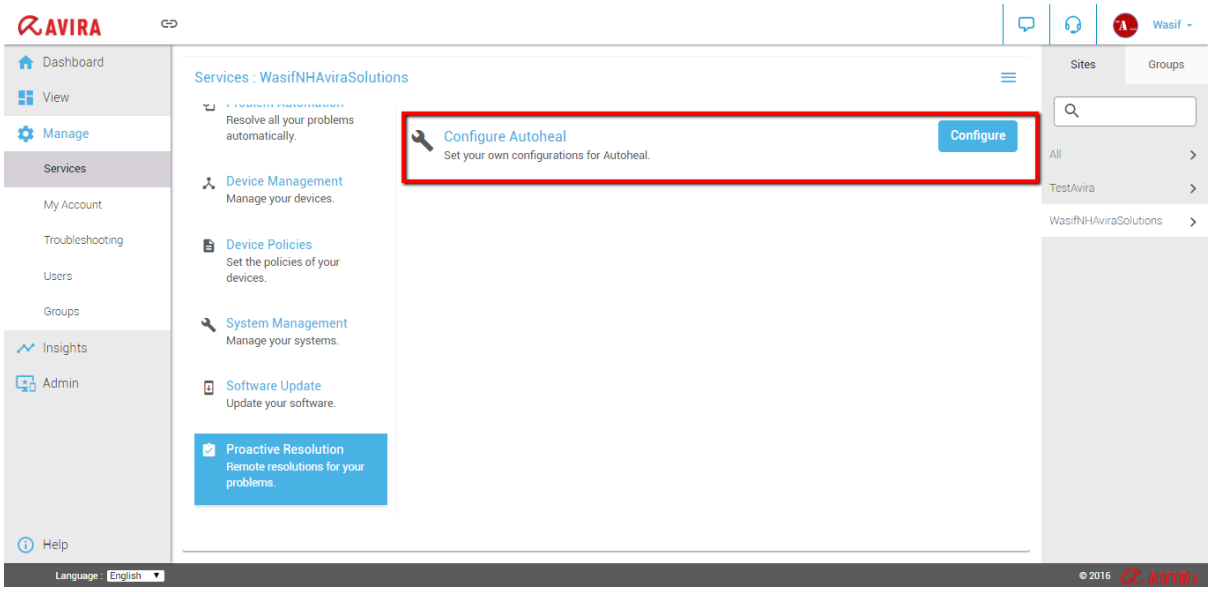
Software Update section in has sub sections. Namely - Nanoheal Software Update as shown here.



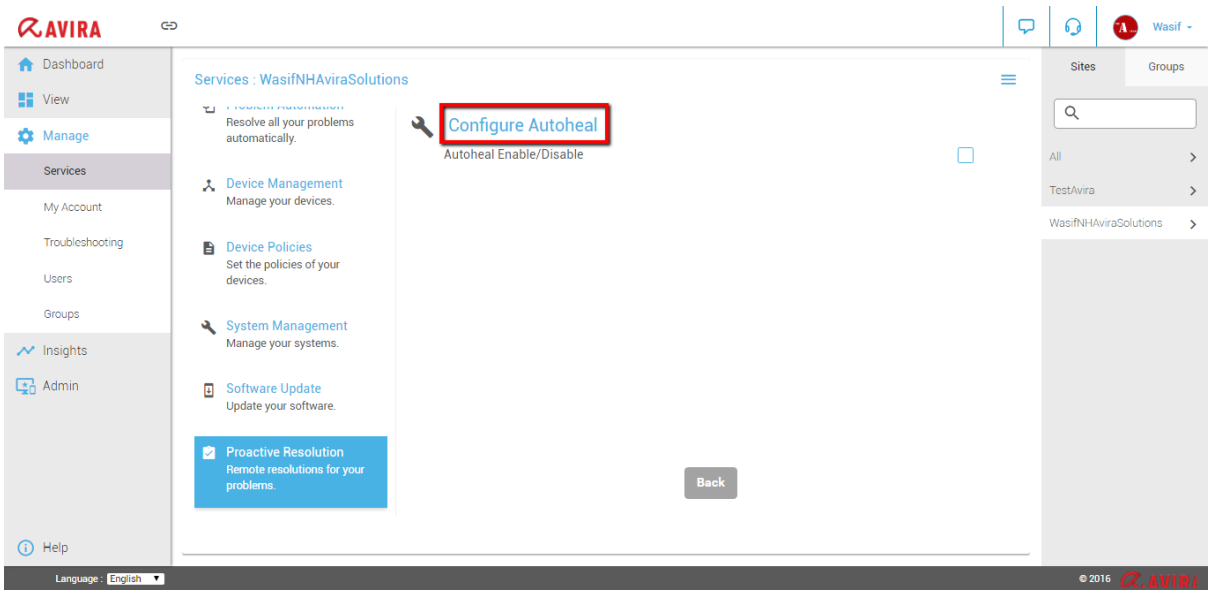
Click of the Configure button will open up the Software Update Screen. Click Here to know more about Software Update.

Proactive Resolution

The Software Update section has sub sections. Namely - Configure Autoheal as shown here:

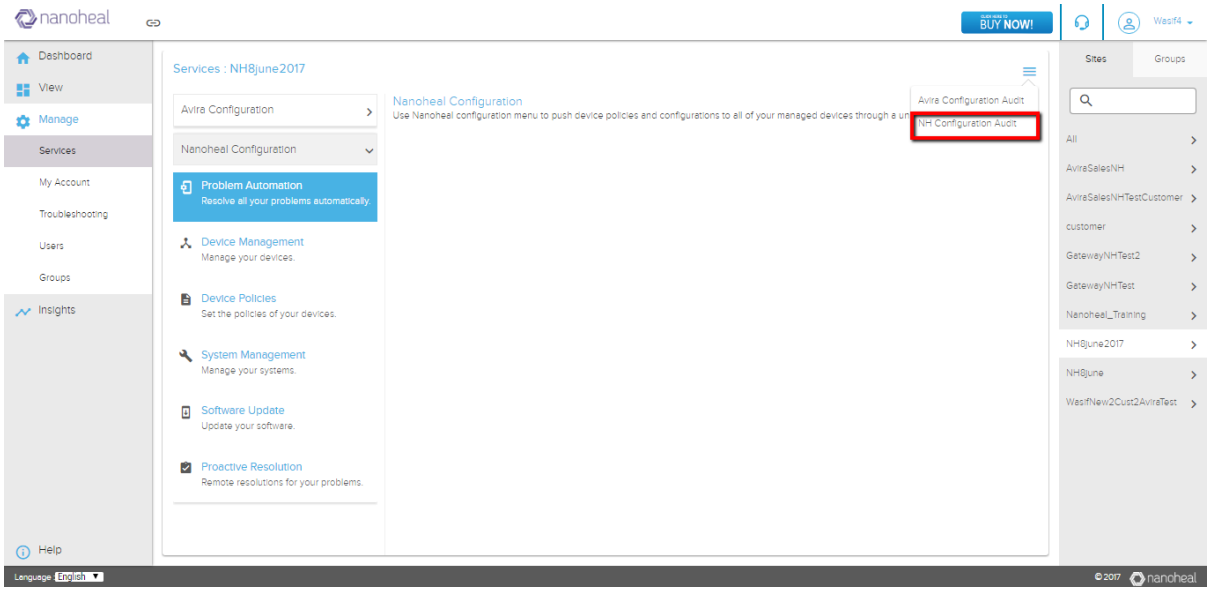


Clicking on the Configure button will display a pop up window to configure Autoheal as shown here.

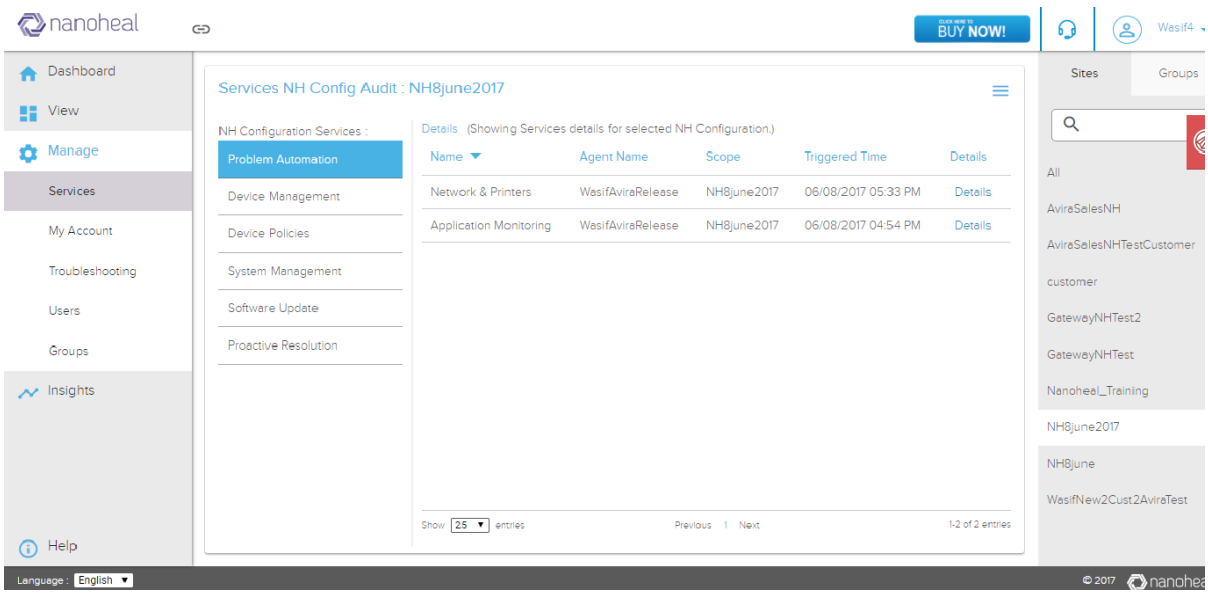


NH Configuration Audit

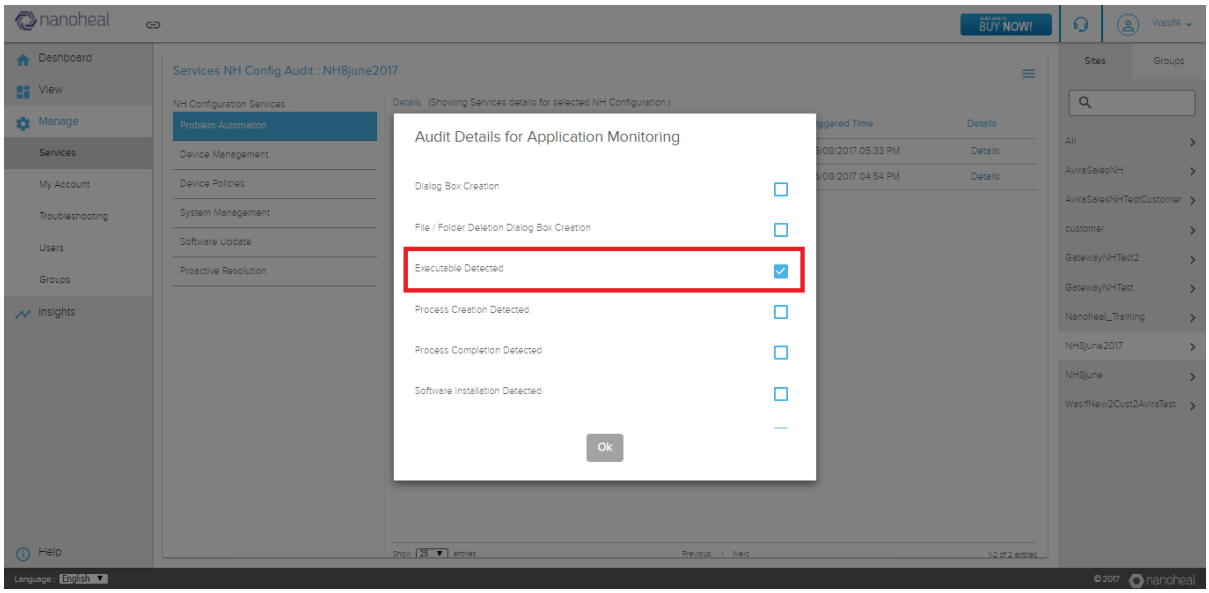
The user can see the audit data by navigating to the Menu at the top-right corner and selecting the option, "Export to Excel":



Click on Audit will take to the audit page as shown below:



Click on details will show the details of which option have been pushed as shown below:



For ex, in above picture Executable detected option has been pushed from Application Monitoring segment.

Troubleshooting

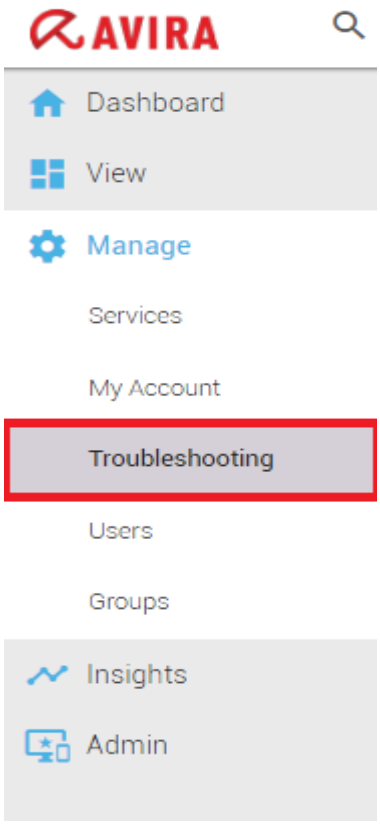
The troubleshooting module helps in analyzing and solving the issues:

1. Troubleshooting aids in resolving the issues on an end device by helping the dashboard user select the fix that is the best match to the issue at hand and by 'pushing' the selected fix/resolutions to the end device or devices.

2. The resolutions pushed are logged on to a server that helps keep a track of the number of solutions pushed.
3. The resolution logs also help the Agent analyze the top call drivers.

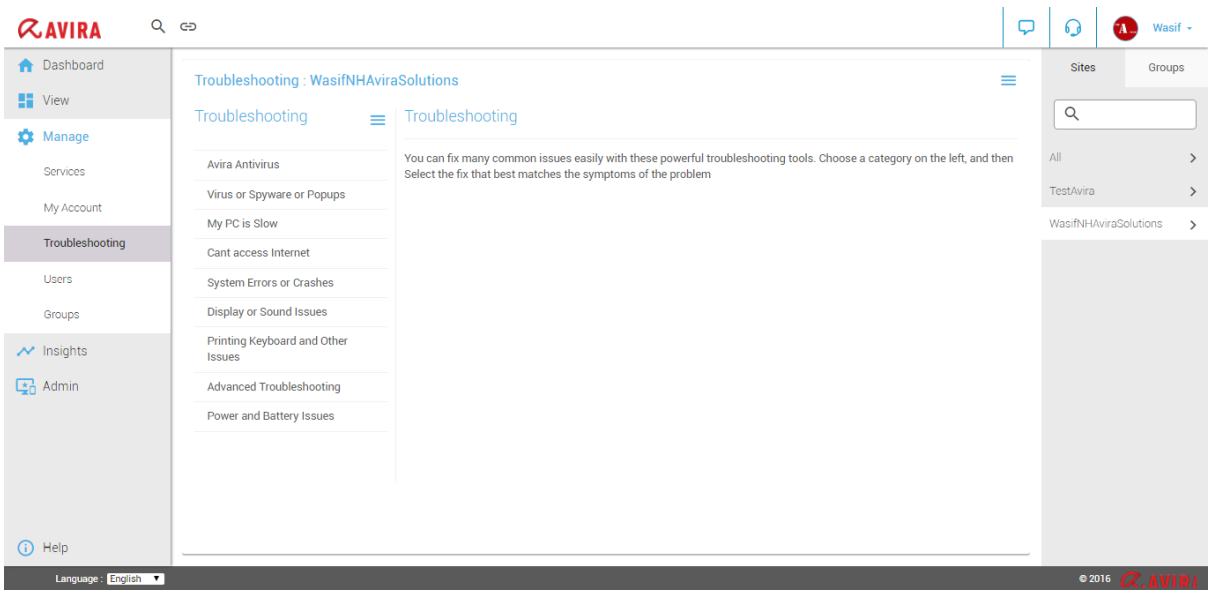
The Dashboard provides information about the online/offline statuses of the devices that report to a particular server. An agent can push resolutions based on the availability of the device.

A user can navigate to 'Troubleshooting' via 'Manage'. As shown below:



Click on 'Troubleshooting' to navigate to the troubleshooting page.

As shown below:

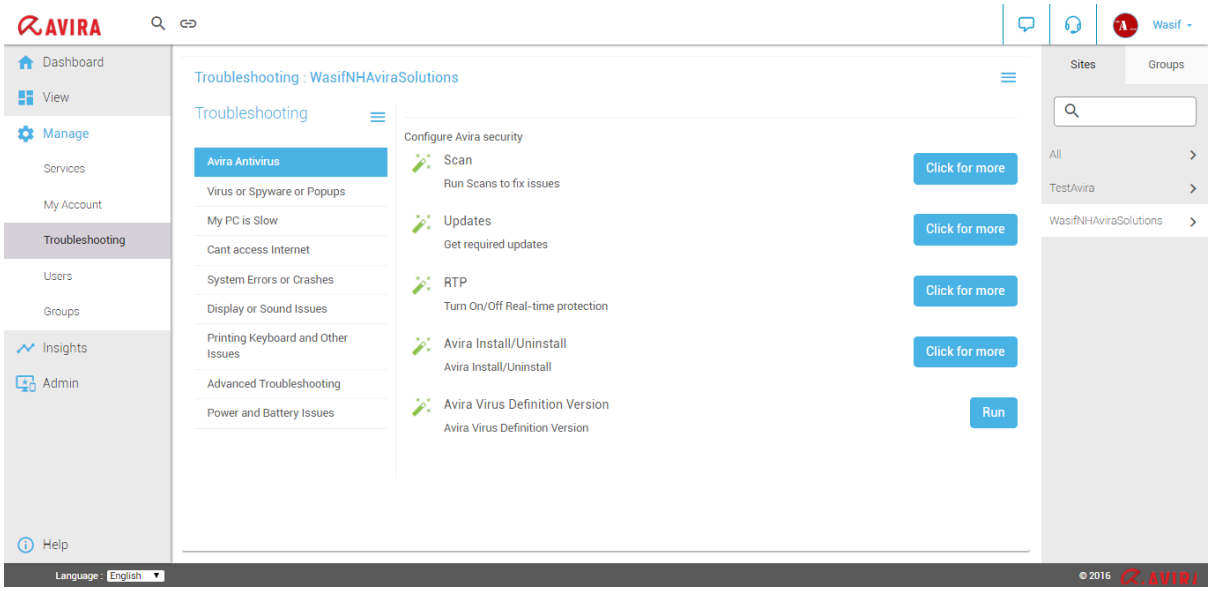


Trouble shooting options are OS specific. On Troubleshooting Page, a user must choose the OS of their choice from the drop down (as shown above). The trouble shooting steps/tools will change automatically based on the type of Machine OS selected (either Windows OS or Mac OS).

By default, troubleshooting will show the fixes that are available for the machines that belong to the first default site (as displayed on Home page) OR for all the machines that the user has selected from the right-hand panel.

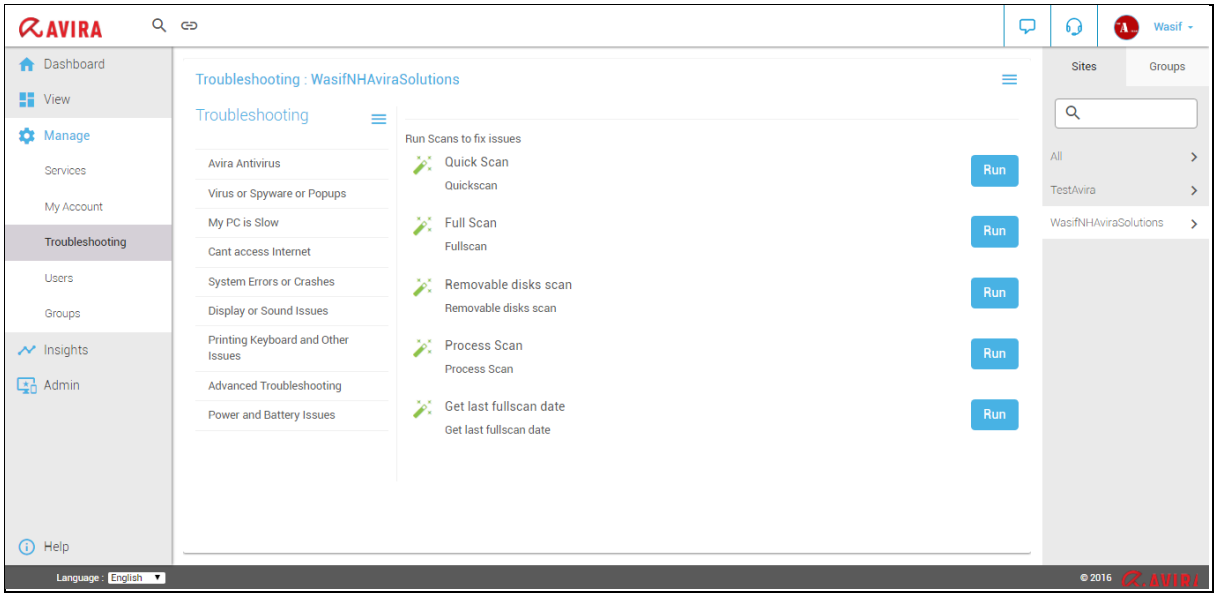
Online and offline machines for a particular site are differentiated using green and grey icons respectively. An icon, green in color indicates that the device is online and grey indicates that the device is offline. Icons next to the machine name (on the right hand side panel) also indicate the device Operating Systems viz. Windows, Android, Mac, etc.

Avira Antivirus Troubleshooting: To access the AV troubleshooting options, click on "AVIRA ANTIVIRUS" form the panel on to the left:

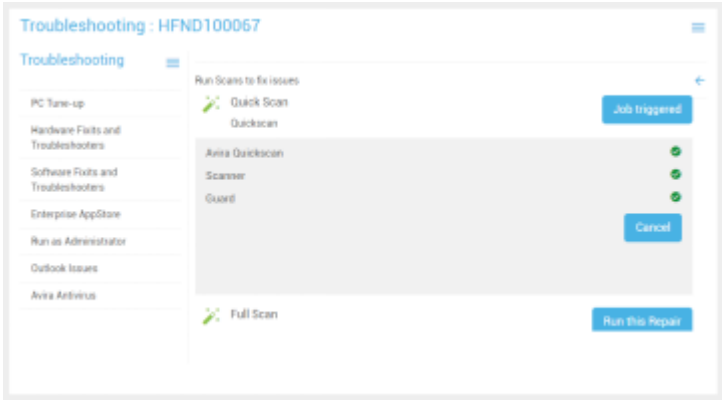


Following options are available for Avira Antivirus troubleshooting:

1. Scan: 'SCAN" provides for a way to scan the device/devices selected. "Click for more" will give you different ways a device could be scanned.

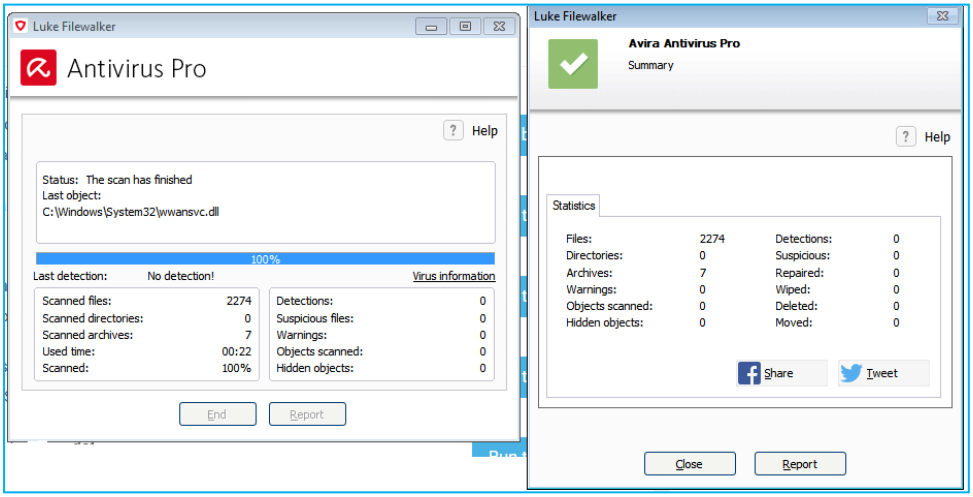


1.1 Quick Scan: Click on the "Run this repair" button next to "Quick Scan" to initiate a quick scan

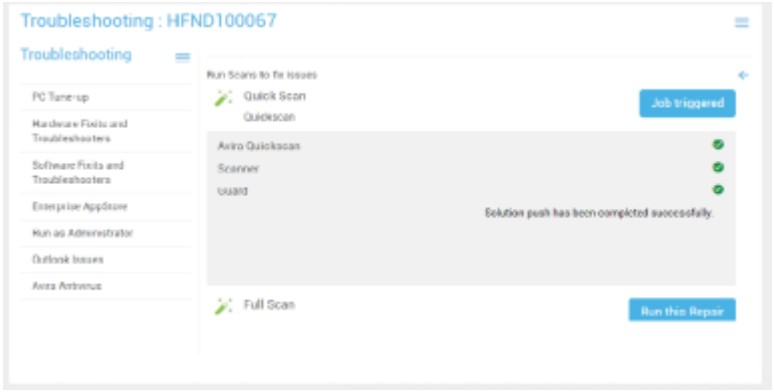


Once the job is triggered, Avira will run on the end device and do a Quick scan:

As shown below:

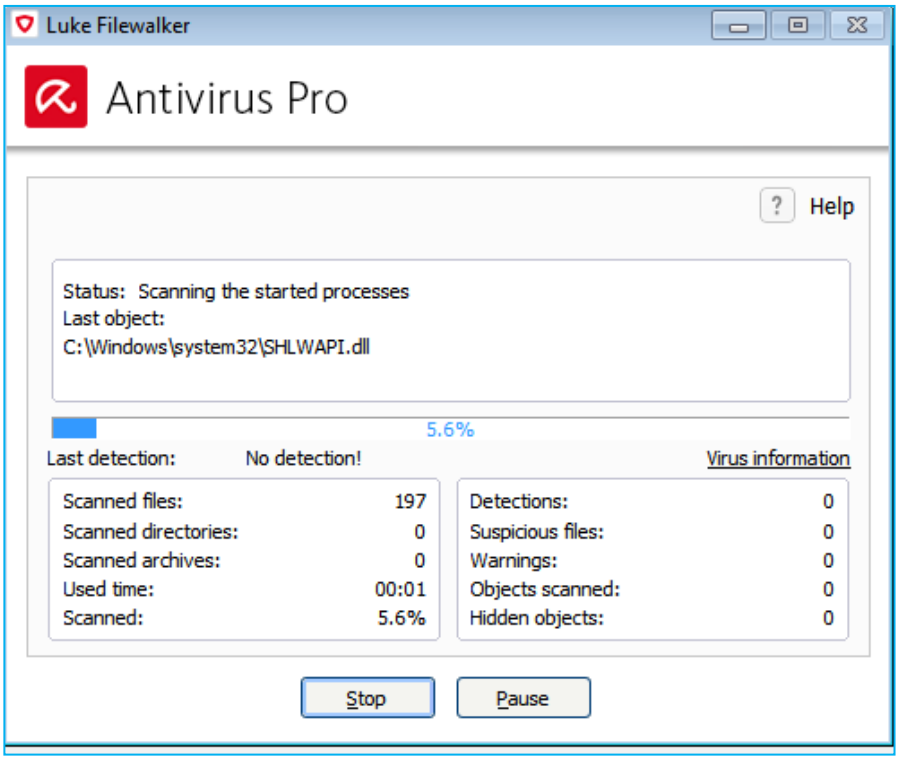


Once the sequence execution is complete, the same is reflected on to the dashboard.

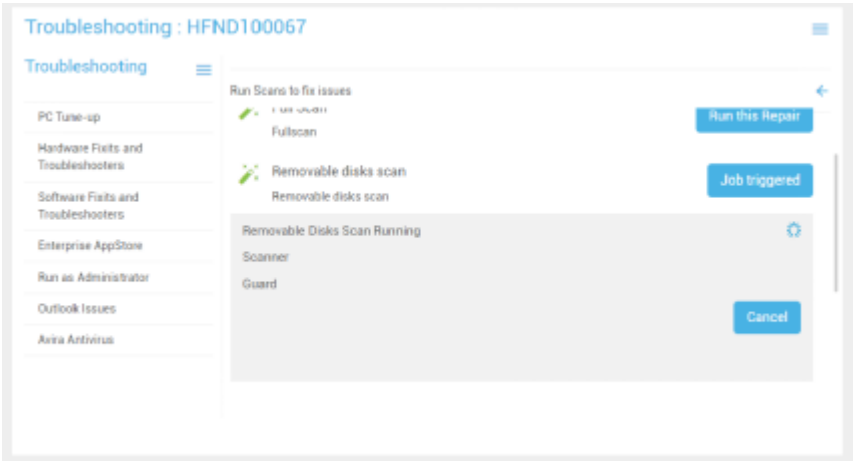


1.2 Full Scan: Click on the "Run this repair" button next to "Full Scan" to initiate a Full scan.

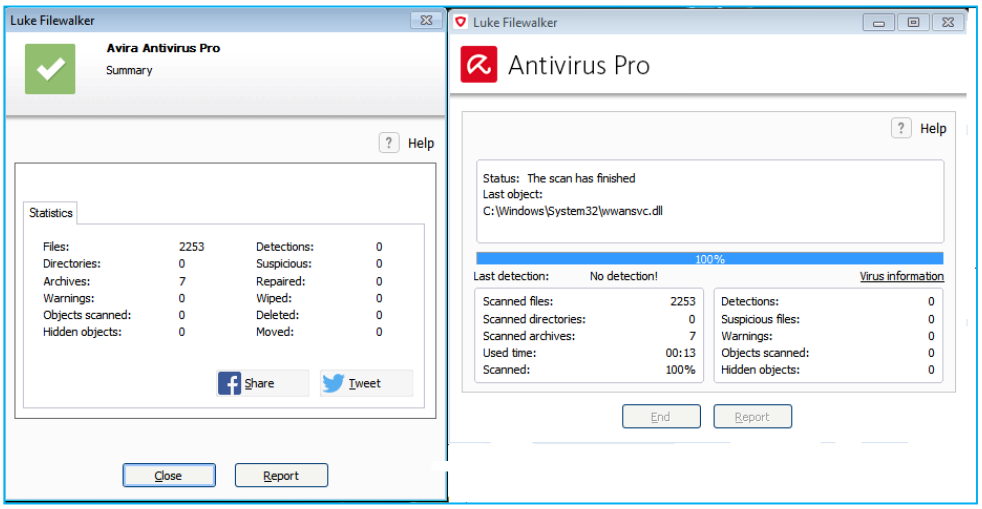
Once the job is triggered, Avira will run on the end device and do a full scan as shown below:



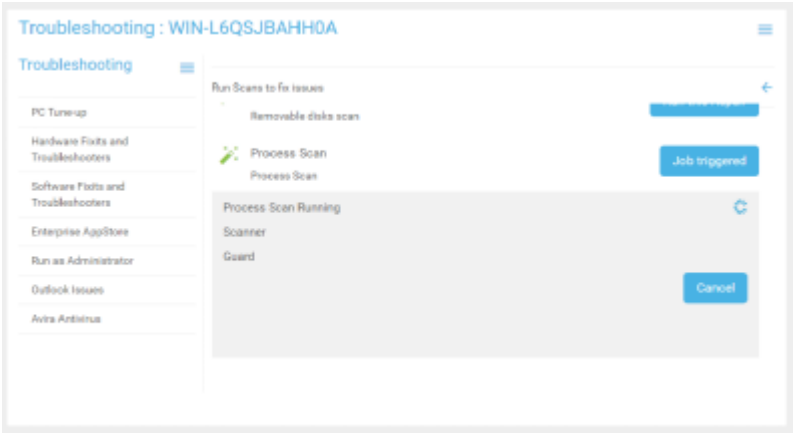
1.3 Removable Disk Scan: Click on the "Run this repair" button next to "Removable Disk scan" to initiate a scan on the removable media.



