N-central Deployment Best Practices



Table of Contents

Step 1 – Create the Customer in N-central	4
Step 2 – Readying the environment	5
Probe Admin Account Creation	5
Network Equipment Changes to SNMP	5
Group Policy Changes to Windows Firewall	5
Ports Required for Agents/Probes	8
ESX(i) Host Preparation	8
DNS Scavenging	9
Server Preparation for Hardware Monitoring	10
Supported Software for Monitoring	10
Step 1a: Install Windows SNMP Software for Windows Vista, 7, 2008 and Newer	10
Step 1b: Install Windows SNMP Software for Windows XP and Windows 2003	11
Step 2: Configure the SNMP Windows service	11
Step 3: Discover the Server Using a Windows Probe	11
Step 4: Apply Service Templates	12
On Premise Only: Check Appliance Settings	13
Initial Discovery and Import of Devices	14
Method A – Automated Deployment: N-able Probe	14
Step 3A – Download a Probe	14
Step 4A – Initial Discovery and Import in a Domain	16
Step 5A – Importing Remaining Devices (Device Class: Other)	19
Method B – Automated Deployment: Previous RMM Tools	21
Step 3B – Customer Specific Agent EXE	21
Step 4B – Discovery Defaults	22
Step 5B – Import Devices	22
Method C – Automated Deployment: GPO Script	23
Step 3C – Download GPO Script	23
Step 4C – Deploy GPO Script	23
Step 5C – Use GPO Script	23
Method D – Manual Deployment: Public Link	25
Step 3D – Copy Public Link Address	25

Step 4D – Discovery Defaults	26
Step 5D – Import Devices	26
Step 6 – Setup Recurring Discoveries for New Assets	27
Step 7 – MAC OS X Agent	29
Appendix A – Probe Troubleshooting and Admin Password reset	31
Appendix B – Troubleshooting SNMP configuration	33

Step 1 – Create the Customer in N-central

Create a Customer in N-central. If you have no customers added in, the landing page is the same as navigating to:

- 1. Service Organization Level (SO Orange) > Actions > Add Customer/Site
- 2. Provide a name, it must be different than the SO level and any other Customer
- 3. License Type: Select Professional, you can change the setting afterwards if required
 - > Optional: Map to the corresponding PSA.
- 4. Network Credentials, provide **Domain Admin** credentials (domain\username) and Password (do not leave as "Inherit").
 - If there is no Domain, an administrative set of credentials is required. If no common set of credentials are available, tasks default to LocalSystem credentials. These credentials are not used for deployment of agents.
- 5. Click "Save and Continue". You will now be at your new Customer level (Green).



Step 2 – Readying the environment

Before deploying, review the below headings and see if any are applicable to your environment and desired devices to discover and manage. The bolded headings are absolutely necessary for production environments. For On-Premise environments there is one additional step.

- Probe Admin Account Creation
- \succ
- Network Equipment Changes to SNMP
- Group Policy Changes to Windows Firewall
- Ports Required for Agents/Probes
- ESX(i) Host Preparation
- DNS Scavenging
- Server Preparation for Hardware Monitoring
- On Premise Only: Check Appliance Settings

Probe Admin Account Creation

Create an account in the clients Active Directory that is part of the **Domain Admins** group (ie. full domain administrative privileges) and a **password that never expires**. We will give this account to the Windows Probe during installation to allow for Agent install and a host of other functions. If you ever need to reset the probe password, simply re-install the probe or refer to <u>Appendix A –</u> <u>Probe Troubleshooting and Admin Password reset</u>. The password cannot be reset from within the N-central UI.

NOTE: The account name cannot be longer than 20 characters

Network Equipment Changes to SNMP

Ensure SNMP is enabled on all network devices with Read Only access. Ensure SNMP is set to accept packets from the probe. Refer to <u>Appendix B – Troubleshooting SNMP configuration</u> for additional help.

- Refer to your device documentation on how to setup SNMP. Some devices require SNMP to be turned on in multiple locations such as both Administration and the LAN interface.
- The probe acts as a Syslog server or SNMP Trap Receiver. If you are planning to monitor Syslog/Traps point the output to the Probe.

NOTE: Most devices will already default to community string of 'public' as will N-central. If you choose to change this you will need to be diligent in changing this string when running your discoveries. SNMP settings in N-central on individual devices is located on their respective Properties tabs.

Group Policy Changes to Windows Firewall

During discovery from the probe, Windows Devices may get discovered as a Device Class of **"Other"**. Perform these necessary changes to ensure a smooth deployment process along with remote control and ping functionality.

Create a New GPO Object

Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Windows Firewall >

- 1. Allow inbound file and print sharing exception
- 2. Allow ICMP exceptions
- 3. Allow inbound remote administration exception

The numbered images below reference the three above GPO Changes.

NOTE: Where referenced for an IP address in steps 1 and 3, you can either type in * to allow messages from any network, or the IP of the probe.





2	æ w	/indows Firewall: Allow ICMP exceptions – 🗖 💌
2	Windows Firewall: Allow ICMP exce	ptions Previous Setting Next Setting
	 Not Configured Enabled Disabled Supported on: 	At least Windows XP Professional with SP2
	Options:	Help:
	 Allow outbound destination unreach Allow outbound source quench Allow redirect Allow inbound echo request Allow inbound router request Allow outbound time exceeded Allow outbound parameter problem Allow inbound timestamp request Allow inbound mask request Allow outbound packet too big 	able Defines the set of Internet Control Message Protocol (ICMP) message types that Windows Firewall allows. Utilities can use ICMP messages to determine the status of other computers. For example, Ping uses the echo request message, If you do not enable the "Allow inbound echo request message type, Windows Firewall blocks echo request messages sent by Ping running on other computers, but it does not block outbound echo request messages sent by Ping running on this computer. If you enable this policy setting, you must specify which ICMP message types Windows Firewall allows this computer to send or receive. If you disable this policy setting, Windows Firewall blocks all the listed incoming and outgoing ICMP message types. As a result, utilities that use the blocked ICMP message swill not be able to send those messages to or from this computer. If you enable this policy setting, Windows Firewall deletes the list of message types that you had enabled.
		OK Cancel Apply

