Monitoring Third Party A/V with the A/V Status Service

1-Oct-20

Author: Chris Reid

Table of Contents

Introduction 3

Overview 4

Testing 4

Deployment 9

Confirmation 19

FAQ 20

- What A/V Products does the AV Status script support? 20
- What AV Products are not supported by the AV Status script? 21

Introduction

MSP N-central provides built-in, marketing leading A/V support based on the Bitdefender engine, and that integration includes monitoring the overall state of the A/V solution. For other A/V products though, SolarWinds MSP recommends the use of the **AV Status** service.

This document outlines how to configure N-central to monitor 3rd party A/V products, using the AV Status service and the AV Status script, and is meant for a technical audience who is familiar with both N-central and managing Windows environments.

Overview

To monitor one of the supported third party antivirus solutions you will need to add the “AV Status” service to a device that has been licensed with a Professional node and execute the “AV Status” script found on the NRC 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.

For an up to date list of supported antivirus products, please refer to the FAQ section at the end of this document.

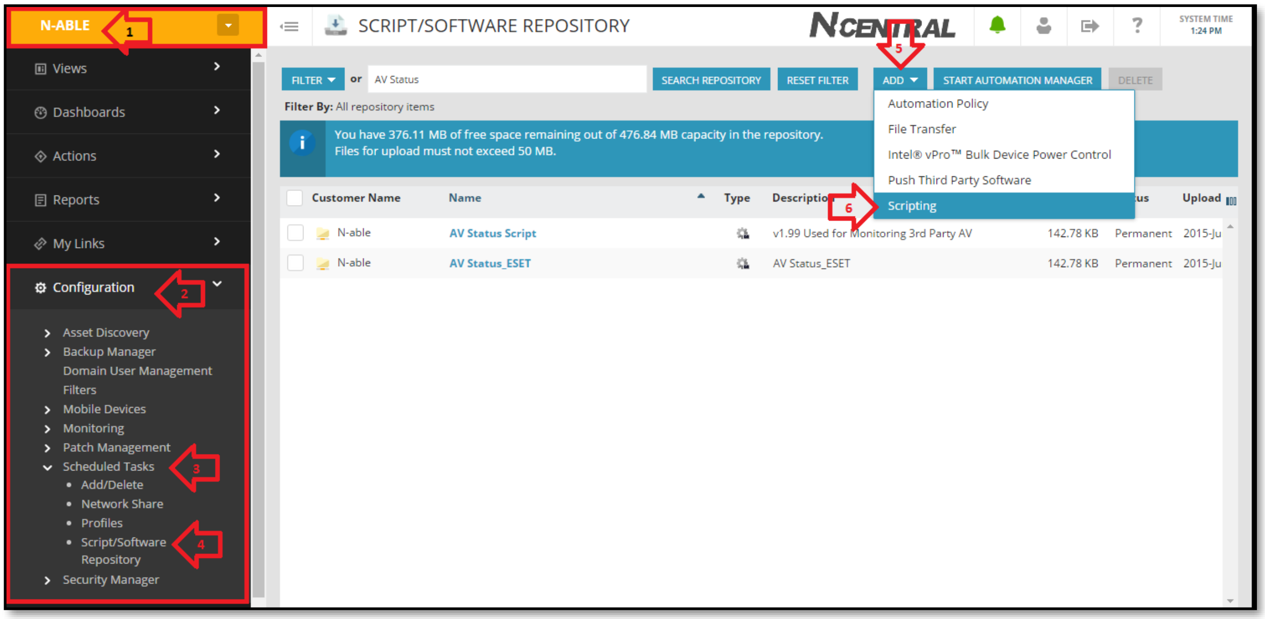
Testing

If you are unsure if the AV Status script will work with your AV, then you can test it on a few devices. This step is not necessary as the AV Status script more often than not can detect any AV. If you wish to skip this section, jump to Deployment.

1. Navigate to the NRC and download the script:

   https://nrc.n-able.com/Community/Scripts-Automation-Policies?fileid=418

2. Extract the AVStatus.vbs file
3. Import the script into N-central
   1: Go to the SO level
   2: Navigate to **Configuration -> Scheduled Tasks -> Script/Software Repository**
   3: Click the **Add** button, and choose **Scripting** from the drop-down menu



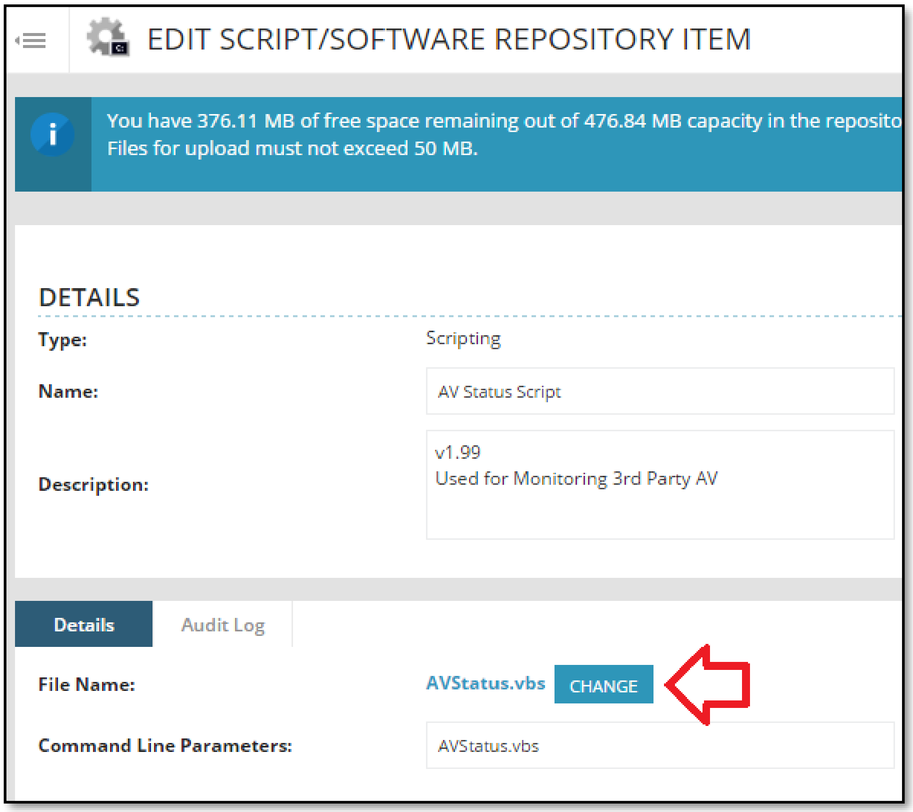
Filter By: All repository items

You have 376.11 MB of free space remaining out of 476.84 MB capacity in the repository.
Files for upload must not exceed 50 MB.

Customer Name	Name	Type	Descriptio…		…us	Upload
N-able	AV Status Script		v1.99 Used for Monitoring 3rd Party AV	142.78 KB	Permanent	2015-Ju
N-able	AV Status_ESET		AV Status_ESET	142.78 KB	Permanent	2015-Ju

***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.



You have 376.11 MB of free space remaining out of 476.84 MB capacity in the reposito
Files for upload must not exceed 50 MB.

DETAILS

Type: Scripting

Name: AV Status Script

Description: v1.99
Used for Monitoring 3rd Party AV

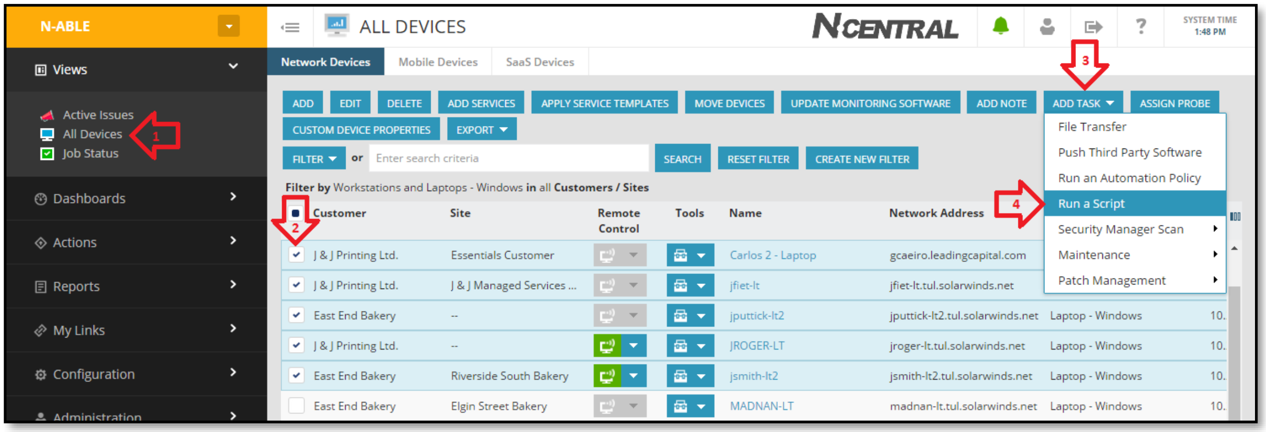
File Name: AVStatus.vbs

Command Line Parameters: AVStatus.vbs

4. Run the script across a few devices that have third party AV:
   1: Navigate to the All Devices view (any level)

2: Select a few devices that have professional licenses. (remember them)

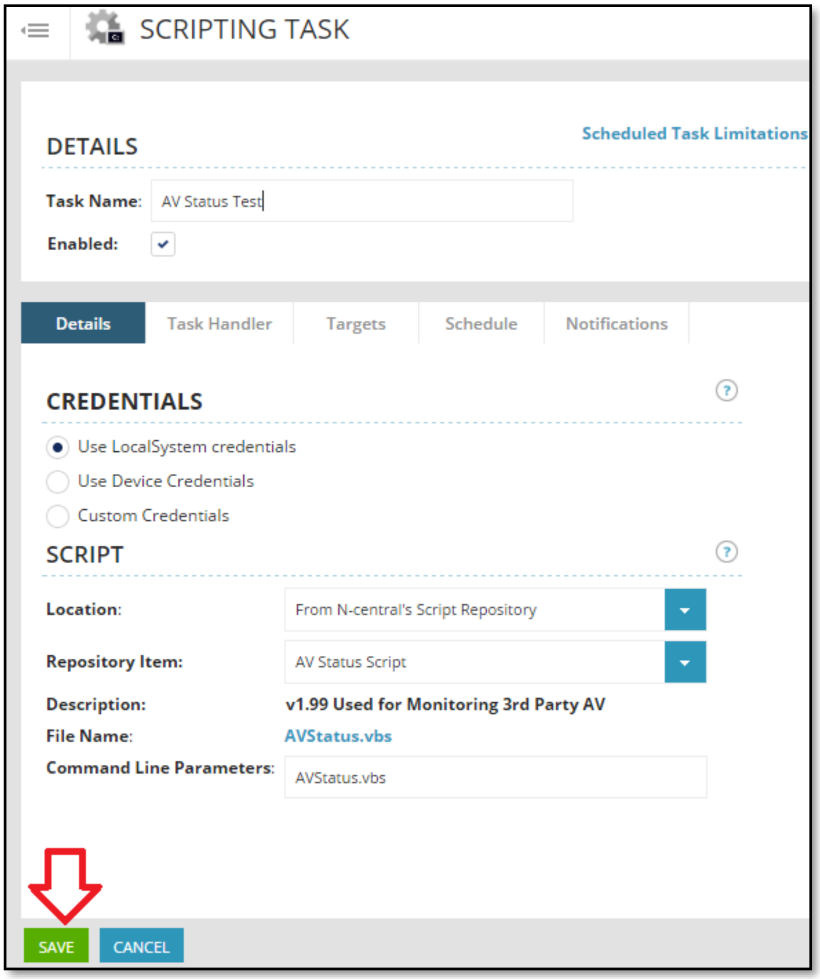
3: Click the **Add Task** button and choose **Run a Script** from the drop-down menu