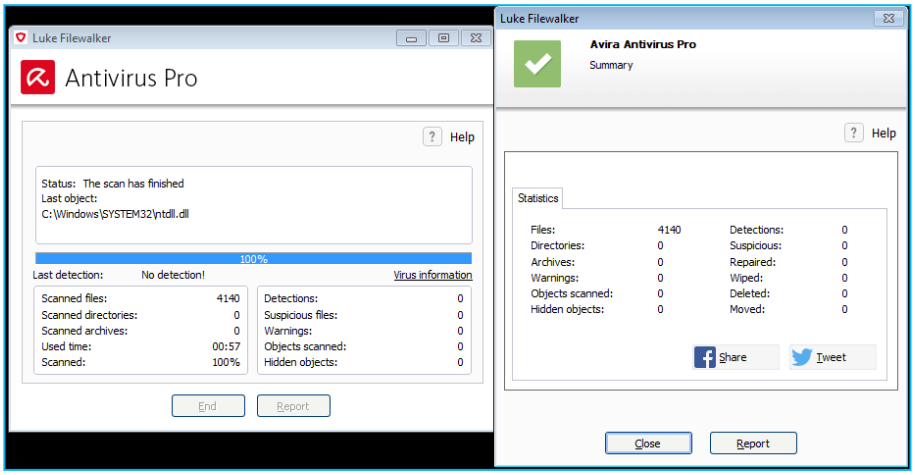
Once the job is triggered, Avira will run and run a removable disk scan:



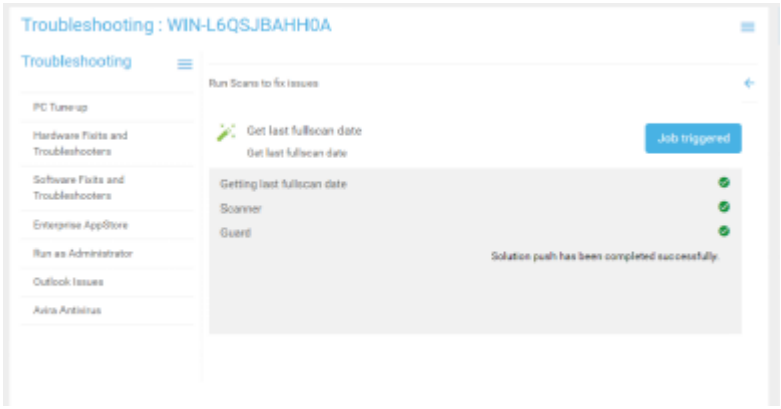
1.4 Process Scan: Clicking on "run this repair" will initiate process scan.



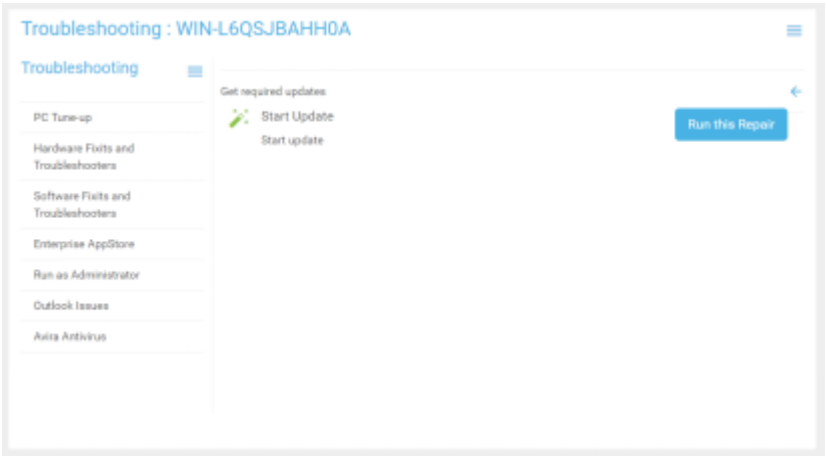
Once the job is triggered, Avira will run and run the scan as shown below:



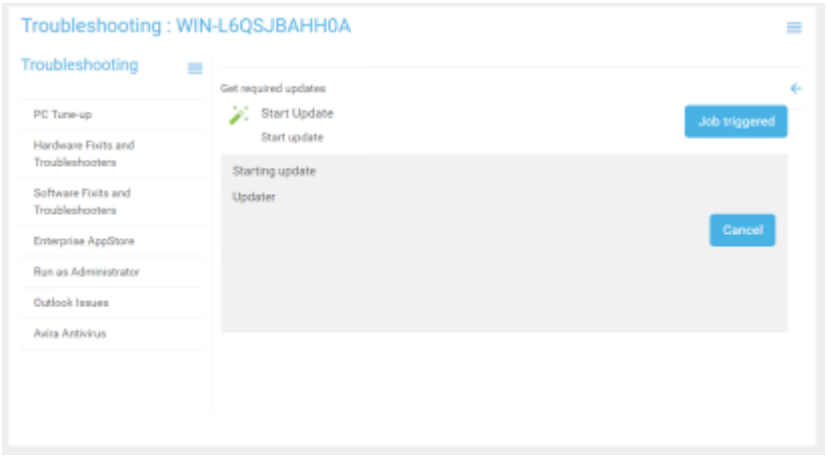
1.5 Get Last Full Scan Date: This tile when executed will give you the dates on which a full scan was triggered previously.

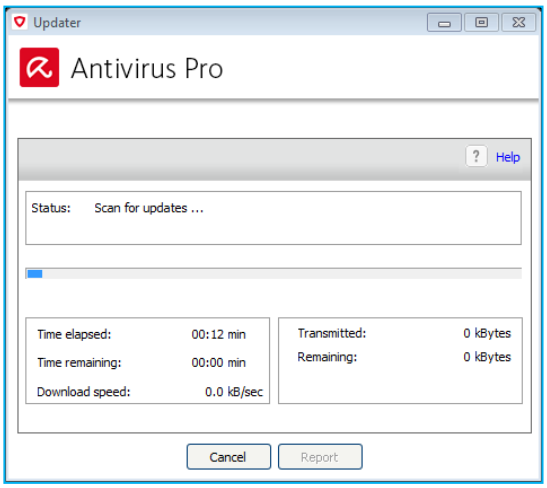


2. Updates: Updates section will allow the user to trigger Avira update on the end devices

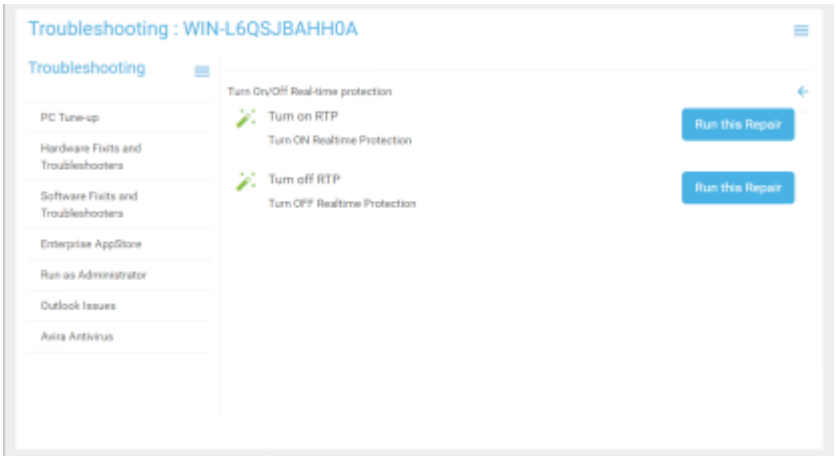


Click on "Run this repair" to start updating Avira.





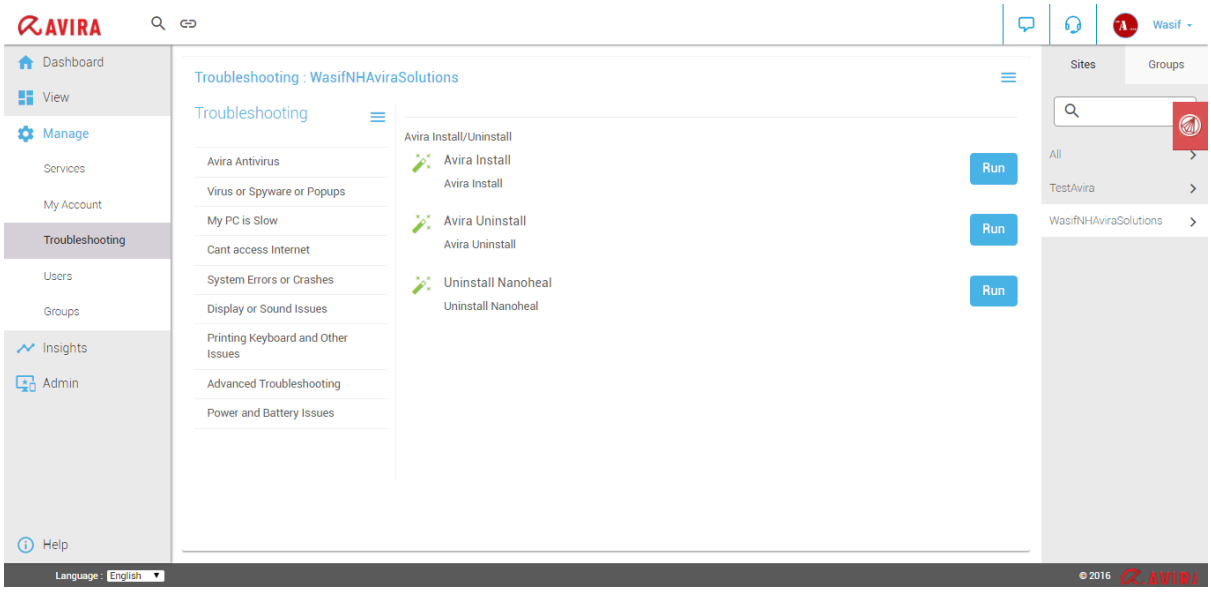
3. RTP: This tile will help in enabling/disabling the RTP.



Turn on RTP: Click on "run this repair" to turn on RTP on the machine.

Turn Off RTP: Click on "run this repair" to turn off RTP on the machine

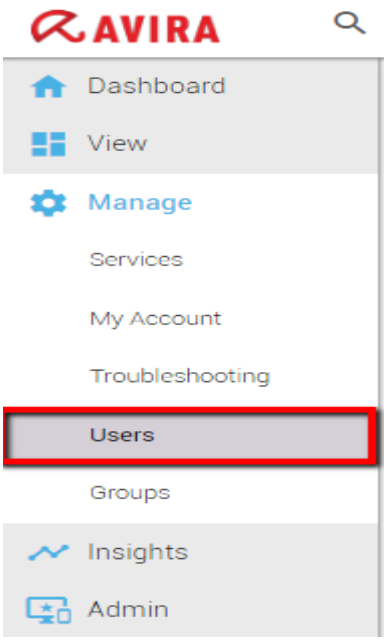
4. Avira Uninstall/Reinstall: This section gives the user an option to install/ uninstall Avira, uninstall nanoheal from the connected devices. An example is shown below



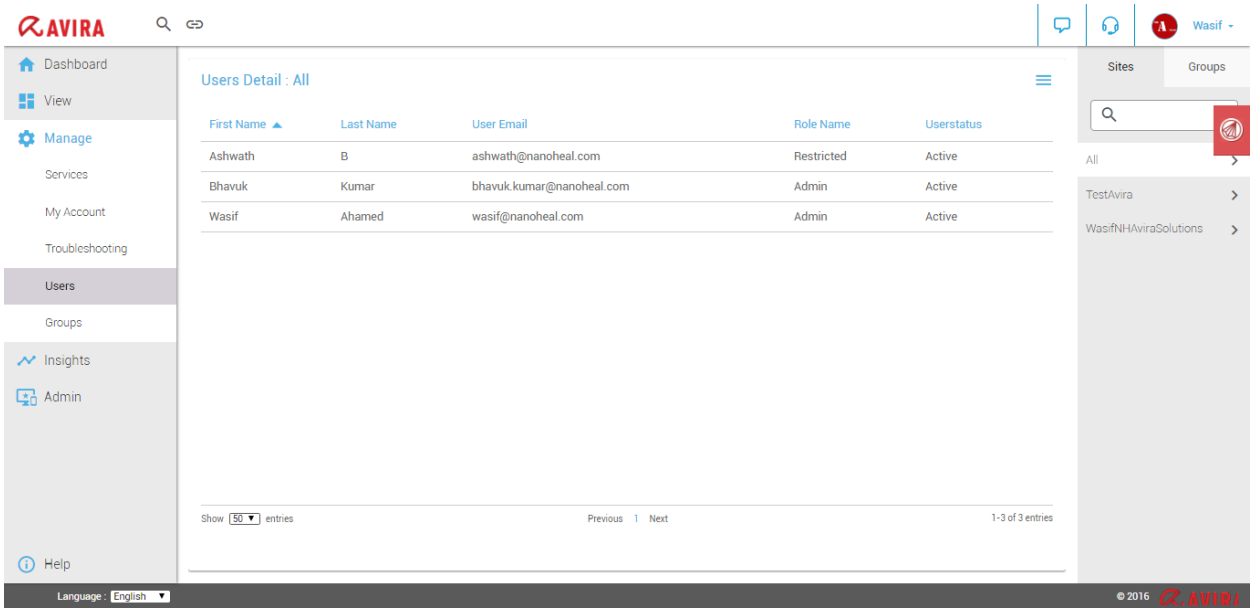
Users

Using the Nanoheal Dashboard, we can create **Users** by providing specific privileges or user roles to each user.

In order to on-board a User, Sign-in to Dashboard and navigate to Manage > Users as shown in the example below:

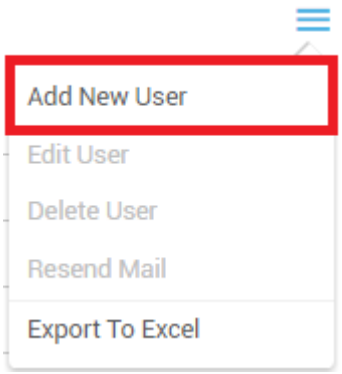


On clicking "Users", the screen below appears:

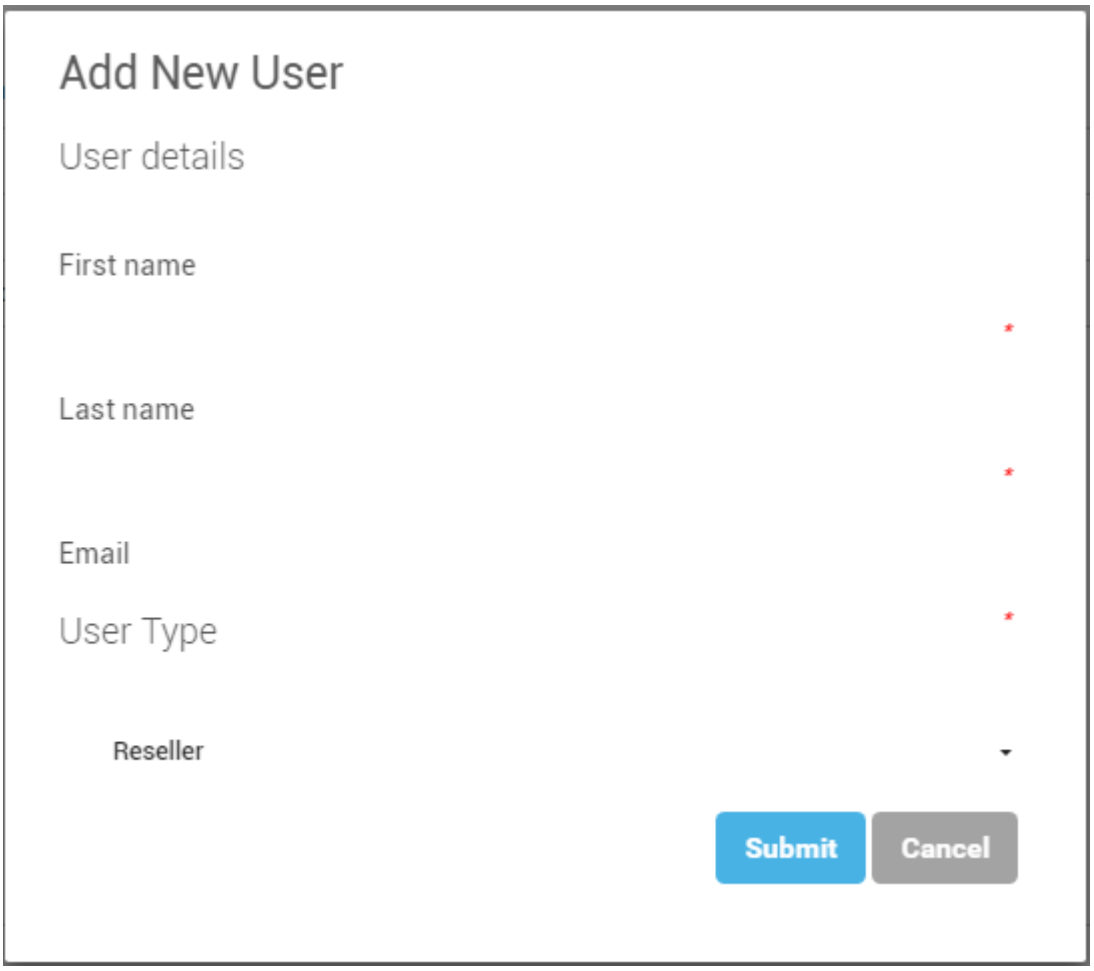


Add New User

In Order to add a new user - Click on the menu icon and click on 'Add New User' as shown below.



Upon clicking Add New User, 'Add New User' pop up will be shown as seen in the screenshot below.



As shown in the pop up, we need to fill First Name, Last Name, and Email. The User Role and User Type will be selected by default based on the logged in user role and type, the User can edit them. Then select any one site by clicking on the radio button and click on Submit Button to create the User.

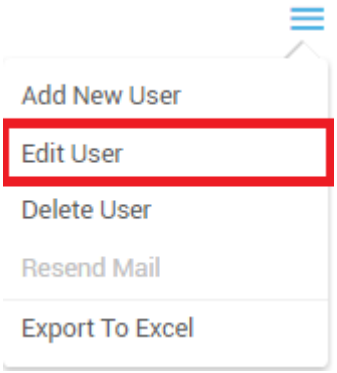
Once the User is created successfully, a confirmation email will be sent to the user on the email address with a link to set the password.

Once a password is set successfully, he/she can login to Dashboard with his/her credentials.

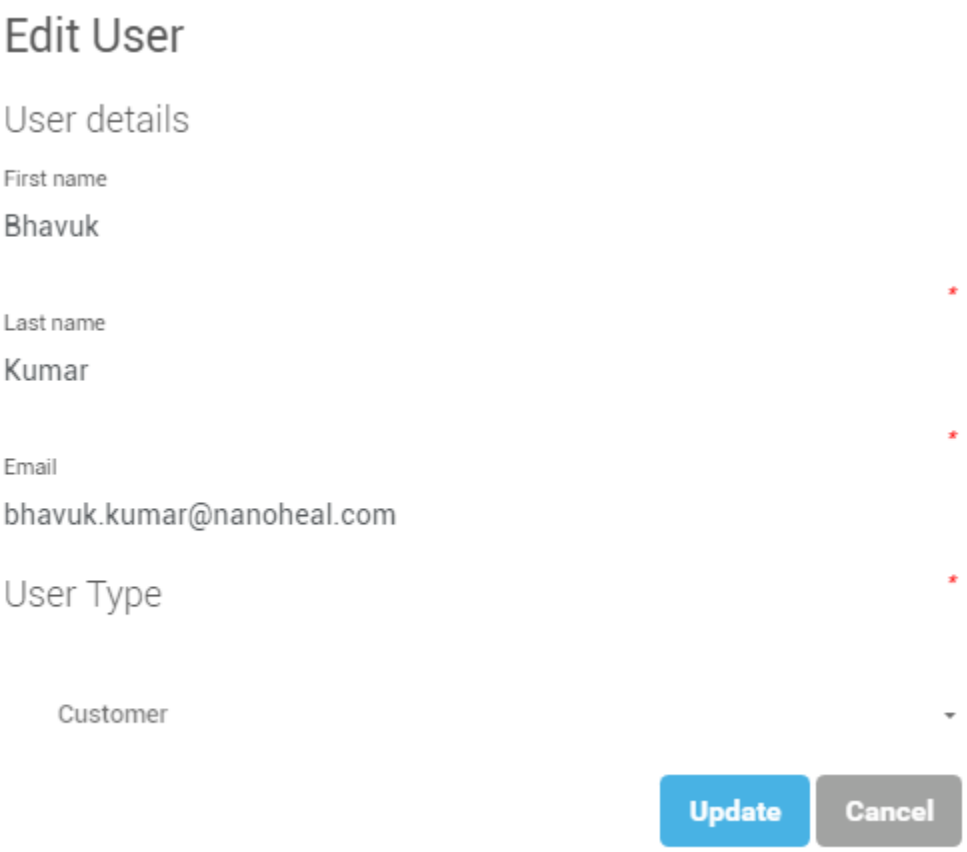
Edit User

We can always edit user details like First Name, Last Name & Site selection.

In order to edit the user, click on the menu and click on Edit User as shown below.

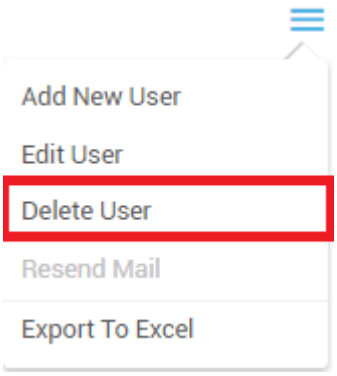


Upon clicking Edit User, Edit User pop up will be shown as seen in the screenshot below.

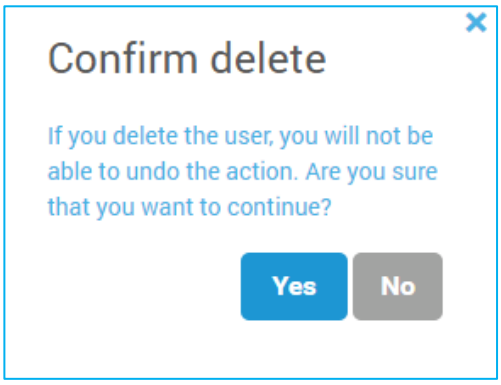


Delete User

User can always be deleted, if he/she is no longer accessing the Dashboard. In order to delete a user, click on menu and click on Delete User as shown below.



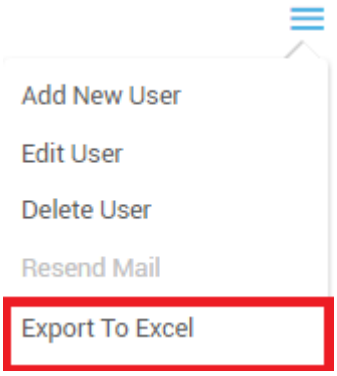
As shown above, clicking on the "Delete user" link form menu will open up confirmation pop up for delete as shown below.



As shown in the screenshot above, clicking on Yes will delete the user successfully & clicking on No will discard the user deletion.

Export

User Details can be exported by clicking on the menu icon & selecting 'Export To Excel' as shown below.



Upon clicking Export to Excel, user details will be exported to .xls format. Example:

	A	B	C	D	E
1	**First Name**	**Last Name**	**User Email**	**Role Name**	**Userstatus**
2	Senthil	Padmanaban	hp@nanoheal.com	Agent	Active
3	HP	Reseller	hpchannel@nanoheal.com	Reseller	Active
4	Jay	Cook	jay.cook@hp.com	Agent	Active
5	Kevin	Glasco	kevin.glasco@hp.com	Agent	Active
6	Linda	Godwin	linda.godwin@hp.com	Agent	Active
7	Ryan	Cortez	ryan.bra.cortez@hp.com	Agent	Active
8	Senthil	Solutions	hpcustomer@nanoheal.com	Customer	Active
9	Shawn	Storey	Shawn.Storey@hp.com	Agent	Active
10	Wasif	Ahamed	wasif6@nanoheal.com	Agent	Active
11	Wasif22	Ahamed22	wasif22@nanoheal.com	Agent	Pending
12	Wasif	Ahamed	wasif11@nanoheal.com	Agent	Active
13	Wendy	Rojas	wendy.rojas@hp.com	Agent	Active

Note: User Status varies. Active/Pending are the two status codes for the user. A used is coded, "Active" if the user has set a password else the user is coded 'Pending'.

User Roles

There are 3 User roles namely:

- Admin
- Normal
- Restricted

These user roles are defined based upon following table as described below:

Module	Sub-Module	Breadcrumb Options	Admin	Normal	Restricted
View	**Sites**		YES	YES	YES
		Export List	YES	YES	YES
		View Events	YES	YES	YES
		Machine Remote	YES	NO	NO
	Compliance		YES	YES	YES
		Reset	YES	NO	NO
	Notification		YES	YES	YES
		Fix	YES	NO	NO
		Other Action	YES	NO	NO

		Details	YES	YES	YES
		Export to Excel	YES	YES	YES
Manage	**Services -> MUM**		YES	YES	YES
		Configure	YES	NO	NO
		Approve Update	YES	NO	NO
		Decline Update	YES	NO	NO
		Remove Update	YES	NO	NO
	Services -> Software Distribution		YES	YES	YES
		FTP/CDN Configuration	YES	NO	NO
		View Software Details	YES	NO	NO
		Add New Package	YES	NO	NO
		Edit Existing Packages	YES	NO	NO
		Distribute Packages	YES	NO	NO
		View Software Distribution	YES	NO	NO
		Delete Package	YES	NO	NO
	Services -> Active Directory Reset		YES	YES	YES
		Configure Questions	YES	NO	NO
		Change Password	YES	NO	NO
		Reset Security Answers	YES	NO	NO
		Unlock Account	YES	NO	NO
	Troubleshooting		YES	YES	YES
		Run Buttons	YES	NO	NO
	Users		YES	YES	YES
		Add New User	YES	NO	NO
		Edit User	YES	NO	NO
		Delete User	YES	NO	NO
		Export To Excel	YES	YES	YES
	Groups		YES	YES	YES
		Add New group	YES	NO	NO
		Rebuild group	YES	NO	NO
		View Details	YES	YES	YES
		Export group details	YES	YES	YES
		Export group list	YES	YES	YES
		Delete group	YES	NO	NO

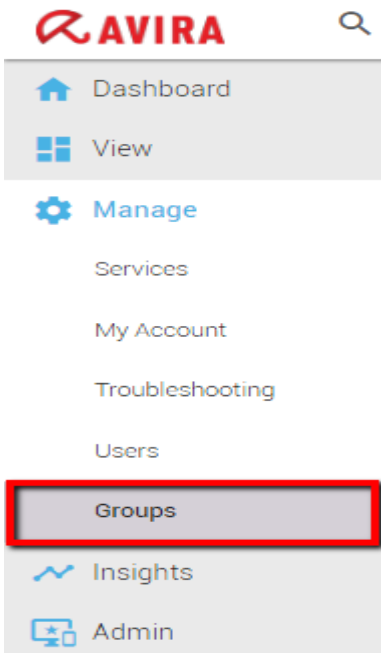
Insights	**Incident Trend**		YES	YES	YES
		Export List	YES	YES	YES
	Compliance Trend		YES	YES	YES
		Export List	YES	YES	YES
	Resolution		YES	YES	YES
		Proactive	YES	YES	YES
		Predictive	YES	YES	YES
		Export To Excel	YES	YES	YES
	Capacity Report		YES	YES	YES
		Export To Excel	YES	YES	YES
	Mange Report/Services Insights		YES	YES	YES
		Add New	YES	NO	NO
		Edit	YES	NO	NO
		View	YES	YES	YES
		Download	YES	YES	YES
		Delete Report File	YES	NO	NO
		Delete Report	YES	NO	NO
		Run Now	YES	NO	NO
		Refresh	YES	YES	YES
	Sales Insights		YES	YES	YES
		Add New	YES	NO	NO
		Edit	YES	NO	NO
		View	YES	YES	YES
		Download	YES	YES	YES
		Delete Report File	YES	NO	NO
		Delete Report	YES	NO	NO
		Run Now	YES	NO	NO
		Refresh	YES	YES	YES
	Asset Information		YES	YES	YES
		Export List	YES	YES	YES
		Information Portal	YES	YES	YES
Quick Links	Event Information		YES	YES	YES
	Asset Information		YES	YES	YES
	Deployment		YES	YES	YES
		Export	YES	YES	YES

		Impersonation Setting	YES	NO	NO
		Scan	YES	NO	NO
		Deploy	YES	NO	NO
	Manage Customers		YES	YES	YES
	Edit My Profile		YES	YES	YES
	Change Profile Picture		YES	YES	YES
	My Account		YES	YES	YES

Note: We can also create new User Roles & define the type of access as needed for the dashboard. Also, existing User roles ACD's can be edited upon request. This can be achieved with an email request to the Nanoheal Team.

