

Monitoring Third Party Antivirus

Using the AV Status service

Version 2.6



AV Status Service Fast Track

Third party Antivirus status monitoring

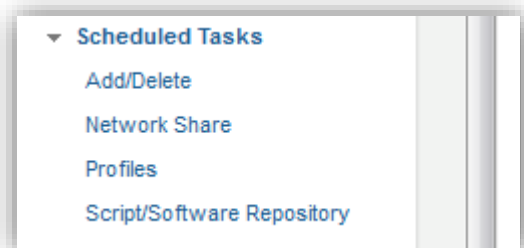
To monitor one of the supported third party antivirus (AV) solutions you will need to add the “AV Status” service to the professionally licensed device and execute the “AV Status” script (provided by N-able from the NRC, the N-able Resource Center) as a scheduled task once a day. The AV Status script will edit a WMI value that the AV Status service will monitor; keeping you up to date on the third party AV details including the type installed, whether or not the AV product is running and whether or not it is up to date.

Note: For an up to date list of supported antivirus products, download the AV Status script referred to in this document and edit it using Microsoft Notepad or a similar text editor. The list of antivirus solutions this service will monitor is contained within.

Deployment:

We will be building a collection of Rules, Templates and Filters in N-central at the SO (Service Organization – Orange) level that will automate the application and removal of the Third Party AV monitoring service “AV Status” depending on whether it is needed or not.

1. Download the AV Status script from the N-able Resource Center (<http://nrc.n-able.com>) under the **COMMUNITY > Scripts & Automation Policies** section.
2. Extract the AVSTATUS.VBS file and have it ready for use.
3. Import the script into N-Central’s Script Repository.
 - From the Service Organization Level (orange) under the **Scheduled Tasks** option on the Configuration menu.
 - Select **Script/Software Repository**.
 - Click **ADD** and choose Scripting and point to the downloaded AV Status VBS script.
 - Once uploaded, it will be available for use.



Note: The AV Status script is updated regularly. It is highly recommended you update the script in your repository on a regular basis.

To update the script in future, simply open the Script Repository as detailed above, select the existing AV Status script and click on “CHANGE”. You will be prompted to direct N-central to import the new version. Once uploaded, this new version will be used on all devices moving forward.

4. Create a Filter to Identify Devices without our integrated AV installed (Panda or AV Defender). These devices will need the AV STATUS service and script in place to monitor their third party AV such as Symantec, Trend, AVG etc. They must have a Professional license for this to function.

- Generate a CUSTOM EXPRESSION with the following criteria:
 - (((A OR B OR C) AND (D AND E AND F AND G)))

Filter Name: AV Status - Apply to All Devices Without Bit Defender or Panda is available to: Everyone

Description: Apply the AV Status service to all devices that do not have our integrated AV/Bit Defender service or Panda. Devices must also be in Professional Mode for AV status to work so we will ensure that is a requirement as well.

Show in my Drop-Down: ☐

Find devices where:

Custom Expression: (((A OR B OR C) AND (D AND E AND F AND G))) Generate

A:	Device	Class	EQUAL TO	Laptop - Windows
B:	Device	Class	EQUAL TO	Workstations - Windows
C:	Device	Class	EQUAL TO	Servers - Windows
D:	Application	Application Name	NOT EQUAL TO	Security Manager Endpoint
E:	Application	Application Name	NOT EQUAL TO	Security Manager AV Defender
F:	Device	Endpoint Security Enabled	EQUAL TO	False
G:	Device	License Mode	EQUAL TO	Professional Mode

5. Create a Filter to Identify Devices with our integrated AV installed (Panda or AV Defender). We will use this to REMOVE AV Status from devices that don't require it. Essential devices will also be removing AV Status as it cannot run its script on them.

