USG Single Sign-On Installation Guide

1 Requirement for Domain Controller, Domain workstation

1.1 Requirement for Domain Controller(DC)

- Operating System
  - Windows Server 2008 Enterprise Edition (32/64)
  - Windows Server 2008 R2 (64)
  - Windows Server 2012 Standard (64)
- Support Power Shell for Group Policy Object command and power shell Command

1.2 Requirement for Domain Workstation(Workstation)

- Operating System
  - Windows 7 Pro (32/64)
  - Windows Server 2008 Enterprise Edition (32/64)
  - Windows Server 2008 R2 (64)
  - Windows Server 2012 Standard (64)
- Support Power Shell Command

1.3 Common requirement

- Microsoft Visual C++ 2010 Redistributable Package
- Microsoft .NET Framework 4

1. Create GPO for Firewall
2. Set client's administrator permission for SSO Agent User
3. Reboot workstation computer (to apply new firewall rule on workstation)

2 Scenario 1: Installation SSO Agent on Domain Controller

Note: this scenario is for the domain with only one domain controller.

If you have 2 domain controllers, then go for scenario 2.

2.1 Preparing for Installation

2.1.1 Prepare package of SSO Agent into your hard disk

- Copy the ZIP package file to your domain controller and extract to local file folder

2.1.2 Install .NET Framework v4.0.30319 or above

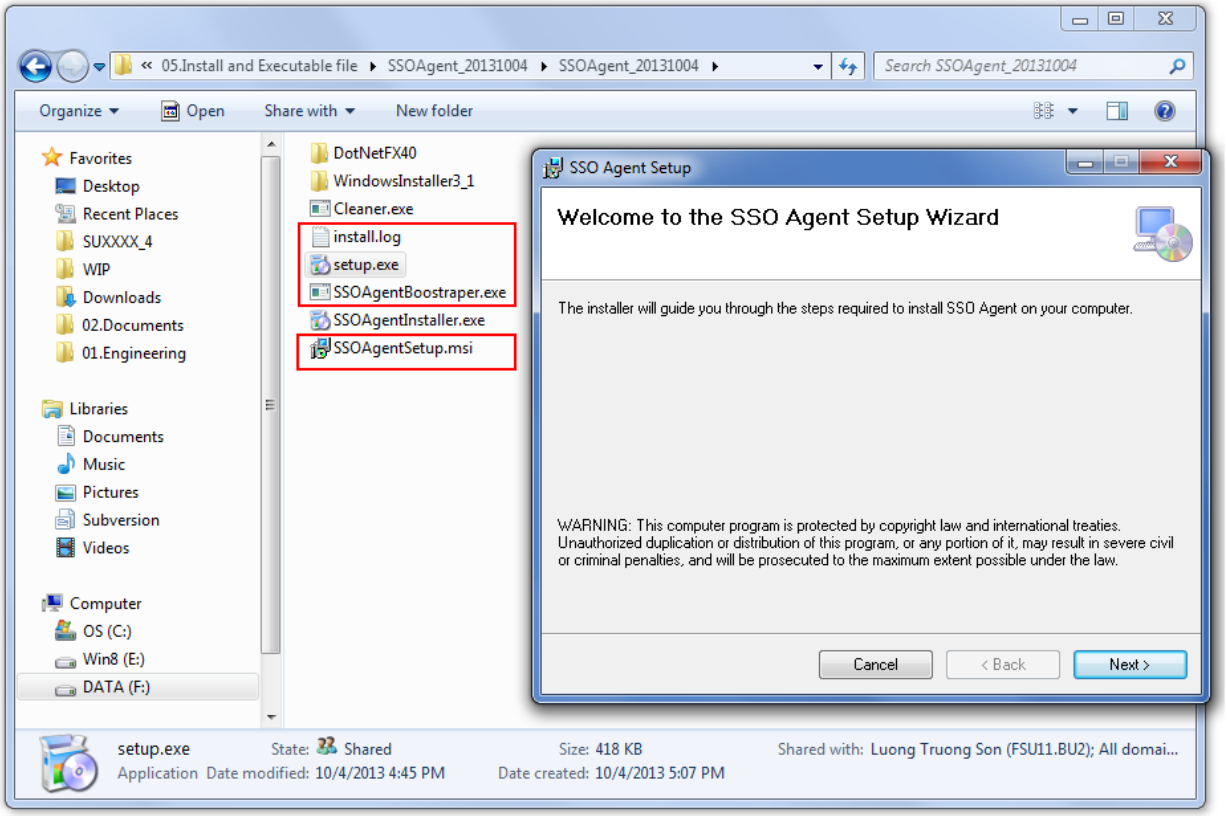
- Double-click /SSOAgent_Install_package/DotNetFX40/dotNetFx40_Full_x86_x64.exe to install

2.1.3 Create a domain account for SSO Agent service

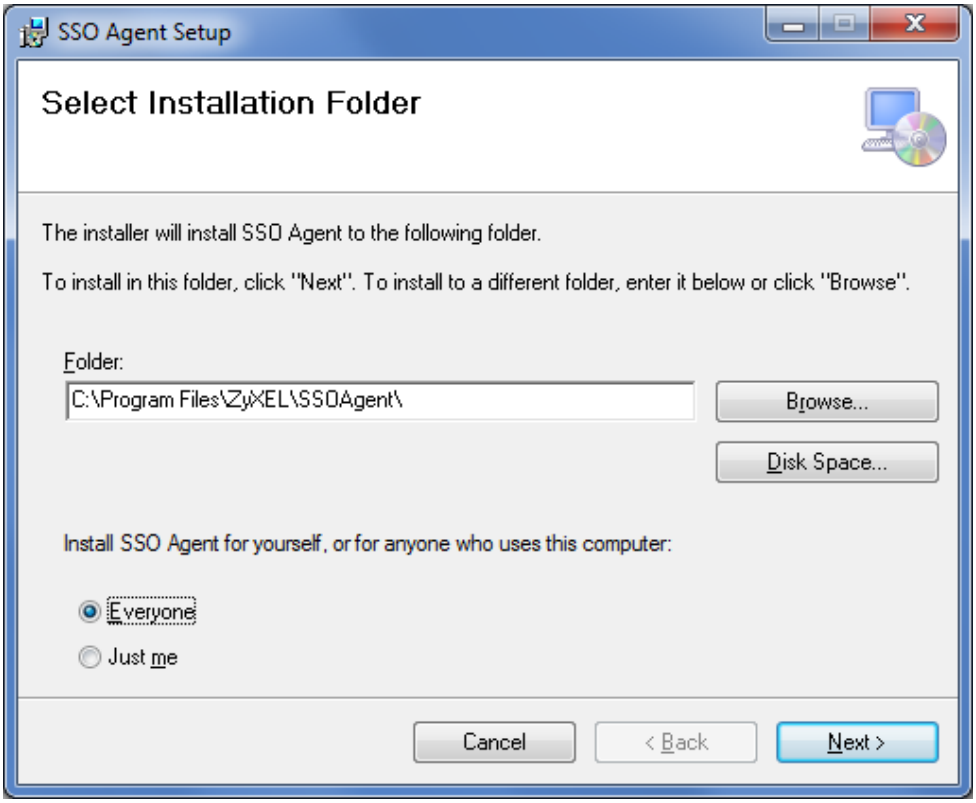
- It's recommend to use another domain account instead of domain administrator to run the SSO Agent service
- Using Active Directory Users and Computers tool to create a new domain account, for example "ssoadmin", and join this account to Domain Admins group.

2.2 Install SSO Agent on domain controller

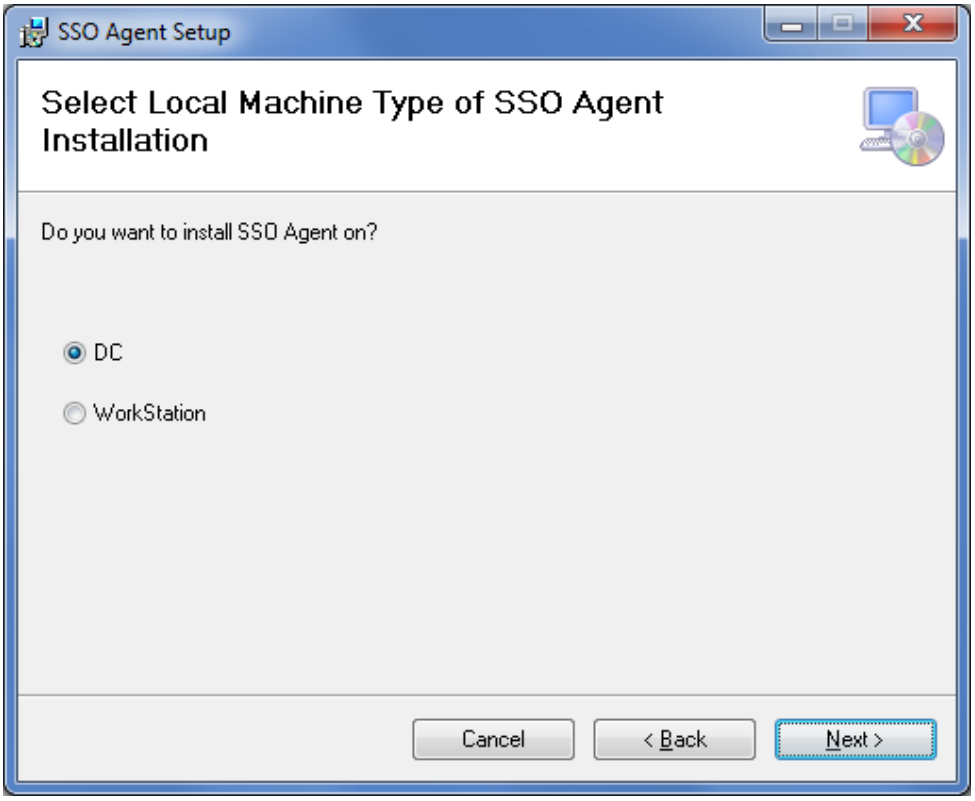
- Double click the install file : **SSOAgentInstaller.exe**
- A windows for unzip package will be display for a while and after that Dialog Welcome of installer will be displayed immediately.
- When run installer, there are some files for install are displayed in folder of package SSO Agent. These files will be removed when finish install.



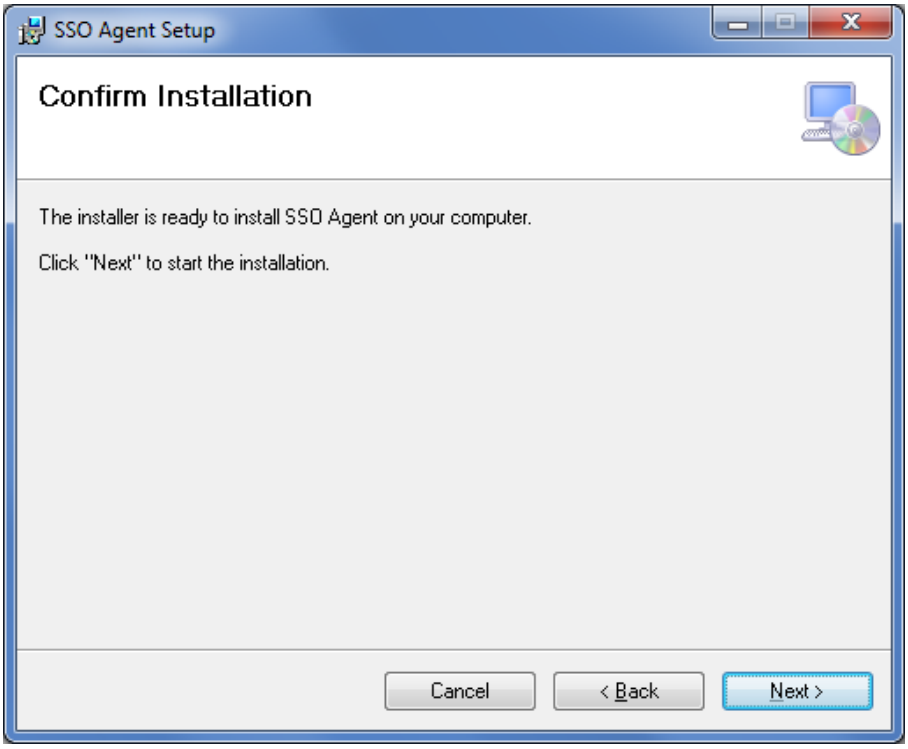
- Click [Next], Dialog Select folder setup will be displayed:
- Select folder or setup with default location, then click Next