Filter by Workstations and Laptops - Windows **in** all **Customers / Sites**

■	Customer	Site	Remote Control	Tools	Name	Network Address		
☑	J & J Printing Ltd.	Essentials Customer			Carlos 2 - Laptop	gcaeiro.leadingcapital.com		
☑	J & J Printing Ltd.	J & J Managed Services ...			jfiet-lt	jfiet-lt.tul.solarwinds.net		
☑	East End Bakery	--			jputtick-lt2	jputtick-lt2.tul.solarwinds.net	Laptop - Windows	10.
☑	J & J Printing Ltd.	--			JROGER-LT	jroger-lt.tul.solarwinds.net	Laptop - Windows	10.
☑	East End Bakery	Riverside South Bakery			jsmith-lt2	jsmith-lt2.tul.solarwinds.net	Laptop - Windows	10.
□	East End Bakery	Elgin Street Bakery			MADNAN-LT	madnan-lt.tul.solarwinds.net	Laptop - Windows	10.

5. Run the script with the following options:
   1: **Credentials:** Use LocalSystem credentials
   2: **Script:** From N-central's Script Repository
   3: **Repository Item:** AV Status Script
   4: No Command Line Parameters other than the default
   5: Leave everything else as default and **Save** to run



DETAILS

Task Name: AV Status Test

Enabled: ☑

CREDENTIALS

● Use LocalSystem credentials
○ Use Device Credentials
○ Custom Credentials

SCRIPT

Location: From N-central's Script Repository

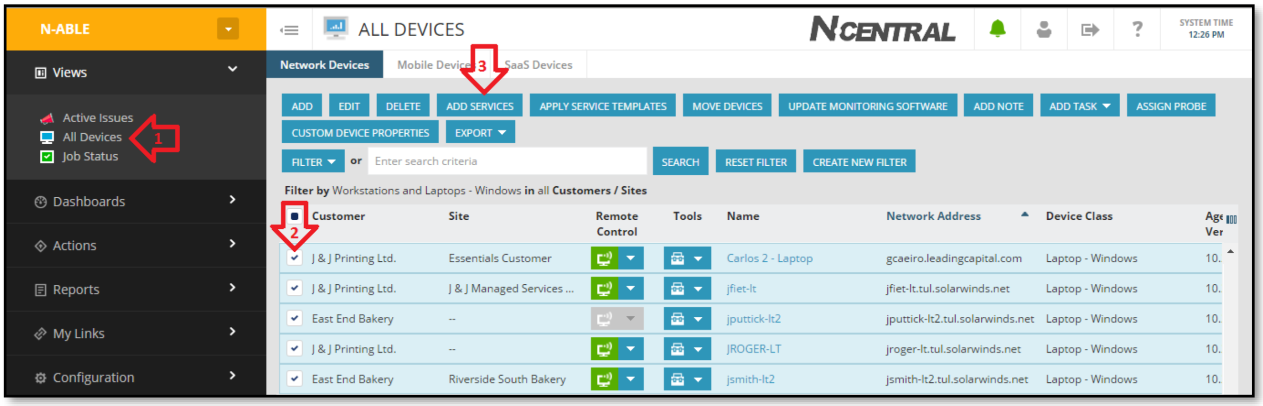
Repository Item: AV Status Script

Description: v1.99 Used for Monitoring 3rd Party AV

File Name: AVStatus.vbs

Command Line Parameters: AVStatus.vbs

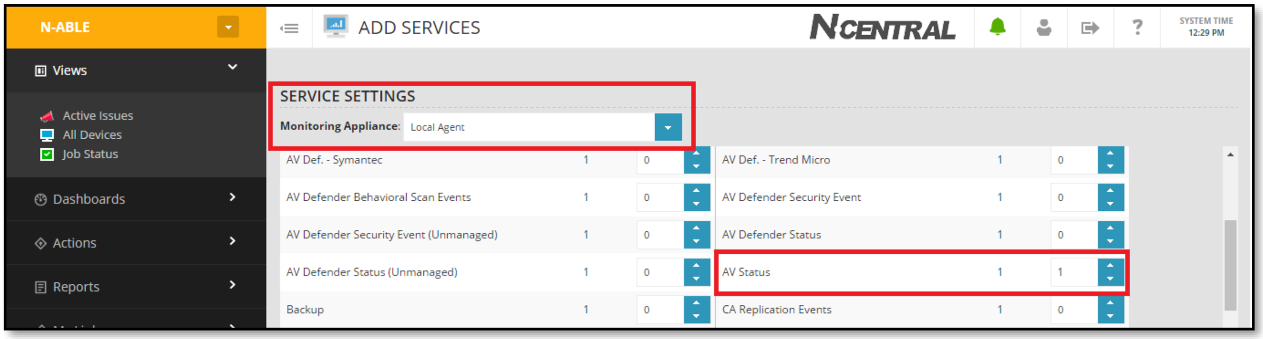
6. Add the AV Status service to the earlier targeted devices. Navigate to:
   1: All Devices view
   2: Select the same few devices as before
   3: Add Services



Filter by Workstations and Laptops - Windows **in** all **Customers / Sites**

■	Customer	Site	Remote Control	Tools	Name	Network Address	Device Class	Age Ver
☑	J & J Printing Ltd.	Essentials Customer			Carlos 2 - Laptop	gcaeiro.leadingcapital.com	Laptop - Windows	10.
☑	J & J Printing Ltd.	J & J Managed Services ...			jfiet-lt	jfiet-lt.tul.solarwinds.net	Laptop - Windows	10.
☑	East End Bakery	--			jputtick-lt2	jputtick-lt2.tul.solarwinds.net	Laptop - Windows	10.
☑	J & J Printing Ltd.	--			JROGER-LT	jroger-lt.tul.solarwinds.net	Laptop - Windows	10.
☑	East End Bakery	Riverside South Bakery			jsmith-lt2	jsmith-lt2.tul.solarwinds.net	Laptop - Windows	10.

7. Change the number of instances for the AV Status service to 1. Ensure that the monitoring appliance is selected as the Local Agent. If that option does not exist, it means a device selected does not have an agent installed.

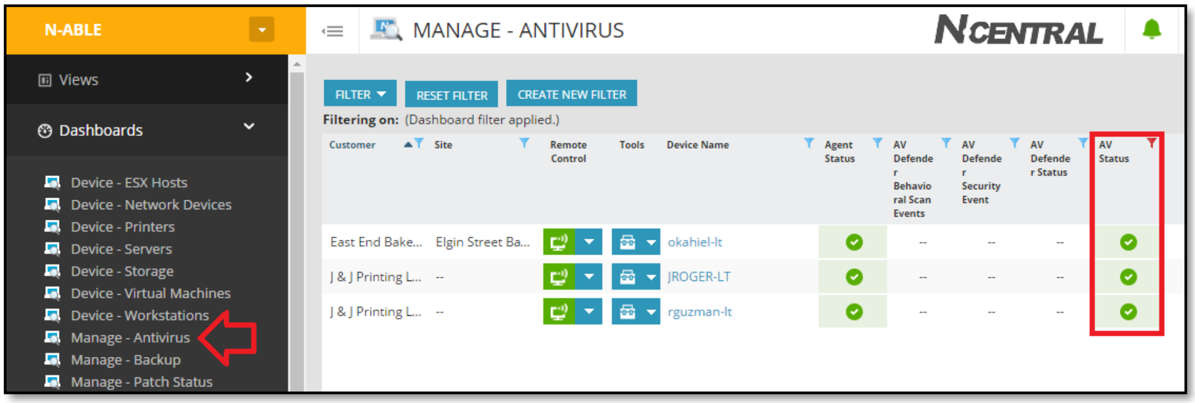


SERVICE SETTINGS

Monitoring Appliance: Local Agent

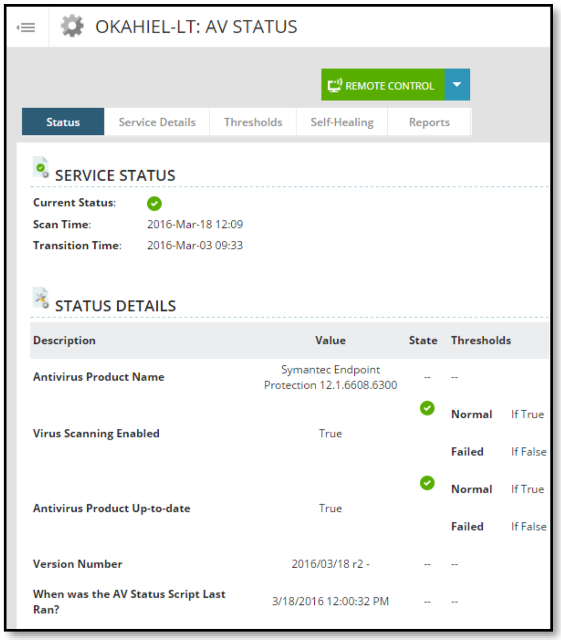
AV Def. - Symantec	1	0	AV Def. - Trend Micro	1	0
AV Defender Behavioral Scan Events	1	0	AV Defender Security Event	1	0
AV Defender Security Event (Unmanaged)	1	0	AV Defender Status	1	0
AV Defender Status (Unmanaged)	1	0	AV Status	1	1
Backup	1	0	CA Replication Events	1	0

8. Confirm the monitoring is working correctly by either checking the Manage – Antivirus dashboard (default) or navigating to a device:



Filtering on: (Dashboard filter applied.)

