ShutdownAgent 2012

User Manual

Doc. Version 02.09
Date: 1/11/2024

About this manual

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

Please 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 2

1.1 Features 3
1.2 Supported OS 3

2. Installation/ Uninstallation 4

2.1 For Windows System 4
2.1.1 Installation Process 4
2.1.2 Uninstallation Process 7
2.2 For Linux System 8
2.2.1 Installation Process 8
2.2.2 Uninstallation Process 9
2.3 For IBM AIX System 9

3. Console Configuration 10

3.1 Console Menu 10

4. Operation in Windows 12

4.1 Web Monitor 12
4.2 Property 12
4.3 Show Countdown 15
4.4 Cancel Countdown 15
4.5 Stop Service 15

5. Web Interface 16

5.1 Run a Web Browser 16
5.2 Monitor >> Information >> Summary 17
5.3 Monitor >> Information >> Event Log 18
5.4 Monitor >> Information >> Log Configure 19
5.5 Device >> Host >> Configure 19
5.6 Device >> Host >> Control 25
5.7 Device >> Host >> Forward Trap 25
5.8 Device >> SNMP >> SNMP Access 26
5.9 Device >> SNMP >> SNMPv3 USM 26
5.10 System >> Administration >> Information 27
5.11 System >> Administration >> Login User 28
5.12 System >> Administration >> Web 29
5.13 System >> Administration >> Batch Configuration 31

6. 2008 Server Core Setup for ShutdownAgent 32

7. VMWare ESXi 4.0 Setup for ShutdownAgent 34

7.1 Configure the Firewall for ESXi 4.0 34
7.2 Install VMware Tools for Guest OS 34
7.3 Configure ShutdownAgent for ESXi4.0 35

8. VMWare ESXi 4.1/ 5/ 6 Setup for ShutdownAgent 36

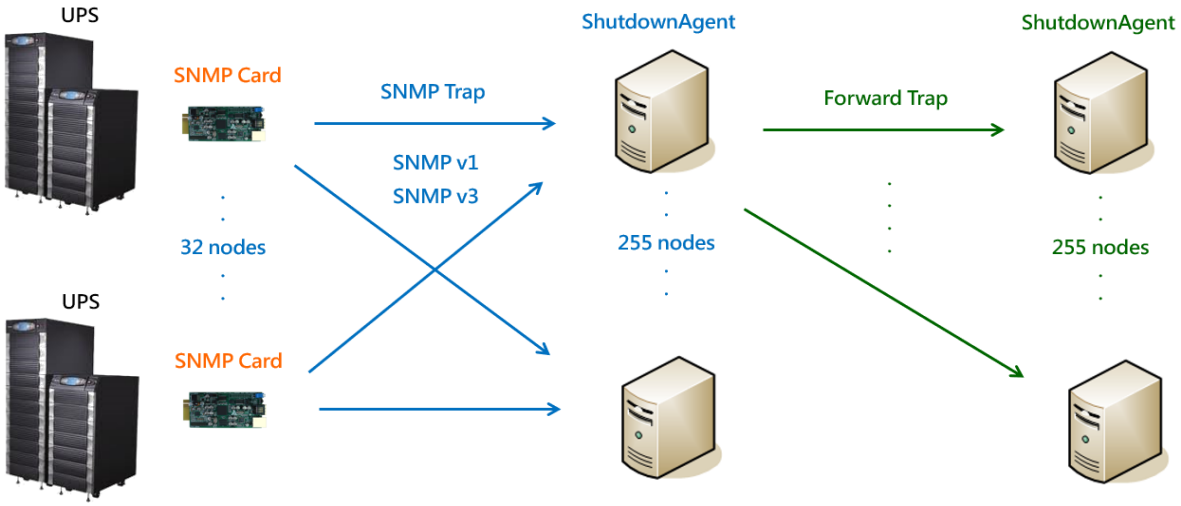
8.1 Configure the Firewall for vMA 36

8.2 Install VMware Tools for Guest OS 37
8.3 Configure ShutdownAgent for ESXi4.1/ 5/ 6..... 37
9. ShutdownAgent Shutdown VMWare ESXi 6.5 and Above . 39
9.1 ShutdownAgent Linux Edition..... 39
9.1.1 Test the esxcli command 39
9.2 ShutdownAgent Windows Edition..... 41
9.2.1 Add the Windows shutdownagent account..... 41
9.2.2 Install VMWare vCLI 42
10. VMWare vCenter Shutdown 45
10.1 Shutdown Individual ESXi Host 45
10.1.1 VMWare ESXi Maintenance and Shutdown 45
10.1.2 VMWare ESXi Shutdown 46
10.1.3 VMWare ESXi v4 46
10.2 VMWare vCenter Shutdown Instructions..... 47
10.2.1 Shutdown Steps..... 48
11. Shutdown Scenarios..... 49
11.1 Power Supply from One UPS 49
11.1.1 Configure 49
11.2 UPS Power Supply in Parallel 50
11.2.1 Configure 50
11.3 UPS Redundant Power Supply 51
11.3.1 Configuration 51
11.4 ESXi Host Shutdown Scenarios 52
11.4.1 ShutdownAgent Runs Outside the ESXi Host 52
11.4.2 ShutdownAgent Runs Inside ESXi Host..... 53
11.5 vCenter Shutdown Scenarios 54
11.5.1 ShutdownAgent Runs Outside vCenter..... 54
11.5.2 ShutdownAgent Runs Inside vCenter 56
12. Quickly deploy ShutdownAgent with vCLI OVA file..... 58
12.1 Download the pre-made OVA file 58
12.2 Import the OVA file to the ESXi host 58
12.3 Connect to ShutdownAgent in vCLI..... 58
13. XenServer Setup for ShutdownAgent 61
13.1 Install PV driver for Guest OS 61
13.2 Configure ShutdownAgent for Xen 61
14. Linux KVM Setup for ShutdownAgent..... 62
14.1 Install libvirt Tools for KVM 62
14.2 Configure ShutdownAgent for KVM..... 62
15. Work with the SNMP Card 63
15.1 Legacy Delta InsightPower SNMP Card..... 63
15.2 Delta InsightPower SNMP IPv6 Card 65
15.3 New Delta InsightPower G3 Mini SNMP Card..... 68

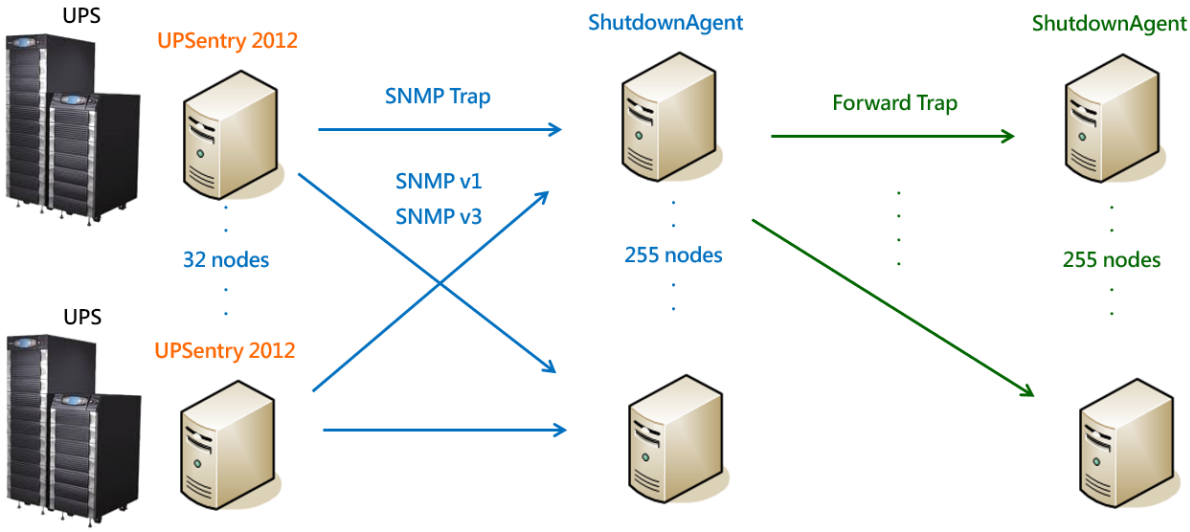
1. Overview

ShutdownAgent 2012 is a software that protects your operating system during input power fail. UPS provides stable power supply for your operating system. However, when power fail occurs, the UPS can only supply the output load for a period of time with battery power. It is required for you to plan and configure the settings of the software. With simply a Web Browser, you can easily view the current UPS events, shutdown strategy and countdown to shutdown information.

The following picture shows that the SNMP trap can be sent by SNMP card and forwarded to other ShutdownAgent that is installed on other servers.



The SNMP Trap sent by UPSentry 2012 can also be received and forwarded.



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 with HTTP and HTTPS.
4. Provide batch configuration that makes it easier to deploy.
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 Supported OS

Windows 7, 8, 10, 11
Windows Server 2012, 2016, 2019, 2022
Windows Hyper-V Server Core 2016/2019
Redhat Linux Exterprise 6.8, 7.7, 8.3, 9.0
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, 7.5, 8 (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

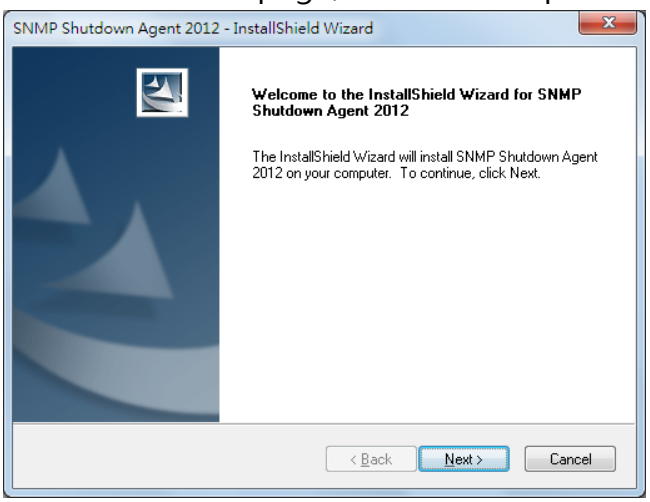
There are 2 setup programs: ShutdownAgent-2012-Setup(win32).exe and ShutdownAgent-2012-Setup(x64).exe. These are designed for different processors of servers.

Before the installation, please log in to the Windows account with local administrator privilege.

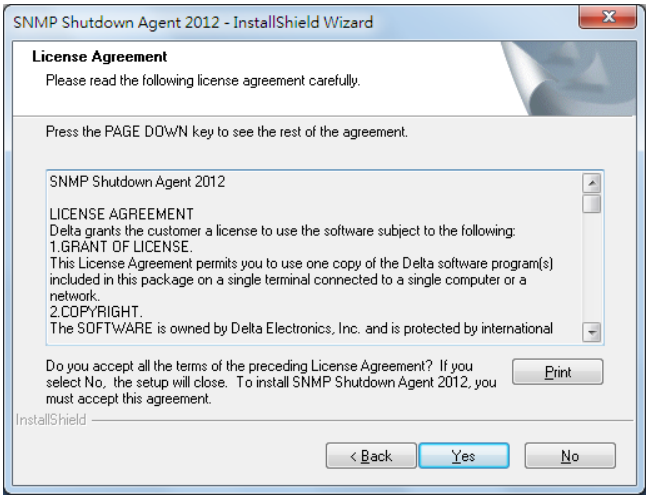
2.1.1 Installation Process

Execute ShutdownAgent-2012-Setup(xxx).exe to run the setup program.

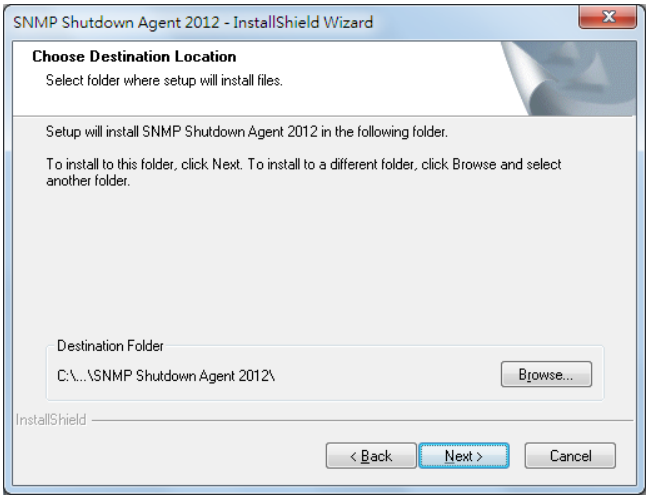
On the welcome page, click **Next** to proceed.



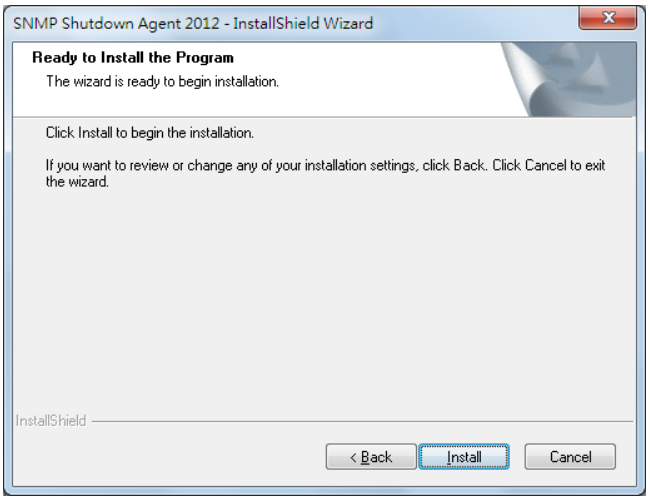
On the license agreement page, click **Yes** to proceed.



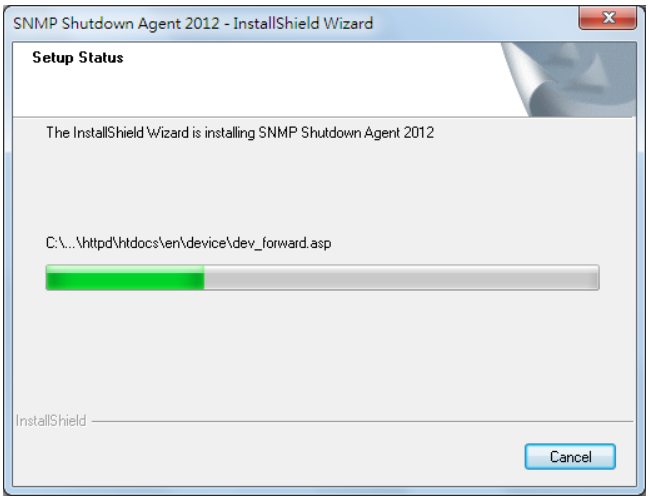
At this step, you can click Browse to change the destination location, or just click **Next** to install the software in the default path.



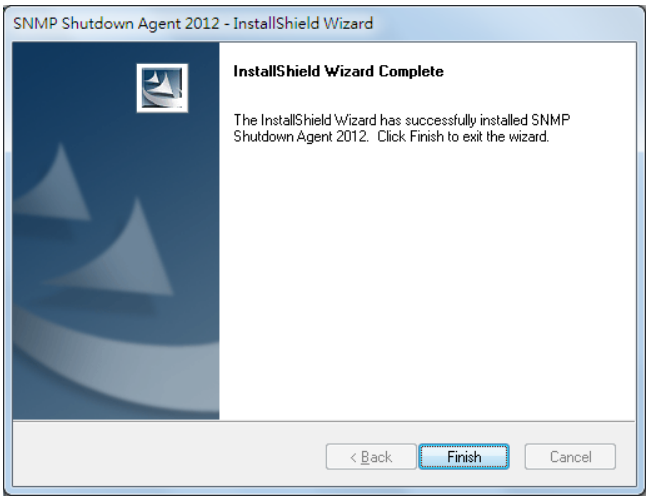
Now the setup program is ready for your confirmation to start copying the related program files. Click **Install** to start installation of the software.



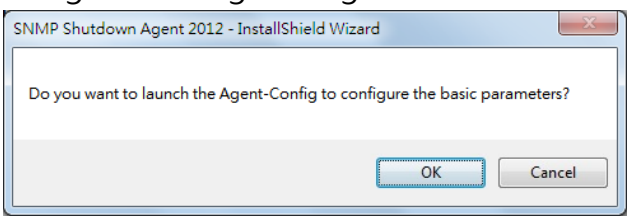
Now the setup program is copying files.



Click **Finish** to exit the installation process.



When the installation is complete, ShutdownAgent will start the service program automatically and add a status icon in the desktop tool bar. Meanwhile, a dialog box will be popped up asking for launching the Agent-Config application. If you are not using a Windows server core operating system, please ignore it. Just press **No** to finish the installation. Press **Yes** to launch the Agent-Config in the shell mode. Please refer to Chapter 3 for details of Agent-Config settings.



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 the installation is complete, 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.

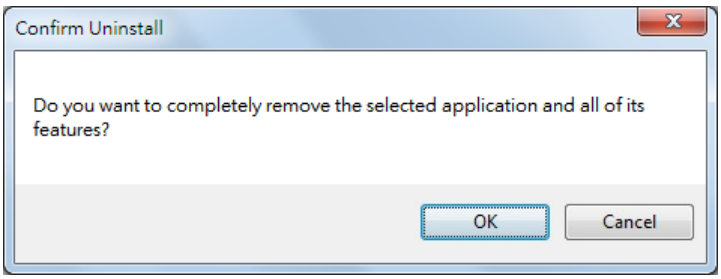
Uninstall: To remove the **SNMP ShutdownAgent 2012** from your hard disk, the configuration data will still be kept in the installed directory.

User Manual: The user manual in pdf format.

