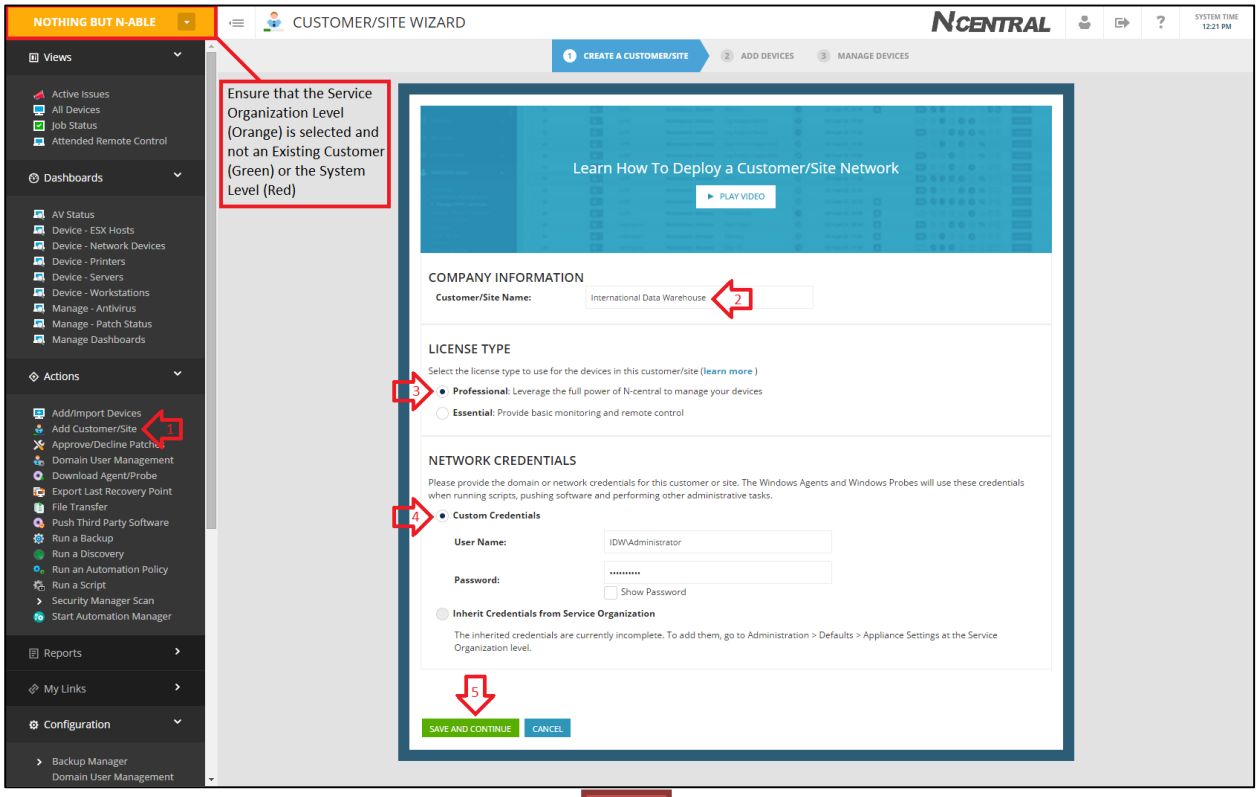
N-central Deployment Best Practices

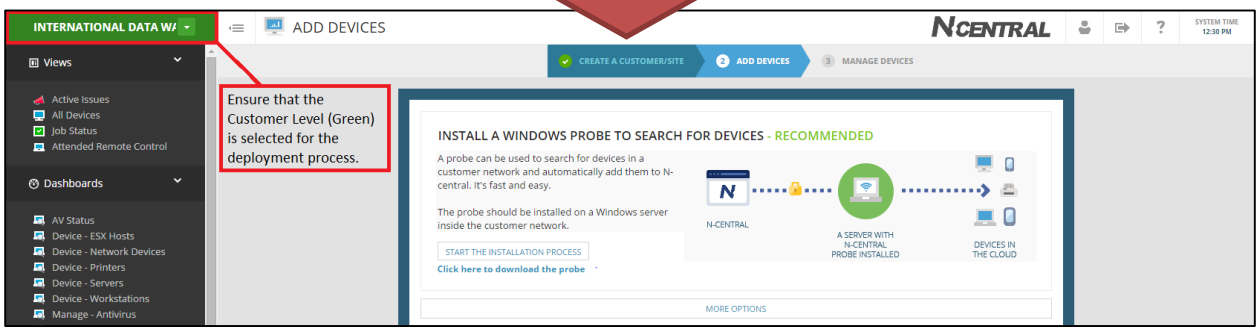
Table of Contents

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**
-
- **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 Appendix A – Probe Troubleshooting and Admin Password reset. 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 Appendix B – Troubleshooting SNMP configuration 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. I**f 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.

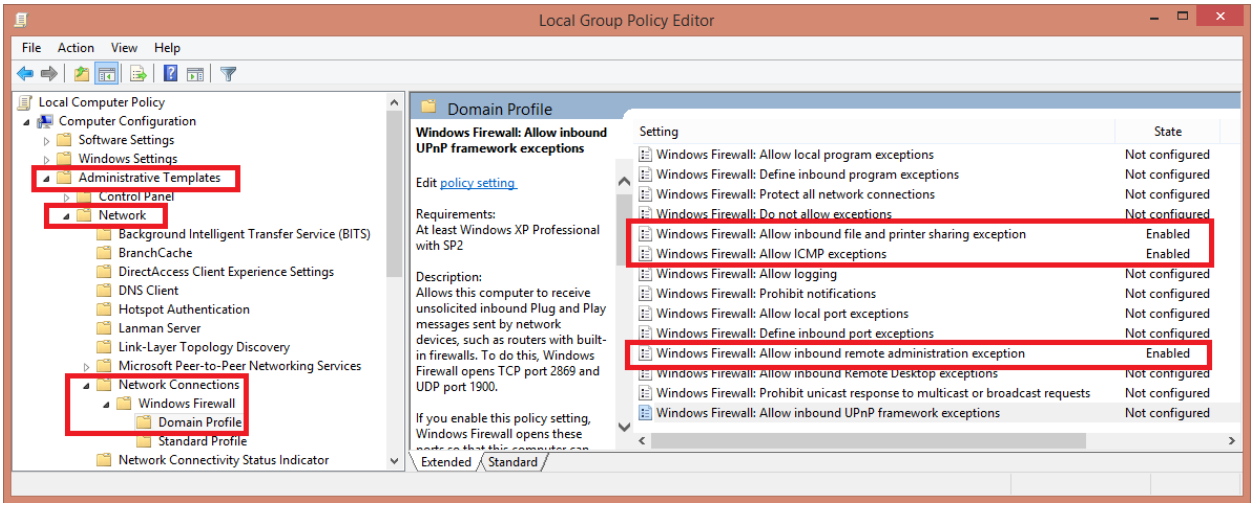
Create a New GPO Object

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

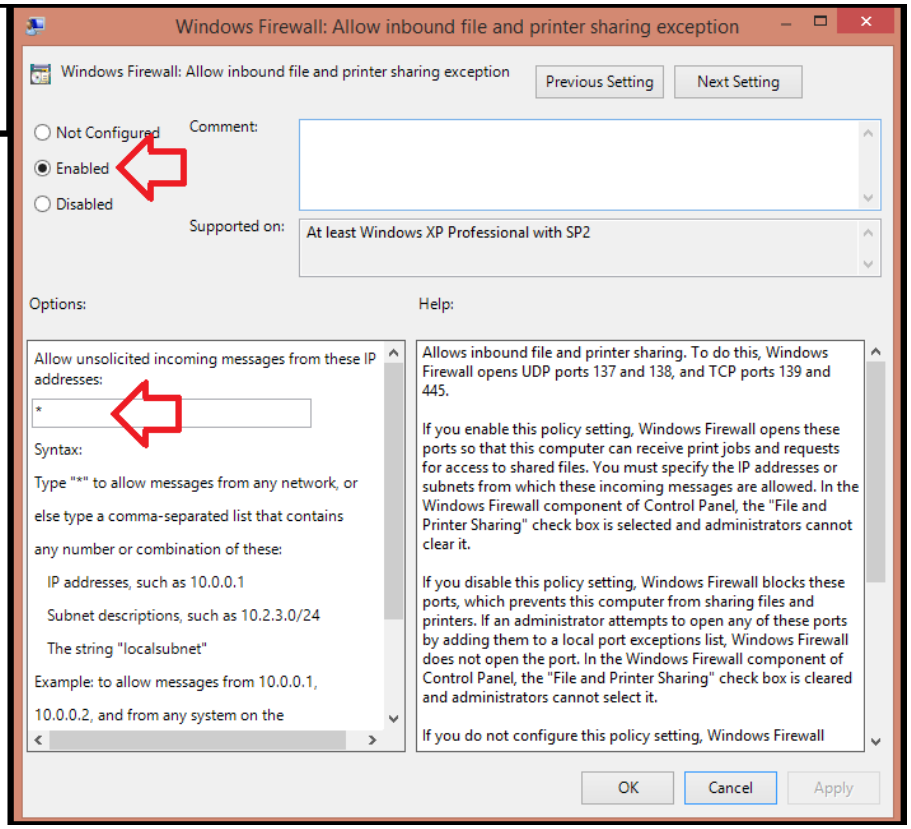
1. Allow inbound file and print sharing exception
2. Allow ICMP exceptions
3. Allow inbound remote administration exception

The numbered images below reference the three above GPO Changes.

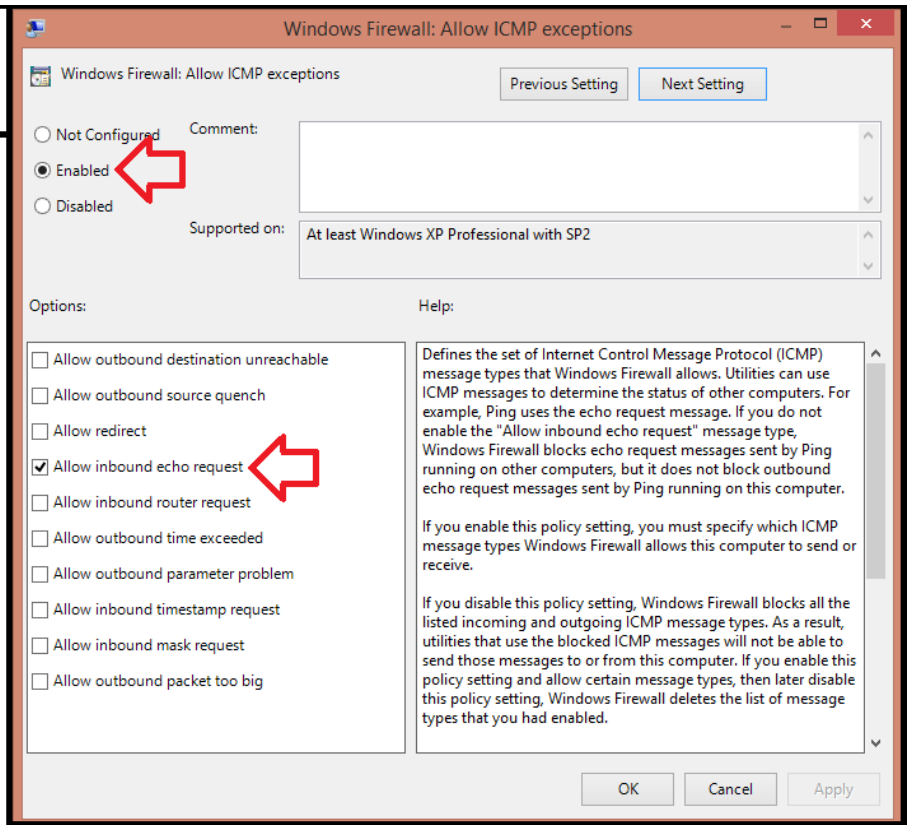
NOTE: Where referenced for an IP address in steps 1 and 3, you can either type in * to allow messages from any network, or the IP of the probe.

