



**N-Partner**

**N-REPORTER**

WMI syslog management of  
Windows AD Server  
**V 1.1.2 (English)**

## Preface

This document introduces how to use WMI to manage the syslog of Windows AD Server for N-Reporter.

### Contents :

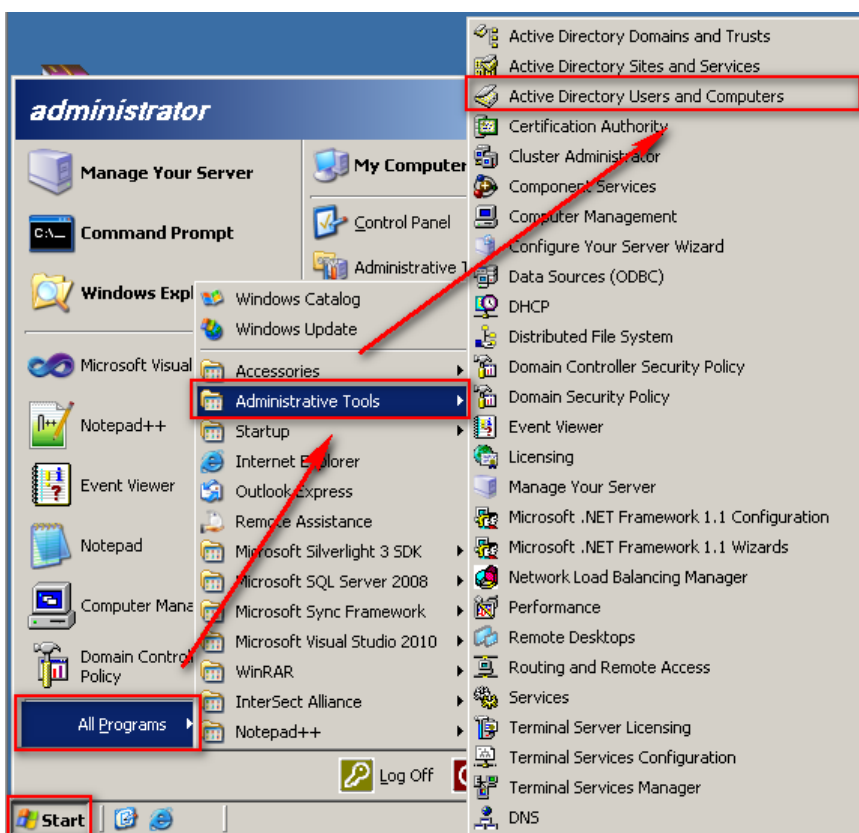
1.Configuration of WMI in Windows AD Server.....	2
1-1 Configuration of WMI in Windows 2003 AD Server .....	2
1-1-1 Add a new WMI remote login user to Active Directory .....	2
1-1-2 Windows 2003 AD Server Audit Configuration .....	7
1-1-3 Windows 2003 AD Server Firewall configuration .....	7
1-2 Windows 2008 AD Server Configuration.....	10
1-2-1 Add new WMI Remote login Domain User.....	10
1-2-2 Windows 2008 AD Server Audit Configuration .....	15
1-3 Windows 2012 AD Server Configuration.....	15
1-3-1 Add new WMI Remote login Domain User.....	15
1-3-2 Windows 2012 AD Server Audit Configuration .....	20
2. Add Windows AD Server WMI Device on N-Reporter .....	21
2-1 Add Windows AD Server WMI device .....	21
2-2 Setting NTP Server.....	24
Contact .....	25

# 1. Configuration of WMI in Windows AD Server

## 1-1 Configuration of WMI in Windows 2003 AD Server

### 1-1-1 Add a new WMI remote login user to Active Directory

Logon Windows AD server by administrator. Then click [Start / All Programs / Administrative Tools / Active Directory Users and Computers].



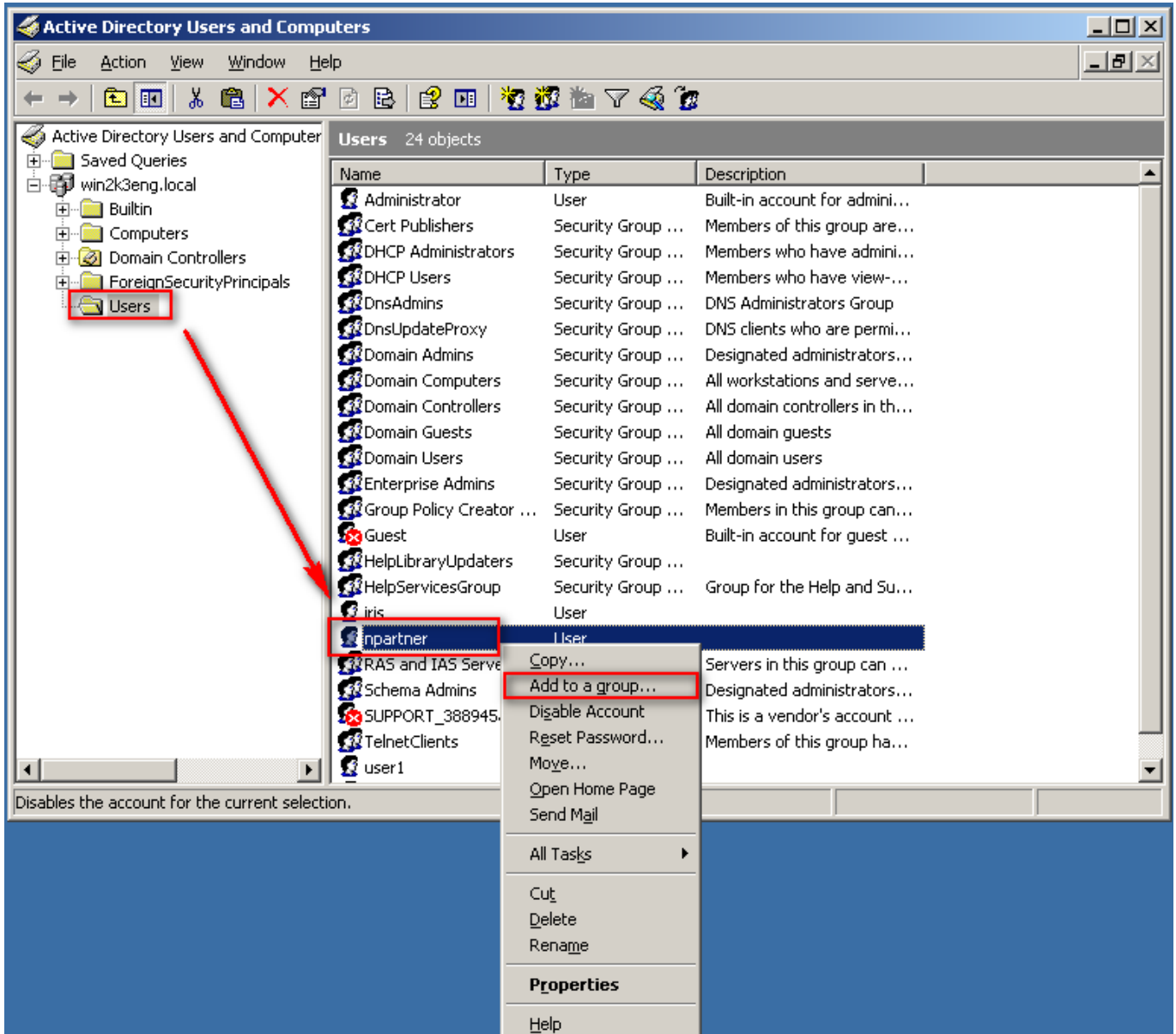


Check [Password never expires] after fill in the password. Click [Next] =>[Finish].