- Generate a CUSTOM EXPRESSION with the following criteria:
 - ((A OR B OR C) AND (D OR E OR F OR G))

Filter Name: AV Status - Devices with Panda or AV Defender or Essential is available to: Everyone

Description: Used to REMOVE AV STATUS from devices you deploy AV Defender to, and will also remove AV status from Essential licensed devices.

Show in my Drop-Down: ☐

Find devices where:

Custom Expression: ((A OR B OR C) AND (D OR E OR F OR G)) Generate

A:	Device	Class	EQUAL TO	Laptop - Windows
B:	Device	Class	EQUAL TO	Workstations - Windows
C:	Device	Class	EQUAL TO	Servers - Windows
D:	Application	Application Name	EQUAL TO	Security Manager Endpoint
E:	Application	Application Name	EQUAL TO	Security Manager AV Defender
F:	Device	Endpoint Security Enabled	EQUAL TO	True
G:	Device	License Mode	EQUAL TO	Essential Mode

6. Create a Scheduled Task Profile (as detailed below) to run the AV Status script once a day during hours the system will typically be online. We will add this to a Rule in a moment that will allow it to globally apply automatically.
- a) From the Service Organization (Orange) level, click under Configuration > **Scheduled Tasks**
 - b) Click **"Profiles"** (*be sure not to select "Add/Delete")
 - c) Click **ADD** to add a profile task with the name of "AV Status Script"
 - d) Create the profile task as seen below:

Scripting Task

Task Name: AV Status Script

Task Handler:

- ☒ Use Agent where available, otherwise use Best available probe
- ☐ Use Best Available probe

Credentials:

- ☒ Use device credentials
- ☐ Custom credentials

Script

Location: From N-central's Script Repository

Repository Item: AV Status Script

Description: AV Status Script

File Name: AVStatus.vbs

Command Line Parameters: AVStatus.vbs

Schedule

Type: Recurring

Task Timeout: 1 hours

Interval: Custom

Start Time:

Add Delete Clear

09:45
15:45

Days of the Week:

- ☒ Every day
- ☐ Selected days

Sun Mon Tue Wed Thu Fri Sat All Clear

**** Recommended: Set your script to run at least twice a day during work hours.**

- e) Click **"Save"**
- f) **ADD** a second Task with the name of "AV Status – First Run"

g) Create the profile task as seen below:

Scripting Task

Details [Scheduled Task Limitations ?](#)

Task Name:

Task Handler:

- ☒ Use Agent where available, otherwise use Best available probe
- ☐ Use Best Available probe

Credentials:

- ☒ Use device credentials
- ☐ Custom credentials

Script [?](#)

Location:

Repository Item:

Description: AV Status Script

File Name: AVStatus.vbs

Command Line Parameters:

Schedule [?](#)

Type:

Task Timeout: hours

Execution Window:

- ☒ Only run at the specified time.
- ☐ If the machine is offline at the specified time, run this task as soon as possible, up to days in the future.

Downtime: ☐ Set device into downtime during task execution.

h) Once saved, you should see both Tasks listed in your profile. Click **“Save”** a final time to complete the Profile. Be **SURE** to **SAVE** back to the Scheduled Task Profiles main list.

Edit Scheduled Task Profile

Name:

Description:

Details Associations

Add

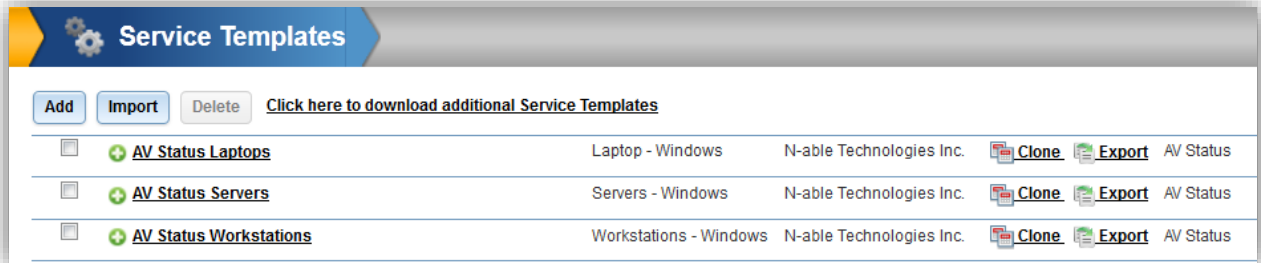
Scripting

Name	Schedule	Actions
<u>AV Status - First Run</u>	Once	✓ ✗
<u>AV Status Script</u>	Recurring	✓ ✗