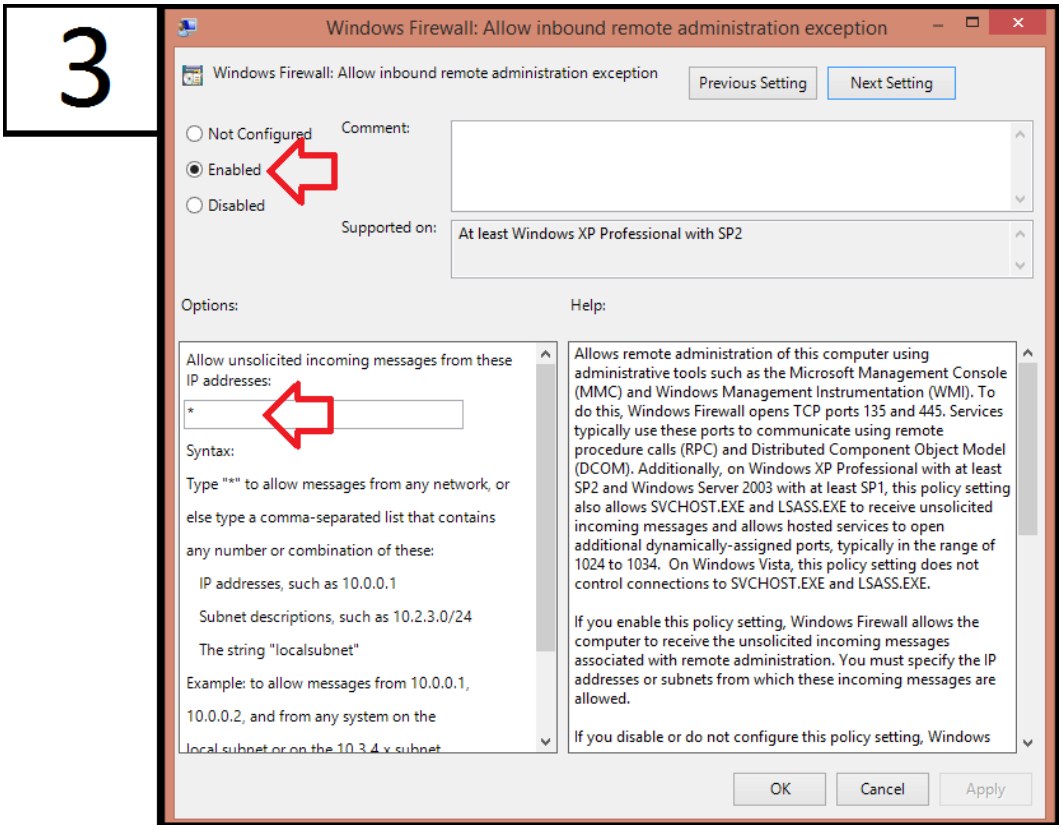


1


Windows Firewall: Allow inbound file and printer sharing exception
Windows Firewall: Allow inbound file and printer sharing exception
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows XP Professional with SP2
Options:
Help:
Allow unsolicited incoming messages from these IP addresses:
*
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
Allows inbound file and printer sharing. To do this, Windows Firewall opens UDP ports 137 and 138, and TCP ports 139 and 445.
If you enable this policy setting, Windows Firewall opens these ports so that this computer can receive print jobs and requests for access to shared files. You must specify the IP addresses or subnets from which these incoming messages are allowed. In the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is selected and administrators cannot clear it.
If you disable this policy setting, Windows Firewall blocks these ports, which prevents this computer from sharing files and printers. If an administrator attempts to open any of these ports by adding them to a local port exceptions list, Windows Firewall does not open the port. In the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is cleared and administrators cannot select it.
If you do not configure this policy setting, Windows Firewall
OK
Cancel
Apply

2


Windows Firewall: Allow ICMP exceptions
Windows Firewall: Allow ICMP exceptions
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows XP Professional with SP2
Options:
Help:
Allow outbound destination unreachable
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
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 messages will not be able to send those messages to or from this computer. If you enable this policy setting and allow certain message types, then later disable this policy setting, Windows Firewall deletes the list of message types that you had enabled.
OK
Cancel
Apply



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

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

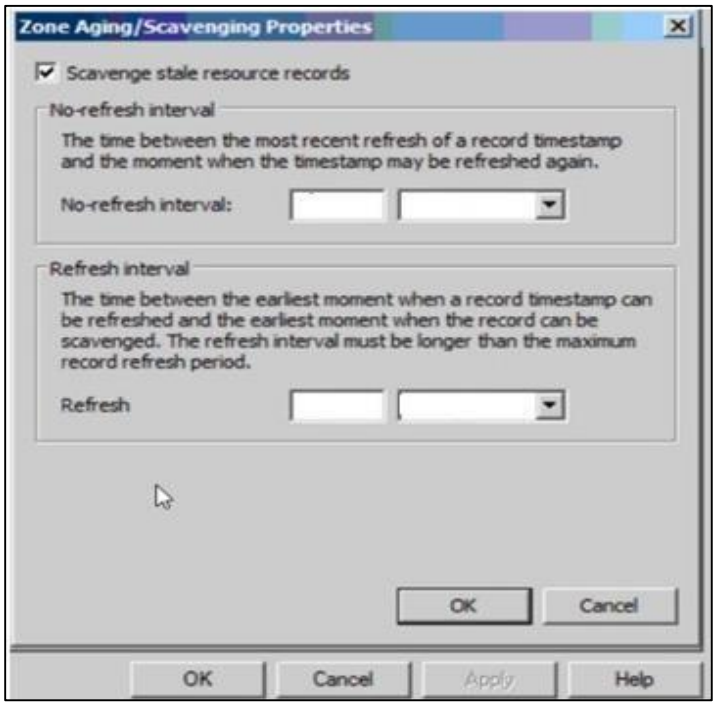
ESX(i) Host Preparation

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.



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

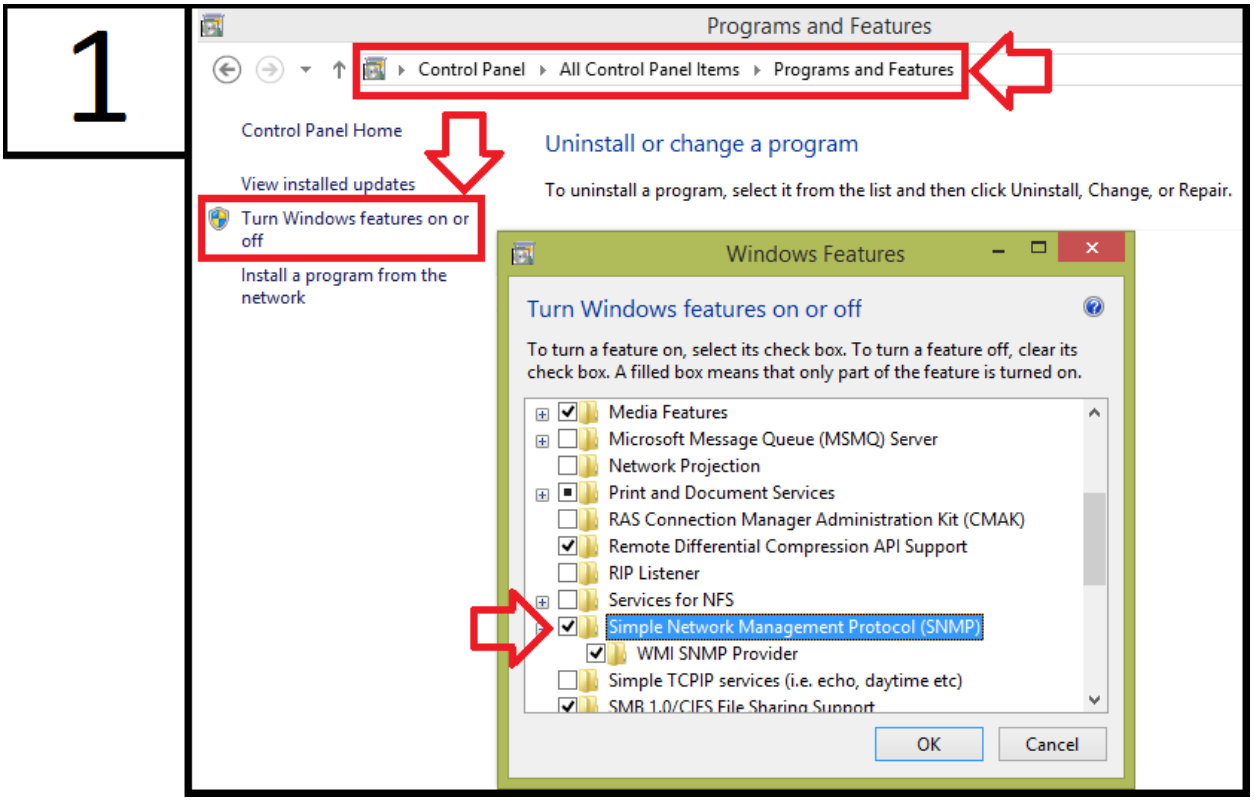
- **Dell OpenManage**
- **HP Systems Insight Manager Agent**
- **IBM ServeRAID** (for RAID-level monitoring) and the **IBM Director Platform agent** (for hardware-level monitoring)
- **Intel System Management Software**

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

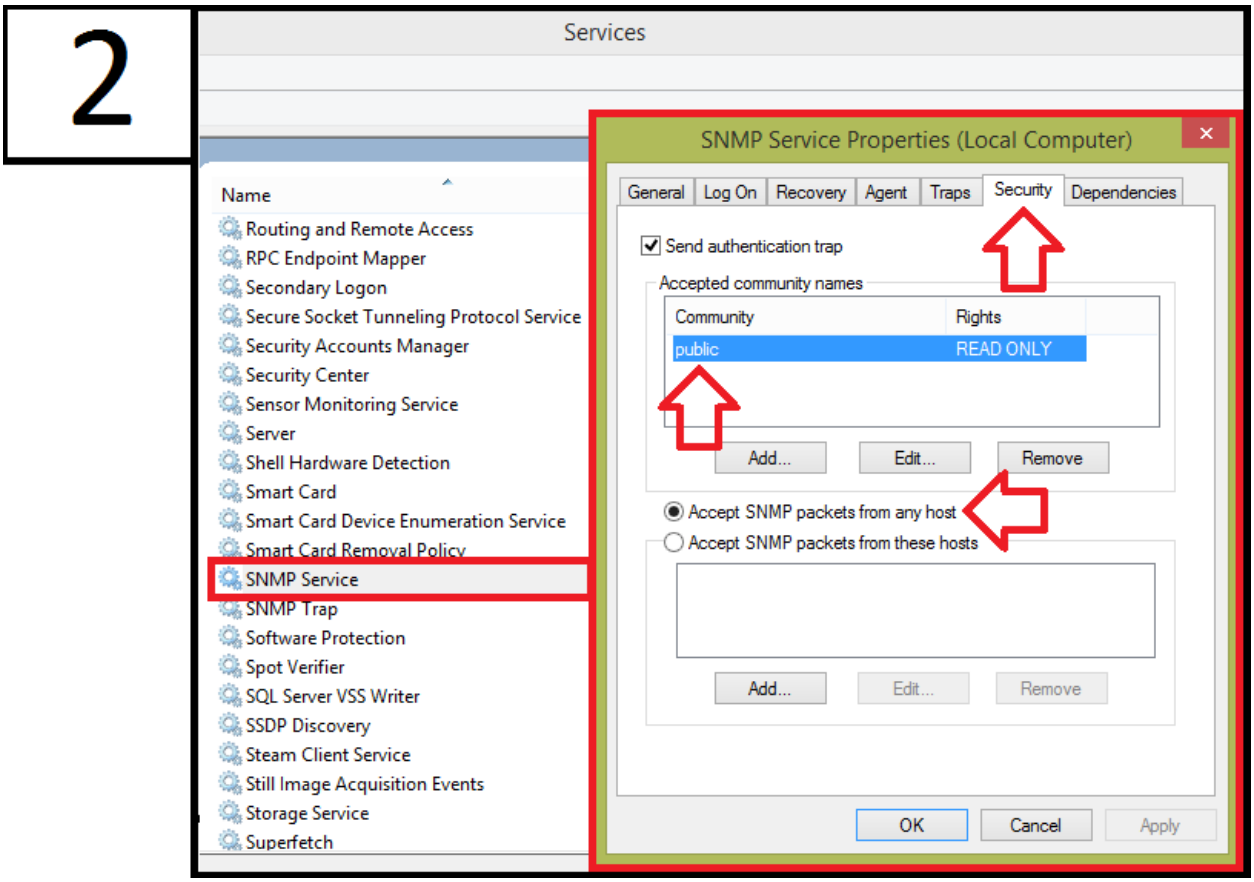
1. **Add or Remove Programs – Add/Remove Windows Components** – Select Simple Network Management Protocol (SNMP).