2	Windows Firewall: Allow inbound remote administration exception				
3	Windows Firewall: Allow inbound remote administration exception Previous Setting Next Setting				
	 Not Configured Enabled Disabled Supported on: At least Windows XP Professional with SP2				
	Options: Help:				
	Allow unsolicited incoming messages from these P addresses: * Allows remote administration of this computer using administrative tools such as the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). To do this, Windows Firewall opens TCP ports 135 and 445. Services typically use these ports to communicate using remote procedure calls (RPC) and Distributed Component Object Model (DCOM). Additionally, on Windows XP Professional with at least Syntax: Type *** to allow messages from any network, or else type a comma-separated list that contains any number or combination of these: IP addresses, such as 10.0.0.1 Subnet descriptions, such as 10.2.3.0/24 The string "localsubnet" Example: to allow messages from 10.0.0.1, 10.0.0.2, and from any system on the Local subnet or on the 10.3.4 x subnet Allows remote administration of this computer using administrative tools such as the Microsoft Management Console (MMC) and Windows Sirewall opens TCP ports 135 and 445. Services typically use these ports to communicate using remote procedure calls (RPC) and Distributed Component Object Model (DCOM). Additionally, on Windows SYP Professional with at least SP2 and Windows Server 2003 with at least SP1, this policy setting allow and allows About Services to open additional dynamically-assigned ports, typically in the range of 1024 to 1034. On Windows Vista, this policy setting does not control connections to SVCHOST.EXE and LSASS.EXE. If you enable this policy setting, Windows Firewall allows the computer to receive the unsolicited incoming messages associated with remote administration. You must specify the IP addresses or subnets from which these incoming messages are allowed. If you disable or do not configure this policy setting, Windows				
	OK Cancel Apply				

If you require additional assistance with these GPO changes, please refer to this video which will walk you through the process: <u>https://www.dropbox.com/s/l434n4ibyc0ljvp/__Gpo-configuration-for-best-practice-deployment-DNS-scavenging.mp4</u>

Group Policy changes are not immediate, you can perform an immediate update by issuing the command: **gpupdate /force**

Ports Required for Agents/Probes

The N-central agents and probes will be sending minimal traffic over ports 443 (HTTP), 80 (HTTPS) and 22 (SSH). Please refer to the Release Notes on the NRC for additional ports.

https://nrc.n-able.com/support/Pages/ProductDocumentation.aspx

ESX(i) Host Preparation

Install the "offline bundle". These bundles are available from your server hardware vendor and will allow you to monitor items such as physical drives and RAID status on your ESX(i) host. Assistance with this install including picking the correct bundle and loading the "vib" files into your system may require you to approach your vendor for assistance.

DNS Scavenging

Configure DNS Scavenging every 12 hours for stale records.

- This setting will help ensure that environments using DHCP do not detect duplicate devices based on multiple DNS entries for the same device.
- No-refresh and Refresh combined should be equal to or less than your DHCP lease. For example, with an 8 day DHCP lease set the No-refresh to 4, and the Refresh to 4.
- While in your DNS server, choose to "Scavenge Now" to get the process started.

one Aging/Scavengin	g Properti	es		×
Scavenge stale reso	urce records			
No-refresh interval				
The time between the and the moment whe	e most recen n the timesta	t refresh of amp may be	a record time refreshed ag	stamp ain.
No-refresh interval:			•	
Refresh interval				
be refreshed and the scavenged. The refre record refresh period	earliest mor esh interval r	nent when the nust be longe	e record can er than the m	be aximum
Refresh			•	
D.				
			× _	Cancel

Server Preparation for Hardware Monitoring

1. Install server management software on physical servers. Refer to your server documentation for details. Be sure to install full suites. The Dell Open Manage "Essentials" package for instance is not adequate.

Supported Software for Monitoring

- o Dell OpenManage
- HP Systems Insight Manager Agent
- **IBM ServeRAID** (for RAID-level monitoring) and the **IBM Director Platform agent** (for hardware-level monitoring)
- Intel System Management Software
- 2. Once the software is installed, ensure SNMP is enabled with Read Only access. Ensure SNMP is set to accept packets from the probe.

NOTE: Most devices will already default to community string of 'public' as will N-central. If you choose to change this you will need to be diligent in changing this string when running your discoveries. SNMP settings in N-central on individual devices is located on their respective Properties tabs.

Step 1a: Install Windows SNMP Software for Windows Vista, 7, 2008 and Newer

1. **Programs and Features – Turn Windows features on or off** – Simple Network Management Protocol (SNMP).



Step 1b: Install Windows SNMP Software for Windows XP and Windows 2003

 Add or Remove Programs – Add/Remove Windows Components – Select Simple Network Management Protocol (SNMP).

Note: For Windows XP and Windows 2003, this is a sub-component of the Management and Monitoring Tools component.

The Windows SNMP software will be installed. A reboot may be required.

Step 2: Configure the SNMP Windows service

- 1. Navigate to Windows Services and configure the SNMP Service
- 2. Select the Security tab. If the tab is unavailable then a reboot is required.
- 3. Add in a community string with READ ONLY access.
- 4. Select Accept SNMP Packets from any host.

2	Ser	vices
2	Name Routing and Remote Access RPC Endpoint Mapper Secondary Logon Secure Socket Tunneling Protocol Service Security Accounts Manager Security Center Sensor Monitoring Service Server Shell Hardware Detection Smart Card Smart Card Device Enumeration Service Smart Card Removal Policy SNMP Service Shume Protection Spot Verifier SQL Server VSS Writer SSDP Discovery Steam Client Service	Vices SNMP Service Properties (Local Computer) × General Log On Recovery Agent Traps Security Dependencies Send authentication trap Image: Community names Accepted community names Rights Jublic READ ONLY Add Edit Remove Accept SNMP packets from any host Accept SNMP packets from these hosts Image: Accept SNMP packets from these hosts
	Still Image Acquisition Events Storage Service Superfetch	OK Cancel Apply

Optional Step: Discover the Server Using a Windows Probe

Perform this step if you're adding in a few servers after initial discovery and import. If you're discovering the whole subnet, jump to the link below Step4A. A Windows Probe must be used to discover the server. The exact same steps can be followed as <u>Step 4A – Initial Discovery and Import in a Domain</u>. Where referenced for an IP Range, provide just the singular IP of the server. Ensure the Discovery SNMP settings correspond to how it was configured on the device.