This Scheduled Task Profile has been modified, to save the changes please press the Save button.

Save Cancel

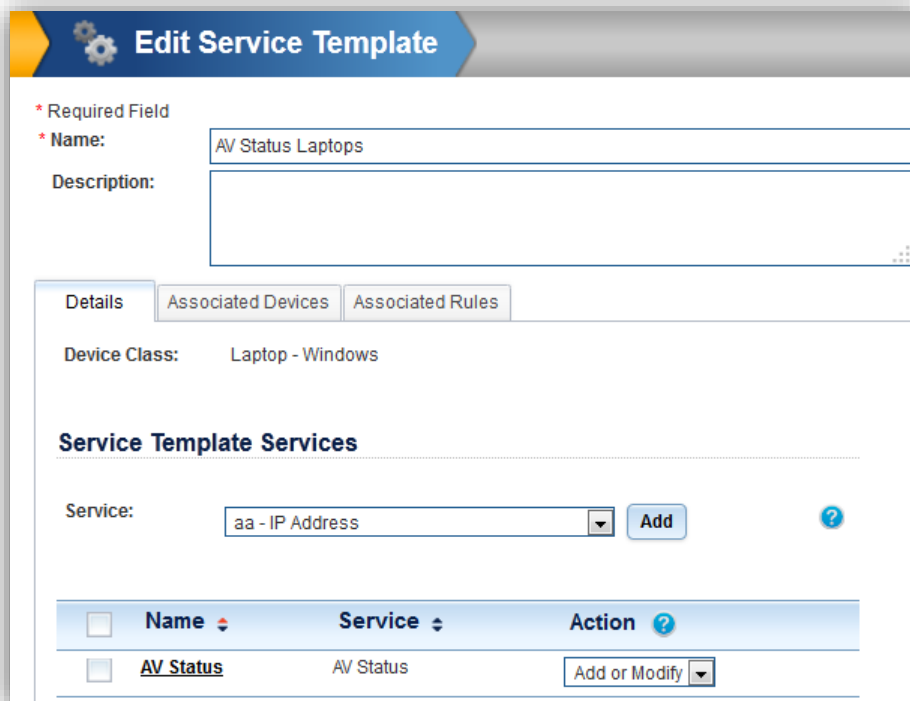
7. Create three Service Templates from the Service Organization level (orange) that will **ADD** the AV Status script.



The screenshot shows the 'Service Templates' management page. At the top, there are buttons for 'Add', 'Import', and 'Delete', along with a link to 'Click here to download additional Service Templates'. Below this is a table listing three service templates: 'AV Status Laptops', 'AV Status Servers', and 'AV Status Workstations'. Each row includes a checkbox, a green plus icon, the template name, the device class (Laptop - Windows, Servers - Windows, Workstations - Windows), the provider (N-able Technologies Inc.), and actions for 'Clone' and 'Export'. The 'AV Status' service is listed at the end of each row.

<input type="checkbox"/>	+ AV Status Laptops	Laptop - Windows	N-able Technologies Inc.	Clone	Export	AV Status
<input type="checkbox"/>	+ AV Status Servers	Servers - Windows	N-able Technologies Inc.	Clone	Export	AV Status
<input type="checkbox"/>	+ AV Status Workstations	Workstations - Windows	N-able Technologies Inc.	Clone	Export	AV Status

- Because Service Templates are tied to their respective device classes, you will need to create three. One for laptops, one for workstations and one for servers. All three will apply the AV Status service.
- In each template, we will add the **AV Status** service with its defaults.
 1. Select the Service from the dropdown and click “Add”. Leave it as the **Add/Modify** action.