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.



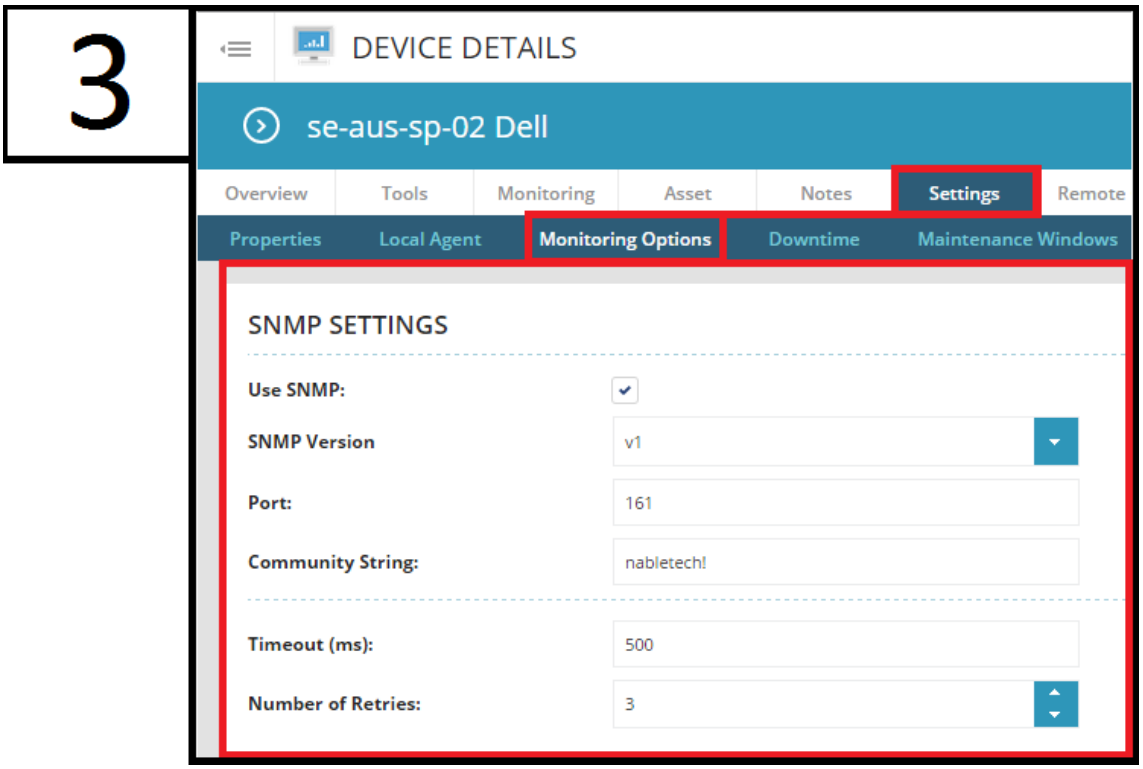
Optional Step: Discover the Server Using a Windows Probe

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 Step 4A – Initial Discovery and Import in a Domain**.** **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.**

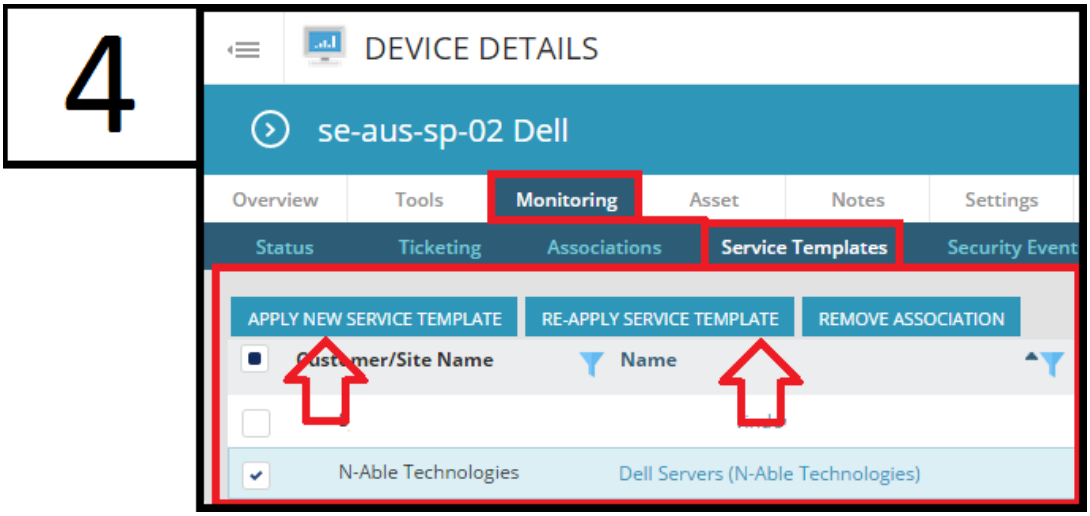
Step 3: Apply Service Templates

Once the device has been discovered in N-central,

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

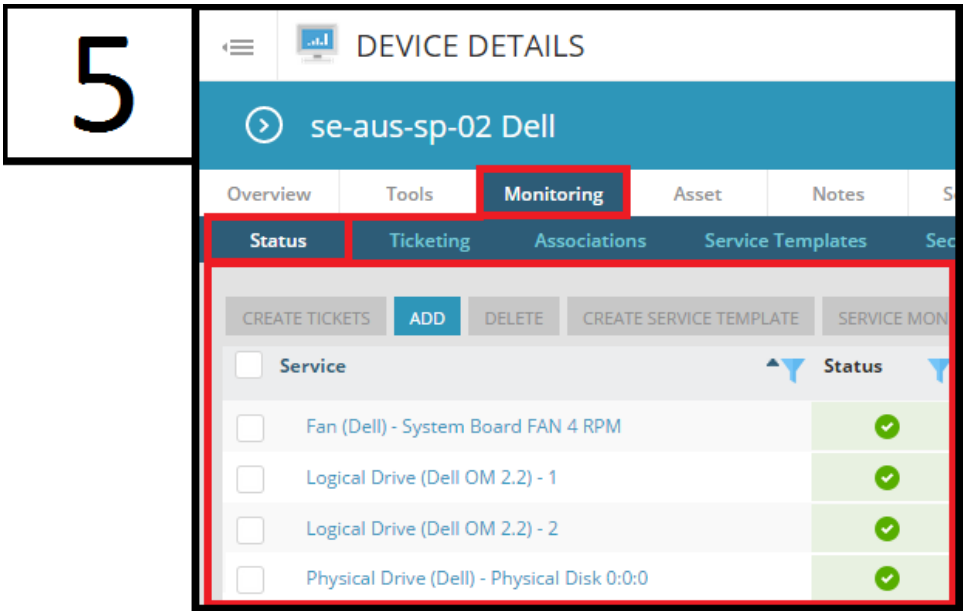


2. Re-Apply the template if it is already there, or Apply New Service Templates



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.

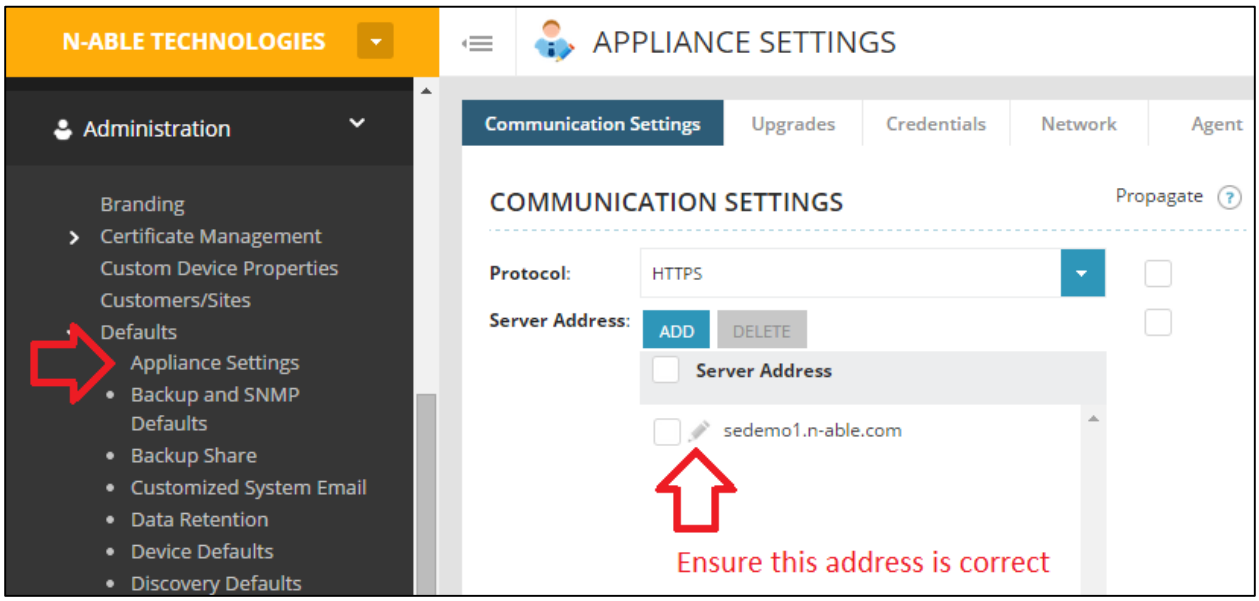
3. Click on the Status tab to verify the services that were added to the device.



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



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

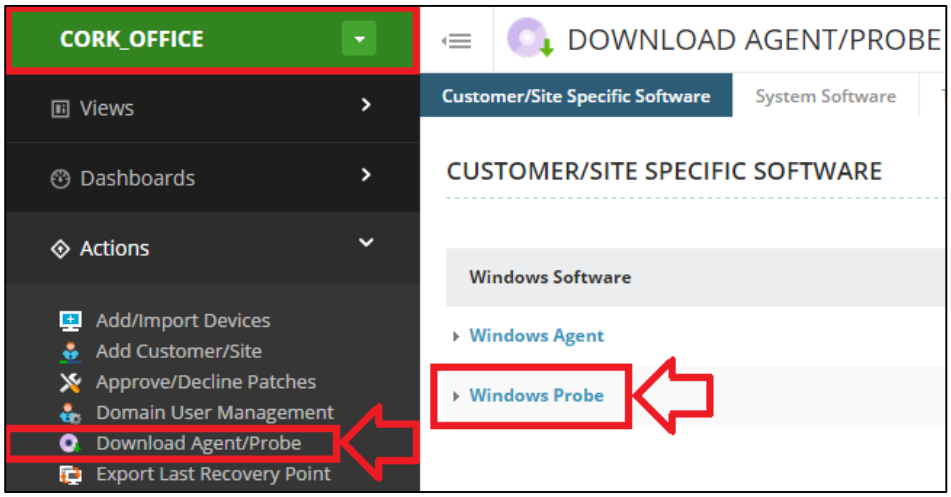
Method A – Automated Deployment: N-able Probe

Step 3A – Download a Probe

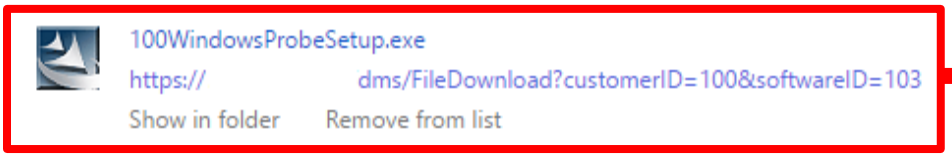
Requirements: **Administrator account**; either a common Local Admin or Domain Admin on all devices.