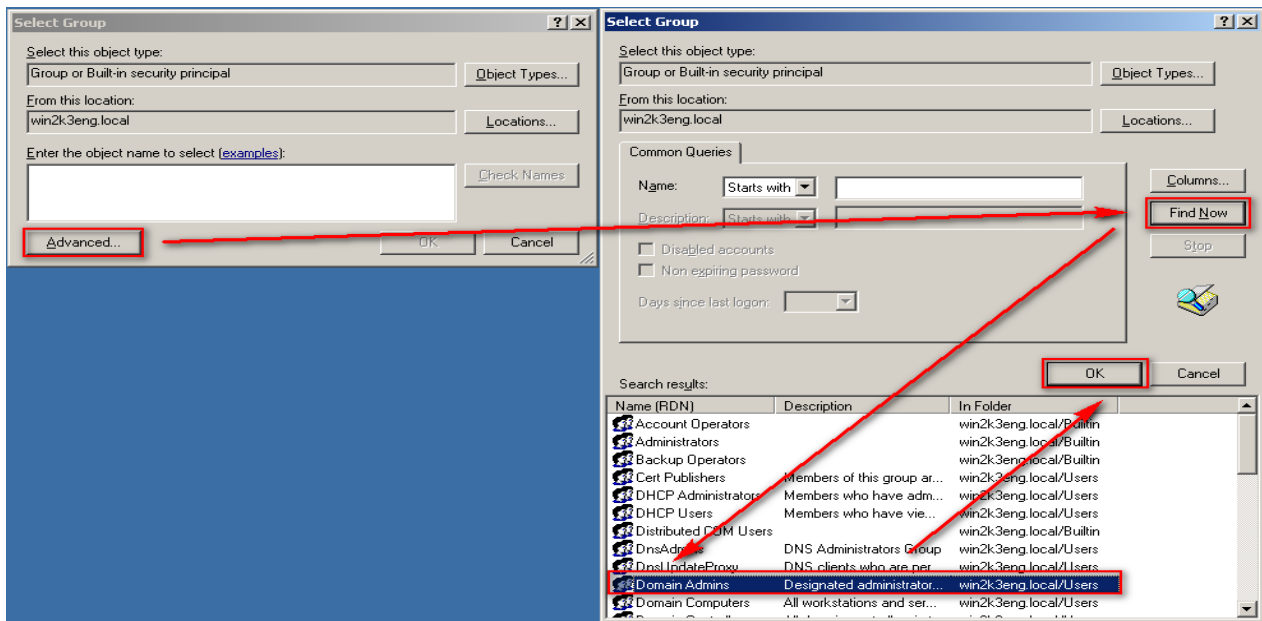
The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: win2k3eng.local/Users'. Below this are two password fields: 'Password:' and 'Confirm password:', both containing masked characters. Below the password fields are four checkboxes: 'User must change password at next logon', 'User cannot change password', 'Password never expires', and 'Account is disabled'. The 'Password never expires' checkbox is checked. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. Red boxes highlight the password fields, the 'Password never expires' checkbox, and the 'Next >' button. Red arrows point from the 'Password never expires' checkbox to the 'Next >' button.

The screenshot shows the 'New Object - User' dialog box in a summary view. It says 'Create in: win2k3eng.local/Users'. Below this, it says 'When you click Finish, the following object will be created:'. A text box contains the following information: 'Full name: npartner', 'User logon name: npartner@win2k3eng.local', and 'The password never expires.'. At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'. The 'Finish' button is highlighted with a red box.

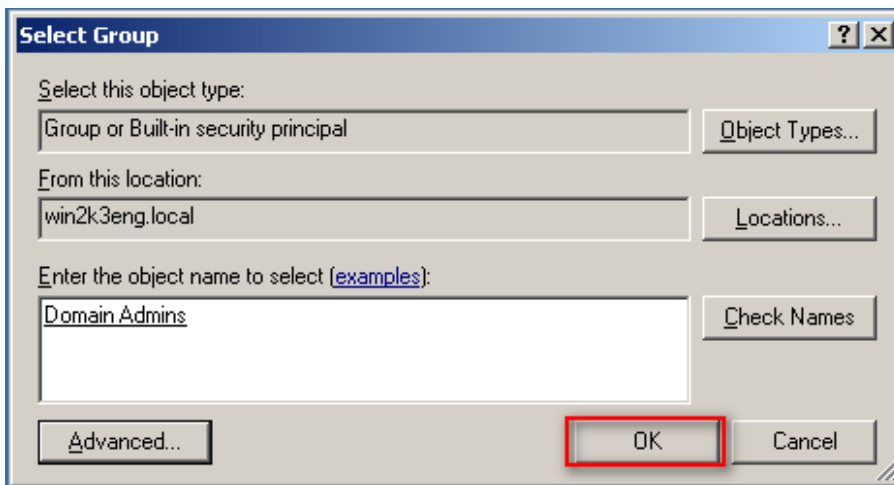
Click [ Users ]. Right click "npartner ", then click [ Add to a group].



Click [Advance/ Find Now/ Domain Admins/ OK], add the WMI remote user npartner into the Domain Admins group.



Click [OK]

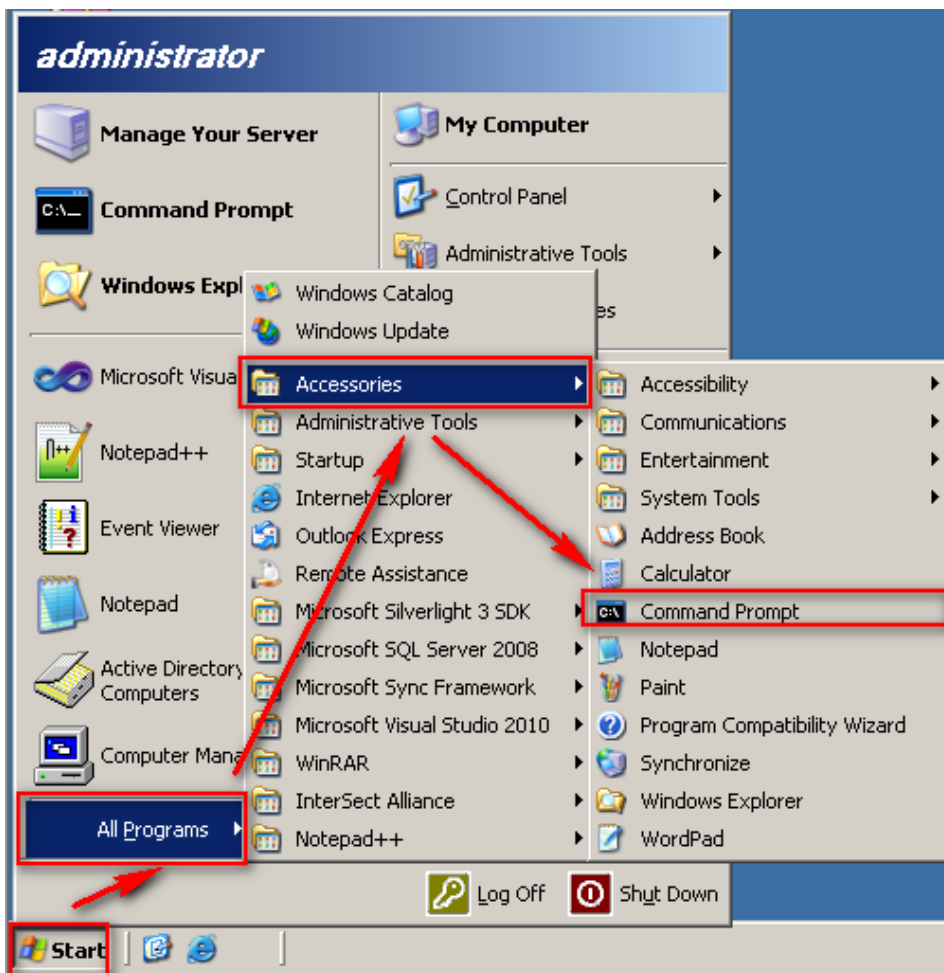


## 1-1-2 Windows 2003 AD Server Audit Configuration

Please refer to the chapter 2 [Windows 2003 AD Server Audit configuration] of the document 「 [Windows AD audit to syslog](#) 」 to setup audit policy of the Default Domain Controller.

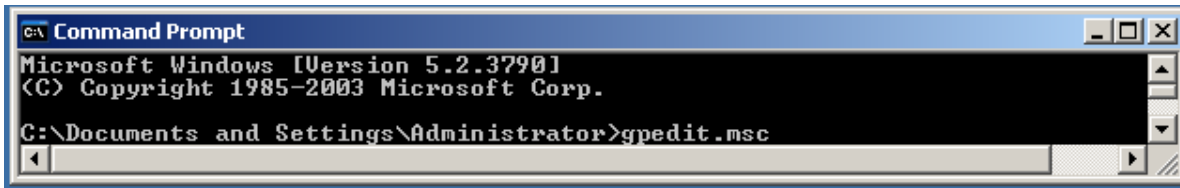
## 1-1-3 Windows 2003 AD Server Firewall configuration

Clikc [Start/ All Programs/ Accessories/ Command Prompt].

