

Router Changes - Port Forwarding

Open ports 22, 443, and 10000 for the machine you will be installing the probe software on.

DC Changes - Windows 2003 with Group Policy Management Console (GPMC):

1. Navigate to Start Menu -> Administrative Tools -> Group Policy Management
2. In the left-hand pane, navigate to Forest: "Domain Name" -> Domains -> "Domain Name", where "Domain Name" is then name of the domain you wish to modify
3. Right-click on "Domain Name" in the left-hand pane, and select "Create and Link a GPO Here..."
4. Name the new policy "WMI Permissions"
5. Ensure that the "WMI Permissions" policy is highlighted, and click on the button until the policy has a Link Order of 1.

DC Changes - Configuring DCOM Permissions

Note: All steps outlined in this section have been sourced from Microsoft articles available on the internet.

Before applying these steps on a network, please have a Microsoft certified engineer review and approve them for application to the network.

Note: the specific security rights outlined in this section were sourced from the following Microsoft document:

<http://msdn2.microsoft.com/en-us/library/aa393266.aspx>

1. Navigate to the "WMI Permissions" Group Policy, either by the "Group Policy Management" plug-in, or by the "Active Directory Users and Computers" plug-in. Please see the previous sub-chapter for the appropriate steps.
2. Ensure that the "WMI Permissions" policy is highlighted, and then click on the Edit button
3. Navigate to Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options
4. In the right-hand UI pane, double-click on DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax
5. Put a check-mark in the box beside Define this policy setting
6. Click on the Edit Security button

7. Click on the Add button; in the resulting pop-up window, specify the domain administrator account that is used by the N-able Windows Probe
8. Click on the OK button
9. In the Group or user names field, select the domain administrator you specified in step #7
10. In the Permissions for Administrators field, ensure that there is a check-mark in the Allow column for the Remote Access option
11. Click on the OK button
12. Click on the OK button
13. In the right-hand UI pane, double-click on DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax
14. Put a check-mark in the box beside Define this policy setting
15. Click on the Edit Security button
16. Click on the Add button; in the resulting pop-up window, specify the domain administrator account that is used by the N-able Windows Probe
17. Click on the OK button
18. In the Group or user names field, select the domain administrator you specified in step #16
19. In the Permissions for Administrators field, ensure that there is a check-mark under the Allow column for both Remote Launch and Remote Activation
20. Click on the OK button
21. Click on the OK button
22. Close the Group Policy Object Editor window
23. Click on the OK button, and close the Active Directory Users and Computers window

DC Changes - Enabling the Remote Administration Exception in Windows Firewall

Note: This section does not need to be followed if Windows Firewall is not enabled on the network

Note: The steps outlined in this section were sourced from the following Microsoft document:

<http://technet2.microsoft.com/windowsserver/en/library/b8057a7a-a0d3-40b5-8224-ea6a4f5e17231033.msp?mfr=true>

1. Navigate to the Group Policy plugin and edit the “WMI Permissions” group policy, as outlined in the Windows SBS section or the Windows 2003 section of this chapter
2. Navigate to Computer Configuration -> Administrative Templates -> Network -> Network Connections -> Windows Firewall -> Domain Profile
3. In the right-hand UI pane, double-click on Windows Firewall: Allow remote administration exception
4. Under the Settings tab, click on the Enabled radio button
5. In the Allow unsolicited incoming messages from: text field, input * to accept messages from anyone, or the IP address of your Windows Probe
6. Click on the OK button
7. Close the Group Policy Object Editor window
8. Close the Active Directory Users and Computers window

DC Changes - Pushing out Group Policy Changes

Any changes made to the Group Policy of a domain will not be applied by members of the domain until one of the following conditions are met:

1. The computer is rebooted
2. The default update interval has been exceeded (90 minutes on domain members, and 5 minutes for domain controllers)
3. The following command is run on the domain member: gpupdate /Target:computer

Probe Machine Changes - Giving an Account the right to “Log on as a service”

Before installing the probe, you’ll need to give the probe’s network account the right to “log on as a service” – this will allow the probe services to correctly function.

1. On the server/workstation on which you’ll be installing the probe, click on the Start menu, and then select Run
2. Type “gpedit.msc” (without the double-quotes), and press <ENTER>
3. In the resulting window, expand “Computer Configuration” in the left-hand pane
4. Navigate to the following location:

Windows Settings->Security Settings->Local Policies->User Rights Assignment

5. In the right-hand pane, double-click on “Log on as a service”
6. Click on the “Add User or Group” button, and specify the account you intend to give the probe during the probe installation process (**I have been using Administrator**)
7. Click the OK button in the “Select Users or Groups” window
8. Click the OK button in the “Log on as a service Properties” window
9. Click on the Start menu, and then select Run
10. Apply the changes:
 - a. For Windows XP/Windows 2003 devices, type “gpupdate /force” (without the double-quotes), and press <ENTER>.
 - b. For Windows 2000 devices, type “SECEDIT /REFRESHPOLICY MACHINE_POLICY /ENFORCE” (without the double-quotes), and press <ENTER>

Ncentral Changes – Setting up a new customer in Ncentral

1. Login to <https://ncentral.npce.net>
2. Click on Service Organization on the left column.
3. Click on Setup > Customers.
4. Click Add Customer.
5. Fill out the form with as much information as possible, remembering that the customer name will be the name shown on the left column for this customer. Leave the remote settings as default, and then click save and continue.
6. On the limits page, leave all as default and click finish.
7. Click NO on adding accounts now.

Ncentral Changes – Configuring the probe

1. Select the new customer on the left hand column.
2. Click on Setup > Probes.
3. Click on Add Probe button.
4. Name the probe (i.e. Admin-Probe), change probe type to Network – Windows, and set auto update to Always, then click save and continue.
5. Copy down the probe activation key (you will use this when installing the probe software).
6. Click on windowsprobe.exe to download the probe software.
7. Leave all other settings as default then click Finish.

Probe Machine Changes - Installing the Probe Software

1. Run the windowsprobe.exe installer. Make sure to use the administrator account when installing.

Ncentral Changes – Configure asset discovery tasks

1. Select the new customer on the left column.
2. Click on Setup > Asset Management Tasks > Discovery Jobs.
3. Click Add Discovery Job.
4. Name the first job “Initial”.
5. Set the IP Range as x.x.x.1-255, check the box for auto import, then click Finish.
6. Click Add Discovery Job.
7. Name the second job “reoccurring”,
8. Set the IP Range as x.x.x.1-255, check the box for auto import, change schedule to recurring at noon Monday thru Friday, then click finish.

****Note****

At this point the N-Able initial deployment is complete, and the probe will start auto detecting devices on the network. This process can take up to 6-12 hours depending on the network speed, number of devices, and current load on the network. You should however be able to see at least one asset added to the device list in Ncentral within an hour.