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



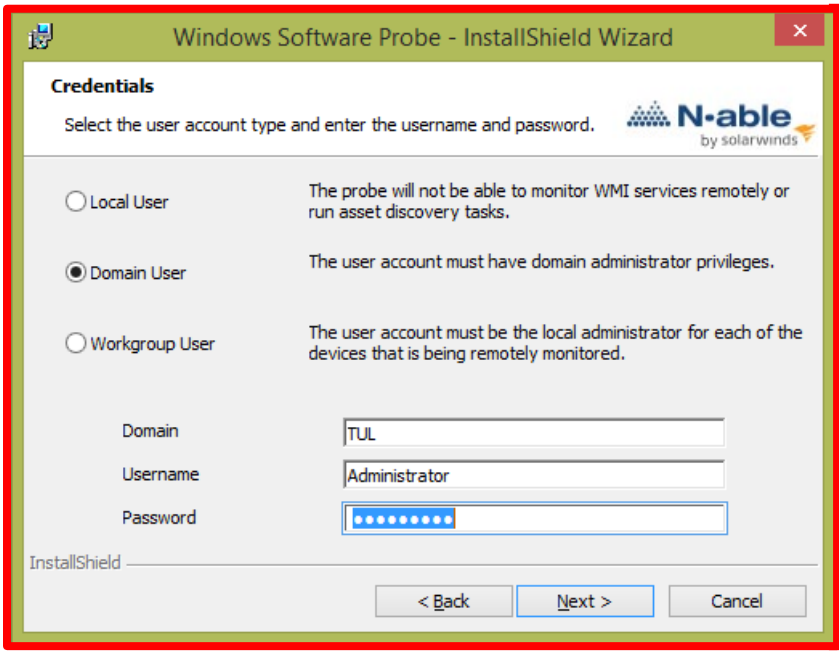
NOTE: The probe download link is public! Save time by right clicking - copying the URL and paste it into a web browser on the remote server.



NOTE: VERY IMPORTANT: The number before the installer ensures it is tied to the customer.

During the Install Process:

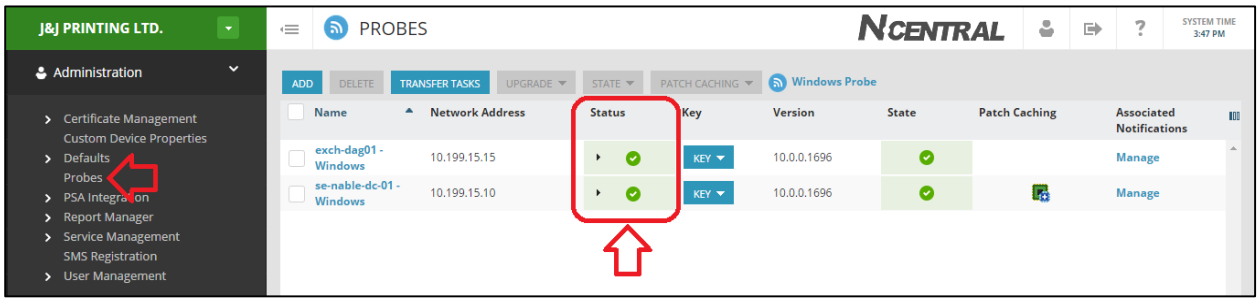
- Do not configure a **proxy** unless required
- Do not enable the **AMT data store**
- Provide the previously created Probe Admin Account Creation credentials when requested.
  - *The domain field should not typically contain ".com", ".local" etc. You should only need to provide the domain name* (ie: **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.



NOTE: The install requires a set of credentials used for deployment of agents. In a Domain Environment this must be a Domain Administrator. In a Workgroup Environment, **there must a common administrator account across all machines** in order to deploy the N-central agent. In absence of this account, the probe will be unable to deploy agents.

Confirm the Probe is installed by navigating to:

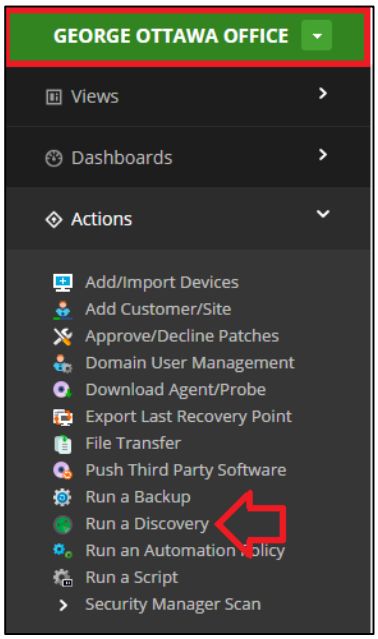
- Administration > Probes



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

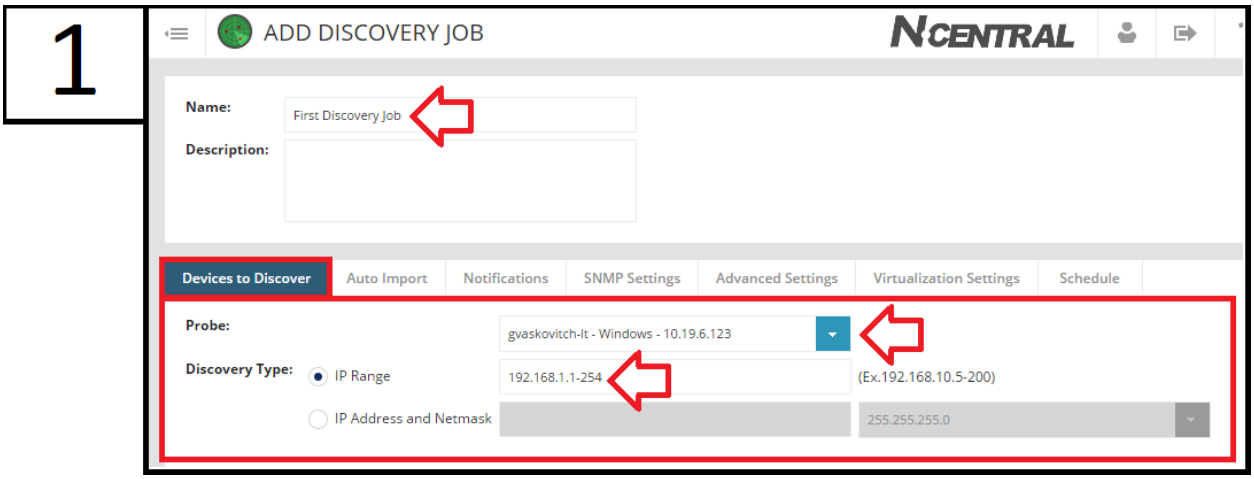


Any discoveries done from the probe are set to recur every day at time of install with default auto-import settings. Therefore it is highly recommended to split the discoveries into two parts:

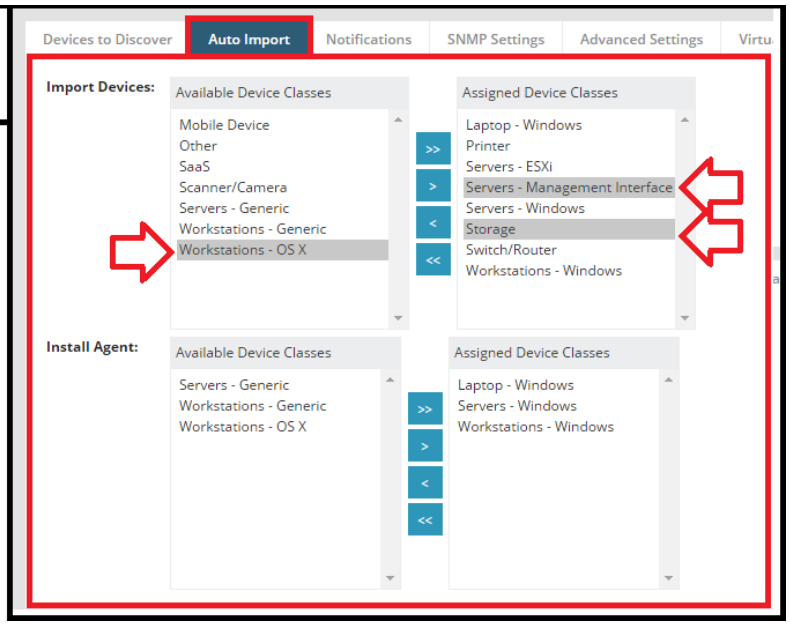
1. Step 4A – Initial Discovery and Import in a Domain
   - *Step 5A – Importing Remaining Devices (Device Class: Other)*
2. Step 6 – Setup Recurring Discoveries for New Assets

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.**

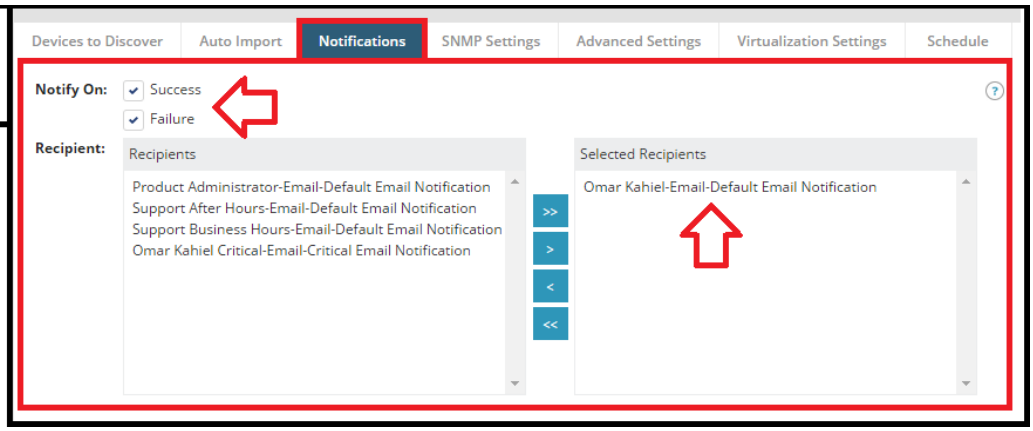


2

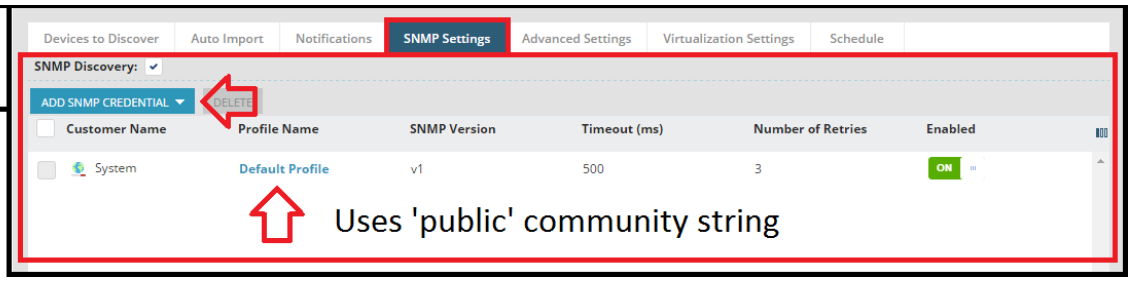


NOTE: Regardless of the IP's scanned. The only imported devices will be those that are discovered and **classified** correctly. Refer to Phase 2 – Readying the environment in a domain for pre-deployment steps to have devices be discovered correctly.