The screenshot shows the 'Edit Service Template' form. It has a header with a gear icon and the title 'Edit Service Template'. Below the header, there's a section for 'Required Field' with a 'Name' field containing 'AV Status Laptops' and a 'Description' field. Below this are tabs for 'Details', 'Associated Devices', and 'Associated Rules'. The 'Details' tab is active, showing 'Device Class: Laptop - Windows'. Below this is a section titled 'Service Template Services'. It contains a 'Service:' dropdown menu with 'aa - IP Address' selected, an 'Add' button, and a help icon. At the bottom, there's a table with columns 'Name', 'Service', and 'Action'. The table has one row with 'AV Status' as the name, 'AV Status' as the service, and 'Add or Modify' as the action.

* Required Field
* Name:
Description:

Details Associated Devices Associated Rules

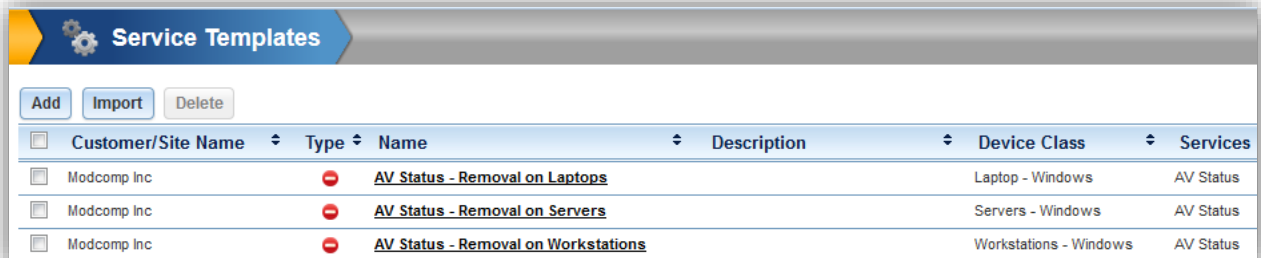
Device Class: Laptop - Windows

Service Template Services

Service: [?](#)

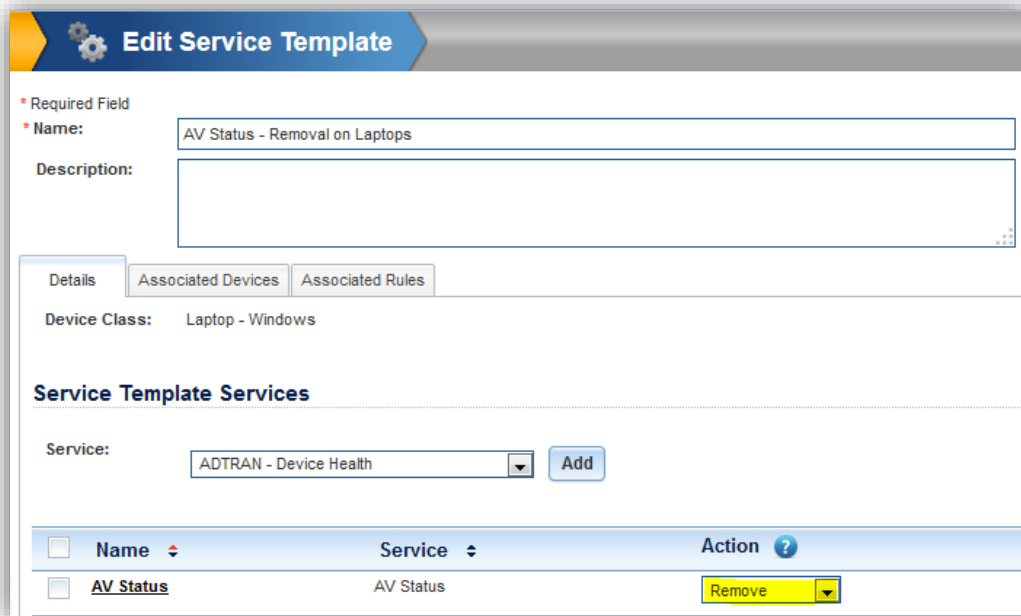
<input type="checkbox"/>	Name	Service	Action
<input type="checkbox"/>	AV Status	AV Status	<input type="button" value="Add or Modify"/>