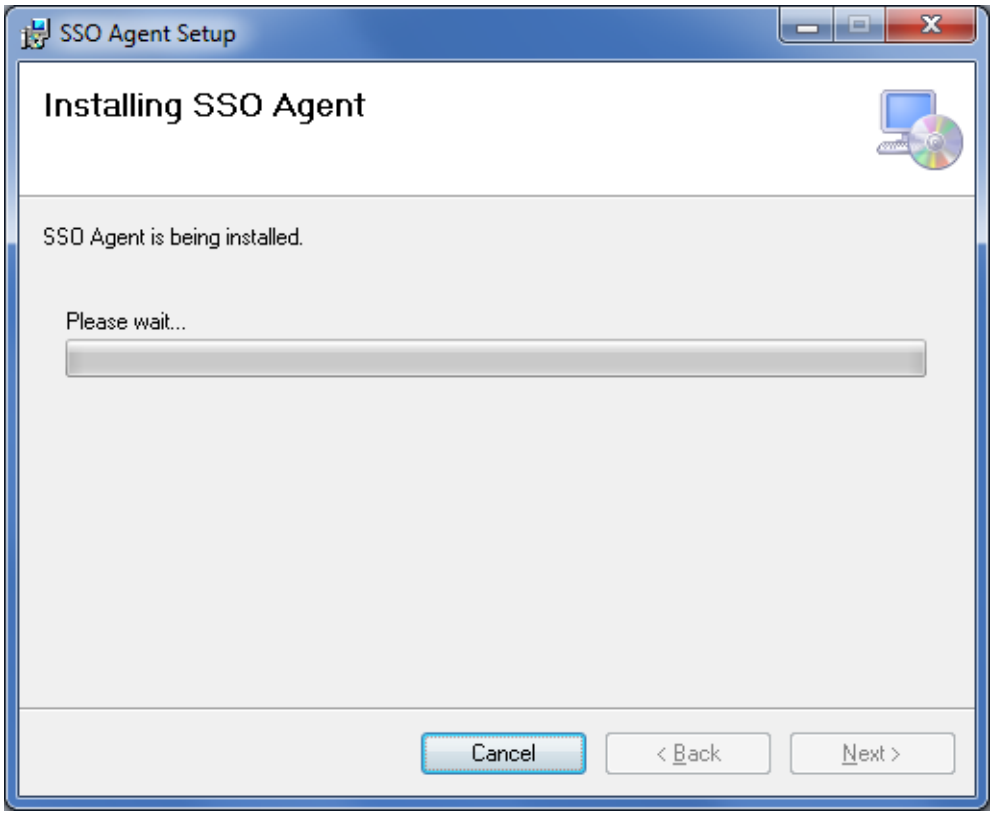
- Select install SSO Agent on DC in this scenario, then click Next.



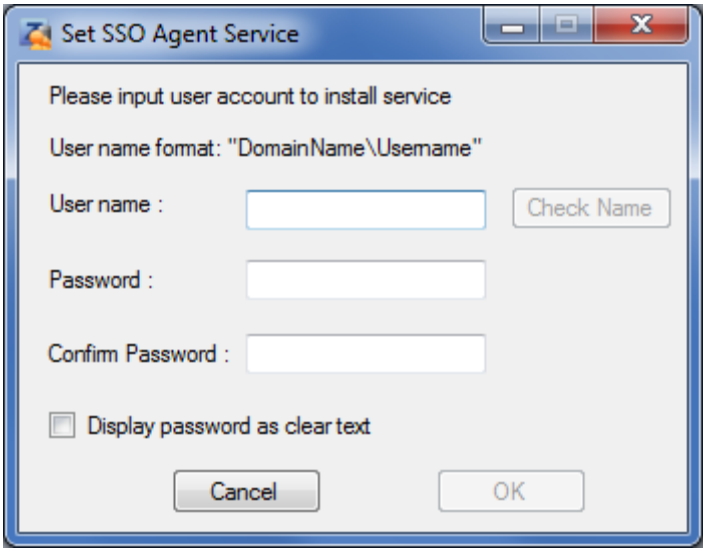
- Then click Next to confirm start to install.



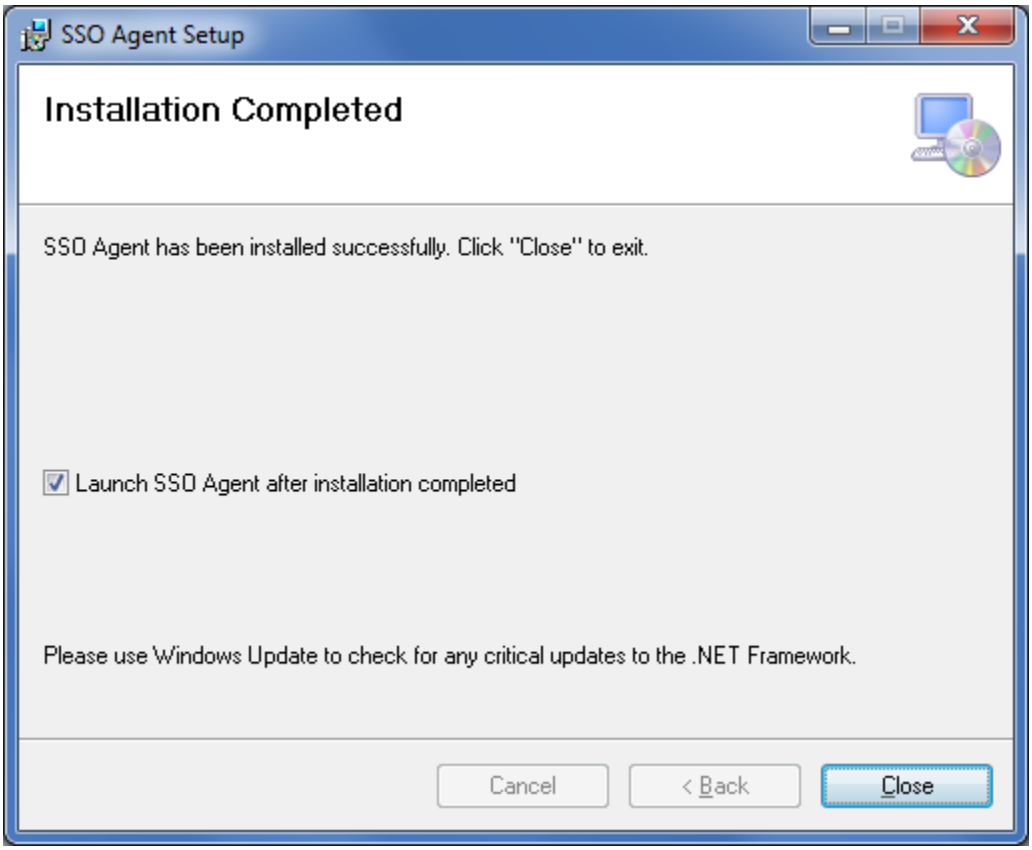
- Click [Next], and wait process setup running.



- After a while, a “Set SSO Agent Service” dialog window will pop-up.
  Please enter the Domain\Username and password of the domain account that created in step 2.1.3.
  Then click OK to continue.



- When installation finish, Dialog notify setup will be displayed with option choose default run application immediately.



- Click Close to finish Install SSO Agent. After install application successfully, Tray Icon of application will be pin to task bar.

3 Scenario 2: Installation SSO Agent on domain workstation

3.1 Preparing for Installation **on domain workstation**

3.1.1 Prepare package of SSO Agent & Configure Logs Collector Tool

- Copy the ZIP package file to your domain workstation and extract to local file folder

3.1.2 Install .NET Framework v4.0.30319 or above

- Double-click /SSOAgent_Install_package/DotNetFX40/dotNetFx40_Full_x86_x64.exe to install

3.1.3 Create a domain account for SSO Agent service

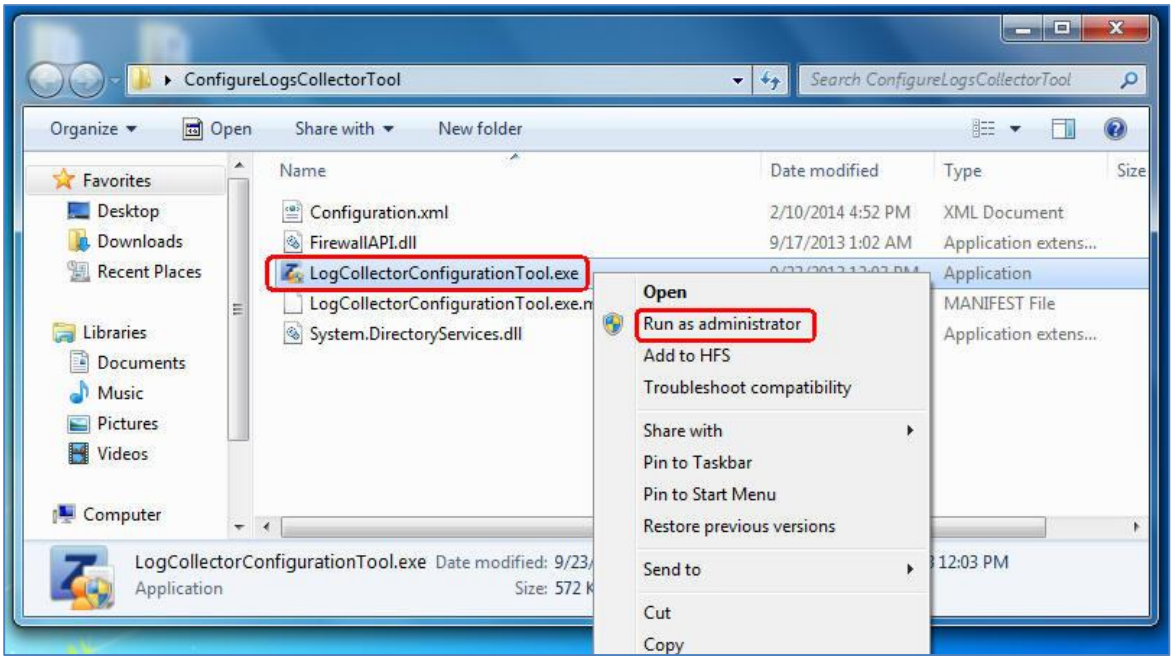
- It's recommend to use another domain account instead of domain administrator to run the SSO Agent service
- Using Active Directory Users and Computers tool to create a new domain account, for example "ssoadmin", and join this account to Domain Admins group.

3.1.4 Login domain workstation with the domain account created in step 3.1.3

3.2 Setup Security Event Logs Collector

3.2.1 Open Configuration Collector Logs Tool

- Run \ConfigureLogsCollectorTool\ConfigureLogsCollector.exe, as administrator.