3



4

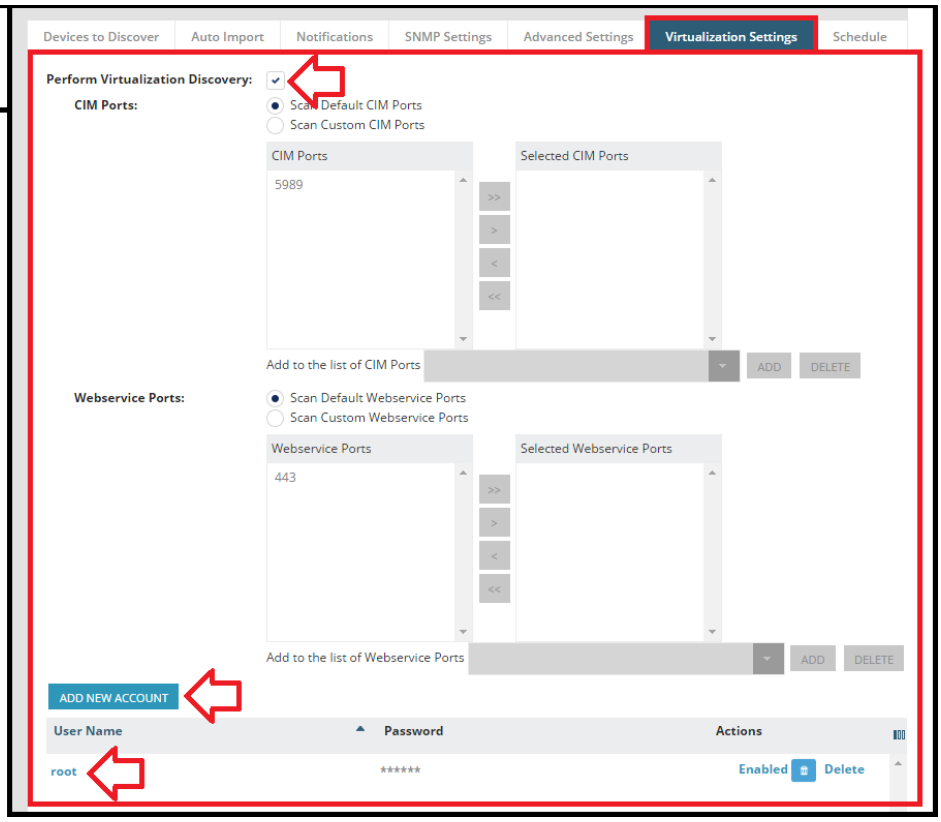


NOTE: Defaults are configured from Administration > Defaults > Backup and SNMP Defaults

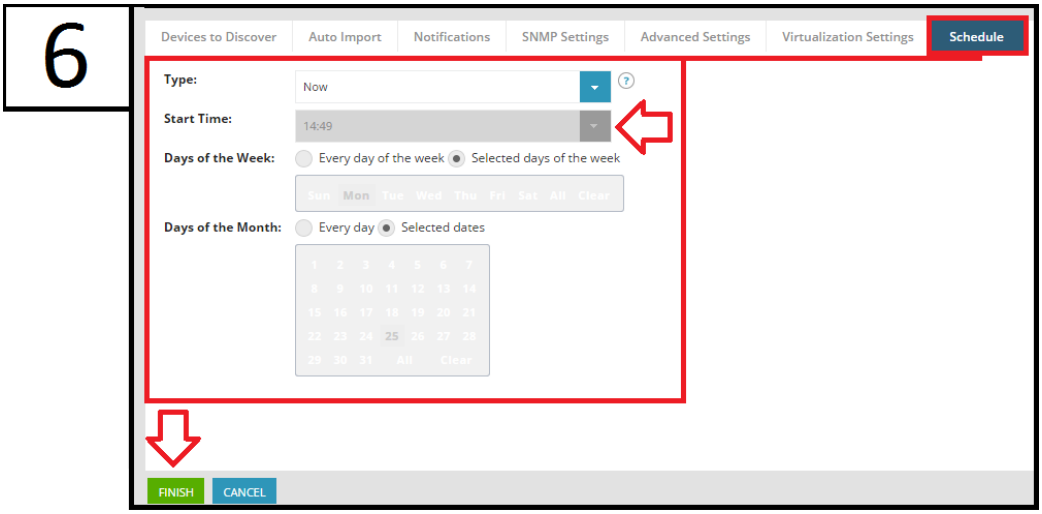
Add in extra SNMP queries if they use a community string other than public

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.

5



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.



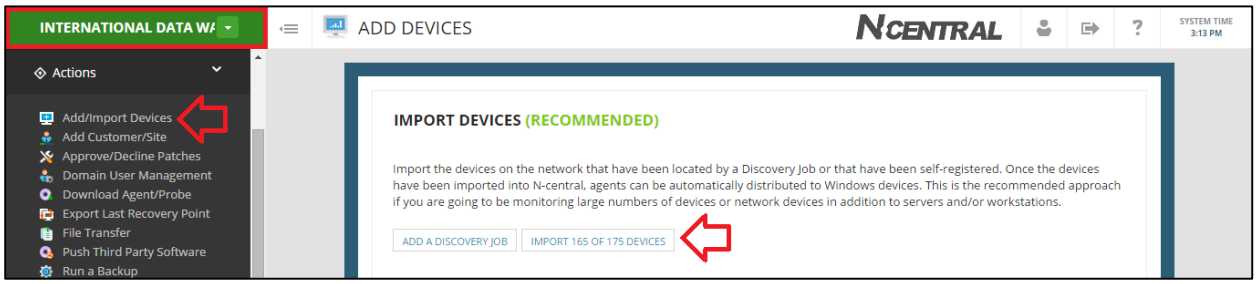
As this discovery is intended for the first import of devices, its schedule is set to Now. If the time does not satisfy you, you can't technically setup a discovery at a later time. However a recurring discovery set **at both** a specific day of the week and month would only occur on that specific day. 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)*

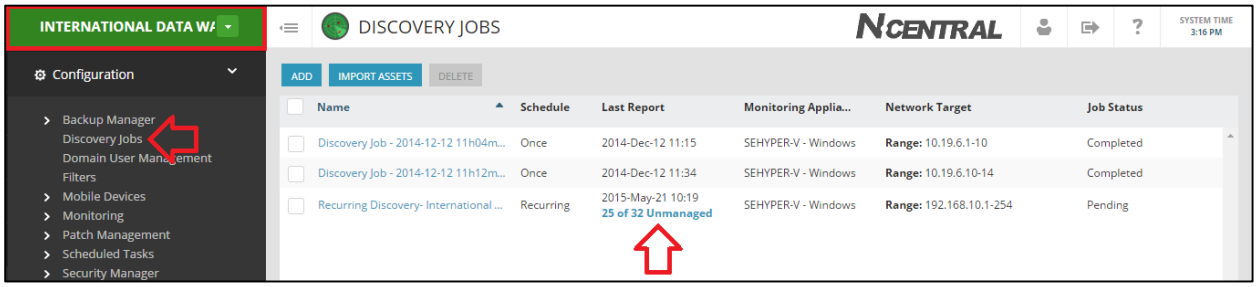
Anything that is not properly classified will be found from the discovery job. Navigate to:

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

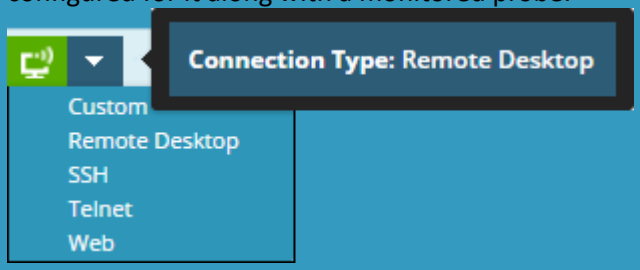
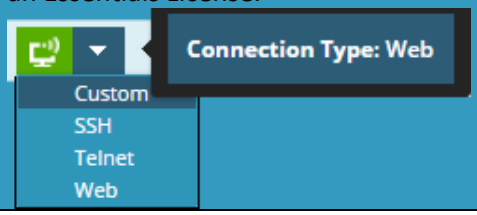


If you ran multiple discoveries and wish to see the import report selectively, navigate to:

- Customer Level (Green) > Configuration > Discovery Jobs



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**Group Policy Changes to Windows Firewall**
The device is not part of the Domain (WMI permissions not allowing probe to pull OS type and therefore device could not be classified.	Ensure proper credentials are used that can access the \Admin$ share of a device: **Probe Admin Account Creation**
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. 
Non-Windows devices (Switch/Router/Printer/Linux OS/MAC OSX/etc.)	
Reason	**Solution**
SNMP is not enabled on the device	Ensure SNMP is enabled with read only access to the probe: **Network Equipment Changes to** 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 Method D – Manual Deployment: Public Link). Jump to page 27 for the next step.

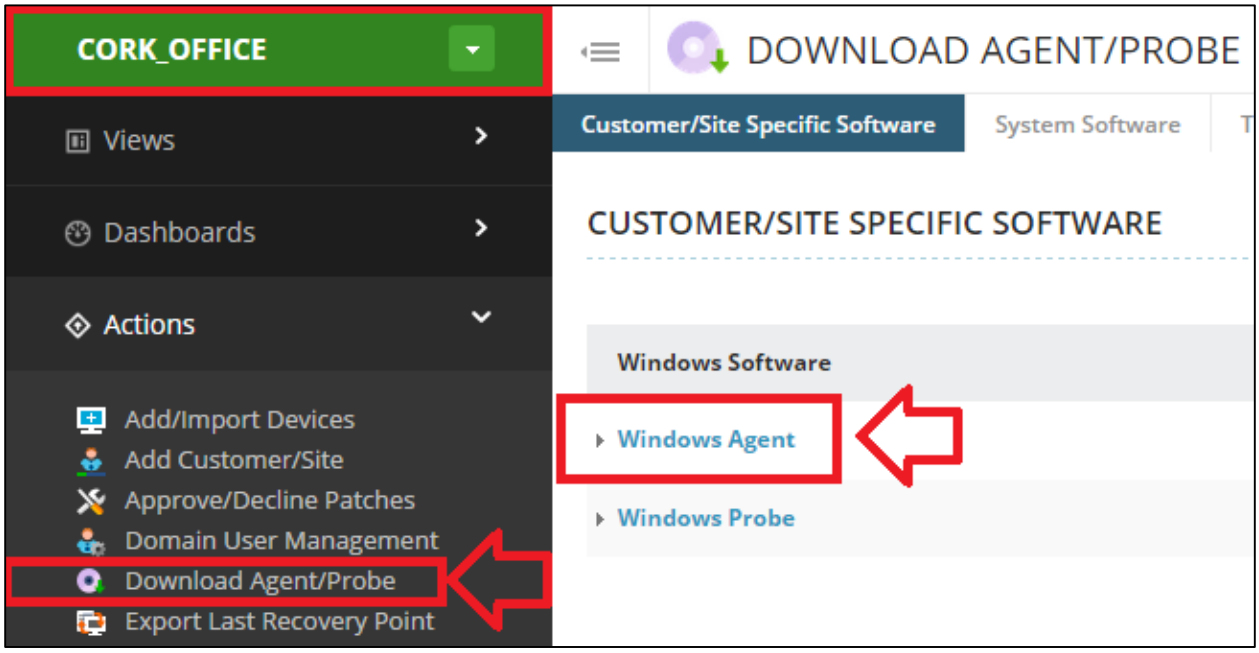
Method B – Automated Deployment: Previous RMM Tools

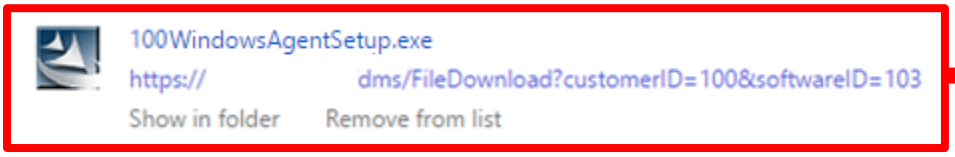
Step 3B – Customer Specific Agent EXE

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

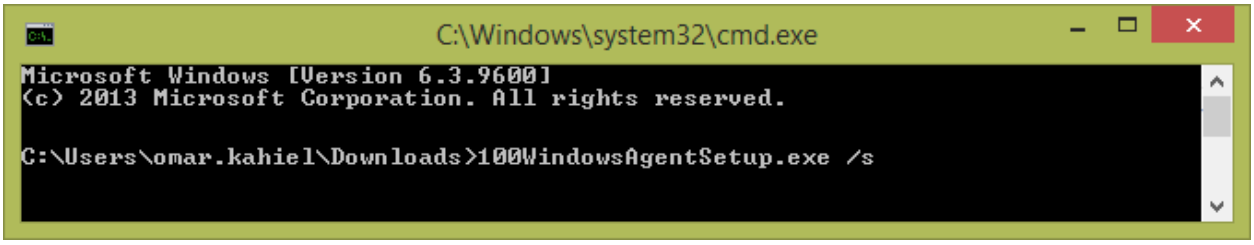




NOTE: VERY IMPORTANT: The number before the installer ensures it is tied to the customer.