Customer	Site	Remote Control	Tools	Device Name	Agent Status	AV Defender Behavioral Scan Events	AV Defender Security Event	AV Defender Status	AV Status
East End Bake...	Elgin Street Ba...			okahiel-lt	✓	--	--	--	✓
J & J Printing L...	--			JROGER-LT	✓	--	--	--	✓
J & J Printing L...	--			rguzman-lt	✓	--	--	--	✓



SERVICE STATUS

Current Status: ✓

Scan Time: 2016-Mar-18 12:09

Transition Time: 2016-Mar-03 09:33

STATUS DETAILS

Description	Value	State	Thresholds	
Antivirus Product Name	Symantec Endpoint Protection 12.1.6608.6300	--	--	
Virus Scanning Enabled	True	✓	Normal	If True
			Failed	If False
Antivirus Product Up-to-date	True	✓	Normal	If True
			Failed	If False
Version Number	2016/03/18 r2 -	--	--	
When was the AV Status Script Last Ran?	3/18/2016 12:00:32 PM	--	--	

Deployment

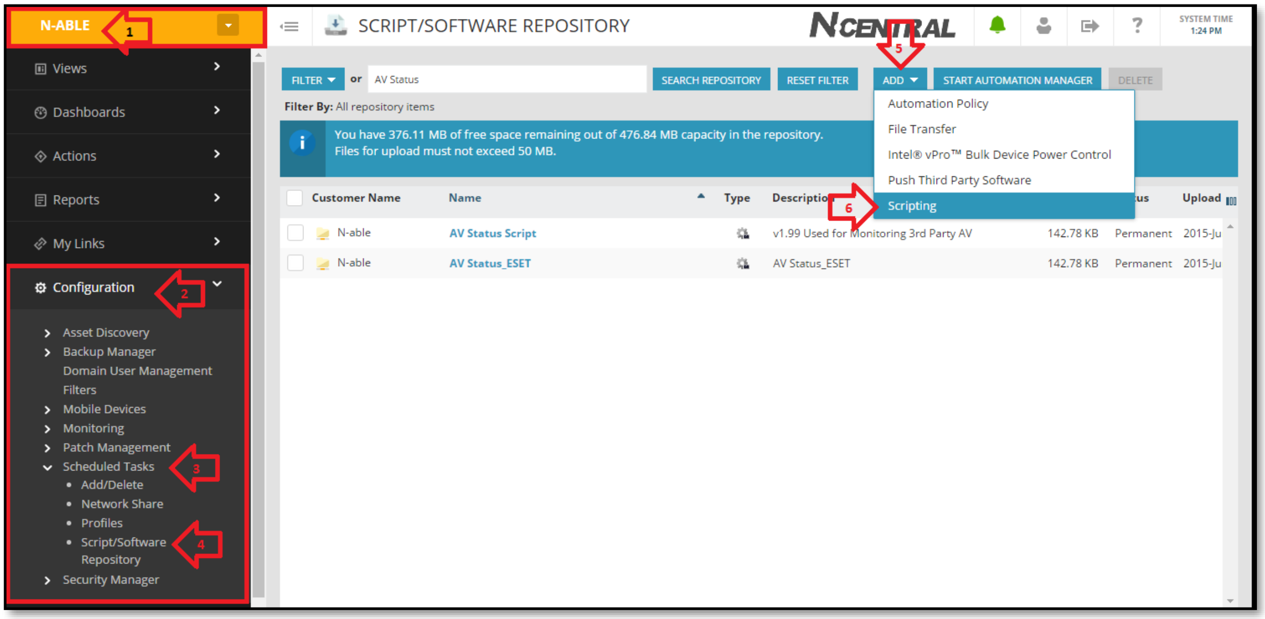
We will be building a collection of Filters, Templates, and Rules in N-central at the Service Organization Level. This will automate the application and removal of the AV Status script/service where needed.

1. Navigate to the NRC and download the script:

   https://nrc.n-able.com/Community/Scripts-Automation-Policies?fileid=418

2. Extract the AVStatus.vbs file

3. Import the script into N-central
   1: Go to the SO level
   2: Navigate to **Configuration -> Scheduled Tasks -> Script/Software Repository**
   3: Click the **Add** button, and choose **Scripting** from the drop-down menu



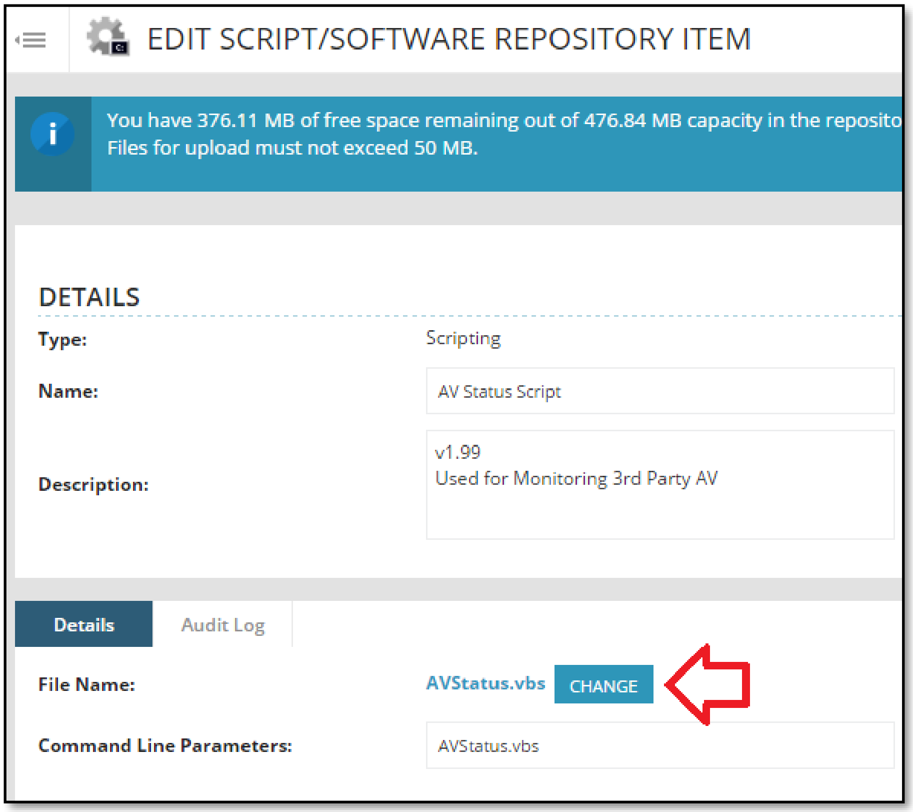
Filter By: All repository items

You have 376.11 MB of free space remaining out of 476.84 MB capacity in the repository.
Files for upload must not exceed 50 MB.

Customer Name	Name	Type	Descriptio		us	Upload
N-able	AV Status Script		v1.99 Used for Monitoring 3rd Party AV	142.78 KB	Permanent	2015-Ju
N-able	AV Status_ESET		AV Status_ESET	142.78 KB	Permanent	2015-Ju

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.



EDIT SCRIPT/SOFTWARE REPOSITORY ITEM

You have 376.11 MB of free space remaining out of 476.84 MB capacity in the reposito
Files for upload must not exceed 50 MB.

DETAILS

Type: Scripting

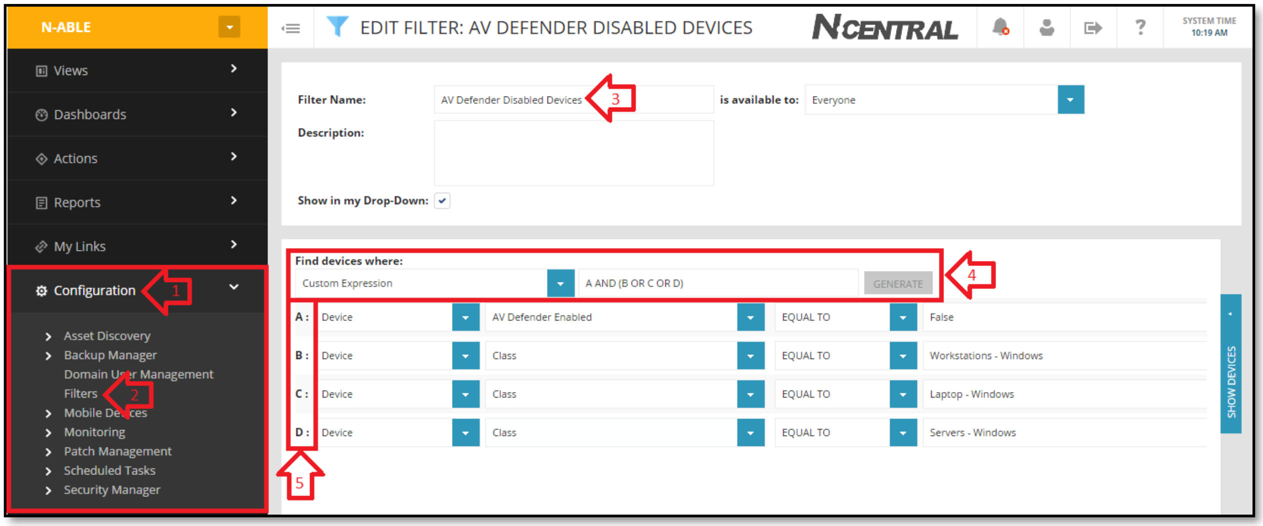
Name: AV Status Script

Description: v1.99
Used for Monitoring 3rd Party AV

File Name: AVStatus.vbs CHANGE

Command Line Parameters: AVStatus.vbs

4. Create a new Filter to identify devices that do not have AV Defender Enabled, Navigate to:
   1: Configuration >
   2: Filters > Add
   3: Name the filter 'AV Defender Disabled Devices'
   4: Set the custom expression under 'Find devices where' to **A AND (B OR C OR D)**
   5: Copy the 4 filtering requirements below



EDIT FILTER: AV DEFENDER DISABLED DEVICES

Filter Name: AV Defender Disabled Devices

is available to: Everyone

Description:

Show in my Drop-Down: ☑

Find devices where:

Custom Expression A AND (B OR C OR D) GENERATE

A :	Device	AV Defender Enabled	EQUAL TO	False
B :	Device	Class	EQUAL TO	Workstations - Windows
C :	Device	Class	EQUAL TO	Laptop - Windows
D :	Device	Class	EQUAL TO	Servers - Windows