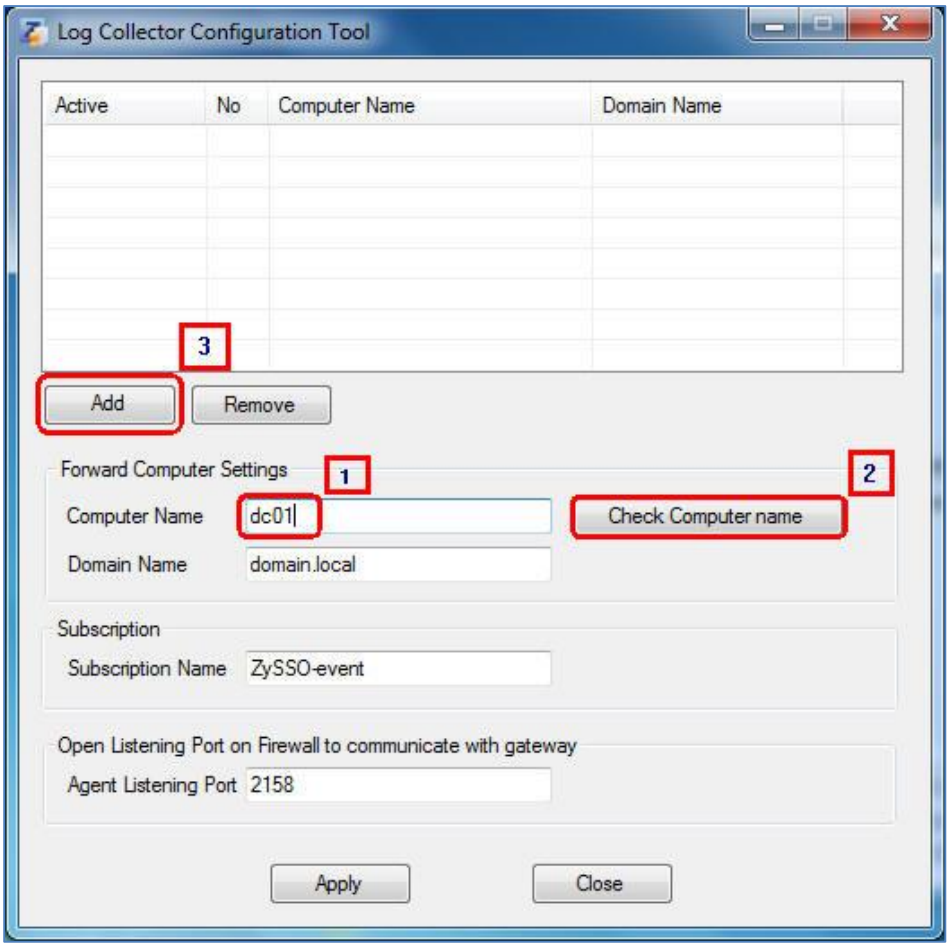

ConfigureLogsCollectorTool
Search ConfigureLogsCollectorTool
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Name
Date modified
Type
Size
Configuration.xml
2/10/2014 4:52 PM
XML Document
FirewallAPI.dll
9/17/2013 1:02 AM
Application extens...
LogCollectorConfigurationTool.exe
Application
LogCollectorConfigurationTool.exe.m
MANIFEST File
System.DirectoryServices.dll
Application extens...
Open
Run as administrator
Add to HFS
Troubleshoot compatibility
Share with
Pin to Taskbar
Pin to Start Menu
Restore previous versions
Send to
Cut
Copy
LogCollectorConfigurationTool.exe Date modified: 9/23/
Application
Size: 572 K
12:03 PM

3.2.2 Add Forward Computers

- [1] Enter the computer name of your domain controller
- [2] Click Check Computer name to make sure the computer name is right
- [3] Click Add to add it to table list

You can repeat these steps to add another domain controller, if there are multiple domain controllers in your Active Directory.

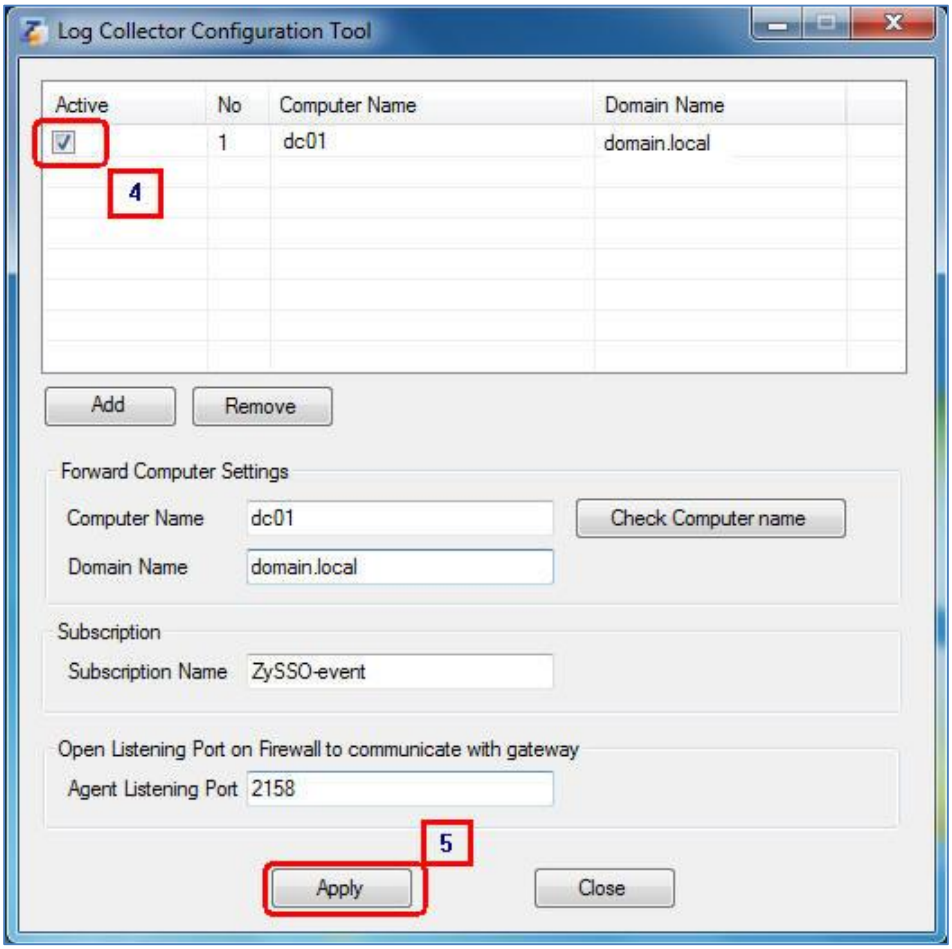
Note: Max. 4 domain controllers can be add to the table list



3.2.3 Active Forward Computers

- [4] Select the check the computers in the table to active log forward.
- [5] After all configuration done. Click Apply to set configuration.

Note: Max. 2 forward computers can be active in the table list



3.3 Setup Security Event Logs Forwarder **(On any one of Domain Controller)**

3.3.1 Prepare Configuration Tool of Event Logs Forwarder

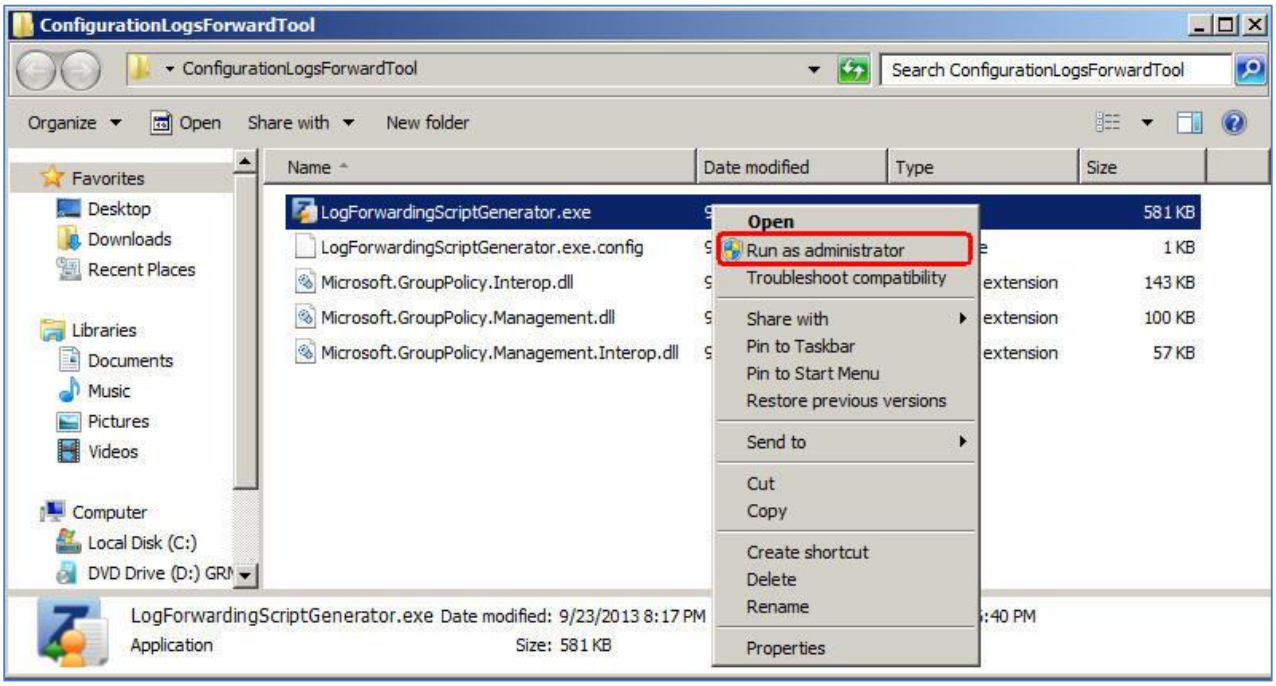
- Copy the ZIP package file to any one of your domain controller and extract to local file folder

3.3.2 Install .NET Framework v4.0.30319 or above

- Double-click /SSOAgent_Install_package/DotNetFX40/dotNetFx40_Full_x86_x64.exe to install

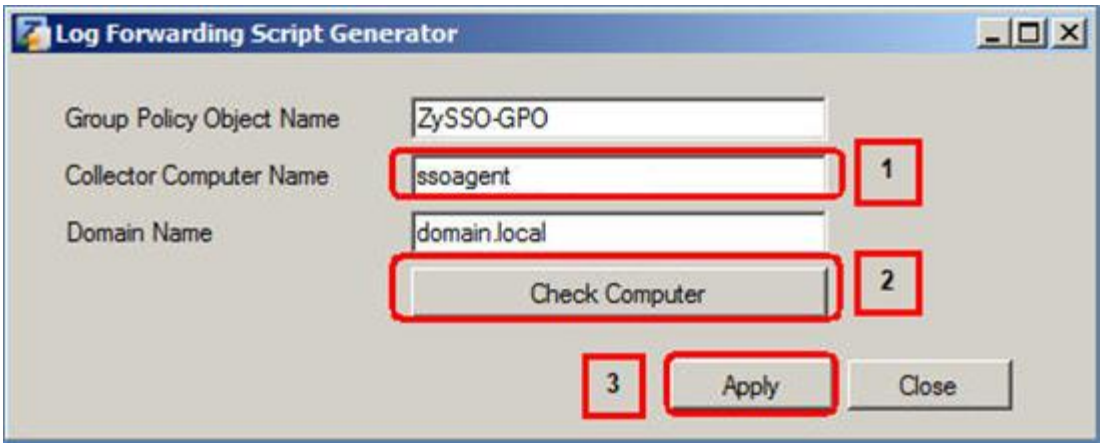
3.3.3 Open Event Logs Forwarder Configuration Tool

- Run \ConfigureLogsForwardTool\LogForwardingScriptGenerator.exe, as administrator.



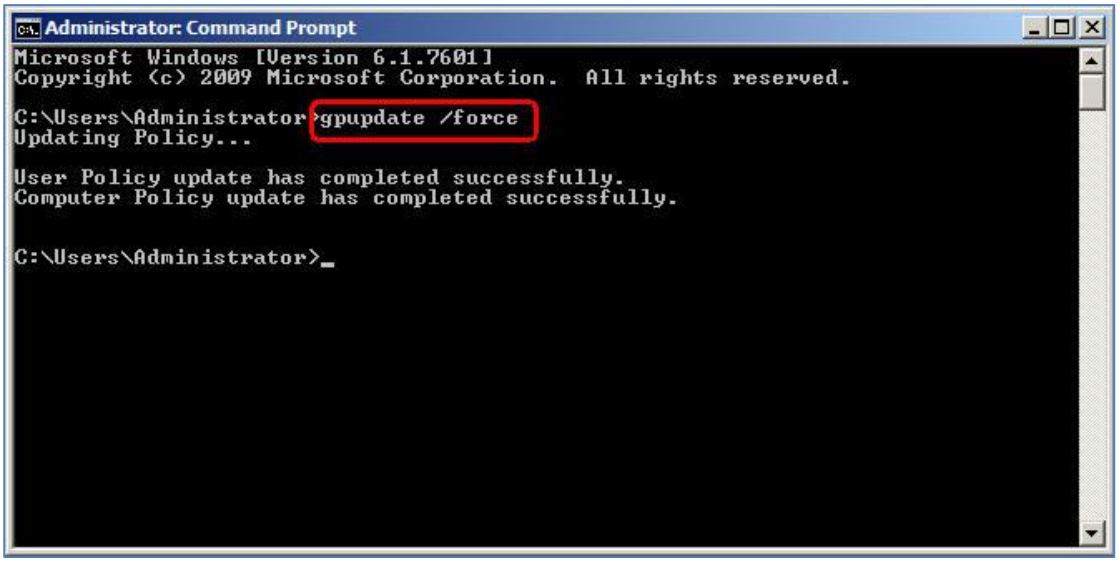
3.3.4 Configure logs forwarding

- [1] Enter the computer name which SSO Agent installed
- [2] Click Check Computer name to make sure the computer name is right
- [3] After all configuration done. Click Apply to set configuration.