Step 3: Apply Service Templates

Once the device has been discovered in N-central,

1. Verify that SNMP has been enabled on the Settings – Monitoring Options Tab

2							
5	🕥 se-a	us-sp-02 [Dell				
	Overview	Tools N	Ionitoring	Asset	Notes	Settings	Remote
	Properties	Local Agent	Monitorir	g Options	Downtime	Maintenance	Windows
	SNMP SET	TTINGS					
	Use SNMP:		·	 Image: A set of the set of the			
	SNMP Version	n		v1			•
	Port:			161			
	Community S	String:		nabletech!			
	Timeout (ms)	:		500			
	Number of Re	etries:		3			÷

2. Re-Apply the template if it is already there, or Apply New Service Templates

Λ	E DEVICE DETAILS					
4	🕥 se	-aus-sp-02	2 Dell			
	Overview	Tools	Monitoring	Asset	Notes	Settings
	Status	Ticketing	Associations	Service	Templates	Security Event
	APPLY NEW S	SERVICE TEMPLAT	E RE-APPLY SERV	ICE TEMPLATE	REMOVE AS	SOCIATION
	🔳 🖉 🔳	mer/Site Name	Y Nam		L	^
	N	-Able Technolog	ies Dell S	Servers (N-Able	e Technologies))

NOTE: Other templates for other servers may be applied. **Do not delete them**. They are applied automatically from the Servers – Windows Rule. They do not apply anything as they rely on Asset Info. The only one that needs to be manually applied is the HP Servers Template.

Г	Image: Image					
3	Se-aus-sp-02 Dell					
	Overview	Tools	Monitoring	Asset	Notes	S
	Status	Ticketing	Associatior	ns Service	e Templates	Sec
	CREATE TICK	ETS ADD	DELETE CREAT	E SERVICE TEMP	LATE SERVICE	E MON
	Fan ((Dell) - System E	oard FAN 4 RPM			
	Logi	cal Drive (Dell O	M 2.2) - 1		0	
	Logi	cal Drive (Dell O	M 2.2) - 2		0	
	Phys	sical Drive (Dell)	- Physical Disk 0:0	:0	0	

3. Click on the Status tab to verify the services that were added to the device.

On Premise Only: Check Appliance Settings

In the event there is any communication errors check to see what address the Agents and Probes communicate with. Navigate to:

Service Organization > Administration > Defaults > Appliance Settings

N-ABLE TECHNOLOGIES	ie 💲 Api	PLIANCE SETTIN	GS		
Administration	Communication S	Settings Upgrades	Credentials	Network	Agent
Branding Certificate Management	COMMUNIC	ATION SETTINGS		Pro	pagate 🍞
Custom Device Properties Customers/Sites	Protocol: Server Address:	HTTPS		•	
Appliance Settings Backup and SNMP		Server Address			
Defaults Backup Share Customized System Email 		sedemo1.n-able	.com	A	
Data Retention Device Defaults		Ensure this ad	dress is corr	act	
Discovery Defaults		LIISUIC UIIS au		CCL	

Initial Discovery and Import of Devices

Four different methods are available to deploy agents and probes depending on the environment.

- Method A Automated Deployment: N-able Probe
- Method B Automated Deployment: Previous RMM Tools
- Method C Automated Deployment: GPO Script
- Method D Manual Deployment: Public Link

Method A – Automated Deployment: N-able Probe

Step 3A – Download a Probe

Requirements: Administrator account; either a common Local Admin or Domain Admin on all devices.

Procedure: At the Customer Level (Green), download a probe to a device to be used for discovery

Customer Level (Green) > Actions > Download Agent/Probe > Windows Probe

CORK_OFFICE	•	😑 🔍 DOWNLOAD AGENT/PROBE	NOTE: The probe
Views	>	Customer/Site Specific Software System Software	public! Save time
🕲 Dashboards	>	CUSTOMER/SITE SPECIFIC SOFTWARE	by right clicking - copying the URL
♦ Actions	~	Windows Software	and paste it into a web browser on
Add/Import Devices			the remote server
👶 Add Customer/Site		➤ Windows Agent	
 Add Customer/Site Approve/Decline Patches Domain User Management Download Agent/Probe Export Last Recovery Point 		Windows Agent Windows Probe	NOTE: VERY IMPORTANT: The number before

During the Install Process:

- > Do not configure a **proxy** unless required
- > Do not enable the **AMT data store**
- > Provide the previously created <u>Probe Admin Account Creation</u> credentials when requested.
 - The domain field should not typically contain ".com", ".local" etc. You should only need to provide the domain name (ie: **Nable**Admin)
- It is recommended to not provide a **Discovery IP Range**. We will do this from within N-central after the probe is installed for more granular control.

🛃 Window	s Software Probe - InstallShield Wizard	NOTE: The install requires a
Credentials		set of credentials used for
Select the user account ty	ype and enter the username and password. N-able by solarwinds	deployment of agents. In a
		Domain Environment this
🔾 Local User	run asset discovery tasks.	must be a Domain
Demain Hann	The user account must have domain administrator privileges.	Administrator. In a
Domain User		Workgroup Environment,
O Workgroup User	The user account must be the local administrator for each of the	there must a common
	devices that is being remotely monitored.	administrator account across
Domain	7.0	all machines in order to
Username	Administrator	deploy the N-central agent. In
Deenward		absence of this account, the
Password		probe will be unable to
InstallShield	< <u>B</u> ack <u>N</u> ext > Cancel	deploy agents.