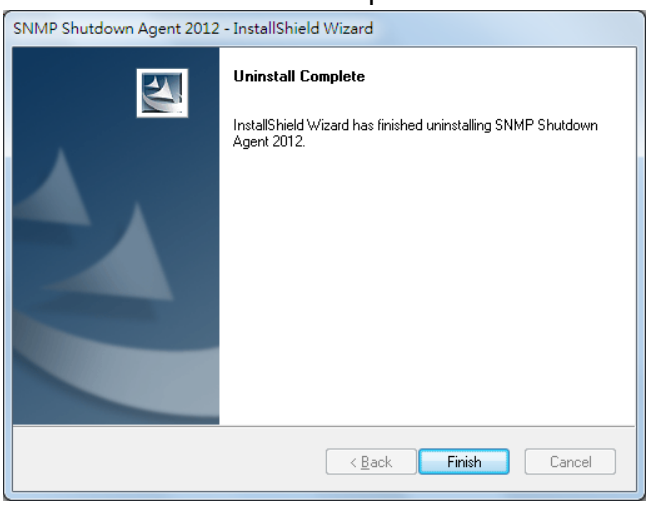
Web Monitor: The major user interface of **ShutdownAgent**, used to monitor and configure the software.

2.1.2 Uninstallation Process

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



3. Click **Finish** to complete the uninstallation 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 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

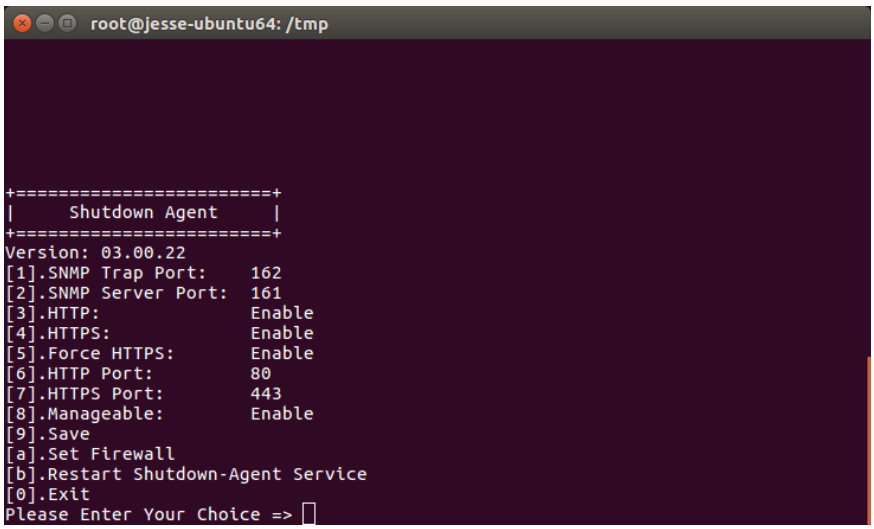
Both of the installation and uninstallation are the same with Linux system, please refer to the section 2.2.

3. Console Configuration

The configuration program is designed to configure ShutdownAgent in the shell mode. The software can be launched immediately when the installation process is complete. You can also go to the installation directory to launch it manually.

For Windows OS, it is located in `C:\Program Files\SNMP Shutdown Agent 2012\Agent-Config.exe`

For Linux system, 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.	Force HTTPS	Force login via HTTPS	Enable
6.	HTTP Port	The TCP port for HTTP	80
7.	HTTPS Port	The TCP port for HTTPS	443
8.	Manageable	Allow the management software to manage ShutdownAgent	Enable
9.	Save	Save the configured parameters to agent.ini	
a.	Set Firewall	Insert or remove the firewall rule for ShutdownAgent. This option is provided for	

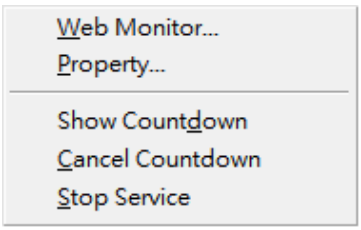
		quickly testing the network communication. The firewall settings may be recovered after the OS reboots.	
b.	Restart Shutdown-Agent Service	Restart service program to apply the changes	
0.	Exit	Exit the configuration program	

4. Operation in Windows

When the installation is complete, an icon in the desktop toolbar will be appeared to indicate the status of the monitored 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 ShutdownAgent icon and click the mouse button to pop up the menu:



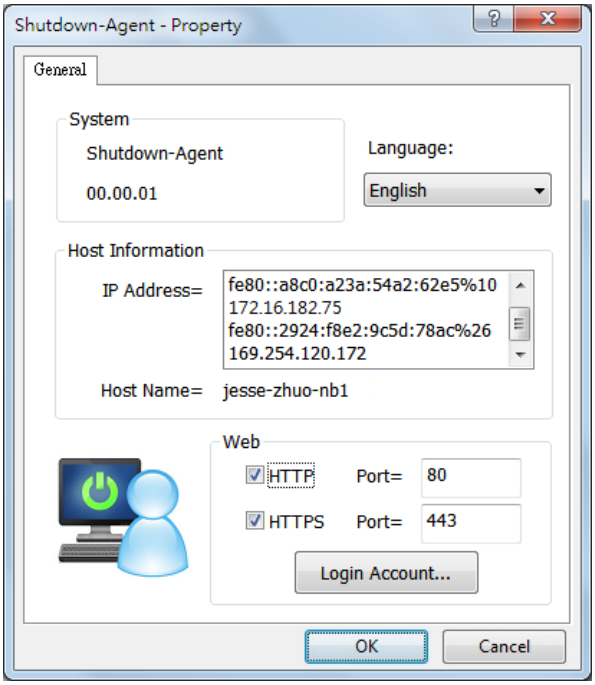
4.1 Web Monitor

ShutdownAgent implements a web engine to provide web interface to interact with end users. You can monitor and configure the software through the web interface. Select **Web Monitor** from the menu to launch your web browser, if your login account in the Windows system belongs to the local Administrators group, ShutdownAgent will login to its web engine automatically with administrator privilege. If you log in from a remote PC, you have to key in the account and password.

For more detail information about Web Monitor, please refer to Chapter 5.

4.2 Property

Select **Property** from the menu, a Property dialog box will be popped up that provides another quick way to configure basic parameters of ShutdownAgent. You can see 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 settings 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 port 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:

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

Administrator:

Has sole right to modify ShutdownAgent system settings.

Device Manager:

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

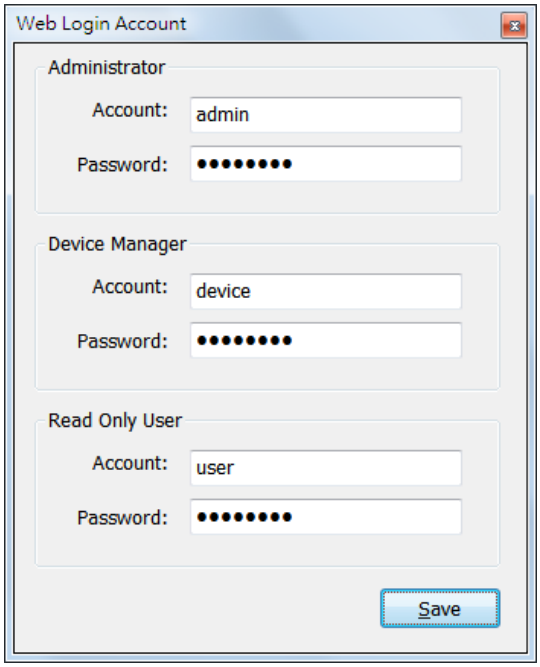
Read Only User:

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

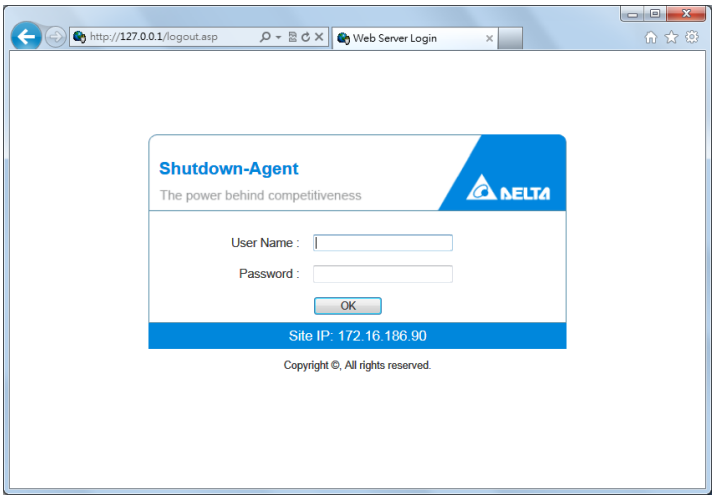
5. Web Interface

5.1 Run a Web Browser

To login Web Monitor with browser from the OS where ShutdownAgent is installed, select **Web Monitor** from the toolbar menu, ShutdownAgent will open your default web browser for login. If your Windows account belongs to local Administrators group, ShutdownAgent will login as an administrator for you automatically. ShutdownAgent allows up to 16 users login at the same time.

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

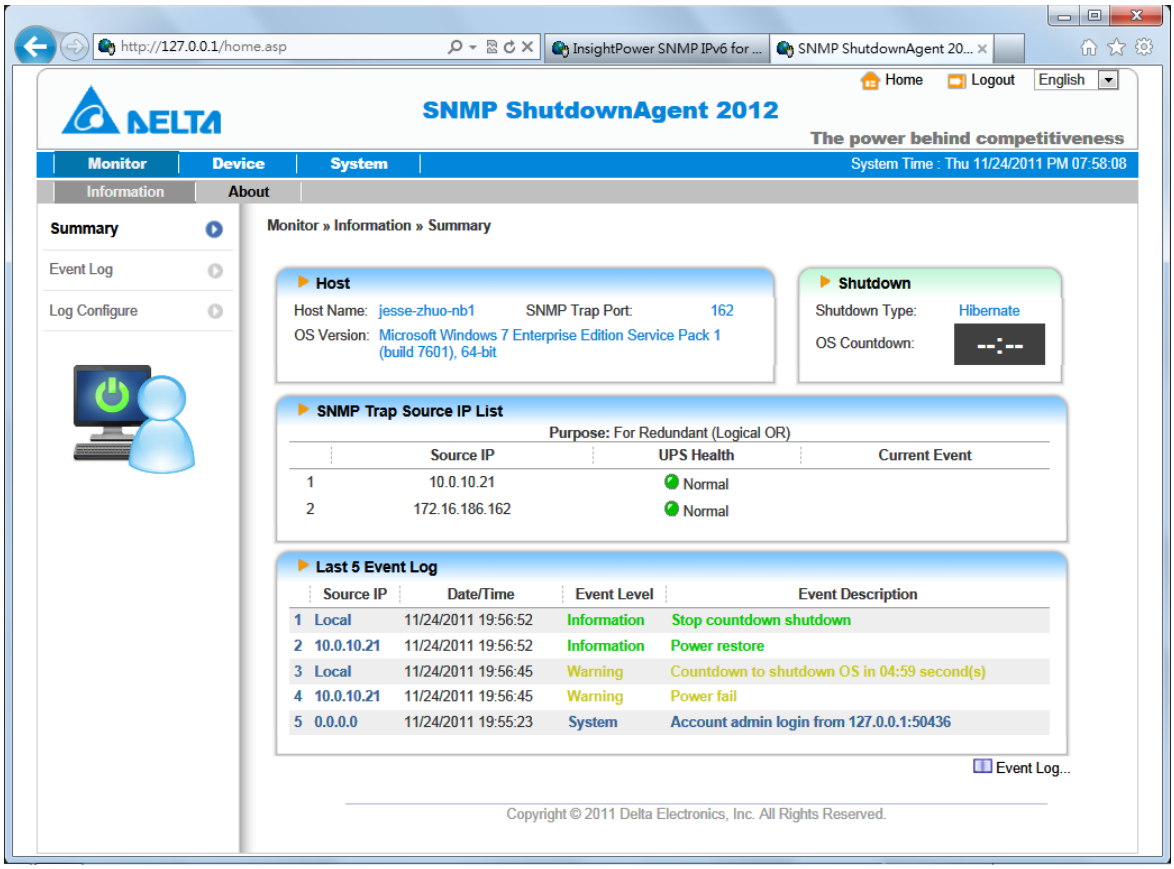
1. Make sure that you have a **TCP/IP** network installed.
2. Open your web browser. Enter `http://host_name` or `http://ip_address` in the address bar for the plain text web transmission or `https: //host_name` or `https: //ip_address` for the encrypted web transmission. If you have changed the port 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
3. Input your account and password for login. ShutdownAgent **Home Page** will appear on the screen when your account is successfully logged in.



Note: 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 shut down 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 Logs:

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:

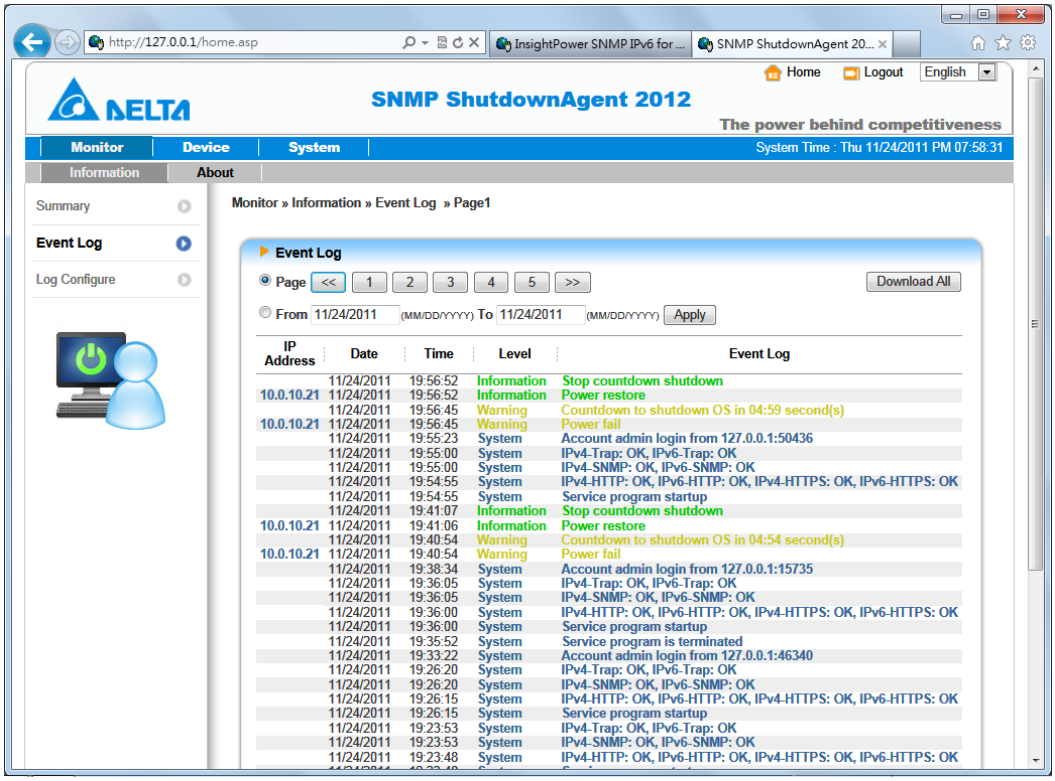
Press the "<<" button to go to the newest page and the ">>" button to go to the oldest page. Click on the page number buttons to observe the event log by page.

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 logs.

Clear Event Log:

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

5.5 Device >> Host >> Configure

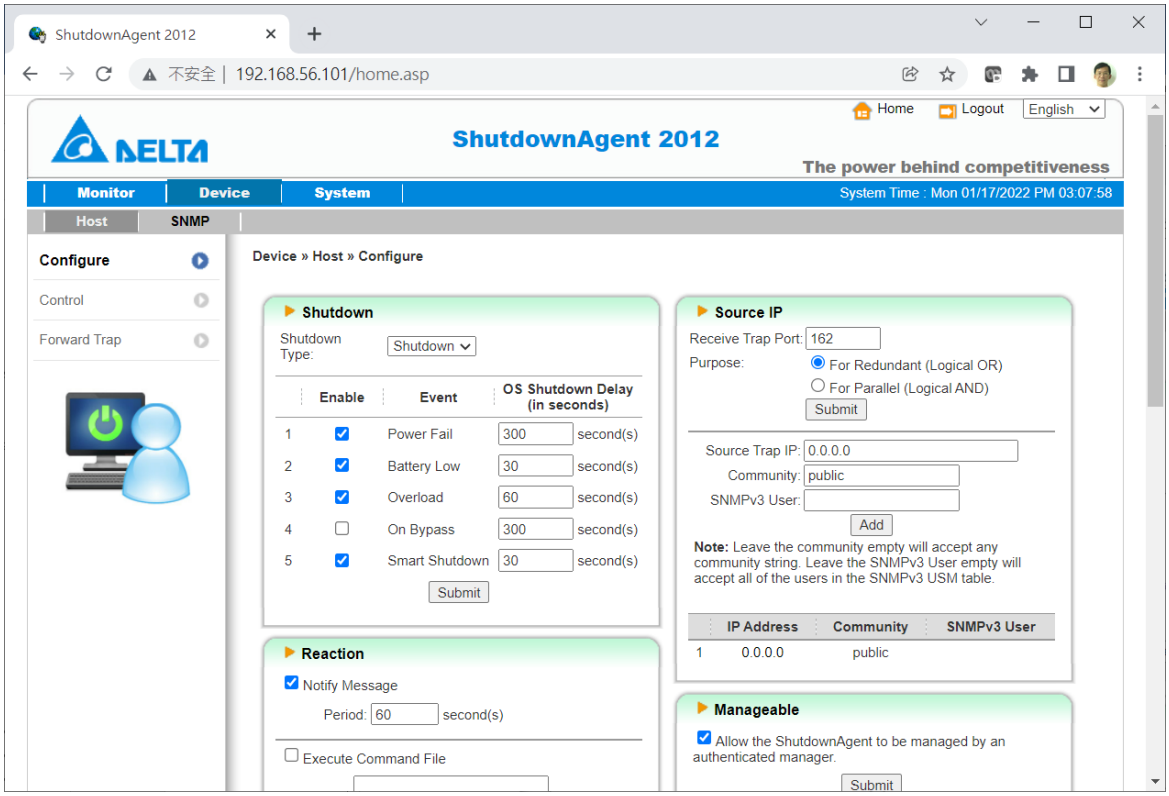
This page is used to configure the major functions, they are: Shutdown, Reaction and Source IP.