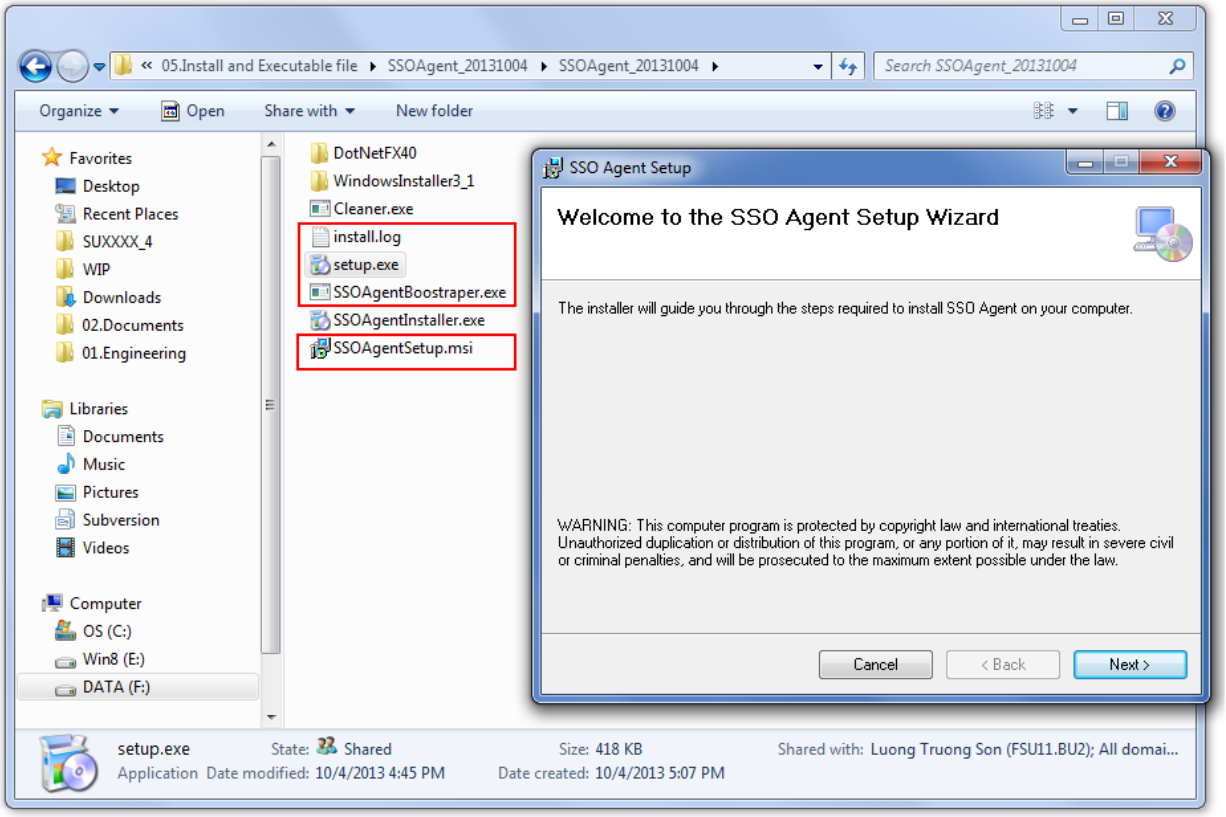
3.3.5 Force Group Policy Update

- Open Command prompt as administrator, run “gpupdate /force” .

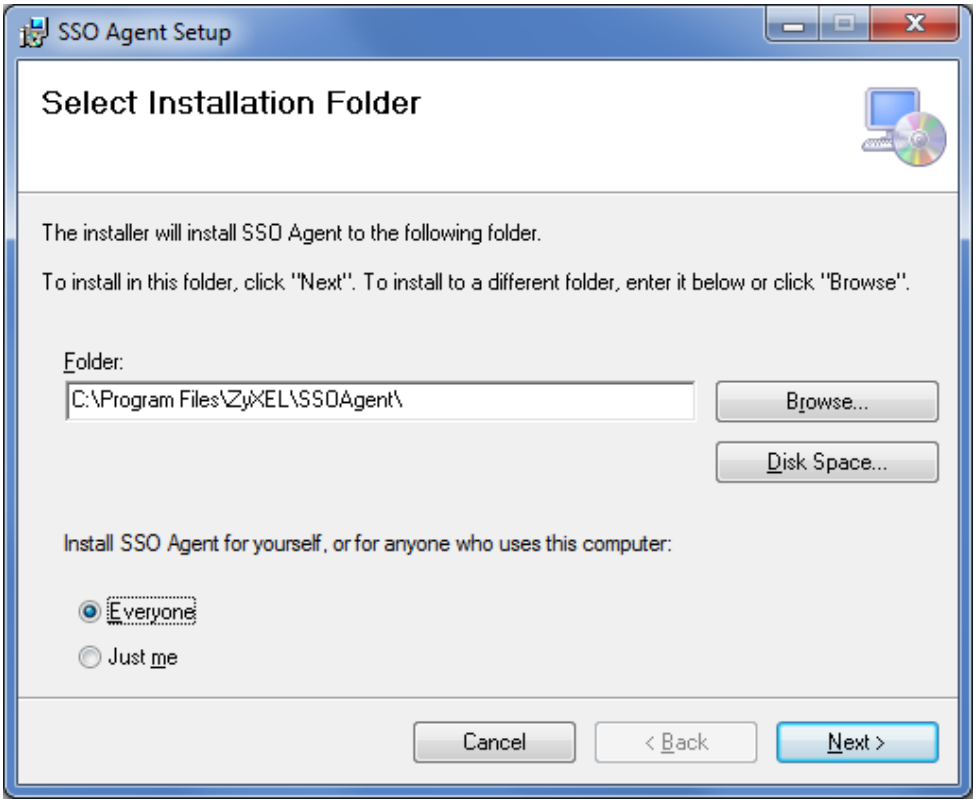


3.4 Install SSO Agent on domain workstation

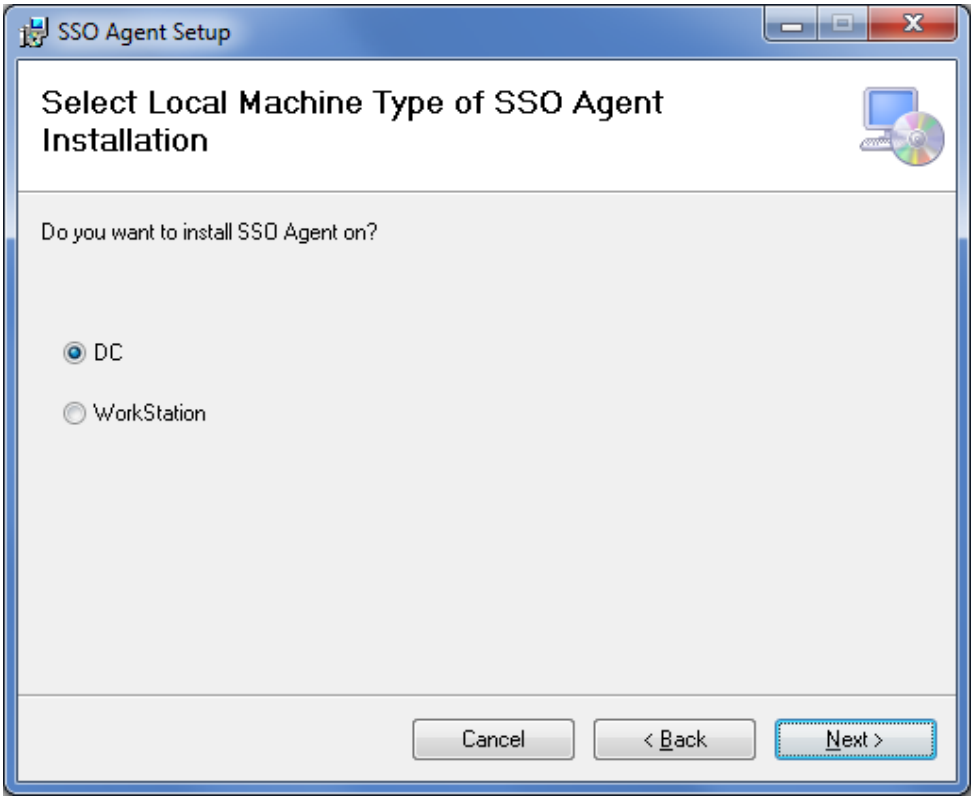
- On the domain workstation
- Double click the install file : **SSOAgentInstaller.exe**
- A windows for unzip package will be display for a while and after that Dialog Welcome of installer will be displayed immediately.
- When run installer, there are some files for install are displayed in folder of package SSO Agent. These files will be removed when finish install.



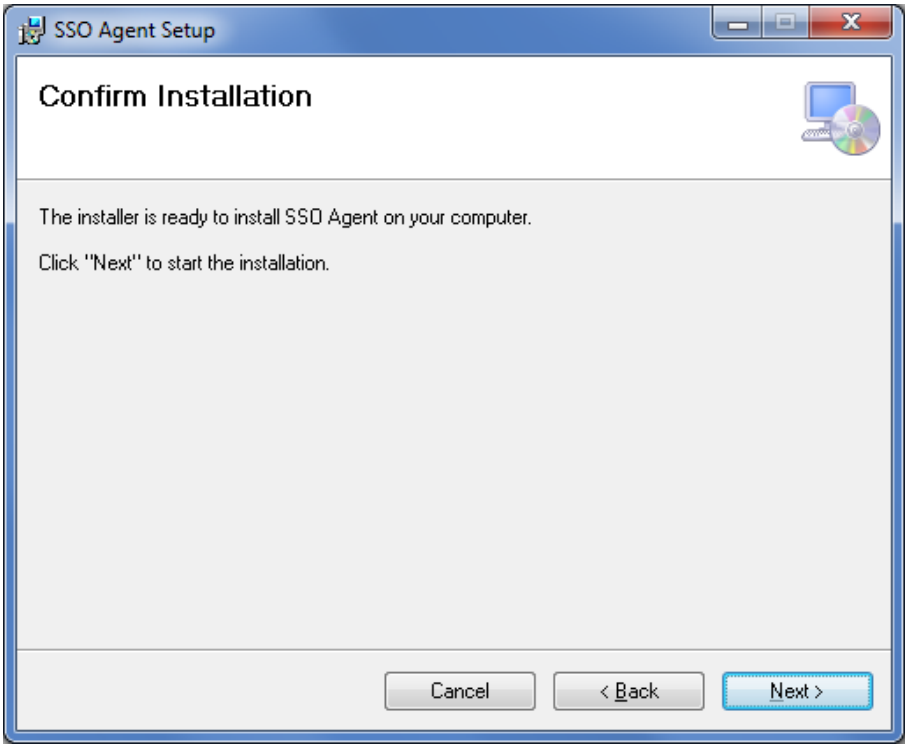
- Click [Next], Dialog Select folder setup will be displayed:
- Select folder or setup with default location, then click Next



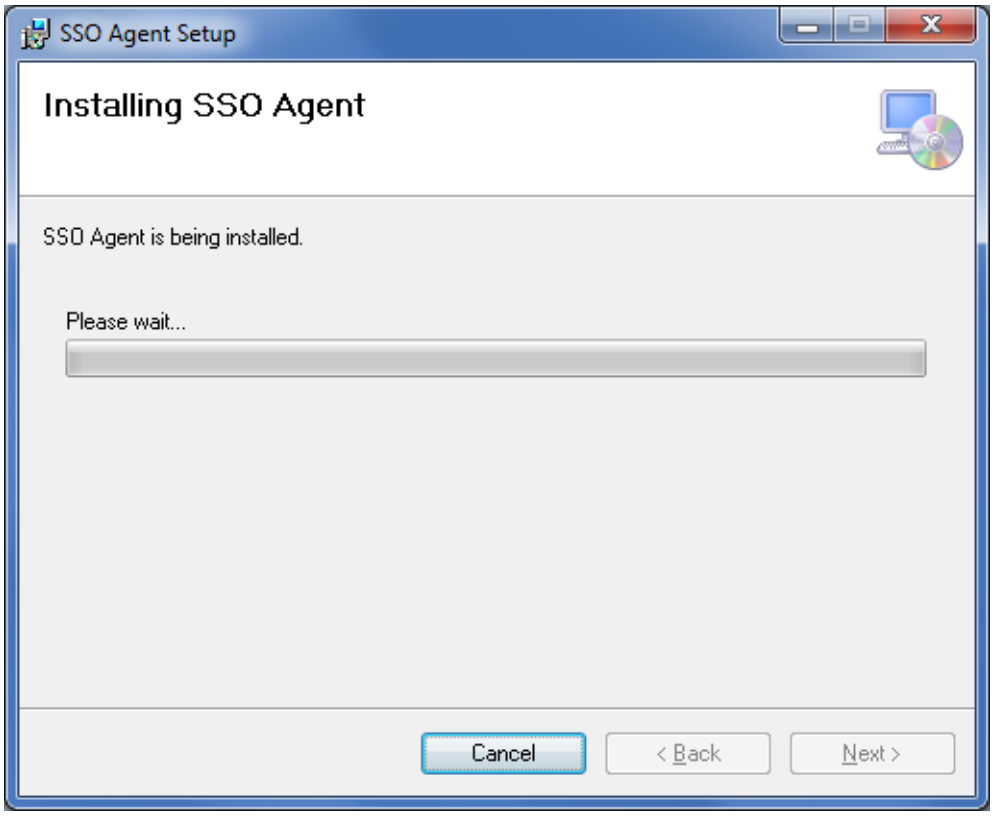
- Select install SSO Agent on DC in this scenario, then click Next.



