ShutdownAgent 2012

User Manual

Doc. Version 02.07

Date: 01/17/2022

About this manual

This manual contains information on installation and operation of the ShutdownAgent 2012 software.

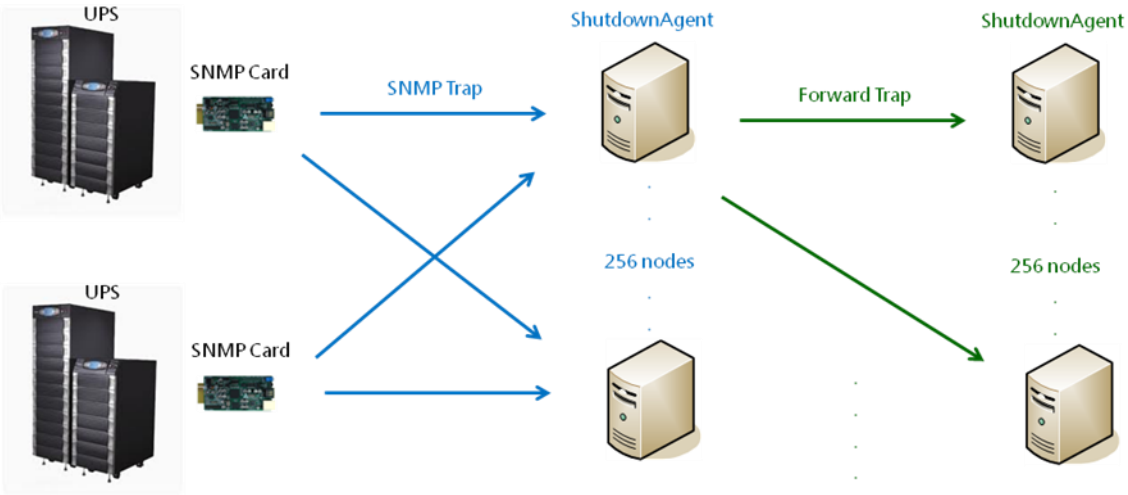
Save this Manual

This manual contains instructions and warnings that should be followed during the installation, operation and storage of this product. Failure to heed these instructions and warnings will void the product warranty.

Contents

1. Overview

The ShutdownAgent 2012 is a software that can protect the operating system which is supplied power by an UPS during input power fail. Through a Web Browser, you can easily obtain current UPS event, shutdown strategy and countdown to shutdown information.



1.1 Features

1. Support SNMPv1, v3 trap.
2. Support SNMPv1, v3 server access for monitoring ShutdownAgent status and configure shutdown parameters.
3. Provide web interface through HTTP and HTTPS.
4. Provide the batch configuration to deploy settings at a finger click.
5. Forward SNMP trap to extend protecting up to 255 servers.
6. Support up to 32 input trap sources for redundant (logical OR) and parallel (logical AND) application.
7. Provide console configuration for basic system parameters setup.
8. Support Windows 32/64 bits setup programs.

1.2 OS Support

Windows 7, 8, 10
Windows Server 2008, 2012, 2016, 2019
Windows 2008/2012 Server Core, Hyper-V 2008/2012
Redhat Linux Enterprise 8.3

Orcale Linux 7.1
Linux OpenSUSE 11.4
Linux ubuntu 10.04, 12.04.5, 16.04, 20.04
Linux Fedora 3.1.9
CentOS 5.8, 6.5
VMWare ESXi 4.1, 5, 5.1, 5.5, 6, 7 (with essential license after version 5)
Citrix XenServer 6.0.0
Linux KVM
IBM AIX 7.1

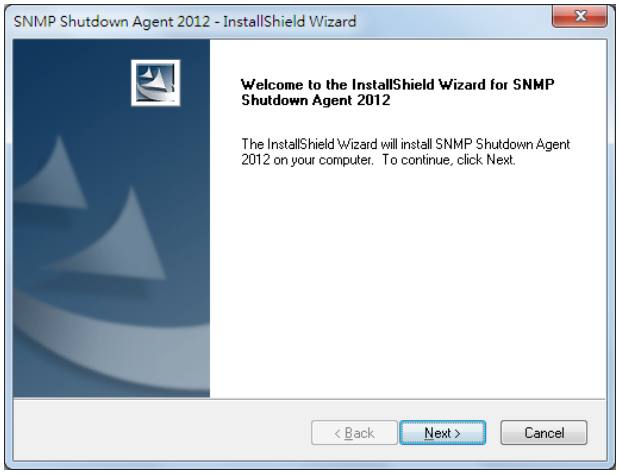
2. Installation/ Uninstallation

2.1 For Windows System

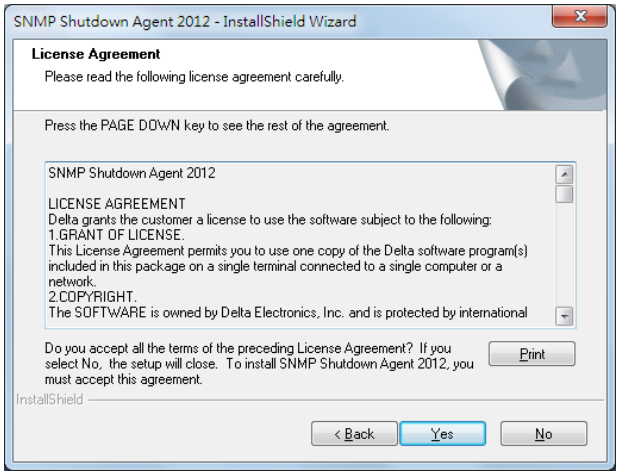
There are 2 of setup programs: ShutdownAgent-2012-Setup(win32).exe and ShutdownAgent-2012-Setup(x64).exe. One is for 32 bit Windows operating system and the other one is designed for 64 bit Windows environment. Please login the Windows account with local administrator privilege before install the software.

2.1.1 Installation Process

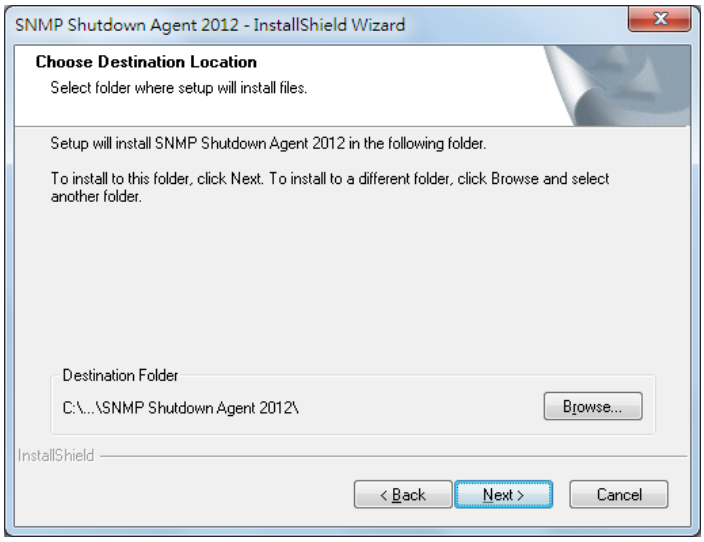
1. Execute the ShutdownAgent-2012-Setup(xxx).exe to run the setup program.
2. The welcome page will first display, press the "Next" button to continue the installation or press the "Cancel" to stop the installation.



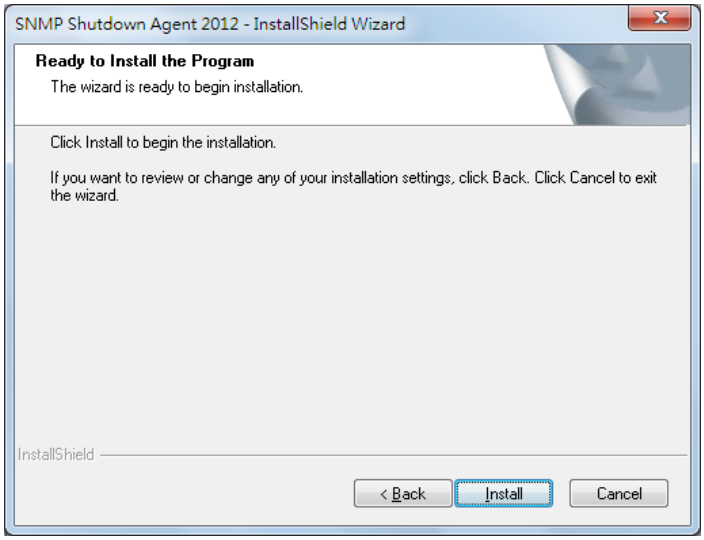
3. Then continue to show the license agreement page. Press "Yes" button to continue the installation and "No" to stop the installation.



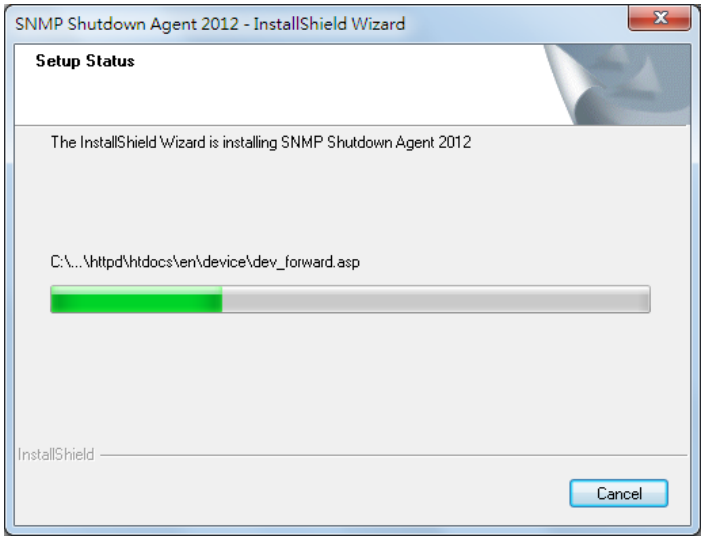
4. At this stage you can change the destination location by pressing the "Browse" button or just press the "Next" to install the software in the default path.



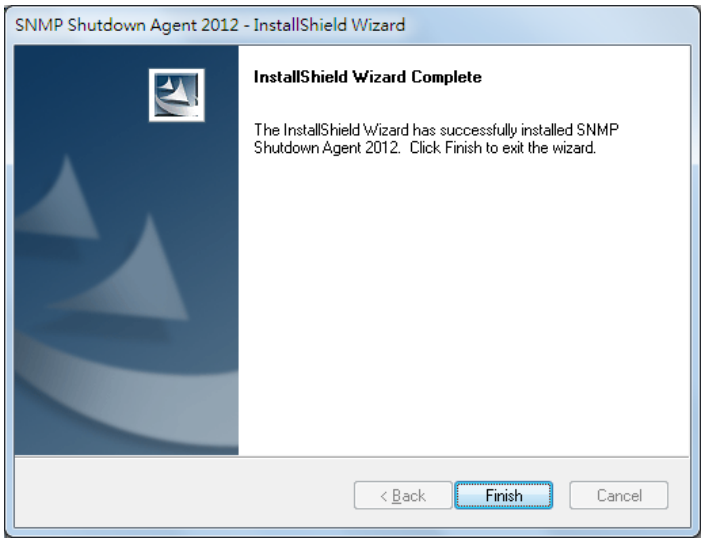
5. Now the setup program is ready for your confirmation to start copying the related program files. Press the "Install" button to start copying the software to the destination location in your hard drive.



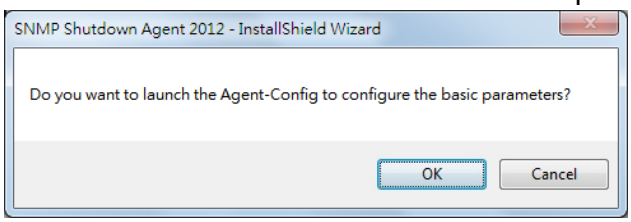
6. Now the setup program is copying the files and shows the progress.



7. After complete the installation, press the "Finish" button to exit the installation process.



8. After finishing the installation, the ShutdownAgent will start the service program automatically and add an icon to indicate its status to the desktop tool bar. Meanwhile, a dialog box pops up to ask for launching the Agent-Config application to do the basic configuration. If you are not operate a Windows server core operating system then you can ignore this ask. Just press "No" to finish the installation. Press "Yes" to launch the Agent-Config in the shell mode. Please refer to the chapter 3 for the detail of Agent-Cofnfig.



The **ShutdownAgent** software is comprised of two modules:

A **Service** module (**Shutdown-Agent Service: Agent-Service.exe**), which runs in the background as a Service and listen for the SNMP trap from the source IP addresses.

A **Status** module (**Agent-Status.exe**), which enables you to control and configure the software through drop down menus and dialog boxes. It also allows you to launch the web browser and login automatically to monitor, configure and control the software.

After finishing the installation, the setup program will create a **SNMP ShutdownAgent** association with the following shortcuts:

Console Configure: To launch the Agent-Config.exe for you to quickly configure the basic communication parameters.

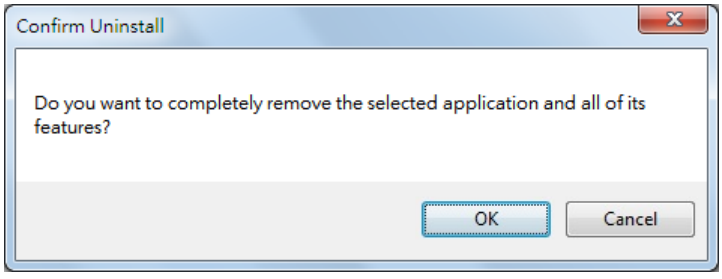
Uninstall: To remove the **SNMP ShutdownAgent 2012** from your hard disk, the configuration data will still be kept in the installed directory.

User Manual: The user manual in pdf format.

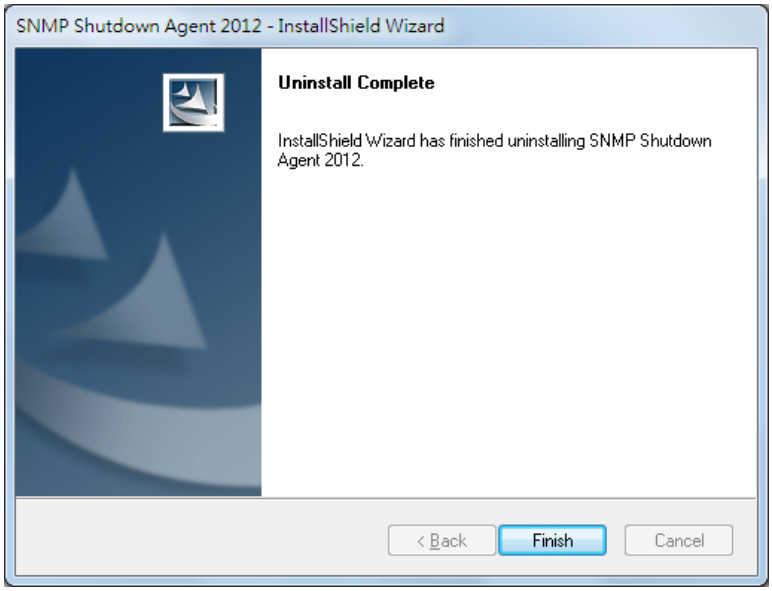
Web Monitor: The major user interface of **ShutdownAgent**, used to monitor and configure the software.

2.1.2 Uninstallation Process

1. Select the Uninstall from the **SNMP ShutdownAgent** program folder to start the un-installation process. Or you can start the **SNMP ShutdownAgent** uninstallation process from the Add/Remove Program of the Control Panel.
2. Press the "OK" button to confirm removing all of the application from the hard drive or "Cancel" to cancel the un-installation process.



3. Press the "Finish" button to complete the un-installation process.



2.2 For Linux System

2.2.1 Installation Process

1. Please login to the Linux system and change to the root account:
su root
2. Copy the sa2012-linux.tar.gz to the /tmp directory:
cp sa2012-linux.tar.gz /tmp
3. Change your working directory to /tmp:
cd /tmp
4. uncompress the sa2012-linux.tar.gz:
gunzip sa2012-linux.tar.gz
5. extract the sa2012-linux.tar:
tar xvf sa2012-linux.tar
6. Run the install script:
./install

```
+---------------------------------------------+
|  SNMP ShutdownAgent 2012 0.0.1 for Linux    |
|  Copyright (c) 2011 Delta Electronics, Inc. |
|  All Rights Reserved.                       |
+---------------------------------------------+

Do you want to install the ShutdownAgent? [y|n]
```

7. Press ‘y’ to proceed the installation process:

```
+---------------------------------------------+
|  SNMP ShutdownAgent 2012 0.0.1 for Linux    |
|  Copyright (c) 2011 Delta Electronics, Inc. |
|  All Rights Reserved.                       |
+---------------------------------------------+

The destination directory is /usr/local/upsagent.

Copying files ..............
Install service link.

shutdownagent             0:off  1:off  2:off  3:on   4:off  5:on   6:off

Starting ShutdownAgent(upsagentd) ... done

Do you want to configure the ShutdownAgent right now? [y|n]
```

8. Now the ShutdownAgent has been installed in the following directory /usr/local/upsagent/ and the service program starts up automatically.
Press ‘y’ to launch the /usr/local/upsagent/configure program to configure the basic networking parameters for ShutdownAgent or press ‘n’ to finish the install process.
Please see chapter 3 for more information if you want to configure the basic networking parameters.

2.2.2 Uninstallation Process

1. Please login to the Linux system and change to the root account:
su root
2. Change your working directory to /usr/local/upsagent:
cd /usr/local/upsagent
3. Run the uninstall script to remove ShutdownAgent:
./uninstall
4. Press ‘y’ to start the uninstallation process.

2.3 For IBM AIX System

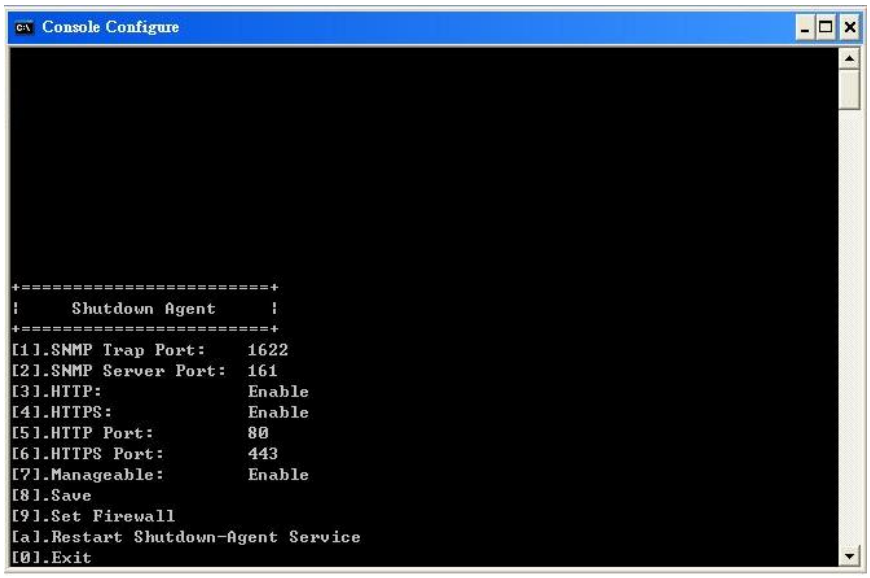
Both of the installation and uninstallation are the same with Linux system, please refer to the section 2.2.