Groups

Groups are created by grouping the devices manually under a specific group name.
In order to create a group, the user needs to navigate to Groups from the left panel as shown in the example below:

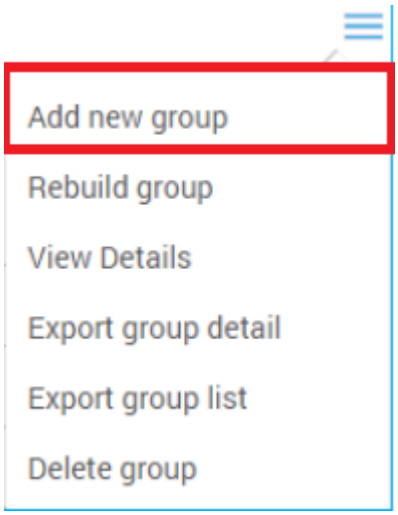


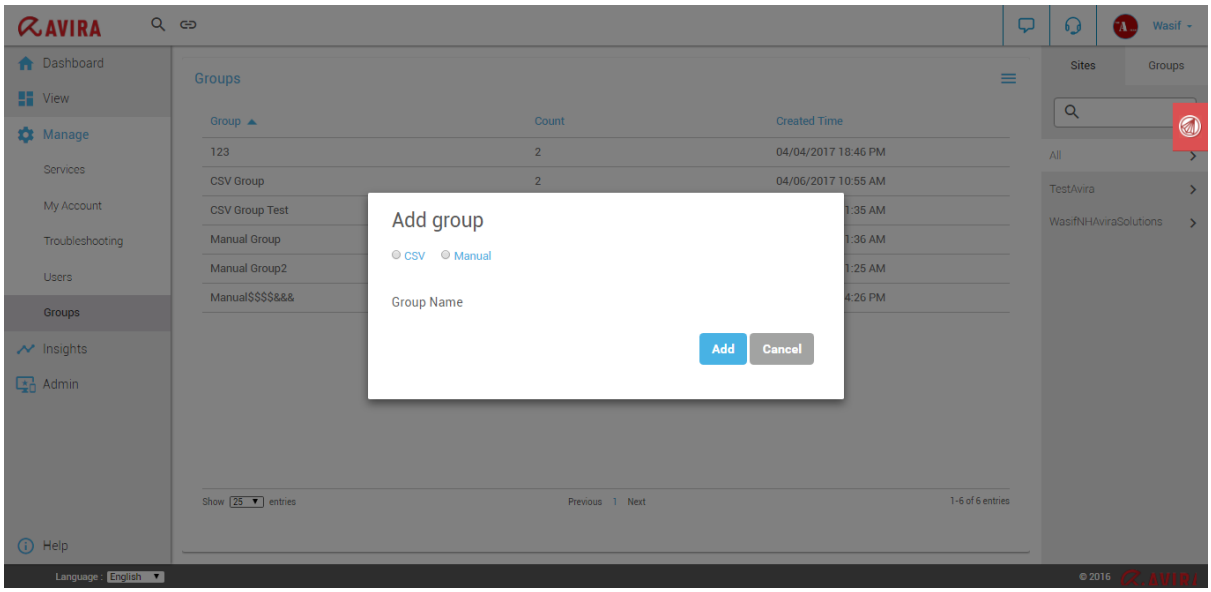
Add New Group

Groups can have devices that belong to one customer or several customers.

For example, users can create a "MAC" group which contains devices that have Mac OS X as their operating system, but belong to different customers. Groups give users the flexibility to push common resolutions.

To add a group, the user needs to click on the right Menu & select 'Add group' from the drop-down. An example is shown below:





CSV: To create a group using CSV, a user must enter the group name and import a sample csv file. To import the sample csv file, he/she, must click on the 'sample file' link that they would see on the 'Add group' pop-up. A file called 'deviceList.csv' is downloaded. And the file will look similar to the sample shown below:

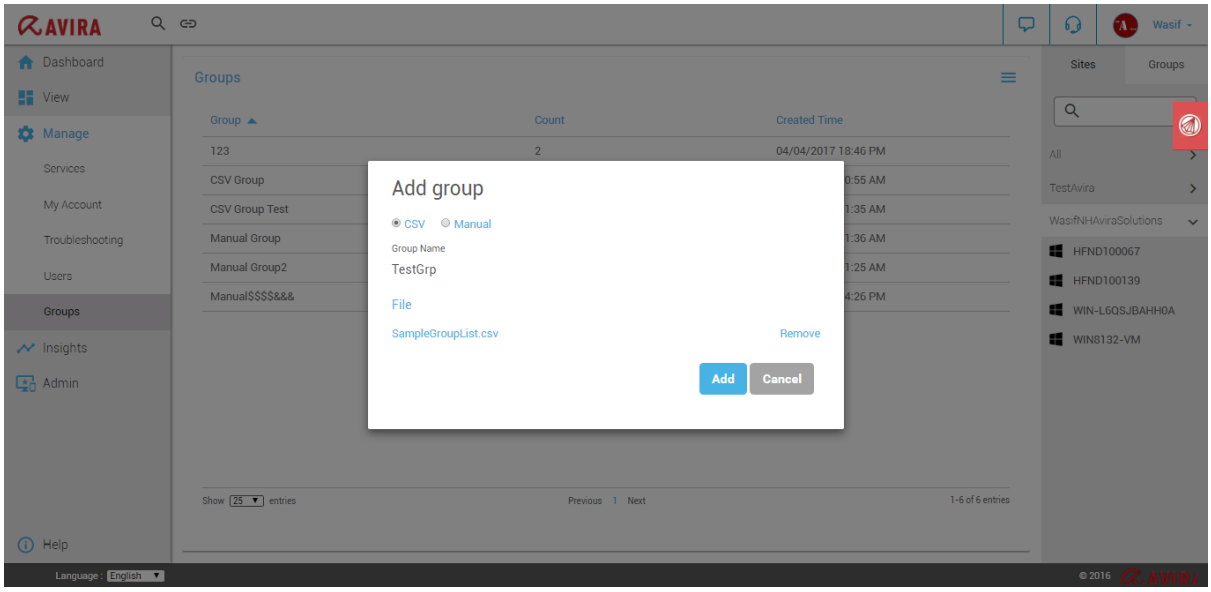
	A	B
1	**Sites**	**Machines**
2	Nanoheal_Customer1	5CG52822LW
3	Nanoheal_Customer2	C07M81RYDWYL

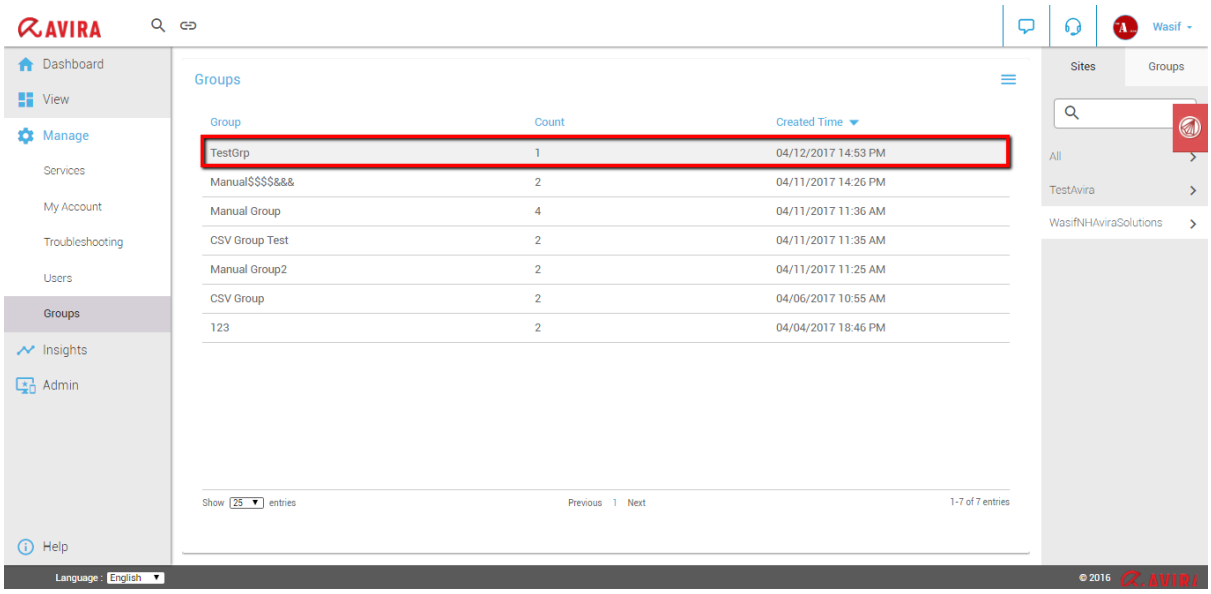
User must now enter the Site name and Machine names in corresponding columns similar to the example .csv file that was downloaded.

Save the file in .csv format and upload it to the 'Add group' pop-up through 'browse'.

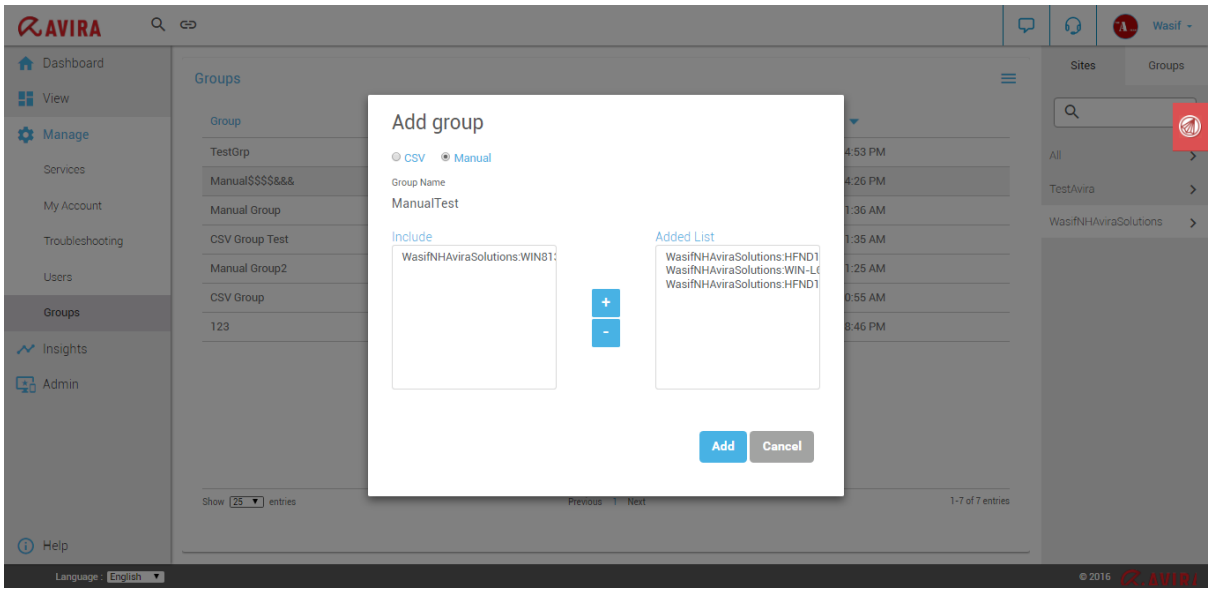
A new group with the Machine names mentioned in the .csv file will now be created.

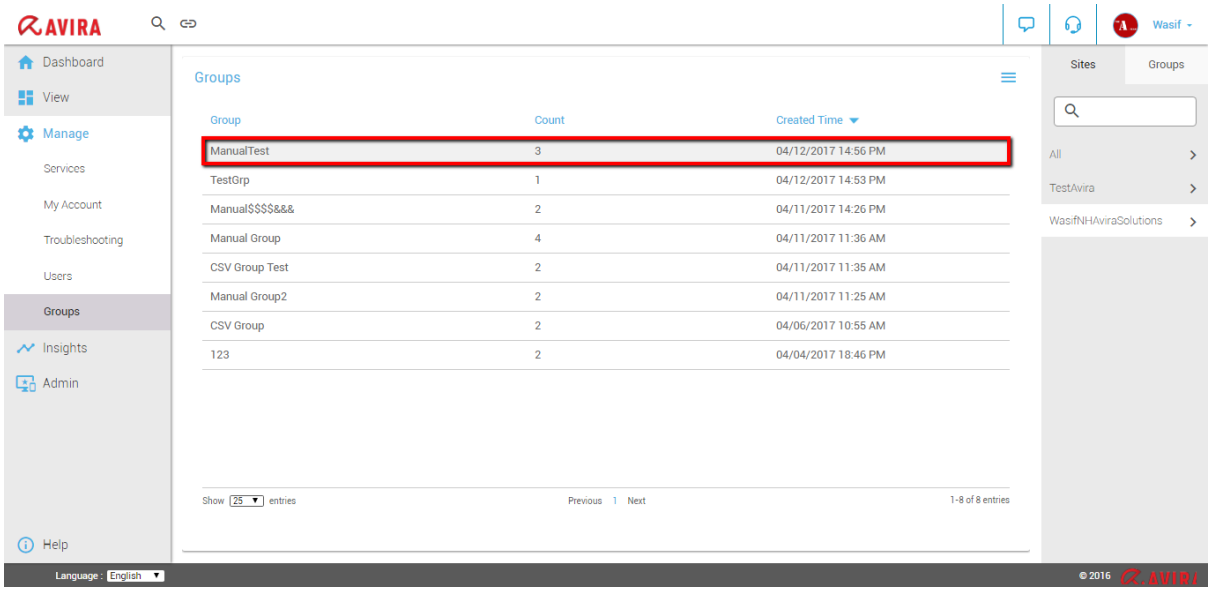
As shown below:





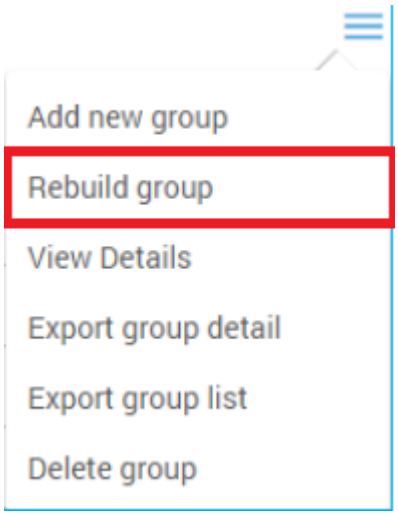
Manual: To create a group manually, user should select manual option. All machine details along with site name will appear in Inclusion list. User should give group name and select machine of which they want to create group by clicking on + symbol and then click on add as shown below:



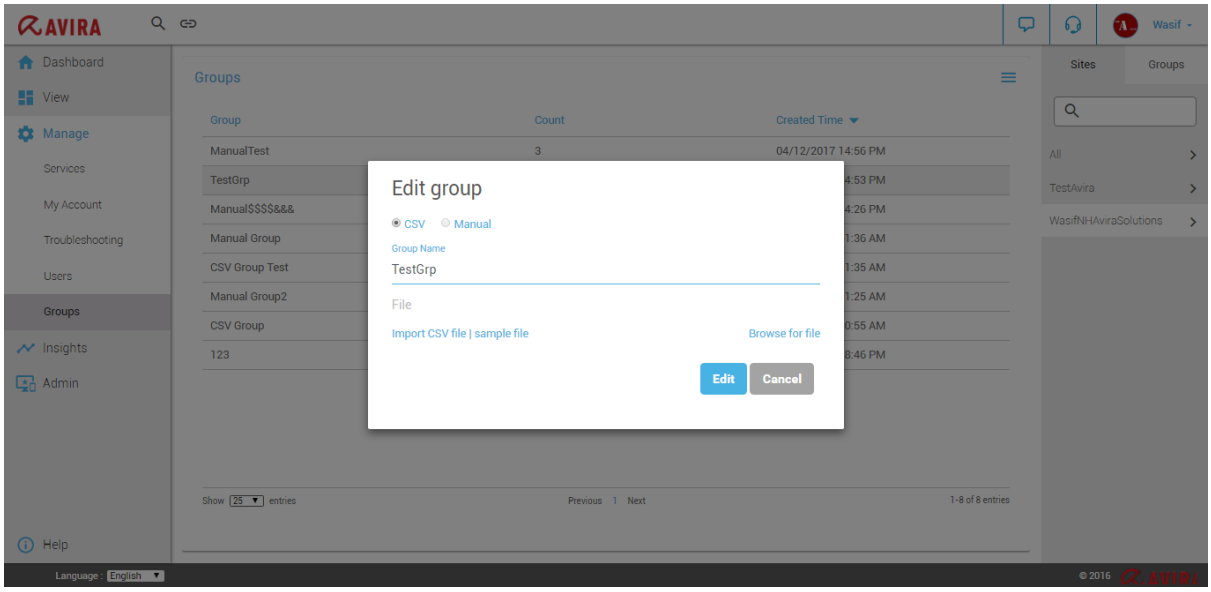


Rebuild Group

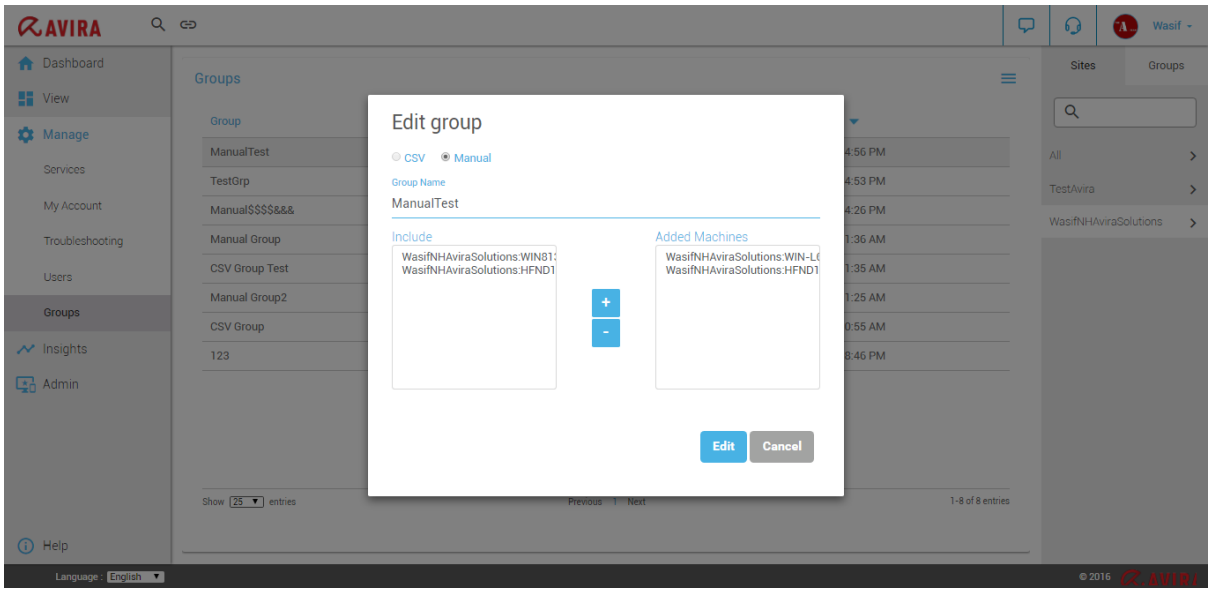
Users can edit the existing group. User has to select the group which he wants to edit and then has to choose rebuild group option from the drop-down in menu button.



Users can change the machines included in the group by uploading a new .csv file by clicking on Browse for file.

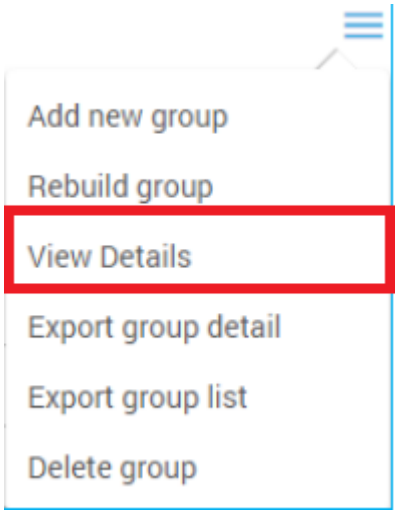


Or User can select/deselect machine if it is a manual group.

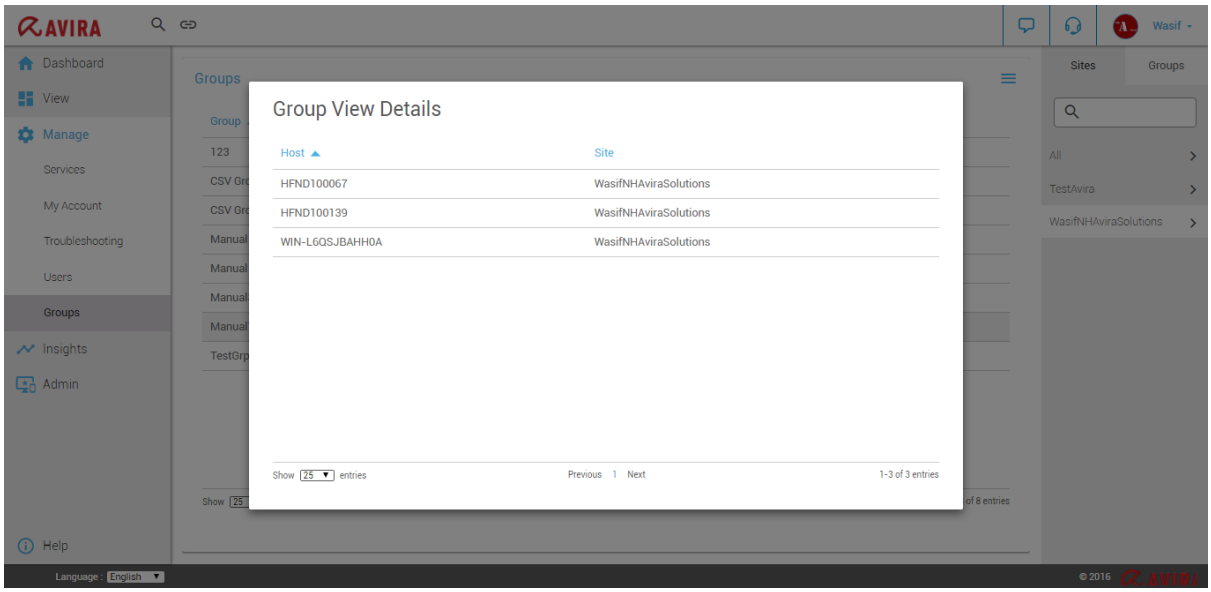


View Details

In order to view the created group details, the user needs to select the group and choose View Details link from the drop-down menu.

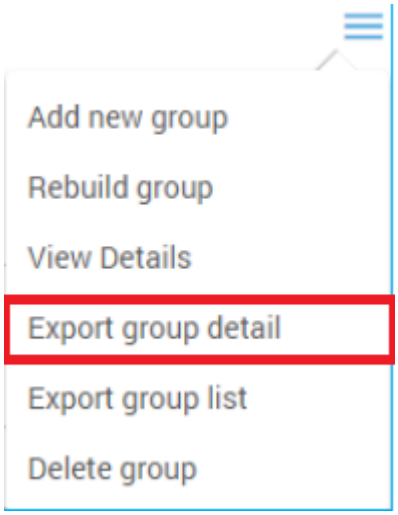


A pop-up will display the group details.



Export Group Detail

In order to export the group data, user has to select the group and choose Export group detail from the drop-down menu. Only the selected group data is exported to a .xls file.

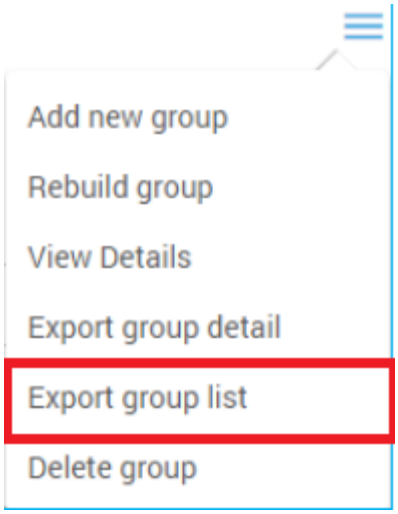


A sample .xls file is shown below:

	A	B
1	**Group**	**Device List**
2	Mac Devices	NanohealV2768SEP01@VMWVk0zIsaAiwxwubzqTYrroQ
3		SenthilSolutionsnew@CPWQT77BG940
4		NanohealV2768SEP01@VMWVk3T1i04USe4at6vhI6k1Q

Export Group List

In order to export the group list data, the user has to choose Export group list from the drop-down menu.

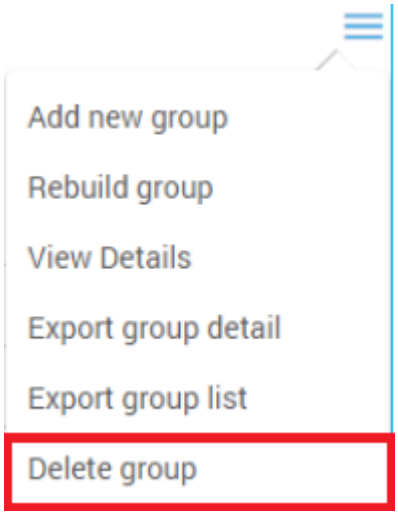


After the user clicks on the Export group list, all the group list data will be exported to .xls. A sample .xls is shown below:

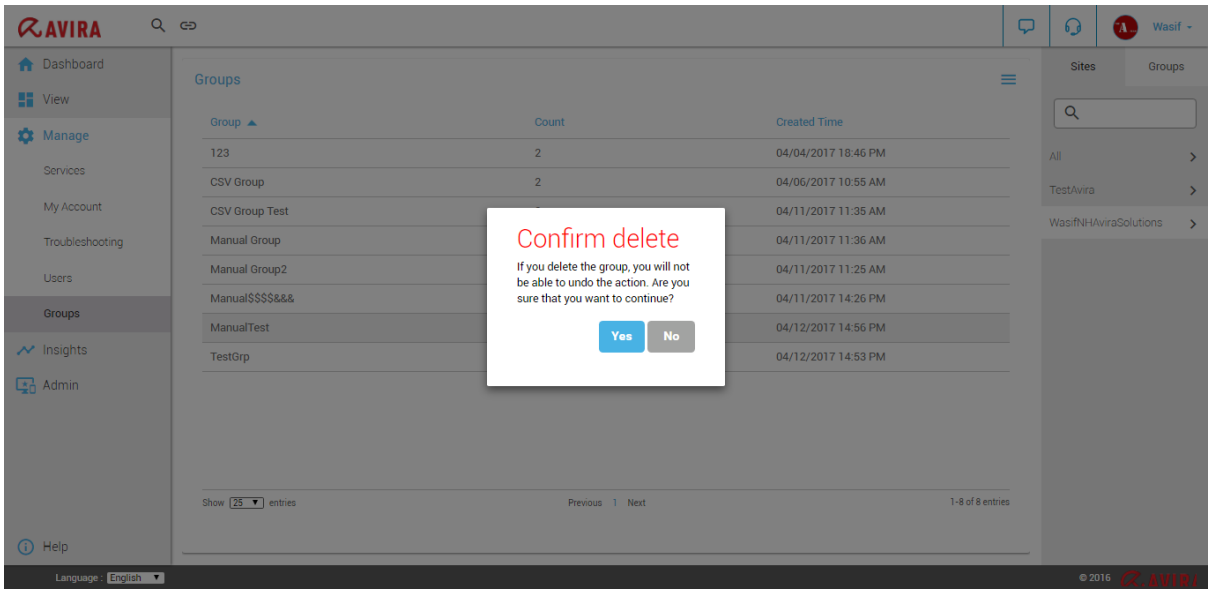
	A	B	C
1	**Group**	**Device Count**	**Created Time**
2	Mac Devices	3	11/15/2016 00:10 AM
3	Test Group	1	10/27/2016 23:43 PM
4	V6 Manual Group	2	10/20/2016 06:54 AM
5	test123	1	10/27/2016 23:43 PM

Delete group

A Group can be deleted by using the Delete group link under the drop-down menu as shown below:



Selecting an existing group & clicking on Delete group link under menu will open up the Confirm Delete pop up as shown below.

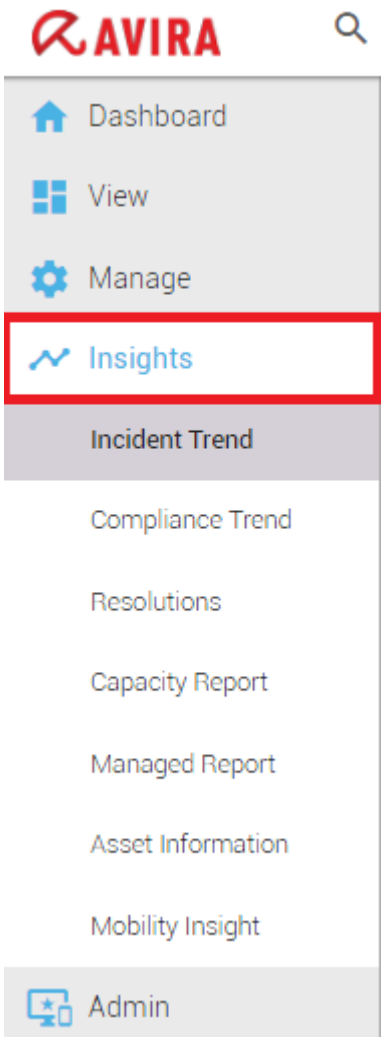


When prompted, click on "Yes" to delete the group, and "No" to cancel deleting the group.