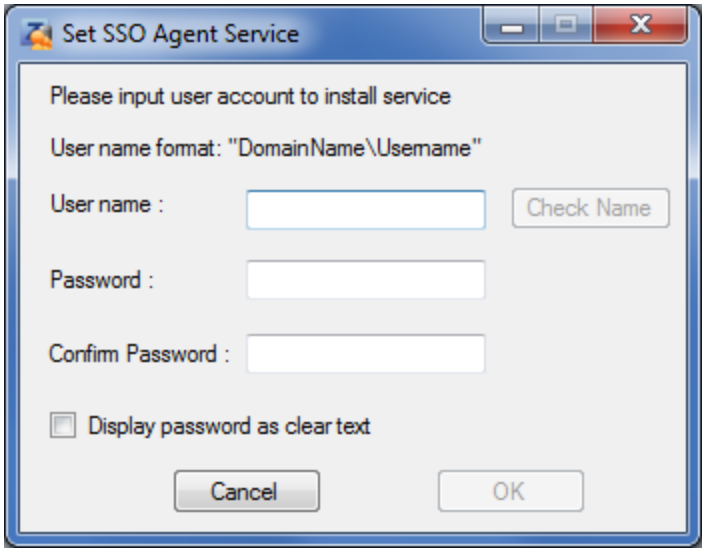
- Then click Next to confirm start to install.



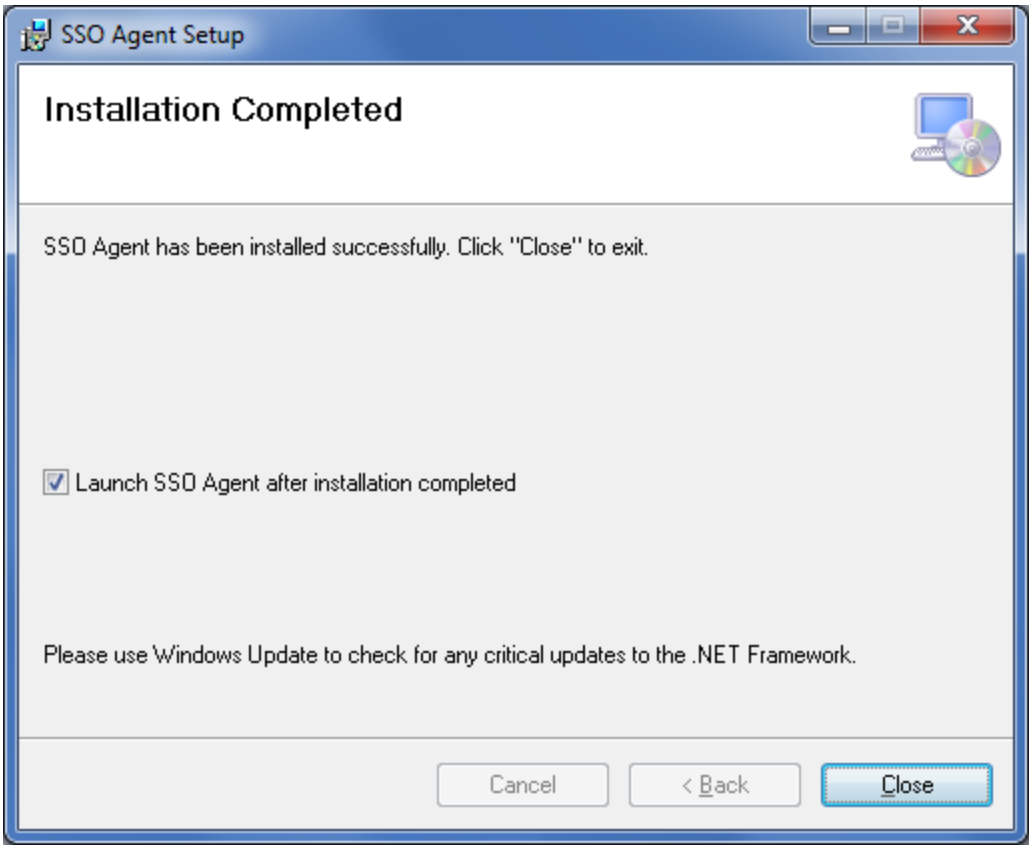
- Click [Next], and wait process setup running.



- After a while, a “Set SSO Agent Service” dialog window will pop-up.
  Please enter the Domain\Username and password of the domain account that created in step 3.1.3.
  Then click OK to continue.



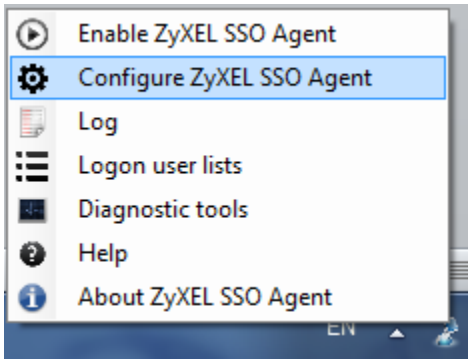
- When installation finish, Dialog notify setup will be displayed with option choose default run application immediately.



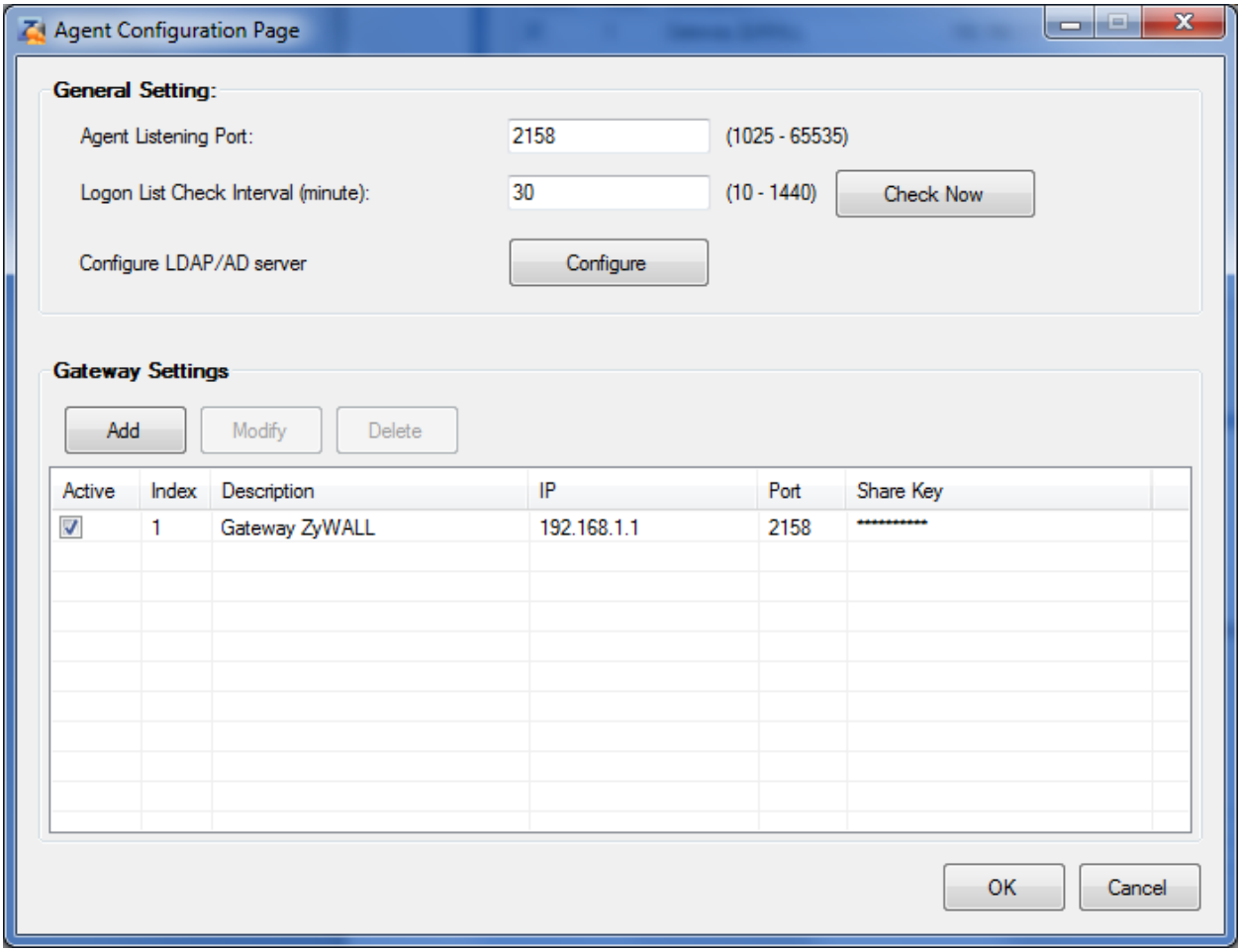
- Click Close to finish Install SSO Agent. After install application successfully, Tray Icon of application will be pin to task bar.

4 Configuration SSO Agent

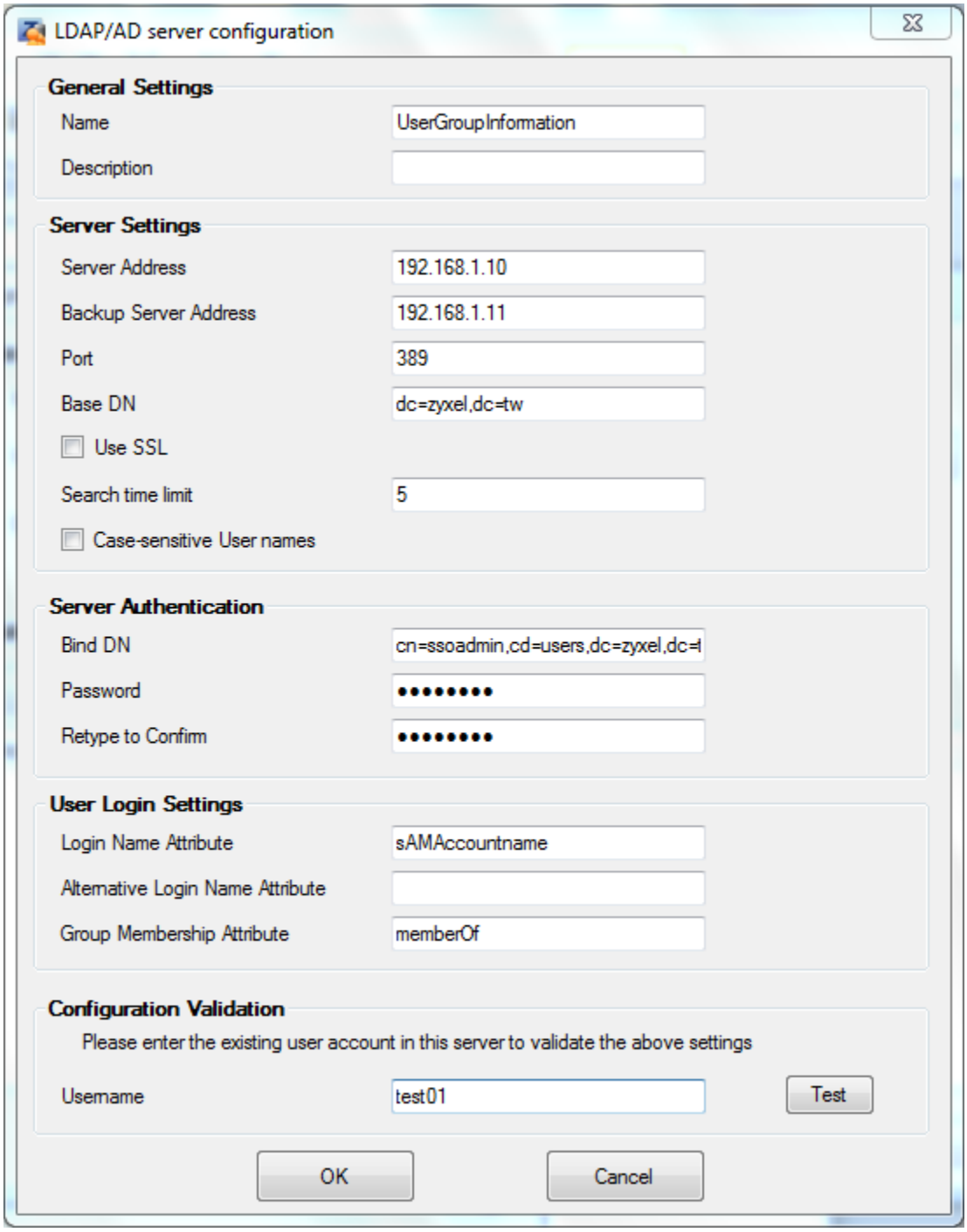
- Click on “Configure ZyXEL SSO Agent”