3. Console Configuration

The configuration program is design to do the basic configuration for the ShutdownAgent in the shell mode. The software can be launched at the end of the installation process or you can go to the installed directory to launch it manually.

For Windows it locates in "C:\Program Files\SNMP Shutdown Agent 2012\Agent-Config.exe"

For Linux it is installed in "/usr/local/upsagent/configure"



3.1 Console Menu

No.	Function	Description	Default
1.	SNMP Trap Port	The UDP port to listen for the SNMP trap	162
2.	SNMP Server Port	The UDP port for replying get/set commands	161
3.	HTTP	Enable or disable the HTTP protocol	Enable
4.	HTTPS	Enable or disable the HTTPS protocol	Enable
5.	HTTP Port	The TCP port for HTTP	80
6.	HTTPS Port	The TCP port for HTTPS	443
7.	Manageable	Allow the management software to manage ShutdownAgent	Enable
8.	Save	Save the configured parameters to agent.ini	
9.	Set Firewall	Insert or remove the firewall rule for the	

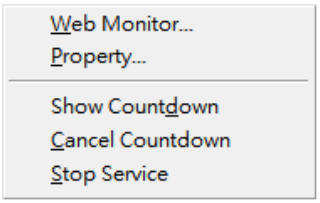
		ShutdownAgent. This option is provided for quickly testing the network communication. The firewall settings may be recovered after the OS reboots.	
a.	Restart Shutdown-Agent Service	Restart service program to apply the changes	
0.	Exit	Exit the configuration program	

4. Operation in Windows

After installation, the ShutdownAgent places an icon in the desktop toolbar to indicate the status of monitoring UPS.

Icon	Description
	Normal
	Service stop
	UPS on battery mode
	UPS battery low
	UPS on bypass mode

To show the pop up menu, please move the mouse cursor over the ShutdownAgent icon and click the mouse button to pop up the menu:



4.1 Web Monitor

ShutdownAgent implemented a web engine to provide the web interface to interact with the end customers. You can monitor and configure the software through the web interface.

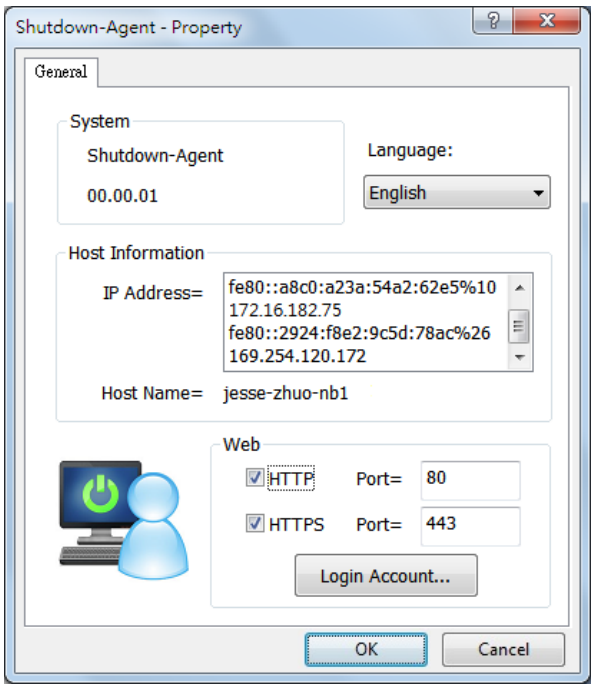
Select the **Web Monitor** menu item from the menu to launch the default web browser, if your login account in the Windows system belongs to the local Administrators group then ShutdownAgent will login to its web engine automatically as the administrator privilege. If you connect a web browser from a remote PC then you have to key in the account and password by yourselves.

For more detail information about the web operation, please refer to the chapter 5.

4.2 Property

Select the **Property** menu item will pop-up the Property dialog box which provides another quick way to configure the basic parameters of ShutdownAgent.

From the General page you can observe the software version number, IP addresses and host name.



Language:

Select the supported language from this option.

HTTP:

To enable/ disable the HTTP protocol, assign a different number of the Port number to change the HTTP connection through the other network port. The default value is 80.

If you have changed the HTTP port number from 80 then you have to key in the connection URL as the following:

http://192.168.1.100:8001

where 192.168.1.100 is the ip address of the PC which ShutdownAgent installed and the 8001 is the port number which you assigned.

NOTE: Please check the Windows firewall setting if the HTTP connection is refused.

HTTPS:

To enable/ disable support the HTTPS protocol, assign a different number of the Port number to change the HTTPS connection through the other network port. The default value is 443.

If you have changed the HTTPS port number from 443 then you have to key in the connection URL as the following:

https://192.168.1.100:4430

where 192.168.1.100 is the ip address of the PC which ShutdownAgent installed and the 4430 is the port number which you assigned.

NOTE: Please check the Windows firewall setting if the HTTPS connection is refused.

Login Account:

The ShutdownAgent implements 3 levels of authentication for the web login as the following:

Administrator:

Has sole right to modify the ShutdownAgent system settings.

Device Manager:

Is not permitted to change the system settings but has the ability to configure the device settings.

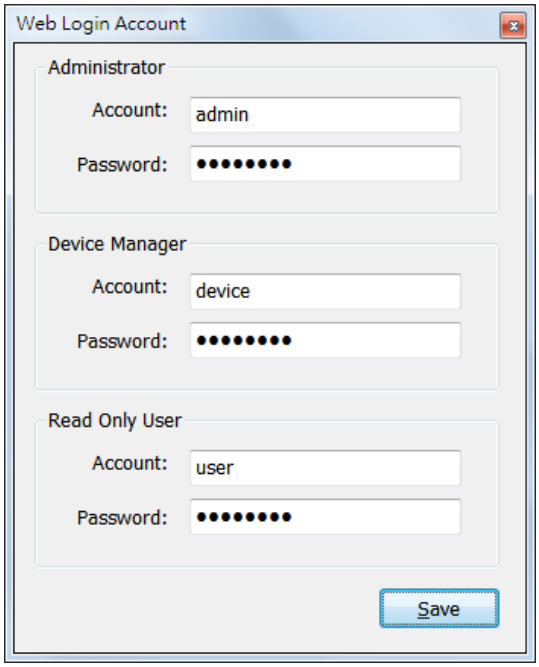
Read Only User:

Can observe the connected devices only.

The following is the default account and password list, please note that they are case-sensitive.

Please continue to modify all of the default passwords to ensure the system security.

	Account	**Password**
Administrator	admin	password
Device Manager	device	password
Read Only User	user	password



4.3 Show Countdown

Select the Show Countdown menu item to display the countdown windows when the ShutdownAgent start to counting down the OS shutdown delay.

4.4 Cancel Countdown

Select the Cancel Countdown menu item during the counting down to stop the shutdown process. To resume the shutdown process, please de-select the Cancel Countdown menu item to counting down the OS shutdown delay.

In addition to de-select the Cancel Countdown menu item to continue the countdown process, when the shutdown event changes the software will start a new countdown process.

4.5 Stop Service

Select the Stop Service menu item to stop the ShutdownAgent service module. To start the service again please de-select the Stop Service menu item.

5. Web Interface

5.1 Run a Web Browser

To connect a web browser from the same PC which ShutdownAgent installed, please select the **Web Monitor** from the toolbar menu, ShutdownAgent will open your default web browser and if your Windows account belongs to the local Administrators group then the ShutdownAgent will login as an administrator for you automatically.

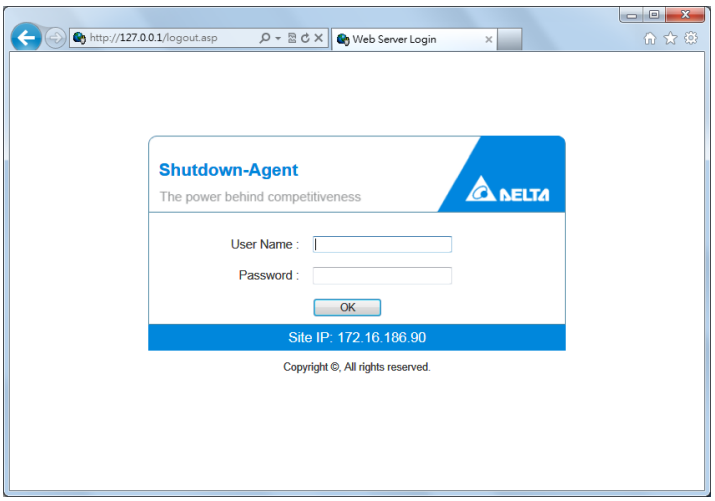
ShutdownAgent allows at most 16 users login at the same time.

You can also connect a web browser from a remote PC, please follow the steps:

Make sure that you have a **TCP/IP** network installed.

Start your Web Browser. Enter **http: //host_name** or **http: //ip_address** in the address bar for the plain text web transmission or **https: //host_name** or **https: //ip_address** for the encrypted web transmission. If you have changed the port number of HTTP or HTTPS then please enter **http: //host_name:port_number** or **http: //ip_address:port_number** in the address bar for the plain text web transmission or **https: //host_name:port_number** or **https: //ip_address:port_number** for the encrypted web transmission

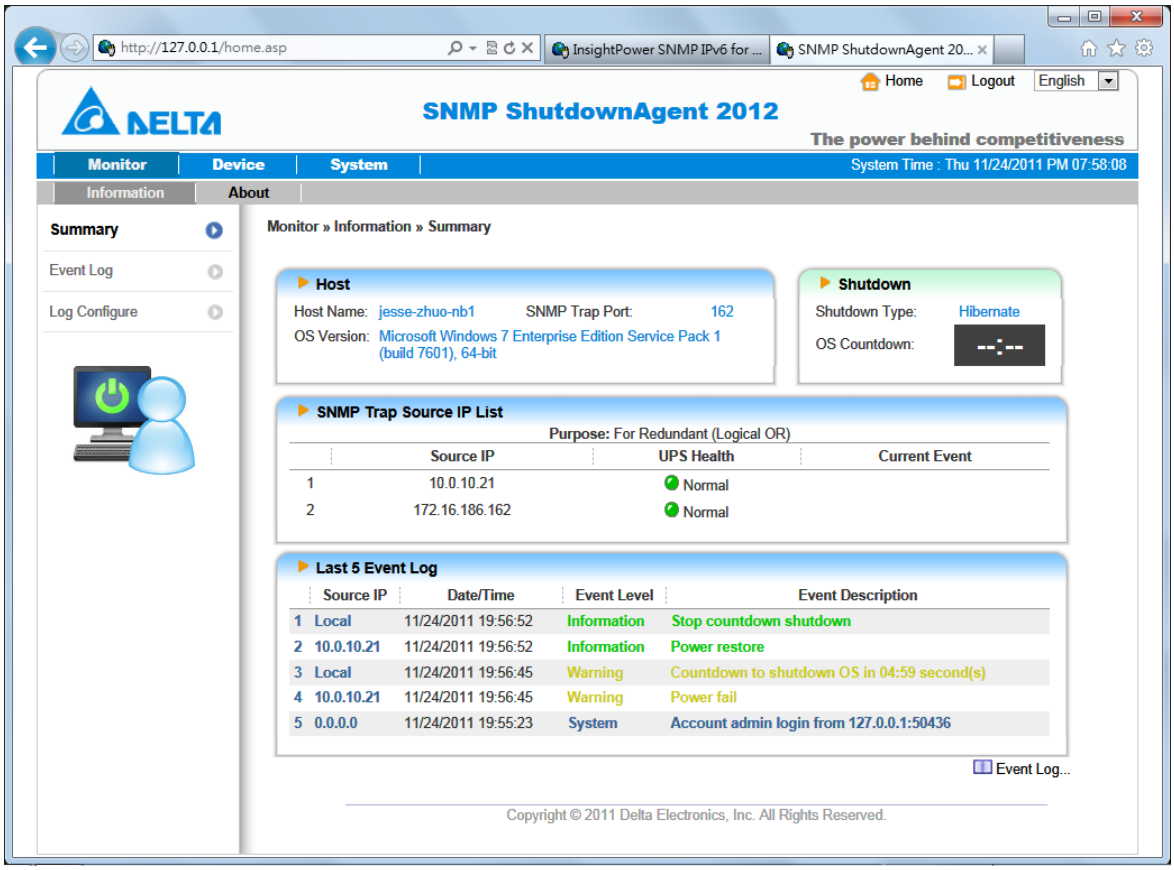
The ShutdownAgent will then ask your account and password. After keying in the correct **account** and **password**, the **ShutdownAgent Home Page** will appear on the screen.



Note: The ShutdownAgent will logout the user automatically if there is no any data transmission through HTTP/HTTPS for more than 30 minutes.

5.2 Monitor >> Information >> Summary

This web page includes the information of identification, shutdown status, source IP status and the last 5 event logs.



Host:

Include the host name, the listen UDP port for SNMP trap and the description of operating system.

Shutdown:

Display the shutdown type (Shutdown, Power Off, Hibernate) and the countdown time to shutdown the OS in second.

SNMP Trap Source IP List:

ShutdownAgent is capable of receiving SNMP traps from multiple source hosts then decide to determine the event by logical OR for redundant application and logical AND for parallel application.

Last 5 Event Log:

Show the last 5 event logs, if you want to see more please visit the Event Log page.

5.3 Monitor >> Information >> Event Log

This web page lists all the events that have detected by the software. The existing logs are overwritten when the maximum number of entries (rows) has been reached. And the maximum number of event is 10,000. You can also download the software event log to a .csv format file.

Log Page Buttons:

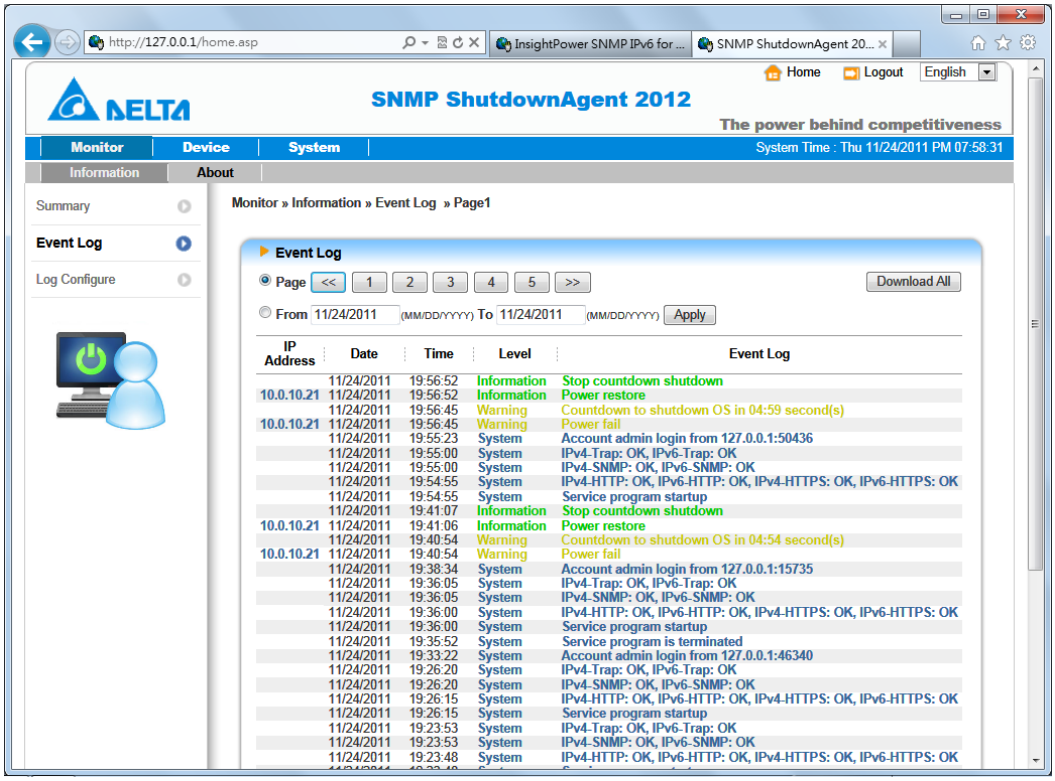
Press the "<<" button to go to the newest page and the ">>" button to go to the oldest page. Click on the page number buttons to observe the event log by page.

Range of Date:

You can also filter the event log by assigning a period of date. Fill in the From and To text boxes then press the Apply button to request the event log by your assigned period of date.

Download All:

Press the **Download All** button to export all of the event log to a .csv format of file.



5.4 Monitor >> Information >> Log Configure

This page lets the Device Manager clear event log.

Clear Event Log:

To clear all of the data log by clicking this button.

5.5 Device >> Host >> Configure

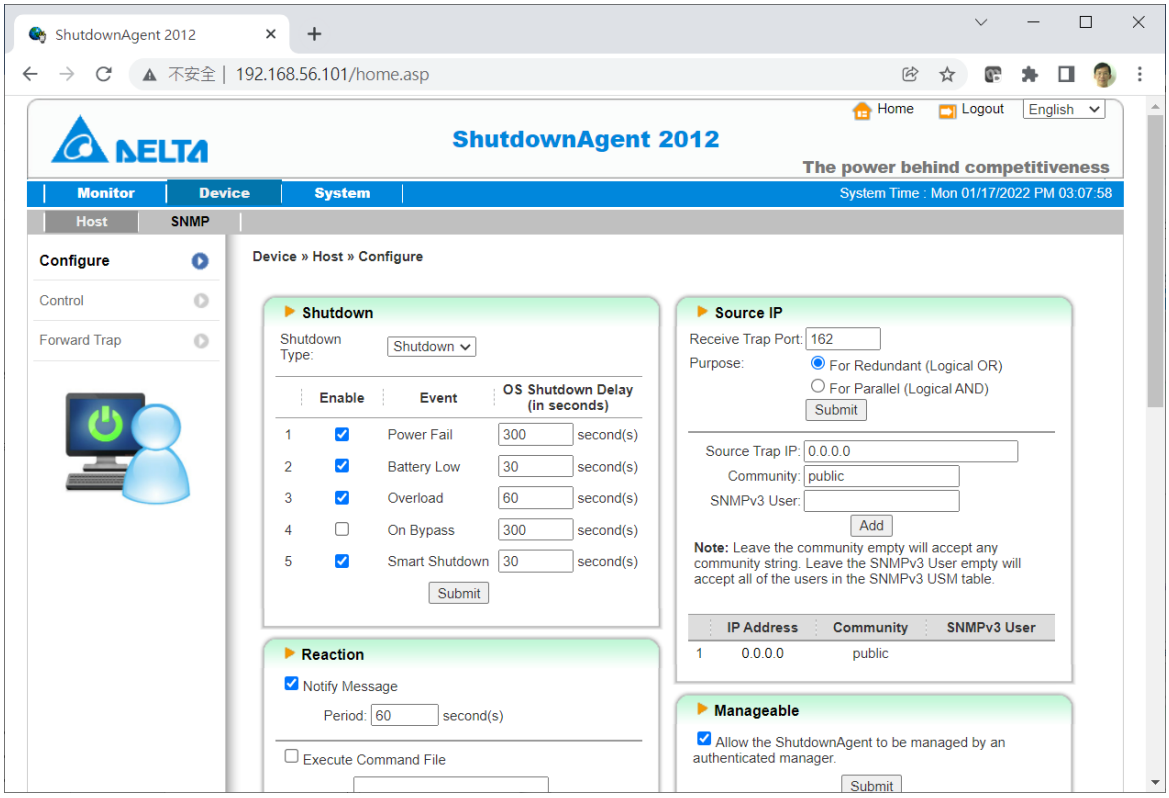
This page is used to configure the major functions, they are: Shutdown, Reaction and Source IP.