Insights

Nanoheal provides an efficient way to give environment overview to the administrators on scheduled or on demand basis. This module is known as Insights. Insights can help the administrator to carry out capacity planning, as it covers virtually all details of the device. The administrator has the ability to make their own reports by adding multiple sections to it. Additionally they can schedule reports to run at a time convenient to them or run them on demand.

Insights are divided into different sections as shown below:

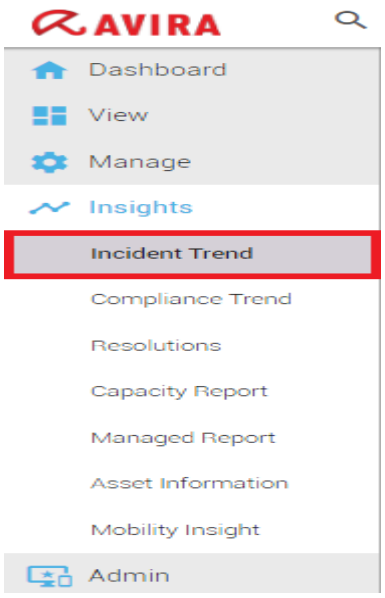


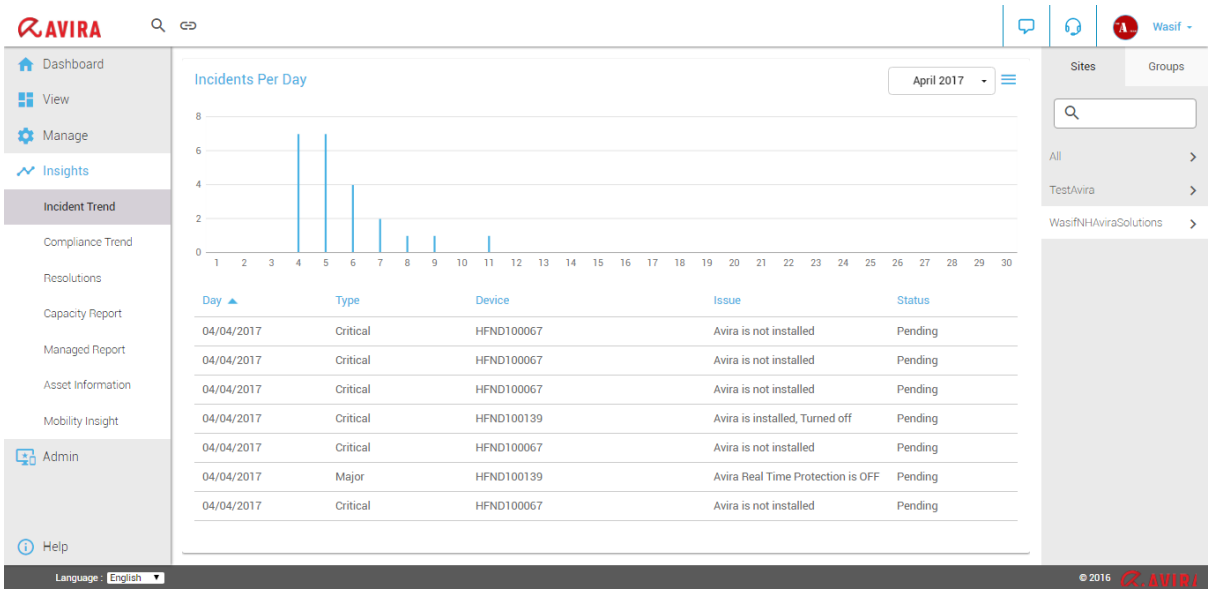
1. Incident Trend
2. Compliance Trend
3. Resolutions
4. Capacity Report
5. Managed Report
6. Asset Information

7. Mobility Insight

Incident Trend

This shows the summary of Incidents that have been reported per day. An example is shown below:

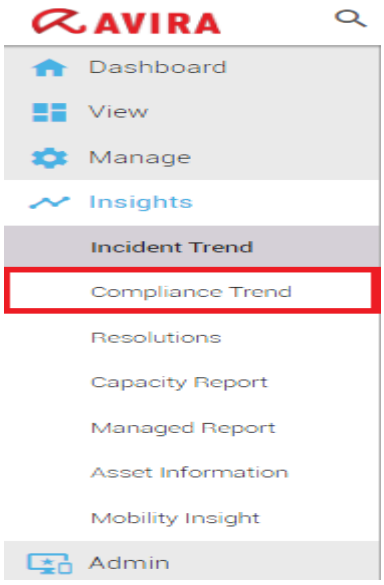


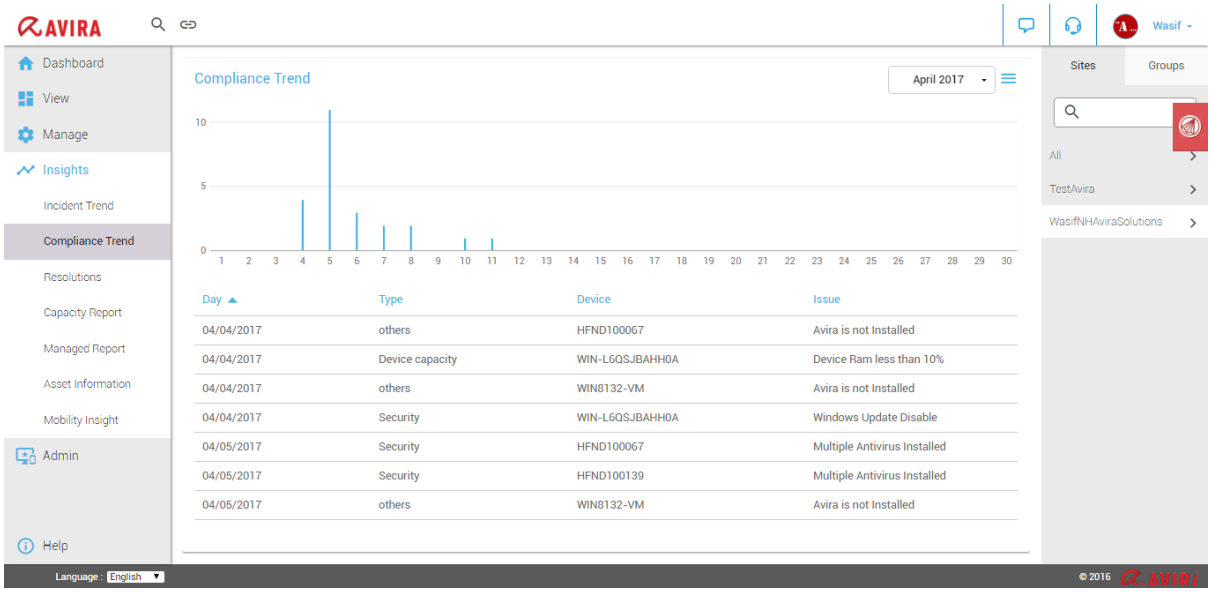


Sample graph displayed above, highlights various issues that have occurred on different devices for the month of 'April 2017'. These issues mainly include Avira Installed/Uninstalled State, RTP On/Off, Windows update enable/disable etc.

Compliance Trend

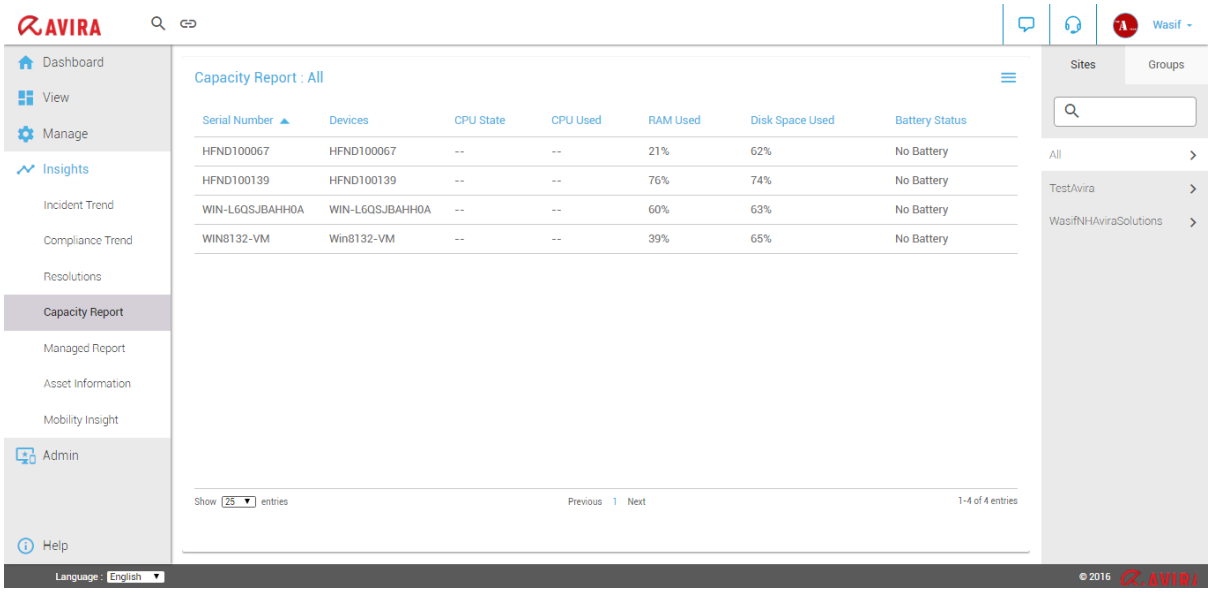
This shows the summary of machines that have been compliant. An example is shown below:





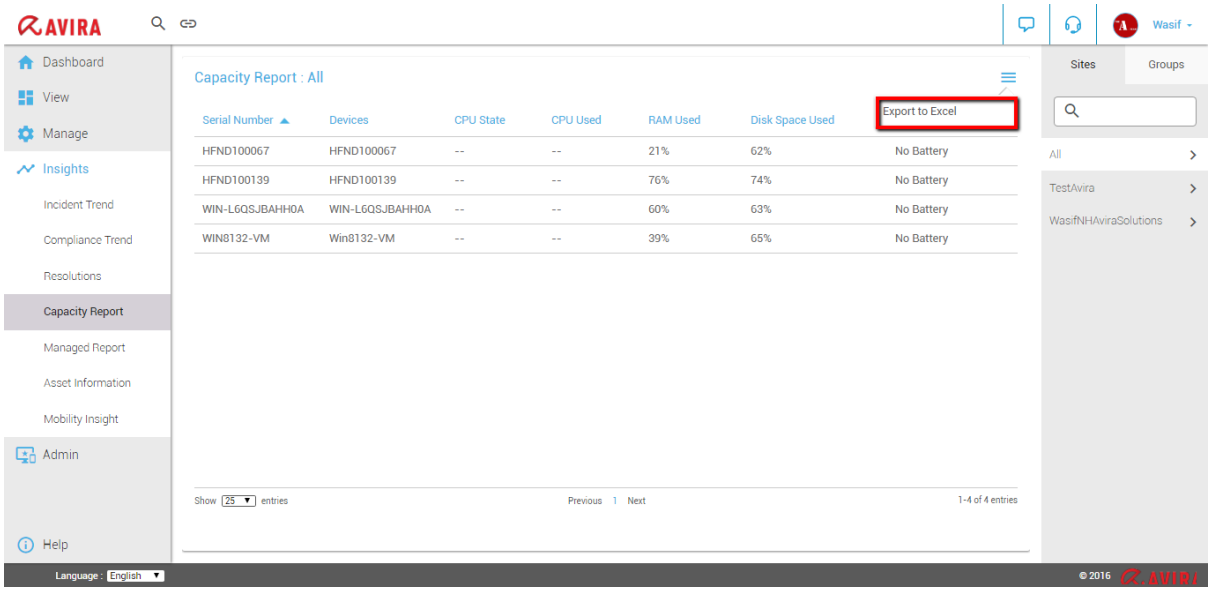
Capacity Report

This will show details on the CPU, RAM & Disk Space Usage data for a specific device and Host Name as shown below:



User can also export this data to a .xls format by using the Export list link under the menu drop-down.

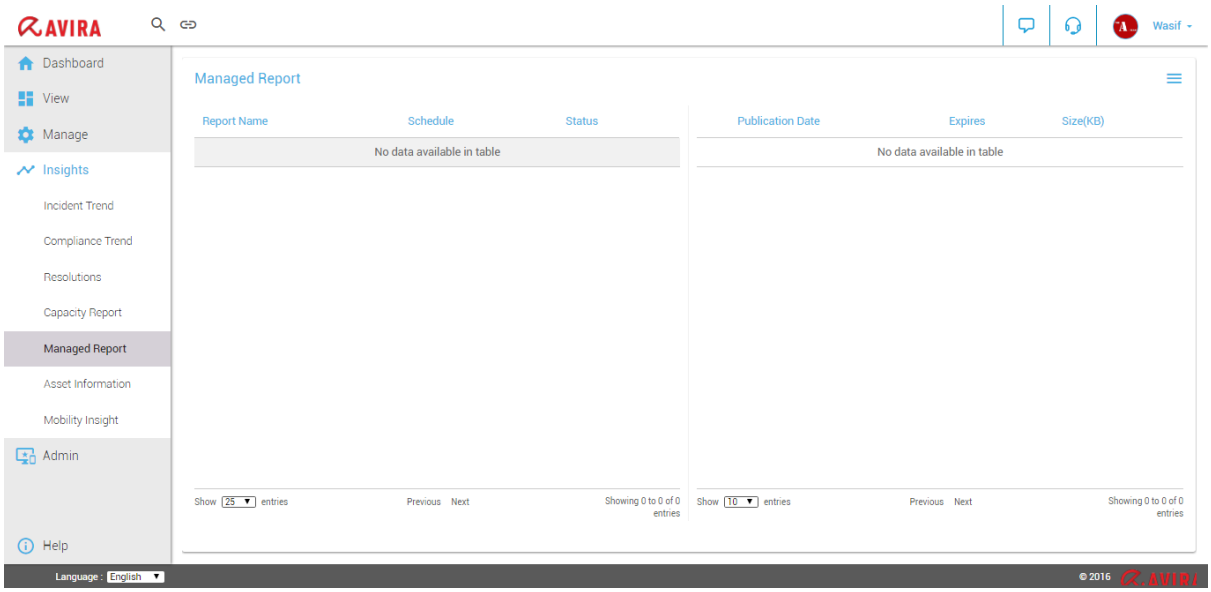
An example on how to navigate to 'Export list' and a sample .xls file is shown below:



	A	B	C	D	E	F	G
1	Serial Number	Device	CPU State	CPU Use	RAM Used	Disk Spac	Battery Status
2	HFND100067	HFND100067	-	-	21%	62%	No Battery
3	HFND100139	HFND100139	-	-	76%	74%	No Battery
4	WIN-L6QSJBAHH0A	WIN-L6QSJBAHH0A	-	-	60%	63%	No Battery
5	WIN8132-VM	Win8132-VM	-	-	39%	65%	No Battery
6							

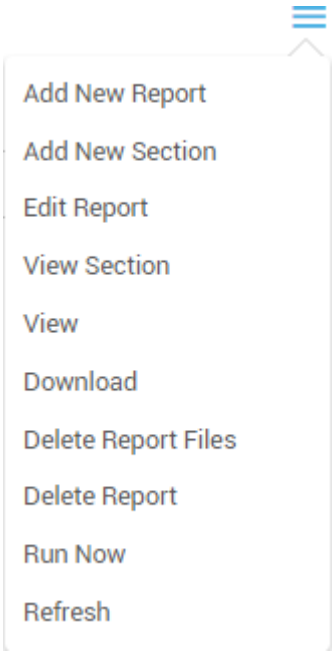
Managed Report

Clicking on Managed Report will open up the screen below.



In order to create a new report, user has to click on right menu icon.

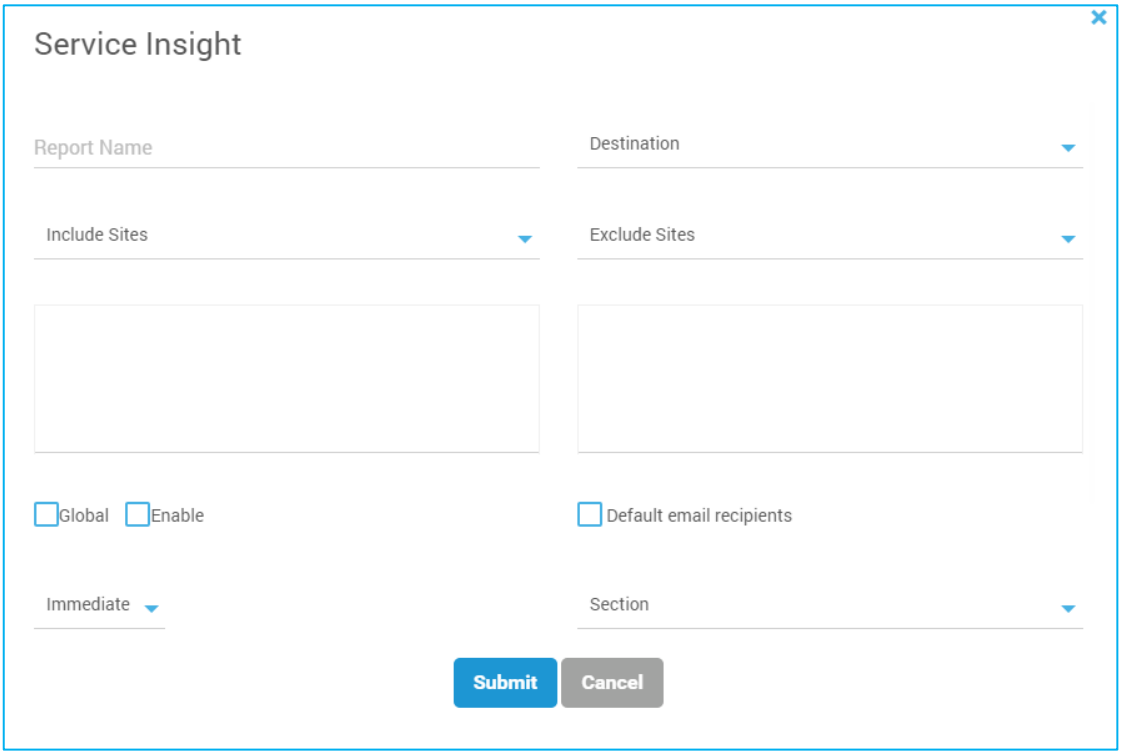
Upon clicking the menu icon, following options will occur.



1. Add New Report

As shown in the screenshot above, click on 'Add New Report' to create new Reports.

Clicking on Add New will open a pop like the one here.



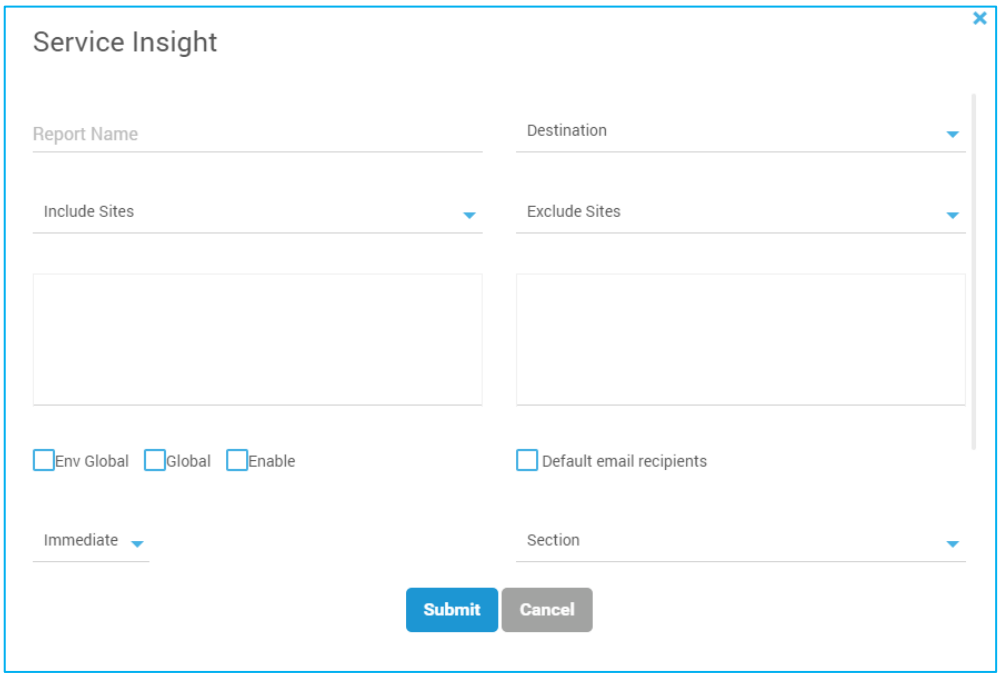
As shown in the screenshot above, we need to enter the below details:

- **Report Name**: Identifiable name for the Report
- **Destination**: Information Portal or Email
- **Information Portal:** If checked, the report would be posted on to Information Portal. Else, the report would be sent via email to specified email recipients
- **Email Recipients:** If "Information Portal" is unchecked & 'Email" is checked - email addresses should specified in this field separated by commas
- **Include:** Choose from the list of sites or machines which should be included on the report. In order to run the same for all the machines on server, we need to select "All"
- **Exclude**: In this, we can choose from list of sites or machines which shall be excluded from this report
- **Global**: Visibility of the report. If checked, report is visible at the user level on the Dashboard. Else, it will be visible for the creator alone.
- **Enable**: We can Enable or Disable the report using this option
- **Default email recipients**: When this option is selected or checked the report will be sent to all the default Email Recipients
- **Schedule**: Schedule on which the report needs to be run. Various schedule options are available, namely **Immediate, Daily, Weekly & Monthly**.

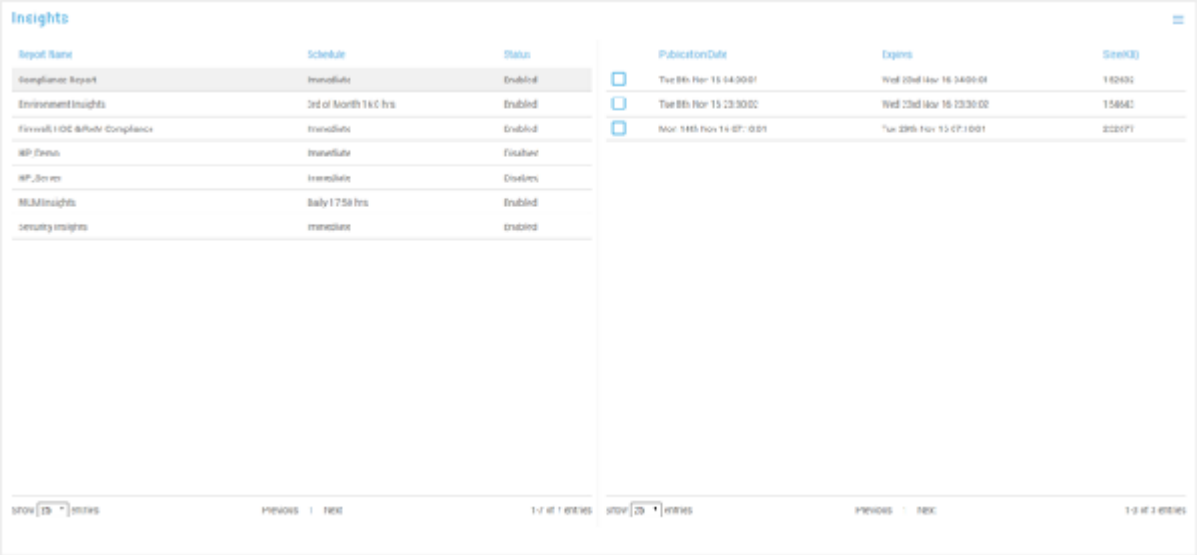
- **Section**: This field displays all the available sections created by the admin. We will be using these sections accordingly based on type of report
  Section will allow the users to attach either an event filter or an asset query or MUM status summary to create a report based on it. We need to enter the following:

- **Select Type of Section: Type of section can be either Summary Section or Event Section or Asset Section or MUM Section.**
- **Section Name: Identifiable name.**
- **Select Chart Type: We can choose the graphical format either bar chart or pie chart or tabular format.**
- **Select Sub-Headers: Sub-headers can be "Single" or "Multiple". If "Single", we can add a single section. i.e, we can attach either an event filter or an asset query. If we choose "Multiple" then we can attach multiple sections. i.e., multiple filters, asset queries to create a combination of asset & event reports.**
- **Sub Header Name: Identifiable name that co-relates to Section Name. i.e. if the Section Name is "Operating System" then the Sub Header Name could be sub categories, like - Chassis Information, Processor Information etc. based on what type of asset data we need on our report.**
- **Selection Criteria: Selection Criteria varies depending upon the selections. If Event Filter is selected, then a drop-down list shows a list of all existing filters. If Asset Queries is selected, then a drop-down list shows the list of existing asset queries. If MUM is selected, then the user needs to select Summary Headers, Update Type, Update Size, Operating System, Month, Year, Patches**

Note: When we login as an admin & try to create report- The add new pop up shows an option- 'Env Global'. When we select this option & create a report the report will be visible to all the users. This is shown in the screenshot below.

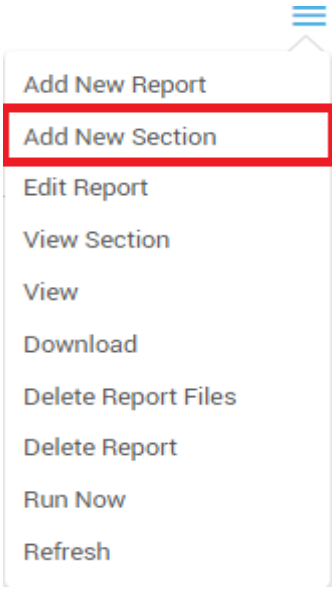


Upon clicking the **submit** button the Services Insights report will be generated as show in the screenshot below.

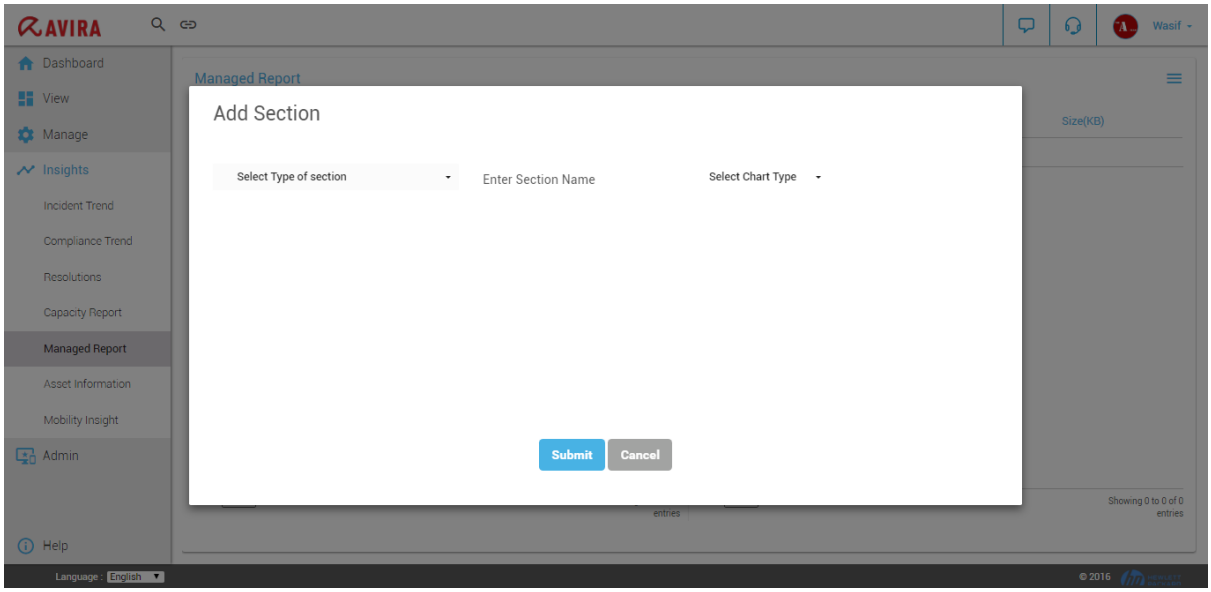


2. Add New Section

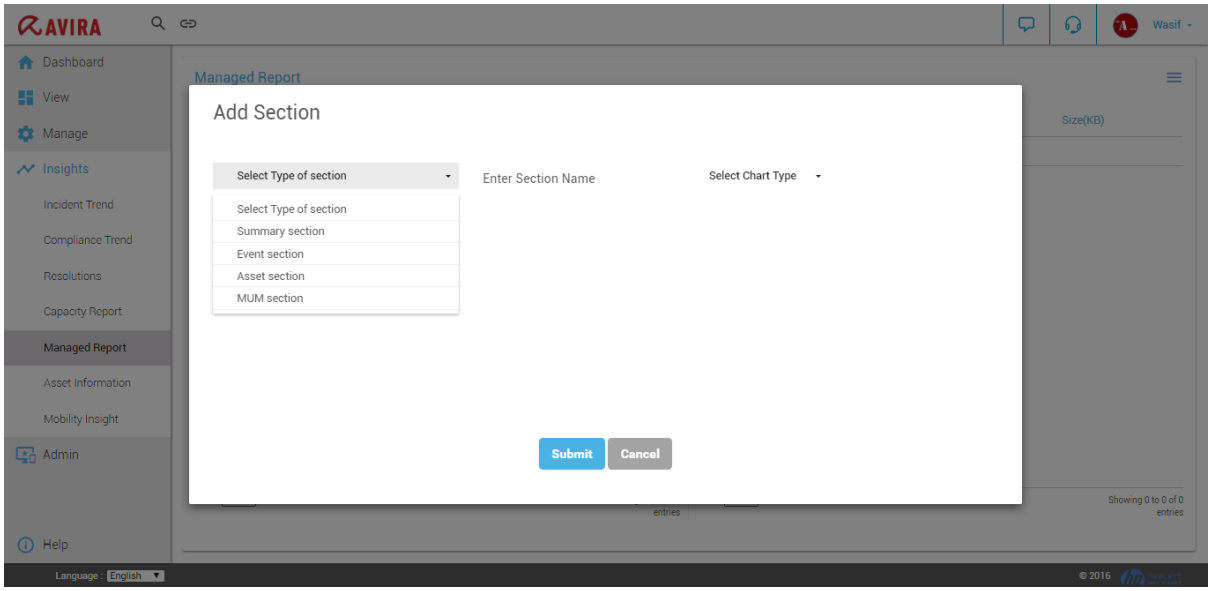
The user can add new section such as event, asset, Mum as shown below:



Click on add new section will open the following window:



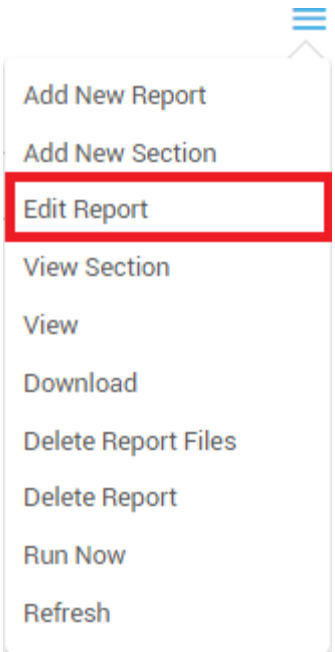
User can select type of section he wants to add like below:



Every section will have different fields as per the section selected.