Shutdown:

Select the **Shutdown Type** to determine the way to shut down 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 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 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.

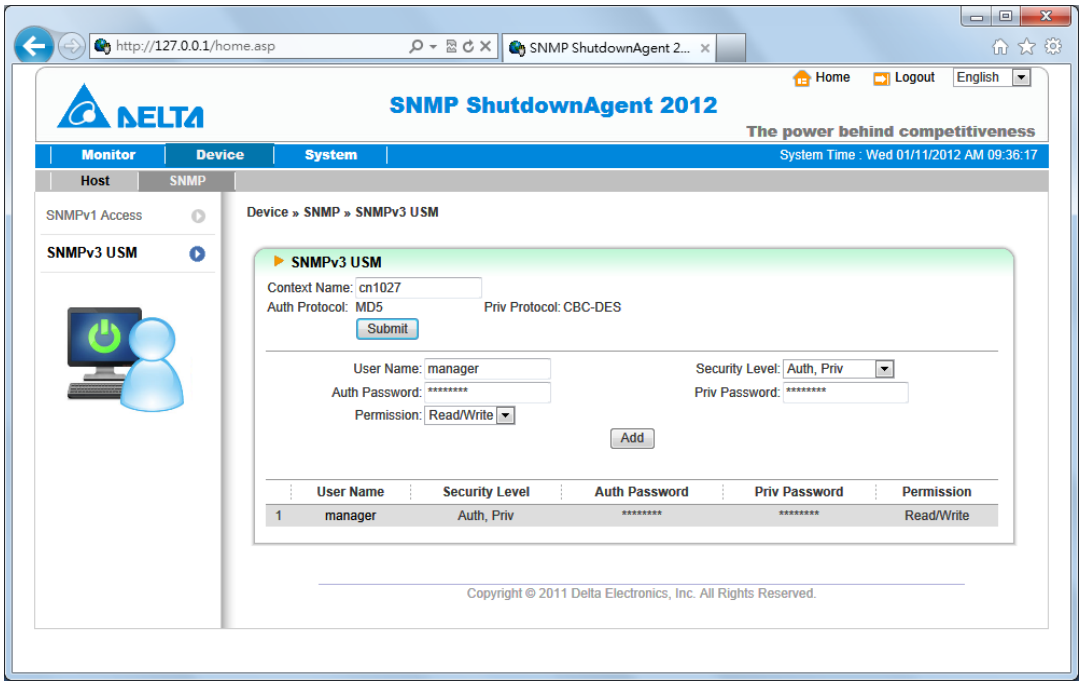
Community: If the value is not empty then only the received trap with the same community string will be accepted. If the value is empty then ShutdownAgent will accept any of the received community string.

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:

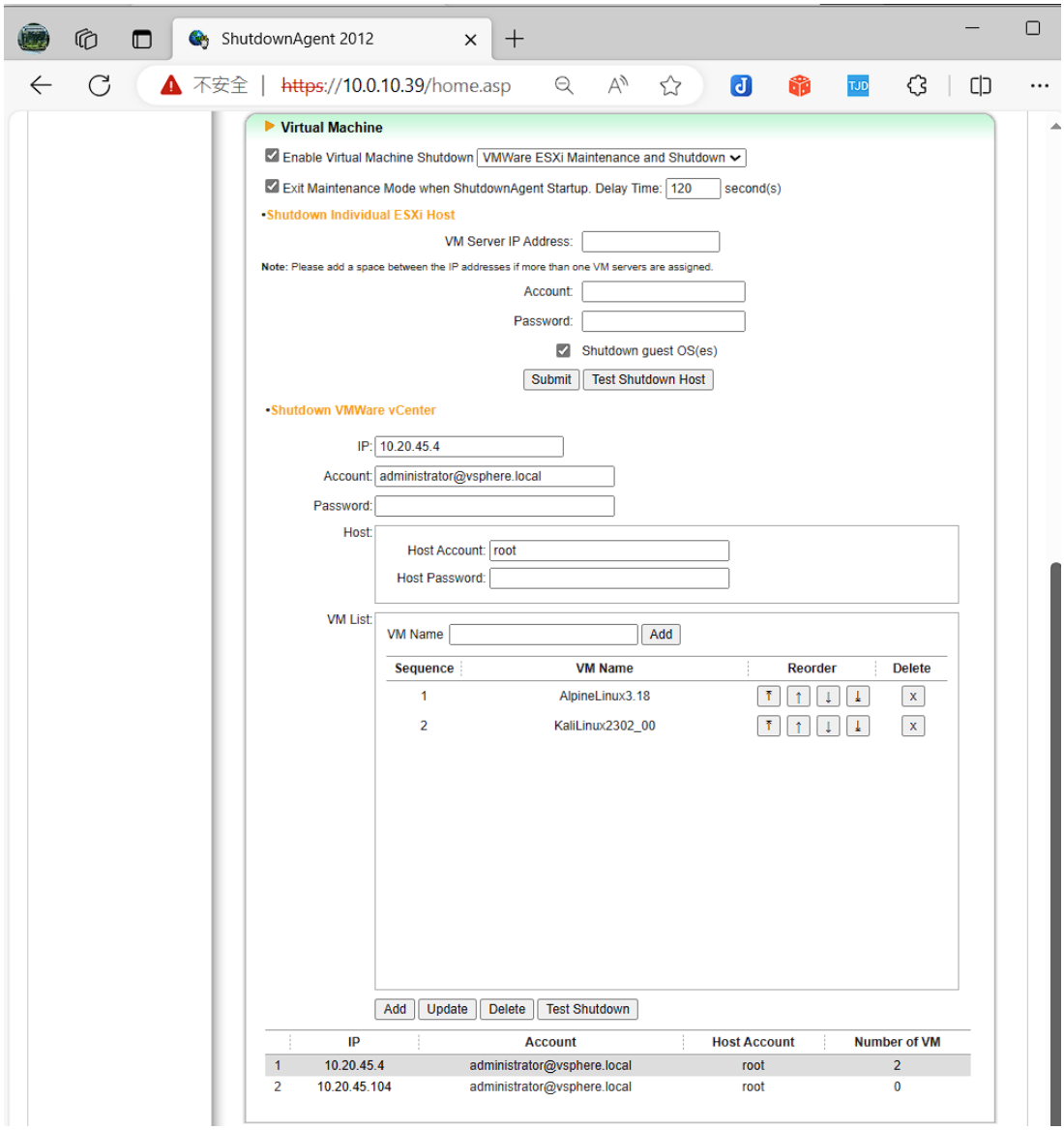
Select the **Allow ShutdownAgent to be managed by an authenticated manager** option to let ShutdownAgent reply the query from any authenticated manager. The authenticated manager can be a SNMP card or a centralized management software. After collecting ShutdownAgent information, the authenticated manager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



In fact, the authenticated manager communicate with ShutdownAgent through SNMPv3 with the first default account in the SNMPv3 USM list. If the **Allow 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 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 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 shut down the ESXi host.

VMWare ESXi v4: Shut down 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 vCenter

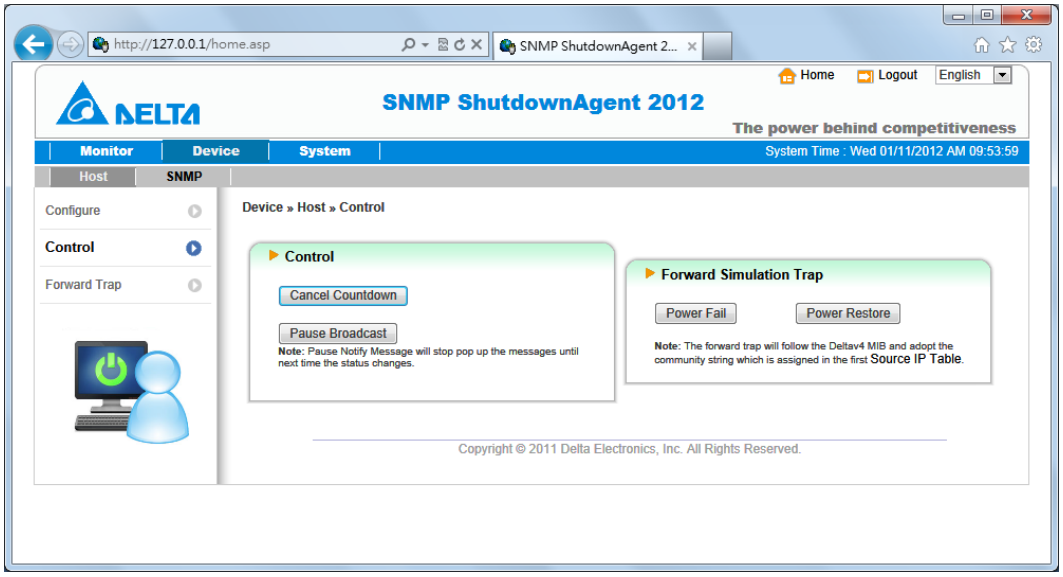
vCenter IP: IP address of vCenter.

vCenter Account, Password: vCenter account and password.

ESXi Host Account, Password: Please unify multiple hosts into one account and password.

VM List: VM name shutdown sequence list.

5.6 Device >> Host >> Control



Control:

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

If you enable **Notify Message** function from **Device>>Host>>Configure**, a popup message window will notify the user after receiving a power event. Press the **Pause Broadcast** button to stop message notifications.

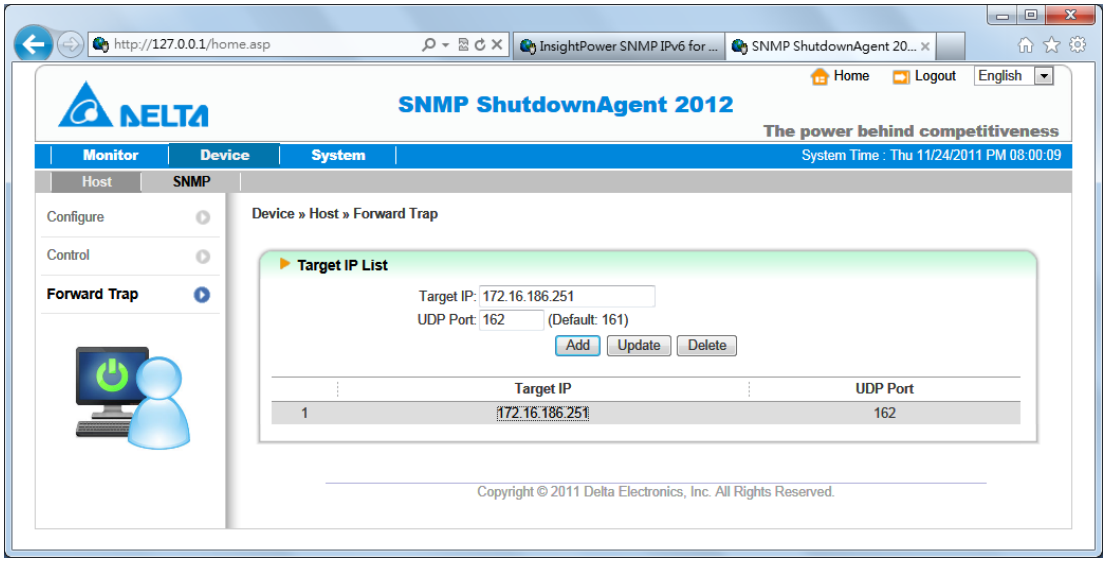
Forward Simulation Trap:

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 function is used to forward the received SNMP trap to extend the size of protection OS shutdown gracefully. The original SNMP Trap is sent by the SNMP IPv6 card, but when the number of servers to be shut down exceeds the maximum number of 255 SNMP IPv6 cards, this mechanism can be used to continue to expand.



5.8 Device >> SNMP >> SNMP Access

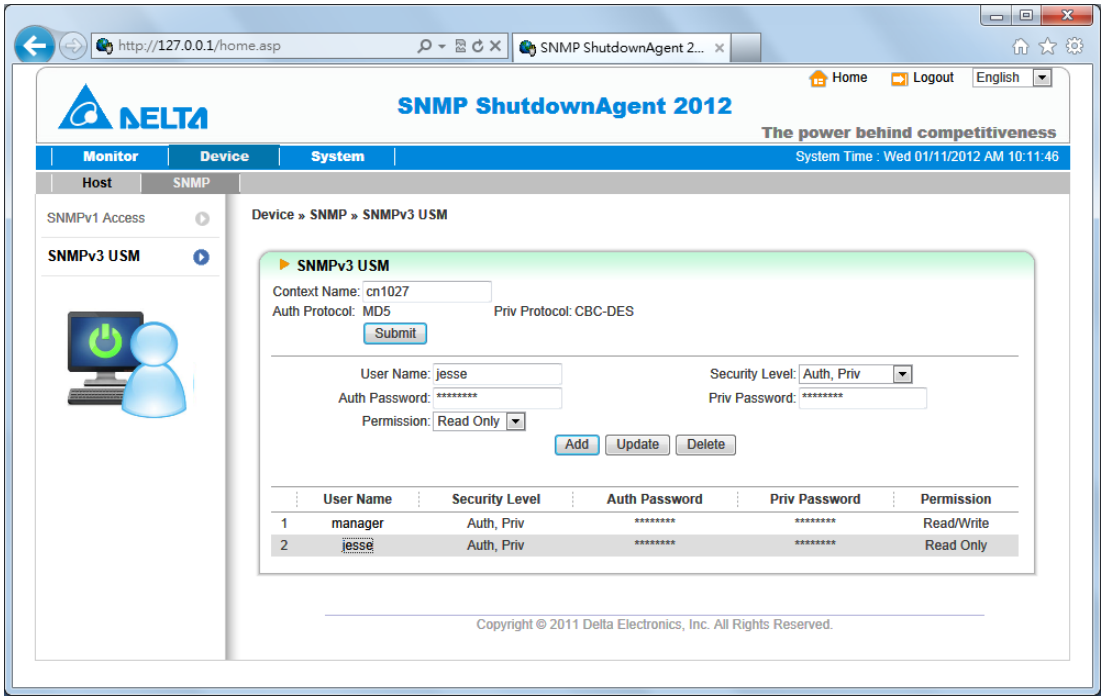
ShutdownAgent supports SNMP protocol and SNMP NMS (Network Management System), which are commonly used to monitor network devices for conditions that call for administrative attention. To prevent unauthorized access, you can specify the NMS IP addresses that are allowed to access, their community strings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

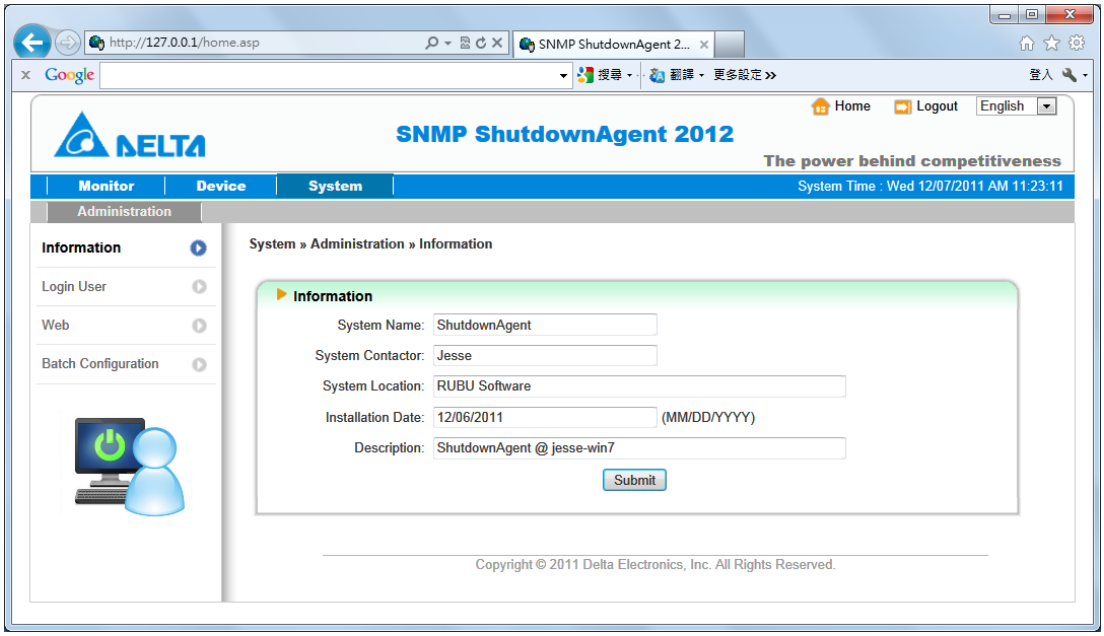
assign 32 User Names whose access is granted via SNMPv3 protocol. You can also define their respective Security Levels, Auth Passwords, Priv Passwords and Permission.

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

System information including Installation Date, Location and Description can be recorded here.



5.11 System >> Administration >> Login User

You can manage the login authentication for web interface by assigning 3 different level of user’ s account and password.

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

Administrator: Permitted to modify all settings.