Shutdown:

Select the **Shutdown Type** to determine the way to shutdown the operating system. There are **Shutdown**, **Power Off** and **Hibernate** types and the default value is Shutdown.

Now we should continue to determine the shutdown delay time for the following 5 power events: Power Fail, Battery Low, Overload, On Bypass and Smart Shutdown. If the power events recover during countdown then the operating system will not be shutdown.

Regarding to the virtual machine shutdown, please refer to the related chapters.



Reaction:

Enable the **Notify Message** to pops up a message box once ShutdownAgent receives the SNMP traps from the source IP addresses. Assign the period value to report the message periodically, set a 0 to the Period will show the message only once.

Enable the **Execute Command File** to run an assigned external file before shutdown. Set a value to the **Run Before Shutdown** to inform ShutdownAgent when to launch the assigned executable file.

Source IP:

Assign the **Receive Trap Port** to open the specific UDP port for receiving SNMP trap. Then select the Redundant(Logical OR) or Parallel(Logical AND) for the application purpose.

Redundant(Logical OR): Summarize the received power event by logical OR for all of the source IP addresses to determine whether the power event occurs or not. So if the power event occurs in one of the source IP addresses then the power event is tenable and the ShutdownAgent starts to countdown accordingly. Only when the power event recovers from all of the source IP addresses the ShutdowAgent stops countdown and cancel the shutdown process.

Parallel(Logical AND): Summarize the received power event by logical AND for all of the source IP addresses to determine whether the power event occurs or not. So if the power event occurs in all of the source IP addresses then the power event is tenable and the ShutdownAgent starts to countdown accordingly. Once the power event recovers from one of the source IP addresses the ShutdowAgent stops countdown and cancel the shutdown process.

Source IP Address: Assign the source IP address, ShutdownAgent will parse the SNMP trap only when the packet is received from the assigned IP addresses.

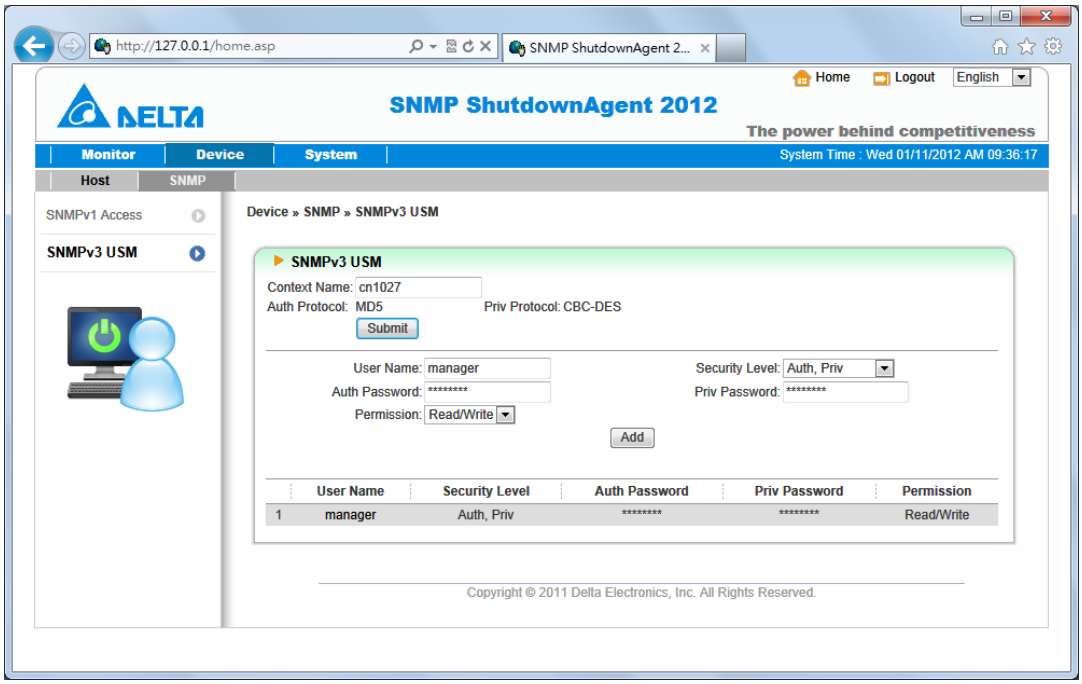
Community: If the value is not empty then only the received trap with the same community string will be accepted. If the value is empty then ShutdownAgent will accept any of the received community string.

SNMPv3 User: This field is used for SNMPv3 packet. If the value is not empty then only the received trap with the same user defined in the

SNMPv3 USM table will be accepted. If the value is empty then ShutdownAgent will accept the users which assigned in the SNMPv3 USM table.

Manageable:

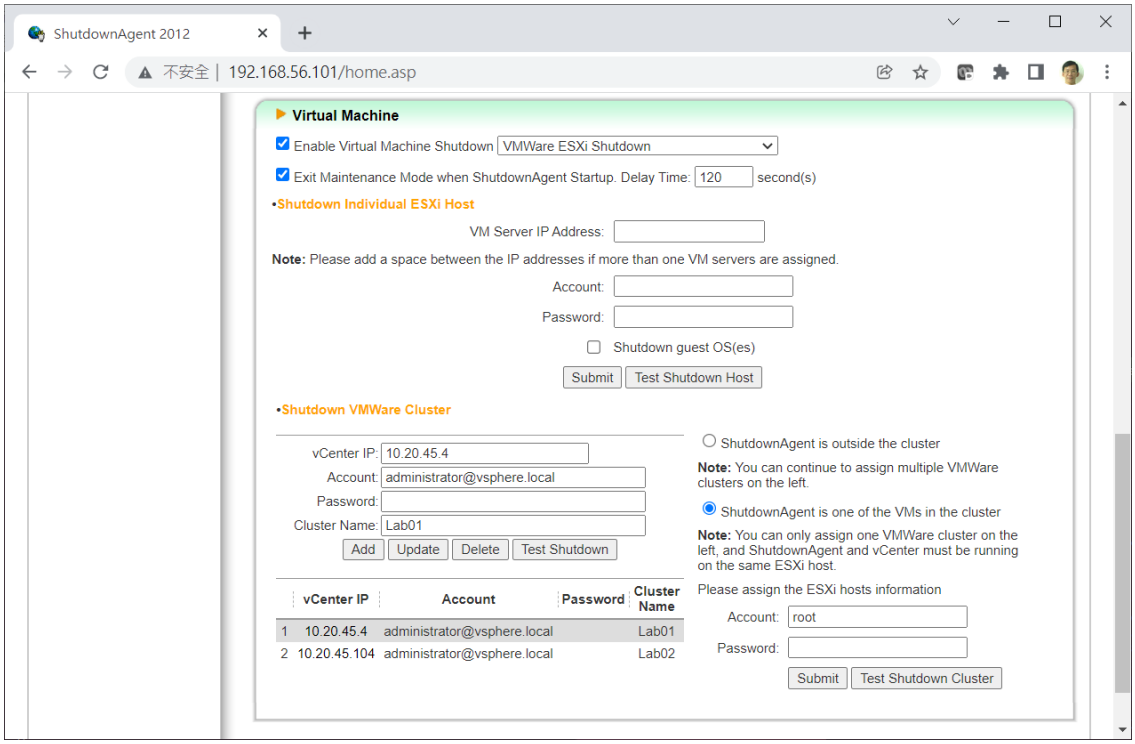
Select the **Allow the ShutdownAgent to be managed by an authenticated manager** option to let the ShutdownAgent reply the query from any authenticated manager. The authenticated manager can be a SNMP card or a centralized management software. After collecting the ShutdownAgent information, the authenticated manager can provide a comprehensive list of all of the ShutdownAgent.



In fact, the authenticated manager communicate with the ShutdownAgent through SNMPv3 with the first default account in the SNMPv3 USM list. If the **Allow the ShutdownAgent to be managed by an authenticated manager** option is enabled then the permission of "manager" account changes to "Read/Write", otherwise the permission is "Disable".

The default setting of **Allow the ShutdownAgent to be managed by an authenticated manager** option is "enabled".

Virtual Machine：(Linux Version)



Enable Virtual Machine Shutdown: Select this option when the virtual machine needs to be shut down by the ShutdownAgent.

VMWare ESXi Maintenance and Shutdown: Perform a shutdown of the ESXi host and enter maintenance mode before shutting down the host. Select this shutdown option when ShutdownAgent is installed on a VM on this ESXi host.

VMWare ESXi Shutdown: Force to shutdown the ESXi host.

VMWare ESXi v4: Shutdown the host of ESXi v4.

Xen Server: Perform the shutdown of Xen server.

Linux KVM: Perform the shutdown of KVM server.

Exit Maintenance Mode when ShutdownAgent Startup: When this option is selected, ShutdownAgent will send a command to exit the maintenance mode when it is started, and restore the host that entered maintenance mode in previous shutdown process.

Delay Time: Delay sending the Exit Maintenance Mode command to vCenter, adjust the delay time to ensure vCenter is up and running before successfully sending the Exit Maintenance Mode command.

Shutdown Individual ESXi Host

VM Server IP Address: When you need to shut down the host individually, please enter the IP address of the host. When entering multiple IPs, please leave a blank between the two IP addresses. Note that shutting down multiple hosts refers to the hosts running independently of each other and not to a clustered architecture.

VM Account, Password: The account and password of the virtual host, when there are multiple virtual hosts, please unify the account and password into one.

Shutdown Guest OS(es): Whether to shut down the running Guest OS before shutting down the ESXi host. To run correctly please install VMWare Tools on each Guest OS. Be sure to select this option when ShutdownAgent is installed on a VM on this ESXi host.

Shutdown VMWare Cluster

ShutdownAgent is outside the cluster: ShutdownAgent is installed outside the cluster. At this time, you do not need to enter the account and password of the ESXi host, just enter the vCenter IP, account, password and Cluster name on the left.

ShutdownAgent is one of the VMs in the cluster: ShutdownAgent is installed outside this cluster. At this time, you need to enter the account and password of the ESXi host. You also need to enter the vCenter IP, account, password and Cluster name on the left.

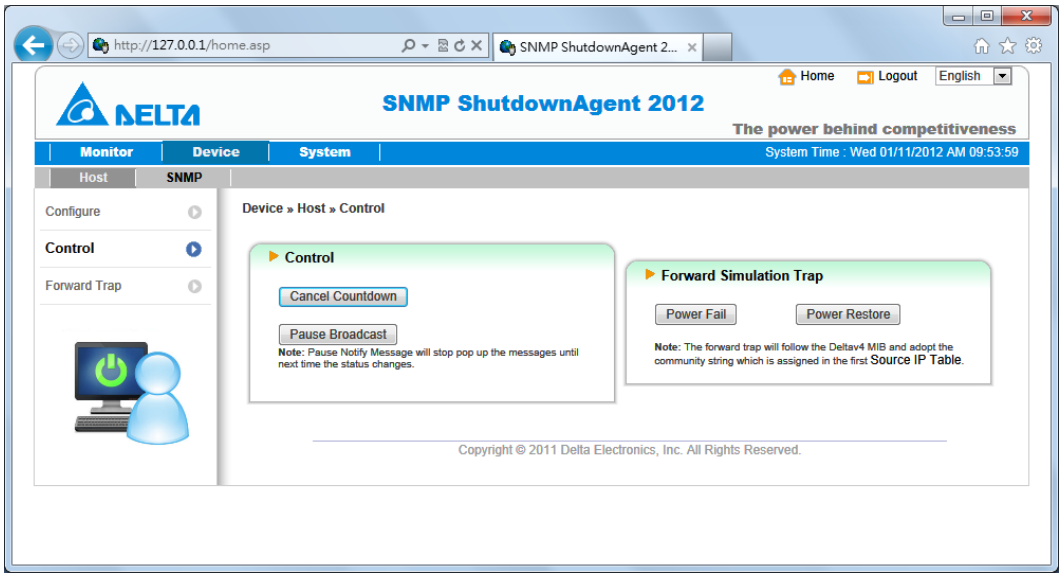
ESXi Host Account, Password: The account and password of the ESXi host running in this cluster. Please unify multiple hosts into one account and password.

vCenter IP: IP address of vCenter.

vCenter Account, Password: vCenter account and password.

Cluster Name: The cluster name.

5.6 Device >> Host >> Control



Control:

Press the Cancel Countdown button during the countdown shutdown process to stop counting down. Press the button again to resume the shutdown process.

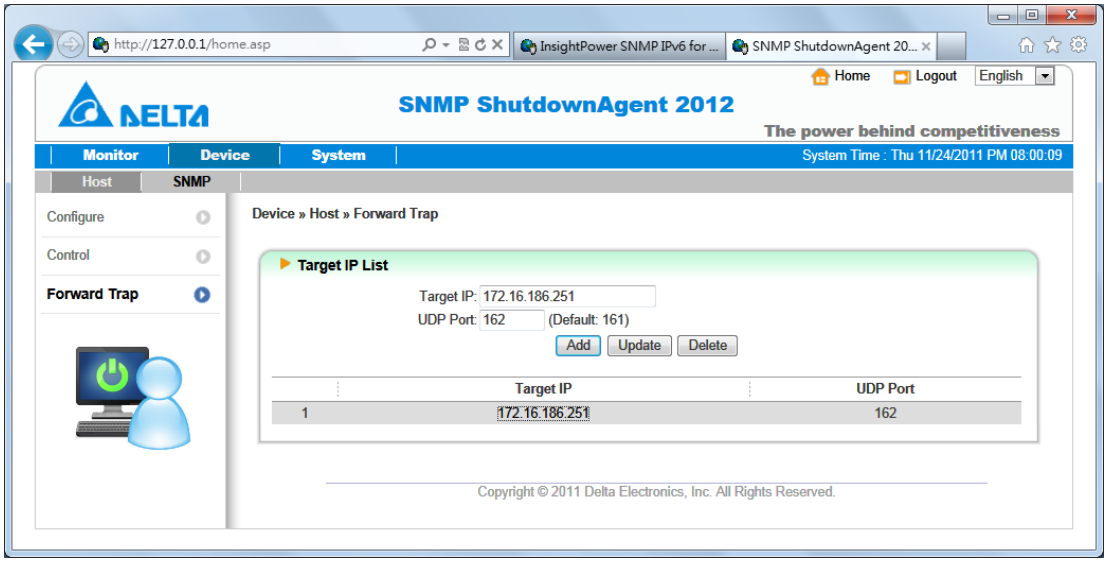
Forward Simulation Trap:

Press the Power Fail button to send the simulated power fail SNMP trap to the assigned forward target IP addresses.

Press the Power Restore button to send the simulated power restore SNMP trap to the assigned forward target IP addresses.

5.7 Device >> Host >> Forward Trap

Forward Trap is used to forward the received SNMP trap to extend the size of protection OS shutdown gracefully.



5.8 Device >> SNMP >> SNMP Access

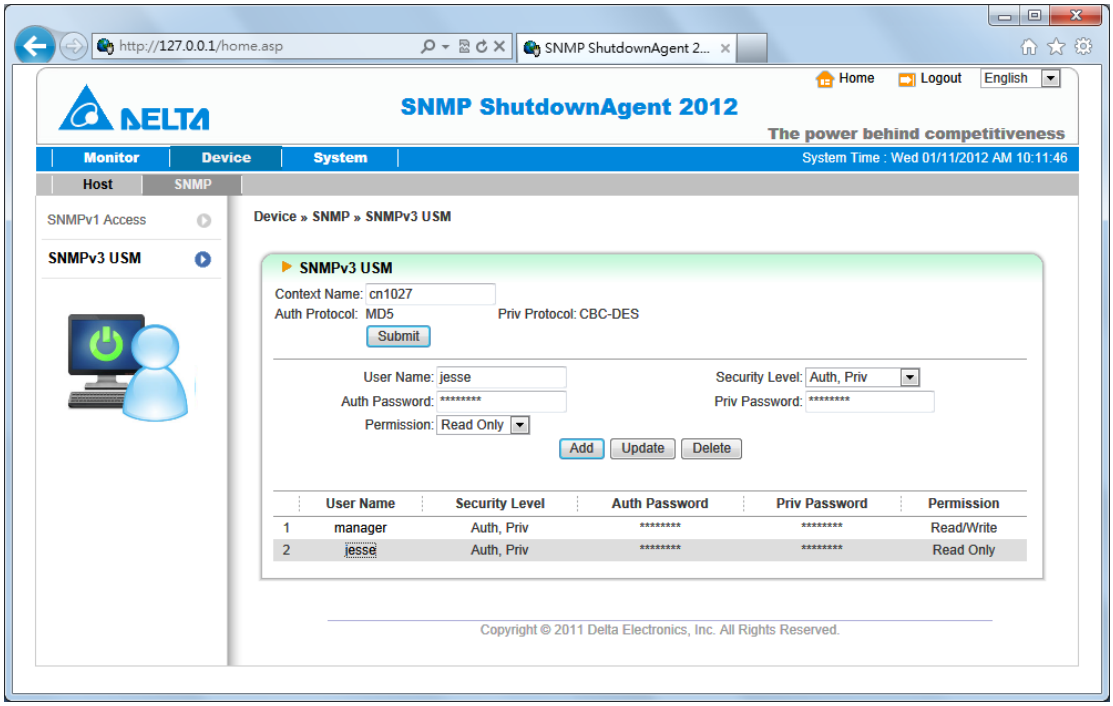
The shutdownAgent supports SNMP protocol and SNMP NMS (Network Management System), which are commonly used to monitor network devices for conditions that call for administrative attention. To prevent unauthorized access, you can specify the NMS IP addresses that are allowed to access, their community strings and access levels. The maximum number of IP entries is 255.