8. Create three Service Templates from the Service Organization level (orange) that will **REMOVE** the AV Status script. These will be used to automatically clean up the AV Status services from any device you choose to deploy AV Defender or Panda endpoint to (AV Status is not needed on those devices).



<input type="checkbox"/>	Customer/Site Name	Type	Name	Description	Device Class	Services
<input type="checkbox"/>	Modcomp Inc		<u>AV Status - Removal on Laptops</u>		Laptop - Windows	AV Status
<input type="checkbox"/>	Modcomp Inc		<u>AV Status - Removal on Servers</u>		Servers - Windows	AV Status
<input type="checkbox"/>	Modcomp Inc		<u>AV Status - Removal on Workstations</u>		Workstations - Windows	AV Status

- Because Service Templates are tied to their respective device classes, you will need to create three. One for laptops, one for workstations and one for servers. All three will remove the AV Status service.
- In each template, we will add the **AV Status** service with its defaults, and switch its action to **REMOVE**.
 - Select the AV Status service from the dropdown and click “Add”. Change the Action to Remove as highlighted below.



Edit Service Template

* Required Field
* Name:
Description:

Details | Associated Devices | Associated Rules

Device Class: Laptop - Windows

Service Template Services

Service:

<input type="checkbox"/>	Name	Service	Action
<input type="checkbox"/>	<u>AV Status</u>	AV Status	<input type="button" value="Remove"/>

9. Create a SO level RULE to deploy the AV Status Script and three Service Templates by using our newly-created N-Central Filter for “Devices without Panda or AV Defender” as shown below:

Edit Rule

Type: ☒ Public ☐ Private

Name: AV Status - Add the AV Status to devices without Bit Defender or Panda

Description: Add AV Status for Third Party AV Monitoring

Devices to Target | Network Device Configuration Options | Mobile Device Configuration Options | Scheduled Task Profiles | Monitoring Options | Grant Customers/Sites Access

Filters

Choose device filters to target

Filters

- _QC EQUIPMENT
- _SH EQUIPMENT
- _ST EQUIPMENT
- _VD EQUIPMENT
- acrobat
- Agent Check-In greater than 30 days
- Autodesk
- AV Defender Enabled Devices
- AV Status - Devices with Panda or AV Defender or Essential Licensing
- Backup Exec Devices

Selected Filters

- AV Status - Apply to All Devices Without Bit Defender or Panda

► Ineligible Filters (5)

Edit Rule

Type: ☒ Public ☐ Private

Name: AV Status - Add the AV Status to devices without Bit Defender or Panda

Description: Add AV Status for Third Party AV Monitoring

Devices to Target | Configuration Options | Scheduled Task Profiles | Monitoring Options | Grant Customers/Sites Access

Scheduled Task Profiles

Scheduled Task Profiles

- Desktop Maintenance Package
- EPS Weekly Scan
- Onboard customer
- Server Maintenance Package

Selected Scheduled Task Profiles

- AV Status Script

Devices to Target | Network Device Configuration Options | Mobile Device Configuration Options | Scheduled Task Profiles | **Monitoring Options**