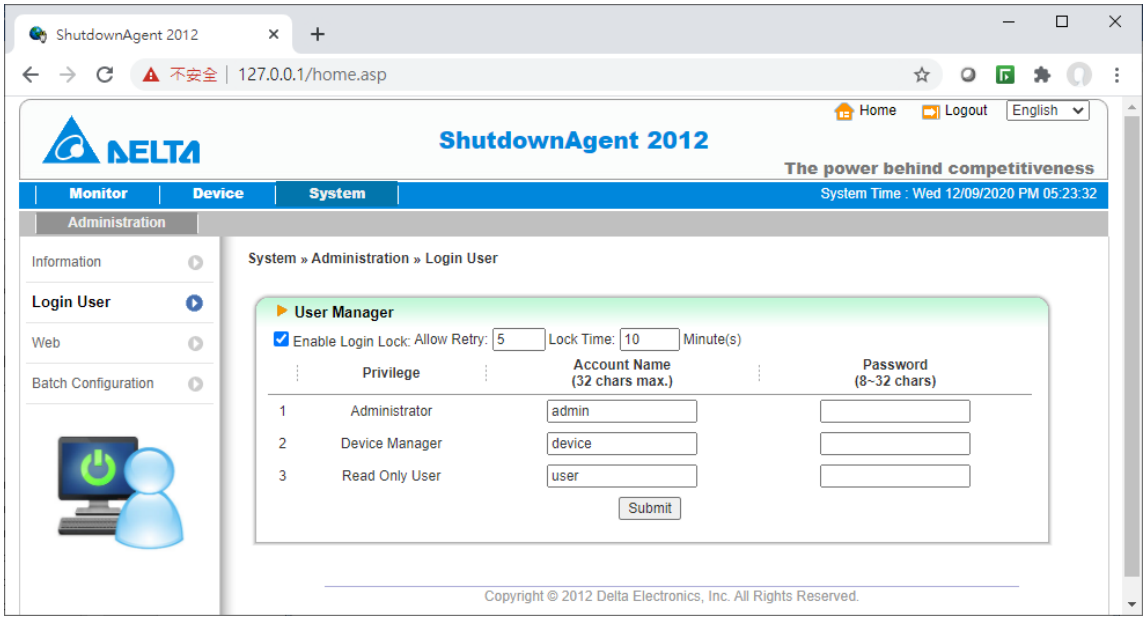
Device Manager: Permitted to modify device-related settings.

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.

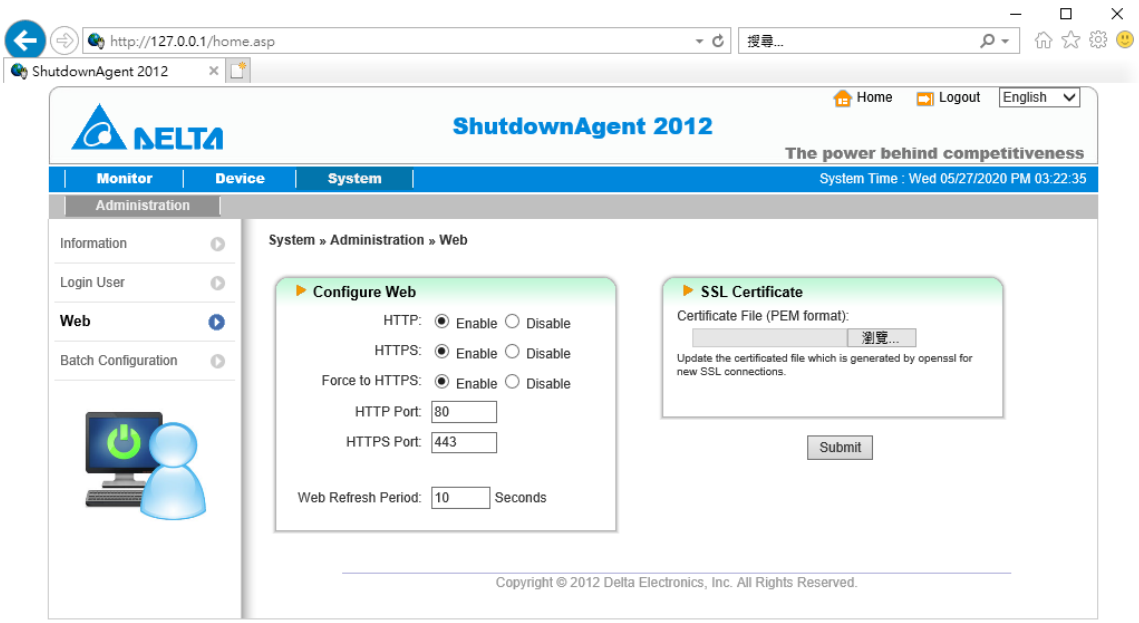
Allow Retry: Lock after wrong number of logins.

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



5.12 System >> Administration >> Web

The administrator can enable or disable HTTP/HTTPS communication protocols available in ShutdownAgent.



HTTP:

Enable or disable HTTP communication of ShutdownAgent.

HTTPS:

Enable or disable HTTPS communication of ShutdownAgent.

Force to HTTPS:

Enable or disable forced HTTPS communication. When the user logs in with http://IP_Address , the software will redirect the user to https://IP_Address for a secure connection.

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 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. 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.

5.13 System >> Administration >> Batch Configuration

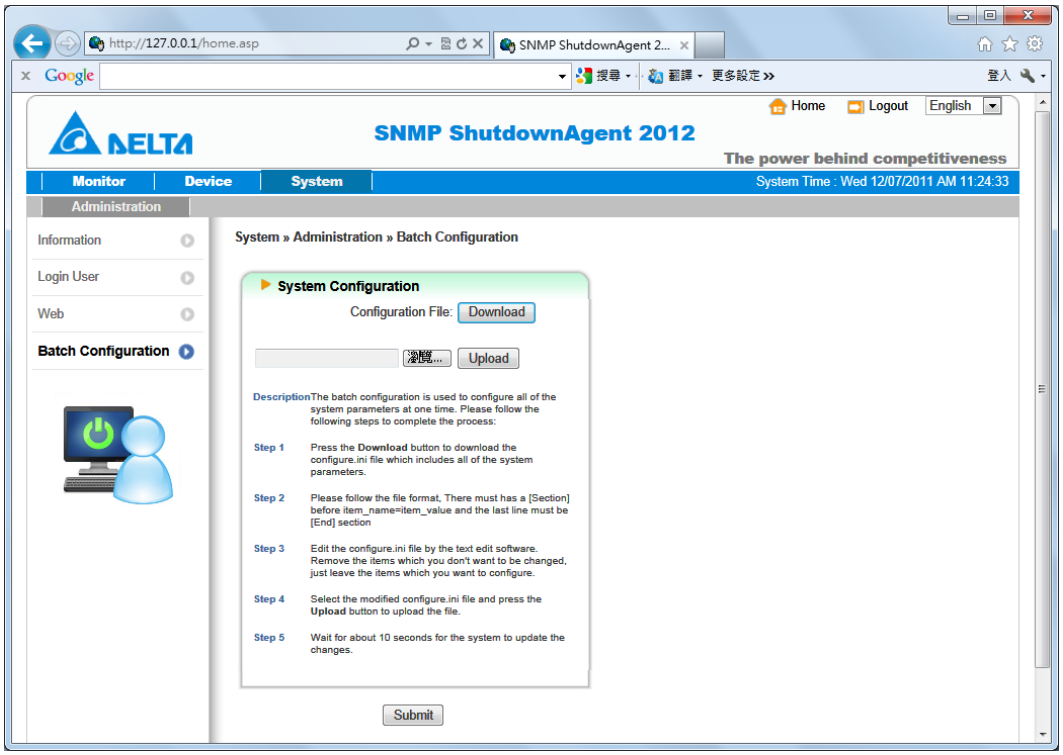
ShutdownAgent provides batch configuration to allow quick and effortless setup on multiple ShutdownAgent hosts. You can duplicate settings by downloading the configuration file from ShutdownAgent that you have successfully configured, and upload the configuration files on other hosts.