Confirm the Probe is installed by navigating to:

Administration > Probes

J&J PRINTING LTD.	😑 🔕 PROBES		N	CENTRAL	•	⇒ ? ⁵	/STEM TIME 3:47 PM
Administration	ADD DELETE TRANSFER TASKS UPGRADE	▼ STATE ▼ PATCH CACHING ▼	🔊 Windows Probe				
 Certificate Management Custom Device Properties 	Name 📤 Network Address	Status Key	Version	State Patch	Caching	Associated Notifications	100
> Defaults	exch-dag01 - 10.199.15.15 Windows	• 🥥 Key 🔻	10.0.0.1696	0		Manage	*
ProbesPSA Integration	se-nable-dc-01 - 10.199.15.10 Windows) 📀 Key 🕶	10.0.0.1696	0	6	Manage	
 Report Manager Service Management 		$\overline{}$					
SMS Registration		<u>ن</u>					
 Oser management 							

Step 4A – Initial Discovery and Import in a Domain

If you have chosen to skip the discovery from the probe and perform it within N-central, navigate to:

Customer Level (Green) > Actions > Run a Discovery



Any discoveries done from the probe are set to recur every day at time of install with default auto-import settings. Therefore it is highly recommended to split the discoveries into two parts:

- Step 4A Initial Discovery and Import in a Domain
 Step 5A Importing Remaining Devices (Device Class: Other)
- 2. Step 6 Setup Recurring Discoveries for New Assets

Perform the next steps. The numbered steps correspond with the numbers on the images.

- 1. Discover the entire IP Range, do not scan multiple subnets in one discovery.
- 2. Auto-Import all Desired Devices
- 3. Setup Notifications on both success and failure
- 4. Configure SNMP for all available Community Strings
- 5. Enable Virtualization Discovery with Credentials added in for any ESX(i) Host(s)
- 6. Set the Schedule to now or later, not Recurring.

1	E ADD DISCOVERY JOB		NCENTRAL -	₽ .
_	Name: First Discovery Job			
	Devices to Discover Auto Import Notif	ications SNMP Settings Advanced Settings	Virtualization Settings Schedule	
	Probe:	gvaskovitch-lt - Windows - 10.19.6.123		
	Discovery Type: IP Range	192.168.1.1-254	(Ex.192.168.10.5-200)	
	O IP Address and Netmask	N	255.255.255.0	





NOTE: Defaults are configured from Administration > Defaults > Backup and SNMP Defaults

Add in extra SNMP queries if they use a community string other than public

NOTE: Some equipment may lock down from several failed attempts via SNMP. If a discovery is configured with multiple community strings, the probe will attempt all of them on a configured number of retries until a response is found. A device may be locked out before the probe has a change to communicate with the proper string.

Г	Devices to Discover Auto Im	nport Notifications	SNMP Settings	Advanced Settings	Virtualization Settings	Schedule
<u> </u>	Perform Virtualization Discove CIM Ports:	ry: Scan Default CIM	Ports Ports			
		CIM Ports		Selected CIM Ports		
		5989	× ×		*	
		Add to the list of CIM	Ports		▼ ADD	DELETE
	Webservice Ports:	 Scan Default Web Scan Custom Web 	service Ports oservice Ports			
		Webservice Ports		Selected Webservice P	orts	
		443	× >>> < << < <		*	
		Add to the list of Web	service Ports		- A	DD DELETE
	ADD NEW ACCOUNT					
	User Name	▲ p	assword		Actions	800
	root	**	****		Enabled 🖀	Delete

Optional step only to be used only if ESX(i) environments are to be monitored. If vCenter is to be monitored, please refer to your solutions architect for how to setup monitoring.

Start Time: 14:49 Days of the Week: Every day of the week I Selected days of the week Sum Mon Tue Wed Thu Fri Sat All Clear Days of the Month: Every day I Selected dates 1 2 4 5 1 2 4 5 1 2 4 5 1 1 1 12 1 1 1 14 1 1 1 12	Start Time: 14:49 Days of the Week: Every day of the week (•) Selected days of the week Sum Mon Ture Wed The Pri Sat All Clear Days of the Month: Every day (•) Selected dates 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 23 24 25 26 27 28 29 30 31 All Clear	Туре:	Now		-	?	
Days of the Week: Every day of the week Selected days of the week Sun Mon Trie Wed This Fri Sat All Clear Days of the Month: Every day Selected dates 1 2 3 4 5 7 5 10 11 12 14 15 16 17 18 19 20	Days of the Week: Every day of the week Selected days of the week Sun Mon Tue Wed The Fri Sat All Clear Days of the Month: Every day Selected dates 1 2 3 4 5 6 7 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 26 25 30 31 All Clear 	Start Time:	14:49		-		
Sun Mon Tue Wed Thu Fri Sat All Clear Days of the Month: Every day Selected dates 1 2 3 4 5 7 8 9 10 11 12 14 15 16 17 18 19 20 21	Sun Mon Tue Wed Thu Pri Sat All Clear Days of the Monte: 	Days of the Week:	Every day of the	e week 💿 Select	ed days of the week		
Days of the Month: Every day Selected dates 1 2 3 4 5 7 1 2 3 4 5 6 7 1 1 1 1 1 1 1 1 15 16 17 18 19 2 2 1	Days of the Month: Every day Selected dates 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 All Clear		Sun Mon Tue				
1 Z 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 23 30 31 All Cleer	Days of the Month:	Every day	elected dates			
8 9 10 11 12 13 14 15 16 17 18 19 20 21	8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 All Clear						
15 16 17 18 19 20 21	15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 All Clear						
22 23 24 25 26 27 28	29 30 31 All Clear						
29 30 31 All Clear							

As this discovery is intended for the first import of devices, its schedule is set to <u>Now</u>. If the time does not satisfy you, you can't technically setup a discovery at a later time. However a <u>recurring</u> discovery set **at both** a specific day of the week and month would only occur on that specific day. For instance, Mon the 25th only occurs on May 25th **2015**, and the next instance is January 25th **2016**.

Once saved, the probe will scan the network and import all the devices that are classified properly.