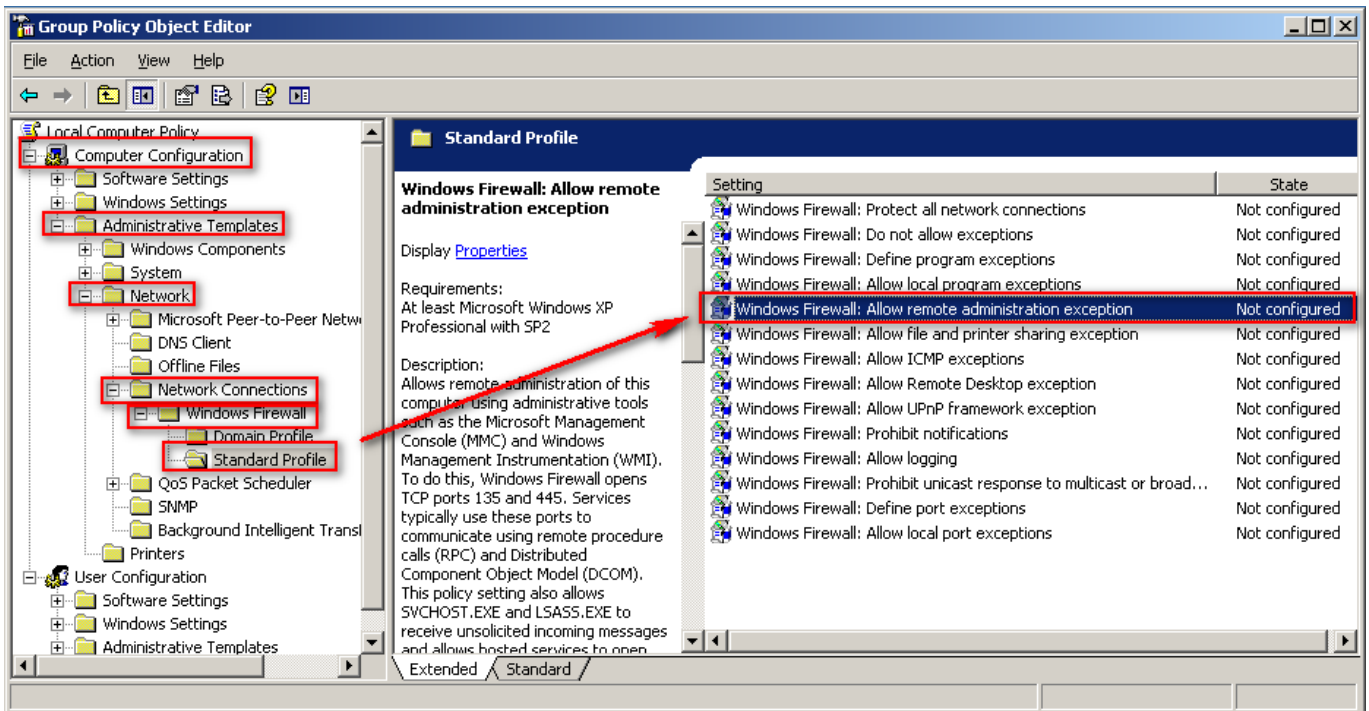




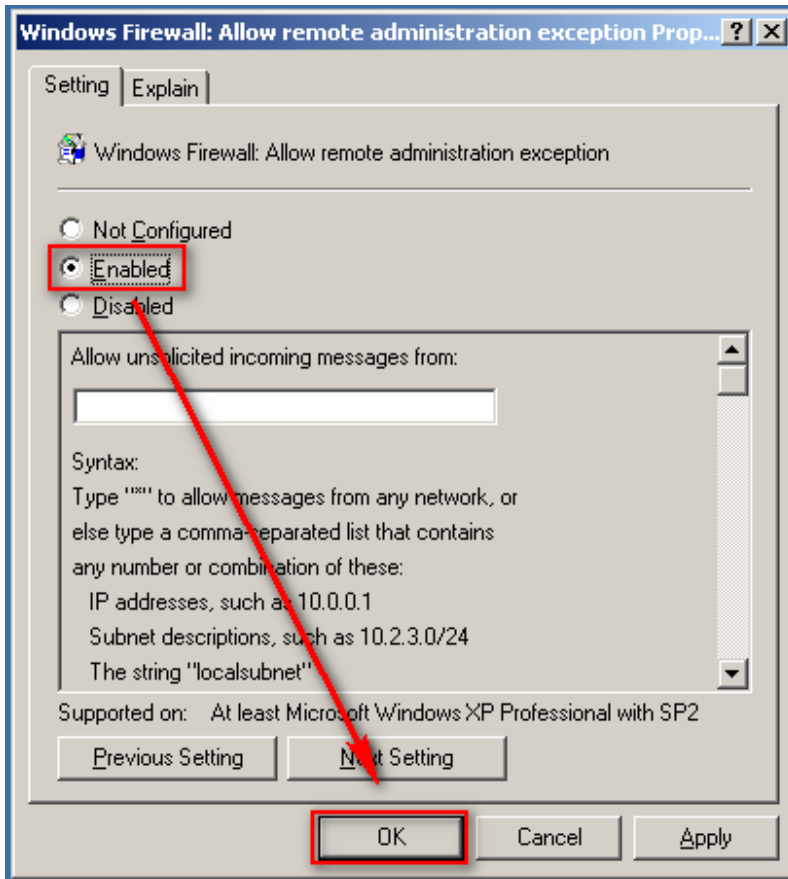
Type 『gpedit.msc』 and open the [Group Policy Object Editor] to setup the [Local Computer Policy].



Double click [Computer Configuration/ Administrative Templates/Network/Network Connections /Windows Firewall/Standard Profile]. Double click (Windows Firewall: Allow remote administration exception) ].



Check [ Enabled ]. Click [ OK ].

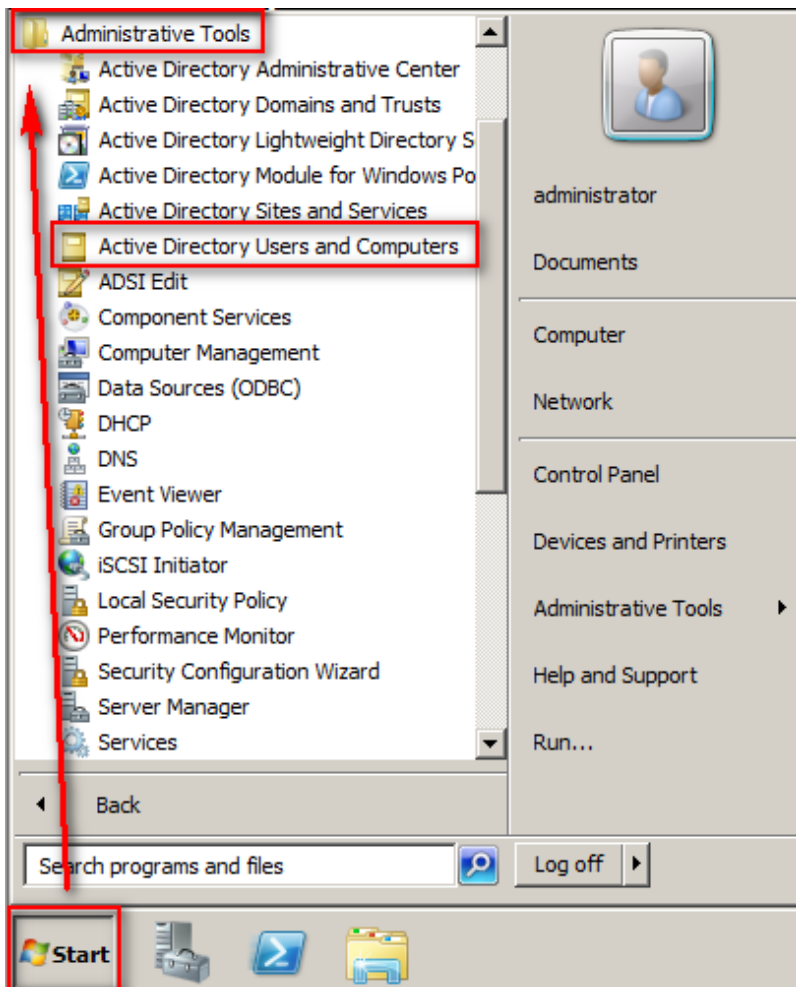


Remark : Please allow the Windows AD Server DCOM port TCP 135 on the firewall.