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 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
   ```

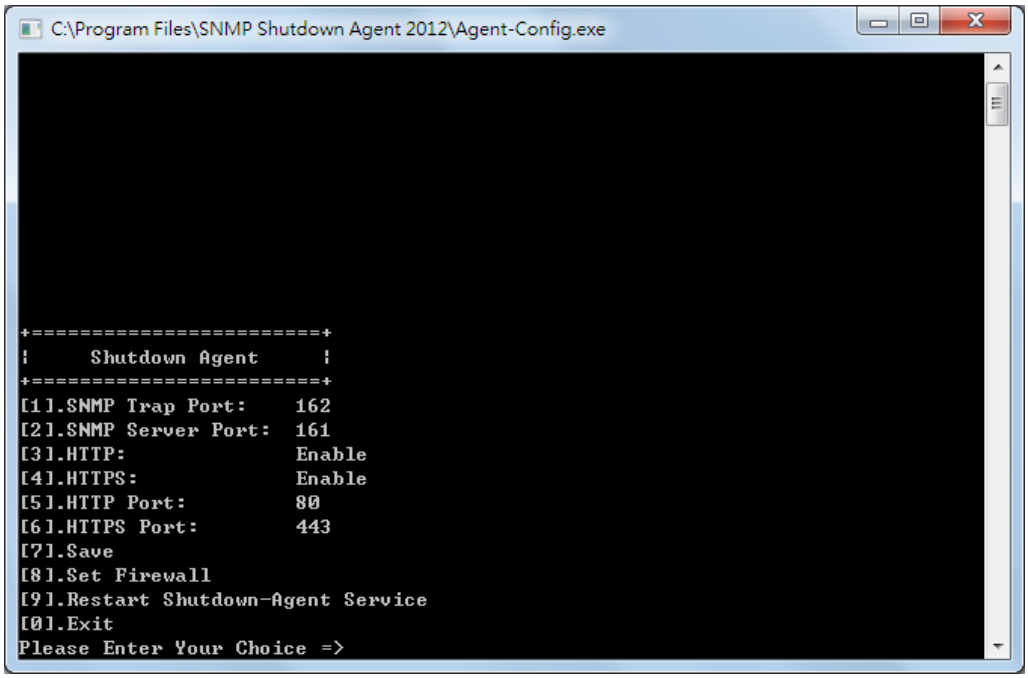
7. Open HTTPS TCP 443

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

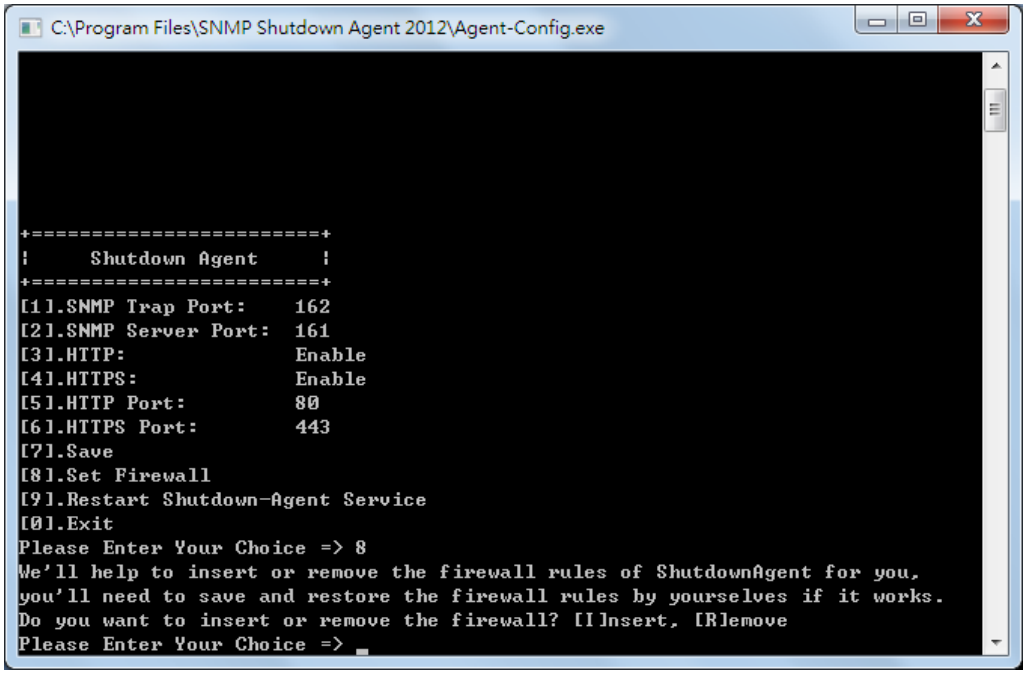
First, put the Shutdown-Agent-2012-Setup(x64).exe setup file in the 2008 server directory. If there is no CD-ROM you can set the “Disable firewall” command, “Add a remotely shared directory” command then copy the file from your PC to the 2008 server. Please remember to set the “Enable firewall” command when complete.

Secondly, follow the chapter 2 to install 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 ShutdownAgent.



7. VMWare ESXi 4.0 Setup for ShutdownAgent

Before installing ShutdownAgent in the ESXi4.0 server, please transmit 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).

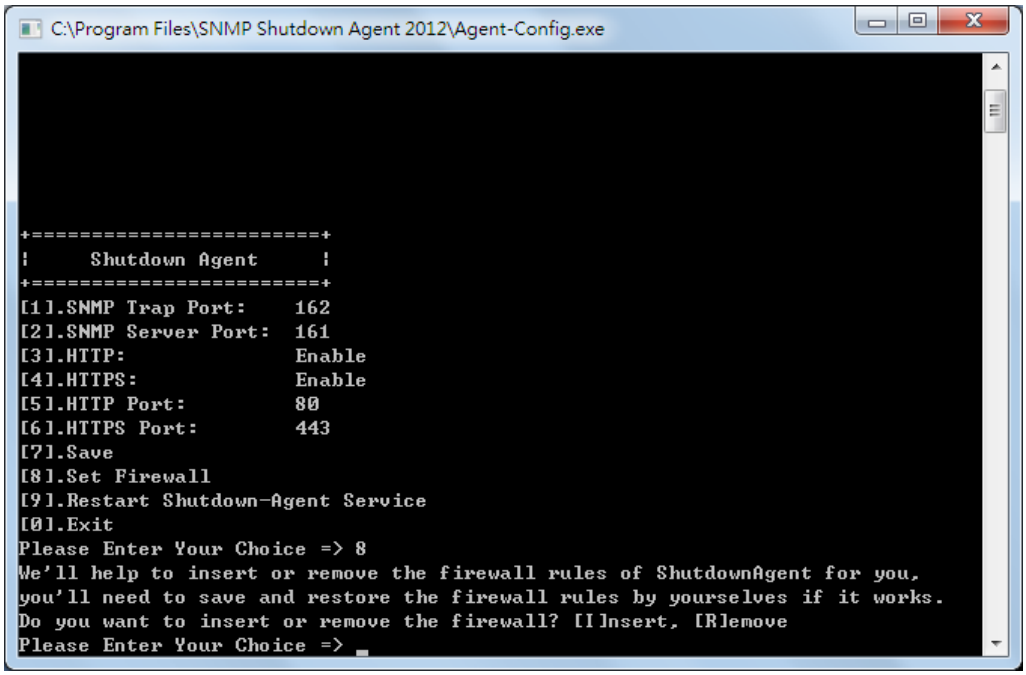
Please continue to follow the section 2.2 For Linux Installation/ Uninstallation.

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 ShutdownAgent.



7.2 Install VMware Tools for Guest OS

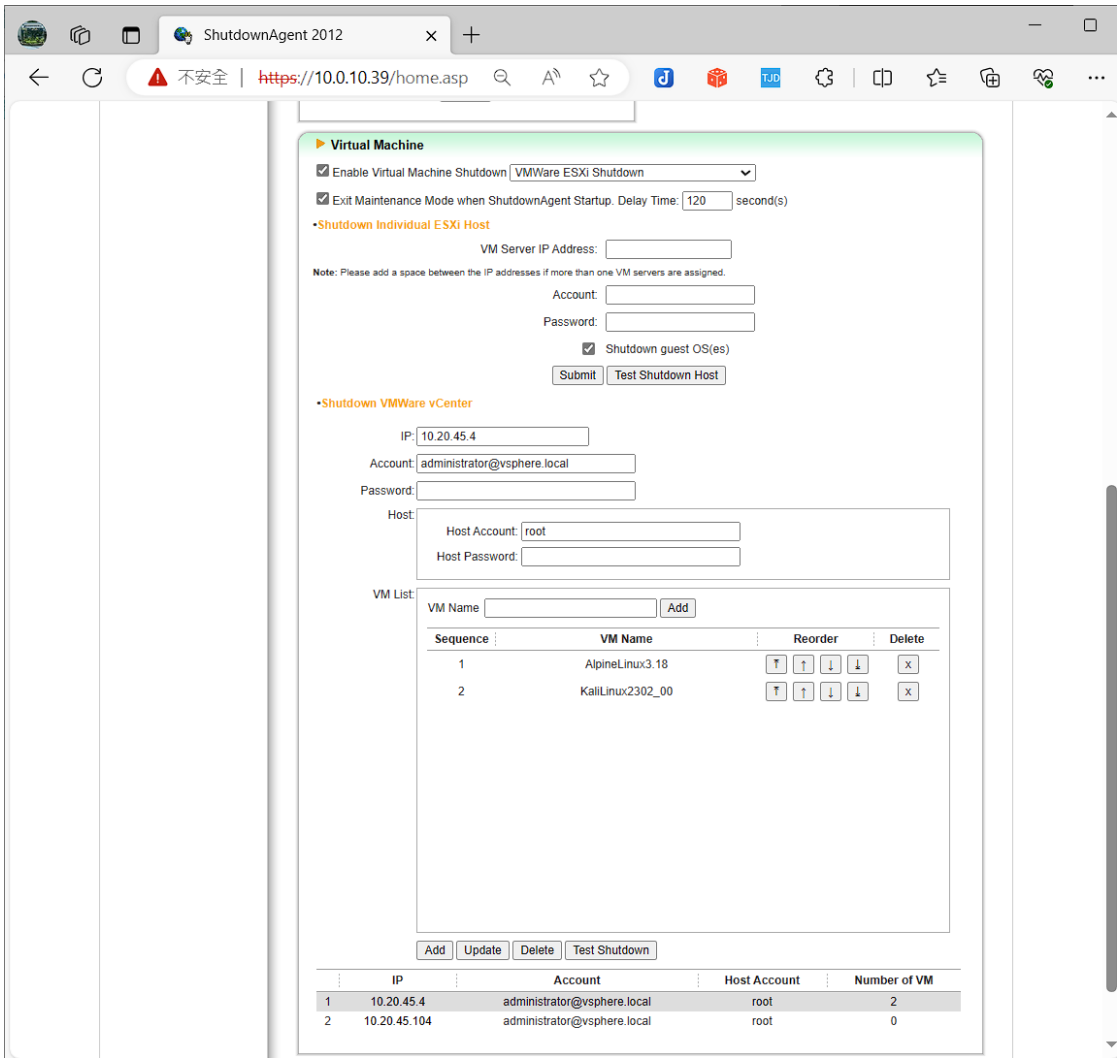
To shut down the guest OS from ESXi server, it' s better for you to install the VMware tools for all of them so as to inform the guest OSes shutdown smoothly.

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. Go to: Device → Host → Configure web page to enable the **Enable Virtual Machine Shutdown** checkbox then select the **VMWare ESXi4** option.



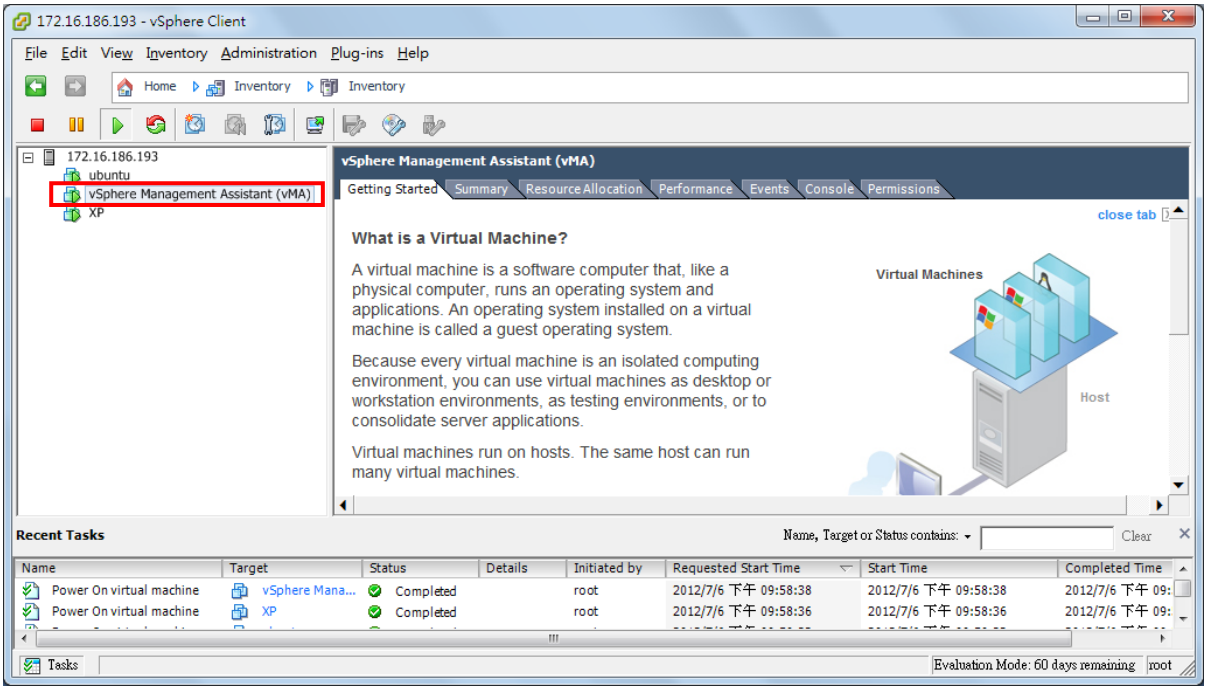
3. Press **Submit** to update your changes.

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

Before installing 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 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.

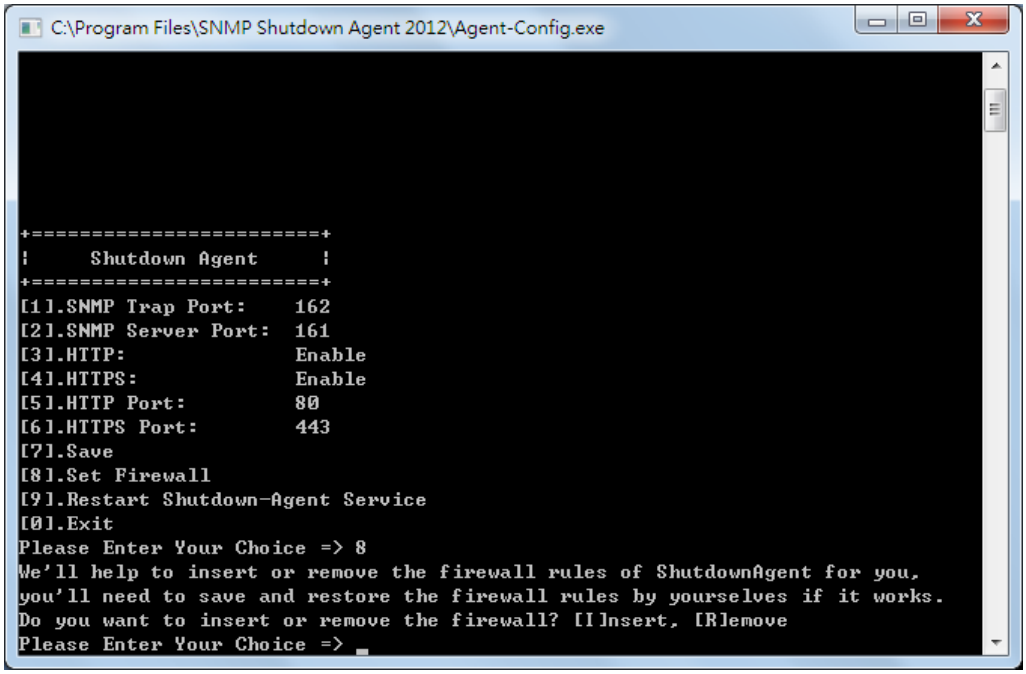
To configure the basic networking parameters including the vMA firewall, please see chapter 3 Console Configuration.



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 ShutdownAgent.



8.2 Install VMware Tools for Guest OS

To shut down 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 ShutdownAgent installed on the guest OS of the same ESXi host, please choose the **VMWare ESXi Shutdown** option.
4. If 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

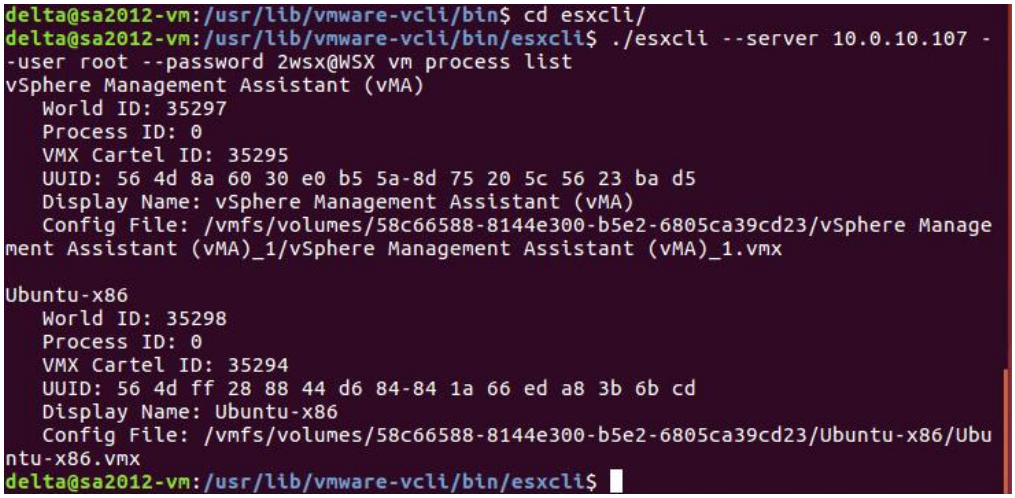
Since the vMA is deprecated after version 6.5, you have to install one public Linux OS such as SUSE, CentOS or Ubuntu. Then install the vCLI in the management Linux OS. Please note that the network communication between the ESXi server and this management Linux must work normally.

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, go 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:



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 ShutdownAgent in the management Linux and make sure the **VMWare tools** is installed in all of the guest OSes. Please then transmit 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.

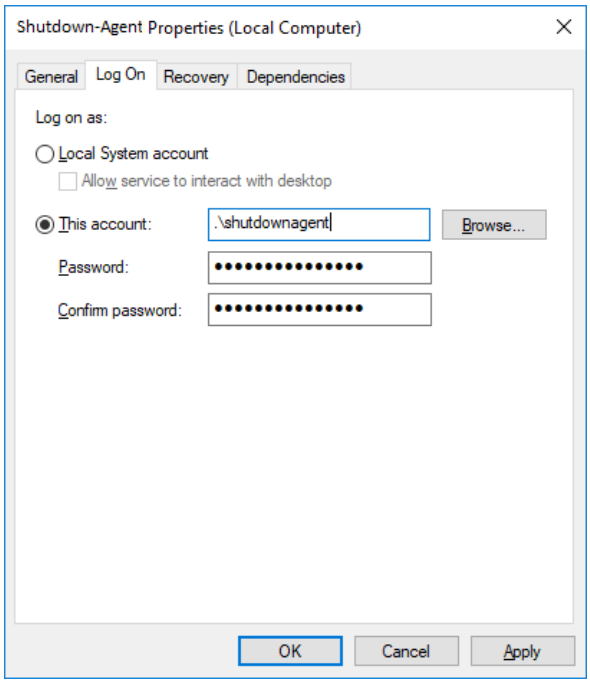
9.2 ShutdownAgent Windows Edition

Please note, to shut down the ESXi host or cluster, you cannot install ShutdownAgent Windows Edition in the same cluster or host. This will cause 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 account must be assigned as a local administrator, this account will be used to execute ShutdownAgent service program.
2. Please login to Windows system by ShutdownAgent account, select 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 ShutdownAgent account and password then press the OK button.



9.2.2 Install VMWare vCLI

You have to login to Windows system by 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:

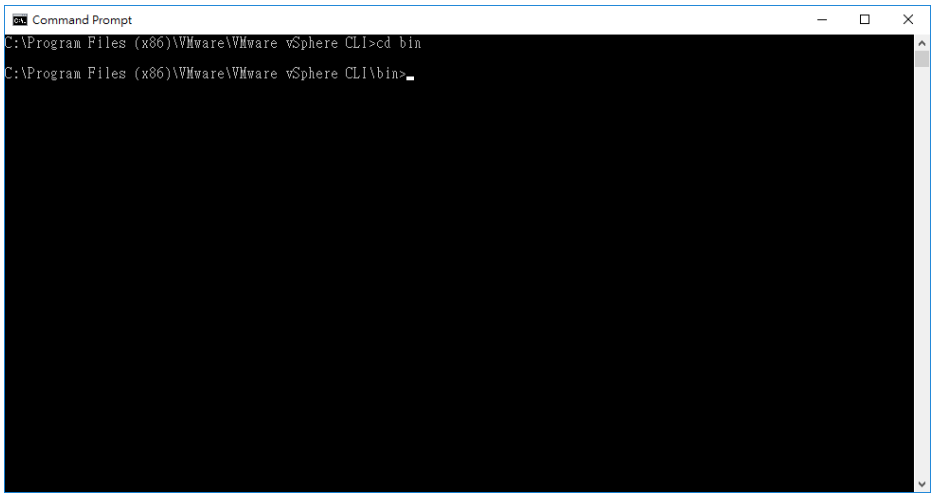
2.1 Select Windows Start > Strawberry Perl > CPAN Client

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`.

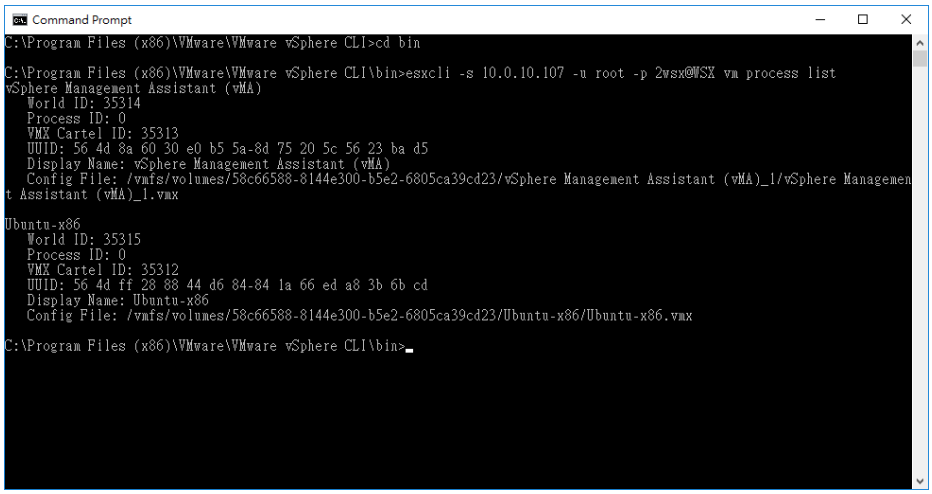


3.2 Test to get the guest OS information from each ESXi host. Please key in:

```
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:

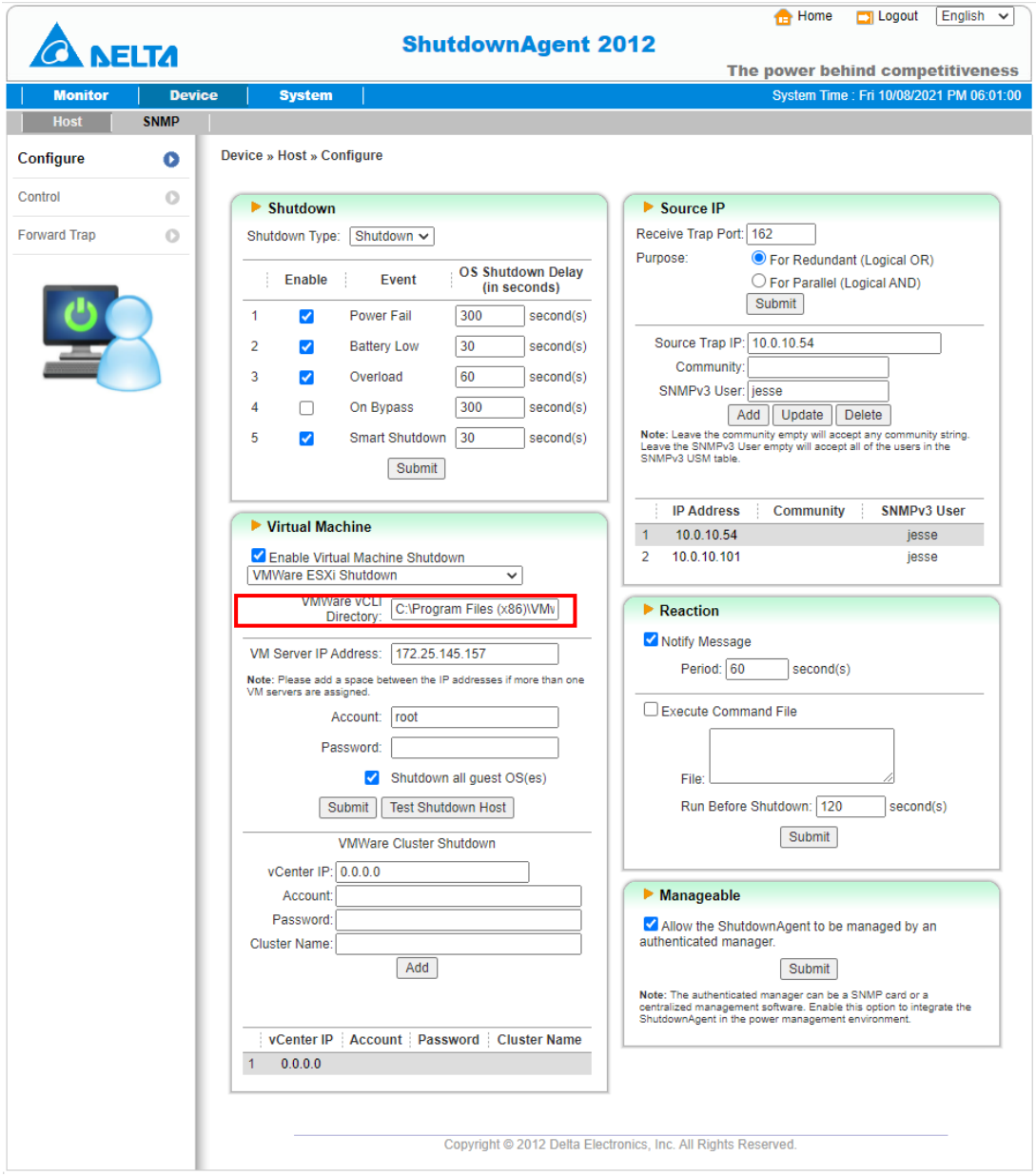
perl credstore_admin.pl add --server 10.0.10.107 –username root –password 2wsx@WSX

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.

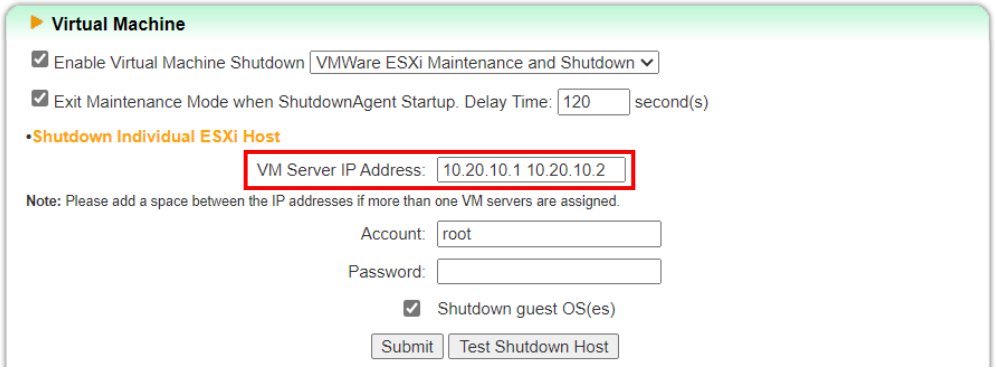
10. VMWare vCenter Shutdown

10.1 Shutdown Individual ESXi Host

Turn on the "**Enable Virtual Machine Shutdown**" option and select the **VMWare ESXi Maintenance and Shutdown**, **VMWare ESXi Shutdown**, or **VMWare ESXi v4** option to shut down one or more ESXi hosts. To shut down multiple ESXi hosts, you need to enter multiple IP addresses in the virtual host IP address field, leaving spaces between addresses, and set the ESXi host account and password to be consistent.