Step 5A – Importing Remaining Devices (Device Class: Other)

Anything that is not properly classified will be found from the discovery job. Navigate to:

Customer Level (Green) > Actions > Add/Import Devices



If you ran multiple discoveries and wish to see the import report selectively, navigate to:

Customer Level (Green) > Configuration > Discovery Jobs

INTERNATIONAL DATA W/		Y JOBS		1	CENTRAL	≗	SYSTEM TIME 3:16 PM
🕸 Configuration 🛛 💙	ADD IMPORT ASSETS D	ELETE					
> Backup Manager 🤞	Name	Schedule	Last Report	Monitoring Applia	Network Target	Job Status	
Discovery Jobs	Discovery Job - 2014-12-1	2 11h04m Once	2014-Dec-12 11:15	SEHYPER-V - Windows	Range: 10.19.6.1-10	Completed	*
Domain User Management Filters	Discovery Job - 2014-12-1	2 11h12m Once	2014-Dec-12 11:34	SEHYPER-V - Windows	Range: 10.19.6.10-14	Completed	
Mobile Devices Monitoring Patch Management Scheduled Tasks Scrucity Management	Recurring Discovery- Inte	rnational Recurring	2015-May-21 10:19 25 of 32 Unmanaged	SEHYPER-V - Windows	Range: 192.168.10.1-254	Pending	

Common reasons and troubleshooting steps for a device to be discovered with a device class of **Other**:

	Windows
Reason	Solution
WMI permissions not allowing probe to pull OS type and therefore device could not be classified	Ensure Windows Firewall is turned off or configured: Group Policy Changes to Windows Firewall Changes to Windows Firewall
(WMI permissions not allowing probe to pull OS type and therefore device could not be classified.	\Admin\$ share of a device: <u>Probe Admin Account Creation</u>
I don't know why the device is not receiving an agent	Try leveraging N-central remote control – Remote Desktop after the device is imported into N-central. Remote Desktop is accessible with an Essentials License. Remote Desktop does not require a local agent, but it does require the device to be configured for it along with a monitored probe. Connection Type: Remote Desktop Custom Remote Desktop SSH Telnet Web
Reason	Solution
SNMP is not enabled on the device	Ensure SNMP is enabled with read only access to the probe: <u>Network Equipment Changes to</u> SNMP
SNMP is enabled with a different SNMP community string than configured within the Windows Probe Asset Discovery Task	Ensure the community string is defined in the discovery along with accepting packets from the probe. The timeout may need to be adjusted of the device is slower to respond: See Page 16
I don't know what this device is	Try leveraging N-central remote control - Web Page after the device is imported into N-central. Web Page is accessible with an Essentials License.

The overall goal is to have agents deployed to all Windows devices, and ESX/SNMP monitoring setup correctly as well. Troubleshoot the devices with the above information and see if the discovery can be improved. Nonetheless if the time benefit is greater to just manually deploy agents, then the public link can be distributed to devices (see <u>Method D – Manual Deployment: Public Link</u>). Jump to page 27 for the next step.

Method B – Automated Deployment: Previous RMM Tools

Step 3B – Customer Specific Agent EXE

Requirements: Previous RMM Tools such as LabTech, Continuum, Kaseya with a software push feature.

Procedure: Use the Customer Specific Agent Installer and deploy to all desired devices.

Customer Level (Green) > Actions > Download Agent/Probe > Windows Agent



C:\Users\omar.kahiel\Downloads>100WindowsAgentSetup.exe /s



Step 4B – Discovery Defaults

The agents that are being deployed will automatically be added in to your N-central dashboard. If you wish to have control over devices that are being imported, navigate to:

Customer Level (Green) > Administration > Defaults > Discovery Defaults

CORK_OFFICE	
E Views >	
⑦ Dashboards	NETWORK ADDRESS TYPE Image: Optimized state stat
♦ Actions >	Workstations/Laptops: IP Address FQDN
■ Reports >	
🗞 My Links 🔹 🕨	AUTO-ASSIGNED SERVICES
🕸 Configuration	Available Services Assigned Services
Administration	APC UPS - Temperature BES Message Status CCM Media Device
 Certificate Management Custom Device Properties Defaults Appliance Settings Backup and SNMP Defaults Backup Share 	CCM MGCP Gateway CCM Phone CCM Voicemail Device Cisco Unity Express Mailbox Citrix Presentation Server Window Snip Connectivity
Customized System Email Data Retention	AUTO IMPORT (7)
 Device Defaults Discovery Defaults Network Share Notification Templates Remote Control Defaults Remote Control Log Level Service Templates User Defaults Warranty Monitoring Probes PSA Integration 	Import Devices: Available Device Classes Assigned Device Classes Scanner/Camera Servers - ESXi Servers - Windows Servers - Generic Servers - Management Interface Servers - Windows Storage Suitch/Router Voip Phone Workstations - Generic C C Z - Pro node V V

Step 5B – Import Devices

If changes have been made to the discovery defaults, devices will have to be imported. Navigate to:

Customer Level (Green) > Actions > Add/Import Devices.



Jump to page 27 for the next step.

Method C – Automated Deployment: GPO Script

Step 3C – Download GPO Script

Requirements: No Domain or common admin account across all devices. Use this method when there is no access to your devices under management.

Procedure: Use the Group Policy Deployment Script for the Windows Agent, Navigate to:

Actions > Download Agent/Probe > System Software Tab > Windows Scripts

N-ABLE TECHNOLOGIES	•	😑 💽 DOWNLOAD AGENT/PROBE		
Views	>	Customer/Site Specific Software System Software Third Party Software		
🕙 Dashboards	>	SYSTEM SOFTWARE		?
♦ Actions	~	Windows Software	File Size	Version
Add/Import Devices		Windows Agent	16.94 MB	10.0.0.1696
 Approve/Decline Patches Domain User Management 		Windows Probe	11.65 MB	10.0.0.1696
Download Agent/Probe				
Export Last Recovery Point File Transfer		Windows Scripts	File Size	Version
 Push Third Party Software Run a Backup Run a Discovery 		Group Policy Deployment Script for the Windows Agent	1.00 KB	10.0.0.1696

Step 4C – Deploy GPO Script

The most effective method for using this script is through Group Policy Objects. In Group Policy, there are two methods of deploying scripts: **at computer startup or shutdown**, or at user login or logoff.