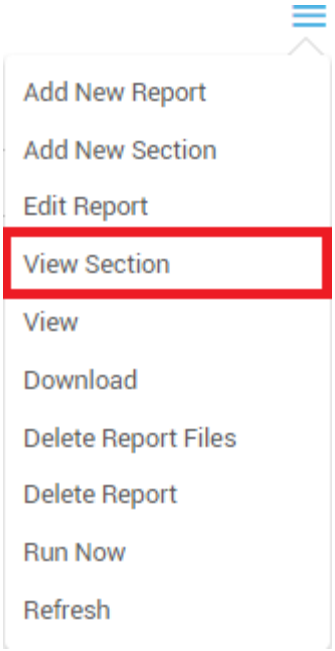
3. Edit

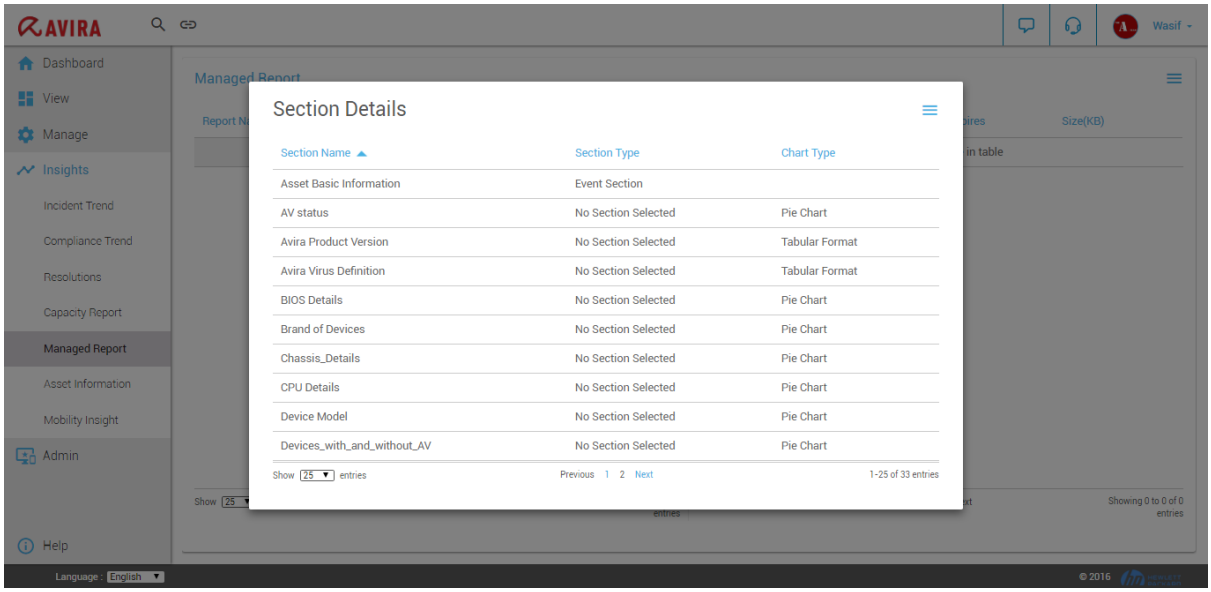
We have an option to edit an already existing report. In order to do the same, select an existing report and click on "Edit Report" as shown below:



4. View Section

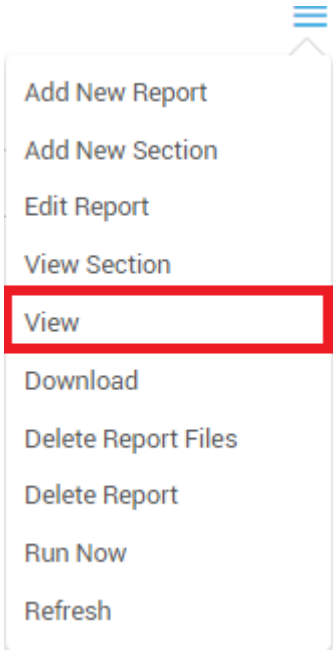
This option will display all the available section with details.



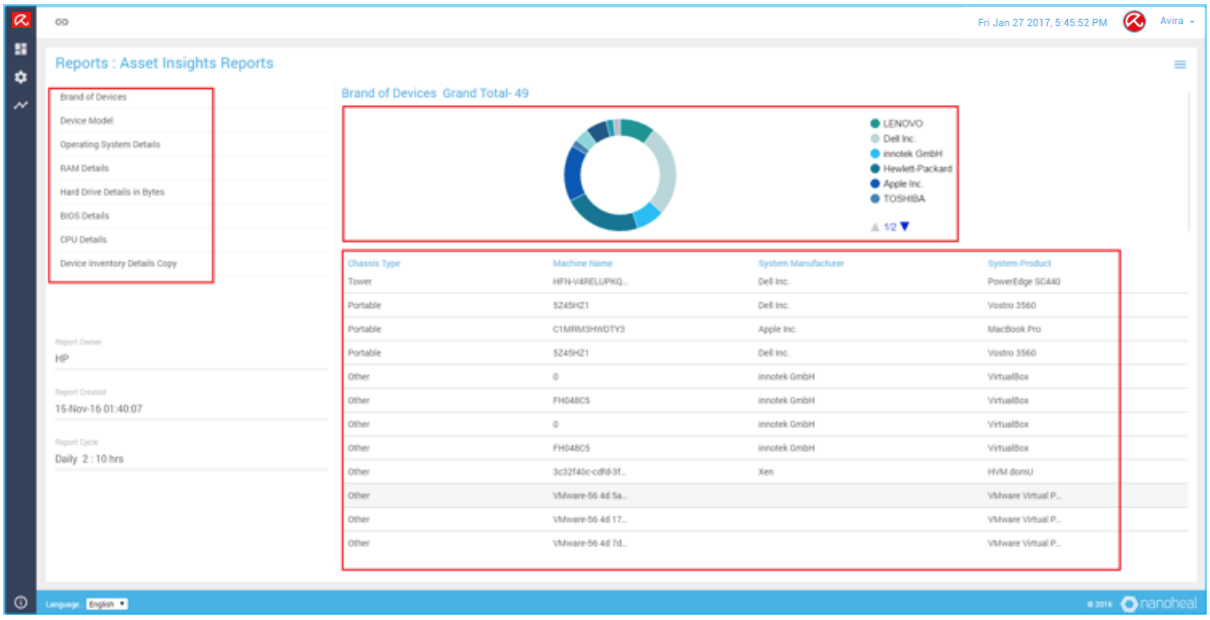


5. View

"View" option will allow the user to view a generated report by selecting a report and clicking on "View" from right menu icon:

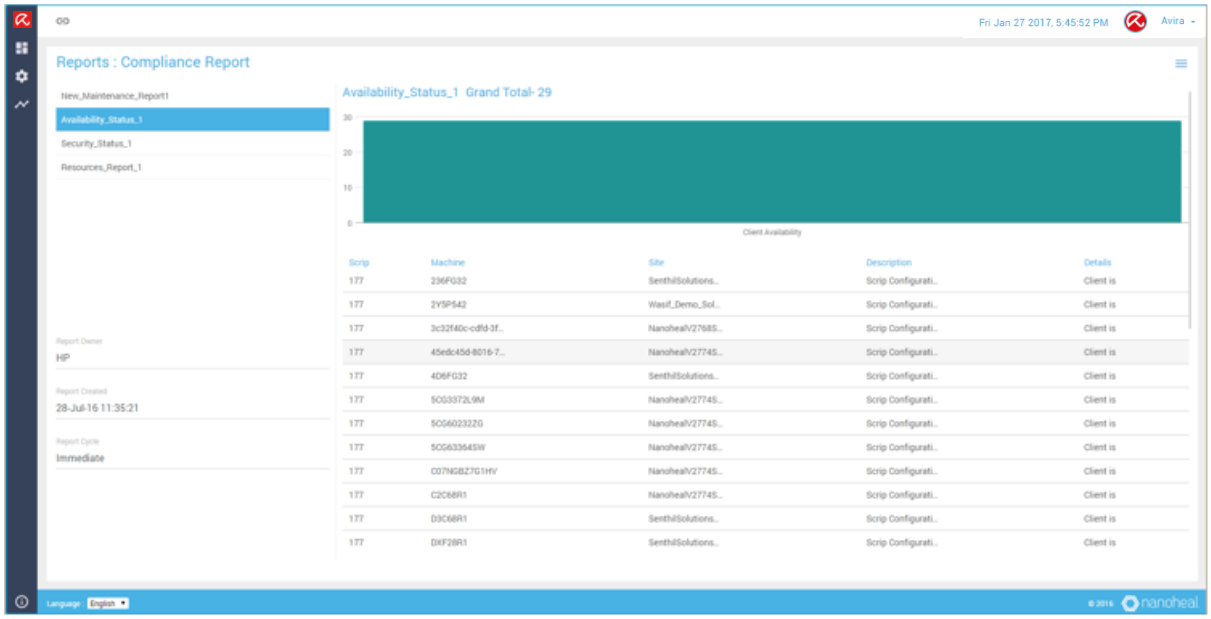


Portal Asset Report: Sample Asset Report from Information portal is shown in the screenshot below. Based on selected Asset sections, report will be generated accordingly.



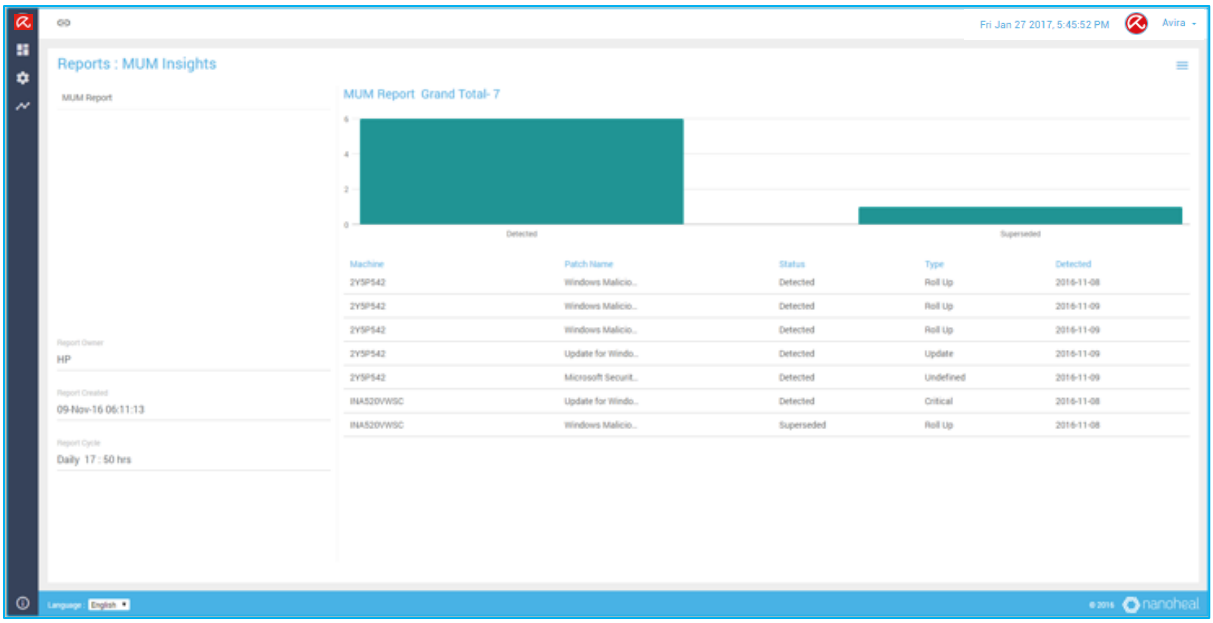
Sample Services Insights Asset Report with Pie Chart: Fig (1)

Portal Event Report: Sample Event Report from Information portal is shown in the screenshot below. Based on selected Event sections, report will be generated accordingly.

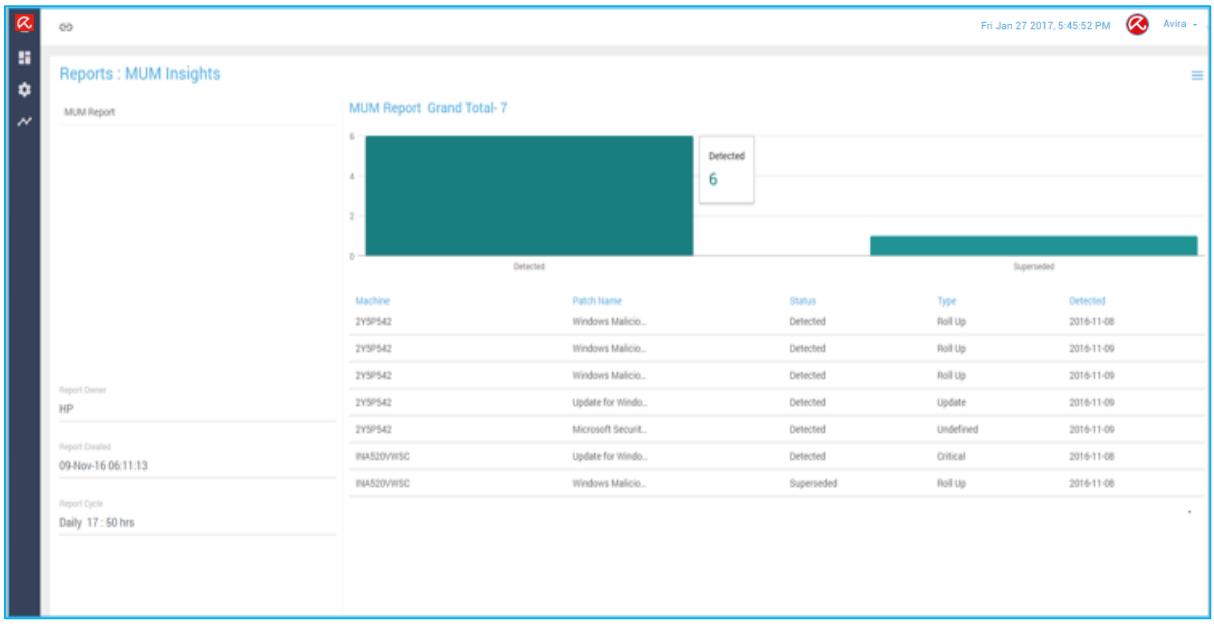


Sample Services Insights Event Report with Tabular format: Fig (2)

Portal MUM Report: Sample MUM Report from Information portal is shown in the screenshot below. Based on selected sections of MUM, report will be generated accordingly with different statuses (Detected, Downloaded, Installed, Superseded, Waiting, etc…) being shown to the user.



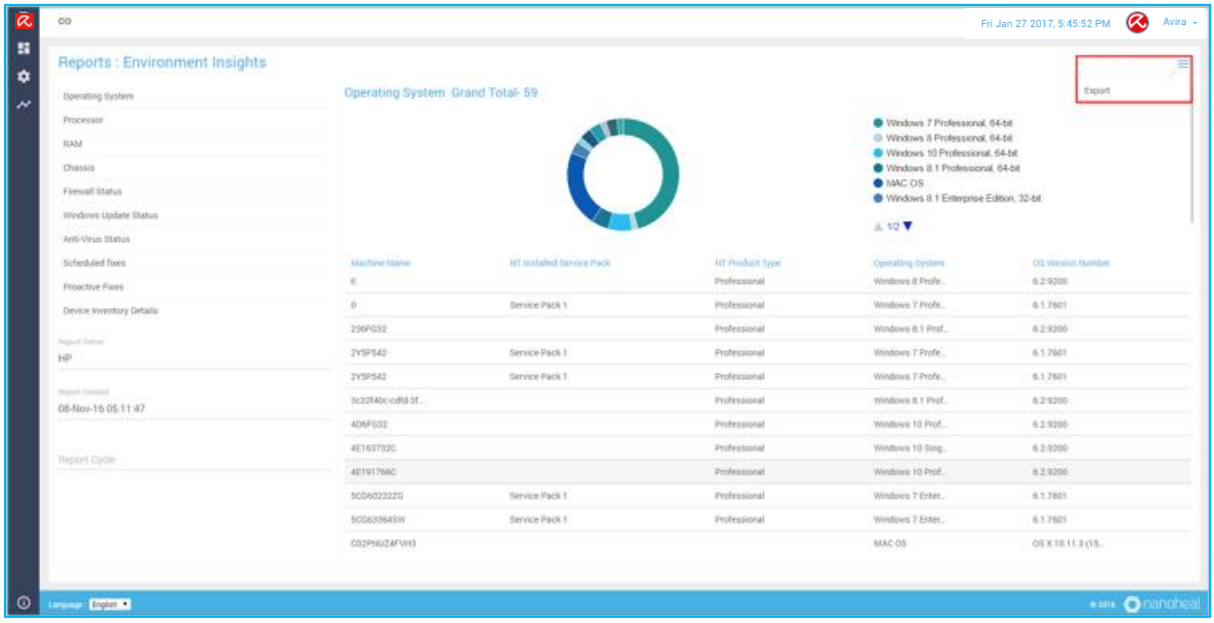
Sample Services Insights MUM Report with Bar Chart: Fig (3)



Sample Services Insights MUM Report with Bar Chart: Fig (4)

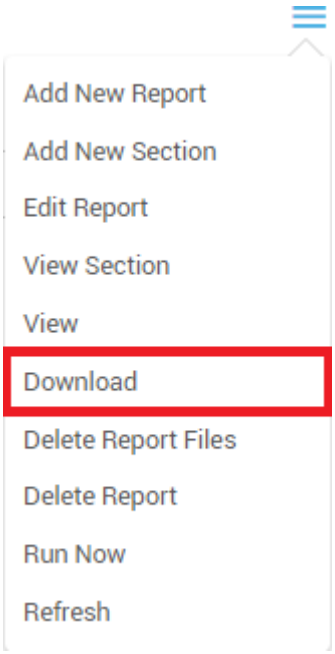
Information Portal Export

This option will allow the user to export the report to XLS format from the information portal, as shown in the screenshot below.



6. Download

It will download the selected report. After a reports gets generated and posted to information portal the same can be downloaded by clicking on the Download link under right menu icon, as shown in the screenshot below:

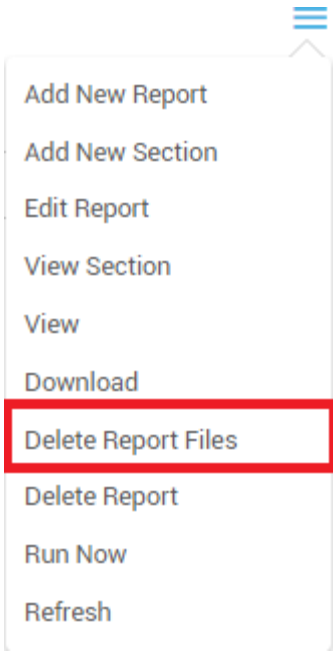


Upon clicking Download the report gets downloaded in .XLS format as shown in the screenshot below.

	A	B
1	**Item**	**count**
2	Windows 7 Professional, 64-bit	27
3	Windows 8 Professional, 64-bit	1
4	Windows 10 Professional, 64-bit	4
5	Windows 8.1 Professional, 64-bit	3
6	MAC OS	13
7	Windows 8.1 Enterprise Edition, 32-bit	2
8	Windows 10 Single Language, 64-bit	1
9	Windows 7 Professional, 32-bit	2
10	Linux "Ubuntu"	2
11	Windows 7 Home Basic Edition, 32-bit	1
12	Windows 7 Enterprise Edition, 64-bit	2
13	Windows 7 Ultimate Edition, 64-bit	1
14	Grand Total	59

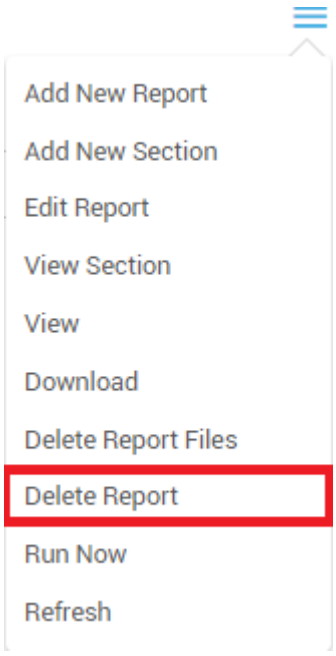
7. Delete Report Files

We also have an option to delete already existing report files. In order to do the same, select an existing report >> from the right side menu "Delete Report Files" as shown in the screenshot below.



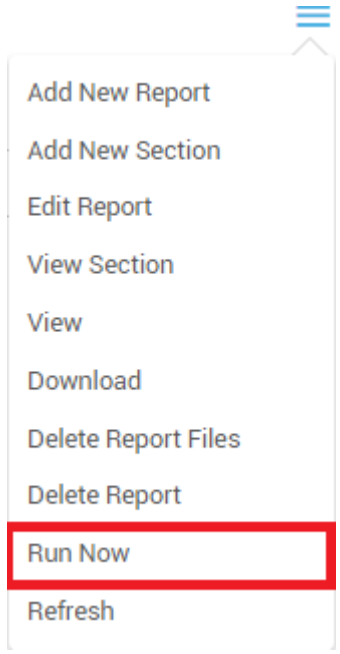
8. Delete Report

We also have an option to delete an already existing report. In order to do the same, select an existing report and from left menu click on "Delete Report" from the right menu as shown in the screenshot below.



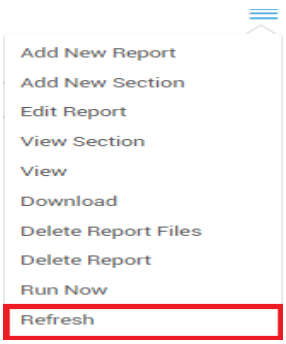
9. Run Now

Without waiting for the report to run at the scheduled time, we can run the report on-demand. In order to achieve the same, select a report and click on "Run Now" option:



10. Refresh

It will refresh the page.



Annexure

Software Distribution

Nanoheal provides a super effective feature to distribute any kind of file across the network. The file can be a software, document file or can be any kind of script. The Nanoheal Software Distribution not only supports distribution but also supports execution.

Following are the features which Nanoheal Software Distribution supports:

1. **Real-time distribution**: NH software can distribute files on real-time. Real-time means if any machine is online then file will be distributed on that device at that moment. In case the device is offline, the file will be distributed on device at that moment it gets online. In this case the distribution rate of any action is higher and faster.

2. **Pre/Post Distribution Check**: NH supports pre-and post-installation check as well. If an administrator wants to distribute Microsoft office on a group of machines, then a check can be applied to ensure no Office version is installed on a machine which already has one. Not only software, Software Distribution can be configured to check for Microsoft patches, software versions and files.
In case of post distribution check, an Admin can configure packages to distribute a file and **success** will be reported only when file is detected on the device which is configured in the POST distribution check field.

3. **Platform Independent**: NH Software Distribution module is a platform independent module. This module supports all kind of platforms like Windows, Android, MAC, Linux and iOS

4. **Amazon CDN and FTP support**: NH Software Distribution module supports both Amazon and enterprise FTP to distribute software's. It makes it easier for the administrator to distribute files form any nearby accessible location.

5. **Enterprise Play Store**: NH Software Distribution provides an enterprise play store for Android and iOS devices where software's will be available on Device by itself, and an admin can configure all important applications on the play store.

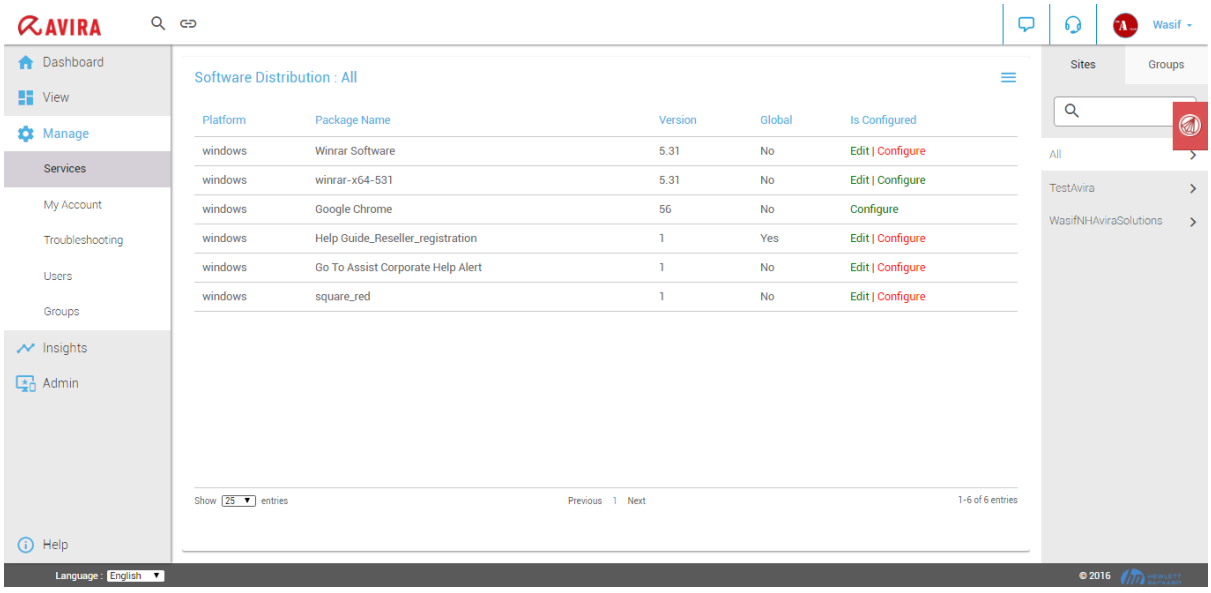
6. **Audit Logs**: Nanoheal provides a complete picture of success and failure of any package. It keeps providing the administrator with a complete picture about status of any Package. For example, if the administrator has distributed a package

on a site with 100 machines- the status will be displayed in detailed format.

Nanoheal Software Distribution modules has many other features, all these features make this module efficient to take care all user needs

The EXE to be distributed is uploaded (to FTP /servers) by giving the path of the executable. The executable is to be saved at a specific location and the validation for successful distribution is done by confirming the presence of the executable at the path mentioned by the engineer. Similarly, for execution after distribution - firstly the path is specified to pick the executable and then the validation is done at the location where the executable after installation is saved.