5.9 Device >> SNMP >> SNMPv3 USM

SNMPv3 offers features such as the encryption of packets and authentication to improve security. The SNMPv3 USM (User Session Management) allows you to

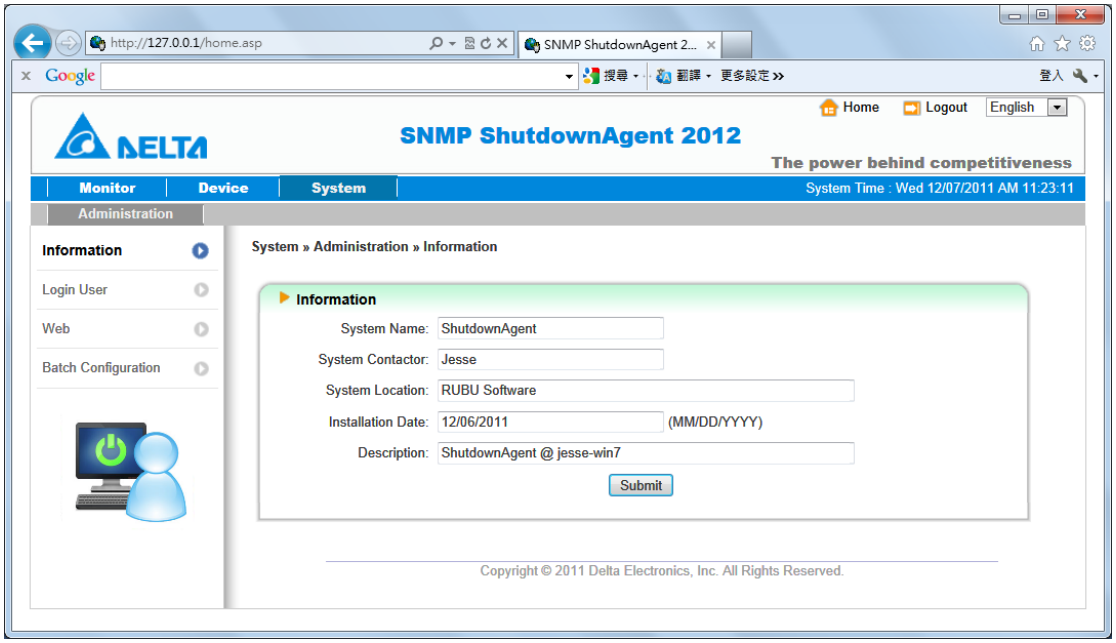
assign 32 User Names whose access is granted via SNMPv3 protocol. You can also define their respective Security Levels, Auth Passwords, Priv Passwords and Permission.

The first one account cannot be deleted, to disable it please go to the Device >> Host >> Configure web page then uncheck the manageable option.



5.10 System >> Administration >> Information

Here to assign the system information for the ShutdownAgent, including Installation Date, Location and Description.



5.11 System >> Administration >> Login User

You can manage the login authentication for web interface by assigning 3 different level of users' account and password.

The access permission for the account types are listed as follows:

Administrator: Permitted to modify all settings.

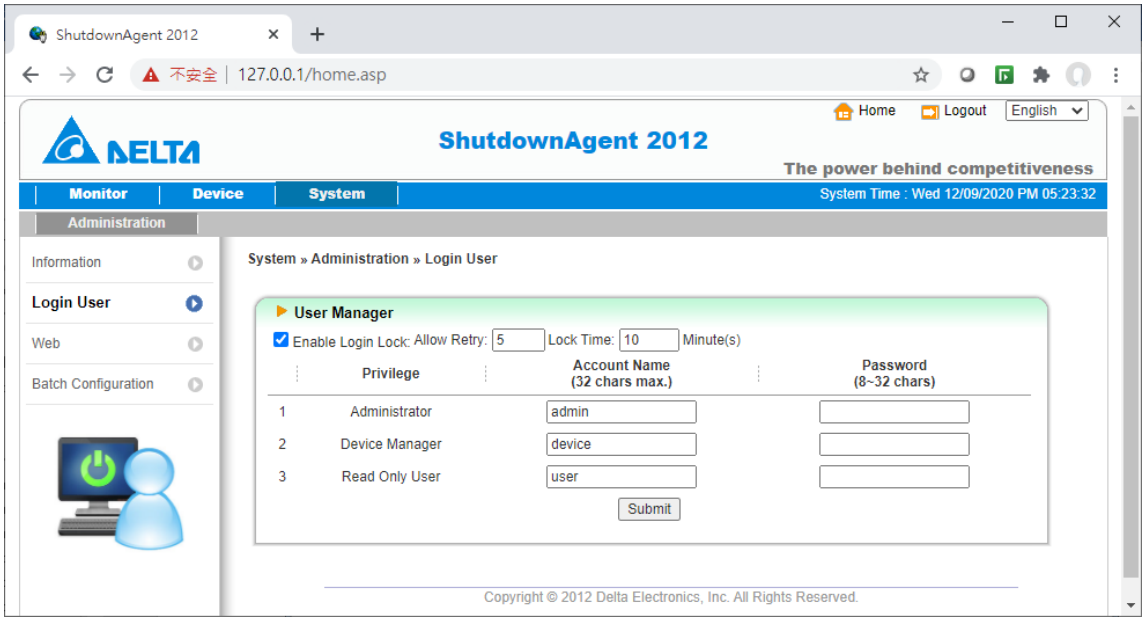
Device Manager: Permitted to modify device-related settings.

Read Only User: Only permitted to observe ShutdownAgent status.

Enable Login Lock: When the user logs in more than the specified number of times, the system will lock the user for a period of time.

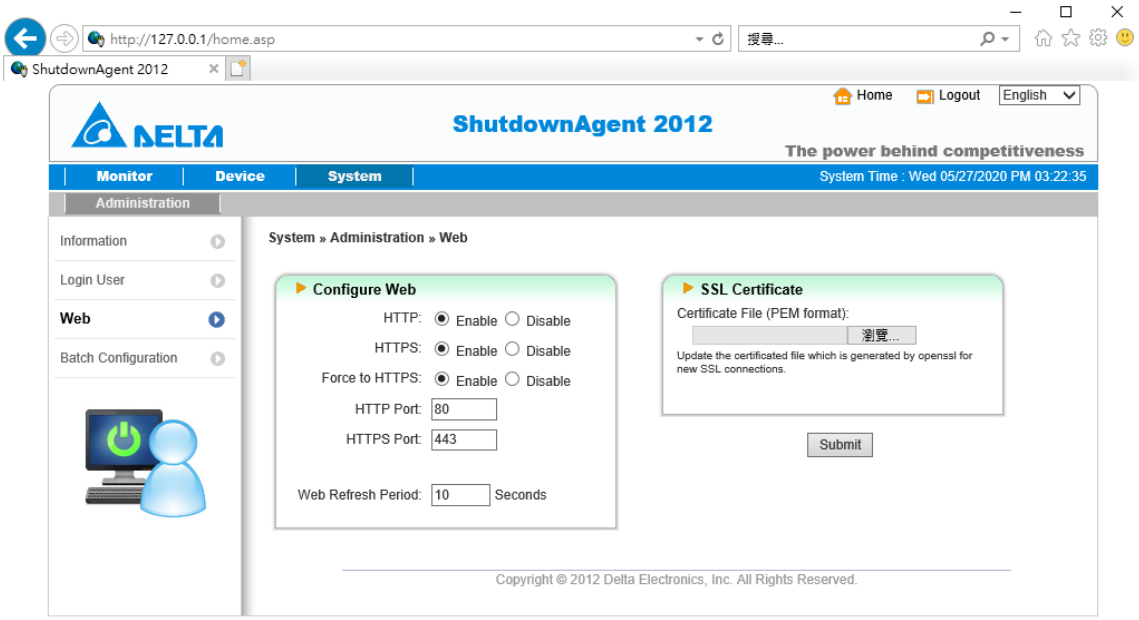
Allow Retry: Lock after wrong number of logins.

Lock Time: Lock the account time, ignore the user login request during the lock time.



5.12 System >> Administration >> Web

This menu lets the administrator enable or disable the HTTP/HTTPS communication protocols available in the ShutdownAgent.



HTTP:

Enabling or disabling the HTTP connection with the ShutdownAgent.

HTTPS:

Enabling or disabling the HTTPS connection with the ShutdownAgent.

Force to HTTPS:

Enabling or disabling the Force to HTTPS connection with the ShutdownAgent. The software will redirect the http://IP_Address to https://IP_Address when the user login.

HTTP Port:

The user may configure HTTP protocol to use a port number other than standard HTTP port (80).

HTTPS Port:

The user may configure HTTPS protocol to use a port number other than standard HTTPS port (443).

Web Refresh Period:

The period of time to update the monitoring web pages. The range is 1~9999 seconds.

SSL Certificate:

To ensure connection security between the ShutdownAgent and the connecting workstation, SSL certificate can be used to encrypt and secure the integrity of transmitting data.

Certificate File: This allows you to replace your own SSL certificate file. The ShutdownAgent supports PEM format which is generated by OpenSSL. Click **Choose File** to upload a certificate file.

***How to generate a private SSL certificate file (in PEM format) for HTTPS?**

To ensure connection security, you can create your own SSL certificate file. Please download and install OpenSSL Toolkit from http://www.openssl.org. Launch terminal mode and enter the following command to create your own certificate file:

openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout cert.pem -out cert.pem

1) Answer the prompted questions. Proceed with the given directions. Once it is completed, a file named cert.pem is created in the current working directory.

2) Upload cert.pem to the Web.

5.12 System >> Administration >> Batch Configuration

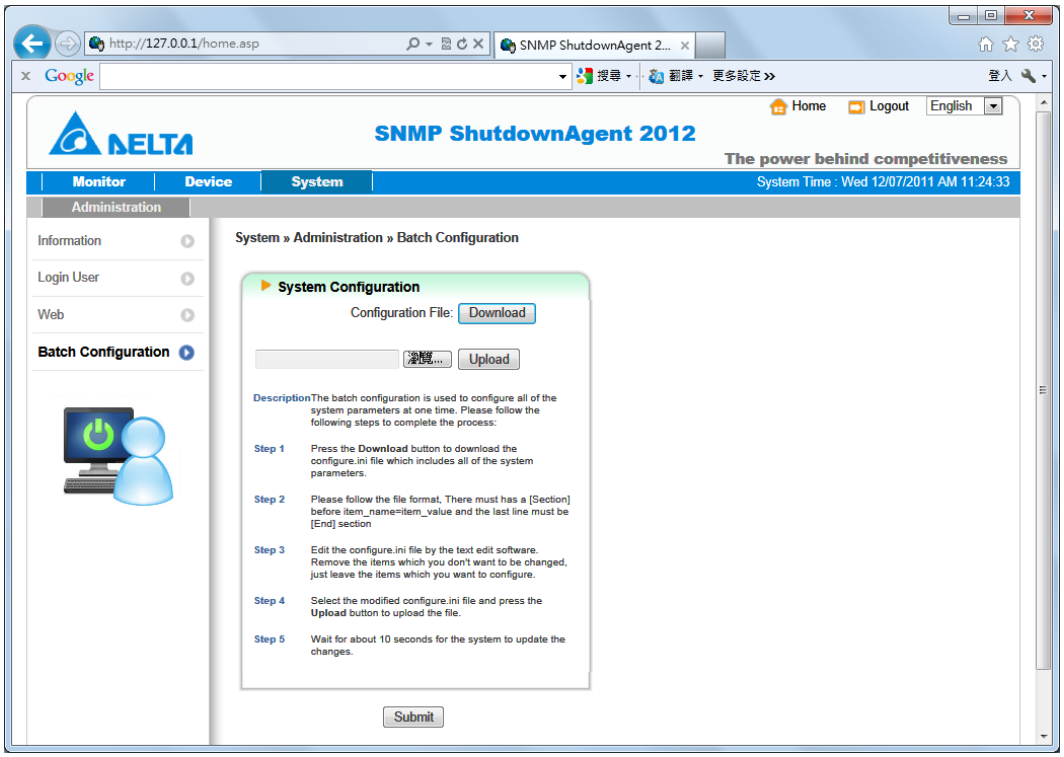
The ShutdownAgent provides batch configuration to allow quick and effortless setup on multiple ShutdownAgent hosts. You can duplicate settings by downloading the configuration file from the ShutdownAgent that you have successfully configured, and upload the configuration files on other hosts.

Download:

Download the agent.ini for you to store or edit the configuration file.

Upload:

Upload the configuration file to ShutdownAgent to apply the change immediately.



6. 2008 Server Core Setup for ShutdownAgent

While installation the ShutdownAgent in the 2008 server core, it requires the following commands to transfer the file and add some rules for firewall.

1. Disable firewall:

   netsh advfirewall set allprofiles state off

2. Enable firewall:

   netsh advfirewall set allprofiles state on

3. Add a remotely shared directory:

   net use e: \\<ip address>\e

4. Open the SNMP Trap UDP 162

   netsh advfirewall firewall add rule name="SNMPTrap" protocol=UDP dir=in localport=162 action = allow

5. Open SNMP Server UDP 161

   netsh advfirewall firewall add rule name="SNMPServer" protocol=UDP dir=in localport=161 action = allow

6. Open the HTTP TCP 80

   netsh advfirewall firewall add rule name="HTTP" protocol=TCP dir=in localport=80 action = allow

7. Open HTTPS TCP 443

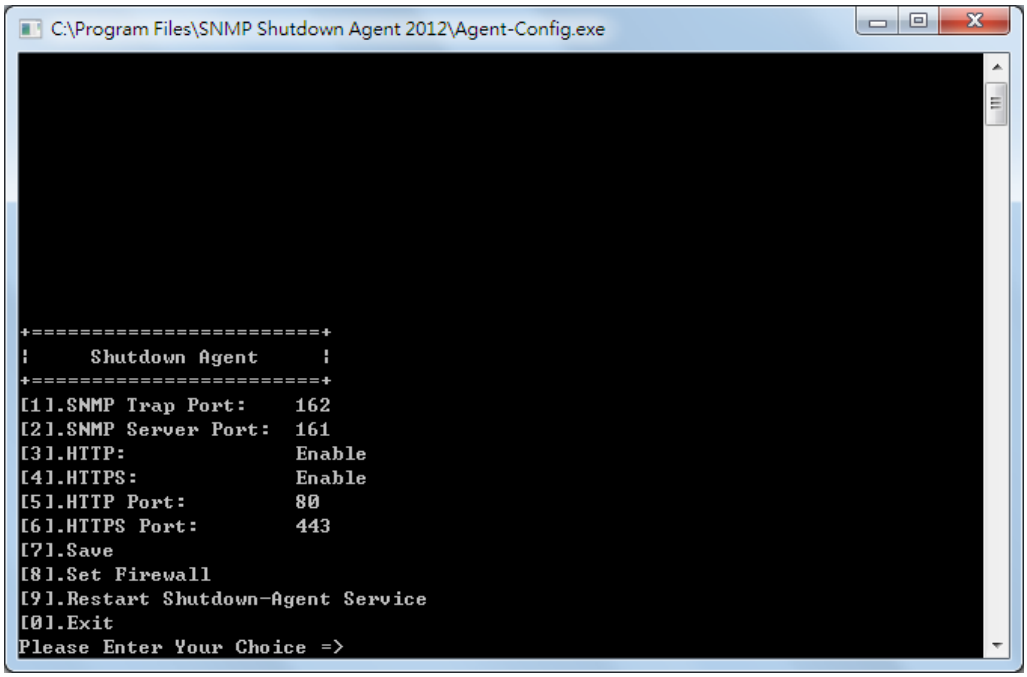
   netsh advfirewall firewall add rule name="HTTPS" protocol=TCP dir=in localport=443 action = allow

Firstly, put the Shutdown-Agent-2012-Setup(x64).exe setup file in the 2008 server directory. If there is no CD-ROM you can set the "Disable firewall" command, "Add a remotely shared directory" command then copy the file from your PC to the 2008 server. Don't forget to set the "Enable firewall" command when complete.

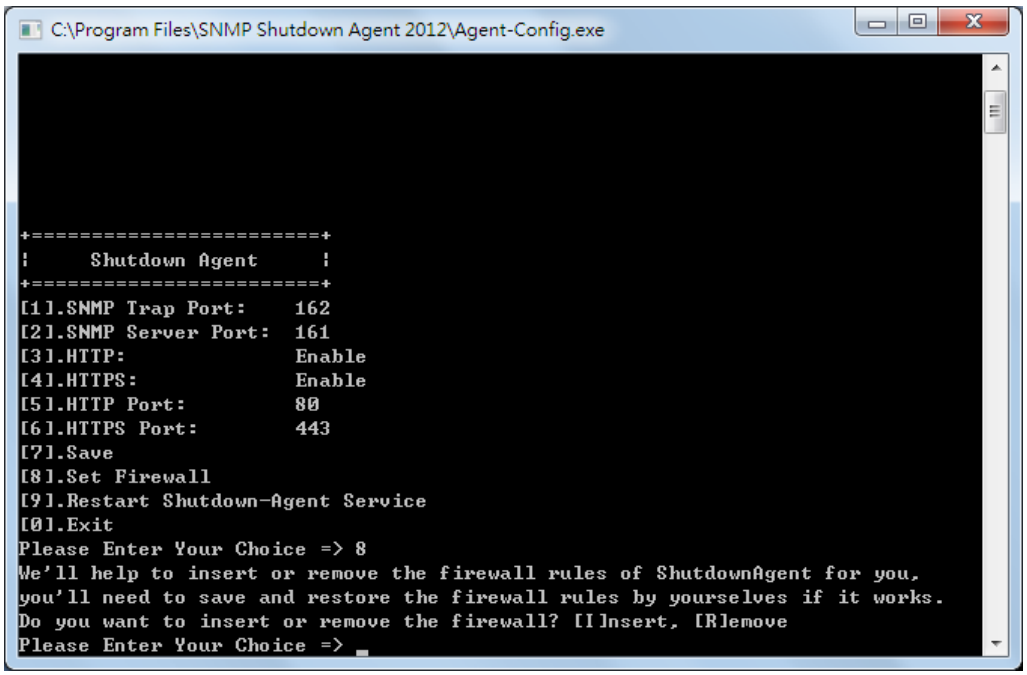
Secondly, follow the chapter 2 to install the ShutdownAgent in the 2008 server.

The last step is use the open HTTP/HTTPS, SNMP Trap/Server port commands to open the necessary which you want.

You can easily run the Agent-Config.exe to configure the basic networking parameters for the web and SNMP network protocols after installation.



Select [8] to help you to insert or remove a firewall rule for the ShutdownAgent.



7. VMWare ESXi 4.0 Setup for ShutdownAgent

Before installing the ShutdownAgent in the ESXi4.0 server, please transmit the ShutdownAgent setup file to the ESX server through SFTP by FileZilla FTP Client or other SFTP client then login to the ESX server by the local console or through your favorite SSH client (such as Putty).