Notification Profiles

Notification Profiles-Triggers

- 0 Minute Delay (Agent Status)-Agent Status
- 0 Minute Delay (Workstation/Laptop ES and BM)-Workstations (AV Defender)
- 0 Minute Delay (Workstation/Laptop ES and BM)-Workstations (Backup Manager)
- 0 Minute Delay (Workstation/Laptop ES and BM)-Workstations (Endpoint Security)
- 0 Minute Delay-Network Devices
- 0 Minute Delay-Servers (Applications)
- 0 Minute Delay-Servers (Hardware)
- 0 Minute Delay-VMware Servers
- 0 Minute Delay-VMware Servers (Hardware Failed)
- 0 Minute Delay-VMware Servers (Hardware Warning)

Selected Notification Profiles-Triggers

Service Templates

Service Templates

- Acronis True Image Echo Server
- Acronis True Image for Microsoft SBS
- ADTRAN
- APC NetBotz
- APC UPS
- AV Defender (Laptops)
- AV Defender (Servers)
- AV Defender (Workstations)
- AV Status - Removal on Laptops
- AV Status - Removal on Servers

Selected Service Templates

- AV Status Laptops
- AV Status Servers
- AV Status Workstations

Devices to Target | Network Device Configuration Options | Mobile Device Configuration Options | Scheduled Task Profiles | Monitoring Options | **Grant Customers/Sites Access**

Customers/Sites

Customers/Sites


Selected Customers/Sites

- FSB
- MOD

☒ Propagate to all new customers/sites.

****This RULE will DEPLOY AV Status and its components to devices that do not have our integrated AV products Bit Defender or Panda Endpoint. These devices must also have a Professional mode license to run the AV Status script.**

10. Create a SO level RULE to REMOVE three AV Status Service Templates if we have a device using our integrated AV. We will do this by using our newly-created N-Central Filter for “Devices with Panda or AV Defender” as shown below:

 **Edit Rule**

Type: ☒ Public ☐ Private ?

Name:

Description:

Devices to Target | Network Device Configuration Options | Mobile Device Configuration Options | Scheduled Task Profiles | Monitoring Options | Grant Customers/Sites Access

Filters

Choose device filters to target

Filters

- _QC EQUIPMENT
- _SH EQUIPMENT
- _ST EQUIPMENT
- _WD EQUIPMENT
- acrobat
- Agent Check-In greater than 30 days
- Autodesk
- AV Defender Enabled Devices
- AV Status - Apply to All Devices Without Bit Defender or Panda
- Backup Exec Devices

>>

>

<

<<

Selected Filters

AV Status - Devices with Panda or AV Defender or Essential Licensing

Devices to Target | Network Device Configuration Options | Mobile Device Configuration Options | Scheduled Task Profiles | **Monitoring Options** | Grant Customers/Sites Access

Notification Profiles

Notification Profiles-Triggers

- 0 Minute Delay (Agent Status)-Agent Status
- 0 Minute Delay (Workstation/Laptop ES and BM)-Workstations (AV Defender)
- 0 Minute Delay (Workstation/Laptop ES and BM)-Workstations (Backup Manager)
- 0 Minute Delay (Workstation/Laptop ES and BM)-Workstations (Endpoint Security)
- 0 Minute Delay-Network Devices
- 0 Minute Delay-Servers (Applications)
- 0 Minute Delay-Servers (Hardware)
- 0 Minute Delay-VMware Servers
- 0 Minute Delay-VMware Servers (Hardware Failed)
- 0 Minute Delay-VMware Servers (Hardware Warning)

>>

>

<

<<

Selected Notification Profiles-Triggers

Service Templates

Service Templates

- Acronis True Image Echo Server
- Acronis True Image for Microsoft SBS
- ADTRAN
- APC NetBotz
- APC UPS
- AV Defender (Laptops)
- AV Defender (Servers)
- AV Defender (Workstations)
- AV Status Laptops
- AV Status Servers