We can navigate to Software Distribution from left pane Manage > Services > System Management > Software Distribution. Upon clicking Configure for Software Distribution, the screen below appears:



Following are the options available in Software Distribution section:

1. FTP/CDN Configuration

2. View Software Details

3. Add New Package

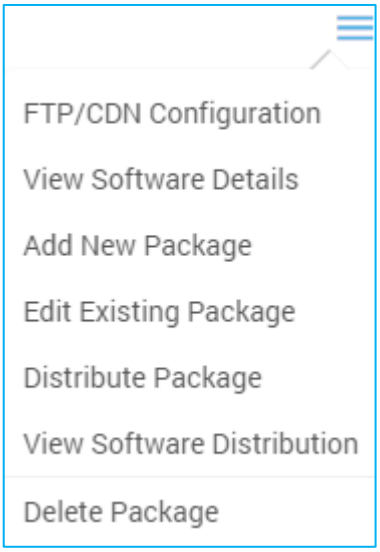
4. Edit Existing Package

5. Distribute Package

6. View Software Distribution

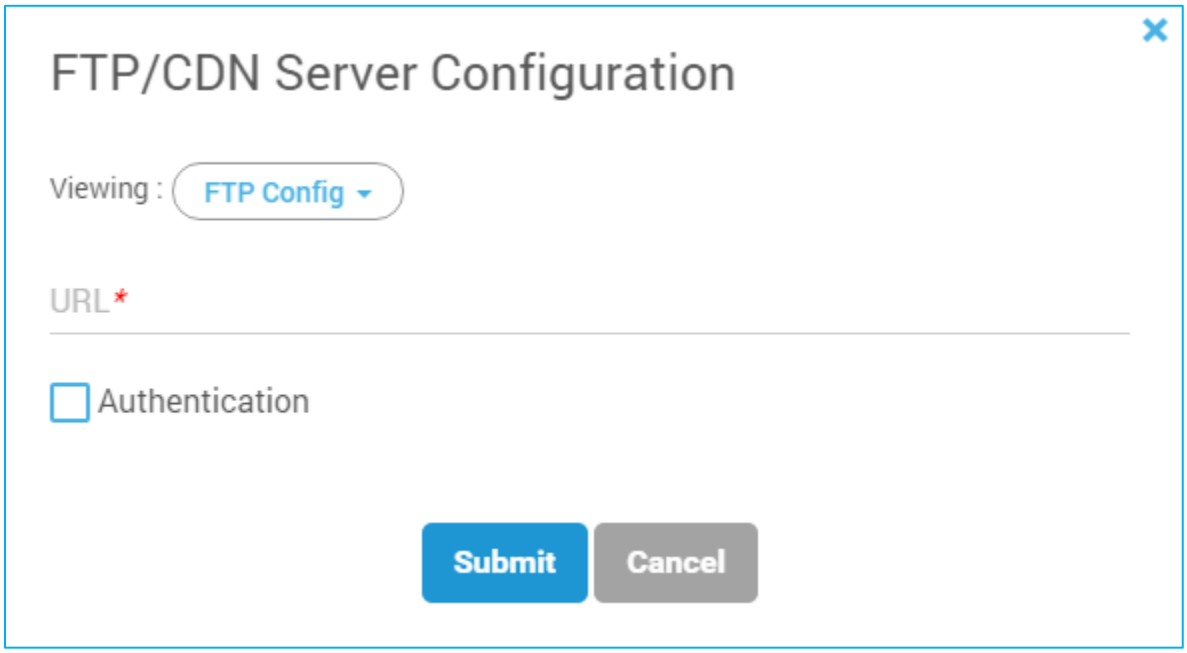
7. Delete Package

As shown below:

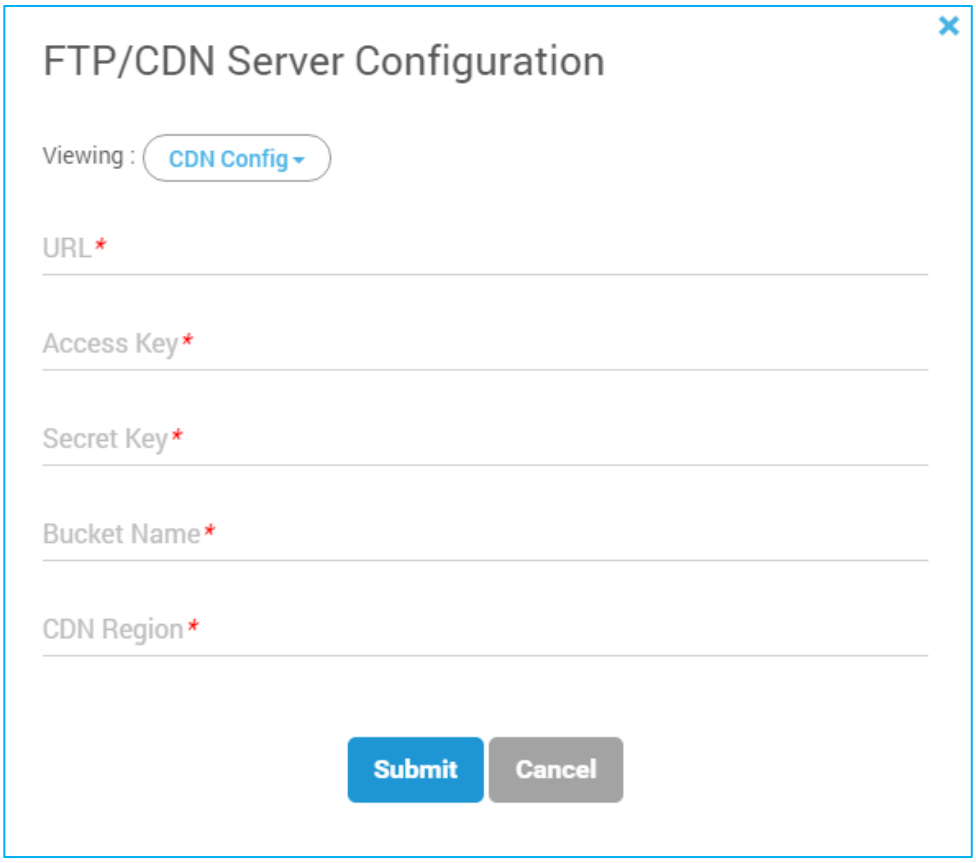


FTP/CDN Configuration

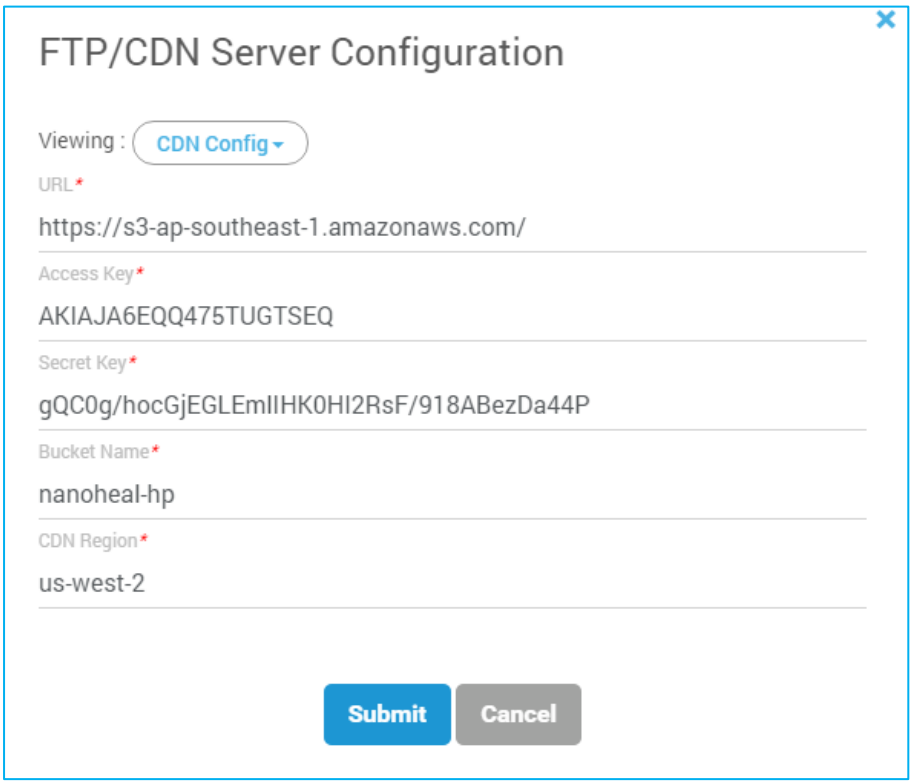
The first available option is "FTP/CDN Configuration".



In order to distribute a file using the Software Distribution (SWD), we have to configure either FTP or CDN locations to upload file / folders for distribution. This can be done using the screen above. For FTP, the user needs to enter the. For CDN, we have to provide URL, Access Key, Secret Key, Bucket name, CDN Region and click on "Submit" as shown below. Configurations get saved accordingly.

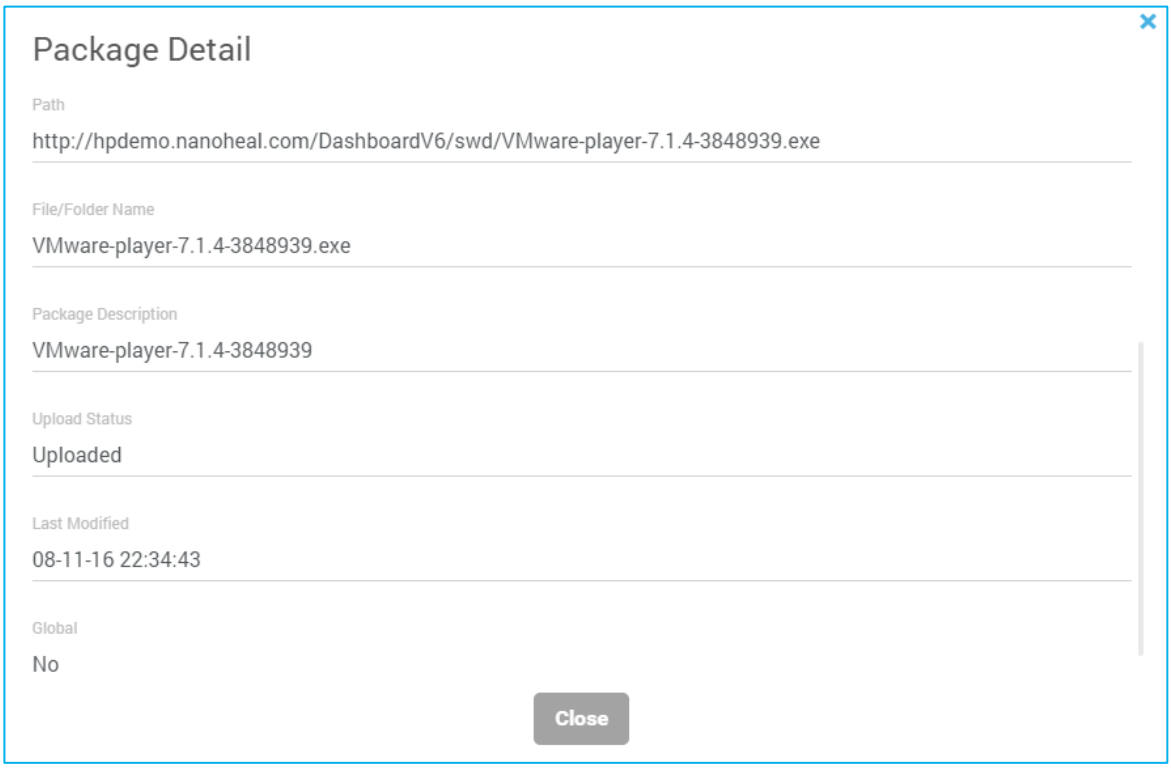


Sample CDN Configuration is shown below:



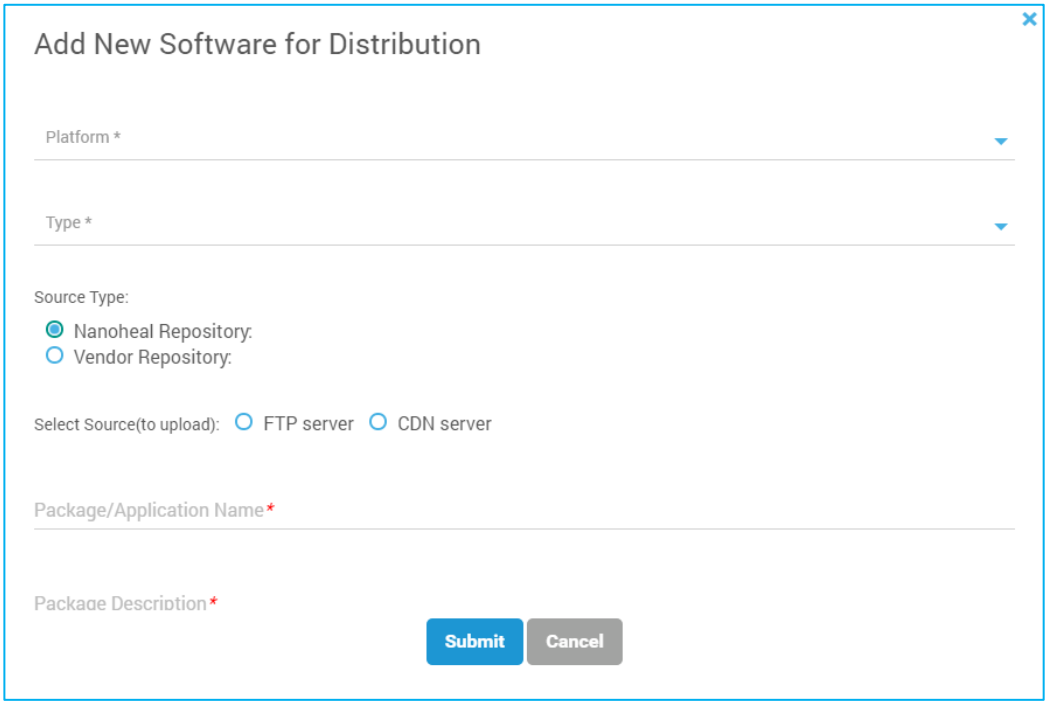
View Software Details

By selecting a software package and clicking on "View Software Details" under the menu on the right - the package details window opens up in viewable format as shown in the screenshot below.

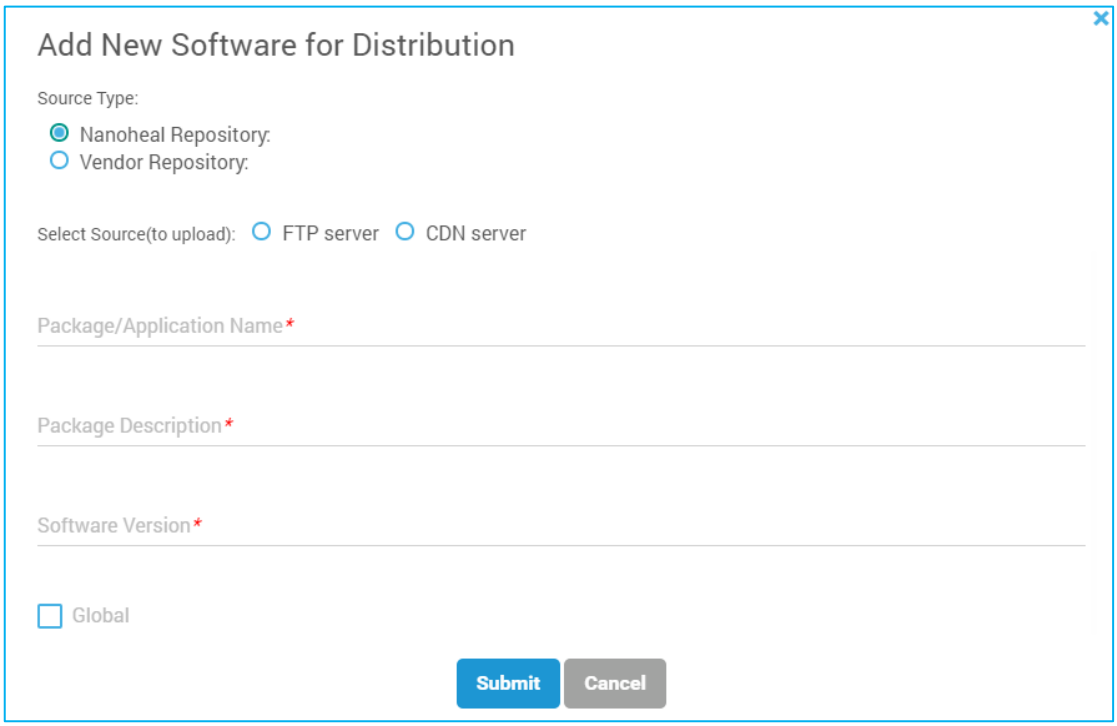


Add Package

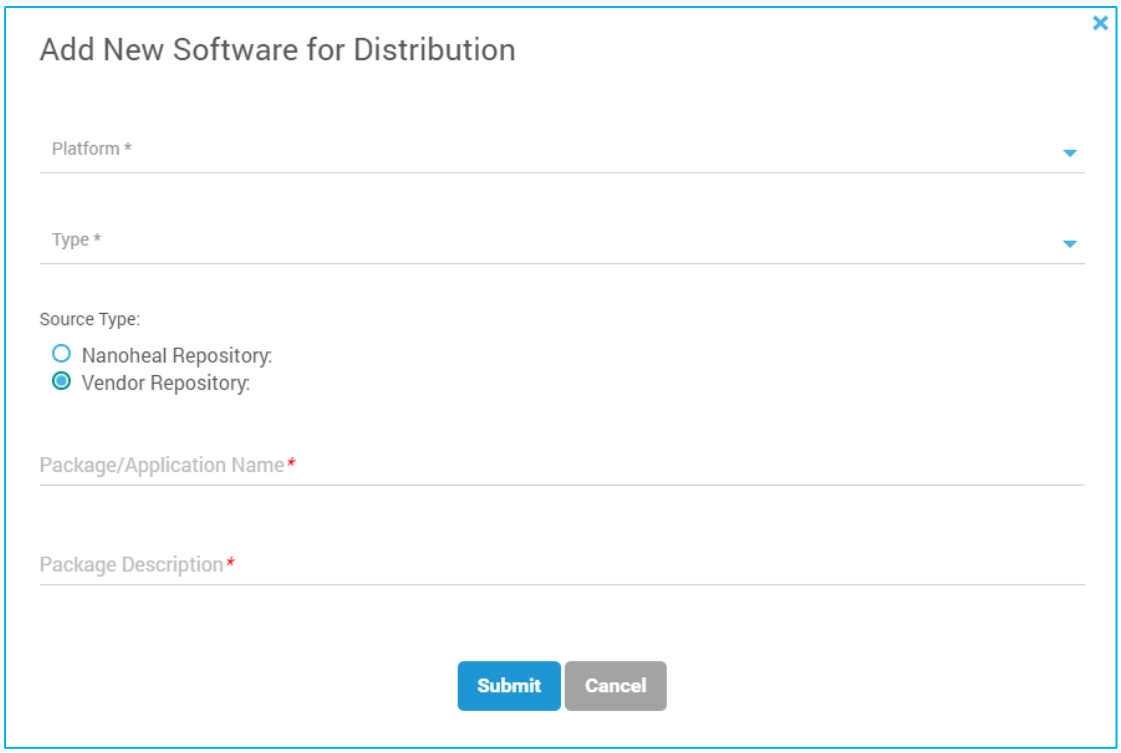
Upon clicking "Add Package" from the right menu the user can create a software package. This is configuration to distribute any file / folder.



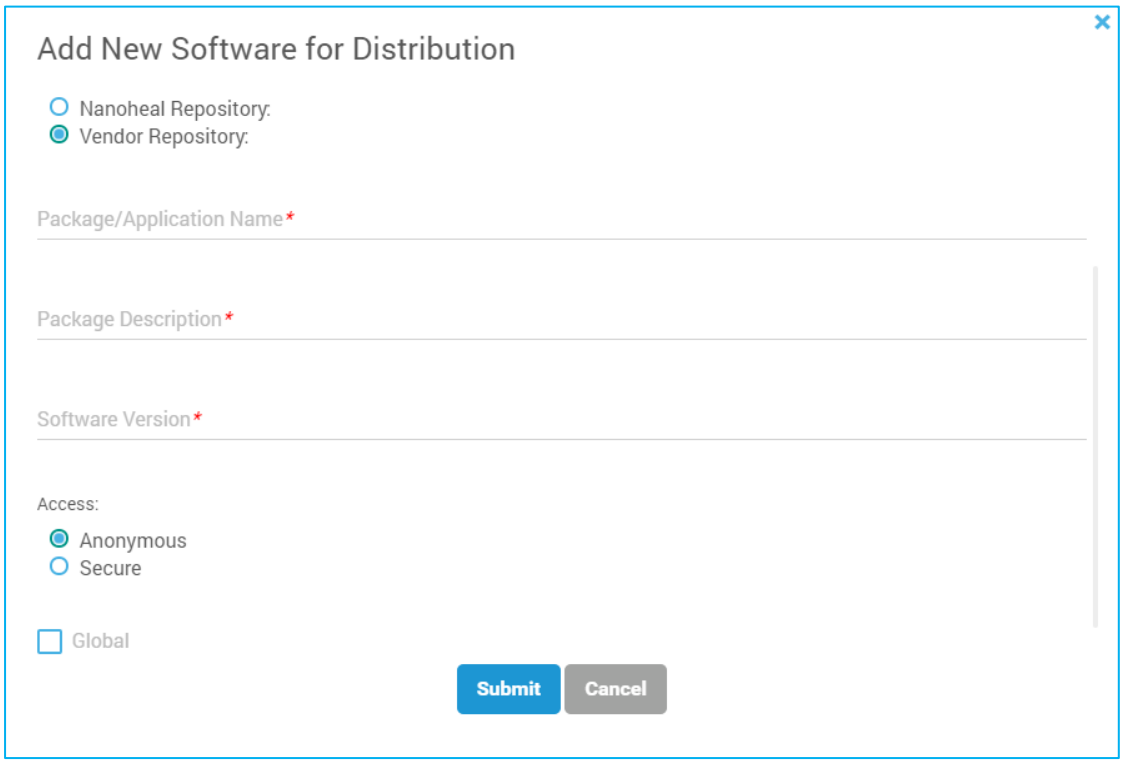
Sample Screenshot for Nanoheal Repository Fig (1)



Sample Screenshot for Nanoheal Repository Fig (2)



Sample Screenshot for Vendor Repository Fig (3)



Sample Screenshot for Vendor Repository Fig (4)

Nanoheal Repository

As shown in the screenshots above, the user has to enter the following details for Nanoheal Repository:

- **Platform**: User has to choose the platform. Windows / Android / iOS / MAC / Linux
- **Type**: User has to select the type. Distribution is for a file or for a folder
- **Source Type**: Source Type to be chosen as Nanoheal Repository
- **Select Source (to upload)**: FTP server or CDN Server
- **Browse**: Browse for file/folder
- **Select from Repository**: To select the already existing packages available in CDN
- Enter **Package / Application Name, Package Description, Software Version**
- **Distribute**: Distribution Path, Distribution Time & Distribution Validation Path
- **Pre-Distribution Check**: File or Software Name or Registry
- **Global:** Global or Local Package

After entering all the details, "Submit" will create the software package for Nanoheal Repository.

Vendor Repository

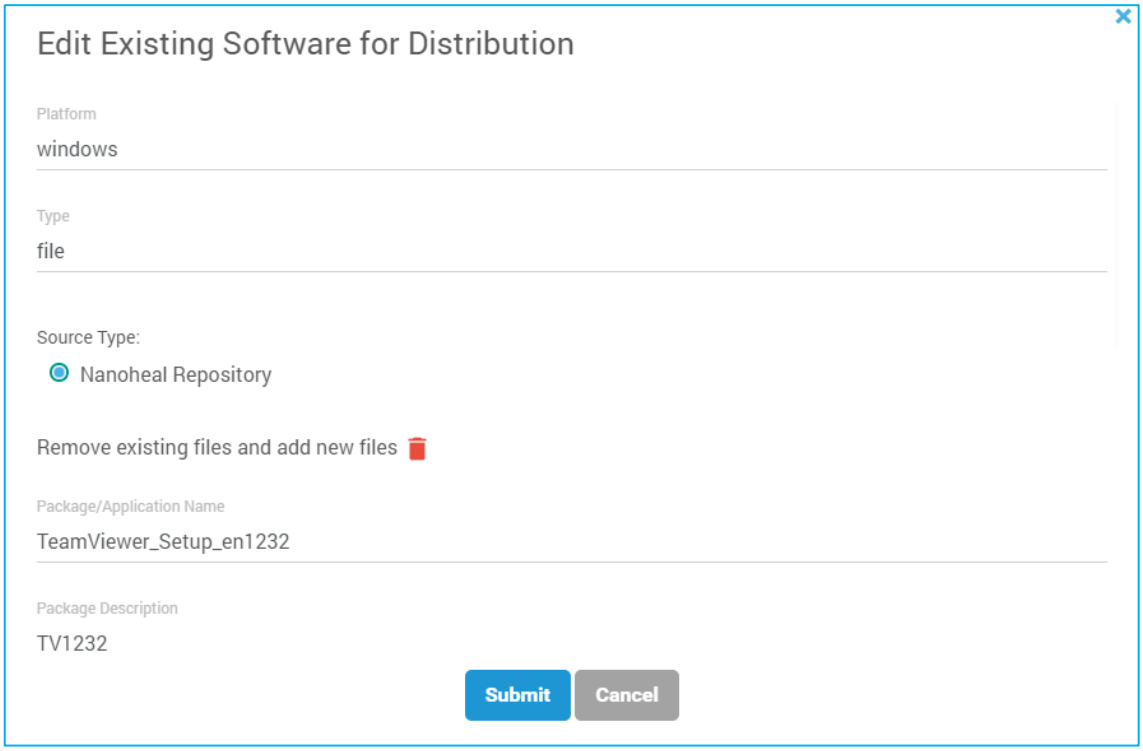
As shown in the screenshot above, user has to enter following details for Vendor Repository:

- **Platform**: User has to choose the platform. Windows / Android / iOS / MAC / Linux
- **Type**: User has to select the type. Distribution is for a file or for a folder
- **Source Type**: Source Type to be chosen as Vendor Repository
- **Select Source (to upload)**: FTP server or CDN Server
- Enter **Package / Application Name, Package Description, Software Version**
- **Access**: Access will be having two options namely, Anonymous & Secure. For Secure, we need to enter the Username, Password & Domain

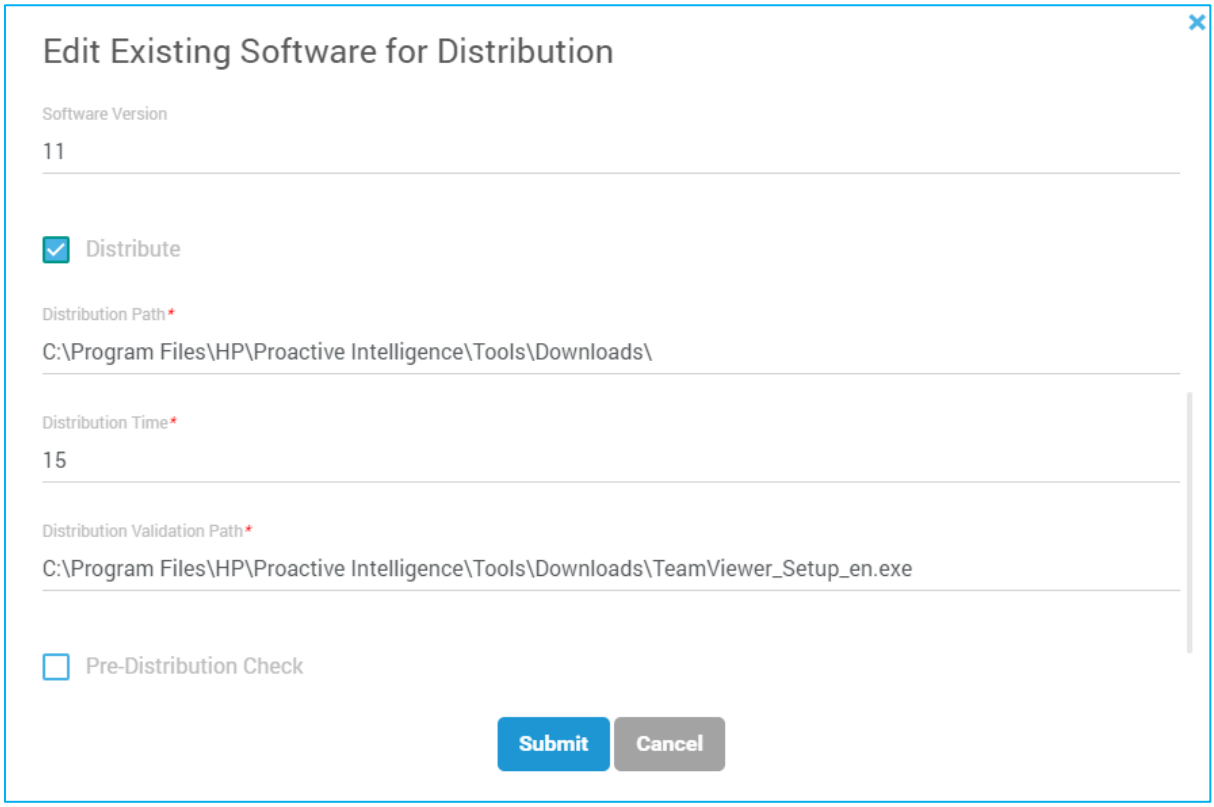
After entering all details, "Submit" will create the software package for Vendor Repository.

Edit Package

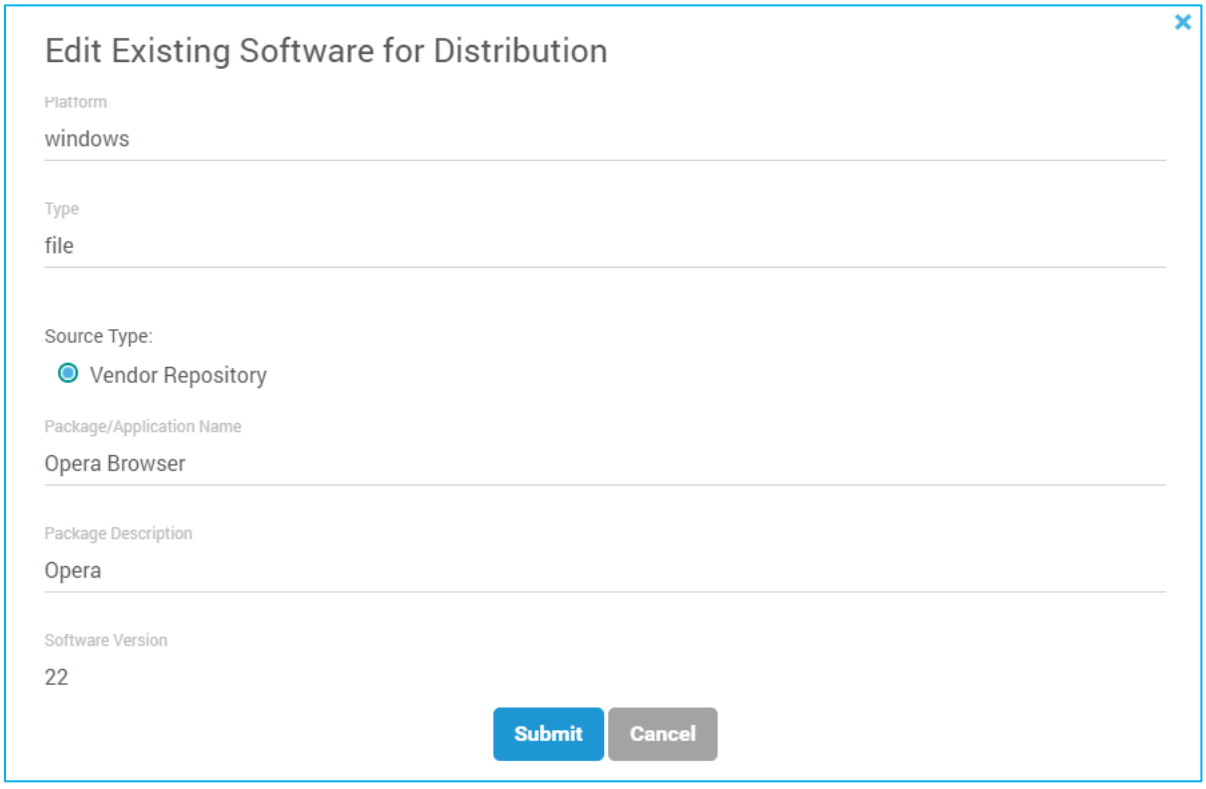
By selecting a software package and clicking on "Edit Package" users can edit the details as shown in the screenshot below.