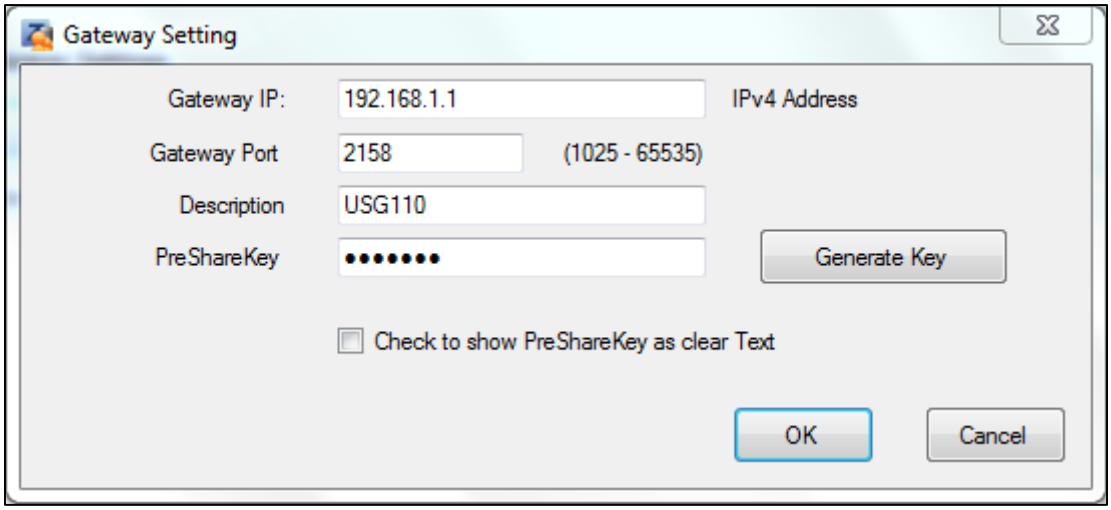
- You will see the “Agent Configuration Page” window



- Under General Setting, click “Configure LDAP/AD server” to configure the LDAP query to get group information of user from Active Directory.



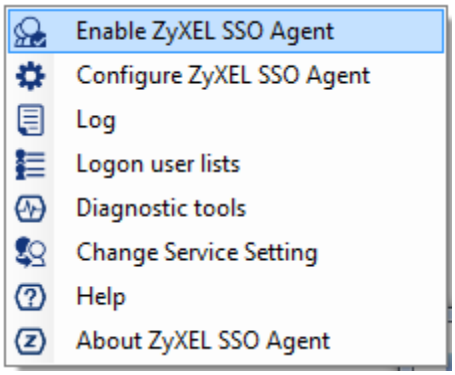
- Under Gateway Settings, click “Add” to configure the IP address of your USG and the Pre-Share Key.



- Go back to “Agent Configuration Page” window, please remember to active the gateway entry. Then click OK to save configuration.

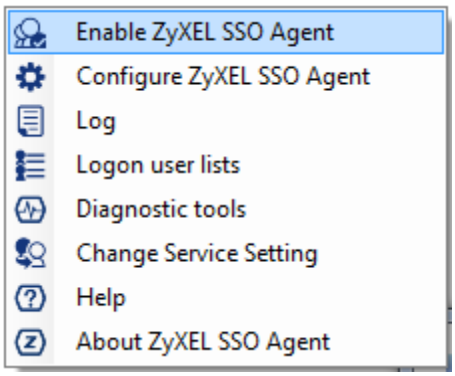
5 Enable/Disable Service

- Right click on icon of SSO Agent Application, one popup menu will appear



5.1 Enable Service

- To enable Service, user clicks on “Enable ZyXEL SSO Agent”



- When Service is started successfully, one popup will appear



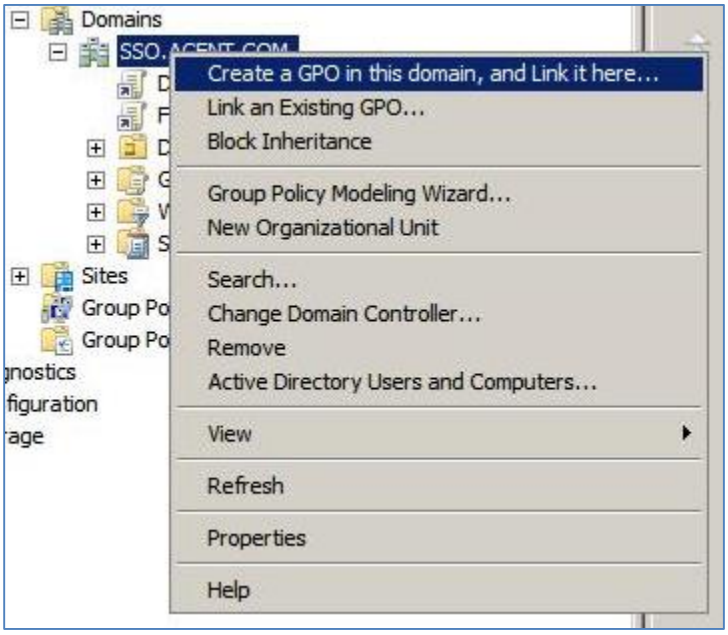
6 Setup Active Directory Group Policy For Domain Clients

Notice: User on SSO Agent Computer must have local Administrator permission

6.1 Setup for Query Client

6.1.1 Create GPO for deploy firewall rules to all domain clients

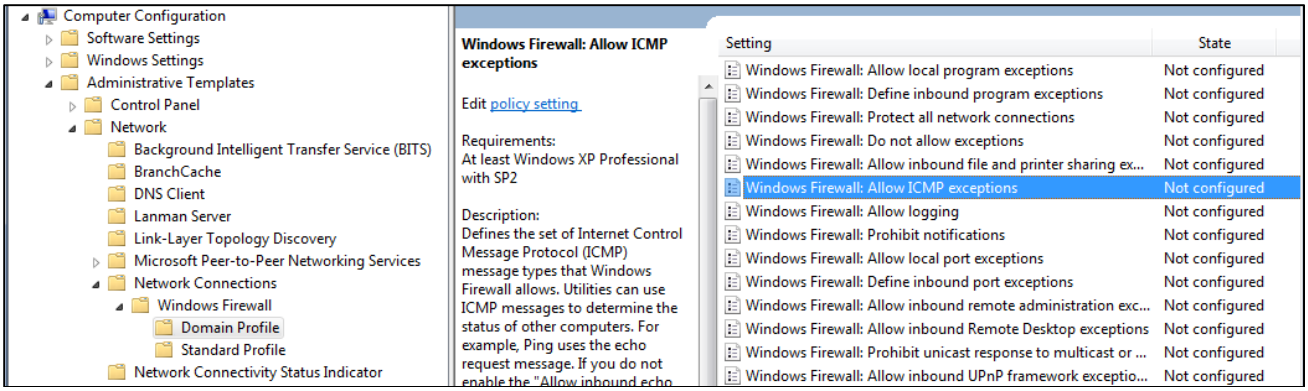
- Create GPO for Domain name (sample: domain name is “sso.agent.com”, right click on “SSO.AGENT.COM” and click to “Create a GPO in this domain and Link it here”



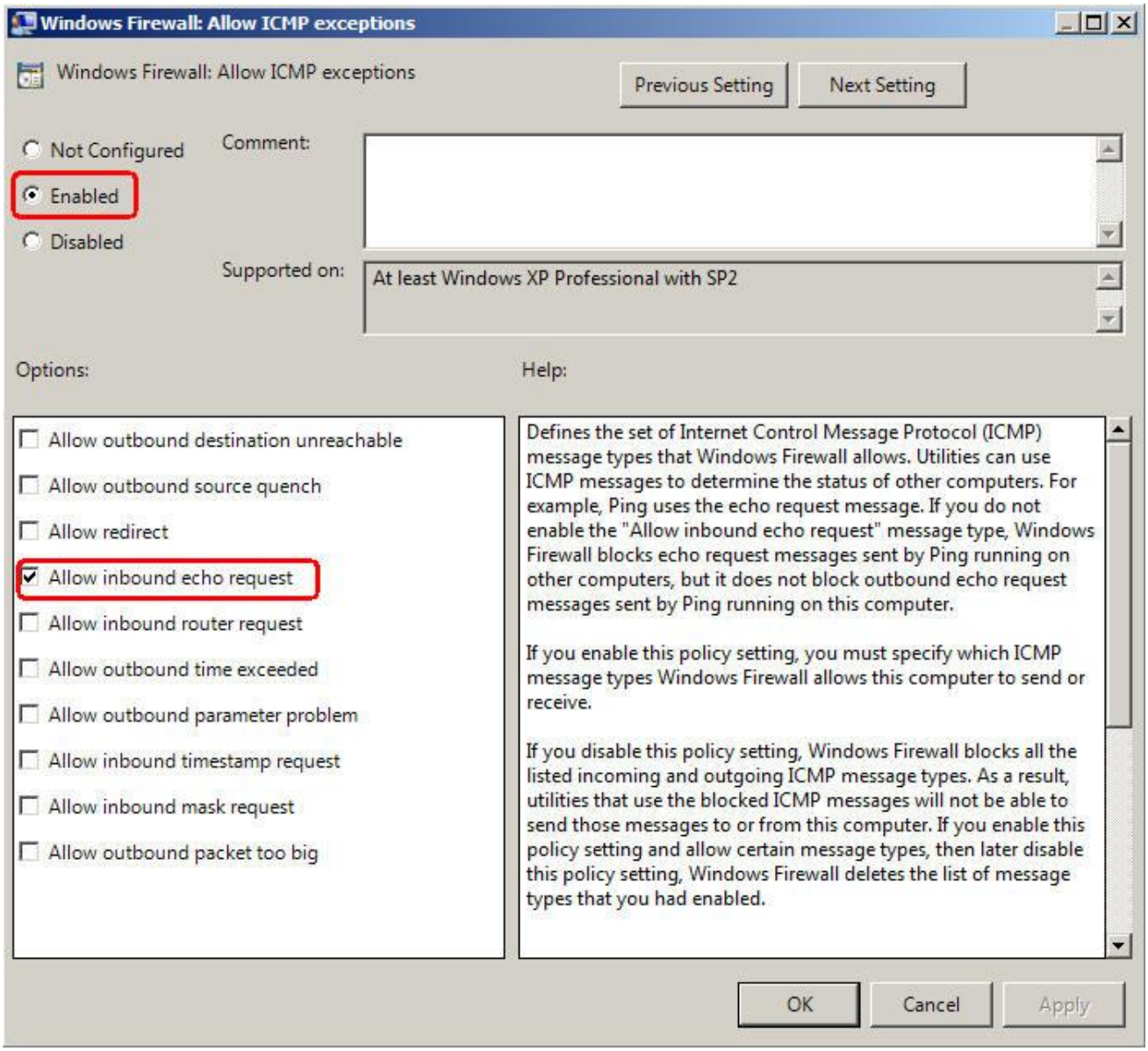
- Enter name of the GPO, for example “Deploy Firewall Rules”

6.1.2 Create firewall rules in GPO

- Right click on the GPO rule created in step 7.1.1, then click Edit
  - Configure firewall rule for ICMP echo
    - On the left side tree panel, select Computer Configuration => Polices => Administrative Templates => Network => Network Connections => Windows Firewall => Domain Profile
    - Double click on “Windows Firewall: Allow ICMP exceptions”