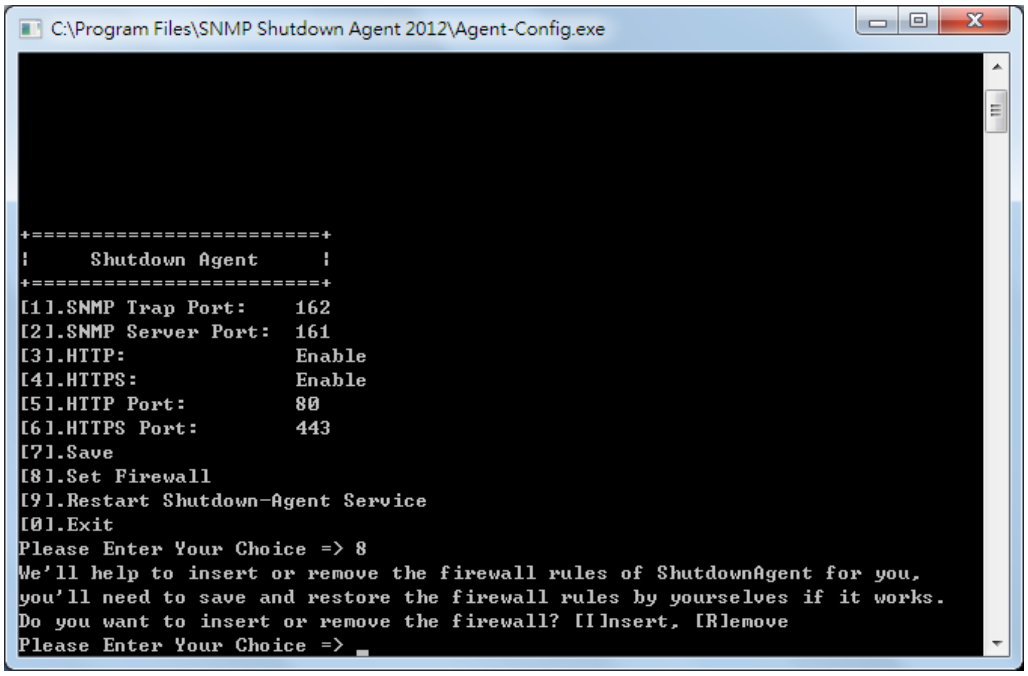
Please continue to follow the section 2.2 For Linux Installation/ Uninstallation.

To configure the basic networking parameters including the ESXi4.0 firewall, please see chapter 3 Console Configuration.

7.1 Configure the Firewall for ESXi 4.0

Run the /usr/local/upsagent/configure

Select [8] to help you to insert or remove a firewall rule for the ShutdownAgent.



7.2 Install VMware Tools for Guest OS

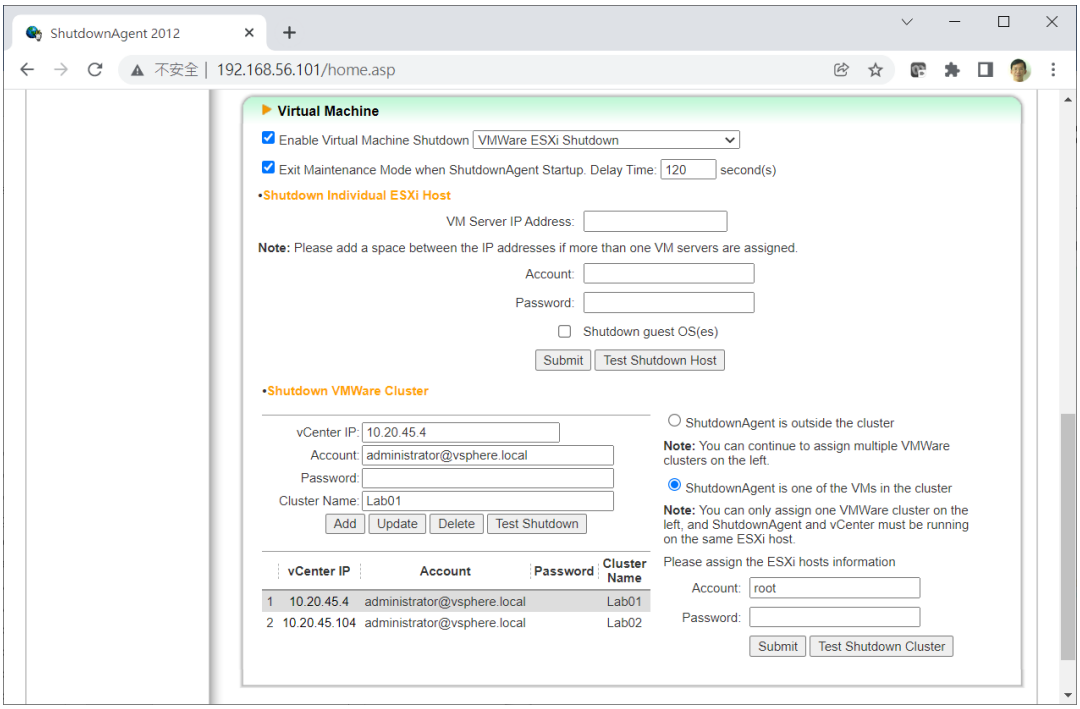
To shutdown the guest OS from ESXi server, it' s better for you to install the VMware tools for all of them so as to inform the guest OSes shutdown smoothly.

For Windows operating system.

Select the following menu Guest → Install/Upgrade VMware Tools

7.3 Configure ShutdownAgent for ESXi4.0

1. Login to the web interface of ShutdownAgent and the account level should greater than or equal to device manager.
2. Goto the Device → Host → Configure web page to enable the **Enable Virtual Machine Shutdown** checkbox then select the **VMWare ESXi4** option.



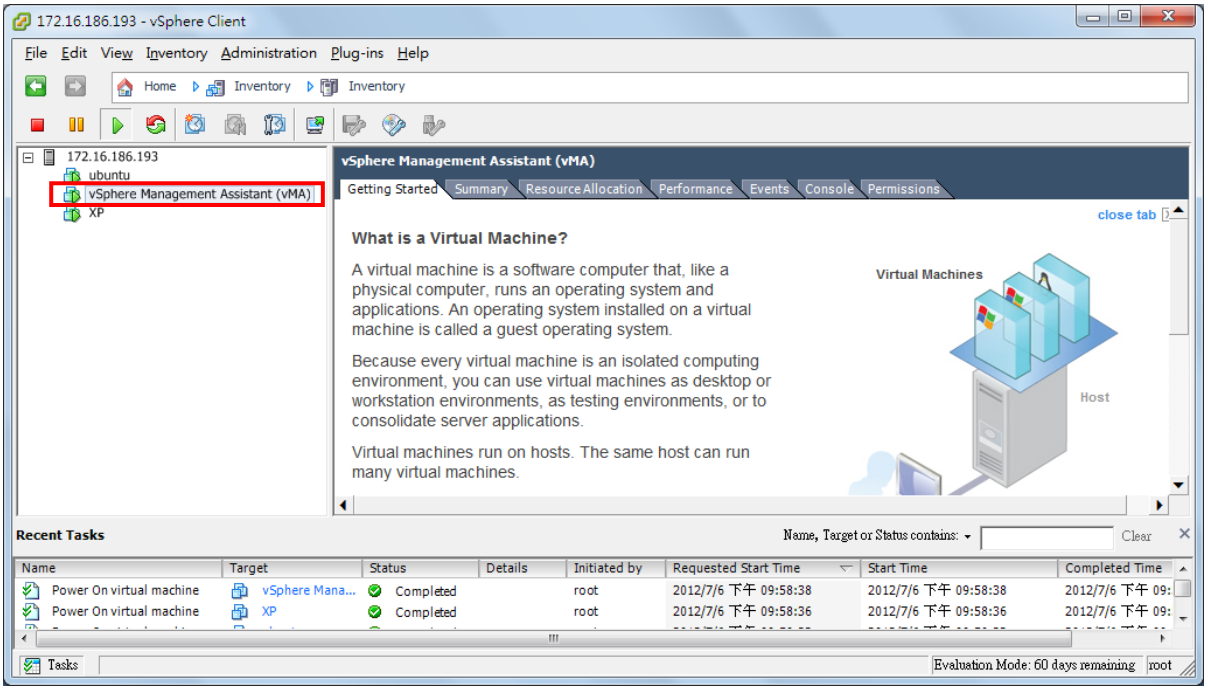
3. Press **Submit** button to update your changes.

8. VMWare ESXi 4.1/ 5/ 6 Setup for ShutdownAgent

Before installing the ShutdownAgent for the ESXi4.1/ 5/ 6, you have to install the **vMA 5(vSphere Management Assistant 5)** or the above version and make sure the **VMWare tools** is installed in all of the guest OSes. Please then transmit the ShutdownAgent setup file to the vMA server through SFTP by FileZilla FTP Client or other SFTP client then login to the vMA server by the local console or through your favorite SSH client (such as Putty).

Please continue to follow the section 2.2 For Linux Installation/ Uninstallation.

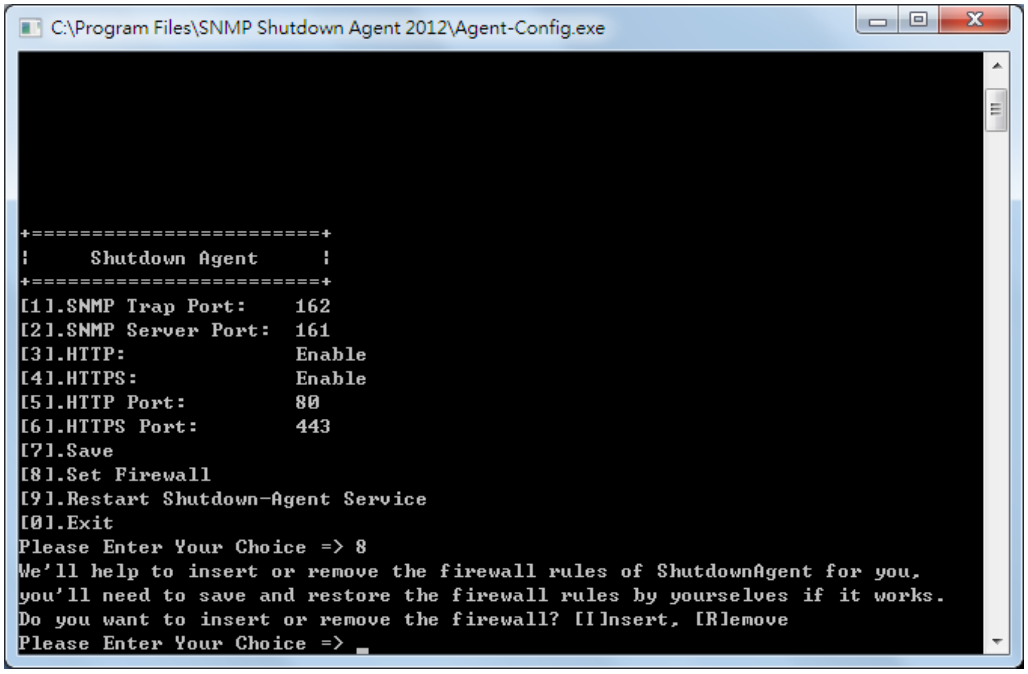
To configure the basic networking parameters including the vMA firewall, please see chapter 3 Console Configuration.



8.1 Configure the Firewall for vMA

Run the /usr/local/upsagent/configure

Select [8] to help you to insert or remove a firewall rule for the ShutdownAgent.



8.2 Install VMware Tools for Guest OS

To shutdown the guest OS from ESXi4.1/ 5/ 6 server, you have to install the VMware tools for all of them so as to inform the guest OSes shutdown smoothly.

For Windows operating system.

Select the following menu Guest → Install/Upgrade VMware Tools

8.3 Configure ShutdownAgent for ESXi4.1/ 5/ 6

1. Login to the web interface of ShutdownAgent and the account level should greater than or equal to device manager.
2. Goto the Device → Host → Configure web page to enable the **Enable Virtual Machine Shutdown** checkbox.
3. If the **ShutdownAgent** installed on the guest OS of the same ESXi host, please choose the **VMWare ESXi Shutdown** option.
4. If the **ShutdownAgent** installed on an external PC, you can chose **VMWare ESXi Maintenance and Shutdown** or **VMWare ESXi Shutdown** option per your application.
5. Description: **VMWare ESXi Maintenance and Shutdown** option will let the ESXi host enter maintenance mode first, then shutdown the host. The **VMWare ESXi Shutdown** option shuts down the host directly.
6. Please continue to setup the followings.

VM Server IP Address: The ESXi server IP address. If there are more than 1 server IP addresses, please separate them by a space character.

Account: The root privilege for ESXi server.

Password: The password of the root account.

Submit: The button to update your changes.

9. ShutdownAgent Shutdown VMWare ESXi 6.5 and Above

9.1 ShutdownAgent Linux Edition

Due to the vMA is deprecated after version 6.5, you have to install one public Linux OS such as SUSE, CentOS or Ubuntu. Then install the vCLI in the management Linux OS. Please note that the network communication between the ESXi server and this management Linux must work normally.
Please refer to the VMWare web site for the detail instructions on how to installation vCLI.

9.1.1 Test the esxcli command

After installing the vCLI, please continue to test the esxcli command.

1. Login the system by the root account.
2. Open the terminal shell, goes to /usr/lib/vmware-vcli/bin/esxcli/ directory.
   Key in `cd /usr/lib/vmware-vcli/bin/esxcli`
3. Test to get the guest OS running on each ESXi host. Please key in:
   `esxcli -s 10.0.10.107 -u root -p 2wsx@WSX vm process list`
   where 10.0.10.107 is the ESXi host IP address, root is the root account, 2wsx@WSX is the password for root. Please key in the correct information based on your environment.
   In a normal condition, the host should reply all of the running guest OS information, as follows:

```
delta@sa2012-vm:/usr/lib/vmware-vcli/bin$ cd esxcli/
delta@sa2012-vm:/usr/lib/vmware-vcli/bin/esxcli$ ./esxcli --server 10.0.10.107 -
-user root --password 2wsx@WSX vm process list
vSphere Management Assistant (vMA)
   World ID: 35297
   Process ID: 0
   VMX Cartel ID: 35295
   UUID: 56 4d 8a 60 30 e0 b5 5a-8d 75 20 5c 56 23 ba d5
   Display Name: vSphere Management Assistant (vMA)
   Config File: /vmfs/volumes/58c66588-8144e300-b5e2-6805ca39cd23/vSphere Manage
ment Assistant (vMA)_1/vSphere Management Assistant (vMA)_1.vmx

Ubuntu-x86
   World ID: 35298
   Process ID: 0
   VMX Cartel ID: 35294
   UUID: 56 4d ff 28 88 44 d6 84-84 1a 66 ed a8 3b 6b cd
   Display Name: Ubuntu-x86
   Config File: /vmfs/volumes/58c66588-8144e300-b5e2-6805ca39cd23/Ubuntu-x86/Ubu
ntu-x86.vmx
delta@sa2012-vm:/usr/lib/vmware-vcli/bin/esxcli$
```

But if the version is old enough of the ESXi host, then you' ll get the certification error message as follows:

Certificate error. Server SHA-1 thumbprint:
04:82:AE:AE:67:C5:F6:DB:1D:0F:CE:5F:1A:92:34:4A:B9:EA:FE:CE (not trusted)

Now, you have to add the thumbprint code in the vCLI, please going to the /usr/lib/vmware-vcli/apps/general directory.

First add the server IP:

./credstore_admin.pl add --server 10.0.10.107 --username root --password 2wsx@WSX

Tehn add the thumbprint:

./credstore_admin.pl add --server 10.0.10.107 --thumbprint 04:82:AE:AE:67:C5:F6:DB:1D:0F:CE:5F:1A:92:34:4A:B9:EA:FE:CE

Continue to get the guest OS information to complete the test, Please test the ESXi hosts one by one.

then install the ShutdownAgent in the management Linux and make sure the **VMWare tools** is installed in all of the guest OSes. Please then transmit the ShutdownAgent setup file to the management Linux through SFTP by FileZilla or other SFTP client then login to the Linux by the local console or remote desktop.

Please continue to follow the section 2.2 For Linux Installation/ Uninstallation. The other configuration, please refer to the chapter 8.

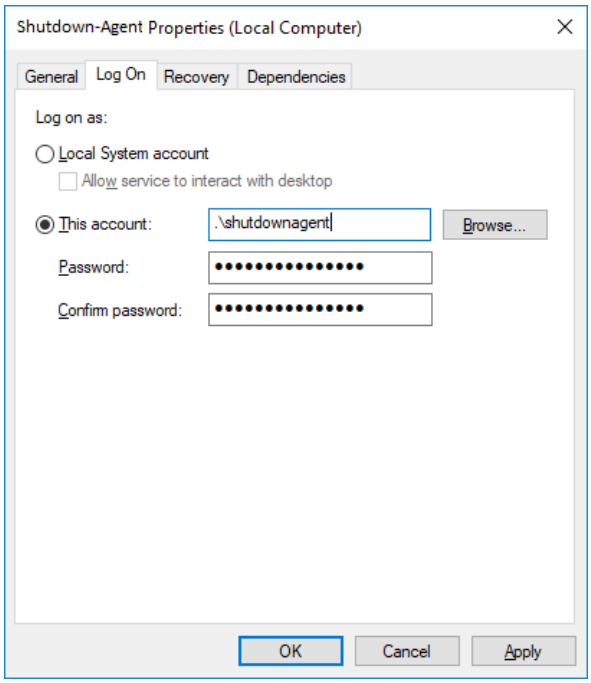
9.2 ShutdownAgent Windows Edition

Please note, to shutdown the ESXi host or cluster you cannot install the ShutdownAgent Windows Edition in the same cluster or host. This will cause the ShutdownAgent to be turned off before sending the complete shutdown commands.

The installation of Windows ShutdownAgent, please refer to section 2.1.

9.2.1 Add the Windows shutdownagent account

1. Please add the Windows "shutdownagent" account. This ccount must be assigned as a local administrator, This account will be used to execute the ShutdownAgent service program.
2. Please login to Windows system by the shutdownagent account, select the Start > Windows Administrative Tools > Services. Click on the Shutdown-Agent service then open its property dialog box and switch to the Log On page. Click on "This account" and key in the shutdownagent account and password then press the OK button.



9.2.2 Install VMWare vCLI

You have to login to Windows system by the shutdownagent account before the installation.