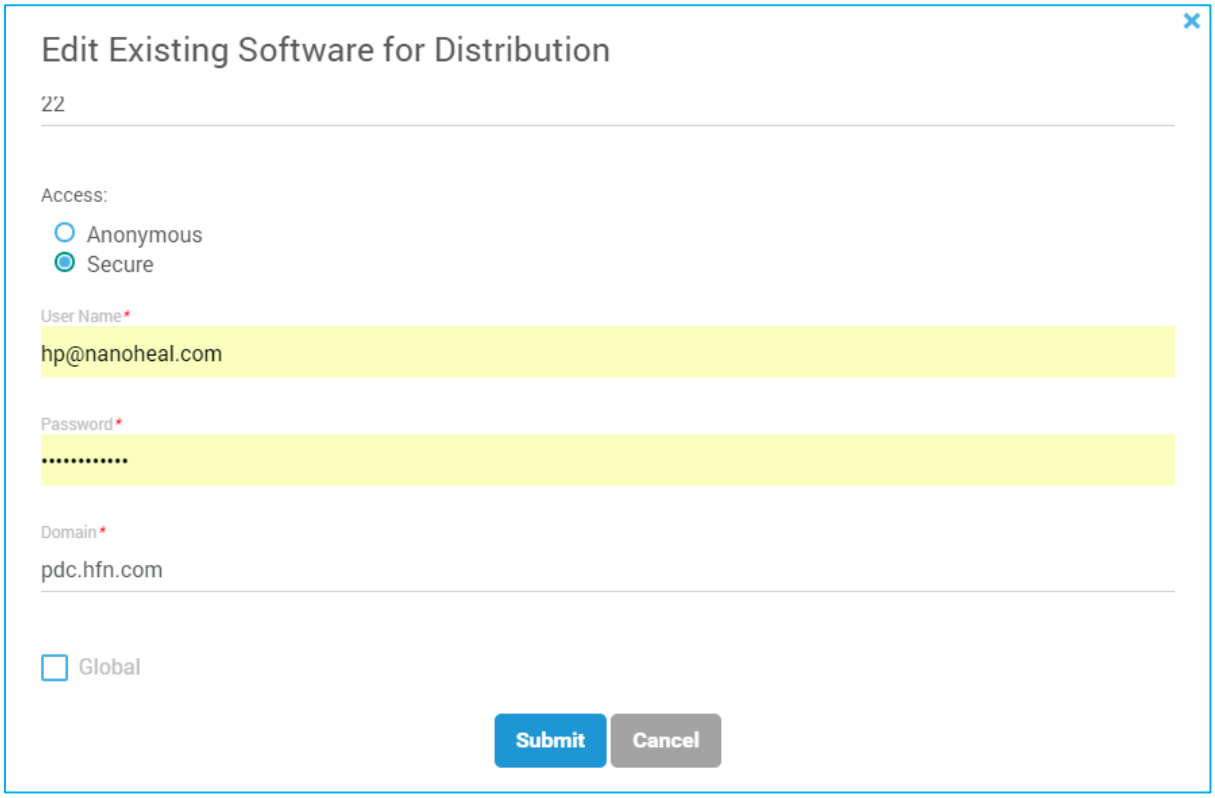
Sample Screenshot for Edit Nanoheal Repository Fig (1)



Sample Screenshot for Edit Nanoheal Repository Fig (2)



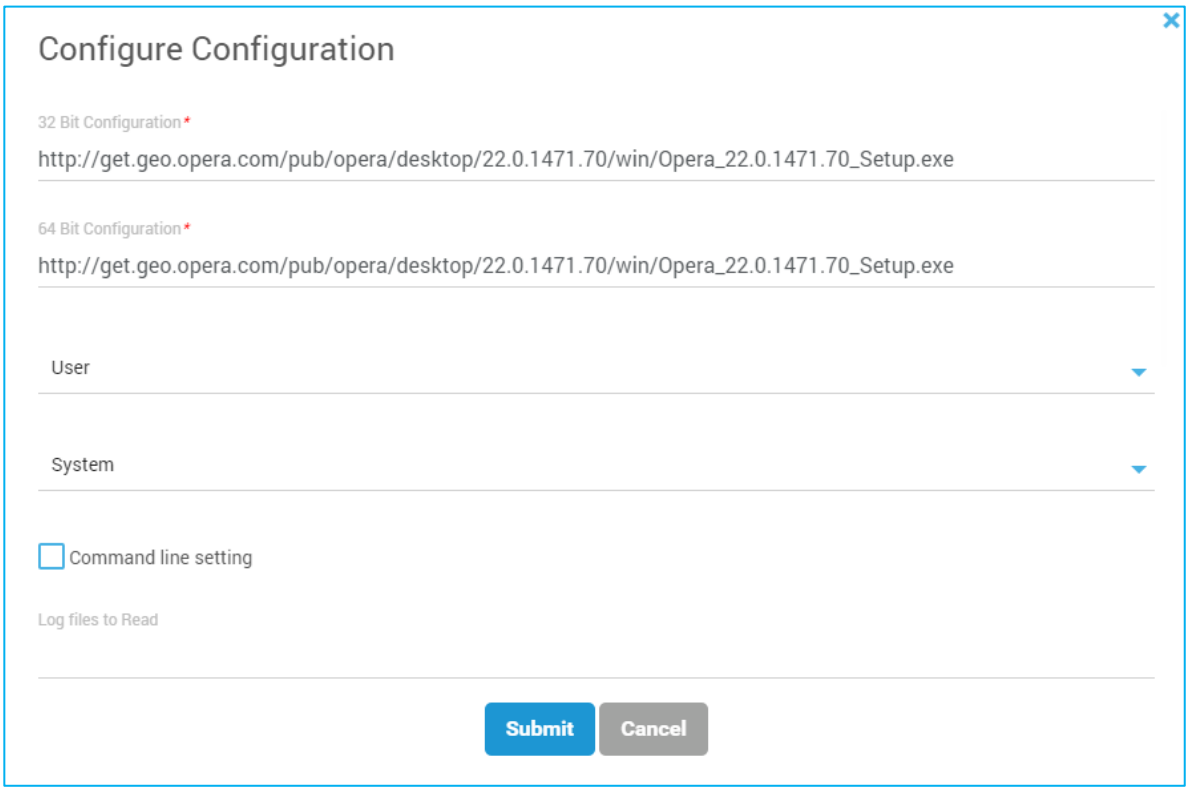
Sample Screenshot for Edit Vendor Repository Fig (3)

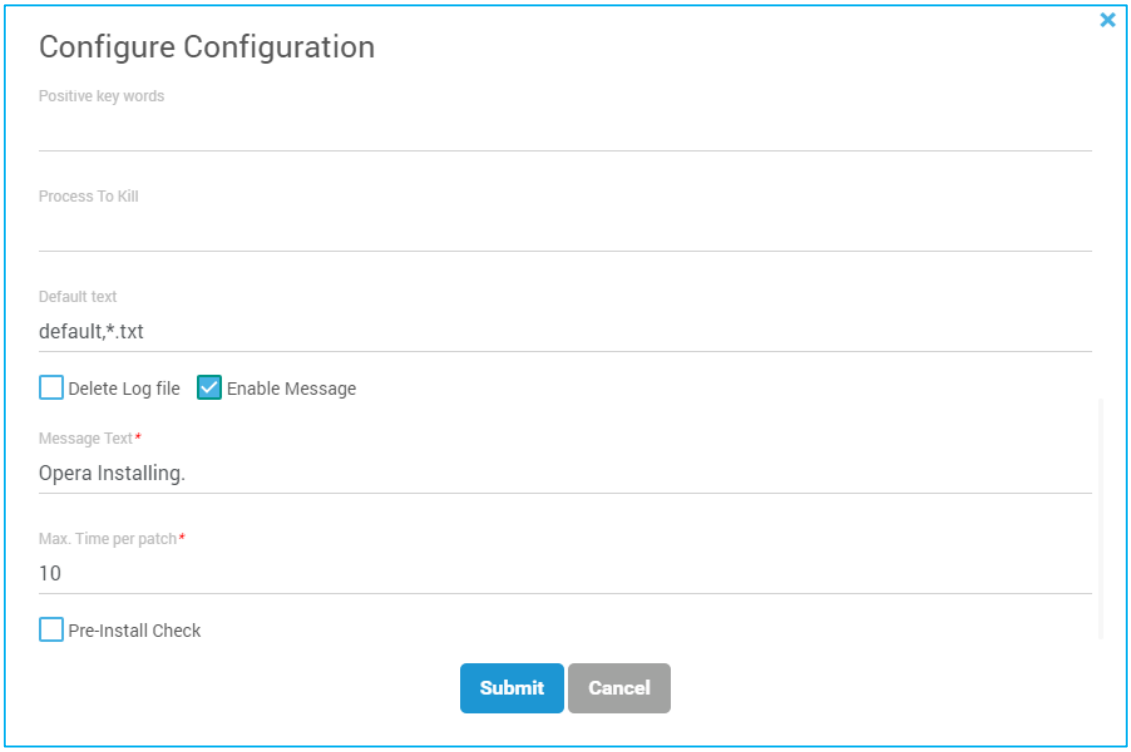


Sample Screenshot for Edit Vendor Repository Fig (4)

Configure Configuration for Vendor Repository

After adding Vendor Repository - Software Package, the user needs to click on 'Configure' text link from the 'Is Configured' column. By clicking this option, the user can configure the configuration for Vendor Repository as shown in the screenshots below.


Configure Configuration
32 Bit Configuration*
http://get.geo.opera.com/pub/opera/desktop/22.0.1471.70/win/Opera_22.0.1471.70_Setup.exe
64 Bit Configuration*
http://get.geo.opera.com/pub/opera/desktop/22.0.1471.70/win/Opera_22.0.1471.70_Setup.exe
User
System
Command line setting
Log files to Read
Submit
Cancel


Configure Configuration
Positive key words
Process To Kill
Default text
default,*.txt
Delete Log file
Enable Message
Message Text*
Opera Installing.
Max. Time per patch*
10
Pre-Install Check
Submit
Cancel

Initially 'Configure' text will be in Red as shown in the screenshot below.

Once Configuration is completed & the Submit button is clicked, the Configure text colour will change to Green as shown here

Pre-Install Check

The user can do a Pre-Install Check with the following options:

File

The path of the file which can be used for Pre-Installation Check

Software Name

The Software Name, Software Version, Knowledge Base & Service Pack

Registry

The Root Key and the Sub key for checking the Pre-Installation

Pre-Install Check can be performed on either the Nanoheal Repository or the Vendor Repository.

Configuration fields are explained below:

The table below describes each field in detail. And each field should be separated by a line.

Field	Field Name	Field Values and Description
1	32Link:	32Link is used to configure 32 bit OS supported patches. The user can add multiple patches by using next line delimiter
2	64Link:	64Link is used to configure 64 bit OS supported patches. The user can add multiple patches by using next line delimiter
3	Session	If the user wants to execute the patch in the background then it should be Interactive else User.

4	Mode	This parameter decides the execution of the exe. For example, the user can use create process or shell execute or with UAC. The user can use 1 to 12 to configure it. System – 1, User – 4, Administrator – 6
4	Positive key words:	Positive: is used to configure button names. So that client can auto click on the buttons whenever any window contains this button. Multiple button names can be configured by comma ',' delimiter. And complete configure should be in the same line of the **Positive** field
5	Negative key words:	Negative: this parameter has been retired. Hence, no need to configure it.
6	Log Files to Read	This parameter is used to configure the log file path. After patch completion it will read the log file and add it into the event. The user can configure multiple log file path by using next line. If there is one single path then it should be in the next line of **LogFile:** field.
7	Default text:	Update later
8	Enable Message:	By using this parameter, the user can handle individual patches toast message. When this parameter is selected the toast message will display for the whole patch. If there is no need to display the toast message for a particular patch, leave the box unchecked
9	Message Text:	Update later
10	Max. Time Per Patch:	This field is for maximum time per patch. It should be numeric and unit is minute. The patch will be killed after this time.
11	Process To Kill:	This field is used to kill the process before the execution of the patch. The user can configure multiple processes name separated by ',' e.g. notepad.exe, cmd.exe, mspaint.exe.

Configuration sample of 32Link and 64Link field is as following:

e.g. **Enable/Disable,WindowType,URL/PATH,Session,APIMode,AppendCommand,CommandLine/DistributionPath,PreCheckMode,PreChecConfiguration,PostValidation,PacthDependency**

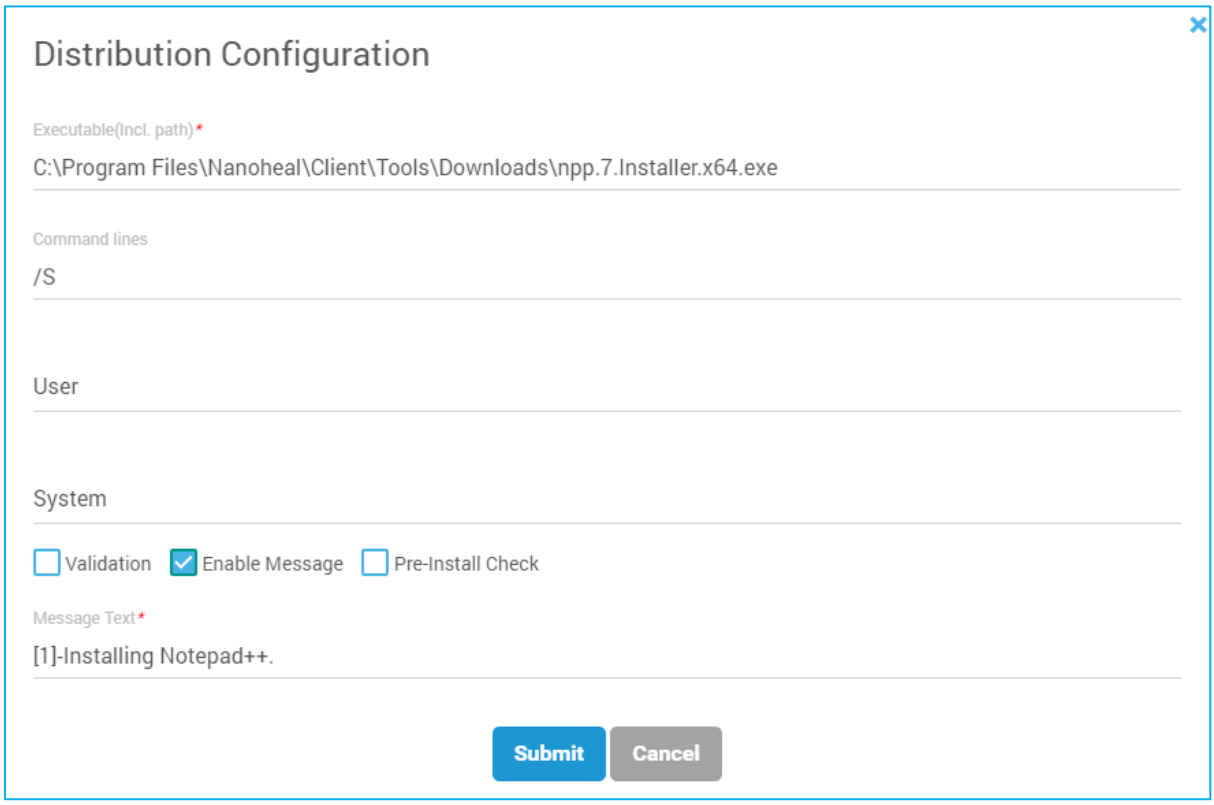
Detail of each filed as following tables

Field	Field Name	Field Values and Description
1	Enable/Disable	This field should be 1 otherwise the patch will not execute.
2	Window Type	This field should be NT for windows.
3	URL/PATH	This field can be a URL (HTTP/FTP/Shared location) or it can be local exe file path.
4	Session	If the user wants to execute the patch in background then it should be 0, else 1.
5	APIMode	This parameter decides the execution of the exe. For example, the user can use create process or shell execute or with UAC. The user can use 1 to 12 to configure it.
6	AppendCommand	There are five values to configure it.(0 or 1 or 2 or 3 or 4). 0= Will not append the process name with the command line 1= Process name will be append with command line for all OS 2= Only for XP Process name will be append with command line 3= Above Xp Process name will be append with command line 4= Will be configured for distribution of the file
7	CommandLine/DistributionPath	It can be a command line or distribution path based on APIMode
8	PreCheckMode	0 = For File Precheck 1 = For software name, version, KB, and service pack. 2 = For registry pre check 3 = Patch dependency
9	Pre Check Configuration	**This parameter is dependent on PreCheckMode.** 0=if PreCheckMode is 0 then it should be a File path e.g-> 1,NT,URL/PATH,Session,APIMode,AppendCommand,CommandLine/DistributionPath,0,C:\temp.txt Here if C:\temp.txt is exist then patch will not execute. 1=if PreCheckMode is 1 then it should be a software name version etc. e.g->

		1,NT,URL/PATH,Session,APIMode,AppendCommand,CommandLine/DistributionPath,1,SoftwareName#Version#KB#ServicePack 2=if PreCheckMode is 2 then it should be registry key e.g.->1,NT,URL/PATH,Session,APIMode,AppendCommand,CommandLine/DistributionPath,2,MainKey#SubKey#ValueName#ValueType#Value 3=if PreCheckMode is 3 then it should be a patch dependency number e.g.->1,NT,URL/PATH,Session,APIMode,AppendCommand,CommandLine/DistributionPath,3,100 100 is just for an example, it can be replaced with any number based on Patch Dependency value.
10	Post Validation	Format of Post Validation is as follows **ValidationMode#ValidationConfig** ValidationMode can be as follows = 0(File validation), 1(Registry validation) ValidationConfig depends on ValidationMode. If ValidationMode = 0 then validation Config should be a path of file. e.g. 0#C:\test.txt If ValidationMode = 1 then validation Config should be a registry path. Following is the format for registry configuration MainKey#SubKey#ValueName e.g. 1#1#SOFTWARE\Nanoheal\Nanoheal Client\Install#HFNload Main Key has the following values. HKLM = 1 HKCC = 2 HKCR = 3 HKCU = 4 HKU = 5 HKDD = 6 HKPD = 7 HKPT = 8 HKPN = 9
11	Patch Dependency	Patch Dependency is basically to skip the patch based on current patch [In case the user wants to skip the patch if current patch has been skipped] The user can configure any number in current patch, and the same number needs to be configured under dependent patch at pre-check configuration.

Distribute Configuration for Nanoheal Repository

After adding the Nanoheal Repository - Software Package, the user needs to click on 'Configure' text link from 'Is Configured' column. By clicking this option, the user can set the configurations for Nanoheal Repository as shown here.

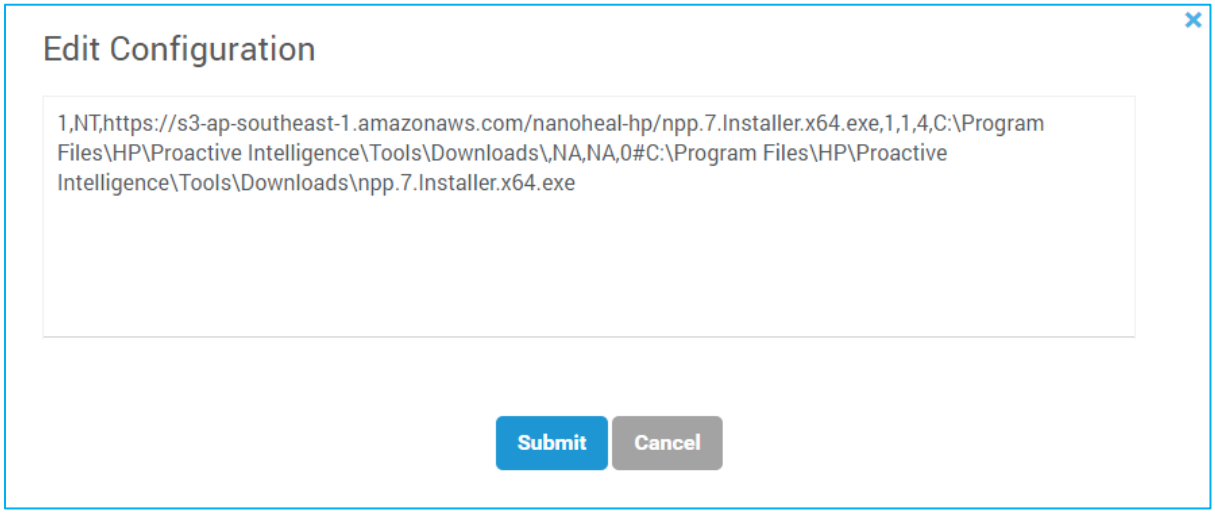


Configuration Post Validation for Nanoheal Repository

If any executables are configured from the Distribution Configuration pop up, then the user can also configure the Post validation by selecting the Validation checkbox and selecting either File or Registry.

Edit Configuration

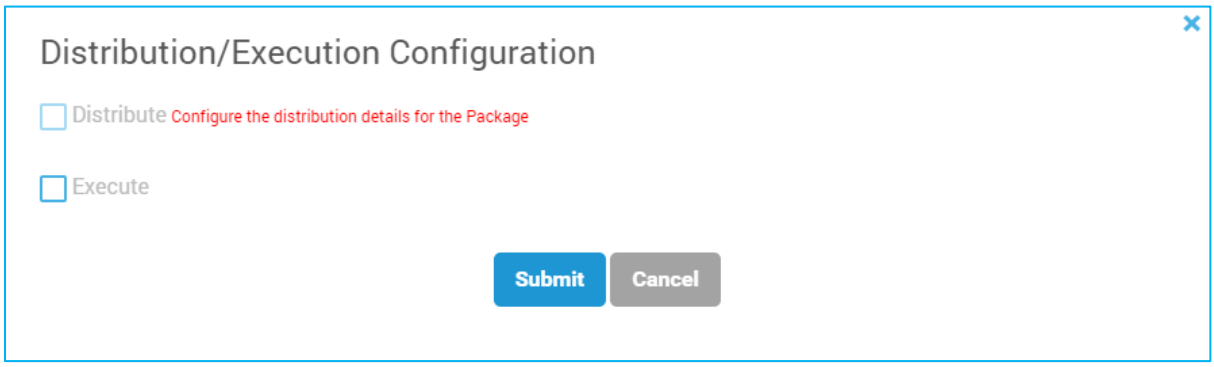
After clicking on submit from the Configure Configuration pop up, the Edit Configuration pop up will be seen as shown here-



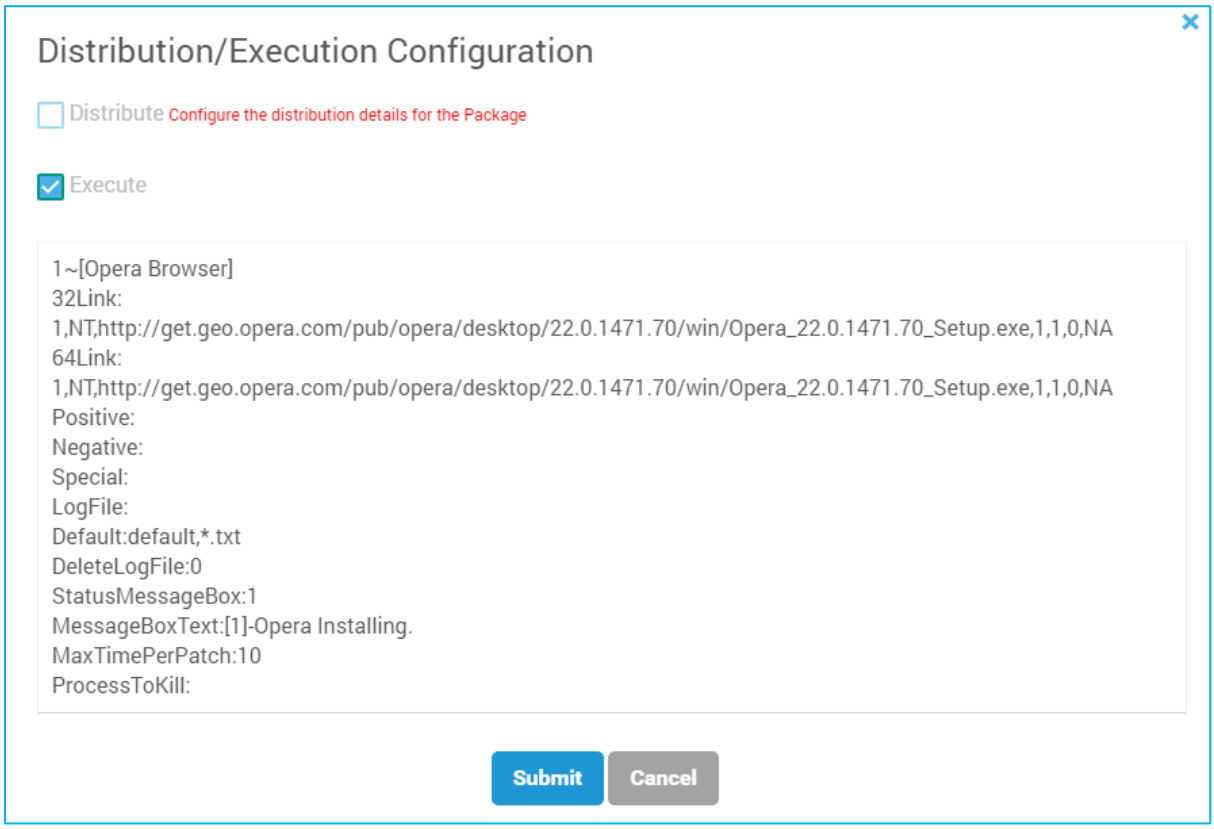
In the Edit Configuration window, the user can edit the configuration & save it before performing the software distribution.

Distribute Package

The actual operation of the 'Distribute' is performing the configuration of the executable file or any folder. Selecting a software package and clicking on "Distribute" will open the screen below:

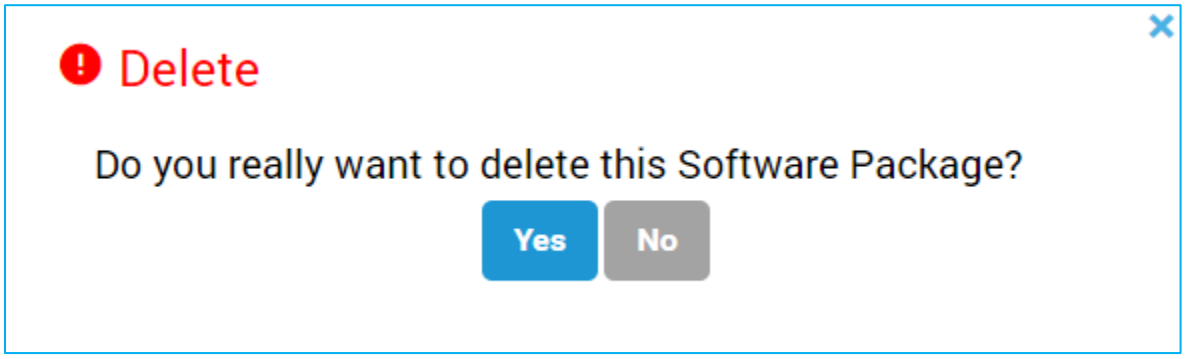


In the screen above, checking the box next to "Distribute" or "Execute" will show the screen below with configuration & will distribute / execute the particular file / folder to respective machines under specified location.



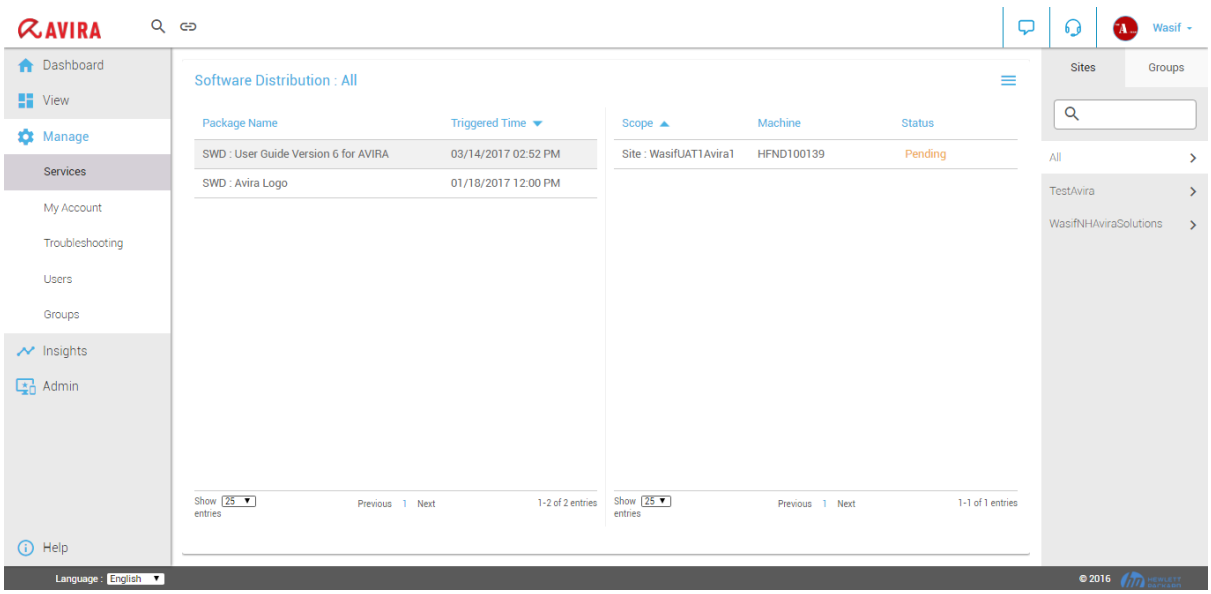
Delete Package

Selecting a software package and clicking on "Delete Package" will delete the particular software package as shown below.



View Software Distribution

This is the Audit screen of Software Distribution. All software packages for which user initiates the distribution / execution action on either All / Site / Machine / Group, entry will come into "View Software Distribution" as shown below:



As shown in the screenshot above, it will display the package name along with the Triggered Time & the name of the Agent who triggered the Software Distribution.