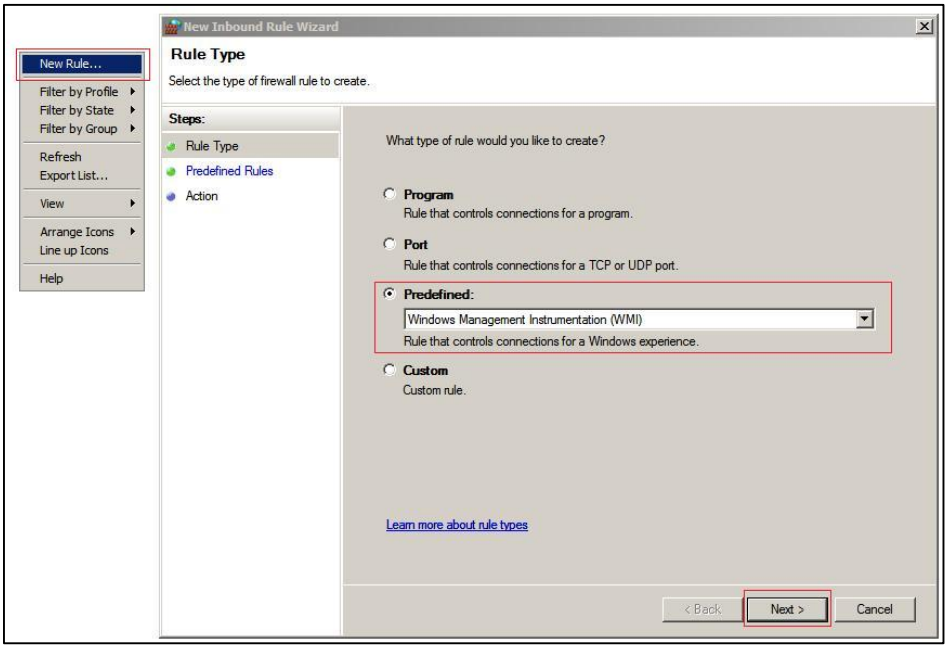
- Click “Enable” and then check “Allow inbound echo request” option, finally click button [OK]



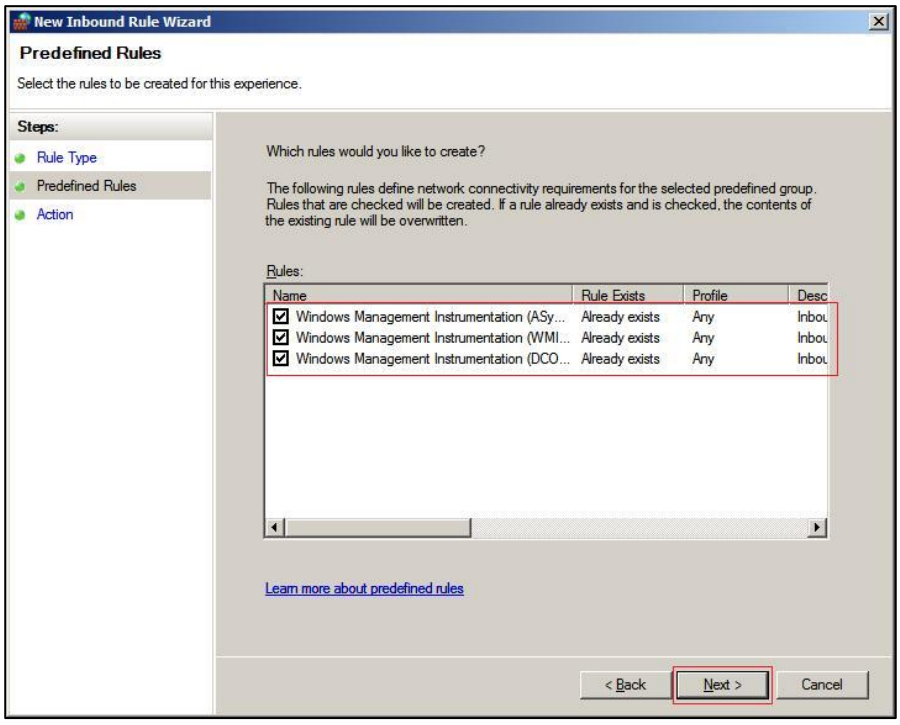
- Configure firewall rule for remote WMI
  - Computer Configuration => Policies => Windows Settings => Security Settings => Windows Firewall with advanced Security
  - Right click on Inbound Rules, then click New Rule…



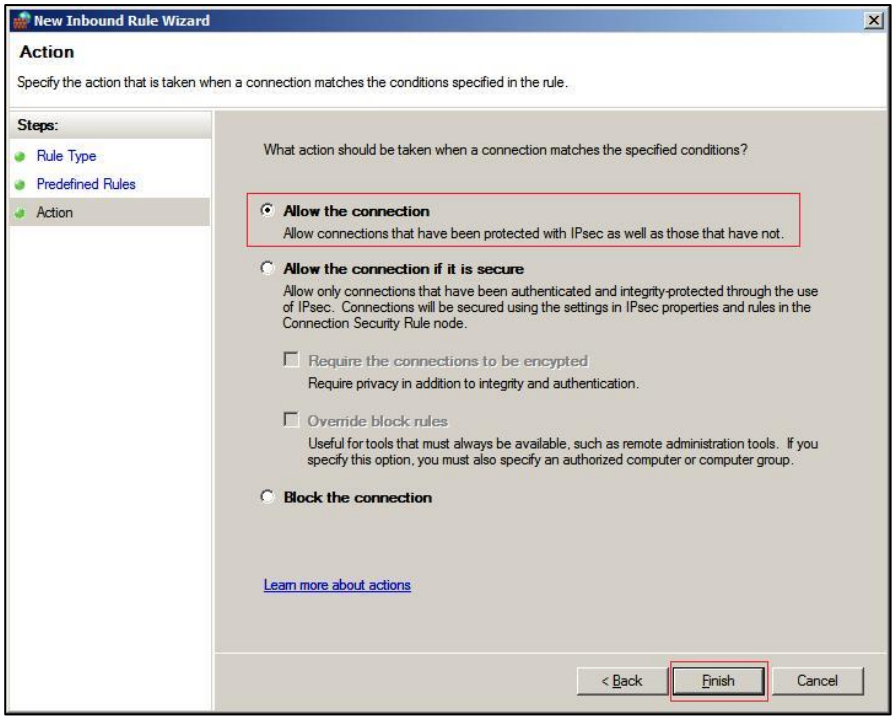
  - Select “Predefined” rule type, and select “Windows Management Instrumentation (WMI)” from the list. Click Next.



- Select all rule, then Next.



- Select “Allow the connection”, then Finish.


New Inbound Rule Wizard
Action
Specify the action that is taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Predefined Rules
Action
What action should be taken when a connection matches the specified conditions?
Allow the connection
Allow connections that have been protected with IPsec as well as those that have not.
Allow the connection if it is secure
Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Require the connections to be encypted
Require privacy in addition to integrity and authentication.
Override block rules
Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.
Block the connection
Learn more about actions
< Back
Finish
Cancel

7 Setup USG SSO authentication

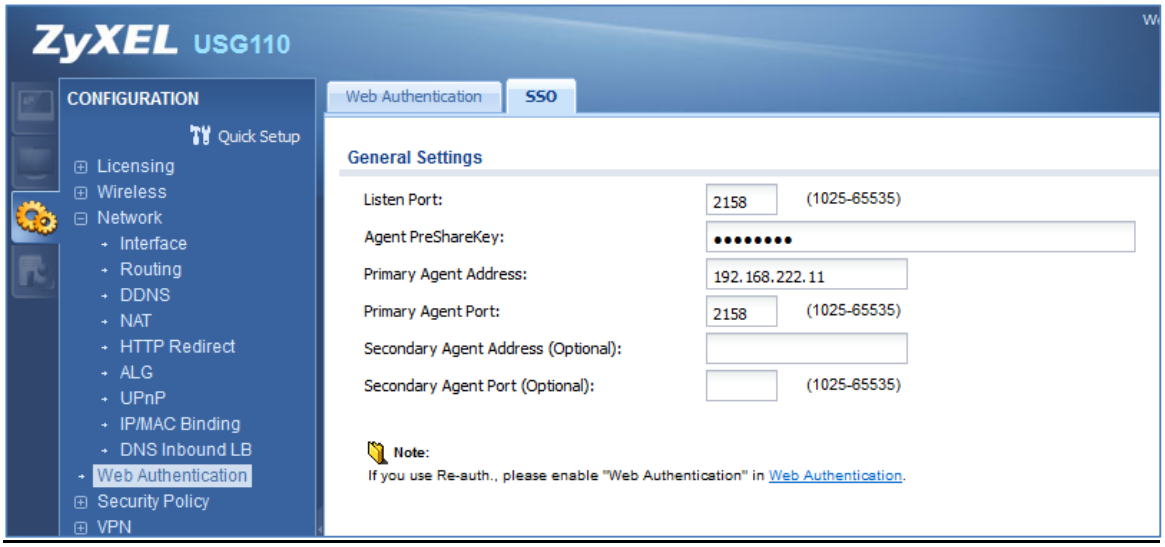
7.1 Configure SSO

- Go to CONFIGURATION > Web Authentication > SSO

- Agent PreShareKey: Enter Agent PreShareKey (same as configured on SSO Agent)

- Primary Agent Address: Enter IP address of the SSO Agent computer

- Primary Agent Port: 2158 (default is 2158, be same as configured on SSO Agent)



7.2 Configure Authentication Policy

- Go to CONFIGURATION > Web Authentication

- Add authentication policy,

Source address: Select a source address or address group for whom this policy applies.

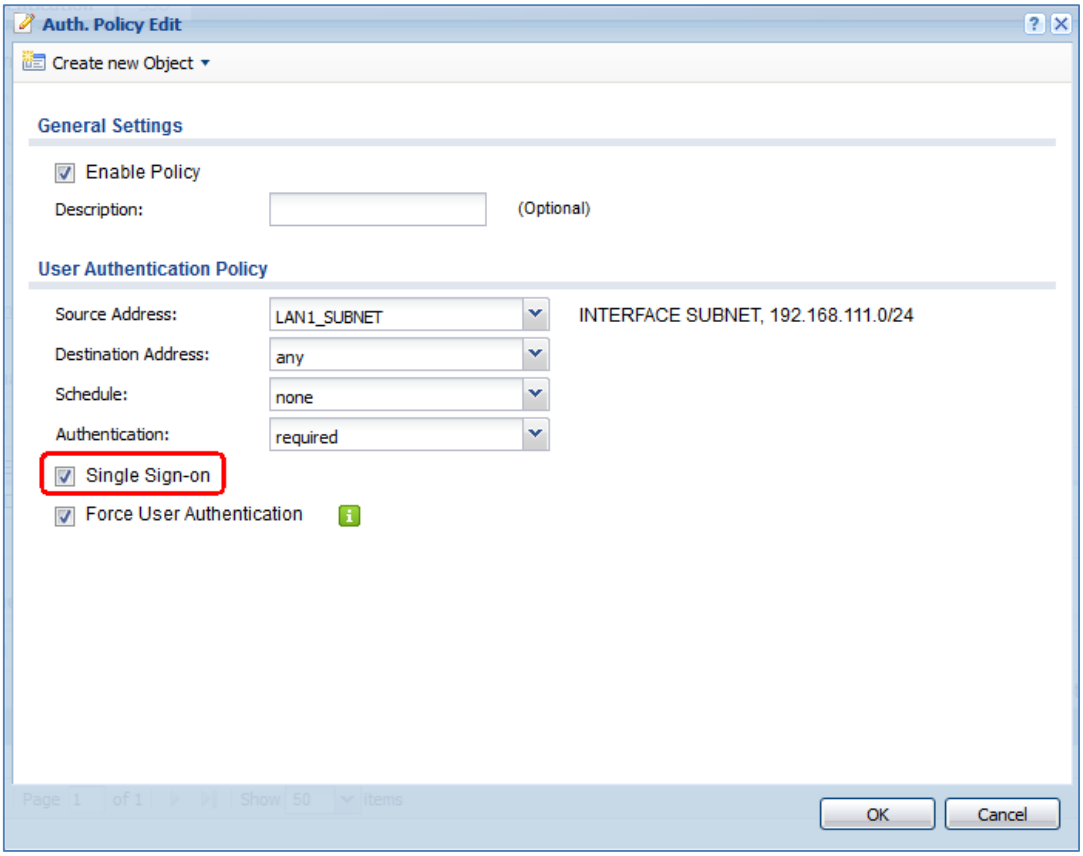
Destination address: Select a destination address or address group for whom this policy applies.