1. Install VMWare vCLI(vSphere CLI), please download the VMWare vCLI Windows setup file from the official VMWare web site then install it.
2. Install Strawberry Perl: please download the Strawberry Perl Windows setup file from the official web site then install it.
   http://strawberryperl.com/

After installation, continue to download the Text::Template and UUID modules, as follows:

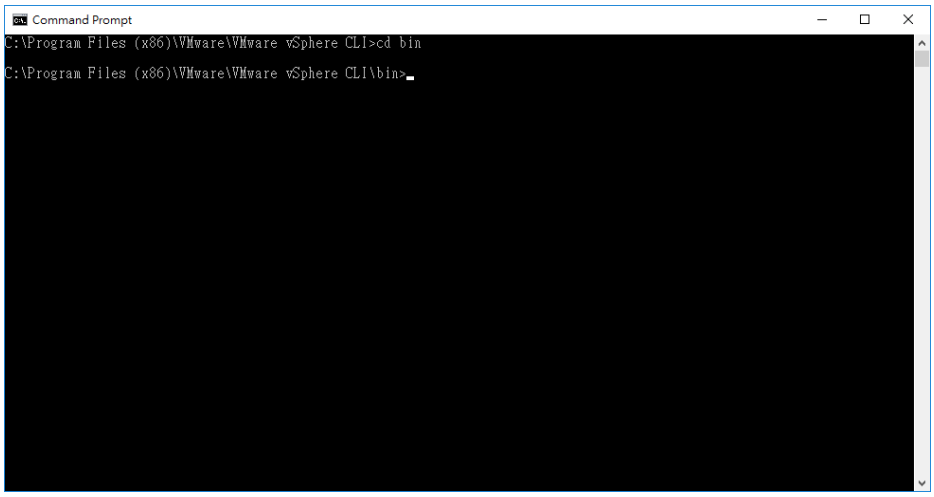
2.1 Select Windows Start > Strawberry Perl > CPAN Client

To install Text::Template Module, please key in: `cpan> install Text::Template`

To install UUID Module, please key in: `cpan> install UUID`

3. We' ll continue to test the esxcli command.

3.1 Select Windows Start > VMware > Command Prompt. Then enter the \bin directory, Please key in: `cd bin`.

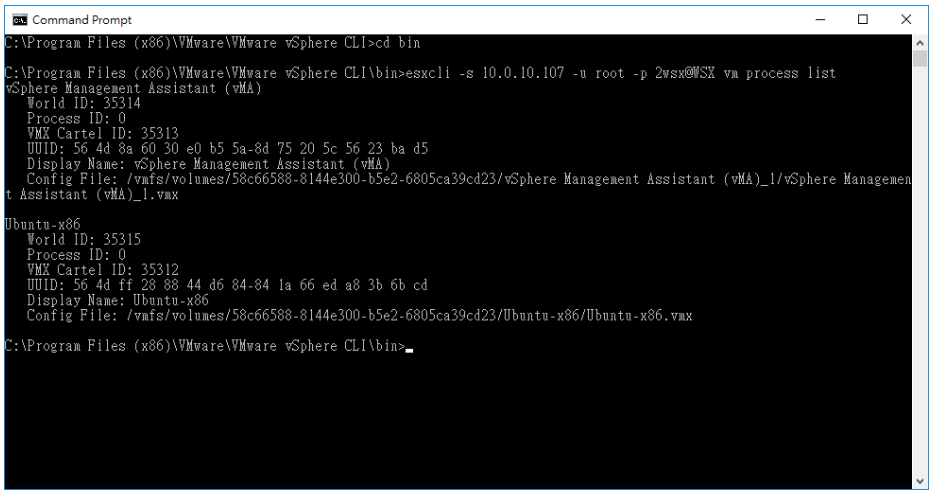


3.2 Test to get the guest OS information from each ESXi host. Please key in:

`esxcli -s 10.0.10.107 -u root -p 2wsx@WSX vm process list`

where 10.0.10.107 is the ESXi host IP address, root is the root account, 2wsx@WSX is the password for root. Please key in the correct information based on your environment.

In a normal condition, the host should reply all of the running guest OS information, as follows:



But if the version is old enough of the ESXi host, then you' ll get the certification error message as follows:

Certificate error. Server SHA-1 thumbprint:
04:82:AE:AE:67:C5:F6:DB:1D:0F:CE:5F:1A:92:34:4A:B9:EA:FE:CE (not trusted)

Now, you have to add the thumbprint code in the vCLI, please going to the C:\Program Files (x86)\VMware\VMware vSphere CLI\Perl\apps\general directory.

First add the server IP:

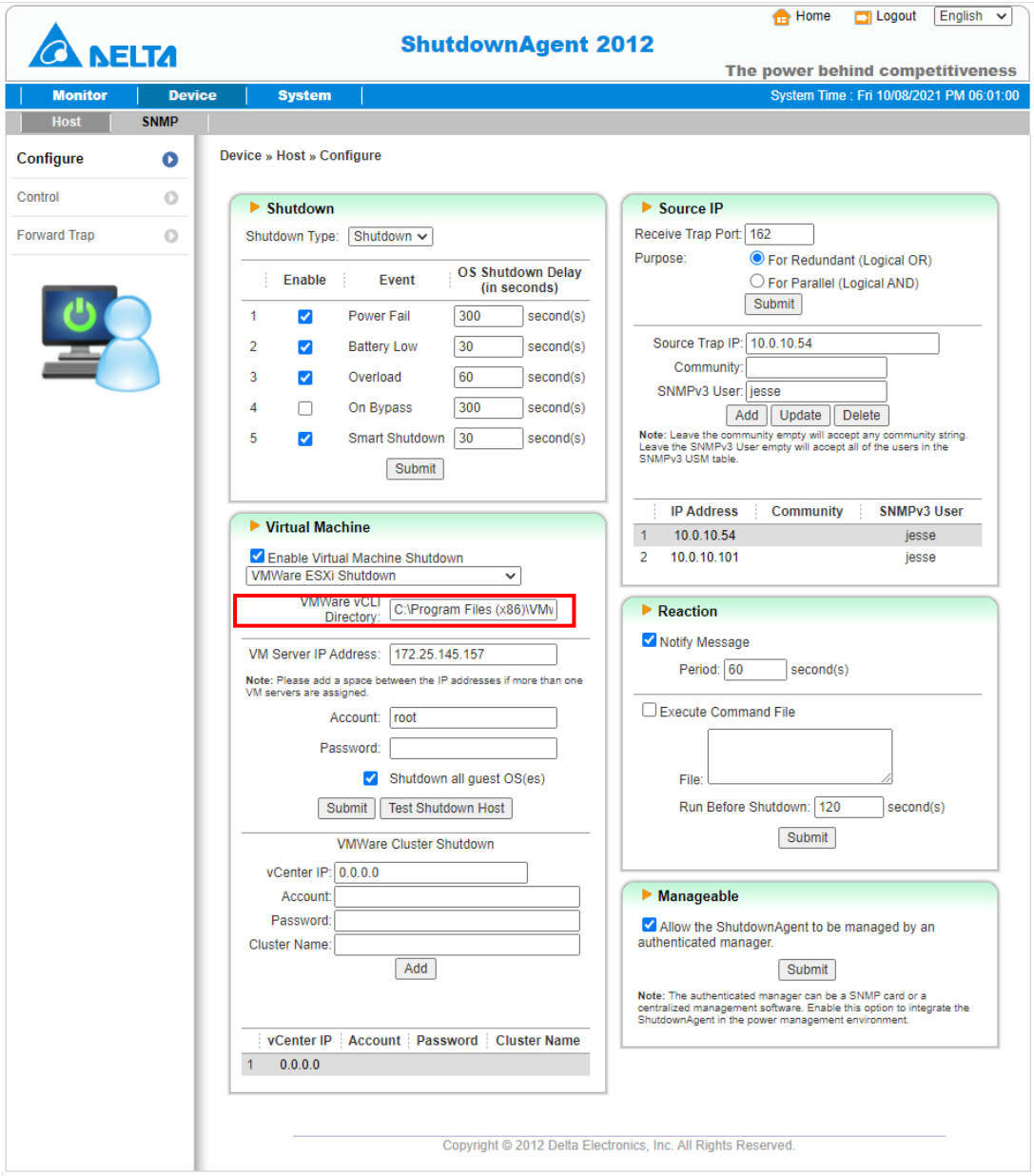
perl credstore_admin.pl add --server 10.0.10.107 –username root –password 2wsx@WSX

Then add the thumbprint:

perl credstore_admin.pl add --server 10.0.10.107 --thumbprint 04:82:AE:AE:67:C5:F6:DB:1D:0F:CE:5F:1A:92:34:4A:B9:EA:FE:CE

Continue to get the guest OS information to complete the test, Please test the ESXi hosts one by one.

4. The other configuration, please refer to the chapter 8, Windows edition requires to provide the Installation directory of VMWare vCLI.


Home
Logout
English
DELTA
ShutdownAgent 2012
The power behind competitiveness
Monitor
Device
System
System Time : Fri 10/08/2021 PM 06:01:00
Host
SNMP
Configure
Control
Forward Trap
Device » Host » Configure
Shutdown
Shutdown Type: Shutdown
Enable
Event
OS Shutdown Delay (in seconds)
1 Power Fail 300 second(s)
2 Battery Low 30 second(s)
3 Overload 60 second(s)
4 On Bypass 300 second(s)
5 Smart Shutdown 30 second(s)
Submit
Virtual Machine
Enable Virtual Machine Shutdown
VMWare ESXi Shutdown
VMWare vCLI Directory: C:\Program Files (x86)\VMv
VM Server IP Address: 172.25.145.157
Note: Please add a space between the IP addresses if more than one VM servers are assigned.
Account: root
Password:
Shutdown all guest OS(es)
Submit
Test Shutdown Host
VMWare Cluster Shutdown
vCenter IP: 0.0.0.0
Account:
Password:
Cluster Name:
Add
vCenter IP
Account
Password
Cluster Name
1 0.0.0.0
Source IP
Receive Trap Port: 162
Purpose:
For Redundant (Logical OR)
For Parallel (Logical AND)
Submit
Source Trap IP: 10.0.10.54
Community:
SNMPv3 User: jesse
Add
Update
Delete
Note: Leave the community empty will accept any community string. Leave the SNMPv3 User empty will accept all of the users in the SNMPv3 USM table.
IP Address
Community
SNMPv3 User
1 10.0.10.54 jesse
2 10.0.10.101 jesse
Reaction
Notify Message
Period: 60 second(s)
Execute Command File
File:
Run Before Shutdown: 120 second(s)
Submit
Manageable
Allow the ShutdownAgent to be managed by an authenticated manager.
Submit
Note: The authenticated manager can be a SNMP card or a centralized management software. Enable this option to integrate the ShutdownAgent in the power management environment.
Copyright © 2012 Delta Electronics, Inc. All Rights Reserved.

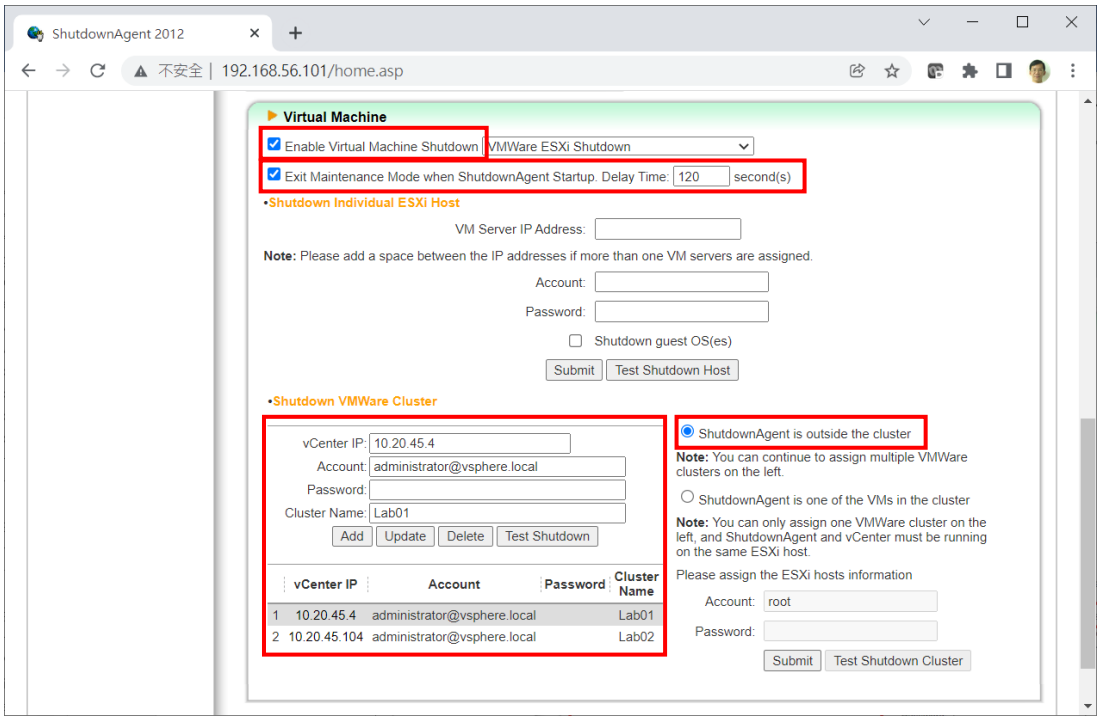
10. VMWare Cluster Shutdown

There are 2 scenarios: One is when ShutdownAgent and vCenter are installed outside the Cluster. The second is that ShutdownAgent and vCenter are installed on the virtual machines in a Cluster.

10.1 ShutdownAgent and vCenter are installed outside the Cluster

Since ShutdownAgent is independent of all clusters, it can perform a complete shutdown procedure for each cluster: First enter maintenance mode and then shut down.

1. Enable the "Enable Virtual Machine Shutdown" option.
2. Enable the "Exit Maintenance Mode when ShutdownAgent Startup".
3. Select the "ShutdownAgent is outside the cluster" option.
4. Input the vCenter IP, account, password and Cluster Name. ShutdownAgent can shutdown multiple set of clusters.

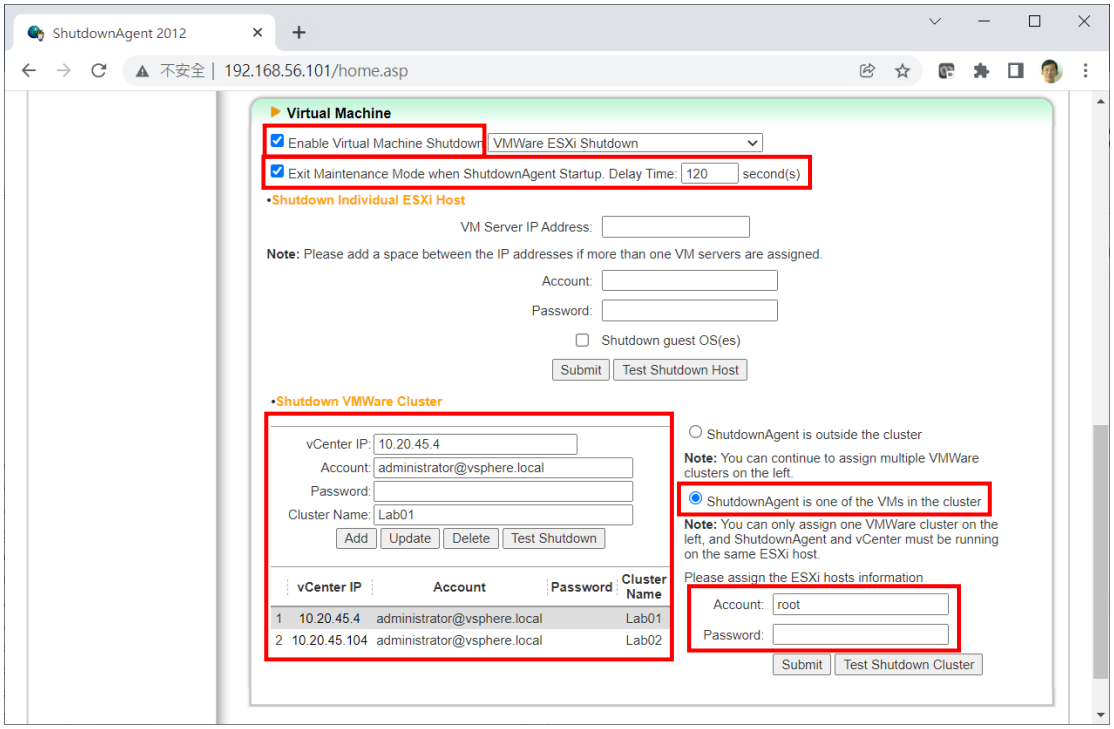


10.1 ShutdownAgent and vCenter are installed on the virtual machines in a Cluster

Note: In this application scenario, ShutdownAgent and vCenter must be running on the same ESXi host.

Since ShutdownAgent is running in the cluster, the ESXi host that is not running ShutdownAgent will be shut down first (enter maintenance mode then shut down), and then the remaining ESXi host will be forced to shut down and the vCenter and ShutdownAgent virtual machines will be shut down at the same time.

1. Enable the "Enable Virtual Machine Shutdown" option.
2. Enable the "Exit Maintenance Mode when ShutdownAgent Startup".
3. Select the "ShutdownAgent is one of the VMs in the cluster" option。
4. Enter the login account and password of the ESXi host that executes ShutdownAgent and vCenter
5. Enter the first set of vCenter IP, account, and password. In this application scenario, only one group of clusters can be shutdown, so only the information provided by the first group is used.



11. Quickly deploy ShutdownAgent with vCLI OVA file

Deploying ShutdownAgent in OVA mode is the fastest and most effective way. With Delta pre-made OVA file, customers can quickly start vCLI guest OS and execute ShutdownAgent. Since this vCLI is executed on the ESXi host, this method cannot be used to shut down the Cluster host but can perform the task of simply shutting down the ESXi host.

11.1 Download the pre-made OVA file

Please go to Delta website to download the vCLI OVA file containing the ShutdownAgent.

https://datacenter-softwarecenter.deltaww.com.cn > UPS > Software > ShutdownAgent 2012 > vCLI 6.0.0 or vCLI 6.7.0 file.

Unzip after download, the file name should be a .ova file.

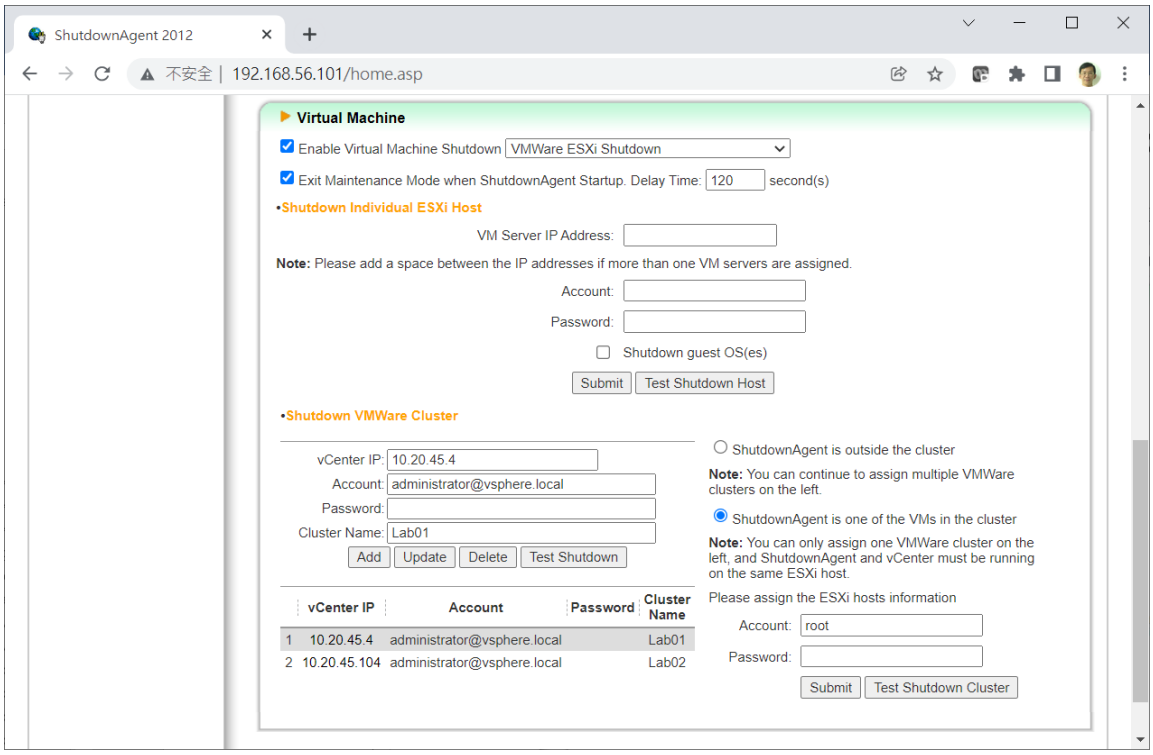
11.2 Import the OVA file to the ESXi host

1. In the vSphere Client, click on the file menu and choose to deploy the OVF template. Follow the prompts to select the unzipped OVA file to complete the deployment. At this time, the guest OS of uXXXX_saXXXX_vcli will appear.
2. Select the guest OS, then power on this guest OS.
3. The default IP address is dynamic, the account is delta and the password is 2wsx@WSX.
4. Please modify the IP address to a static, reboot this vCLI guest to apply the new settings.