Note: ShutdownAgent cannot install VMWare Tools to avoid being shut down prematurely by the ESXi host.

Set the IP addresses of 2 virtual hosts, leaving spaces between the addresses.



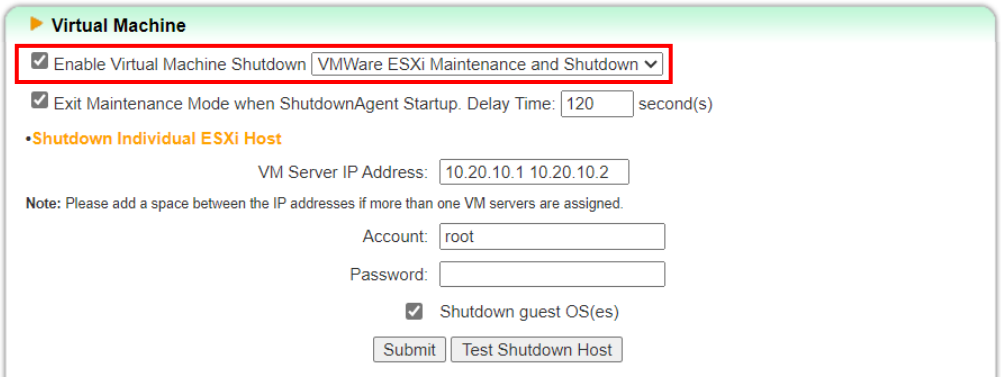
10.1.1 VMWare ESXi Maintenance and Shutdown

Please select this shutdown option for VMWare ESXi version 6.5 or above or when ShutdownAgent is installed on the VM on this ESXi host.

ESXi Host Shutdown Steps:

1. Shut down the Guest OS that has VMWare Tools installed while it is running. (This step can be ignored if automatic guest operating system shutdown is not enabled).
2. The ESXi host enters maintenance mode.
3. Shut down the ESXi host.

If the ShutdownAgent is enabled to exit maintenance mode during startup, the ESXi host will be delayed for a period of time after startup to exit maintenance mode.

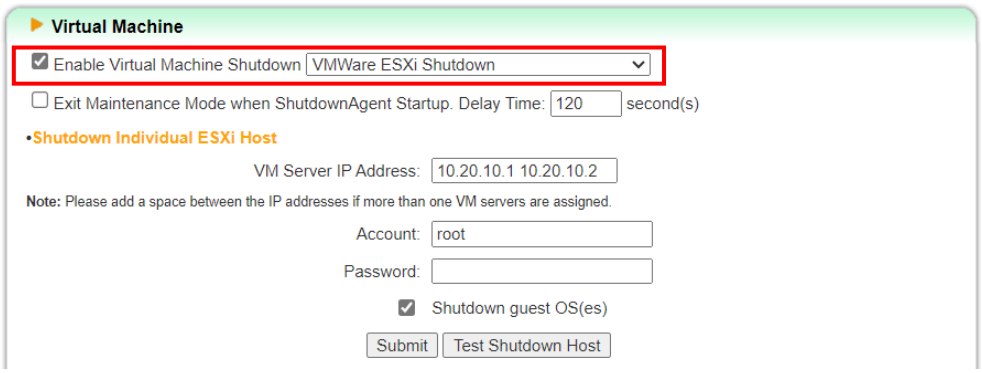


10.1.2 VMWare ESXi Shutdown

Please select this shutdown option for VMWare ESXi version 4.1/5/6 or to force a shutdown of the ESXi host.

ESXi Host Shutdown Steps:

1. Shut down the Guest OS that has VMWare Tools installed while it is running (This step can be ignored if automatic guest operating system shutdown is not enabled).
2. Perform a forced shutdown on the ESXi host.

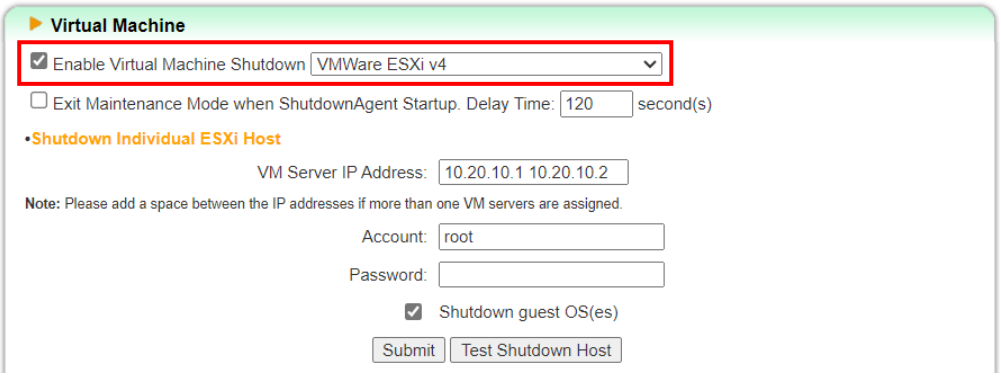


10.1.3 VMWare ESXi v4

Please select this shutdown option for VMWare ESXi version 4.

ESXi Host Shutdown Steps:

1. Shut down the Guest OS that has VMWare Tools installed while it is running.

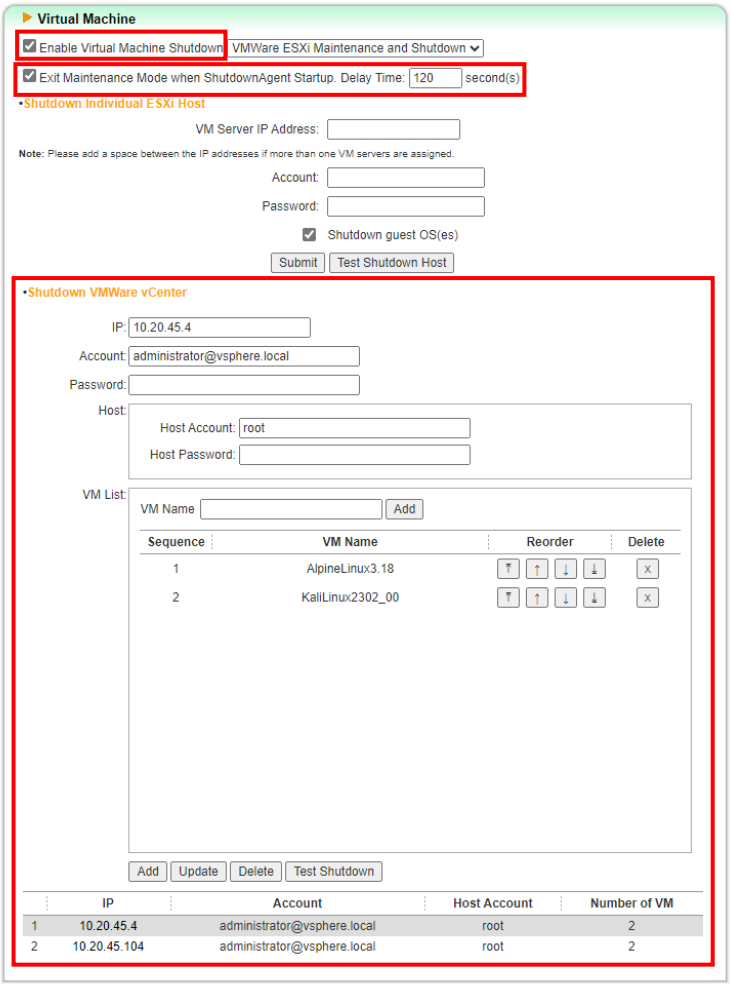


10.2 VMWare vCenter Shutdown Instructions

It is recommended to use VMWare ESXi version 8 or above.

Enable the "**Perform Virtual Shutdown**" option and perform one or more vCenter shutdown procedures. Please enter the vCenter IP, account and password, and VM list. Please set the ESXi host account and password to be consistent.

If the "**Exit Maintenance Mode when ShutdownAgent Startup**" option is enabled, the command will be sent after a period of time.



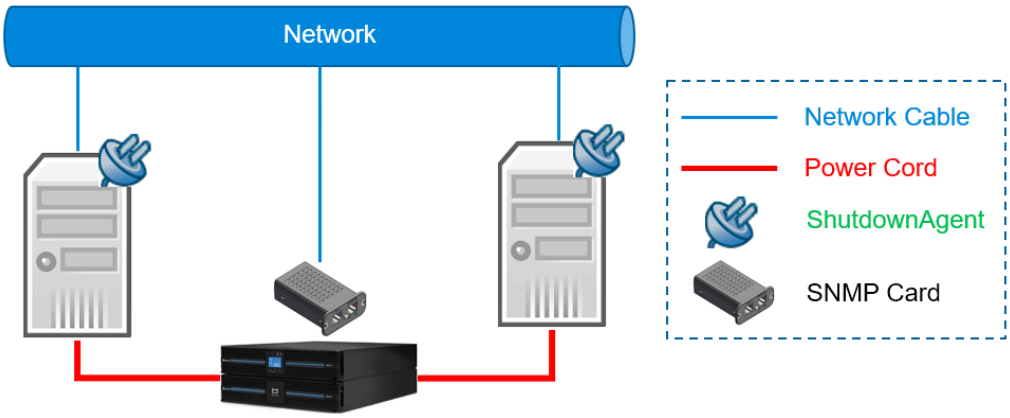
10.2.1 Shutdown Steps

1. Shut down VMs in order according to the VM list.
2. Shut down the VM except ShutdownAgent and vCenter.
3. There is no ESXi Host running ShutdownAgent and vCenter.
   3.1 Enter maintenance mode
   3.2 Close the Host
4. Shut down vCenter and the ESXi Host where it is located.
5. Shut down the ESXi Host where the ShutdownAgent is located.

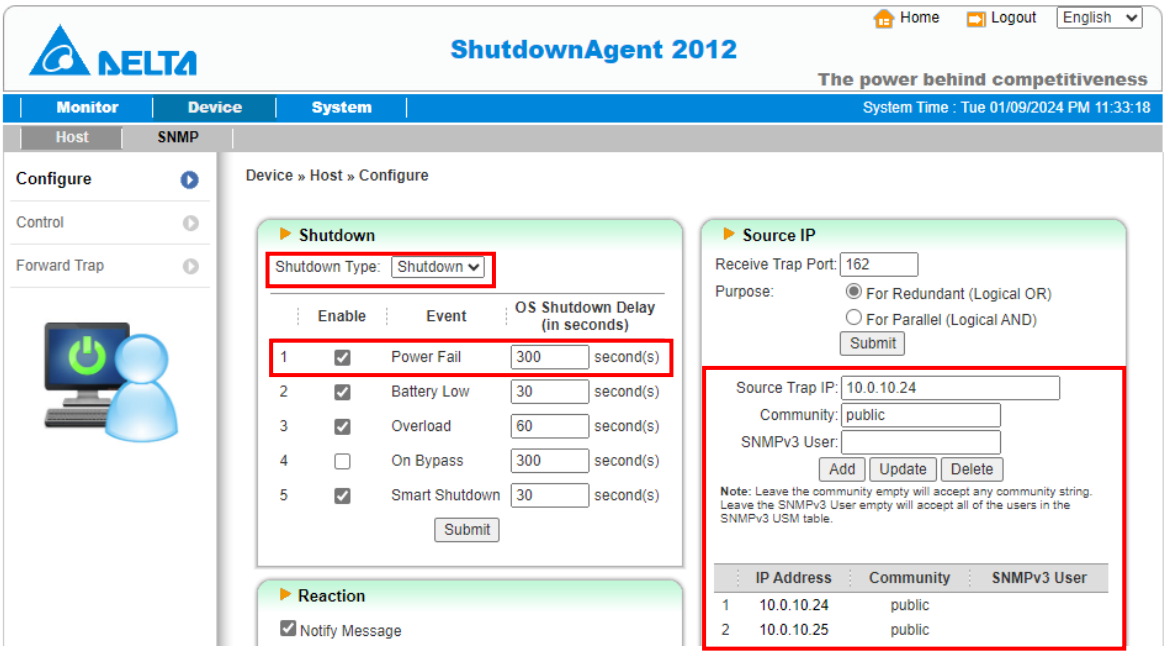
11. Shutdown Scenarios

11.1 Power Supply from One UPS

If there is only one UPS supplies power to multiple servers installed with ShutdownAgent 2012, when the power supply is interrupted, the UPS will send SNMP Traps to the ShutdownAgent through the SNMP Card to shut down, power off or hibernate the servers.



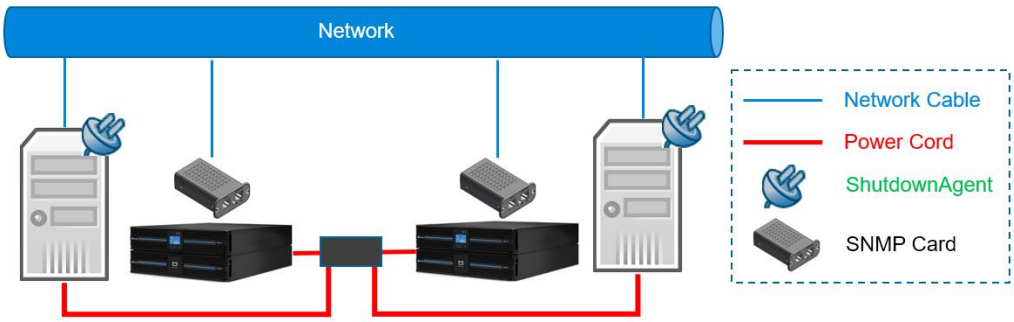
11.1.1 Configure



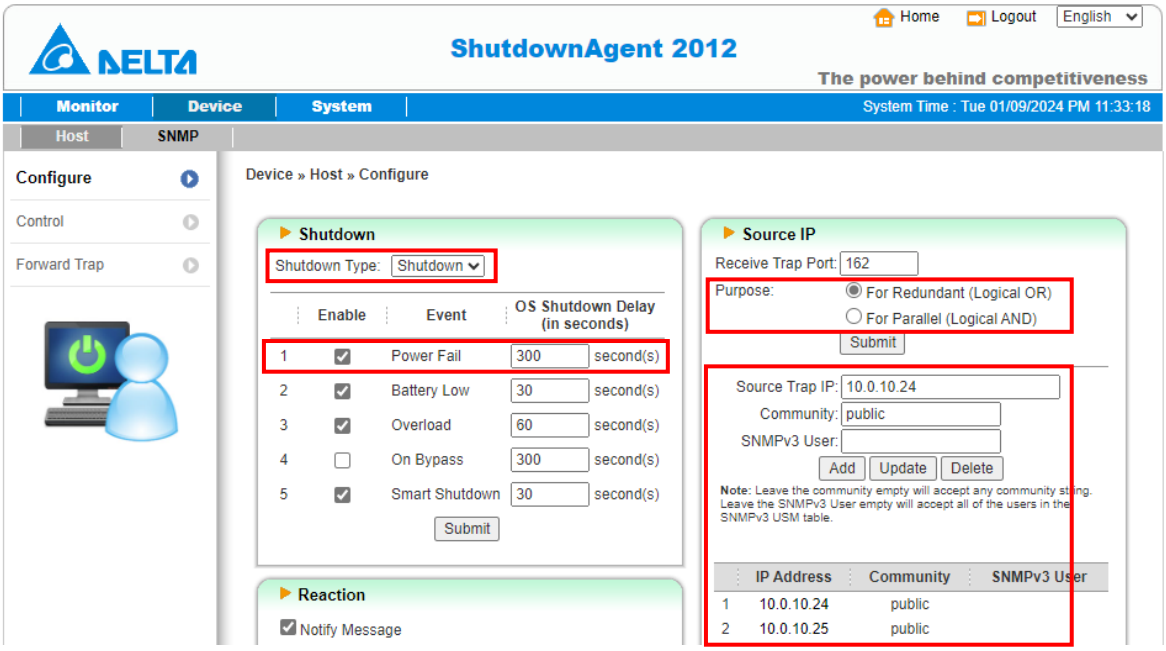
Add the UPS Trap source IP address and enable the input power interruption event, and then set the delay time according to the needs before executing the server shutdown, power off or hibernation. For detailed field description, please refer to 5.5 Device >> Host >> Configure.

11.2 UPS Power Supply in Parallel

Suppose that there 2 UPSs connected in parallel to supply power to multiple servers installed with ShutdownAgent 2012, when the ShutdownAgent receives the power interruption SNMP Trap from one of the UPSs, the servers will be shut down, powered off, or hibernated (logical OR operation).



11.2.1 Configure

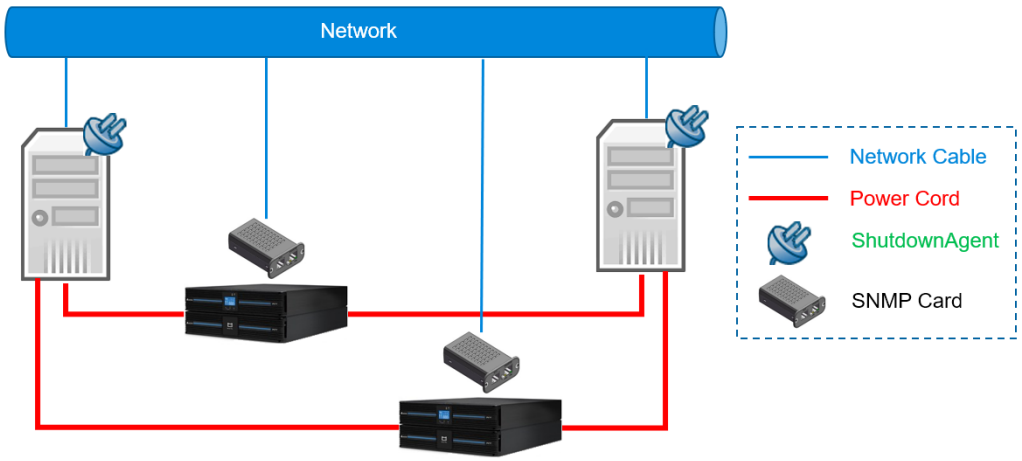


1. Add 2 UPS Source Trap source IP addresses.
2. Set the purpose to redundant use (logical OR) and enable the input power interruption event, and then set the delay time according to the requirements before executing the server shutdown, power off or hibernation.