Computer startup and shutdown scripts are run using the local system account providing suitable access permission to install Windows Agents. Unfortunately, user login and logoff scripts are run by the user performing the login or logoff. This means that this script is only effective if it is run as if by an Administrator user. **As a result, we strongly recommend using computer startup or shutdown script GPOs.** For more information, Microsoft provides documentation about adding a computer Startup/Shutdown script in the following TechNet article:

http://technet.microsoft.com/en-us/library/cc779329%28WS.10%29.aspx

Step 5C – Use GPO Script

- 1. Save the installNableAgent.bat script file in a network shared drive that will be accessible for group policy implementation.
- 2. Configure a computer startup or shutdown script Group Policy Object. For more information, refer to the link above.
- 3. Provide the following command line argument in the script: <N-central server FQDN or IP> <customerID> <installerShare>

Example: installNable.bat ashbury.n-able.com 109 localhost\share

NOTE: The <installerShare> value does not need to begin with \\ or end with a trailing \

Customer ID's can be found from your **Service Organization level**, Navigate to:

Service Organization (Orange) > Administration > Customers/Sites



The next time that the target computers shut down and restart, the GPO will direct the Windows Agent to be installed on the designated devices. To verify that the Agents have checked into N-central properly, click All Devices view in the navigation pane of the N-central UI. If the agents are checking in properly, there will be a version number displayed in the Agent Version column for the device.

N-ABLE TECHNOLOGIES	😑 🖳 ALL DEVICES	Nce
🗈 Views 🗸 🗸	Network Devices Mobile Devices SaaS Devices	
Active Issues	ADD EDIT DELETE ADD SERVICES APPLY SERVICE TEMPLATES MAINTENANCE VUPDATE MONITO FLITER V OF Enter search criteria SEARCH RESET FLITER CREATE NEW F Filter by No Filter in all Customers / Sites	RING SOFTWARE ADD NOTE ADD SCHEDULED TASK V
Attended Remote Control	Customer / Site Remote Tools Name Network Address Control	Status Device Class
Oashboards	J&J Printing Ltd. 👘 👻 🔂 🔽 se-aus-Win8_1-Wks 10.199.5.211	S Workstations - Windows 10.0.0.1696
🖳 Device - ESX Hosts	J&J Printing Ltd. 🛄 👻 🔂 ▼ se-aus-Win8-Wks 10.199.5.212	Workstations - Windows 10.0.0.1696

For a more Advanced GPO Deployment Script, please see the N-able Forums:

https://nrc.n-able.com/community/pages/forums.aspx?action=ViewPosts&fid=2&tid=5650

Jump to page 27 for the next step.

customerID

Method D – Manual Deployment: Public Link

Step 3D – Copy Public Link Address

Requirements: No Domain or common admin account across all devices. Use this method when there is no access to your devices under management. It requires **interaction with your customers.**

Procedure: Use the **Customer Specific Agent Installer** and copy the public link to send to your clients.



Step 4D – Discovery Defaults

The agents that are being deployed will automatically be added in to your N-central dashboard. If you wish to have control over devices that are being imported, navigate to:

Customer Level (Green) > Administration > Defaults > Discovery Defaults

CORK_OFFICE		
E Views		
🕲 Dashboards 🔹 🔸	NETWORK ADDRESS TYPE	?
♦ Actions >	Workstations/Laptops: I P Address FQDN	
■ Reports >		
My Links		
🛱 Configuration 🔹 👌	Available Services Assigned Services	
Administration	APC UPS - Humidity APC UPS - Temperature BES Message Status CCM Media Device CCM MGCP Gateway	
 Certificate Management Custom Device Properties Defaults Appliance Settings Backup and SNMP Defaults Backup Share 	CCM Phone S CCM Voicemail Device S Cisco Unity Express Mailbox Citrix Presentation Server Window Snip Connectivity S	Ŧ
Customized System Email	AUTO IMPORT	(?)
Data Retention Device Defaults Discovery Defaults	Import Devices: Available Device Classes Assigned Device Classes	
Network Share Notification Templates Remote Control Defaults Remote Control Log Level Service Templates User Defaults Warranty Monitoring Probes PSA Integration	Scanner/Camera Servers - ESXi Servers - Generic Servers - Management Interface Storage Suse Linux Switch/Router Voip Phone Workstations - Generic Z - Pro node	
 Keport Manager Service Management 	Install Agent: Available Device Classes Assigned Device Classes	
SMS Registration User Management	Servers - Generic Laptop - Windows Workstations - Generic Servers - Windows Workstations - OS X Workstations - Windows	

Step 5D – Import Devices

If changes have been made to the discovery defaults, devices will have to be imported. Navigate to:

Customer Level (Green) > Actions > Add/Import Devices

INTERNATIONAL DATA W/	Ē	ADD DEVICES	Ncentral	•	•	?	SYSTEM TIME 3:13 PM
♦ Actions							
Add/Import Devices		IMPORT DEVICES (RECOMMENDED)					
 Approve/Decline Patches Domain User Management Download Agent/Probe Export Last Recovery Point 		Import the devices on the network that have been loc have been imported into N-central, agents can be aut if you are going to be monitoring large numbers of de	ated by a Discovery Job or that have been self-registered. Or omatically distributed to Windows devices. This is the recom vices or network devices in addition to servers and/or works	ice the d mended tations.	evices approac	:h	
탄 File Transfer Q Push Third Party Software 행 Run a Backup		ADD A DISCOVERY JOB IMPORT 165 OF 175 DEVICES					

SYSTEM TIMI 3:23 PM

Step 6 – Setup Recurring Discoveries for New Assets

Recurring discoveries can be setup to scan the network on a regular basis to find all new devices and selectively import them as required. A discovery is going to be setup identical to Step 4A - Initial Discovery and Import in a Domain, but without any devices auto-imported. Navigate to:

- NCENTRAL PERSONAL DEVICES ADD DISCOVERY JOB ? 🕹 🛛 🗈 II Views > Name Recurring Discover Description Actions Add/Import Devices Advanced Setting Devices to Discove SNMP Settings Virtualization Set X Approve/Decline Patches Туре 🐁 Domain User Management Import Devices: Available Device Classes Assigned Device Classes Download Agent/Prob Start Time: Laptop - Windows 12:00 Export Last Recovery Point Mobile Device) Every day of the week 💿 Selected days of the week Other Printer 📋 File Transfe Days of the Week: 0 Sun Mon Tue Wed Thu Fri Sat All Clear 🔅 Run a Backup SaaS Scanner/Camera Servers - ESXi Run a Discovery Run an Automation folic Days of the Month:
 Every day
 Selected dates Servers - Generic 🐔 Run a Script Servers - Manage > Security Manager Scan Servers - Windows Install Age Assigned Device Classes Available Device Classes Reports Laptop - Windows Servers - Generic Servers - Windows Workstations - Generic Workstations - OS X Configuration > Workstations - Windows Administration FINISH CANCEL
- Customer Level (Green) > Actions > Run a Discovery \geq

Afterwards, the recurring discovery must be checked to see if new devices are needed to be imported.

Customer Level (Green) > Actions > Add/Import Devices \geq



If you ran multiple discoveries and wish to see the import report selectively, navigate to:

Customer Level (Green) > Configuration > Discovery Jobs

INTERNATIONAL DATA W/		Y JOBS		1	CENTRAL	•	?	SYSTEM TIME 3:16 PM
🛱 Configuration 💙	ADD IMPORT ASSETS D	ELETE						
> Backup Manager	Name	Schedule	Last Report	Monitoring Applia	Network Target	Job	Status	
Discovery Jobs	Discovery Job - 2014-12-1	2 11h04m Once	2014-Dec-12 11:15	SEHYPER-V - Windows	Range: 10.19.6.1-10	Con	pleted	*
Domain User Management Filters	Discovery Job - 2014-12-1	2 11h12m Once	2014-Dec-12 11:34	SEHYPER-V - Windows	Range: 10.19.6.10-14	Con	pleted	
 Mobile Devices Monitoring Patch Management Schedule Tasks 	Recurring Discovery- Inte	rnational Recurring	2015-May-21 10:19 25 of 32 Unmanaged	SEHYPER-V - Windows	Range: 192.168.10.1-254	Pen	ding	

27

The list of devices shown are known as **unmanaged devices.** The intended goal is that the list is cleared of all devices which are not meant to be managed. Therefore there are three options:

- > Import devices that are to be managed.
 - If the device is improperly classified refer to the above troubleshooting steps from <u>Step</u> <u>5A – Importing Remaining Devices (Device Class: Other).</u>
- > Ignore devices that a recurring discovery will continually pickup, such as phones, tablets, etc
 - Ignoring a device is ignoring the MAC Address, not IP.
- > **Delete** devices that a recurring discovery will not pick up again, i.e. travelling laptops.

Check this page regularly and see if any new assets are to be added. Ensure that **Show Ignored Devices** is unchecked to only show new devices.

=	IMPORT DIS	COVERED ASSET	S	
IMPO	DRT IGNORE DELETE	SET DEVICE CLASS / OS	SET LICENSE MODE 🔻	Show Ignored Devices
	Customer Name	Y Device Name	Y Ignored	evice Class Y
~	J&J Printing Ltd.	10.199.15.1	Not Ignored	Other
•	J&J Printing Ltd.	10.199.15.114	Not Ignored	Other

Once devices are added in and have received their agents, the deployment process is finished. The progress of both discoveries and agent install can be seen from the Job Status view.

N-ABLE TECHNOLOGIES	😑 🗖 JOB STATUS				N	CENTRAL 🗳	SYSTEM TIME 6:06 PM
🗉 Views 🖌 🖌	Appliance Jobs System Jobs						
Active Issues All Devices Job Status	Filter: No Filter	Job Type:	Status:]	Status	Scheduled Time	Last Completed
Attended Remate Control Dashboards	Amazon AWS Azure BMG Corp CAC Torch	AV Defender Custom Scan AV Defender Full Scan AV Defender Quick Scan	Created Pending In Progress	wery Task wery Task	Pending	2015-May-27 20:56 2015-Jun-03 18:00	2015-May-26 22:47 2015-May-20 19:49
Device - ESX Hosts	Cork_Office Georgetown Textiles Inc Ottawa Office Georgetown Textiles Inc Texas Office	Agent Install Task Asset Discovery Task Automation Policy	Failed Expired	wery Task wery Task	Pending Completed	2015-May-30 14:38	2015-May-23 15:45 2015-May-26 09:42
Device - Network Equipment Device - Printers Device - Servers	International Data Warehouse J&J Printing Ltd. Office	File Transfer Intel® vPro™ Bulk Device Power Control	Queued Scheduled	wery Task	Pending	2015-Jun-02 09:30	2015-May-27 10:13

Every environment (including workgroups) should have an N-central Probe. They facilitate agent deployment, patch management, device discovery and act as a source for the monitoring of network devices. If you have an environment without a server, consider building a small box running Windows 7 to place into the environment to run your probe. Alternatively, designate a PC in the environment to stay on permanently and run the probe.