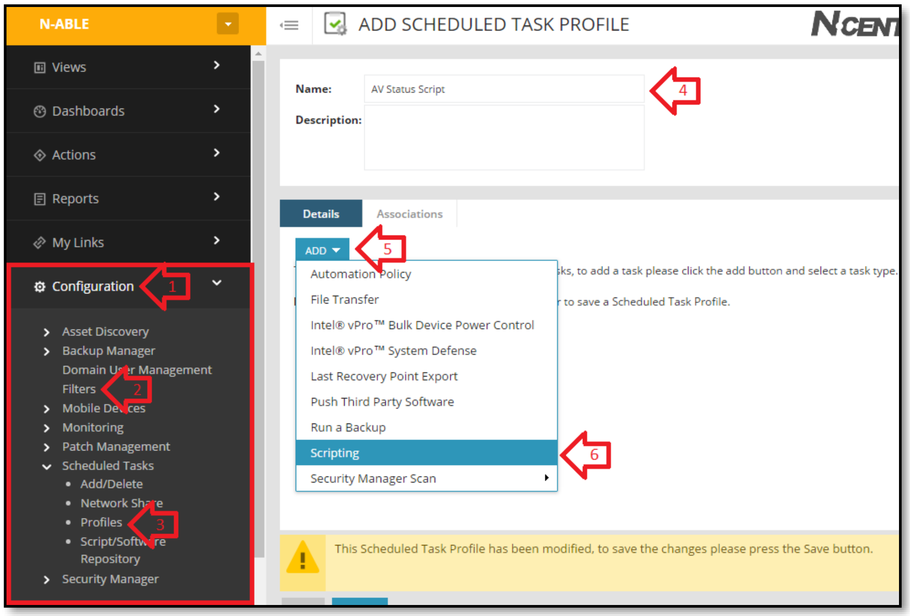
5. Create a Scheduled Task Profile to run the AV Status script:

1: Navigate to **Configuration -> Scheduled Tasks -> Profiles**

2: Click the **Add** button

3: Name the profile ‘AV Status Script’

4: Click the **Add** button, and choose **Scripting** from the drop-down menu



Name: AV Status Script

Description:

...ks, to add a task please click the add button and select a task type.

...r to save a Scheduled Task Profile.

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

5: Name the Task ‘AV Status Script’

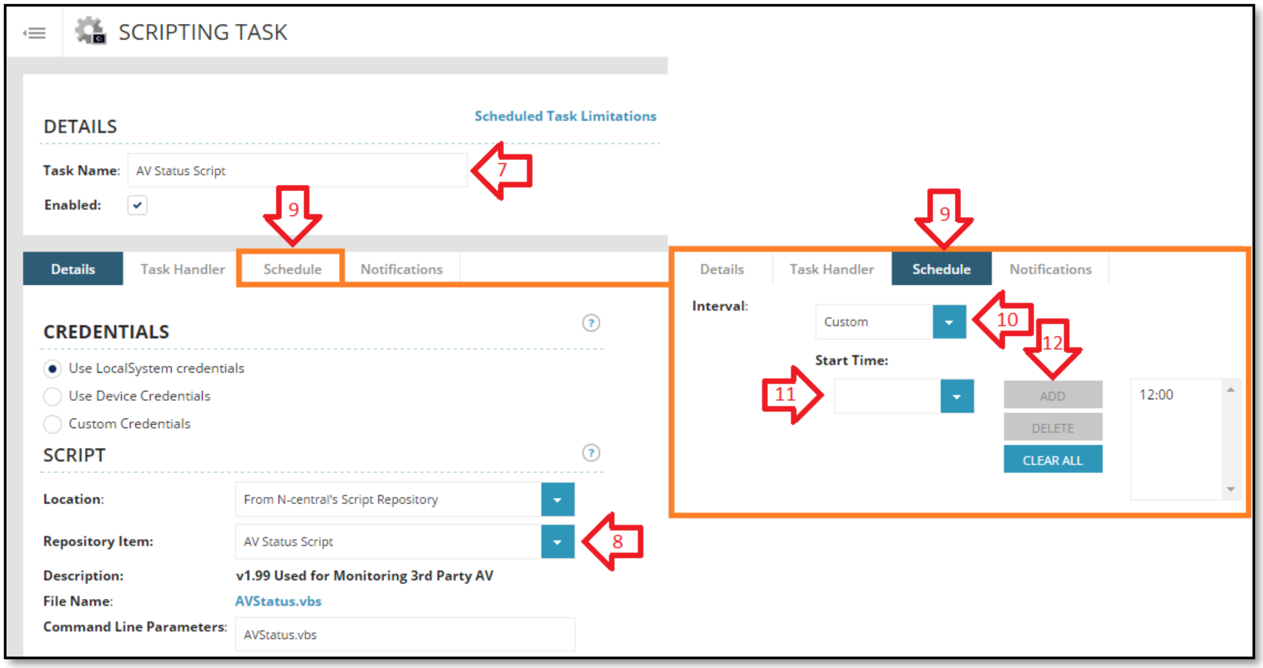
6: Find the AV Status Script from the Repository

7: Click on the **Schedule** tab

8: Choose “Custom” Interval

9: Select a start time where typically the machines are online

10: Click the **Add** button



DETAILS

Task Name: AV Status Script

Enabled: ☑

CREDENTIALS

● Use LocalSystem credentials

○ Use Device Credentials

○ Custom Credentials

SCRIPT

Location: From N-central's Script Repository

Repository Item: AV Status Script

Description: v1.99 Used for Monitoring 3rd Party AV

File Name: AVStatus.vbs

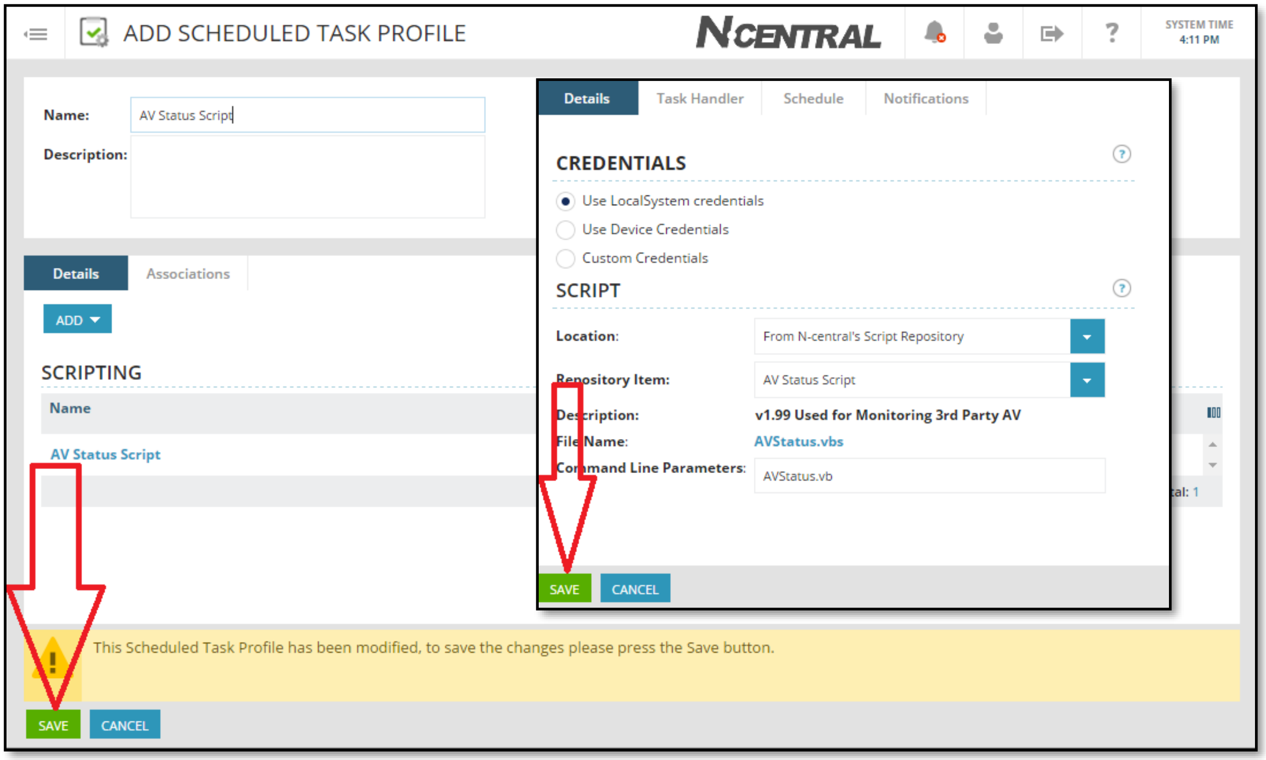
Command Line Parameters: AVStatus.vbs

Interval: Custom

Start Time:

12:00

11: Do not forget to hit **Save**! Twice!



Name: AV Status Script

Description:

SCRIPTING

Name
AV Status Script

CREDENTIALS

● Use LocalSystem credentials
○ Use Device Credentials
○ Custom Credentials

SCRIPT

Location: From N-central's Script Repository

Repository Item: AV Status Script

Description: v1.99 Used for Monitoring 3rd Party AV

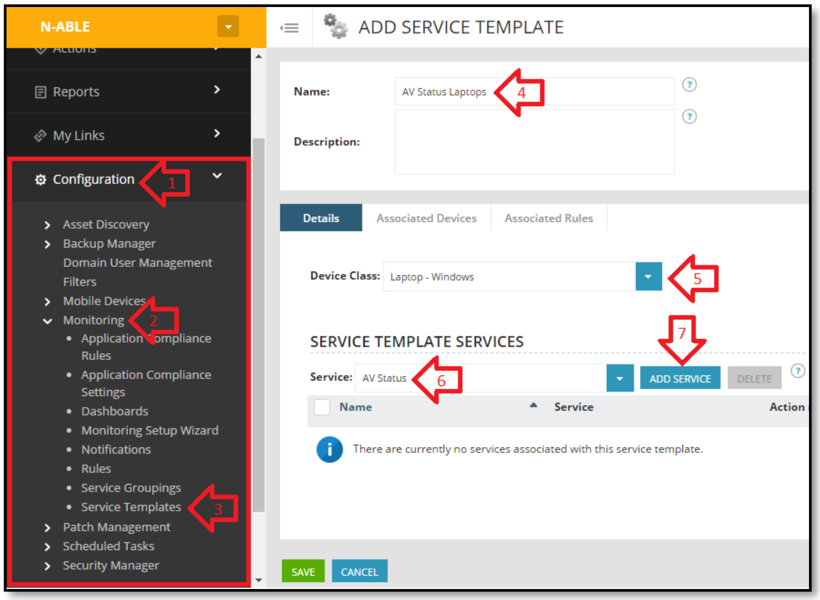
File Name: AVStatus.vbs

Command Line Parameters: AVStatus.vb

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

6. Create three Service Templates from the Service Organization level (orange) that add the AV Status service. Navigate to:

1:   Configuration >
2:   Monitoring >
3:   Service Templates > Add
4:   Name the template 'AV Status Laptops'
5:   Select the device class 'Laptop – Windows'
6:   In the service dropdown find 'AV Status'
7:   Add Service



Name: AV Status Laptops

Description:

Device Class: Laptop - Windows

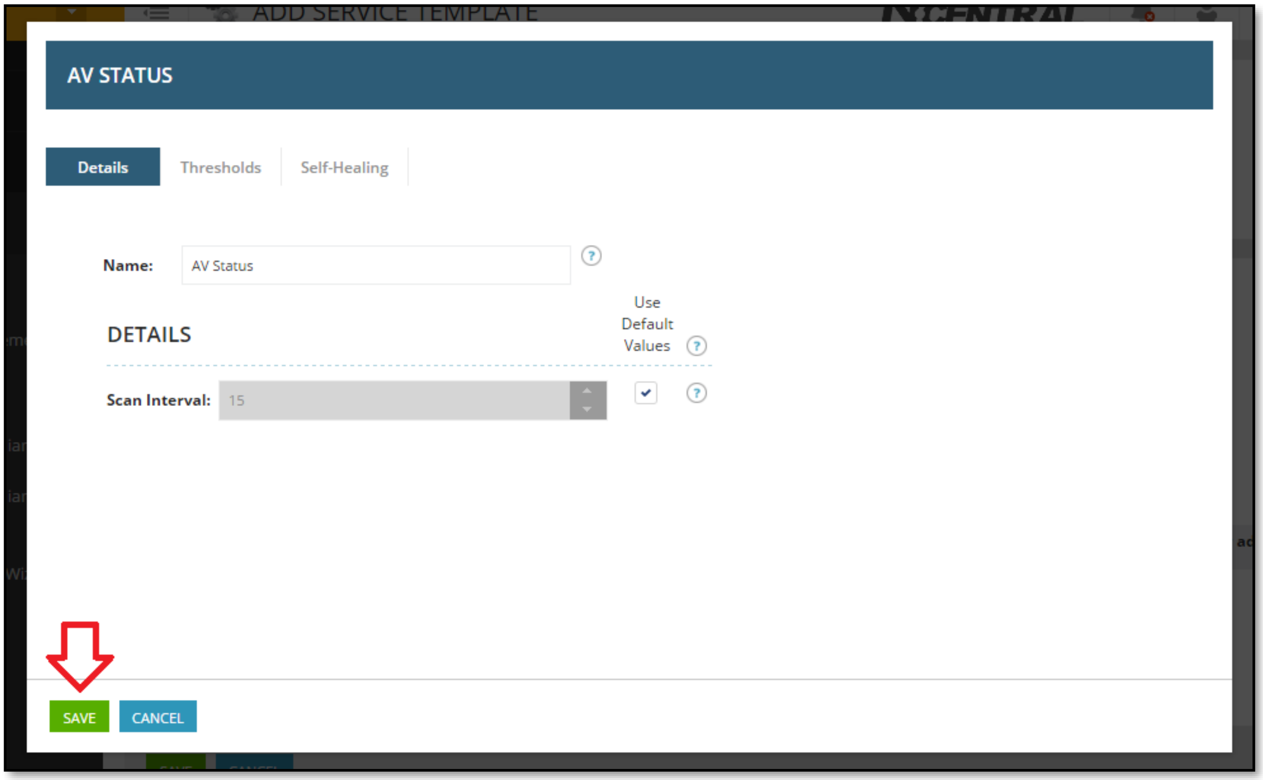
SERVICE TEMPLATE SERVICES

Service: AV Status

Name	Service	Action

There are currently no services associated with this service template.

8: Nothing needs to be done to the service once added, hit **Save**



AV STATUS

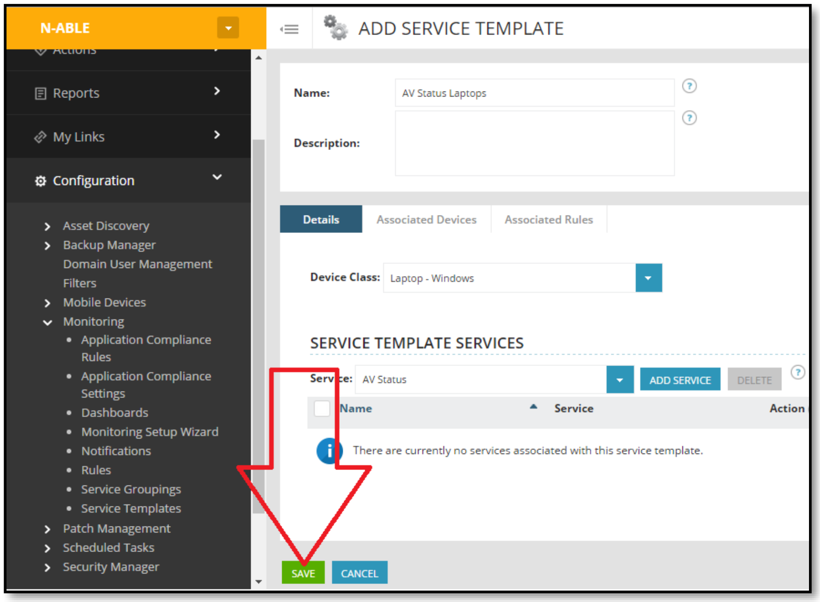
Name: AV Status

DETAILS

Use Default Values

Scan Interval: 15 ☑

9: Do not forget to hit **Save** again!



ADD SERVICE TEMPLATE

Name: AV Status Laptops

Description:

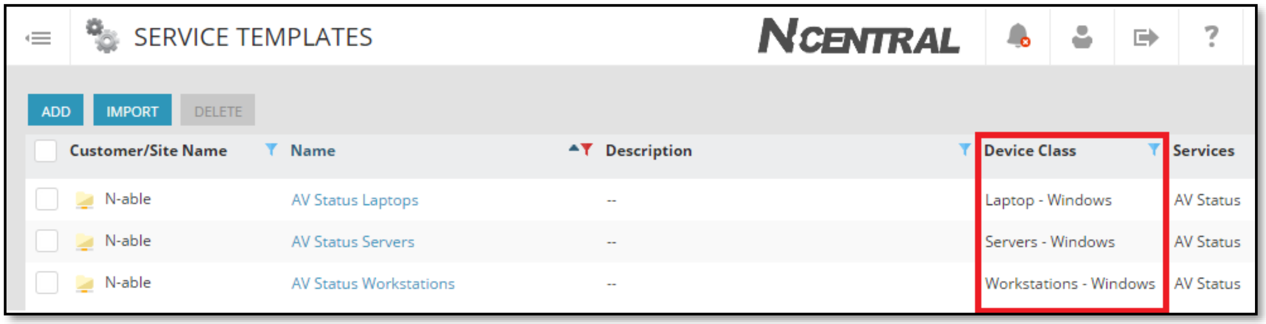
Device Class: Laptop - Windows

SERVICE TEMPLATE SERVICES

Service: AV Status

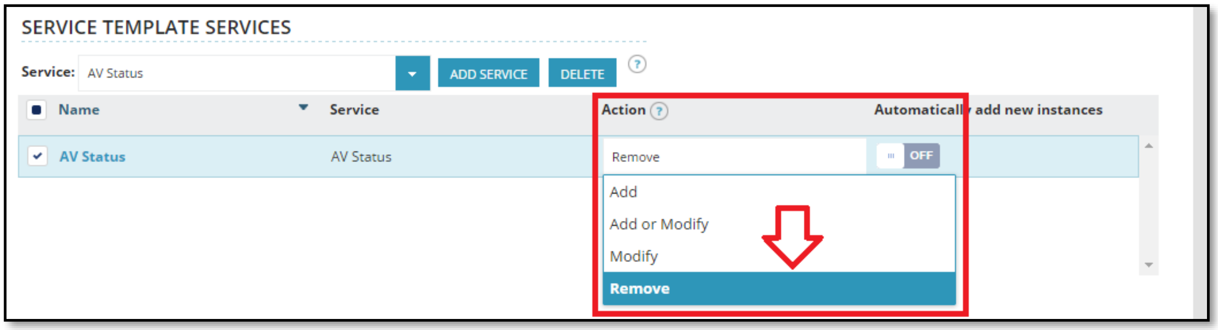
There are currently no services associated with this service template.

7. Repeat this process for Workstations and Servers. Service templates are tied to device classes, which requires a separate template. The templates cannot be cloned. The goal is to have three templates as such (ensure the device classes are unique!):



Customer/Site Name	Name	Description	Device Class	Services
N-able	AV Status Laptops	--	Laptop - Windows	AV Status
N-able	AV Status Servers	--	Servers - Windows	AV Status
N-able	AV Status Workstations	--	Workstations - Windows	AV Status

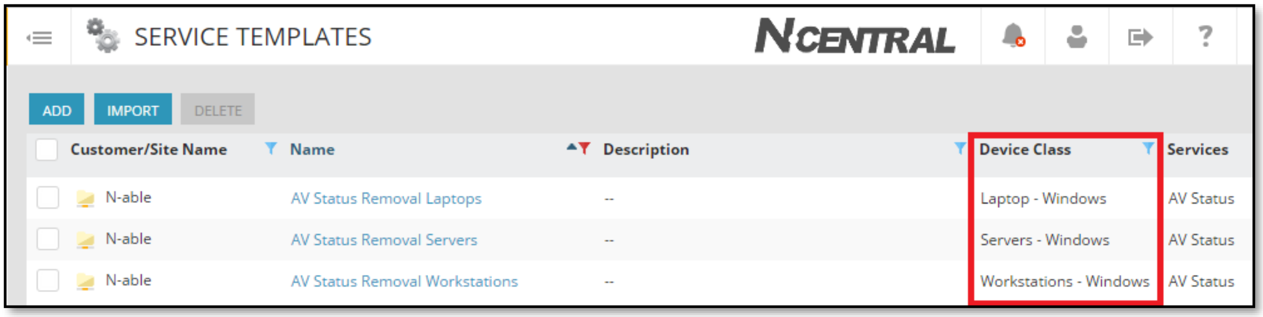
8. Create three more service templates, this time that remove the AV Status service. This template is used when applying AV Defender to devices that already have AV Status applied to them, cleaning up the monitored services. The templates created are largely identical (see step 6), except for this difference.