# 1-2 Windows 2008 AD Server Configuration

## 1-2-1 Add new WMI Remote login Domain User.

Logon the Windows AD server by domain administrator. Click [Start/All Programs/Administrative Tools/Active Directory Users and Computers].



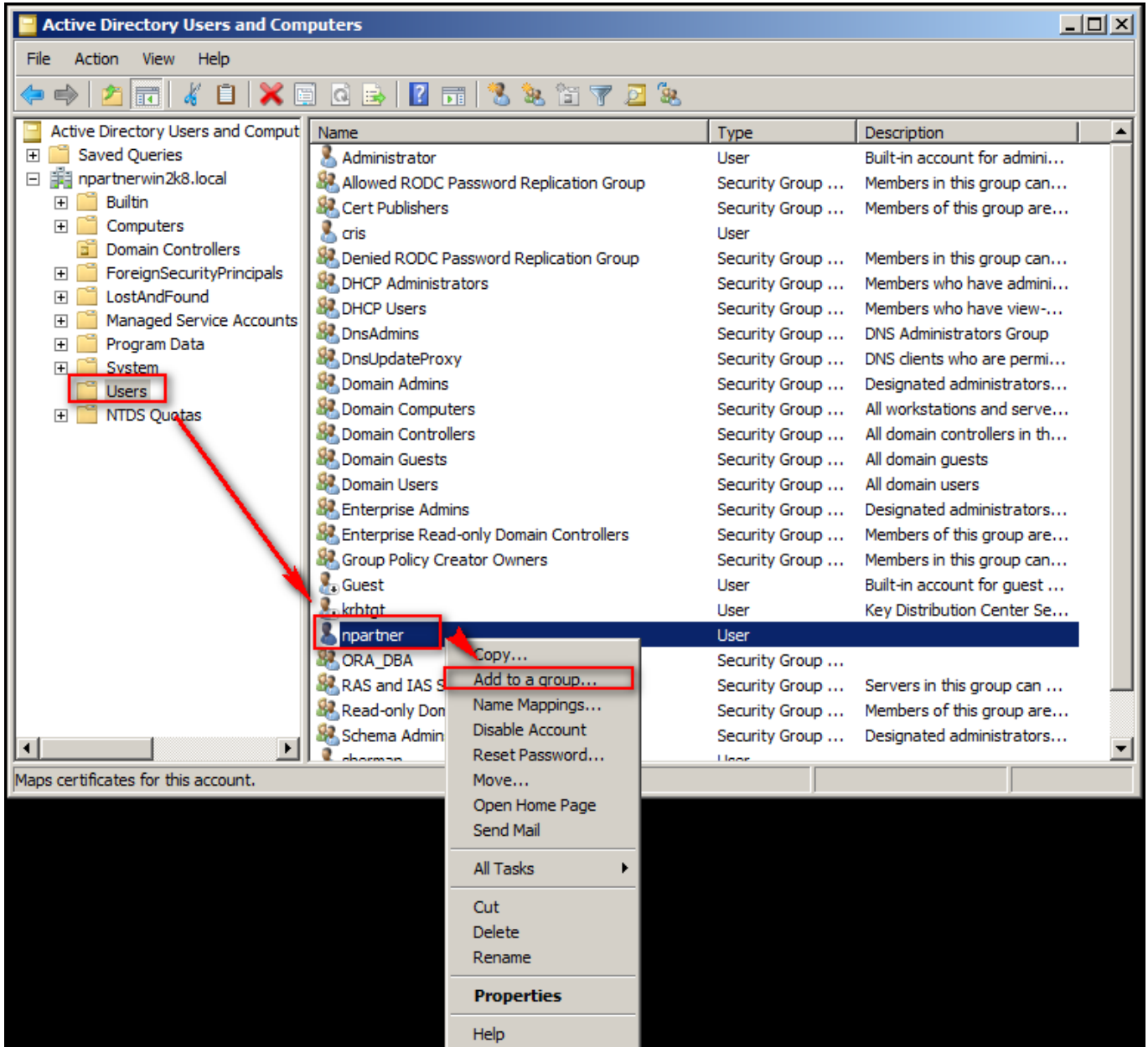


Check [Password never expires] after fill in the password. Click [Next/Finish].

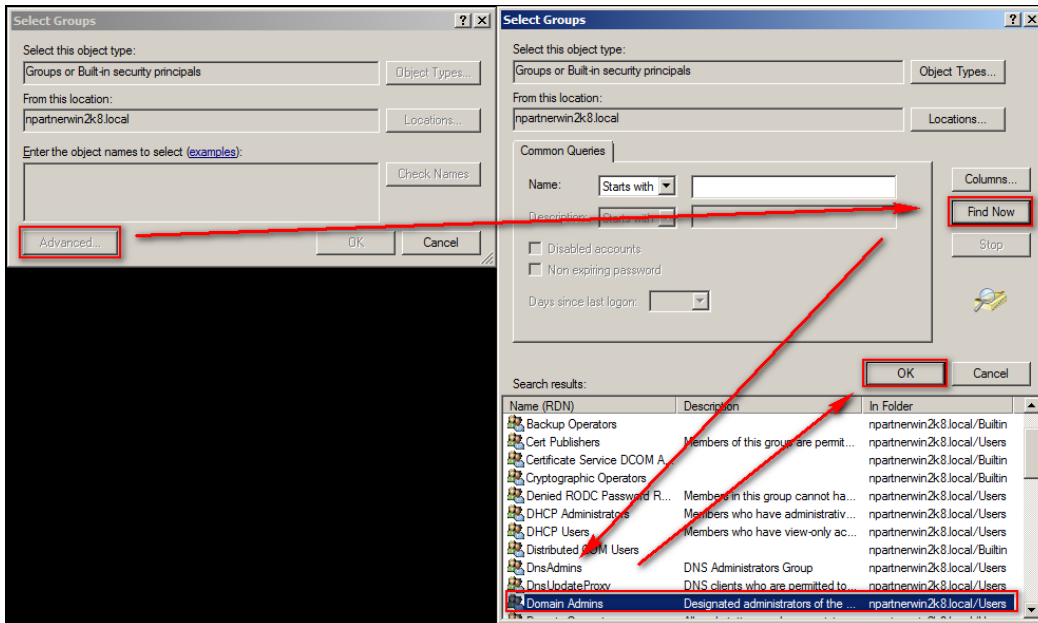
The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: npartnerwin2k8.local/Users'. Below this are two password input fields: 'Password:' and 'Confirm password:', both containing masked characters. Below the password fields are four checkboxes: 'User must change password at next logon', 'User cannot change password', 'Password never expires' (which is checked), and 'Account is disabled'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'. Red boxes highlight the password fields, the 'Password never expires' checkbox, and the 'Next >' button. Red arrows point from the 'Password never expires' checkbox to the 'Next >' button.

The screenshot shows the 'New Object - User' dialog box in a summary view. It says 'Create in: npartnerwin2k8.local/Users'. Below this is a text area that reads: 'When you click Finish, the following object will be created:'. The text area contains the following information: 'Full name: npartner', 'User logon name: npartner@npartnerwin2k8.local', and 'The password never expires.'. At the bottom are three buttons: '< Back', 'Finish', and 'Cancel'. The 'Finish' button is highlighted with a red box.

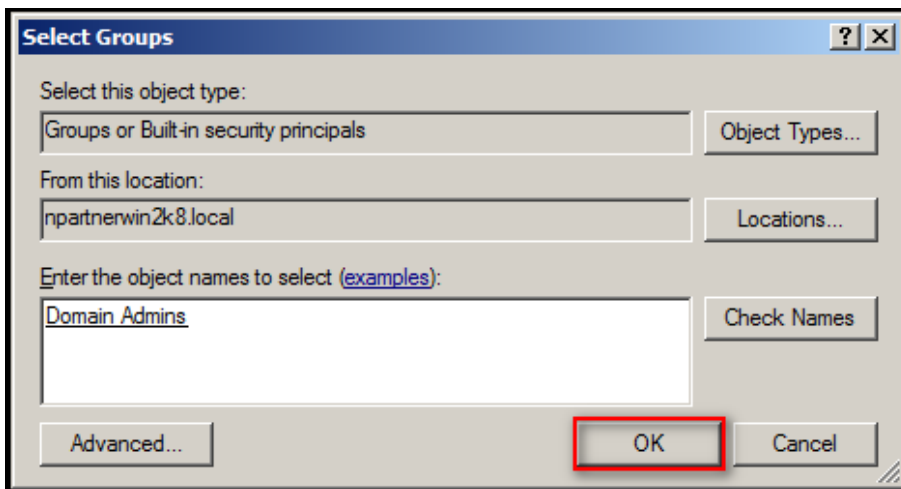
Click [Users]. Right click "npartner" name and click [Add to a group].