>>

>

<

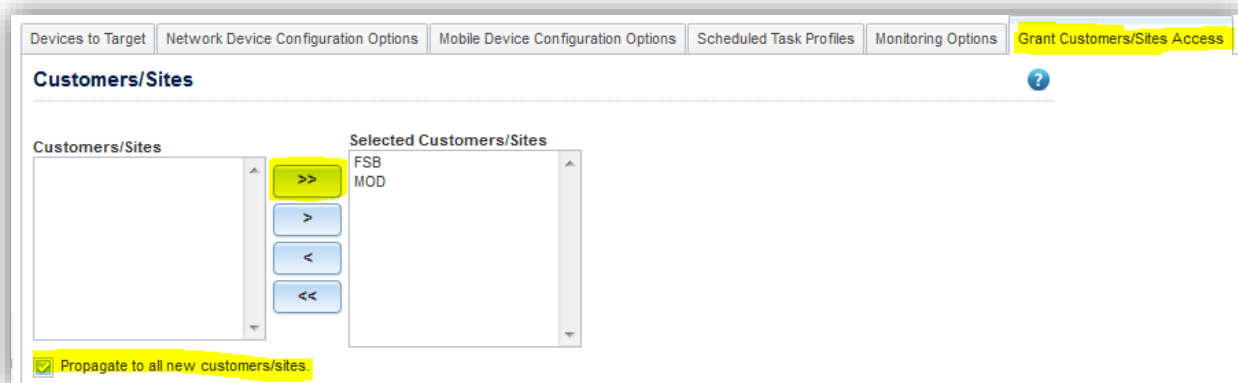
<<

Selected Service Templates

AV Status - Removal on Laptops

AV Status - Removal on Servers

AV Status - Removal on Workstations



The process is completed!

AV Status will now deploy to devices in your system that do not have N-central's native AV products, allowing you to monitor them.

Devices without AV will get AV Status applied, and it will fail. This will draw your attention to devices that are missing Antivirus products.

If you choose to deploy N-central's AV products, AV Status will be cleaned from the device and product specific monitoring will be applied by N-central.

Appendix A – Creating an AV Dashboard

You may wish to create a dashboard to monitor AV Status instead of viewing it in your Active Issues. To do this, follow these steps:

1. Create a CUSTOM EXPRESSION filter as seen below to identify all devices with AV Monitoring deployed regardless of type.
 - a) The format for this filter will be: (((A OR B OR C) AND (D OR E OR F)) AND G)

The screenshot shows the 'Filter Name' field set to 'AV - Devices with AV Monitoring Enabled' and 'is available to' set to 'Everyone'. The 'Description' field is empty. The 'Show in my Drop-Down' checkbox is checked. Below, the 'Find devices where:' section shows a 'Custom Expression' selected with the formula '(((A OR B OR C) AND (D OR E OR F)) AND G)'. A 'Generate' button is next to it. The configuration is broken down into seven parts (A-G) with dropdown menus for device type, class, and specific attributes.

Part	Device	Class	Attribute	Operator	Value
A	Device	Class		EQUAL TO	Laptop - Windows
B	Device	Class		EQUAL TO	Workstations - Windows
C	Device	Class		EQUAL TO	Servers - Windows
D	Monitoring		N-central service is present	EQUAL TO	AV Status
E	Monitoring		N-central service is present	EQUAL TO	AV Defender Security Event
F	Device		Endpoint Security Enabled	EQUAL TO	True
G	Monitoring		N-central service in status	EQUAL TO	Normal

2. At the SO Level of N-central, on the left hand menu structure under Dashboards, click “Manage Dashboards”
3. Click “Add”
4. Create a dashboard named “Manage – AV Status”
5. Add in the filter we created.

The screenshot shows the 'Type' set to 'Public' and 'Name' set to 'Manage - Antivirus'. The 'Description' field is empty. Below, the 'Devices to Target' and 'Monitoring Options' tabs are visible. The 'Filters' section shows a list of filters on the left and a 'Selected Filters' list on the right. The 'Selected Filters' list contains 'AV - Devices with AV Monitoring Enabled'.