11.3 Connect to the ShutdownAgent in vCLI

Please find a client PC and open the web browser. Enter the vCLI IP address to connect. After entering the default ShutdownAgent account and password, go to the Device> Host> Configure page.

Please follow the instructions to set the SNMP card and source IP address and other parameters.



The followings are the Virtual Machine options.

- VMWare ESXi Maintenance and Shutdown: Used for the ESXi host to enter the maintenance mode then shutdown. If ShutdownAgent is running on one of the VMs of the ESXi host, please select this option to shutdown.
- VMWare ESXi Shutdown: Used to force shutdown the ESXi hosts.
- VMWare ESXi v4: Used to shutdown the ESXi version 4. (Please ignore the "Exit Maintnenance Mode" option).
- Xen Server: Used to shutdown the Xen server. (Please ignore the "Exit Maintnenance Mode" option).
- Linux KVM: Used to shutdown the KVM server. (Please ignore the "Exit Maintnenance Mode" option).

12. XenServer Setup for ShutdownAgent

To install the ShutdownAgent in theCitrix XenServer, please see 2.2 For Linux in chapter 2 Installation/ Uninstallation.

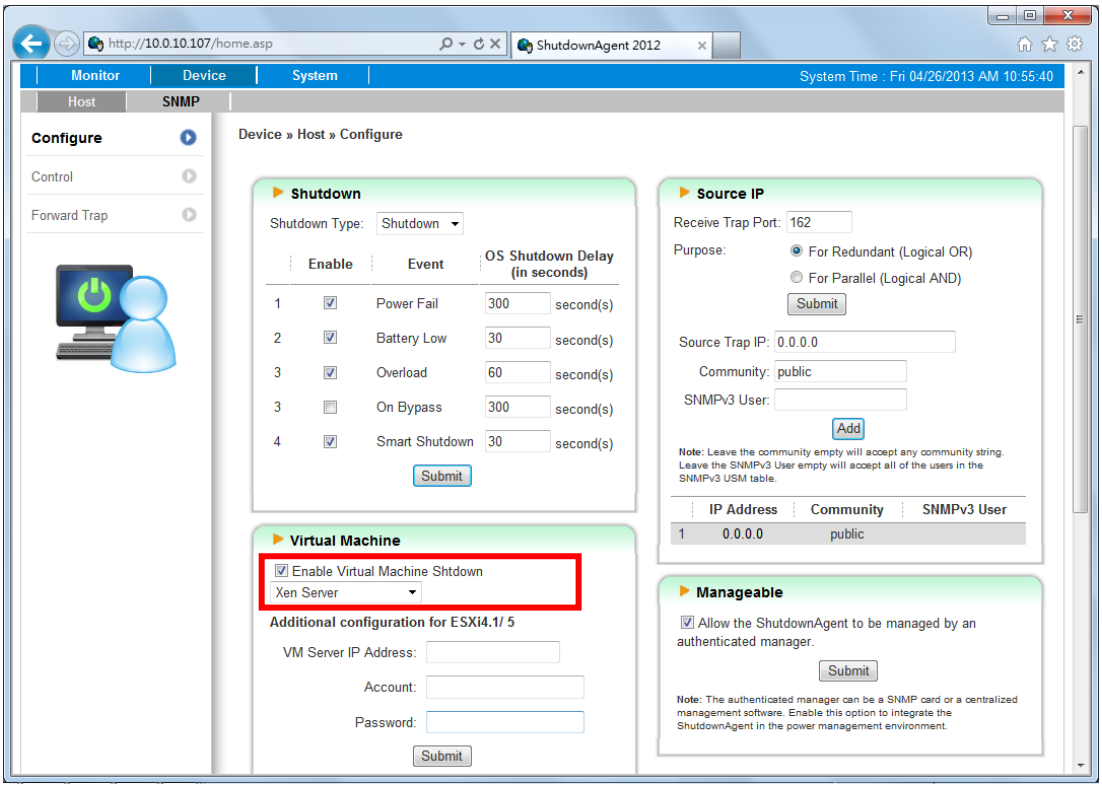
To configure the basic networking parameters including the Xen firewall, please see chapter 3 Console Configuration.

12.1 Install PV driver for Guest OS

To shutdown the guest OS from XenServer, you need to install the PV driver for all of them so as to inform the guest OSes shutdown smoothly.

12.2 Configure ShutdownAgent for Xen

1. Login to the web interface of ShutdownAgent and the account level should greater than or equal to device manager.
2. Goto the Device → Host → Configure web page to enable the **Enable Virtual Machine Shutdown** checkbox then select the **Xen Server** option.



3. Press **Submit** button to update your changes.

13. Linux KVM Setup for ShutdownAgent

To install the ShutdownAgent in the Linux server, please see 2.2 For Linux in chapter 2 Installation/ Uninstallation.

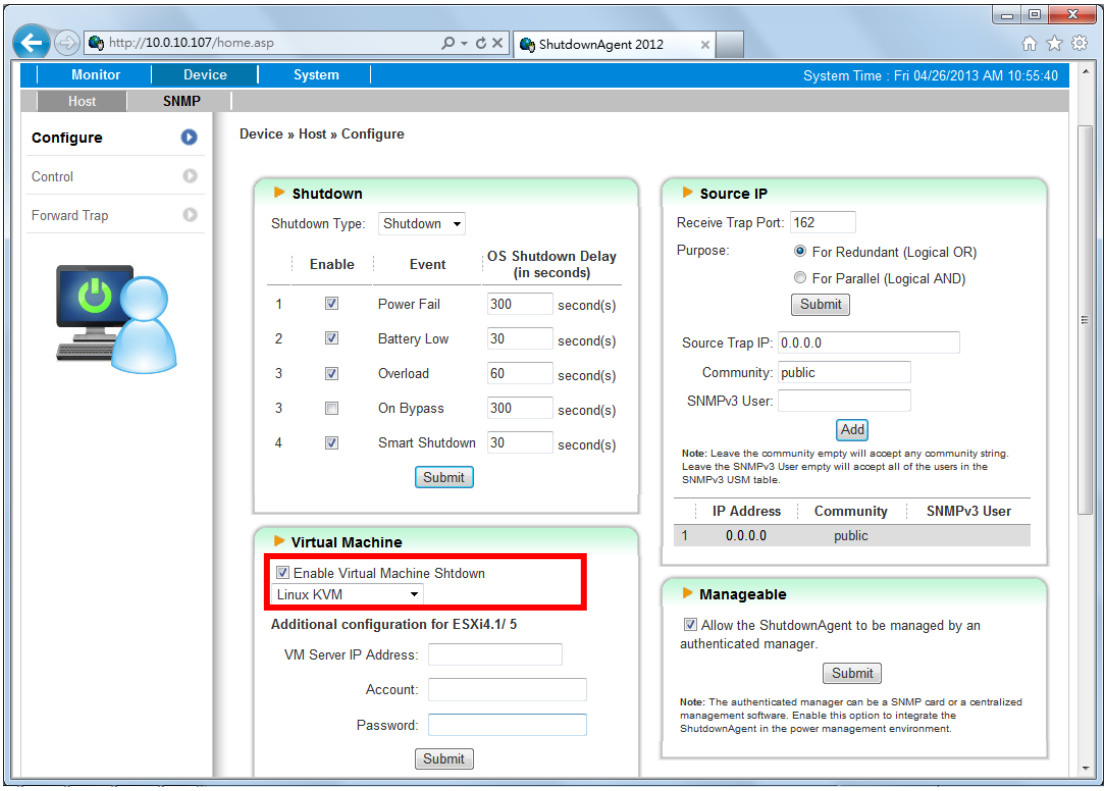
To configure the basic networking parameters including the firewall, please see chapter 3 Console Configuration.

13.1 Install libvirt Tools for KVM

To shutdown the guest OS from Linux server, you have to install the libvirt. ShutdownAgent calls the virsh to shutdown the running guest OSes.

13.2 Configure ShutdownAgent for KVM

1. Login to the web interface of ShutdownAgent and the account level should greater than or equal to device manager.
2. Goto the Device → Host → Configure web page to enable the **Enable Virtual Machine Shutdown** checkbox then select the **Linux KVM** option.



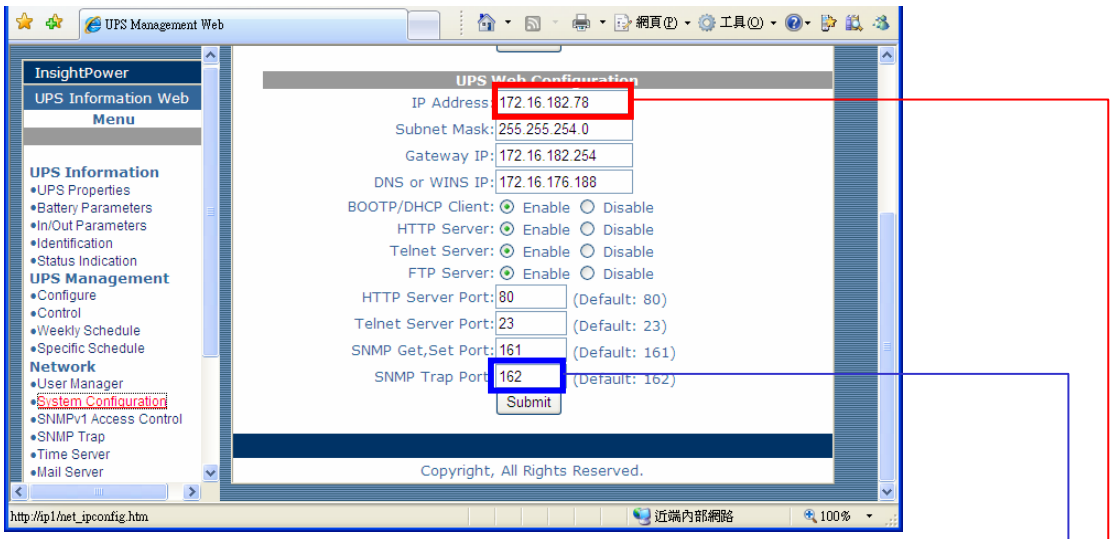
3. Press **Submit** button to update your changes.

14. Work with the SNMP Card

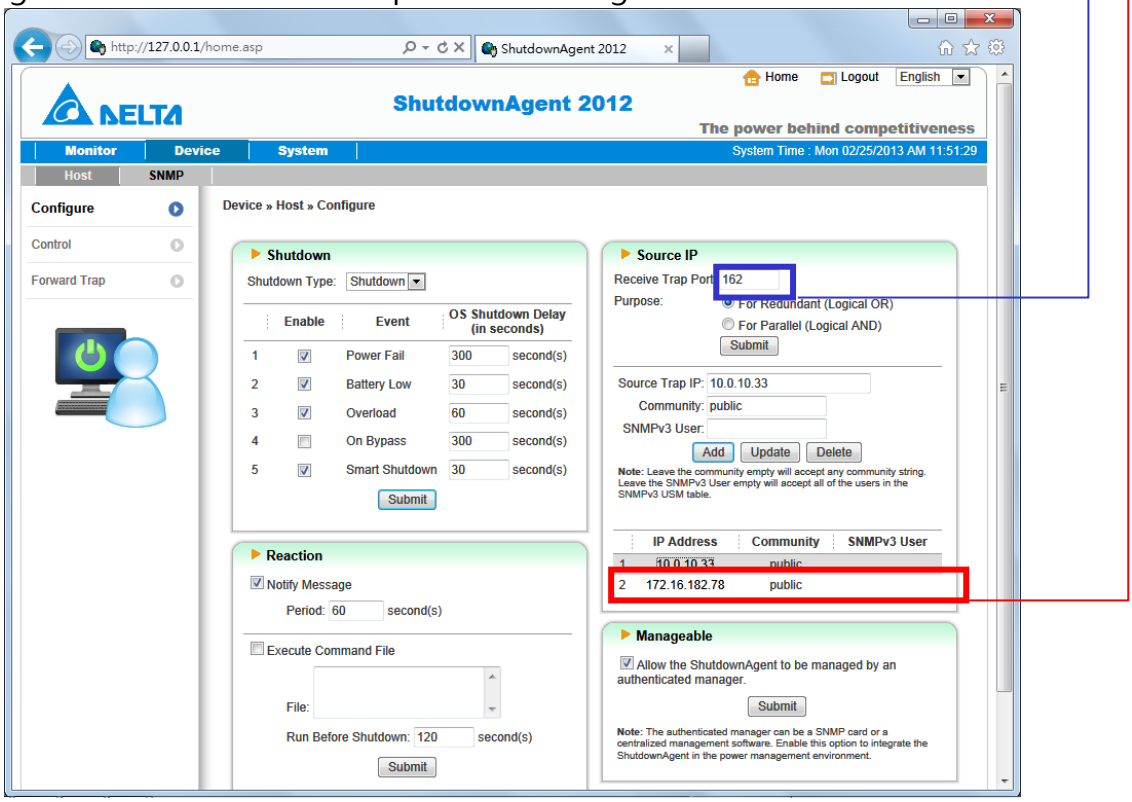
14.1 Legacy Delta InsightPower SNMP Card

1. Open a web browser and connect to the InsightPower SNMP Card.

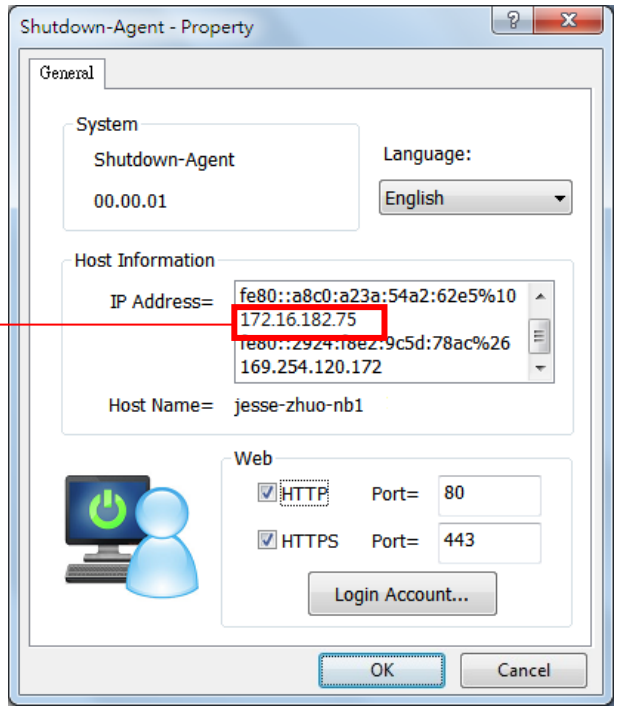
2. Record the IP address and SNMP Trap Port in the System Configuration web page.



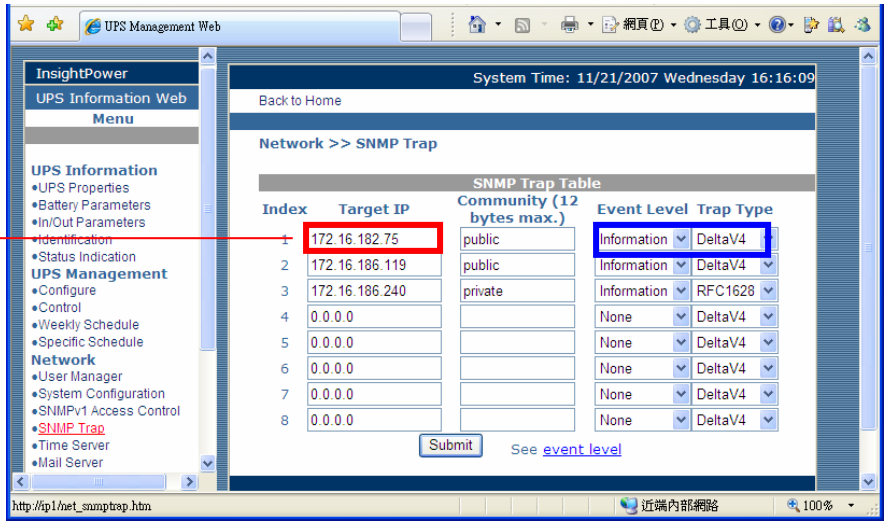
3. Add the SNMP IP address and the trap port to the ShutdownAgent as the following to receive the SNMP trap from the InsightPower SNMP Card.



4. Get the ShutdownAgent ip address form the property dialog box.



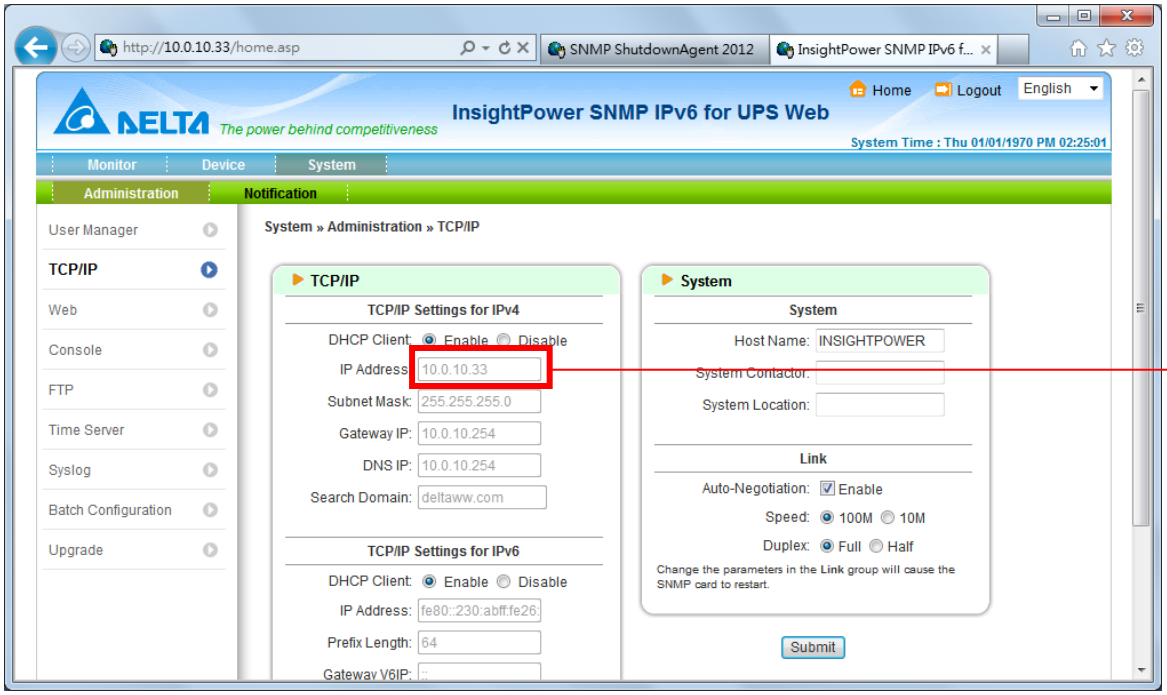
5. Add the ShutdownAgent ip address to the SNMP Trap table in the InsightPower SNMP Card. Please select the "Information" for the Event Level and DeltaV4 as the Trap MIB Type.