Click [Advanced/ Find now/Domain Admins/ok], add the WMI remote user npartner into the Group of the Domain Administrators.



Click [OK].



## 1-2-2 Windows 2008 AD Server Audit Configuration

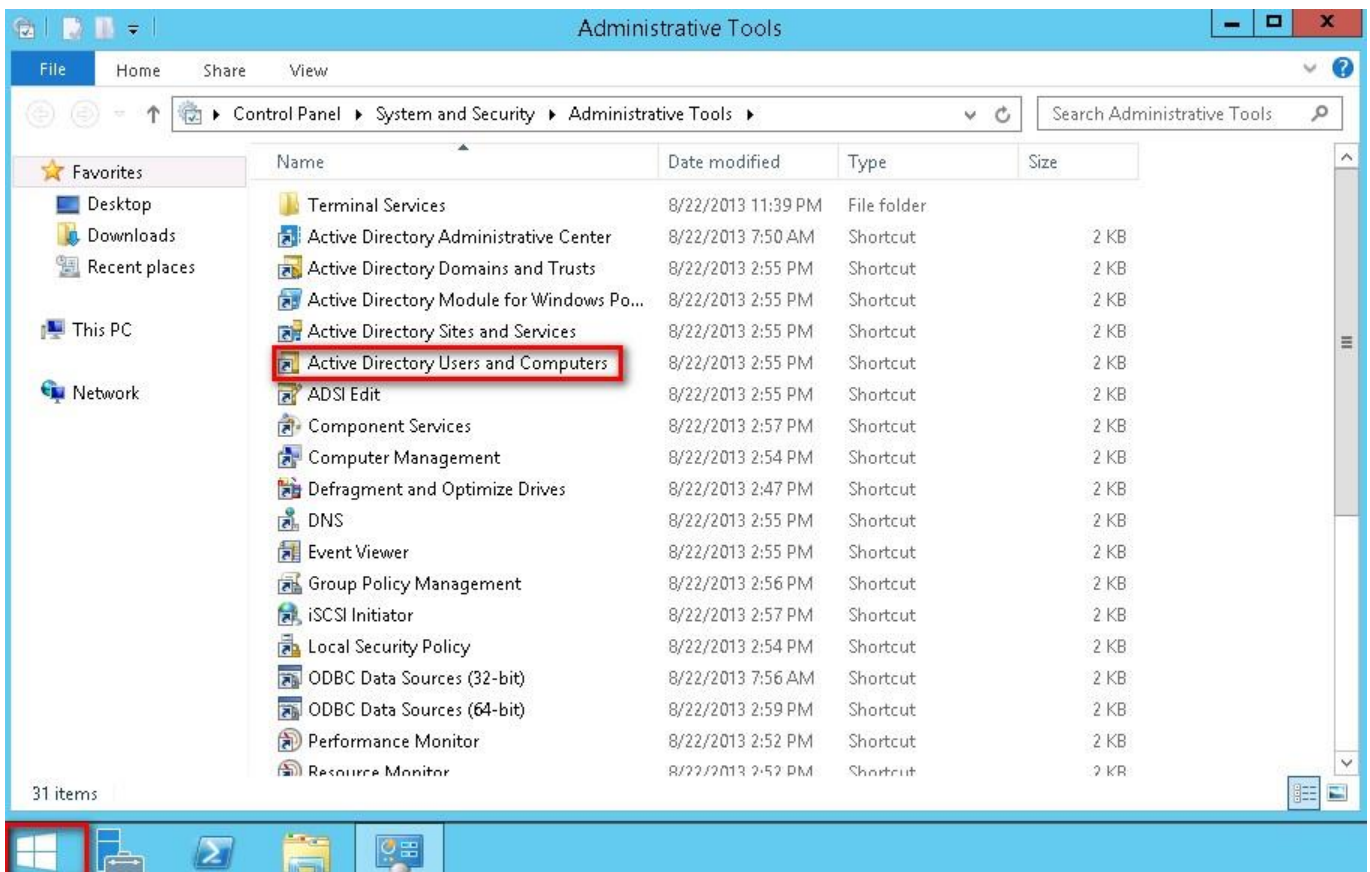
Please refer to the Chapter 3 [Windows 2008 AD Server Audit configuration] of the document 「 [Windows AD audit to syslog](#) 」 to setup audit policy of the Default Domain Controller.

Remark : Please allow the Windows AD Server DCOM port TCP 135 on the firewall.

## 1-3 Windows 2012 AD Server Configuration

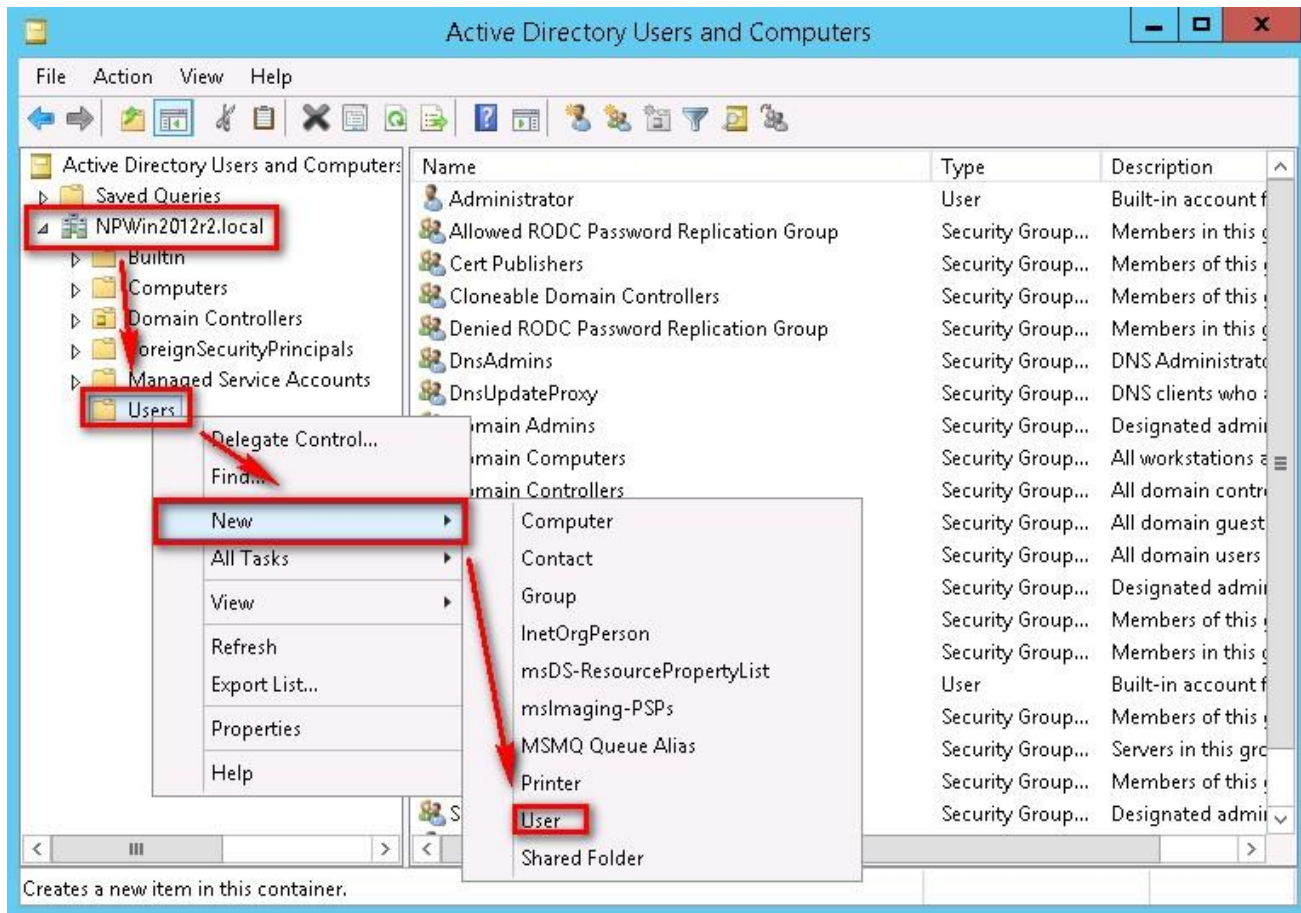
### 1-3-1 Add new WMI Remote login Domain User

Logon the Windows AD server by domain administrator. Click [ Start/All Programs/Administrative Tools/Active Directory Users and Computers].