Service: AV Status

Name	Service	Action	Automatically add new instances
☑ AV Status	AV Status	Remove	OFF

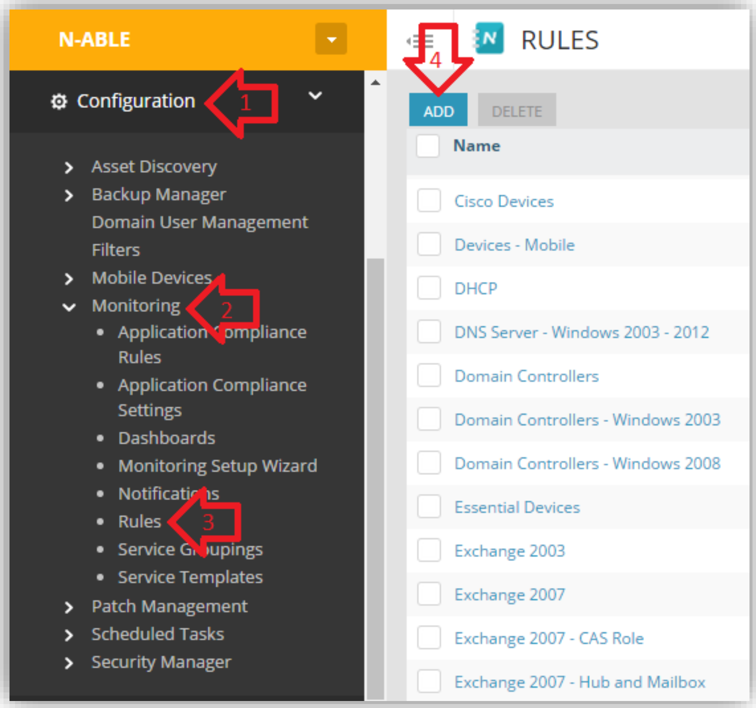
9. The goal is to have 3 more templates that remove AV Status, as such (ensure the device classes are unique again!):



Customer/Site Name	Name	Description	Device Class	Services
N-able	AV Status Removal Laptops	--	Laptop - Windows	AV Status
N-able	AV Status Removal Servers	--	Servers - Windows	AV Status
N-able	AV Status Removal Workstations	--	Workstations - Windows	AV Status

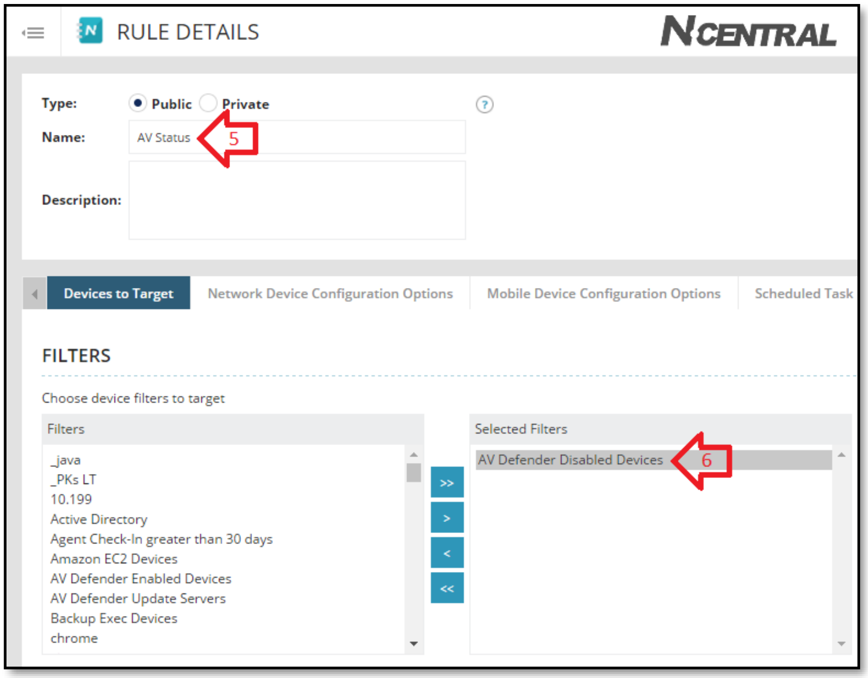
10. Create a Rule to deploy the script and apply the service templates. This will tie together all that was created so far. At your service organization level navigate to:

    1: Configuration >
    2: Monitoring
    3: Rules
    4: Add



Name
Cisco Devices
Devices - Mobile
DHCP
DNS Server - Windows 2003 - 2012
Domain Controllers
Domain Controllers - Windows 2003
Domain Controllers - Windows 2008
Essential Devices
Exchange 2003
Exchange 2007
Exchange 2007 - CAS Role
Exchange 2007 - Hub and Mailbox

    5: Name the rule 'AV Status'
    6: **Devices to Target tab** – AV Defender Disabled Devices


RULE DETAILS
NCENTRAL
5
Devices to Target
Network Device Configuration Options
Mobile Device Configuration Options
Scheduled Task
>>
>
<
<<
6

Type: ● Public ○ Private

Name: AV Status

Description:

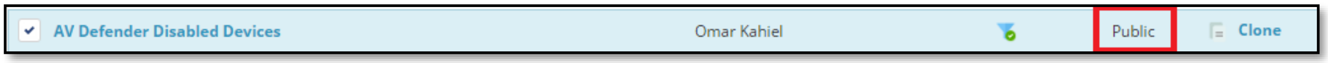
FILTERS

Choose device filters to target

Filters: _java, _PKs LT, 10.199, Active Directory, Agent Check-In greater than 30 days, Amazon EC2 Devices, AV Defender Enabled Devices, AV Defender Update Servers, Backup Exec Devices, chrome

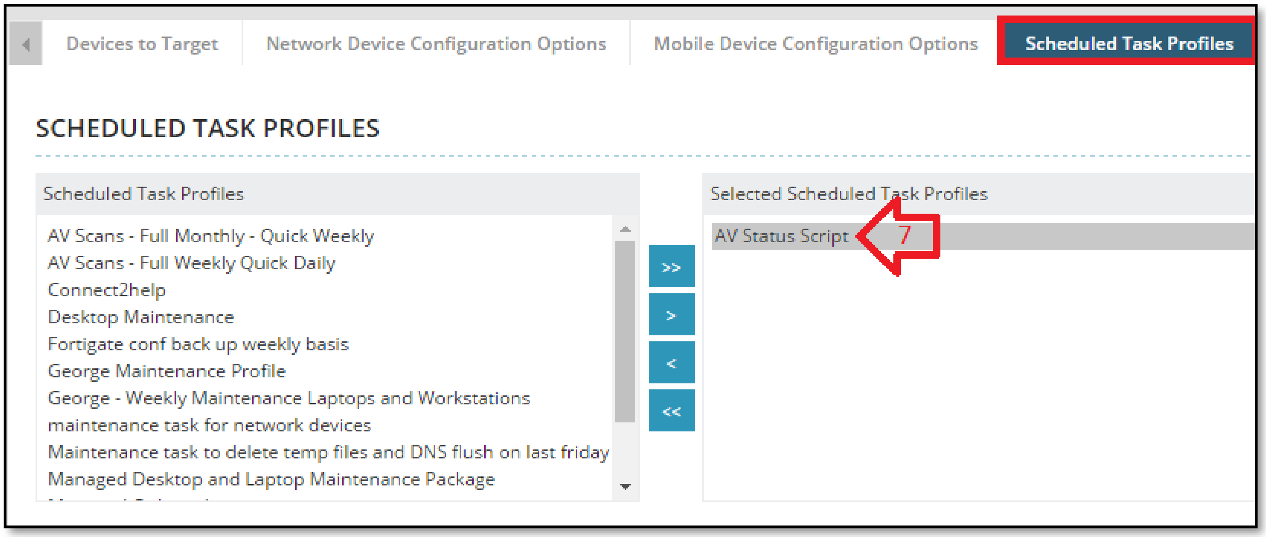
Selected Filters: AV Defender Disabled Devices

i. If the filter is not there, ensure it is public from Configuration > Filters



✓ AV Defender Disabled Devices	Omar Kahiel	Public	Clone

7: **Scheduled Task Profiles tab** – AV Status Script


Devices to Target
Network Device Configuration Options
Mobile Device Configuration Options
Scheduled Task Profiles
>>
>
<
<<
7

SCHEDULED TASK PROFILES

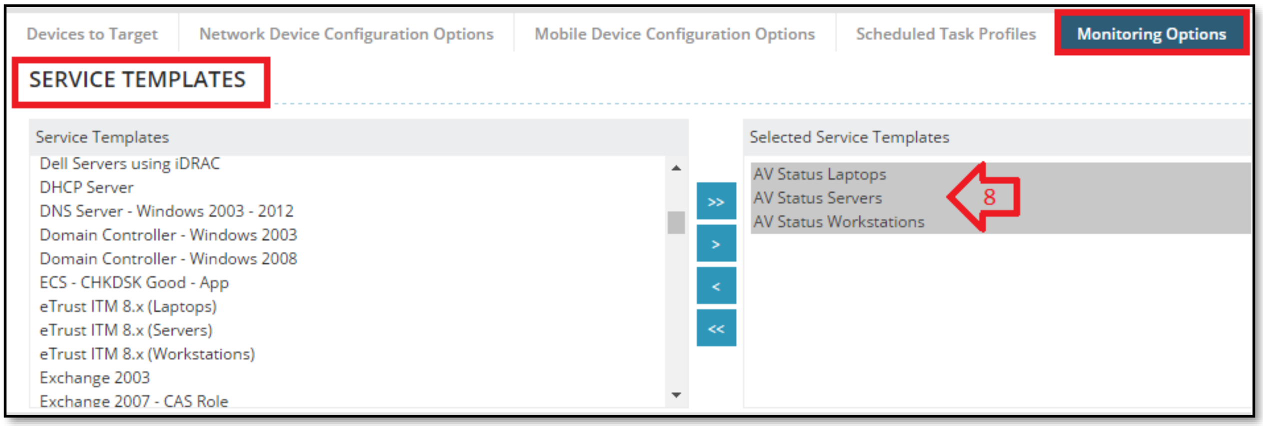
Scheduled Task Profiles

- AV Scans - Full Monthly - Quick Weekly
- AV Scans - Full Weekly Quick Daily
- Connect2help
- Desktop Maintenance
- Fortigate conf back up weekly basis
- George Maintenance Profile
- George - Weekly Maintenance Laptops and Workstations
- maintenance task for network devices
- Maintenance task to delete temp files and DNS flush on last friday
- Managed Desktop and Laptop Maintenance Package

Selected Scheduled Task Profiles

- AV Status Script

8: **Monitoring Options tab** – Service Templates – AV Status Laptops/Workstations/Servers


Devices to Target
Network Device Configuration Options
Mobile Device Configuration Options
Scheduled Task Profiles
Monitoring Options
>>
>
<
<<
8