Filters	Selected Filters
_QC EQUIPMENT	AV - Devices with AV Monitoring Enabled
_SH EQUIPMENT	
_ST EQUIPMENT	
_WD EQUIPMENT	
acrobat	

6. On the Monitoring Options tab, select the following services:
 - a) Agent Status
 - b) AV Status
 - c) AV Defender Status
 - d) AV Defender Events

- e) Endpoint Status
- f) Endpoint Events

7. Save to complete your dashboard:

The screenshot shows a dashboard titled "Manage - AV Status". It includes buttons for "Filter", "Reset Filter", and "Create New Filter". Below these is a table with columns: "Customer/Site", "Device Name", "Agent Status", "AV Defender Security Event", "AV Defender Status", and "AV Status".

Customer/Site	Device Name	Agent Status	AV Defender Security Event	AV Defender Status	AV Status
FSB	4DV4PW1	✓			✓
FSB	BR08-OPS1	✓			✓
FSB	COLO-BUFFALO01	✓			✓
FSB	COLO-DIRECTOROLD	✓			✓

8. You may wish to edit the Filter on your Active Issues view to remove AV Status alerts, and simply refer to the dashboard and/or the AV Status Report in Report Manager (for on-premise customers with Report Manager):

The screenshot shows the "Filter" configuration page. It includes a search bar and buttons for "Reset Filter" and "Create New Filter". The "Filter:" dropdown is set to "No Filter". The "Customer/Site" dropdown is set to "FSB MOD". The "Status:" section has checkboxes for "Failed", "Warning", "Normal", "Misconfigured", "Stale", "No Data", and "Disconnected". The "Notifications:" section has checkboxes for "Unacknowledged", "Acknowledged", and "None". The "License Type:" section has checkboxes for "Professional" and "Essential". The "Services:" section has a "Select All" button and a list of services with checkboxes. The "AV Status" checkbox is highlighted in yellow.

Services: ☐ Select All

A-D (67 of 68) E-H (34 of 34) I-L (23 of 23) M-P (31 of 34) Q-T (25 of 25) U-Z (15 of 15)

☐ All in This Range

<input checked="" type="checkbox"/> Active Directory	<input checked="" type="checkbox"/> ADTRAN - Device Health	<input checked="" type="checkbox"/> ADTRAN - Memory
<input checked="" type="checkbox"/> Agent Status	<input checked="" type="checkbox"/> APC PDU	<input checked="" type="checkbox"/> APC UPS - Humidity
<input checked="" type="checkbox"/> APC UPS - Temperature	<input checked="" type="checkbox"/> APC UPS	<input checked="" type="checkbox"/> Application Compliance
<input checked="" type="checkbox"/> Asigra/XiloCore	<input checked="" type="checkbox"/> AV Activity - McAfee 8	<input checked="" type="checkbox"/> AV Activity - McAfee
<input checked="" type="checkbox"/> AV Activity - Sophos 5	<input checked="" type="checkbox"/> AV Activity - Sophos	<input checked="" type="checkbox"/> AV Activity - Symantec
<input checked="" type="checkbox"/> AV Activity - Trend Micro	<input checked="" type="checkbox"/> AV Def. - McAfee 8	<input checked="" type="checkbox"/> AV Def. - McAfee
<input checked="" type="checkbox"/> AV Def. - Sophos 5	<input checked="" type="checkbox"/> AV Def. - Sophos	<input checked="" type="checkbox"/> AV Def. - Symantec
<input checked="" type="checkbox"/> AV Def. - Trend Micro	<input checked="" type="checkbox"/> AV Defender Security Event	<input checked="" type="checkbox"/> AV Defender Status
<input checked="" type="checkbox"/> AV Status	<input checked="" type="checkbox"/> Backup Exec	<input checked="" type="checkbox"/> Backup Manager Events
<input checked="" type="checkbox"/> Backup Manager Status	<input checked="" type="checkbox"/> BES Message Status	<input checked="" type="checkbox"/> CA Replication Events