Click forest root domain, the NPWin2012r2cht.local in this example. Right click [Users] and Click [New/User].



Type "npartner" into the field "Last Name" . Type "npartner" into the User Logon Name.

After all click [Next].

New Object - User

Create in: NPWin2012r2.local/Users

First name:  Initials:

Last name:

Full name:

User logon name:  @NPWin2012r2.local

User logon name (pre-Windows 2000):

< Back **Next >** Cancel

Check [Password never expires] after fill in the password. Click [Next/Finish].

New Object - User

Create in: NPWin2012r2.local/Users

Password:

Confirm password:

User must change password at next logon

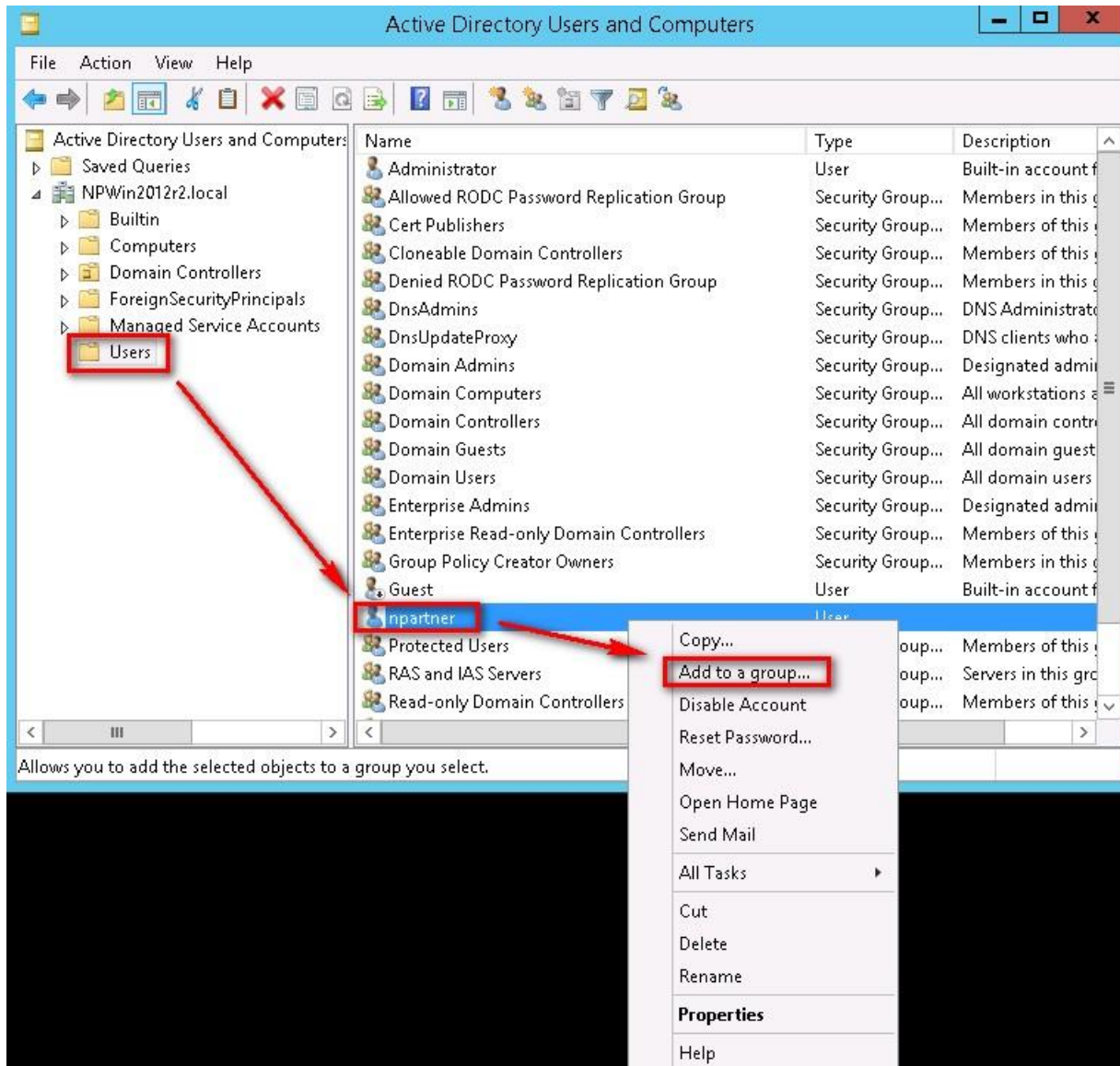
User cannot change password

Password never expires

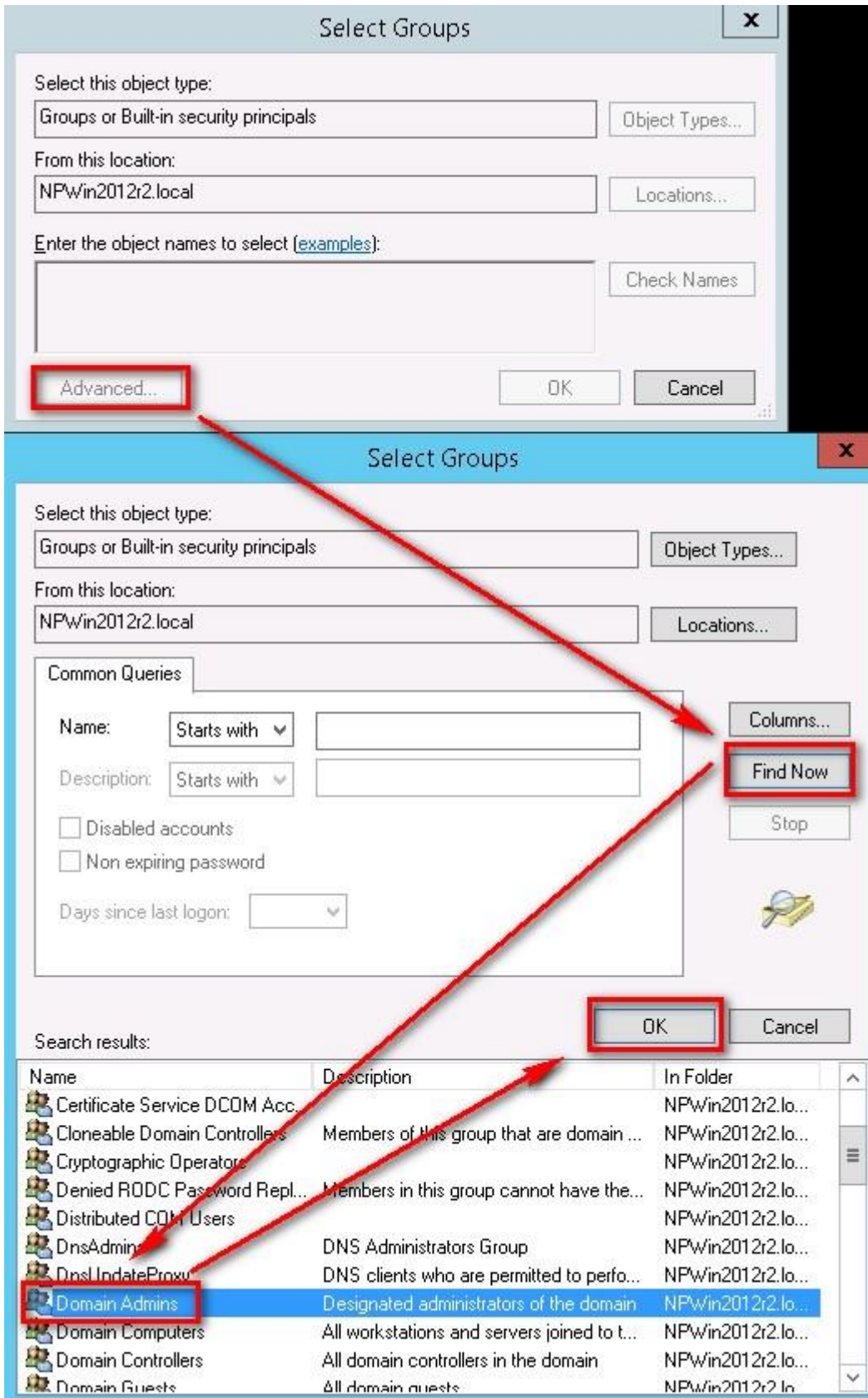
Account is disabled

< Back **Next >** Cancel

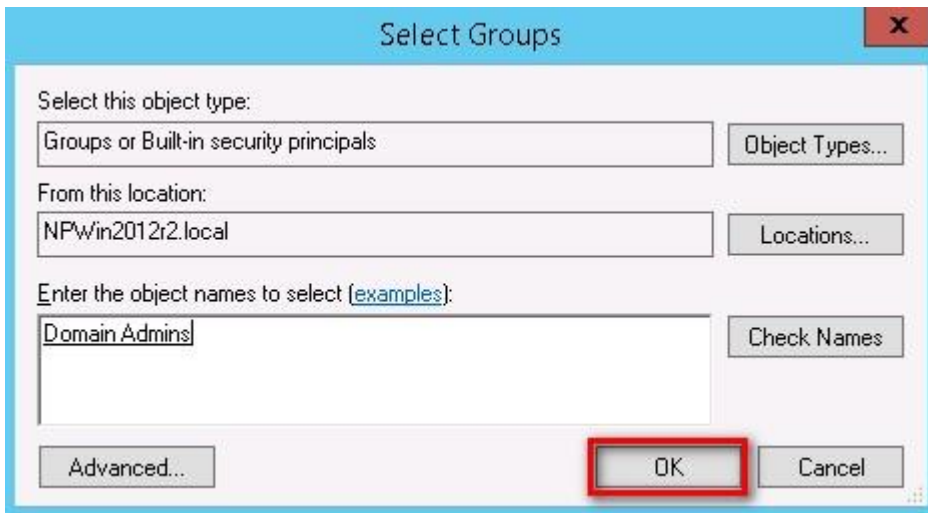
Click [Users]. Right click "npartner" , then click [Add to a group].