Clicking package name on the right side will display the details like Scope, Machine & Status (Completed (Green Colour)/Pending (Orange Colour) /Failed (Red Colour) /Unknown (Blue Colour)) as shown in the screenshot above.

Clicking "Completed" will show the event details pop up.

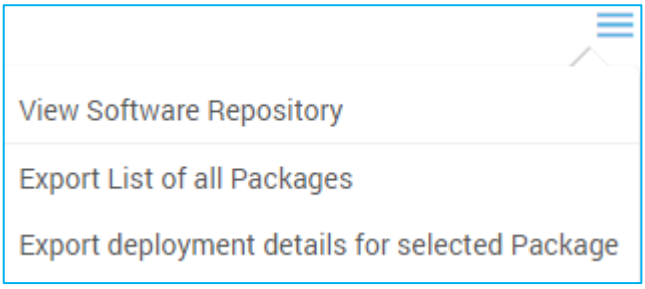
Export

Data can be exported from the View Software Distribution section.

Export can be performed in two ways.

1. Export List of all patches
2. Export deployment details for selected patch

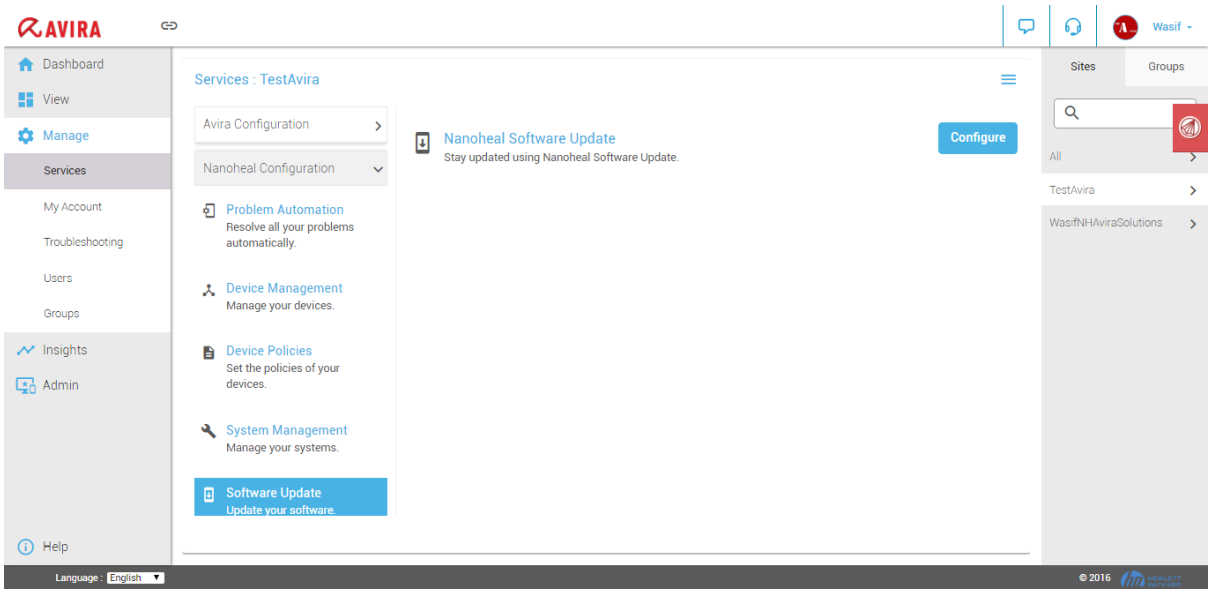
In order to export the data from view software distribution page – the user needs to click on the menu icon on the right hand side and select either of the two options as shown in the screenshot below.



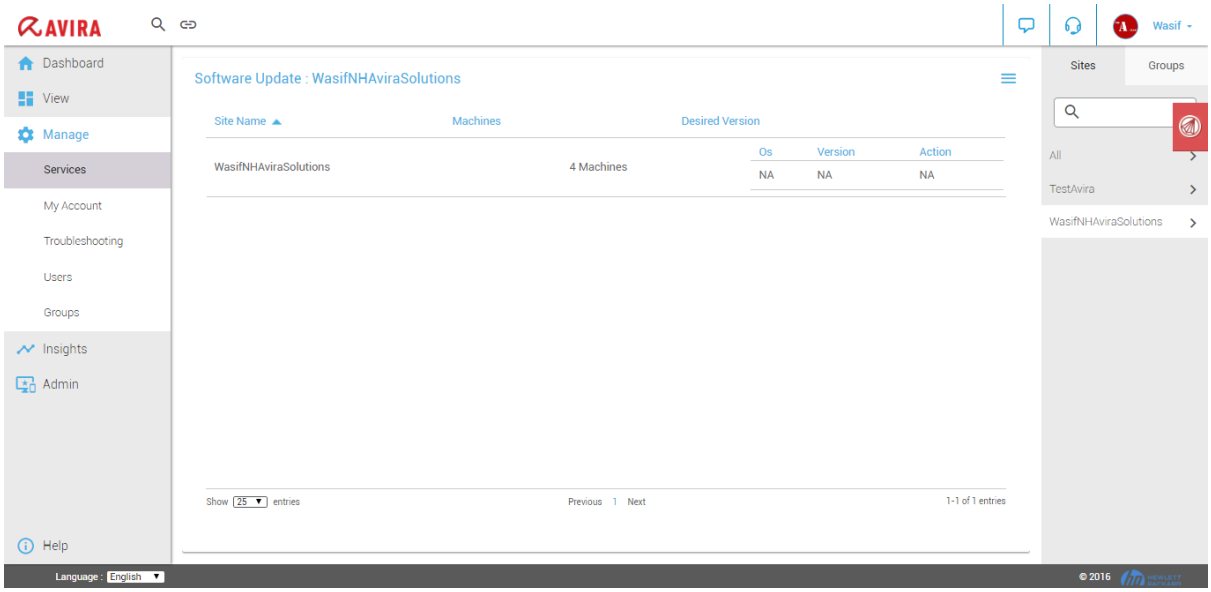
Software Update

Software Update screen will allow the user to auto-upgrade the Nanoheal software, if a new version of it is available.

Software Update is available under Manage >> Services >> Software Update >> Nanoheal Software Update.

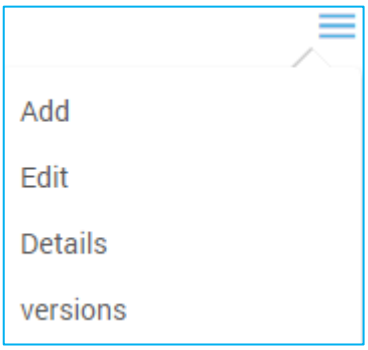


Clicking "Configure", shows the following



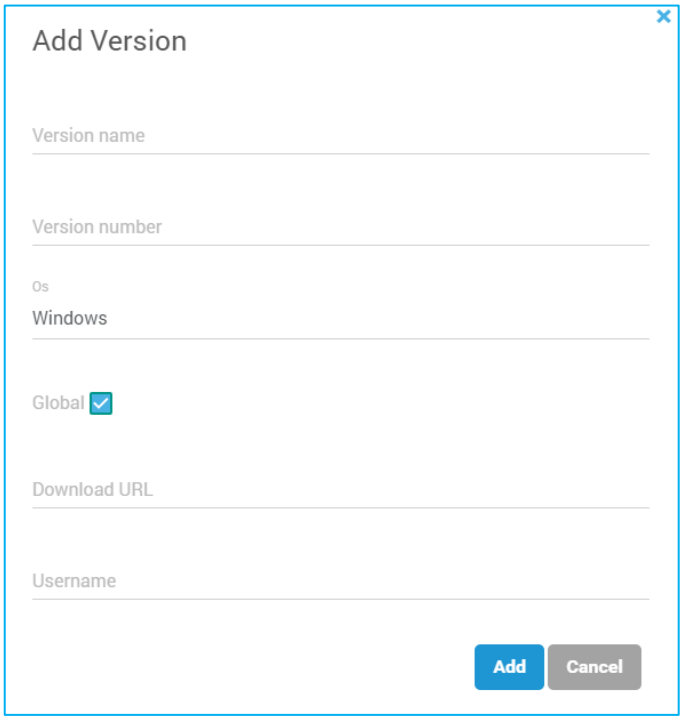
As shown in the screenshot above, the update screen will list out all the sites and machines that need to undergo (or already done) with Nanoheal auto-upgrade.

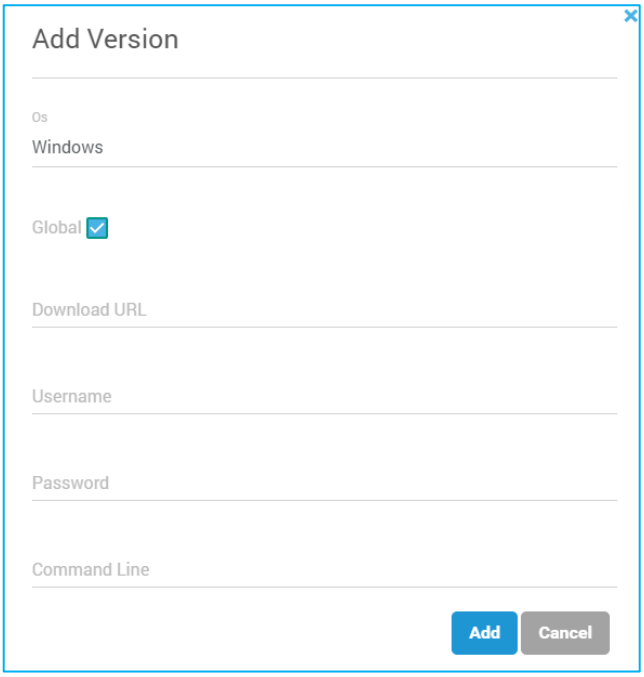
There are 4 options available in the menu of the Software Update screen. These options will be available to the user upon clicking the menu icon as shown in the screenshot below.



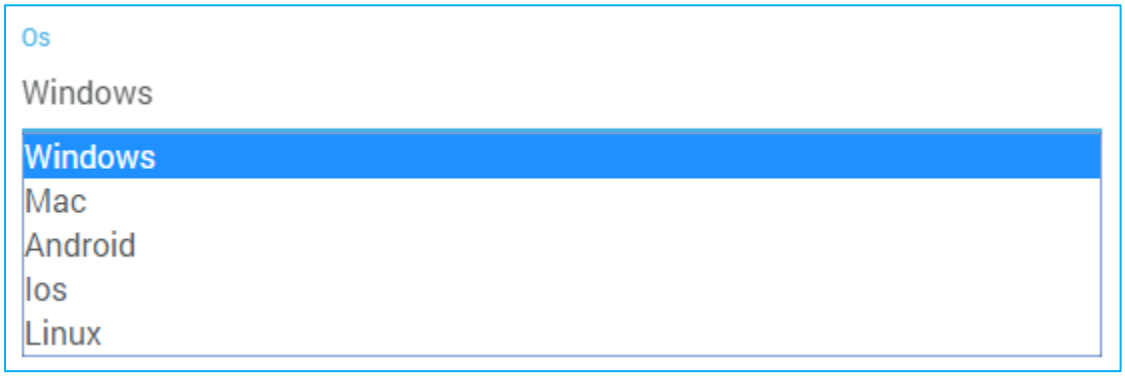
Add

Clicking on the Add link will display the following Pop up to add the Software Update Version.



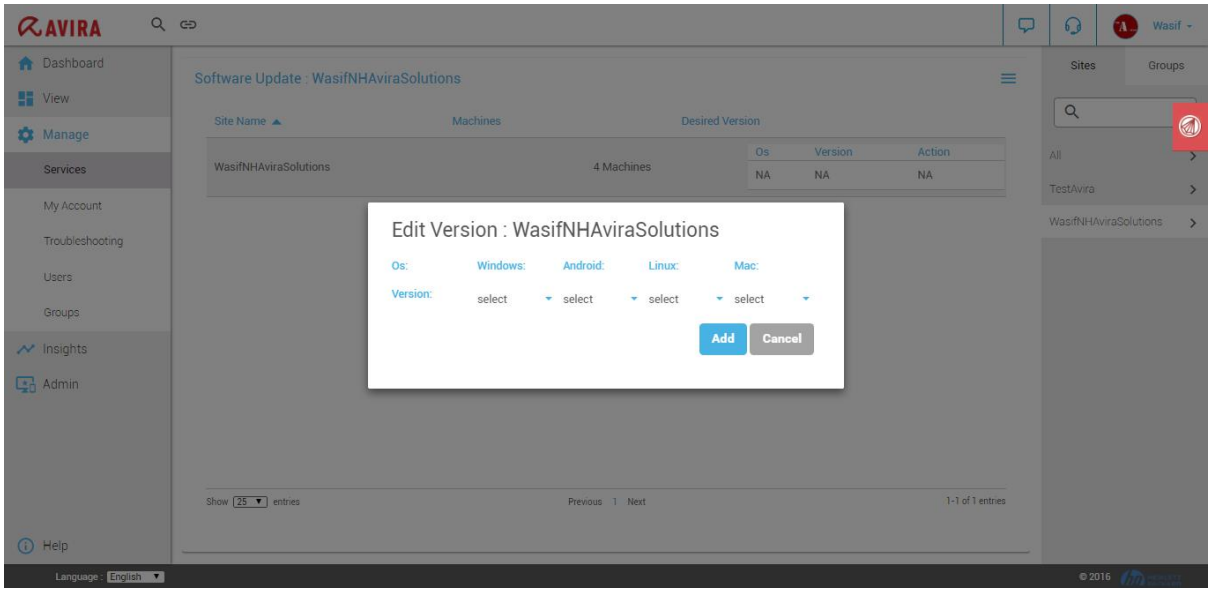


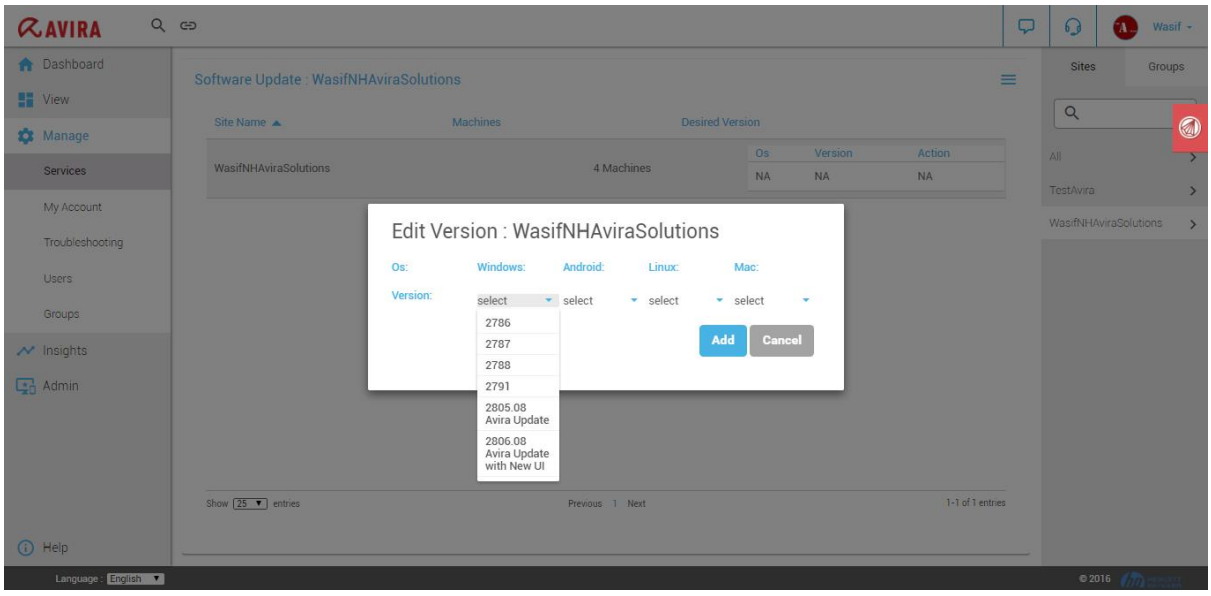
The user needs to fill all the required fields with valid data along with OS selection as shown below and then click on submit button to add the version.



Edit

Selecting a **site>Menu drop down> Edit** would show:

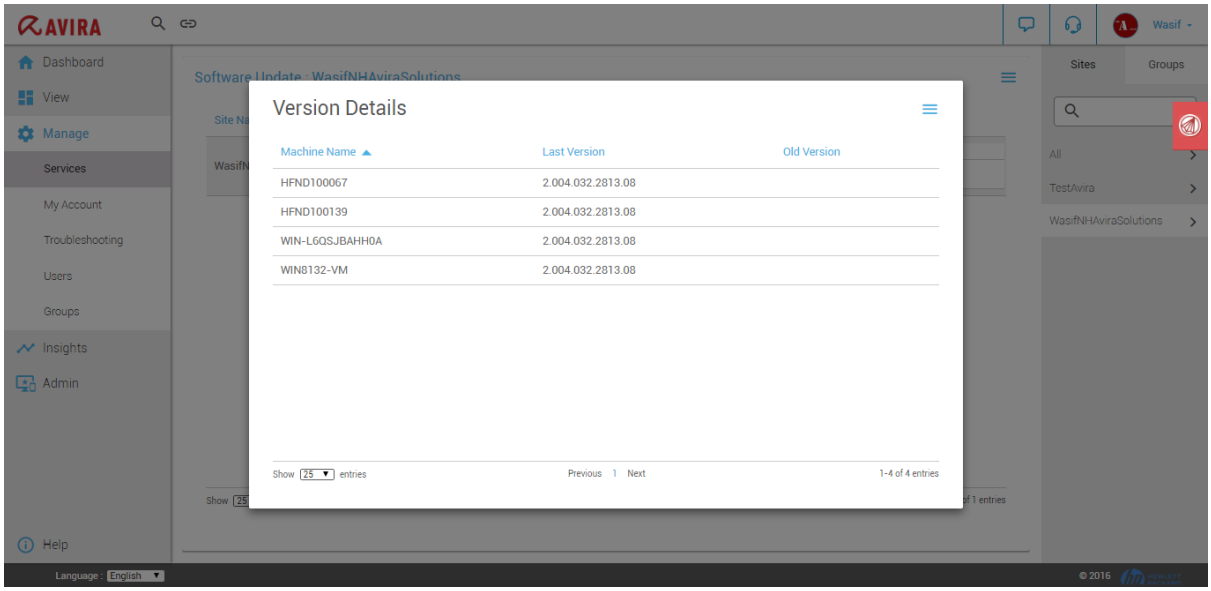




As shown in the screenshot above the Edit screen allows the user to choose a Nanoheal version for which the site / machine needs to be auto upgraded. Selection can be done based on type of Operating System of the machine which needs to be updated.

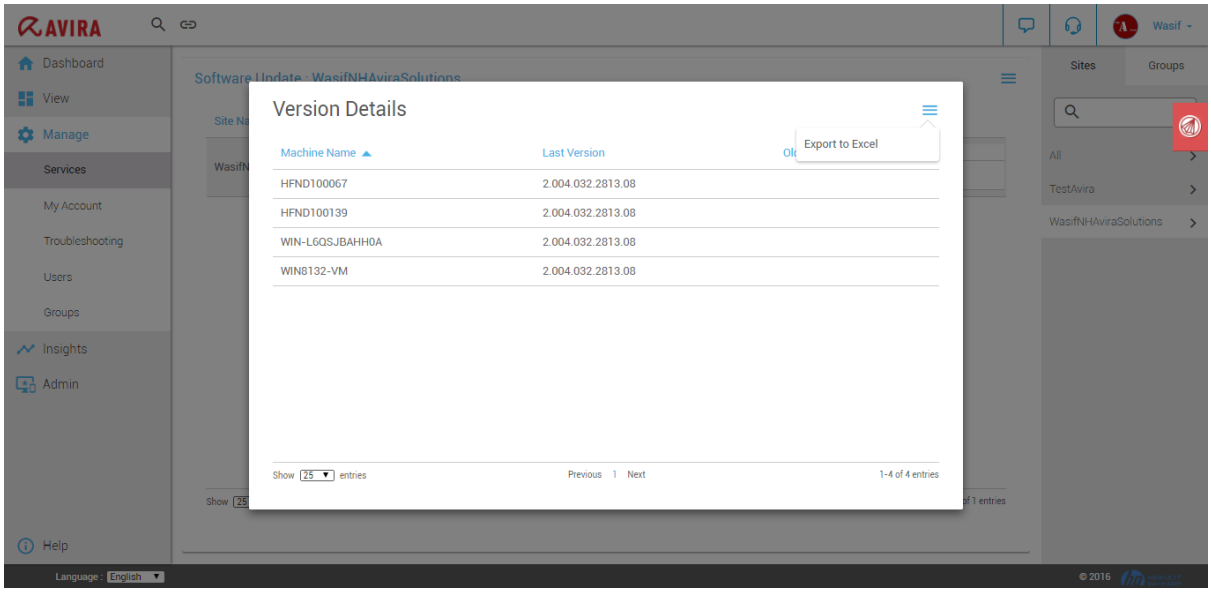
Details

Clocking on the Details link on the right menu brings up the Version Details pop up.



As shown in the screenshot above, version details pop up depicts the Old Version & Last Version of the Machine after auto update.

Version Details can also be exported by clicking on right menu >> Export to Excel:

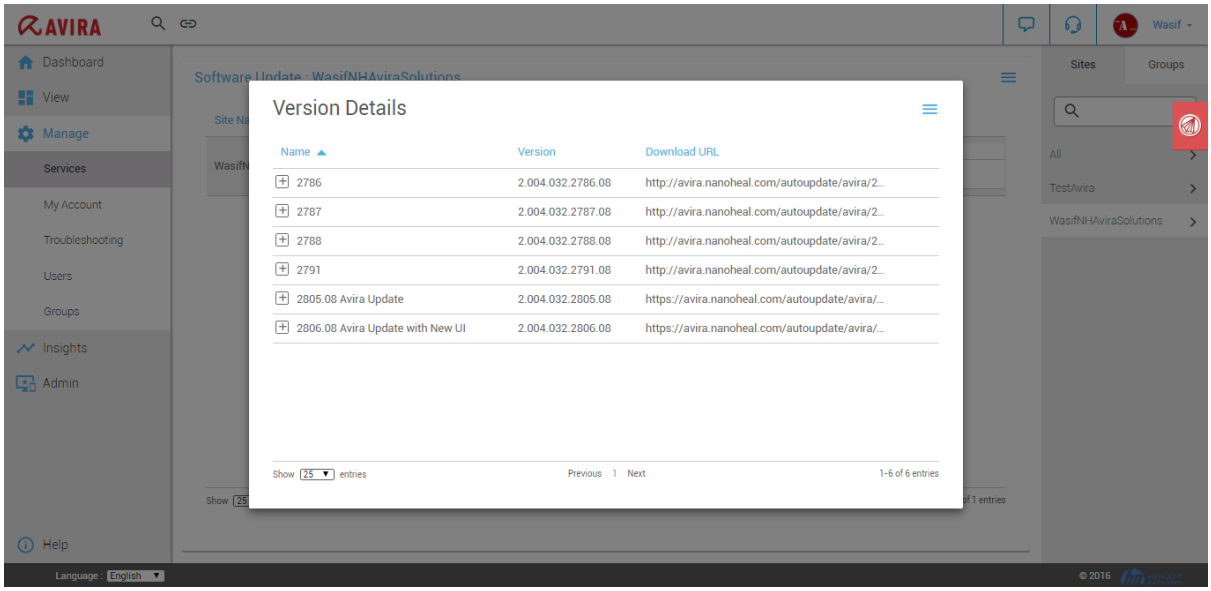


Sample Exported Version Details sheet is shown below.

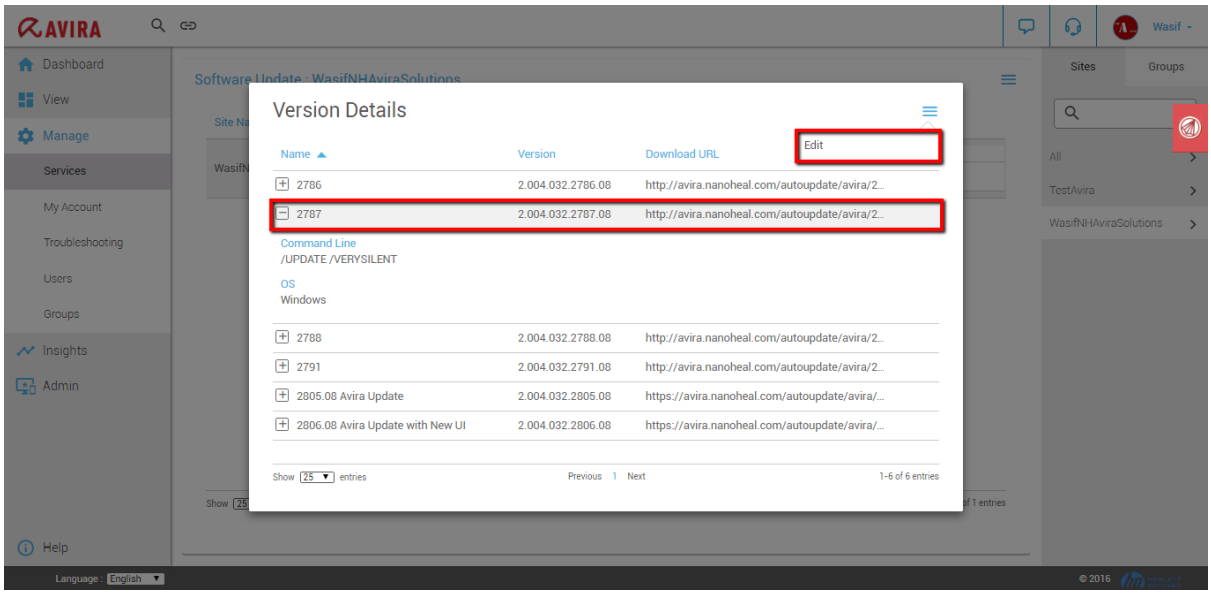
	A	B	C	D	E	F
1	**Machine Name**	**Last Contact**	**Last Version**	**Last Update**	**Old Version**	**New Version**
2	236FG32	10/27/2016 23:36:19	2.004.032.2766.11	09/27/2016 03:37:33	2.004.032.2766.11	2.004.032.2766.11
3	4D6FG32	10/27/2016 06:44:33	2.004.032.2766.11	09/02/2016 05:30:03	2.004.032.2764.11	2.004.032.2766.11
4	CPWQT77BG940	09/07/2016 10:30:06	2.004.032.2763.10	09/07/2016 10:30:06	2.004.032.2763.10	2.004.032.2766.11
5	D3C68R1	10/27/2016 07:28:45	2.004.032.2766.11	09/01/2016 01:42:17	2.004.032.2764.11	2.004.032.2766.11
6	DXF28R1	10/27/2016 03:26:34	2.004.032.2766.11	09/05/2016 23:24:00	2.004.032.2764.11	2.004.032.2766.11
7	ES11915741	10/27/2016 08:20:26	2.004.032.2766.11	09/21/2016 05:30:05	2.004.032.2765.11	2.004.032.2766.11
8	ES12659911	10/27/2016 06:30:44	2.004.032.2766.11	09/15/2016 06:00:20	2.004.032.2763.11	2.004.032.2766.11
9	INA507Q433	08/28/2016 21:30:00	2.004.032.2763.11			
10	INA510R6SG	10/27/2016 07:19:39	2.004.032.2766.11			
11	INA520VWSJ	10/27/2016 23:42:34	2.004.032.2766.11	09/21/2016 23:08:54	2.004.032.2765.11	2.004.032.2766.11

Versions

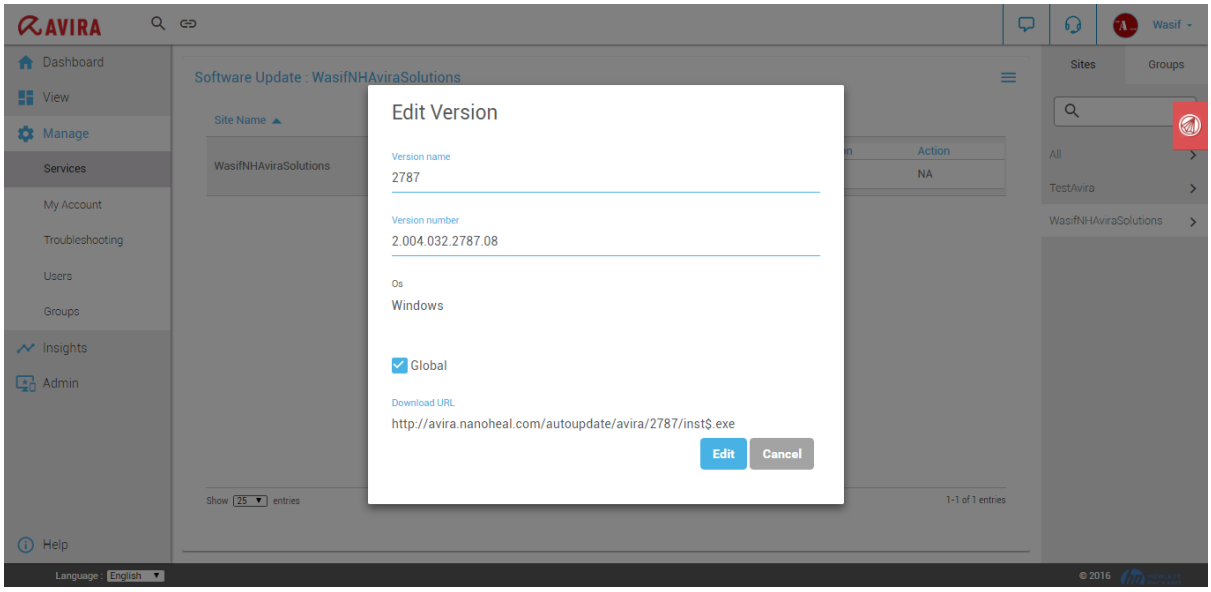
In order to view/edit all the Versions click the menu icon and click on the "Versions" link.



As shown in the screenshot above, the Version pop up shows all the Versions added. If any version needs to be edited, then select the version record and click "Edit" link from right menu.



Clicking on the "Edit" link will open up the Edit Version pop up as shown below.



In the Edit Version pop up, the user can edit the version details and click on "Edit" to save details.