- **Use the command line parameter: /s**
  - **Example:**

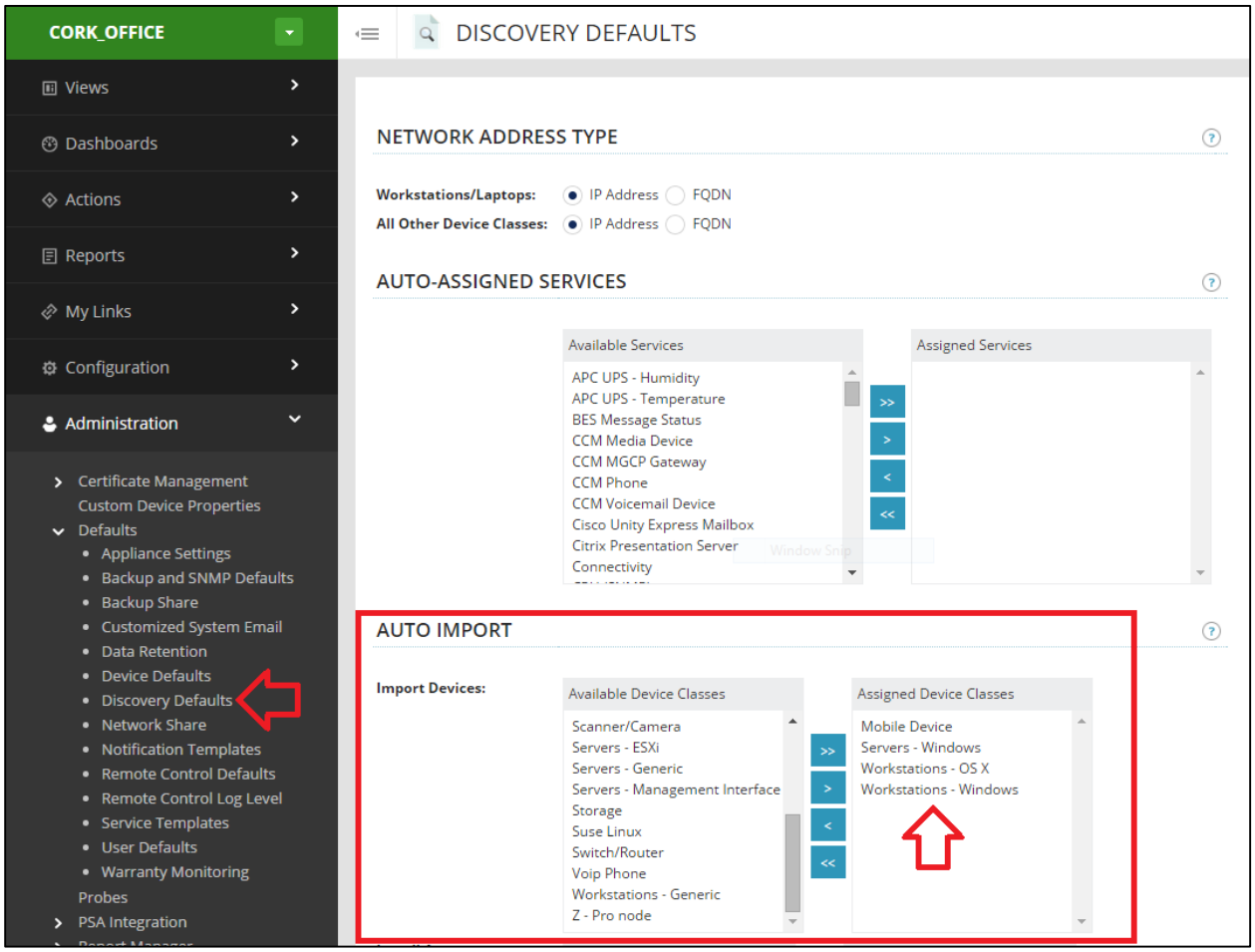
C:\Users\omar.kahiel\Downloads>100WindowsAgentSetup.exe /s



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:

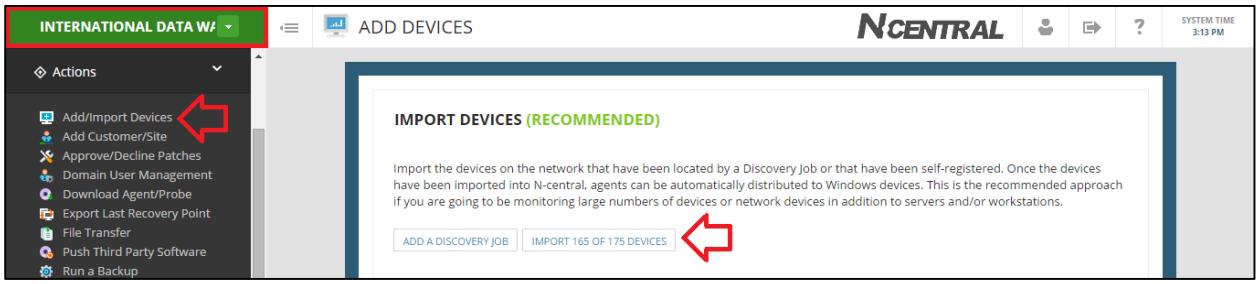
- Customer Level (Green) > Administration > Defaults > Discovery Defaults



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.

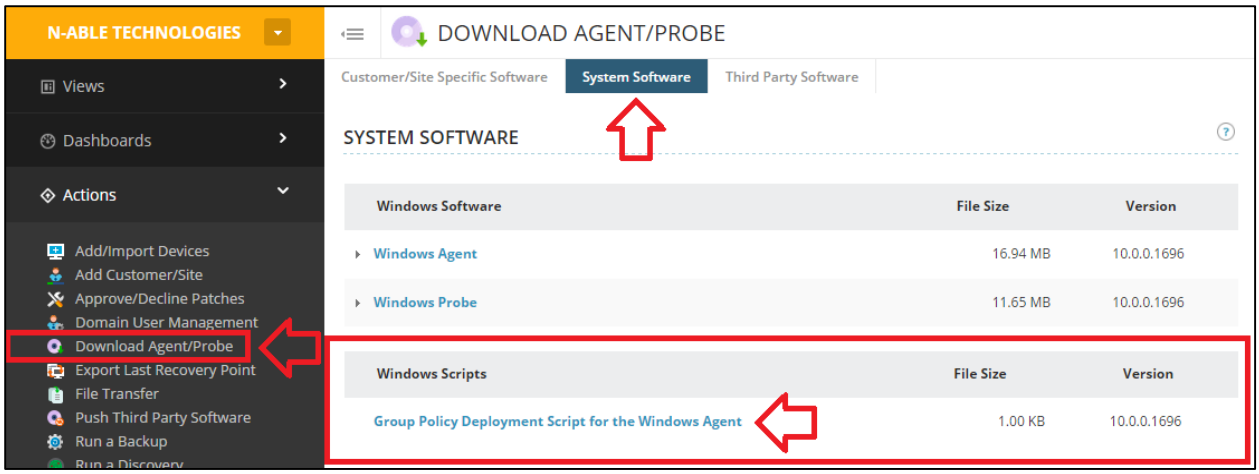
Method C – Automated Deployment: GPO Script

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



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

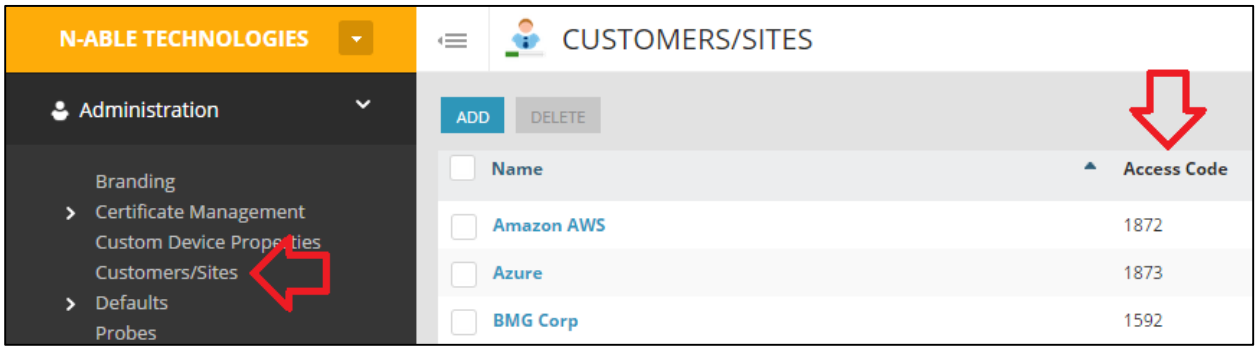
1. Save the installNableAgent.bat script file in a network shared drive that will be accessible for group policy implementation.
2. Configure a computer startup or shutdown script Group Policy Object. For more information, refer to the link above.
3. Provide the following command line argument in the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

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

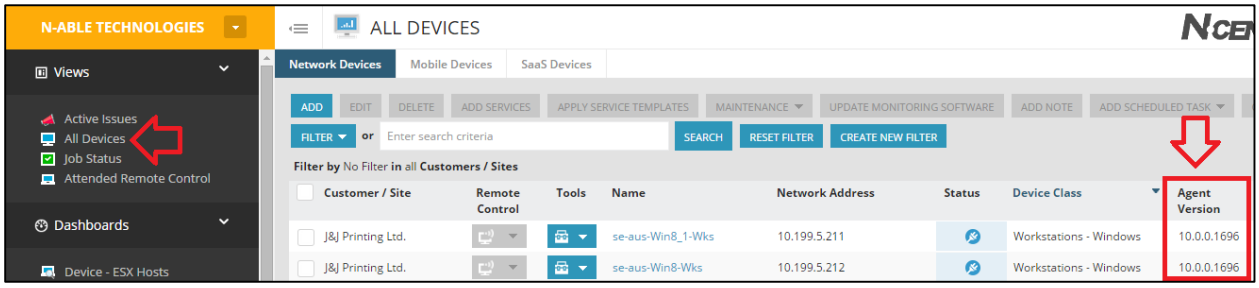
NOTE: The <installerShare> value does not need to begin with \\ or end with a trailing \

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.



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

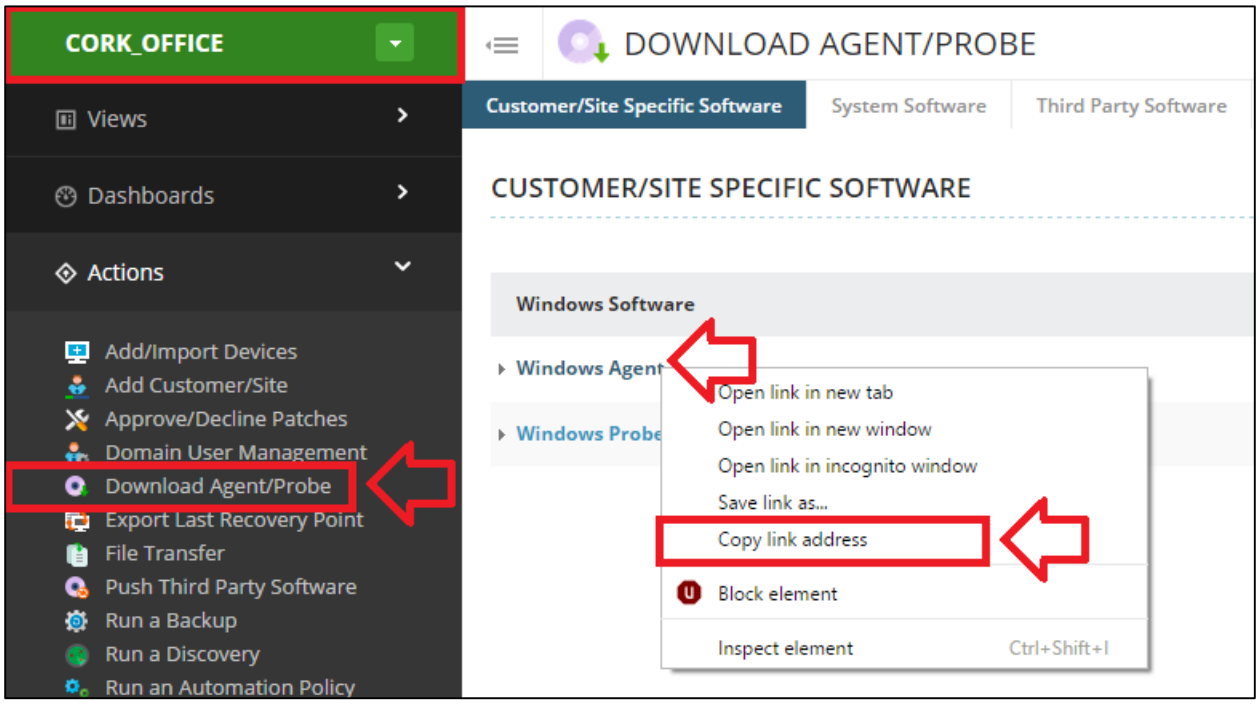
Jump to page 27 for the next step.