Click [Advanced/ Find now/ Domain Admins/ OK], add the WMI remote user npartner into the Group of the Domain Admins.



Click [OK]



### 1-3-2 Windows 2012 AD Server Audit Configuration

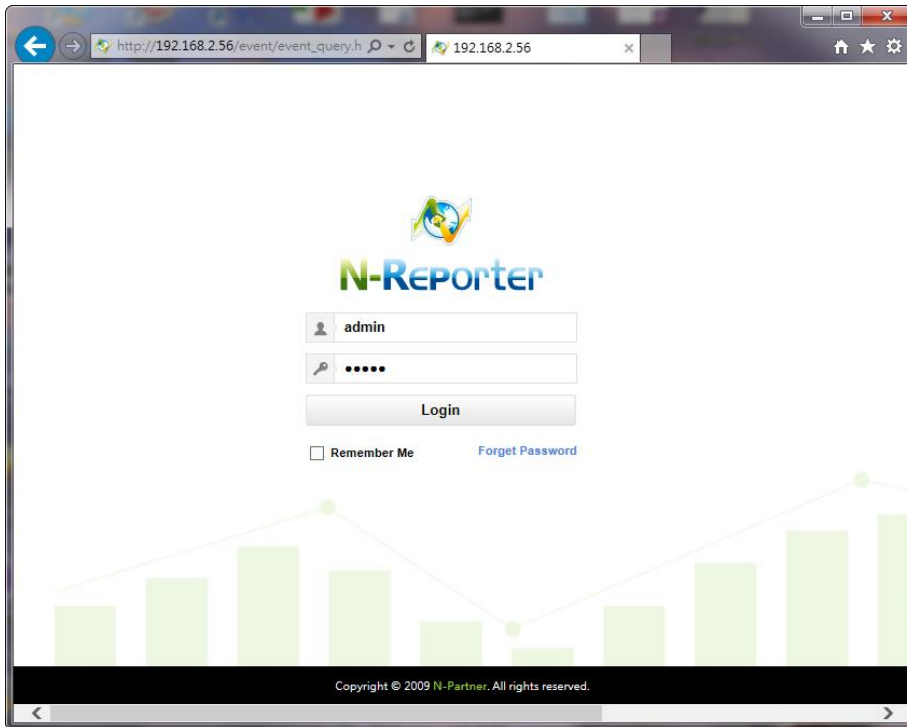
Please refer to the Chapter 4 [Windows 2012 AD Server Audit configuration] of the document 「 [Windows AD audit to syslog](#) 」 to setup audit policy of the Default Domain Controller.

Remark : Please allow Windows AD Server the DCOM port TCP 135 on the firewall

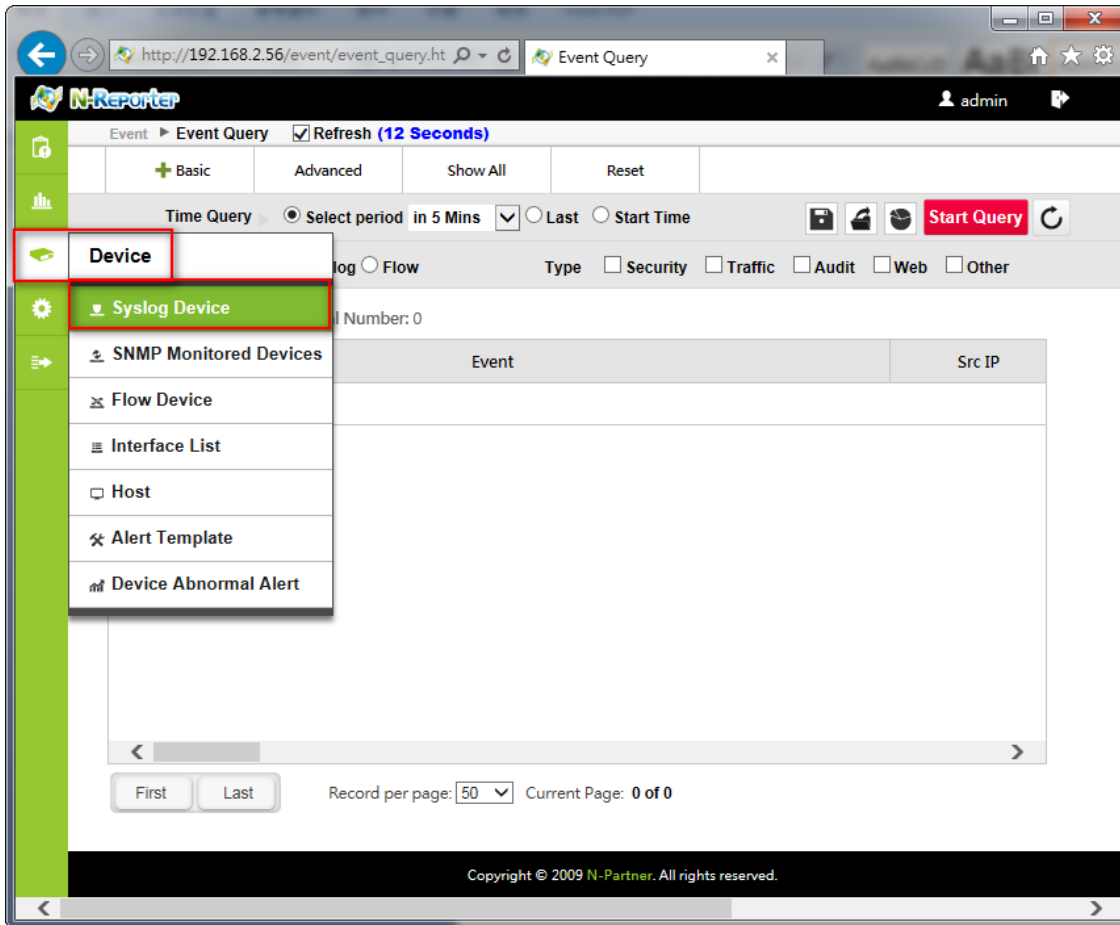
## 2. Add Windows AD Server WMI Device on N-Reporter

### 2-1 Add Windows AD Server WMI device


Login the N-Reporter by go to URL [http://\\$N-Reporter\\_IP](http://$N-Reporter_IP). For example, go to <http://192.168.2.56>. Input account name and password. The default username and password are admin/admin. Click [Login] to logon N-Reporter Web.