SERVICE TEMPLATES

Service Templates

- Dell Servers using iDRAC
- DHCP Server
- DNS Server - Windows 2003 - 2012
- Domain Controller - Windows 2003
- Domain Controller - Windows 2008
- ECS - CHKDSK Good - App
- eTrust ITM 8.x (Laptops)
- eTrust ITM 8.x (Servers)
- eTrust ITM 8.x (Workstations)
- Exchange 2003
- Exchange 2007 - CAS Role

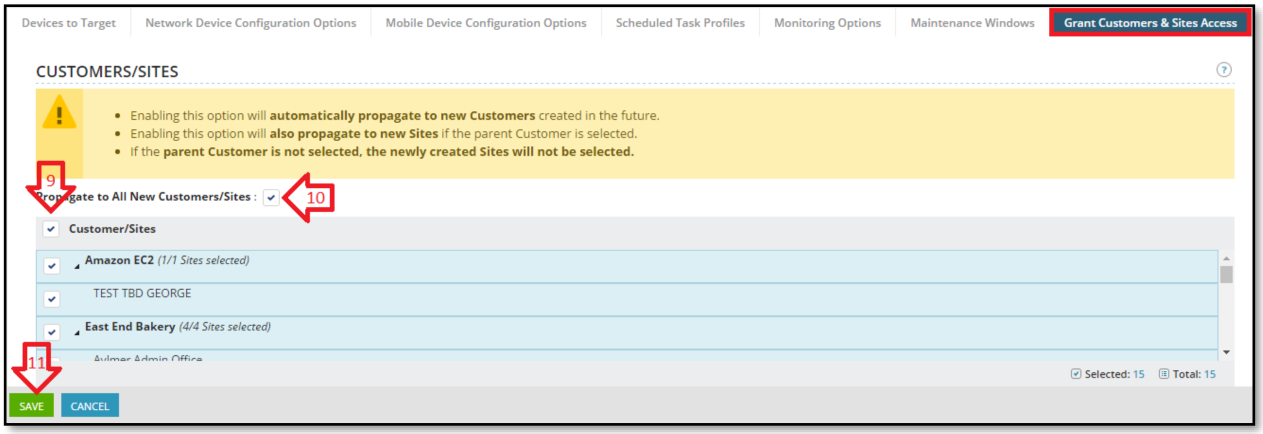
Selected Service Templates

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

9: **Grant Customers & Sites Access tab** – All Customers All Sites

10: Propagate to All New Customers/Sites

11: Save!


Devices to Target
Network Device Configuration Options
Mobile Device Configuration Options
Scheduled Task Profiles
Monitoring Options
Maintenance Windows
Grant Customers & Sites Access
9
10
11
SAVE
CANCEL

CUSTOMERS/SITES

- Enabling this option will **automatically propagate to new Customers** created in the future.
- Enabling this option will **also propagate to new Sites** if the parent Customer is selected.
- If the **parent Customer is not selected, the newly created Sites will not be selected.**

Propagate to All New Customers/Sites : ☑

☑ **Customer/Sites**

☑ **Amazon EC2** *(1/1 Sites selected)*

☑ TEST TBD GEORGE

☑ **East End Bakery** *(4/4 Sites selected)*

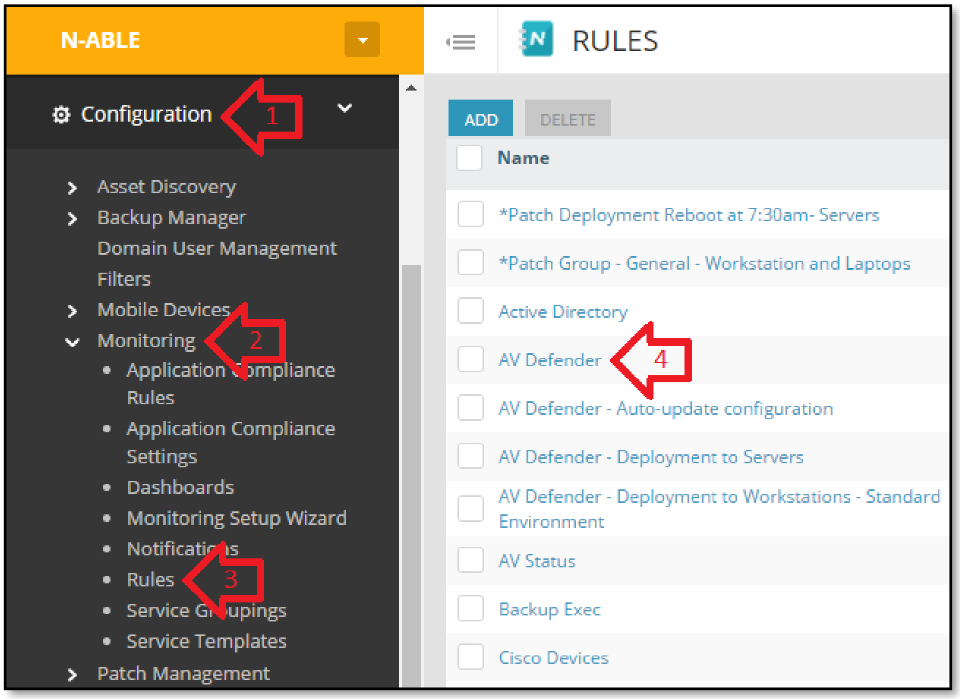
Aylmer Admin Office

☑ Selected: 15 Total: 15

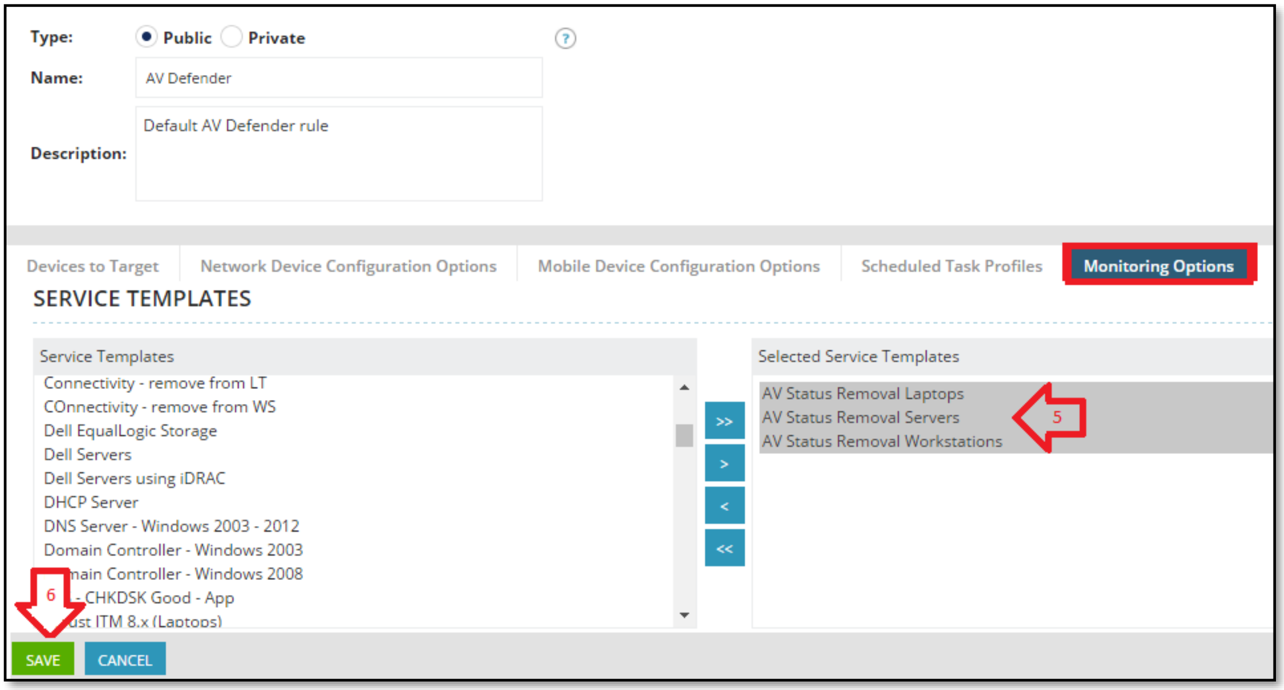
1-Oct-20 Author: Chris Reid

11. The removal templates can be added to a pre-existing Rule, at your Service Organization level navigate to:

   1: Configuration
   2: Monitoring
   3: Rules
   4: AV Defender


N-ABLE
RULES
Configuration
1
Asset Discovery
Backup Manager
Domain User Management
Filters
Mobile Devices
Monitoring
2
Application Compliance Rules
Application Compliance Settings
Dashboards
Monitoring Setup Wizard
Notifications
Rules
3
Service Groupings
Service Templates
Patch Management
ADD
DELETE
Name
*Patch Deployment Reboot at 7:30am- Servers
*Patch Group - General - Workstation and Laptops
Active Directory
AV Defender
4
AV Defender - Auto-update configuration
AV Defender - Deployment to Servers
AV Defender - Deployment to Workstations - Standard Environment
AV Status
Backup Exec
Cisco Devices

   5: **Monitoring Options tab** – Service Templates – AV Status Removal Laptops/Workstations/Servers
   6: **Save**!