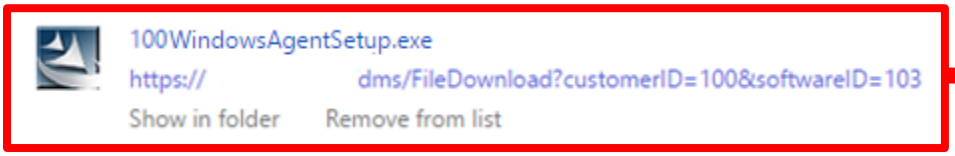
Method D – Manual Deployment: Public Link

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.



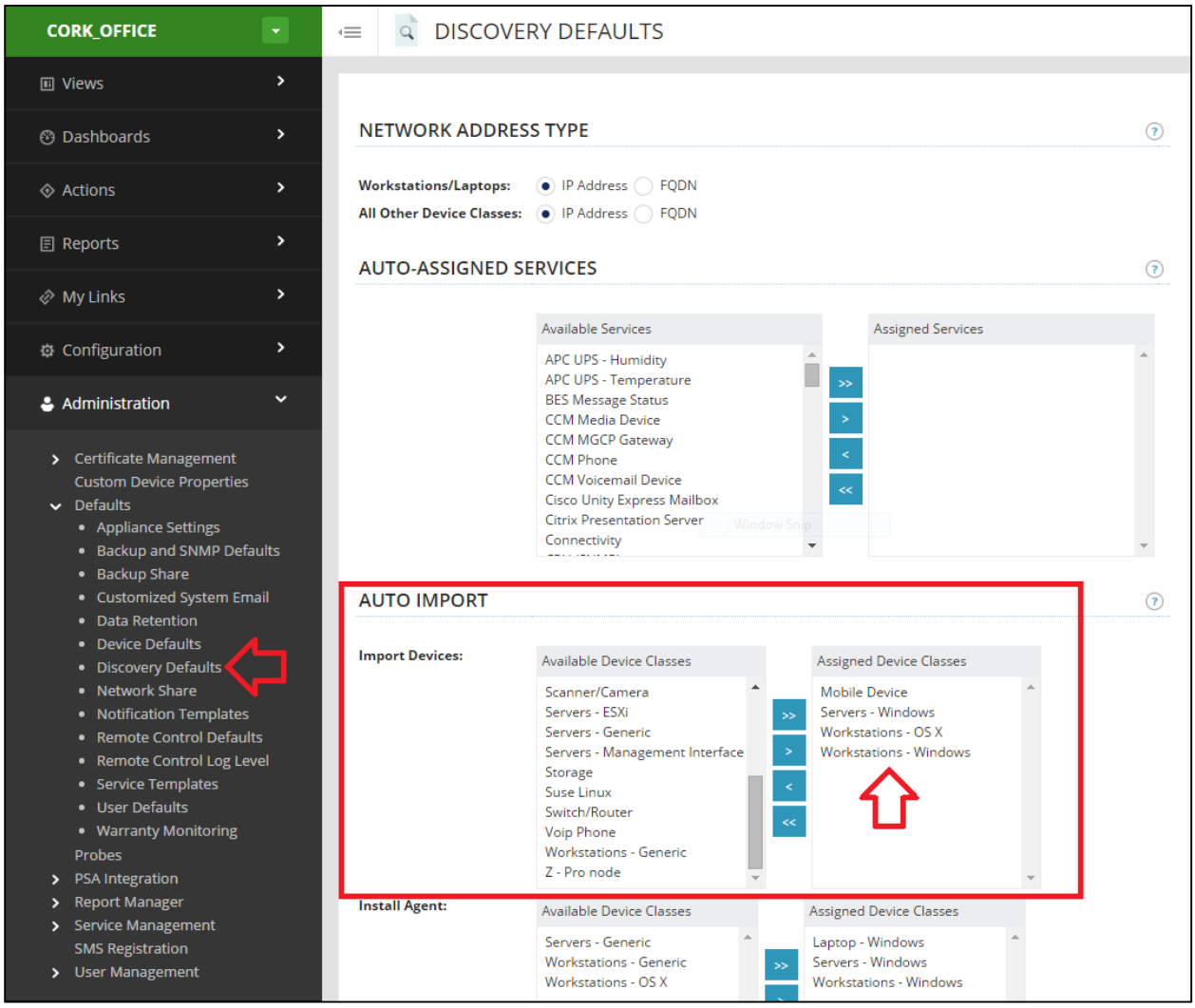


NOTE: VERY IMPORTANT: Ensure the link includes the **customerID**

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:

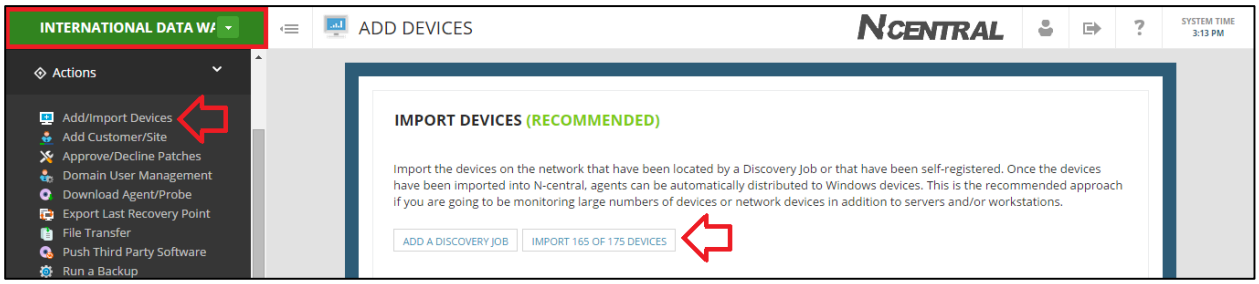
- Customer Level (Green) > Administration > Defaults > Discovery Defaults



Step 5D – Import Devices

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

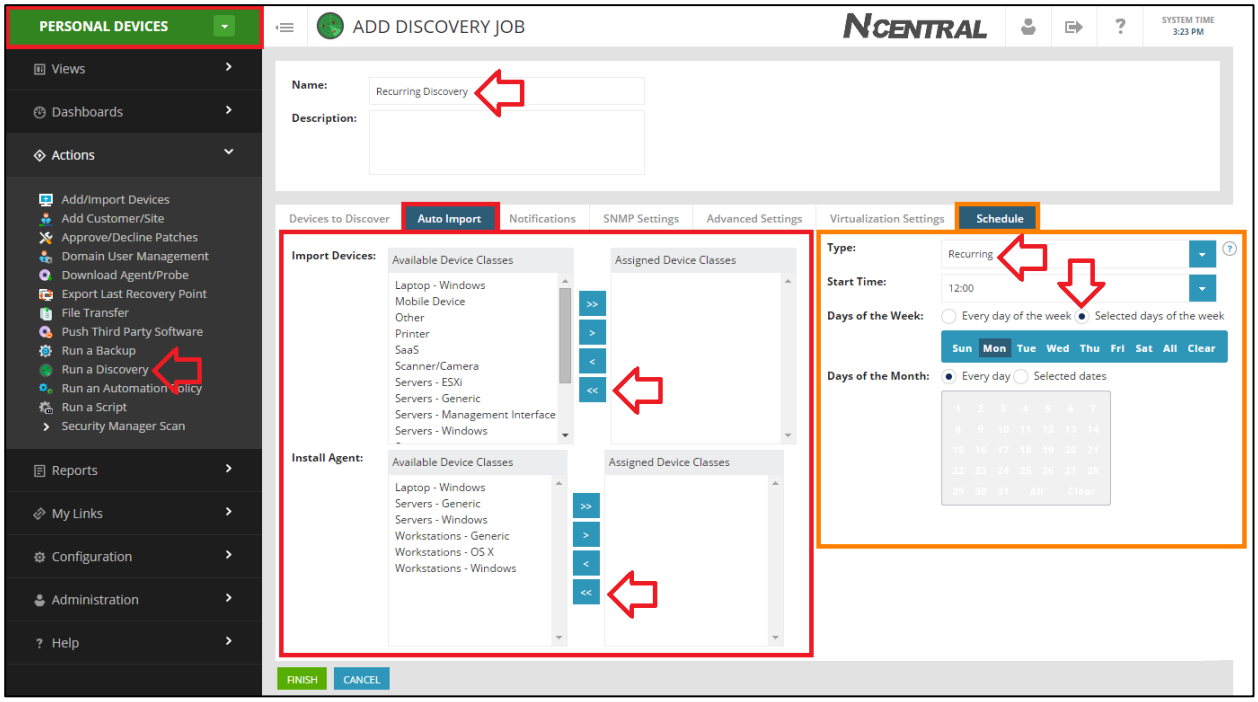
- Customer Level (Green) > Actions > Add/Import Devices



Step 6 – Setup Recurring Discoveries for New Assets

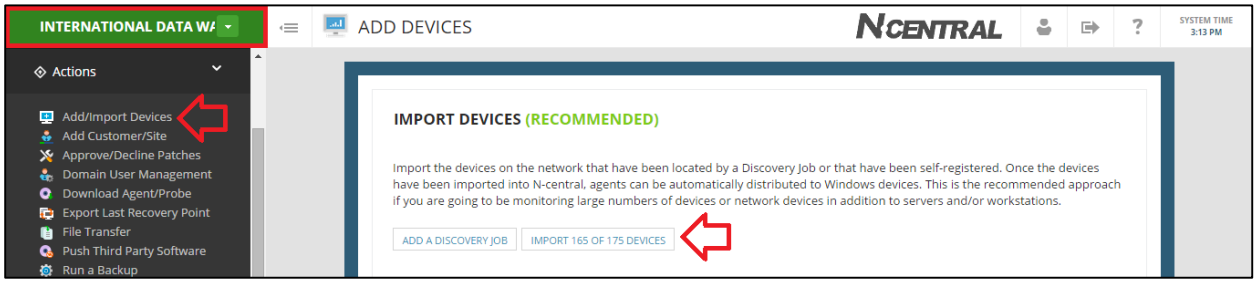
Recurring discoveries can be setup to scan the network on a regular basis to find all new devices and selectively import them as required. A discovery is going to be setup identical to Step 4A – Initial Discovery and Import in a Domain, but without any devices auto-imported. Navigate to:

- Customer Level (Green) > Actions > Run a Discovery



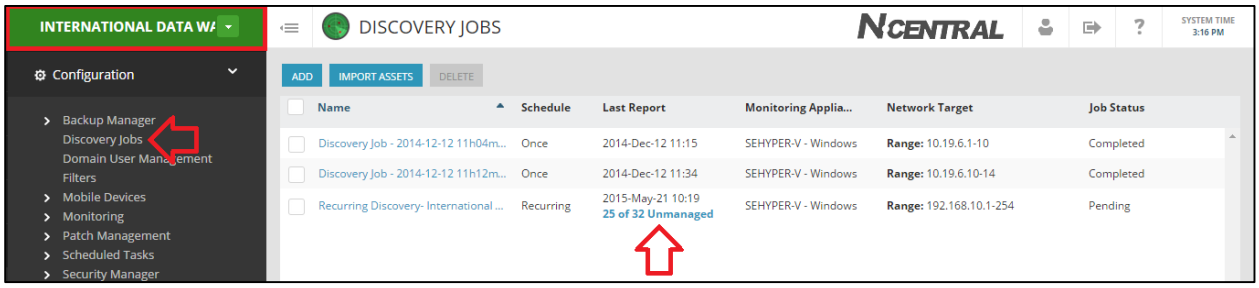
Afterwards, the recurring discovery must be checked to see if new devices are needed to be imported.