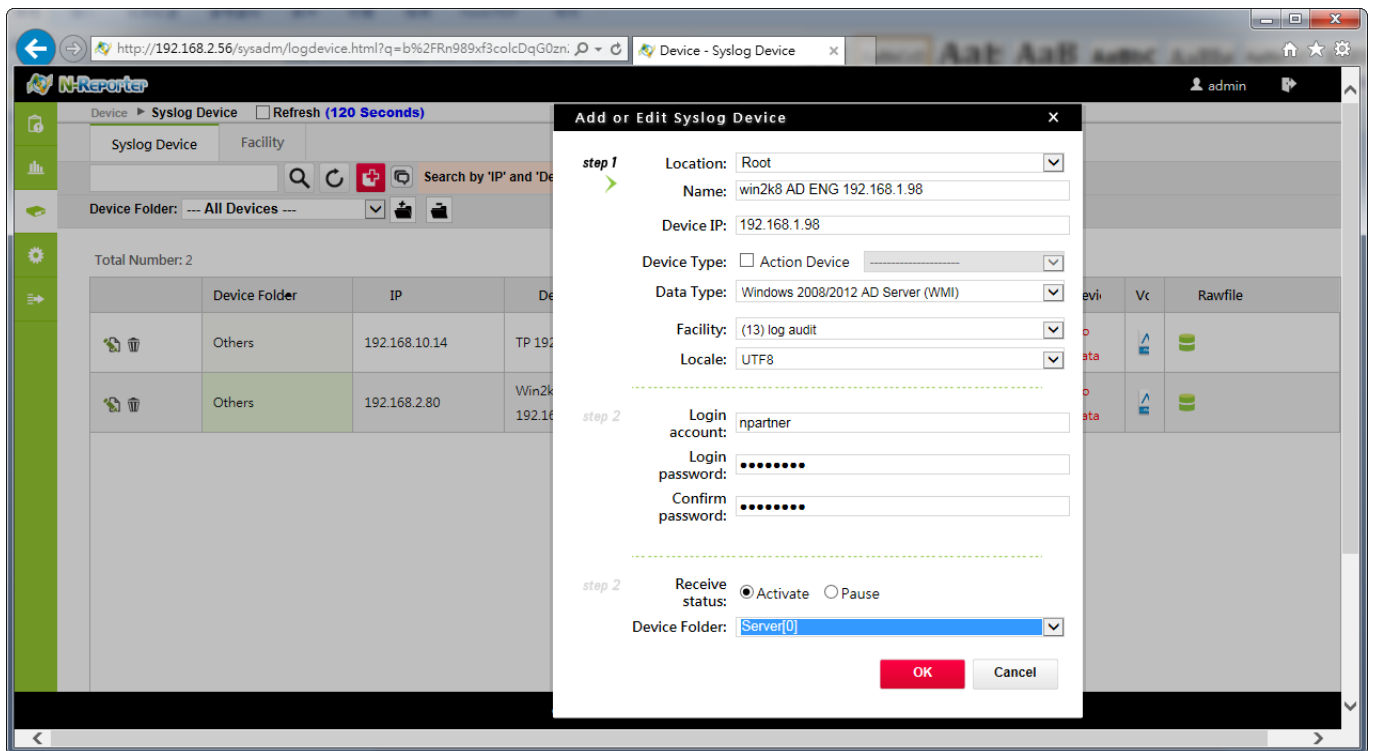


Click [Device / Syslog Device].





Click  to open a windows [Add or Edit Syslog Device]. Select the [Location] where the WMI device is belongs to. For example, the location here is Root. Type Name and Device IP of the WMI device. Select [Windows 2008/2012 AD Server (WMI)] in data type and [(13) log audit] in Facility and Locale as "UTF8". Type in login account, Login password and Confirm password of the WMI device and check [Activate] to start receiving log from the WMI device. Then select the "Device folder" and click [OK].

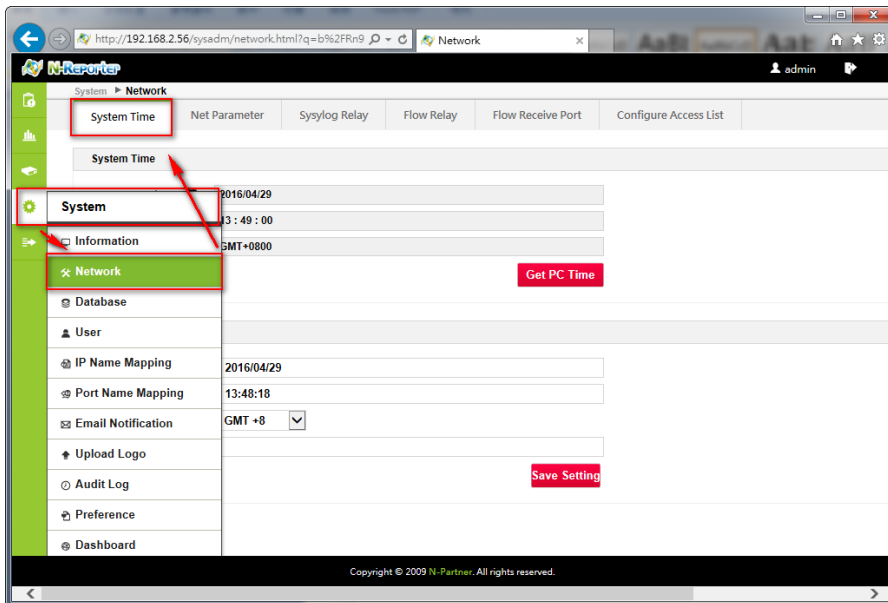


Remark : Choose [BIG5] for Windows 2003 Traditional Chinese Version. Choose [GB2312] for 2003 Simple Chinese Version. Choose [ UTF8] for Windows 2003 English Version. For Windows 2008/2012, please use [UTF8].



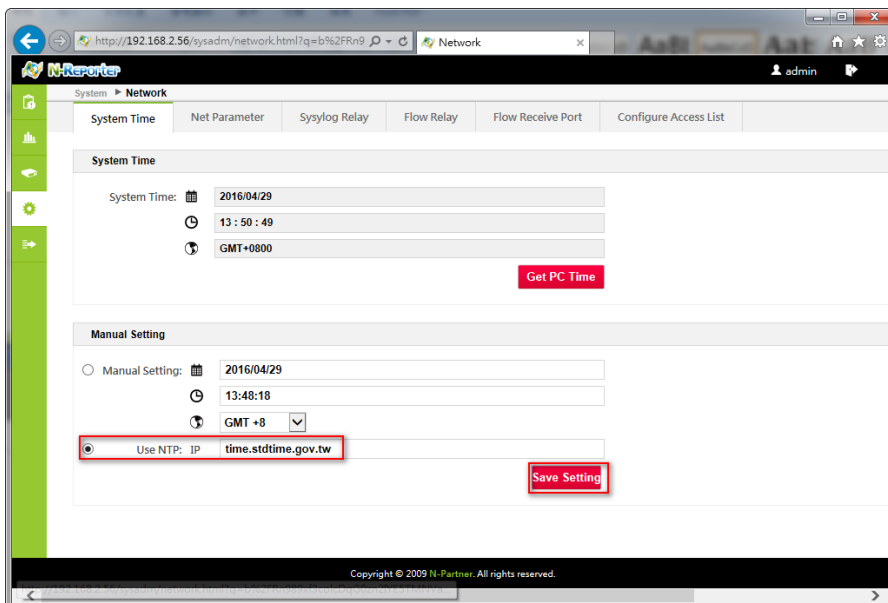
## 2-2 Setting NTP Server

Click [ System / Network / System Time].



Click [Use NTP]. Type NTP server IP or host name, for example "time.stdtime.gov.tw".

Click [Save Setting]. You can also type "tw.pool.ntp.org or internal NTP server IP.



Remark : If the time setting between WMI device and N-Reporter system is not the same, it will cause WMI query data loss. After you add a WMI device, then set the NTP Server, synchronize system time every day.

## Contact

### **N-Partner :**

TEL: +886-4-23752865

FAX: +886-4-23757458

### **TAC Support :**

Email: [support@npartnertech.com](mailto:support@npartnertech.com)

Skype : [support@npartnertech.com](https://www.skype.com/people/support@npartnertech.com)

### **Sales Support :**

Email: [sales@npartnertech.com](mailto:sales@npartnertech.com)