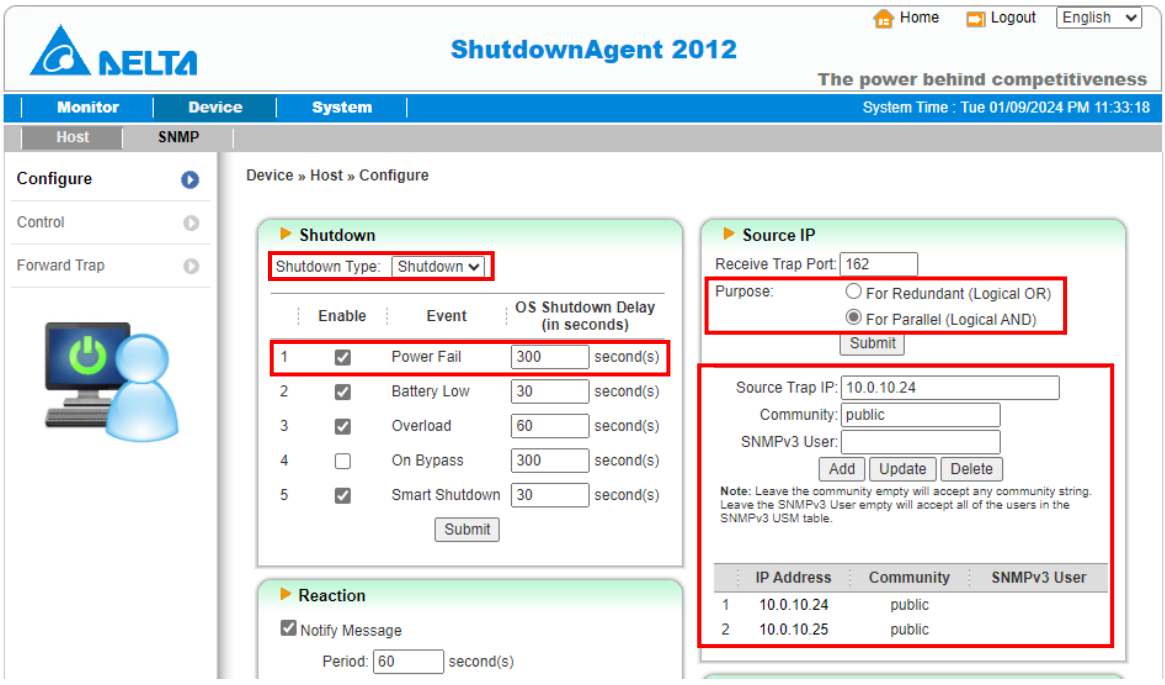
For detailed field description, please refer to 5.5 Device >> Host >> Configure.

11.3 UPS Redundant Power Supply

Suppose that there are 2 UPSs provide redundant power to multiple servers installed with ShutdownAgent 2012, when the ShutdownAgent receives the power interruption SNMP Trap from the 2 UPSs, the servers will be shut down, powered off, or hibernated (logical AND operation).



11.3.1 Configuration



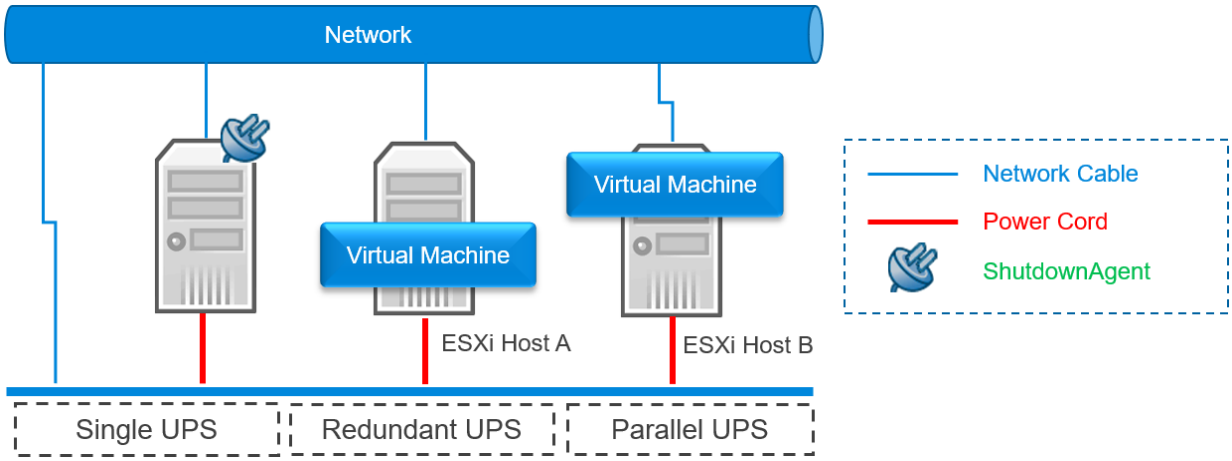
1. Add 2 UPS Trap source IP addresses.
2. Set the purpose to parallel use (logical AND) and enable the input power interruption event, and then set the delay time according to the requirements before executing the server shutdown, power off or hibernation.

For detailed field description, please refer to 5.5 Device >> Host >> Configure.

11.4 ESXi Host Shutdown Scenarios

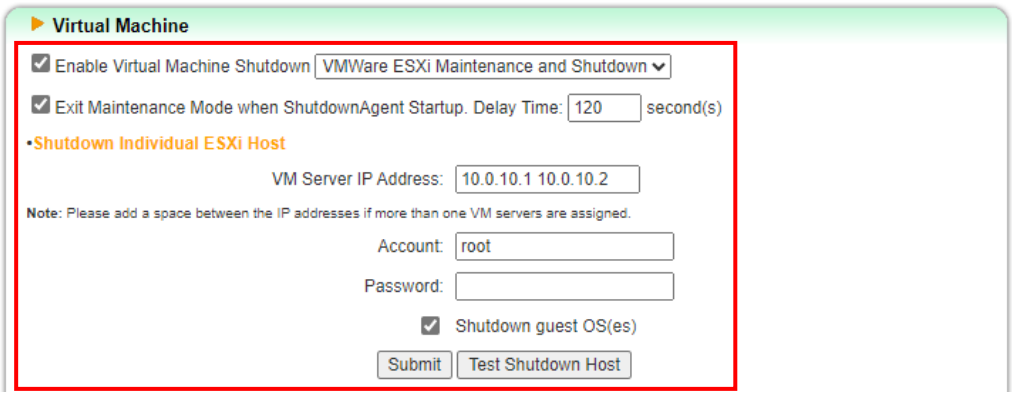
11.4.1 ShutdownAgent Runs Outside the ESXi Host

If ShutdownAgent runs on an independent host outside the ESXi host, when it receives the power interruption SNMP Trap sent by the SNMP Card, the ShutdownAgent immediately shuts down multiple ESXi hosts and the servers where they are located, shuts down the power, or hibernates.



Settings:

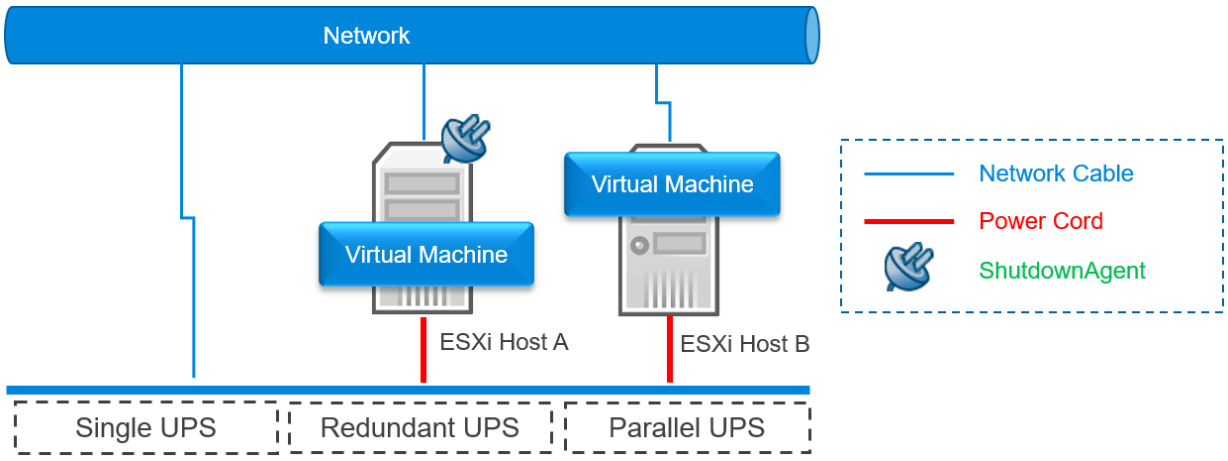
1. Set the UPS Trap source, purpose, shutdown event and method. According to the UPS power supply mode, please refer to 11.1.1 Single UPS power supply setting, 11.2.1 UPS parallel power supply setting or 11.3.1 UPS redundant power supply setting.



2. Activate the "**Enable Virtual Machine Shutdown**" option and select **VMWare ESXi Maintenance and Shutdown** or **VMWare ESXi Shutdown**. Please refer to 10.1.1 VMWare ESXi Maintenance and Shutdown option or 10.1.2 VMWare ESXi Shutdown option.
3. If the virtual shutdown option is "**VMWare ESXi Maintenance and Shutdown**", please activate the option "**Exit Maintenance Mode when ShutdownAgent Startup**".
4. Set the IP addresses of the 2 ESXi hosts. Please leave blank between the addresses.
5. Set the same account and password for the 2 ESXi hosts.
6. Enable "**Shutdown guest OS(es)**".

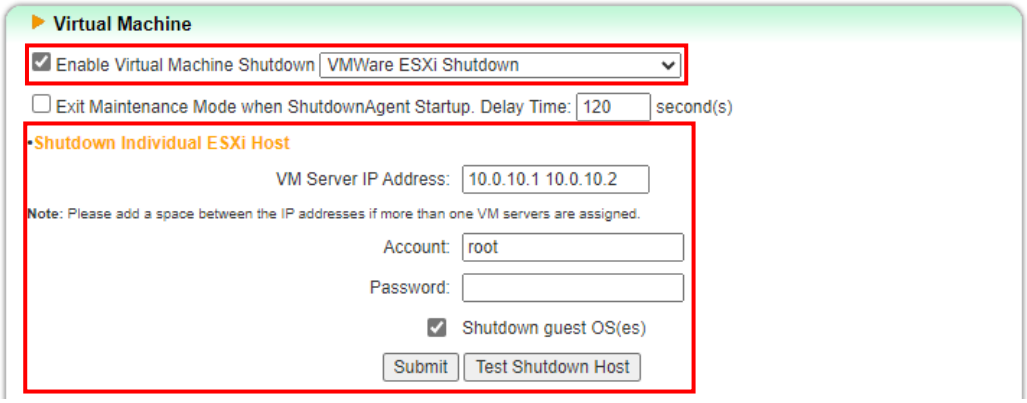
11.4.2 ShutdownAgent Runs Inside ESXi Host

If ShutdownAgent runs on a virtual machine in one of the ESXi hosts, when it receives the power interruption SNMP Trap sent by the SNMP Card, the ShutdownAgent immediately shuts down multiple ESXi hosts.



Settings:

1. Set the UPS Trap source, purpose, shutdown event and method. According to the UPS power supply mode, please refer to **11.1.1 Power Supply from One UPS**, **11.2.1 UPS Power Supply in Parallel** or **11.3.1 UPS Redundant Power Supply**.



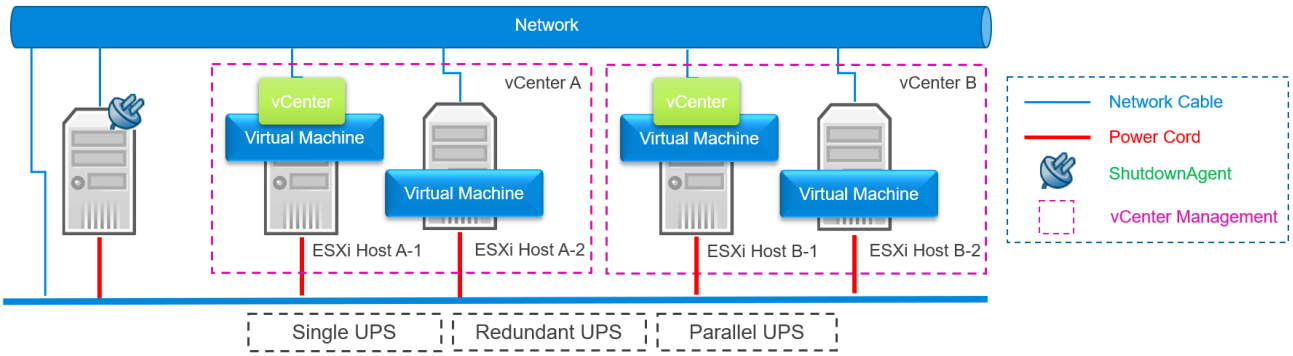
2. Activate the "**Enable Virtual Machine Shutdown**" option and select "**VMWare ESXi Shutdown**". Please refer to 10.1.2 VMWare ESXi Shutdown.
3. Set the IP addresses of the 2 ESXi hosts. Please leave blank between the addresses.
4. Set the same account and password for the 2 ESXi hosts.
5. Enable "**Shutdown guest OS(es)**".

11.5 vCenter Shutdown Scenarios

It is recommended to use VMWare ESXi version 8 or above.

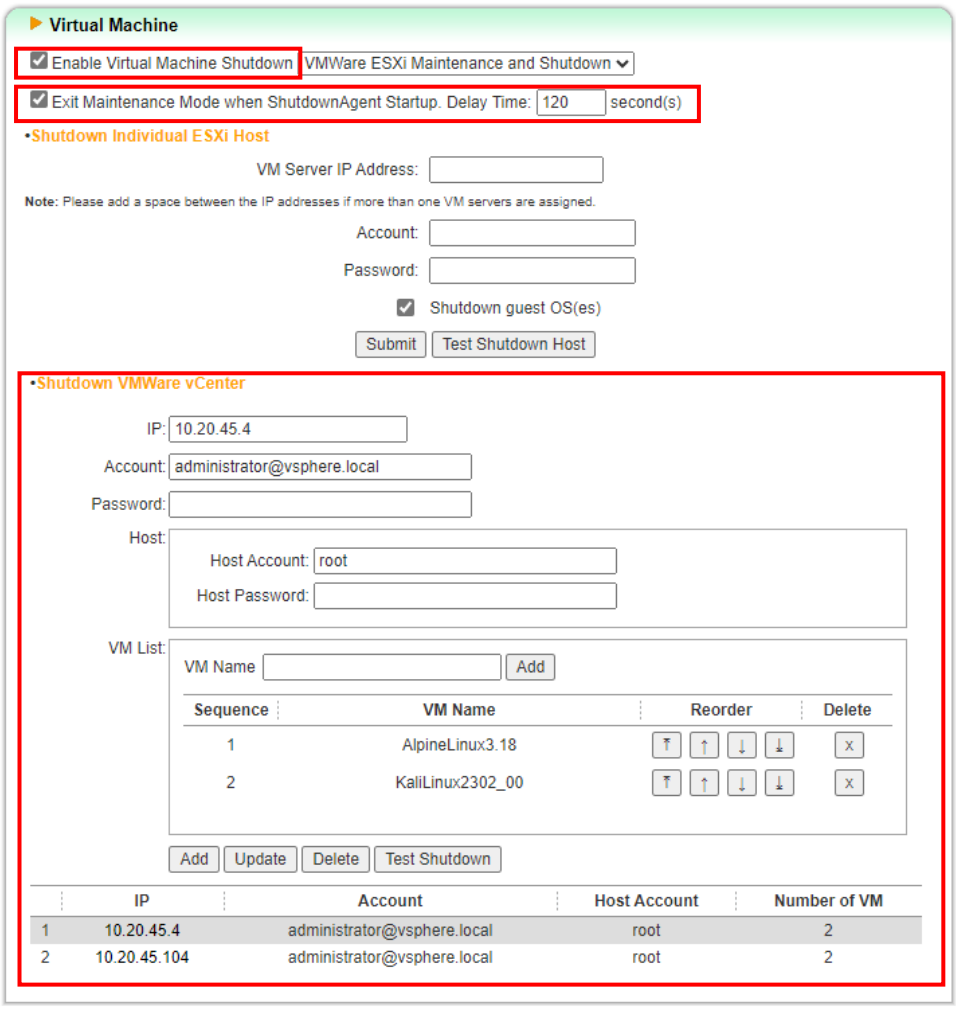
11.5.1 ShutdownAgent Runs Outside vCenter

If ShutdownAgent runs on an independent host outside VMWare vCenter, when it receives the power interruption SNMP Trap sent by the SNMP Card, ShutdownAgent immediately performs VMWare vCenter shutdown steps on multiple vCenters (Please refer to 10.2.1 VMWare vCenter Shutdown Steps) and the server where it is located.



Settings:

1. Set the UPS Trap source, purpose, shutdown event and method. According to the UPS power supply mode, please refer to 11.1.1 Power Supply from One UPS, 11.2.1 UPS Power Supply in Parallel or 11.3.1 UPS Redundant Power Supply.