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



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

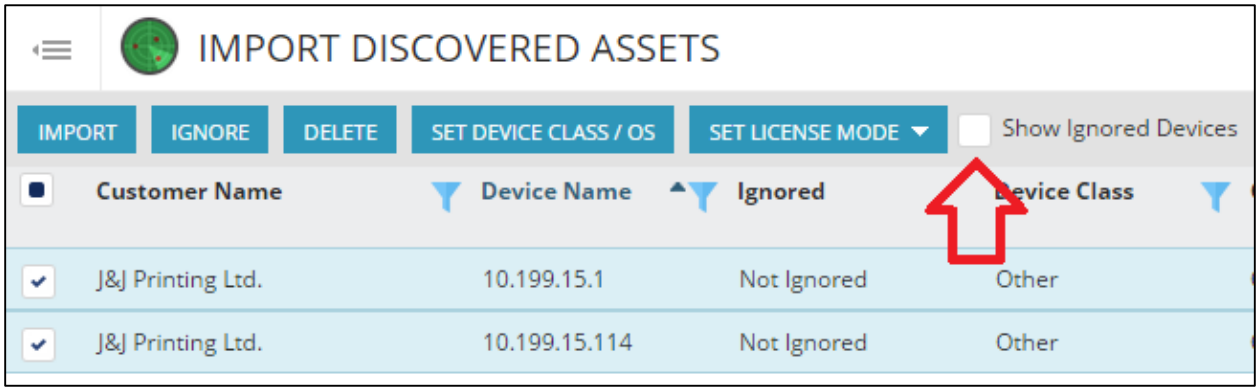
- Customer Level (Green) > Configuration > Discovery Jobs



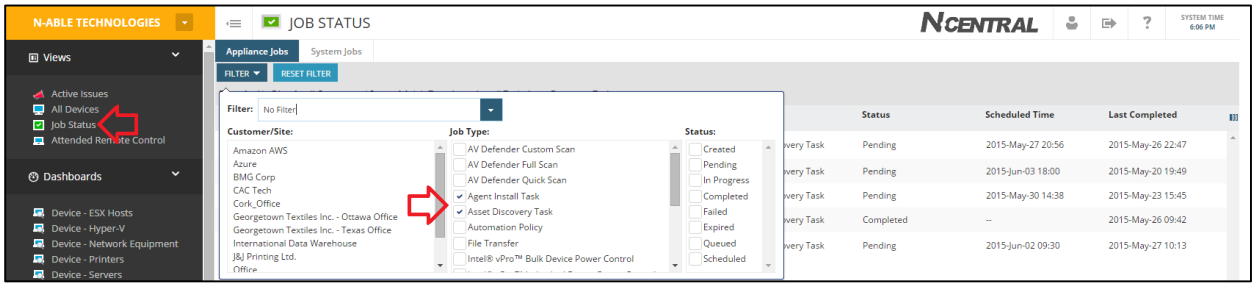
The list of devices shown are known as **unmanaged devices.** The intended goal is that the list is cleared of all devices which are not meant to be managed. Therefore there are three options:

- **Import** devices that are to be managed.
  - If the device is improperly classified refer to the above troubleshooting steps from [Step 5A – Importing Remaining Devices (Device Class: Other).]
- **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.



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.

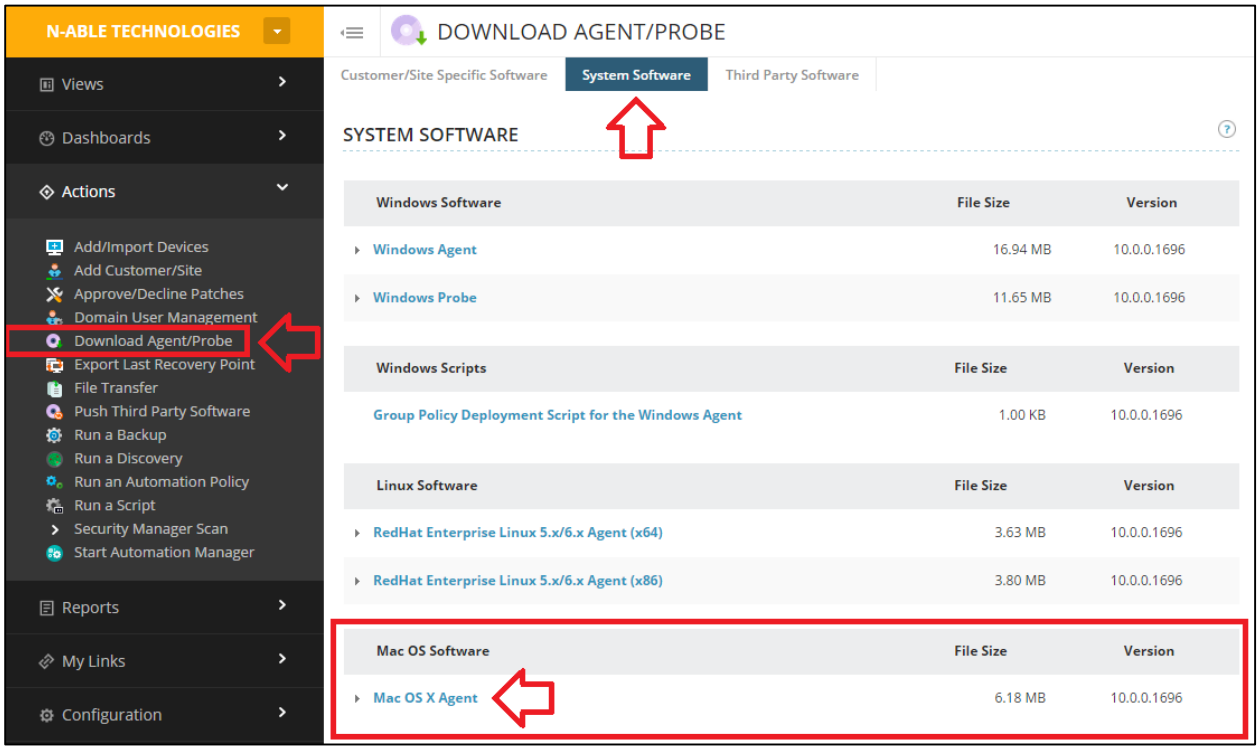


Every environment (including workgroups) should have an N-central Probe. They facilitate agent deployment, patch management, device discovery and act as a source for the monitoring of network devices. If you have an environment without a server, consider building a small box running Windows 7 to place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

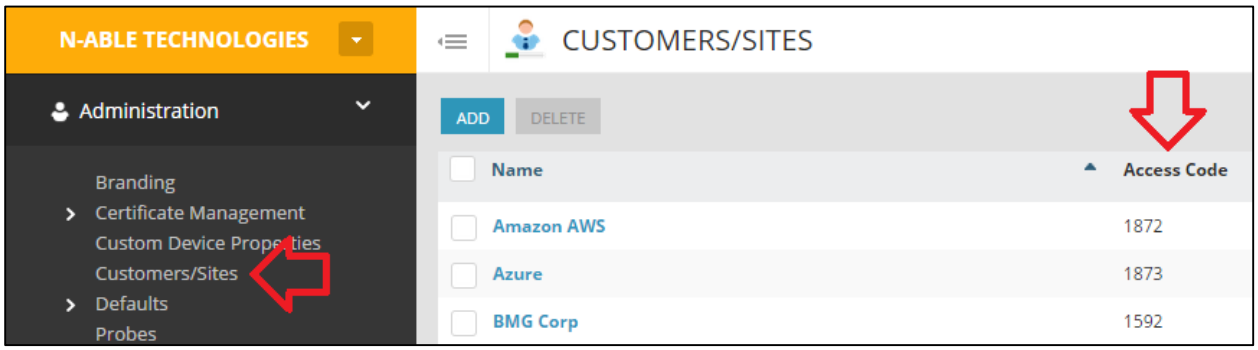
As with workgroup Windows based systems, the Mac agent needs to be deployed manually by following these steps. The online help refers to using the Activation Key to get things going. This is not as reliable of as using the Customer ID (otherwise known as *Access Code*). Navigate to:

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



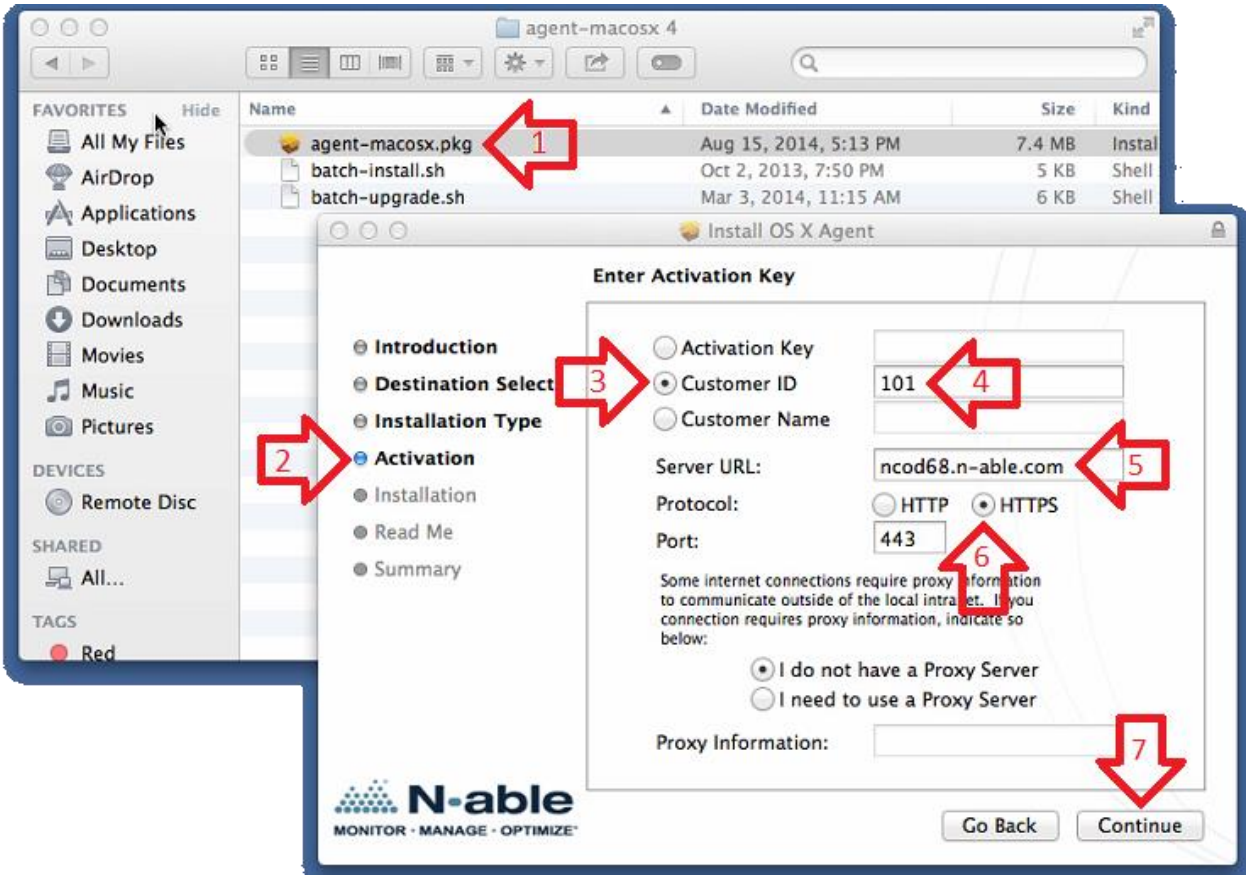
Before the installer is run, we require the customer ID. Customer ID's can be found from your **Service Organization level**, Navigate to:

- **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.

```
Sheeshpauls-Mac-mini:.ssh root# launchctl list | grep com.n-able.agent.macos10_4ppc
94699   -       com.n-able.agent-macos10_4ppc
-       0       com.n-able.agent-macos10_4ppc.logrotate-daily
Sheeshpauls-Mac-mini:.ssh root#
```

Appendix A – Probe Troubleshooting and Admin Password reset

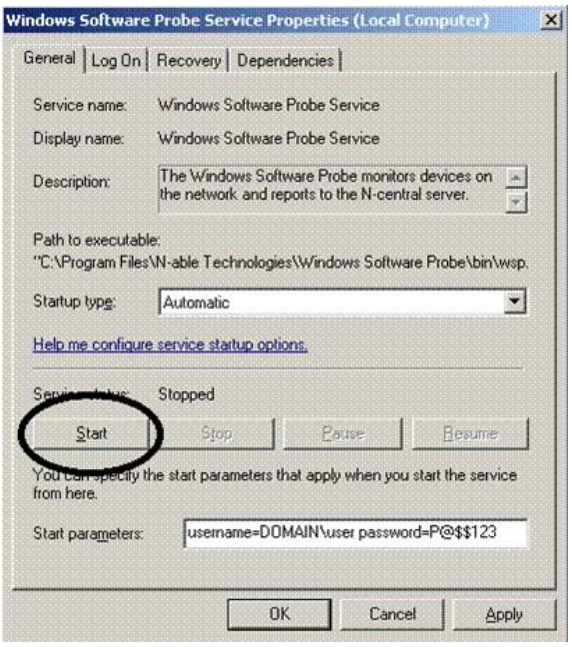
If you encounter issues with your probe or need to change the hard coded credentials that were deployed with it, please review the following:

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 Probe Admin Account Creation 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



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.