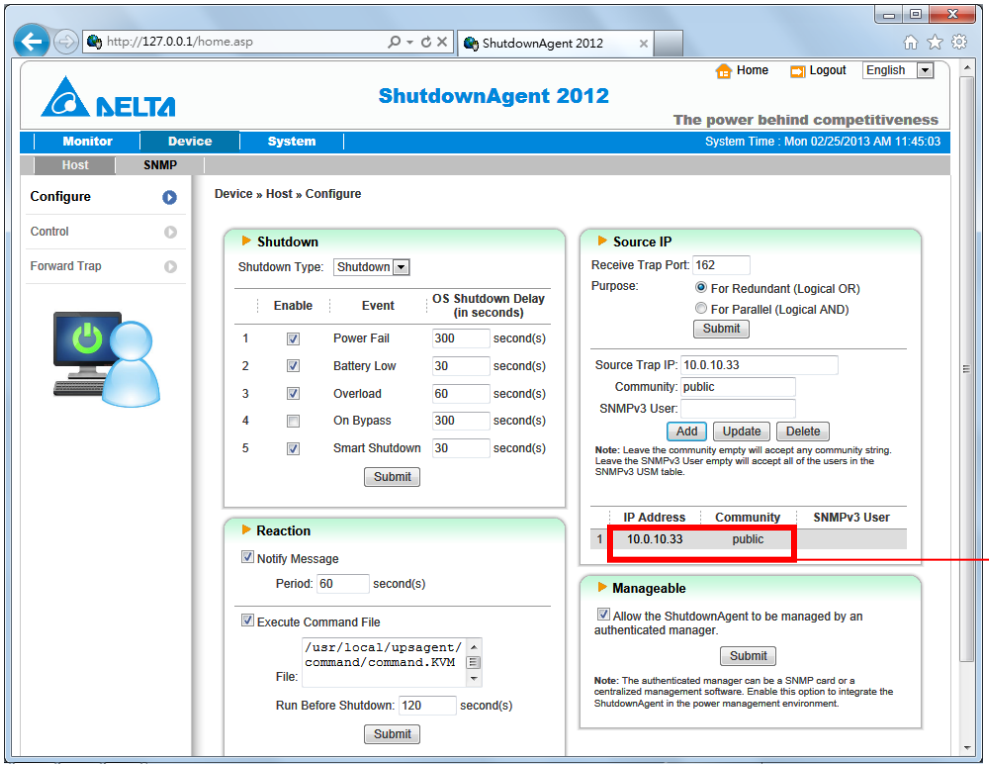
14.2 Delta InsightPower SNMP IPv6 Card

1. Open a web browser and connect to the InsightPower SNMP IPv6 Card.

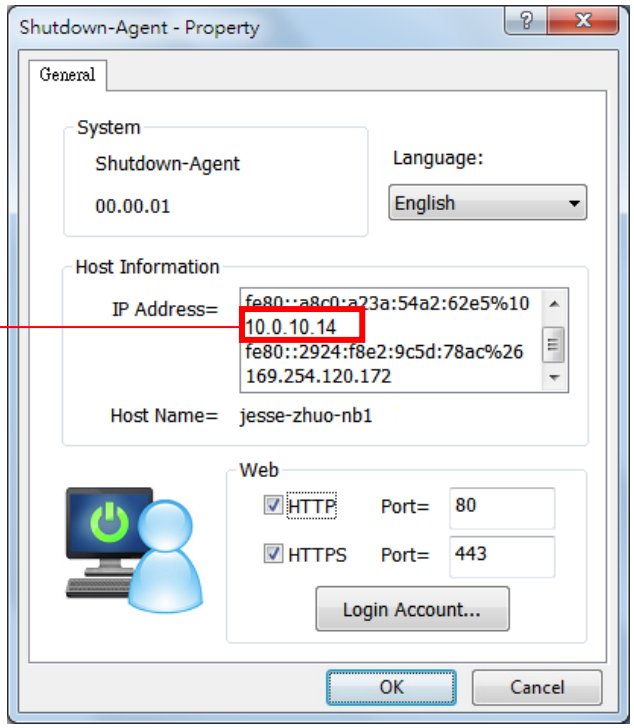
2. Record the IP address in the System Configuration web page. The SNMP Trap is assigned in the SNMP Trap web page individually.



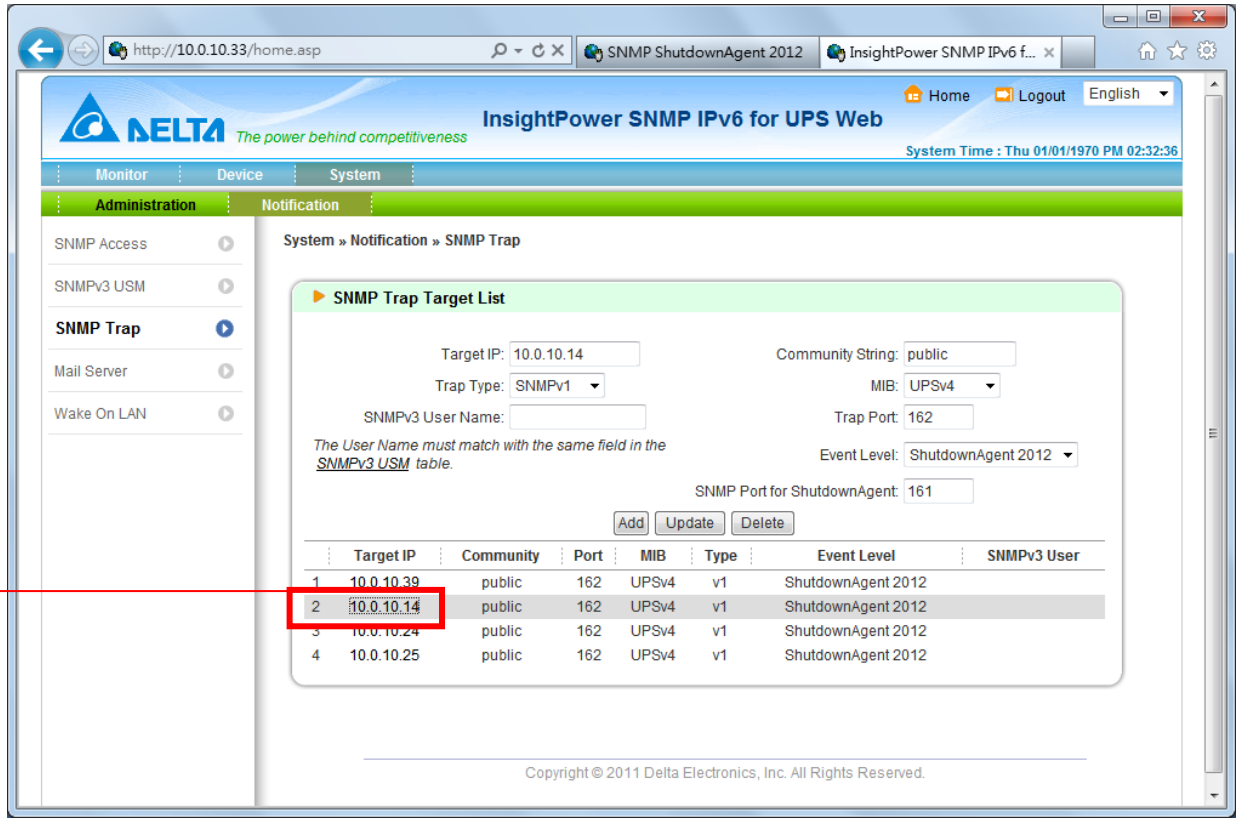
3. Login to the ShutdownAgent web and add the SNMP IP address and the trap port as the following to receive the SNMP trap from the SNMP Card.



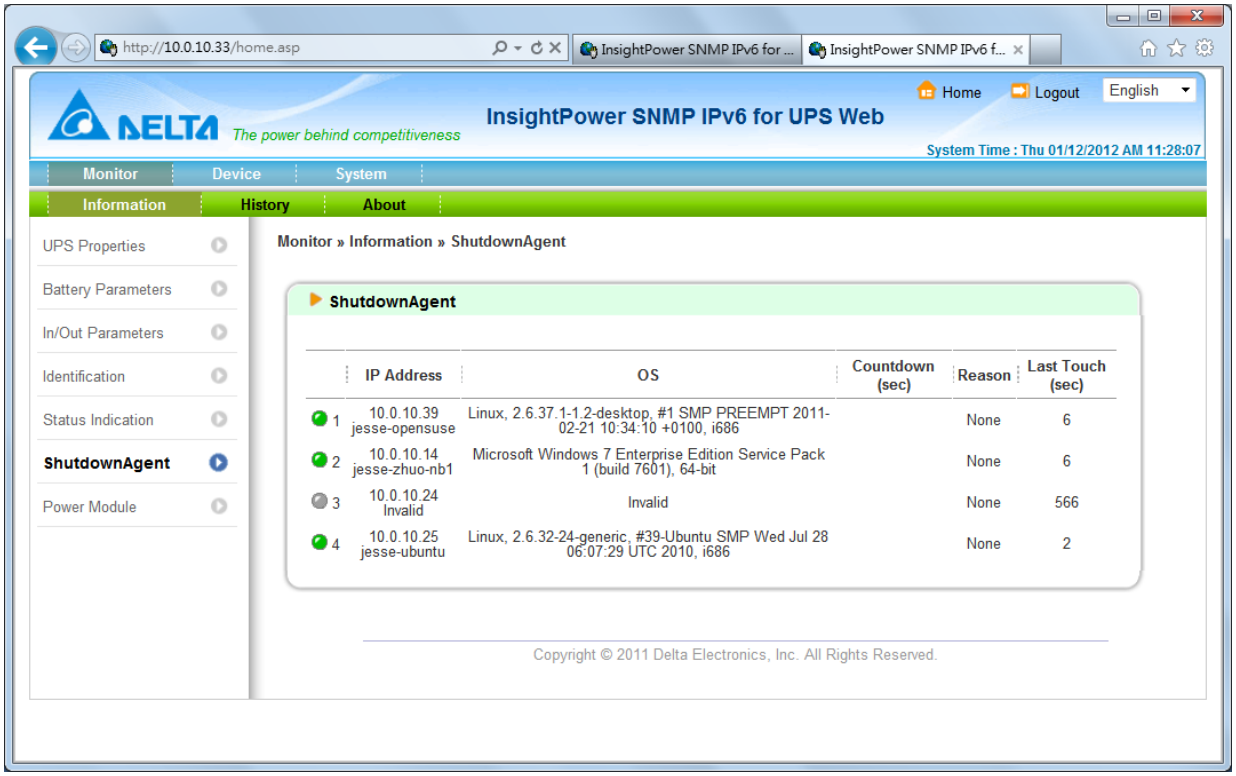
4. Open the ShutdownAgent property from Windows task bar to get the IP address of the server.



5. Back to the InsightPower SNMP IPv6 card web page, add the IP address of ShutdownAgent to the SNMP Trap table. Please select the "ShutdownAgent 2012" for the Event Level and UPSV4 or UPSv5 as the Trap MIB.



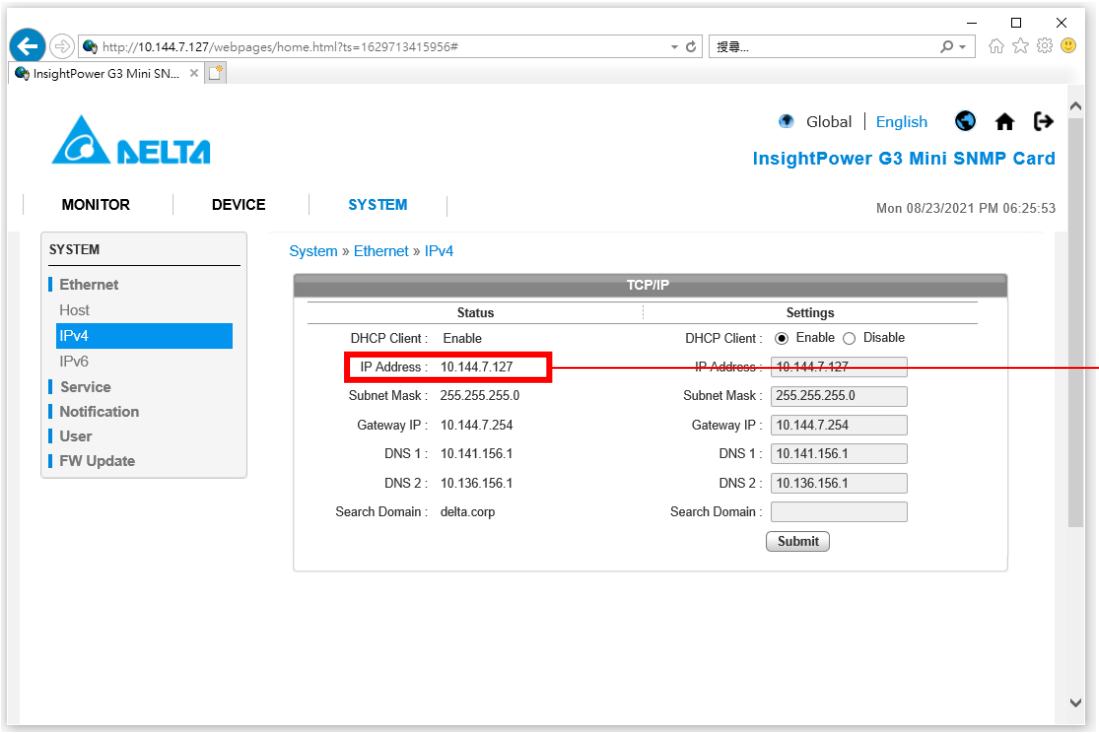
6. If you enable the manageable option in the ShutdownAgent then you can observe all of the shutdown status, countdown timer and shutdown reason from the InsightPower SNMP IPv6 card. The web page is on the Monitor >> Information >> ShutdownAgent.



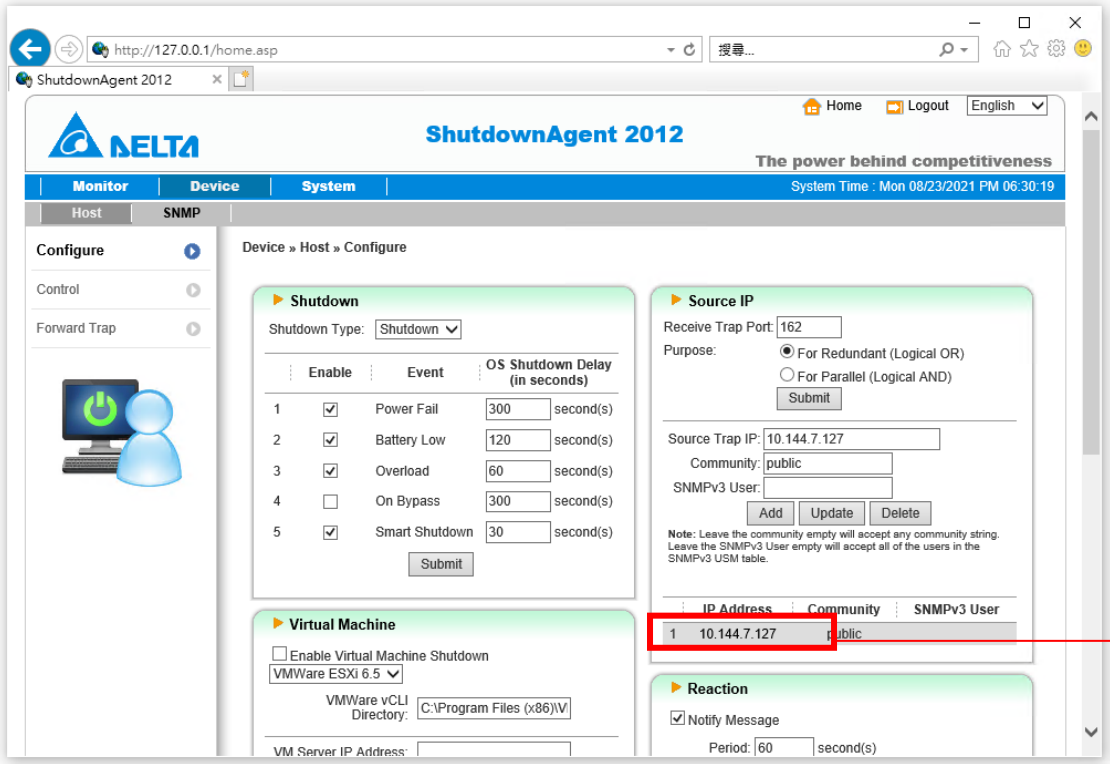
14.3 New Delta InsightPower G3 Mini SNMP Card

1. Open a web browser and connect to the InsightPower G3 Mini SNMP Card.

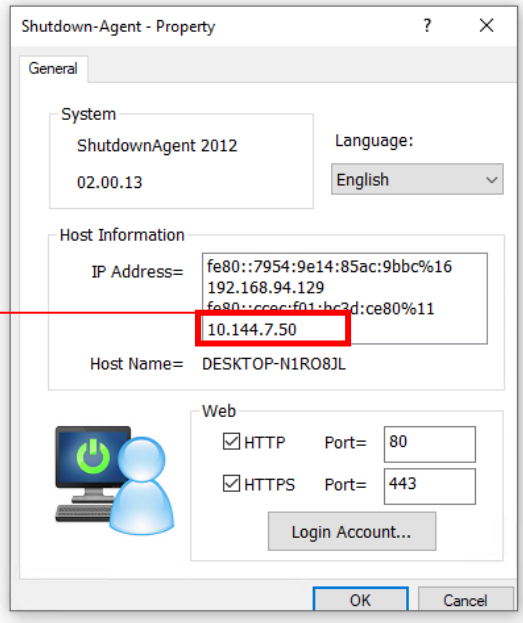
2. Record the IP address in the System Configuration web page. The SNMP Trap is assigned in the SNMP Trap web page individually.



3. Login to the ShutdownAgent web and add the SNMP IP address and the trap port as the following to receive the SNMP trap from the SNMP Card.



4. Open the ShutdownAgent property from Windows task bar to get the IP address of the server. Or find the OS IP address which the ShutdownAgent installed.



4. Back to the InsightPower G3 Mini SNMP card web page, add the IP address of ShutdownAgent to the SNMP Trap table.
   Please select the "ShutdownAgent 2012" for the Event Level and UPSV4 or UPSv5 as the Trap MIB.