Authentication: Select “required”

Single Sign-on: Select to authenticated by SSO

Force User Authentication: Select to authenticated by redirect to login page

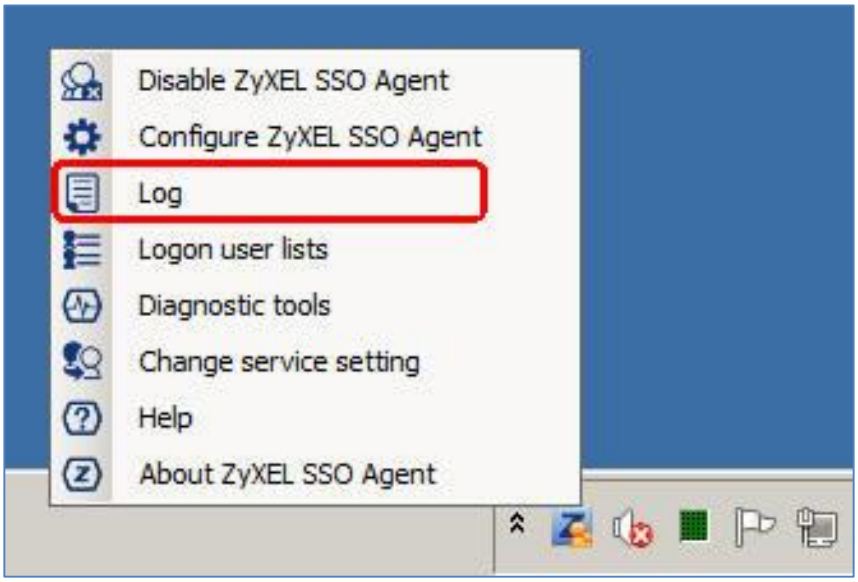
Note: If you enable this with SSO enabled, then any client that hasn't Login Active Directory domain, will be redirect to login page.



8 Single Sign-On test

8.1 Open SSO Agent Log

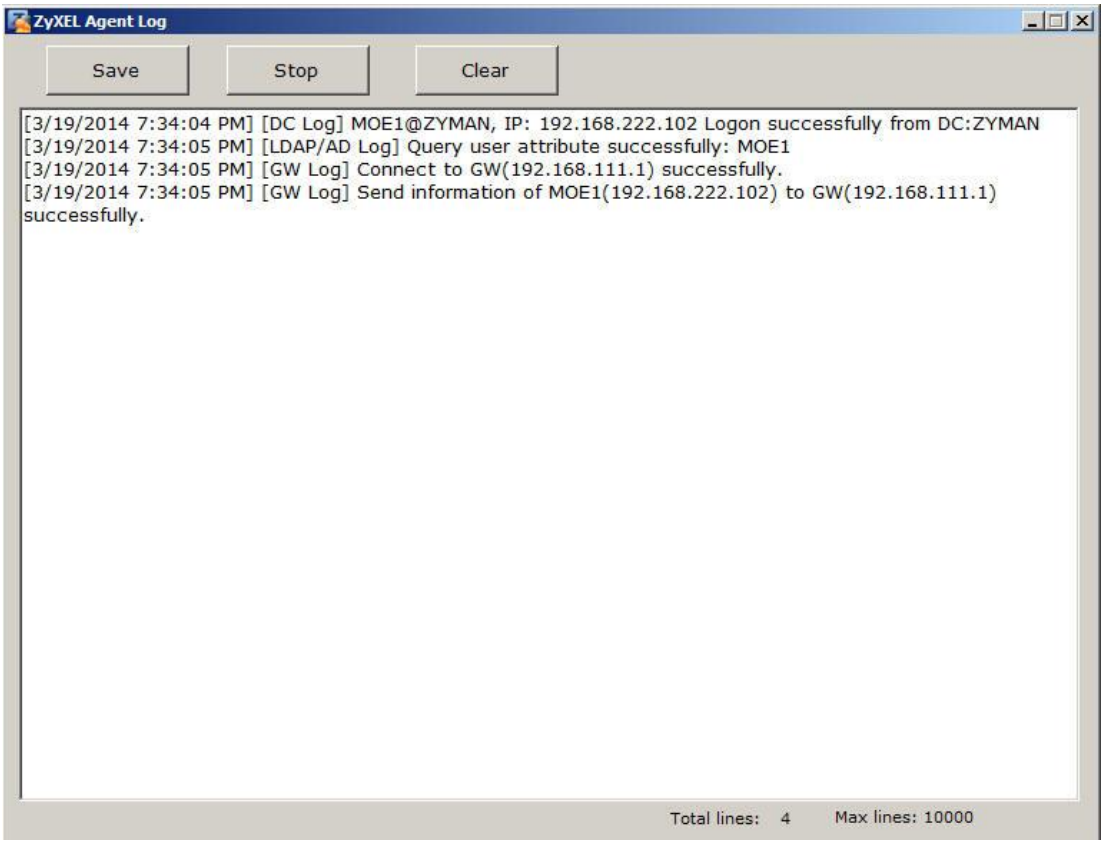
- Right click on icon on system tray and select "Log"


Disable ZyXEL SSO Agent
Configure ZyXEL SSO Agent
Log
Logon user lists
Diagnostic tools
Change service setting
Help
About ZyXEL SSO Agent

8.2 Login Domain

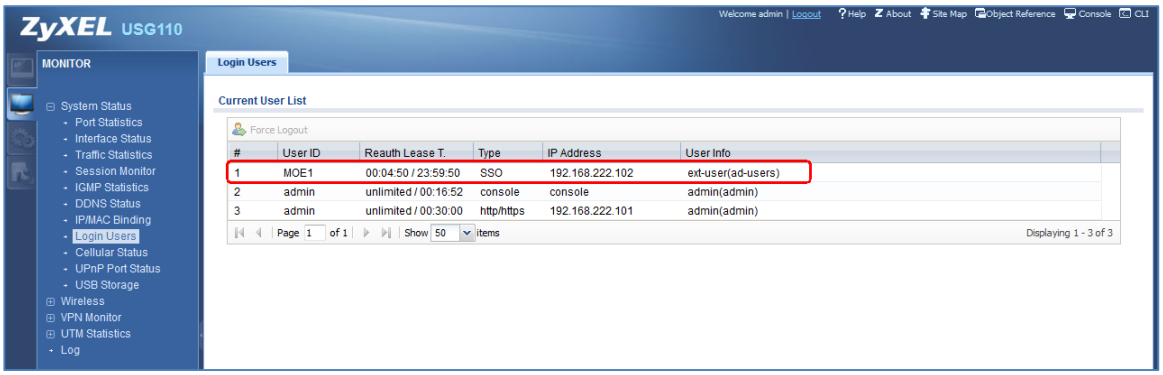
- On clients laptop, login with domain account

- Check SSO Agent log, it show user login successful and Send information to GW (USG) successful



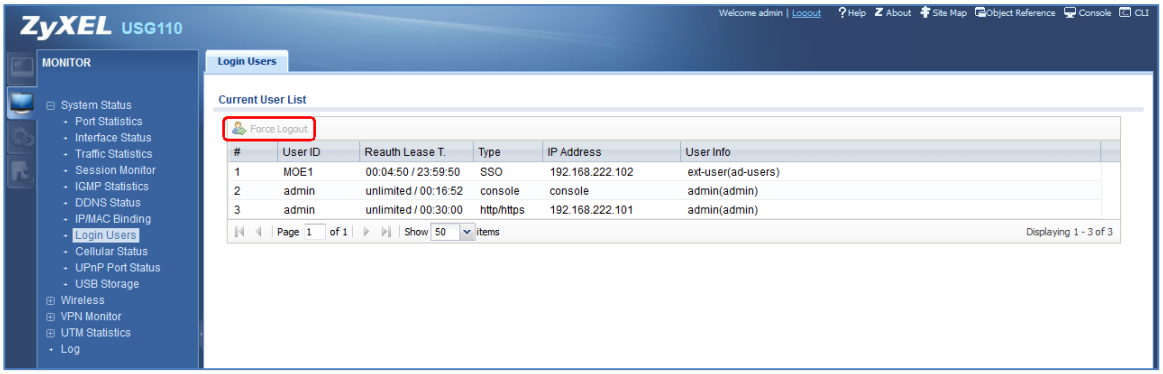
- Open browser or application on client laptop (to trigger traffic to pass USG)

- Check login users information on USG



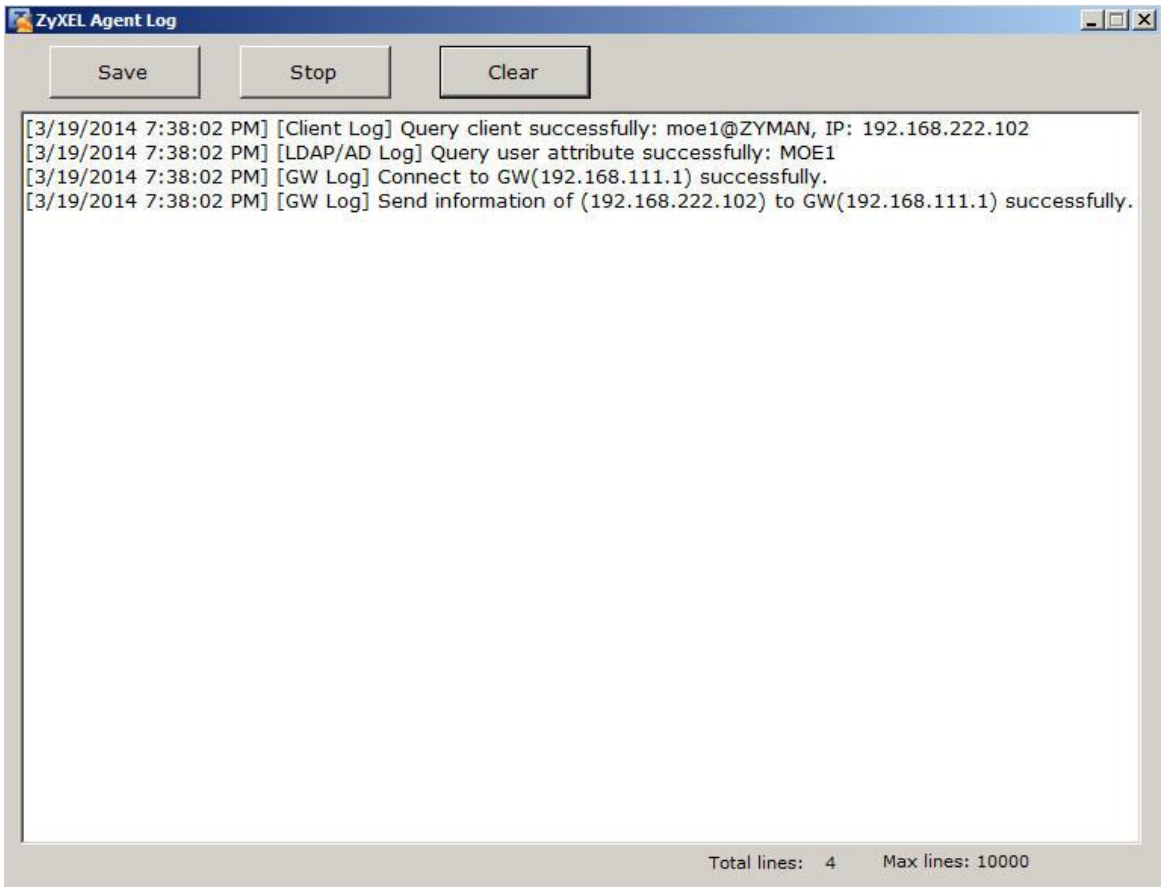
8.3 Check SSO query client

- Force logout user via USG GUI



- Open browser or application on client laptop (to trigger traffic to pass USG)

- Check SSO Agent log, it show query client successful and Send information to GW (USG) successful


ZyXEL Agent Log
Save
Stop
Clear
[3/19/2014 7:38:02 PM] [Client Log] Query client successfully: moe1@ZYMAN, IP: 192.168.222.102
[3/19/2014 7:38:02 PM] [LDAP/AD Log] Query user attribute successfully: MOE1
[3/19/2014 7:38:02 PM] [GW Log] Connect to GW(192.168.111.1) successfully.
[3/19/2014 7:38:02 PM] [GW Log] Send information of (192.168.222.102) to GW(192.168.111.1) successfully.
Total lines: 4
Max lines: 10000