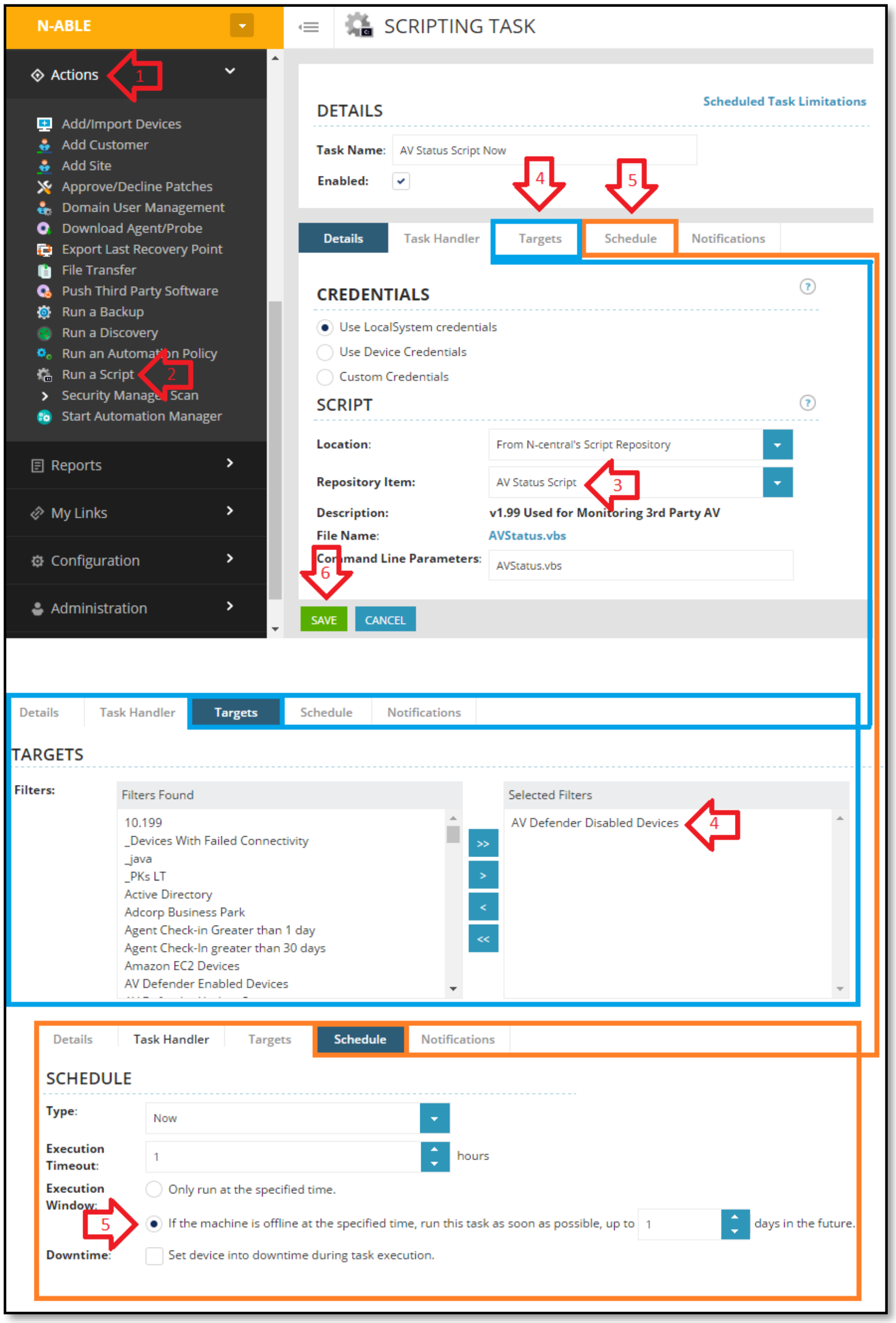
Type: ● Public ○ Private

Name: AV Defender

Description: Default AV Defender rule

Devices to Target
Network Device Configuration Options
Mobile Device Configuration Options
Scheduled Task Profiles
Monitoring Options
SERVICE TEMPLATES
Service Templates
Connectivity - remove from LT
COnnectivity - remove from WS
Dell EqualLogic Storage
Dell Servers
Dell Servers using iDRAC
DHCP Server
DNS Server - Windows 2003 - 2012
Domain Controller - Windows 2003
Domain Controller - Windows 2008
- CHKDSK Good - App
ust ITM 8.x (Laptops)
>>
>
<
<<
Selected Service Templates
AV Status Removal Laptops
AV Status Removal Servers
AV Status Removal Workstations
5
6
SAVE
CANCEL

12. At this point, the configuration is complete, and the AV Status Script will run on the scheduled time back on step 5-11. If you would like to run the script now, Navigate to:
    1: Actions >
    2: Run a Script
    3: AV Status Script
    4: **Targets** > AV Defender Disabled Devices
    5: **Schedule** > If the machine is offline, run this task as soon as possible…
    6: **Save**!



DETAILS

Task Name: AV Status Script Now

Enabled: ☑

CREDENTIALS

● Use LocalSystem credentials
○ Use Device Credentials
○ Custom Credentials

SCRIPT

Location: From N-central's Script Repository

Repository Item: AV Status Script

Description: v1.99 Used for Monitoring 3rd Party AV

File Name: AVStatus.vbs

Command Line Parameters: AVStatus.vbs

SAVE CANCEL

TARGETS

Filters:

Filters Found
10.199
_Devices With Failed Connectivity
_java
_PKs LT
Active Directory
Adcorp Business Park
Agent Check-in Greater than 1 day
Agent Check-In greater than 30 days
Amazon EC2 Devices
AV Defender Enabled Devices

Selected Filters
AV Defender Disabled Devices

SCHEDULE

Type: Now

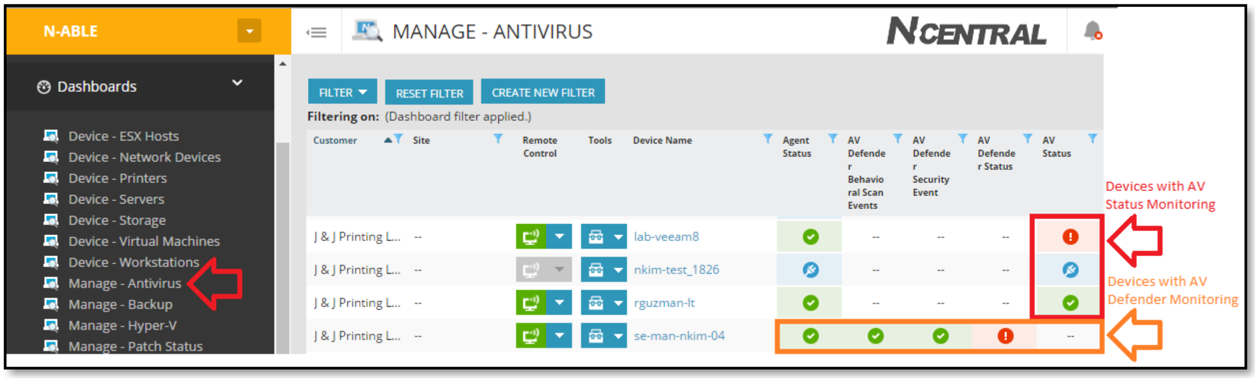
Execution Timeout: 1 hours

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 1 days in the future.

Downtime: ☐ Set device into downtime during task execution.

Confirmation

In order to confirm if the monitoring works correctly, there is already a dashboard you can leverage.
Navigate to Manage –Antivirus under dashboards:



Filtering on: (Dashboard filter applied.)

Customer	Site	Remote Control	Tools	Device Name	Agent Status	AV Defender Behavioral Scan Events	AV Defender Security Event	AV Defender Status	AV Status
J & J Printing L...	--			lab-veeam8	✓	--	--	--	!
J & J Printing L...	--			nkim-test_1826	⊗	--	--	--	⊗
J & J Printing L...	--			rguzman-lt	✓	--	--	--	✓
J & J Printing L...	--			se-man-nkim-04	✓	✓	✓	!	--

Devices with AV Status Monitoring

Devices with AV Defender Monitoring

As for the Status Icons:

- Normal: Monitoring working correctly and a 3rd Party AV was found and is up to date
- Failed: Monitoring working correctly and a 3rd Party AV **was not found** or is out of date
- Disconnected: Workstation/Laptop offline
- Misconfigured: Script didn't run
- **No Data**: Still running first scan
- Stale: Agent is offline

The process is complete, to summarize:

- A filter was created to identify devices with and without AV Defender
- A service template was created to apply monitoring of AV Status
- Another template was created to remove AV Status
- A scheduled task profile was created to run the AV Status Script
- A rule was created to tie it all together and automatically deploy AV Status to current and new devices.

FAQ

What A/V Products does the AV Status script support?

- Avast 9.0
- AVG 2012 (for Windows Vista/7/8 only - Server-class OS' are not supported)
- AVG 2013 (for Windows Vista/7/8 only - Server-class OS' are not supported)
- AVG Antivirus Business Edition (2013) (for Windows Vista/7/8 only - Server-class OS' are not supported)
- AVG 2014 (desktop and server)
- AVG Business Security 18.8
- AVG Protection
- Avira AntiVirus 12.x
- Avira Antivirus 10.x (Server)
- Bitdefender Endpoint Security Tools
- Carbon Black Cloud
- Cisco Advanced Malware Protection (AMP) – *detection of the product only*
- Cylance Protect
- ESET Endpoint Antivirus
- ESET Endpoint Security
- ESET File Security
- ESET Mail Security
- ESET NOD32 Antivirus 4.x
- ESET NOD32 Antivirus 5.x
- ESET NOD32 Antivirus 6.x
- FortiClient AV 6.x
- F-Secure Client Security 8.x, 9.x
- F-Secure Protection Suite Business (PSB) 4.x
- FireEye Endpoint Security
- Kaspersky 6.0
- Kaspersky 8.0
- Kaspersky 6.0 Enterprise
- Kaspersky 8.0 Enterprise
- Kaspersky Endpoint Security 10 for Windows
- Kaspersky Endpoint Security 10 SP1 for Windows
- Kaspersky Endpoint Security 10 SP2 for Windows
- Kaspersky Endpoint Security 11 for Windows
- Kaspersky Anti-Virus 2012
- Kaspersky Small Office Security 2
- Kaspersky Small Office Security 3
- McAfee Antivirus 8.7 thru 8.8
- McAfee Endpoint Security 10
- McAfee Endpoint Security 10.1
- McAfee Move AV Client 5.0

- McAfee Security-As-A-Service 5.x
- Microsoft Defender
- Microsoft Forefront
- Microsoft Security Essentials (MSE)
- Microsoft System Center Endpoint Protection (SCEP)
- Norman Anti Virus
- Panda Adaptive Defence 360
- Panda Cloud Endpoint Protection 6.11
- SentinelOne Endpoint Security
- Sophos Antivirus 9.x
- Sophos Antivirus 10.6 and above
- Sophos Endpoint Protection
- Symantec Antivirus
- Symantec Endpoint Protection 11.x and 12.x
- Symantec Endpoint Security
- Symantec Endpoint.Cloud 20.x and above
- Symantec Endpoint Protection - SBE2013
- Total Defense r12
- Trend Micro Apex One Security
- Trend Micro Deep Security Agent
- Trend Micro Messaging Security Agent
- Trend Micro OfficeScan
- Trend Micro Worry-Free Business Security 16
- Trend Micro Worry-Free Business Security 6.x
- Trend Micro Worry-Free Business Security 7.x
- Trend Micro Worry-Free Business Security 8.x
- Trend Micro Worry-Free Business Security 9.x
- Trend Micro Worry-Free Business Security Services
- Trend Micro WFBSH Agent
- Vipre Antivirus 4.x
- Vipre Enterprise Agent 4.x
- Vipre Antivirus Business 5.x
- Vipre Antivirus 2012
- Vipre Business Agent (ThreatTrack Security, Inc)
- Vipre Business Online 6.x
- Webroot SecureAnywhere
- Windows Defender

What AV Products are not supported by the AV Status script?

Any AV products not explicitly listed above are unsupported by the AV Status script. Notable mentions include AVG CloudCare, AV Defender, and Bitdefender.