Step 7 – MAC OS X Agent

As with workgroup Windows based systems, the Mac agent needs to be deployed manually by following these steps. The online help refers to using the Activation Key to get things going. This is not as reliable of as using the Customer ID (otherwise known as *Access Code*). Navigate to:

Actions > Download Agent/Probe > System Software Tab > MAC OS Software

N-ABLE TECHNOLOGIES	•	😑 🔍 DOWNLOAD AGENT/PROBE		
II Views	>	Customer/Site Specific Software System Software Third Party Software		
⑦ Dashboards	>	SYSTEM SOFTWARE		(?)
♦ Actions	~	Windows Software	File Size	Version
Add/Import Devices		Windows Agent	16.94 MB	10.0.0.1696
 Add Customer/site Approve/Decline Patches Domain User Management 		Windows Probe	11.65 MB	10.0.0.1696
Download Agent/Probe				
Export Last Recovery Point File Transfer		Windows Scripts	File Size	Version
G Push Third Party Software		Group Policy Deployment Script for the Windows Agent	1.00 KB	10.0.0.1696
 Run a Discovery Run an Automation Policy Run a Script 		Linux Software	File Size	Version
 Security Manager Scan Start Automation Manager 		▶ RedHat Enterprise Linux 5.x/6.x Agent (x64)	3.63 MB	10.0.0.1696
E Reports	>	▶ RedHat Enterprise Linux 5.x/6.x Agent (x86)	3.80 MB	10.0.0.1696
🔗 My Links	>	Mac OS Software	File Size	Version
⇔ Configuration	>	Mac OS X Agent	6.18 MB	10.0.0.1696

Before the installer is run, we require the customer ID. Customer ID's can be found from your **Service Organization level**, Navigate to:

Service Organization (Orange) > Administration > Customers/Sites



Follow the steps below, the numbers correspond with the arrows in the picture below.

- 1. Run the installer package
- 2. Proceed to the Activation Step
- 3. Select Customer ID
- 4. Enter in your Customer ID
- 5. Enter in your Server URL
- 6. Select HTTPS
- 7. Click Continue



To confirm the agent is up and running:

You can run command *launchctl list | grep com.n-able.agent.macos10_4ppc*

- If agent is running it will show its PID otherwise "-"
- In following screenshot you can see that agent is running while agent log rotate service is not.



Appendix A – Probe Troubleshooting and Admin Password reset

If you encounter issues with your probe or need to change the hard coded credentials that were deployed with it, please review the following:

Ensure the **Windows Software Probe service** is installed and running. It may simply need to be restarted.

As discussed it is recommended to follow the <u>Probe Admin Account Creation</u> steps for the probe to use. If however the password does expire, or an upgrade does not complete successfully you will see the probe fail due to credential issues. You can reset the password and account the probe is using by following these steps:

- 1. Log on to the server or device that hosts your probe and navigate to Windows Services
- 2. Stop the N-central Probe services:
 - a. Windows Software Probe Maintenance service.
 - b. Windows Software Probe service.
 - c. Windows Software Probe Syslog service.
- 3. Open the **Properties** of the Windows Software Probe service by right clicking the service.
- 4. Select the **Log On** tab.
- 5. Enter the new Domain Administrator credentials.
- 6. Click **Apply**.
- 7. Select the **General** tab.
- 8. Enter the following in the **Start Parameters** field:

username=yourDomain\User Password=Yourpa\$\$word

ieneral Log On	Recovery Depe	endencies		
Service name:	Windows Softwa	re Probe Service		
Display name:	Windows Software Probe Service			
Description:	The Windows Software Probe monitors devices on the network and reports to the N-central server.			
Path to executa ''C:\Program File	ble: Is\N-able Technolog	pies\Windows Softv	vare Probe\bin\wsp	
Startup typg:	Automatic		•	
Help me configu	re service startup or	ations.		
September	Stopped			
Servi <u>S</u> tart	Stopped Stop	Bause	Besume	
Service Live Start You can specify from here.	Stopped Stop the start parameters	Bause that apply when yo	Besume	
Servi tos <u>S</u> tart You can specily from here. Start para <u>m</u> eters	Stopped Stop the start parameters : username=D	Bettee that apply when yo OMAIN user passw	Besume	

- 9. Select the Start button.
- 10. **Re-start** the other Windows Software Probe services.

- If you decide to re-install the probe, you may simply manually install the appropriate customer specific Probe directly over top of the existing one on the customer's server. The first time you launch the installer it will remove the existing probe. You will commonly need to run it a second time to install a new probe service.
- If you choose to install the probe on a different system, DO NOT DELETE THE EXISTING PROBE IN N-CENTRAL until you have performed a Task Transfer in the Administration
 > Probes section of the N-central UI to move the requirements of the one probe to the new device.

Every environment (including workgroups) should have an N-central Probe. They facilitate agent deployment, patch management, device discovery and act as a source for the monitoring of network devices. If you have an environment without a server, consider building a small box running Windows 7 to place into the environment to run your probe. Alternatively, designate a PC in the environment to stay on permanently and run the probe.

Appendix B – Troubleshooting SNMP configuration

To troubleshoot SNMP monitoring that is misconfigured or otherwise non-functional, try these steps:

- 1. Verify you have enabled SNMP on the hardware with a "GET" / "READ ONLY" community string of 'public'.
 - a. Note that some hardware has multiple places to enable this.
- 2. Verify that the devices are able to accept SNMP requests from "ALL" sources rather than specific IPs. (for troubleshooting purposes. If you want to lock it down later, you can).
- 3. Ensure you have enabled SNMP on the Properties tab of the device in N-central with the above community string populated. This is case sensitive.
- 4. Make sure the appropriate device class is chosen on the Properties tab. Server Windows or Switch/Router etc.
- 5. Re-discover the device by running a discovery with the SNMP string populated with the community string.
- 6. Re-apply the Service Templates that may include:
 - a. NETWORK for switches for Network Devices.
 - b. Network and CISCO ASA/PIX for Cisco Firewalls, SonicWall for Sonicwalls etc for Routers/Firewalls.
 - c. Dell, IBM or Intel Server hardware monitoring.

If that doesn't pull the data you need then you probably have typically not got SNMP configured on the device quite right, or the probe can't reach the device properly. If this is the case get an application such as the free MIB BROWSER from iReasoning, install it on the probe server, point it at the SNMP enabled network device by IP and choose to 'walk' the device. It should show a collection of OIDs. If it does not, SNMP is not properly configured.

It's also possible this is not a device that supports much in the way of detail when it comes to SNMP. A search in google for its "MIB" file or "OID" list will confirm that, as well will other peoples experience with monitoring it. Tier 1 devices such as Cisco or Sonicwall, Procurve switches etc. should work without issue.