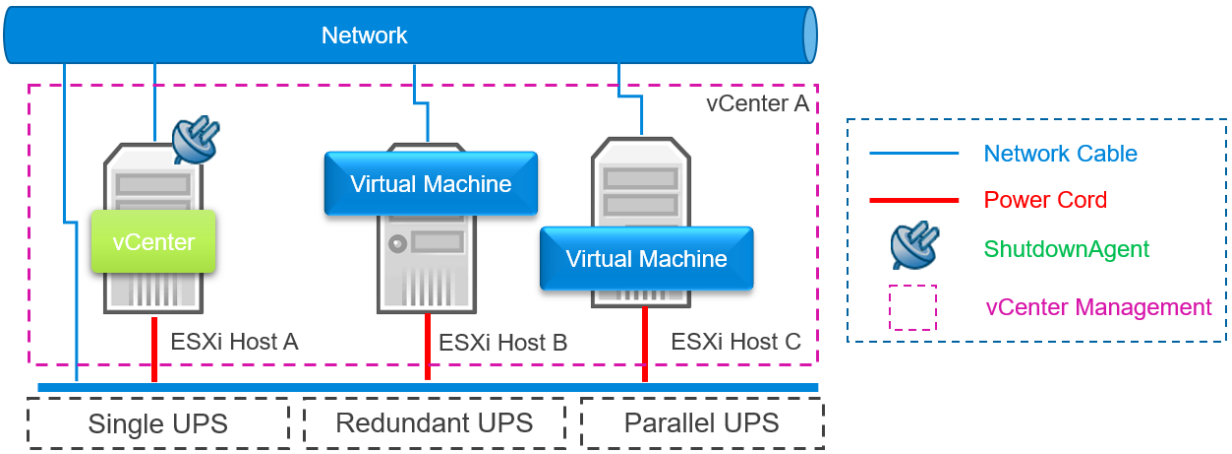


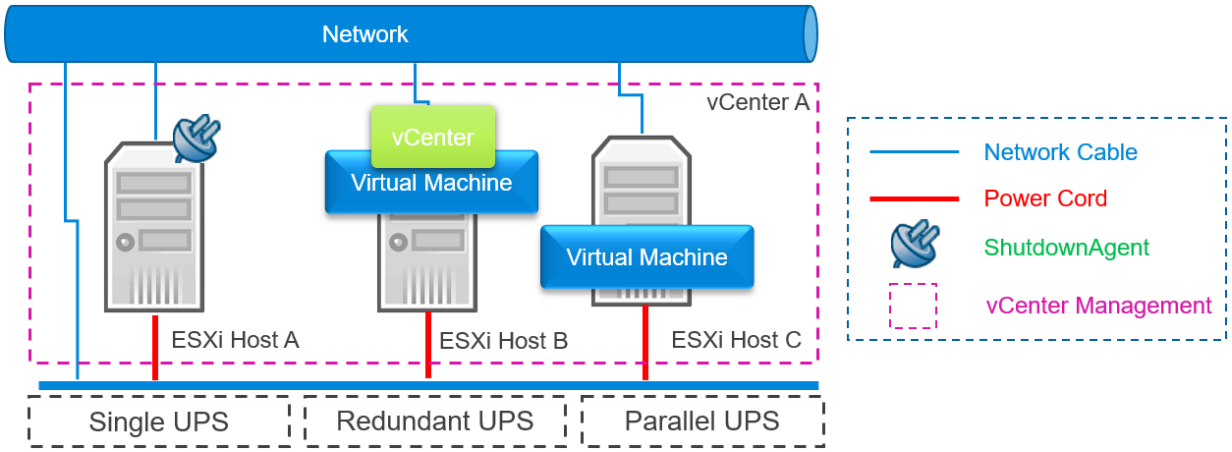
2. Activate the "**Enable Virtual Machine Shutdown**" and "**Exit Maintenance Mode when ShutdownAgent Startup**".
3. In the Shutdown VMware VCenter settings, add two vCenter IP addresses, accounts, passwords, and VM shutdown order list. Please also set the consistent ESXi host accounts and passwords.

11.5.2 ShutdownAgent Runs Inside vCenter

If ShutdownAgent runs on a virtual machine in VMWare vCenter, when it receives the power interruption SNMP Trap sent by the SNMP Card, it immediately performs the VMWare vCenter shutdown steps (Please refer to 10.2.1 VMWare vCenter Shutdown Steps).

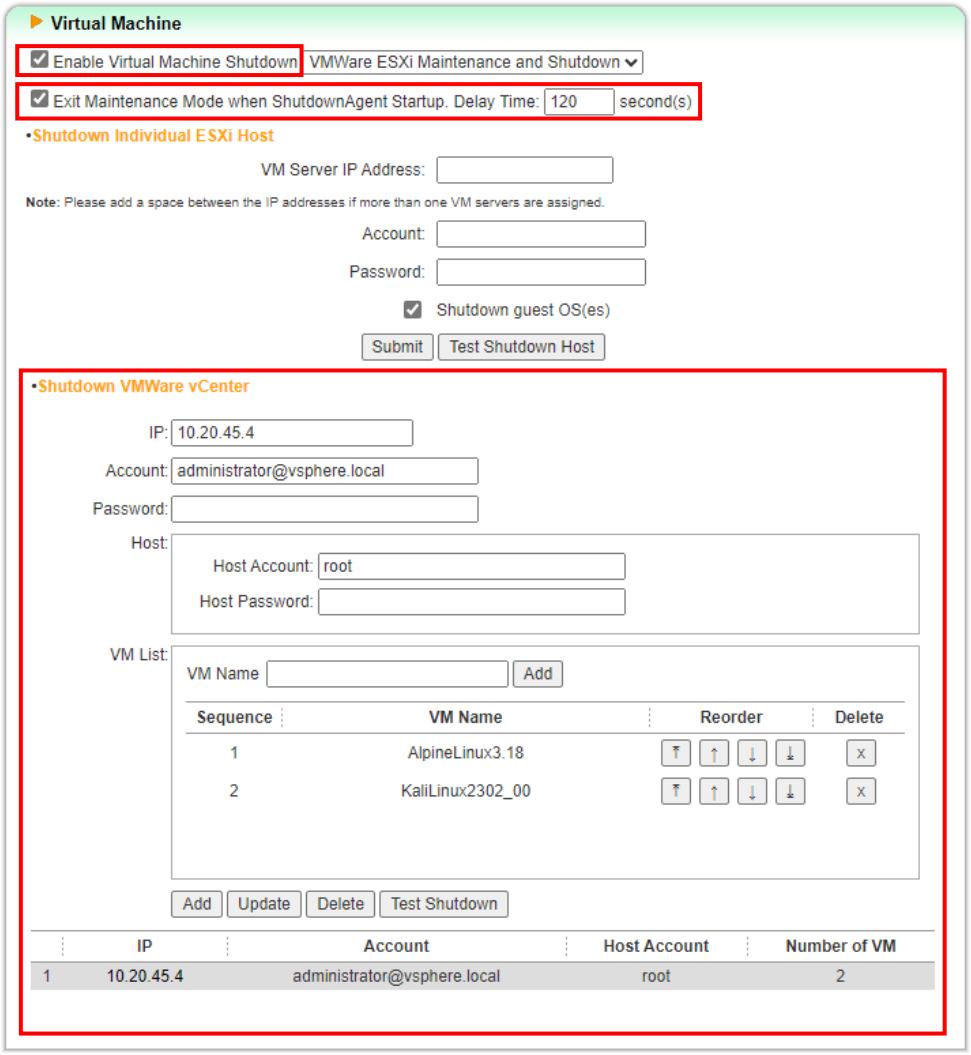
Note: This scenario only supports one vCenter.





Settings:

1. Set the UPS Trap source, purpose, shutdown event and method. According to the UPS power supply mode, please refer to 11.1.1 Power Supply from One UPS, 11.2.1 UPS Power Supply in Parallel or 11.3.1 UPS Redundant Power Supply.



2. Activate the "**Enable Virtual Machine Shutdown**" and "**Exit Maintenance Mode when ShutdownAgent Startup**".
3. In the Shutdown VMware VCenter settings, add the vCenter IP address, account, password, and VM shutdown order list. Please also set the consistent ESXi host accounts and passwords.

12. 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.

12.1 Download the pre-made OVA file

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

https://datacenter-softwarecenter.deltaww.com > 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.

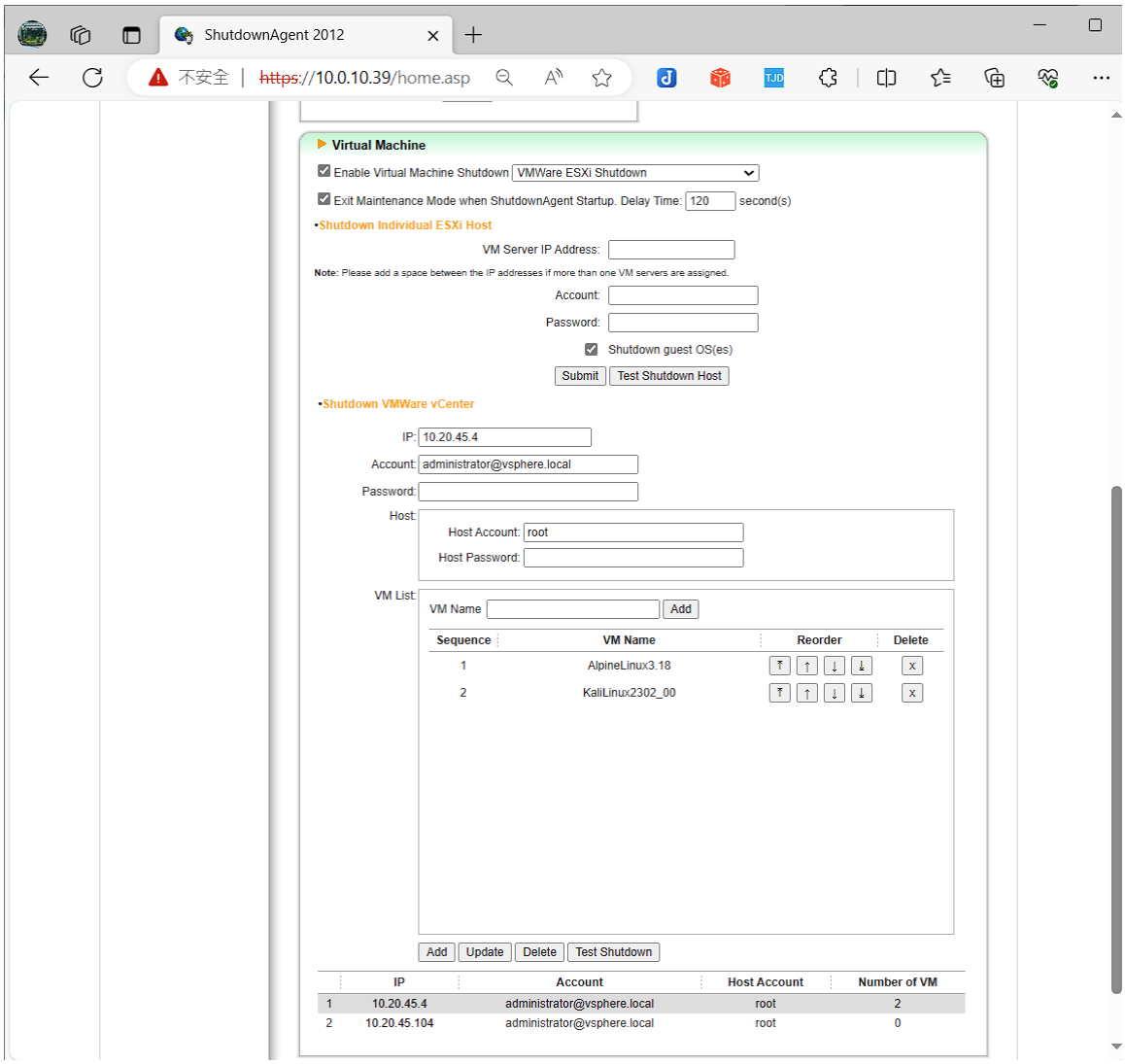
12.2 Import the OVA file to the ESXi host

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.

12.3 Connect to 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 shut down.
- VMWare ESXi Shutdown: Used to force shutdown the ESXi hosts.
- VMWare ESXi v4: Used to shut down the ESXi version 4. (Please ignore the "Exit Maintnenance Mode" option).
- Xen Server: Used to shut down the Xen server. (Please ignore the "Exit Maintenance Mode" option).

- Linux KVM: Used to shut down the KVM server. (Please ignore the "Exit Maintenance Mode" option).

13. XenServer Setup for ShutdownAgent

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

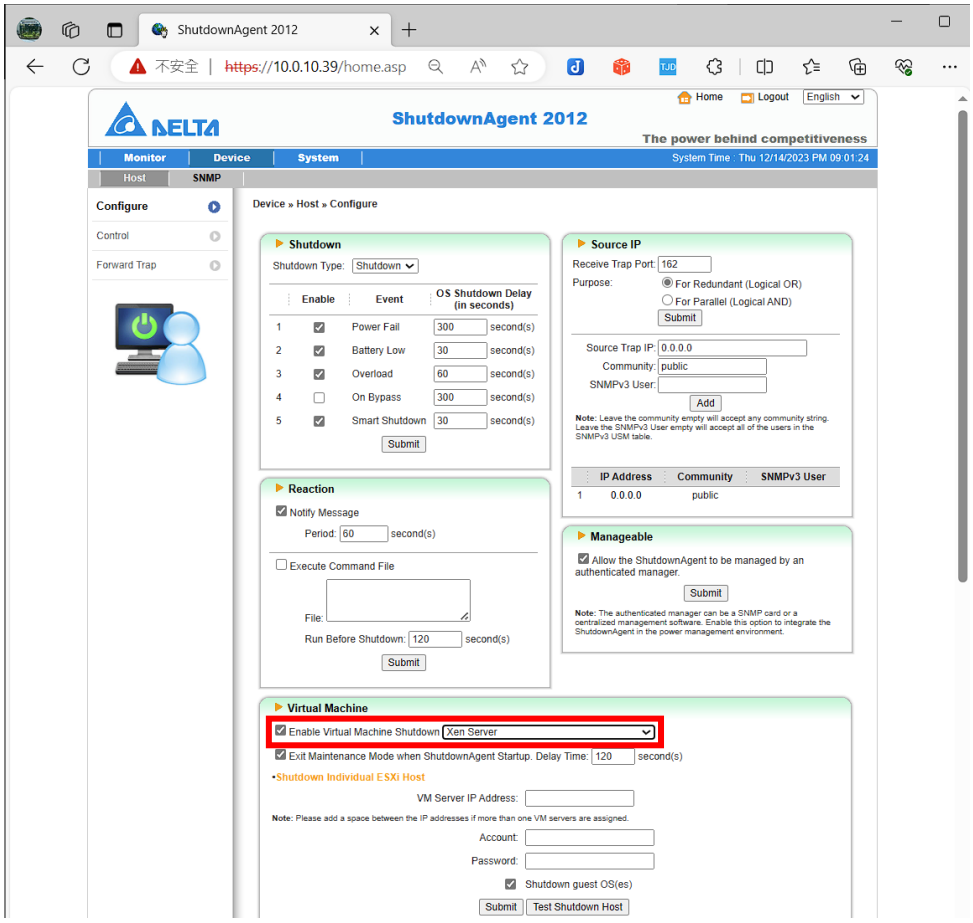
To configure the basic networking parameters including the Xen firewall, please see chapter 3 Console Configuration.

13.1 Install PV driver for Guest OS

To shut down 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.

13.2 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. Go to: 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.

14. Linux KVM Setup for ShutdownAgent

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

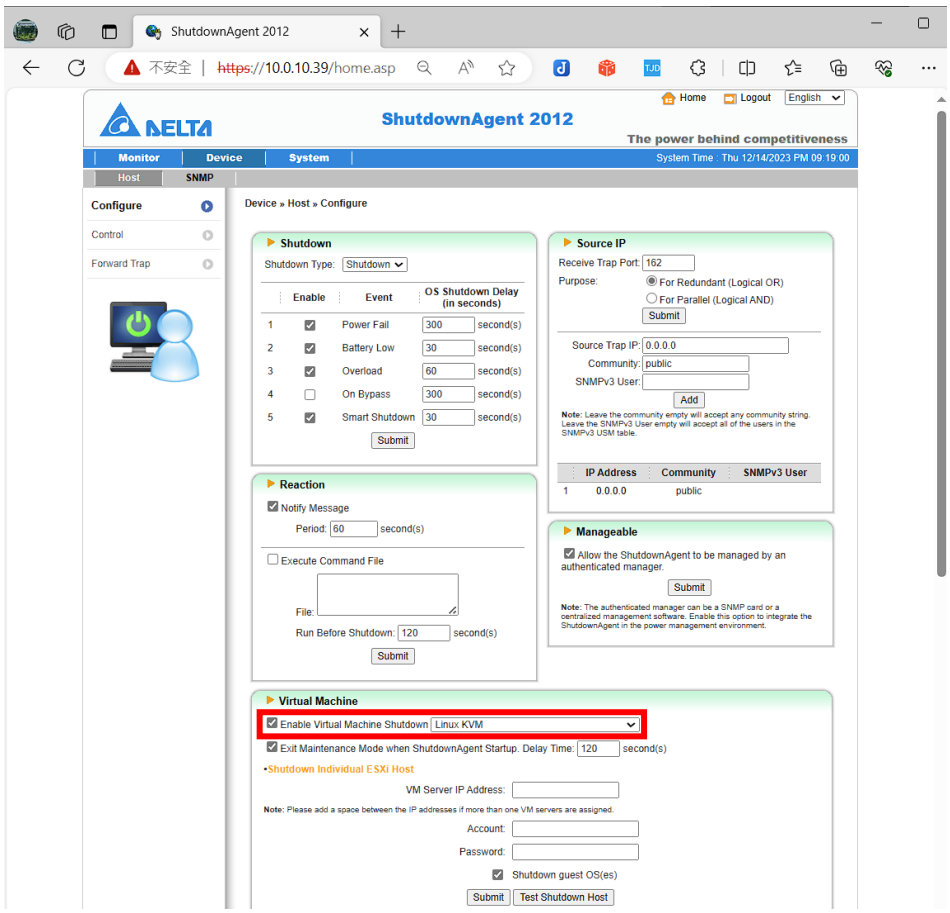
To configure the basic networking parameters including the firewall, please see chapter 3 Console Configuration.

14.1 Install libvirt Tools for KVM

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

14.2 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. Go to: Device → Host → Configure web page to enable the **Enable Virtual Machine Shutdown** checkbox then select the **Linux KVM** option.



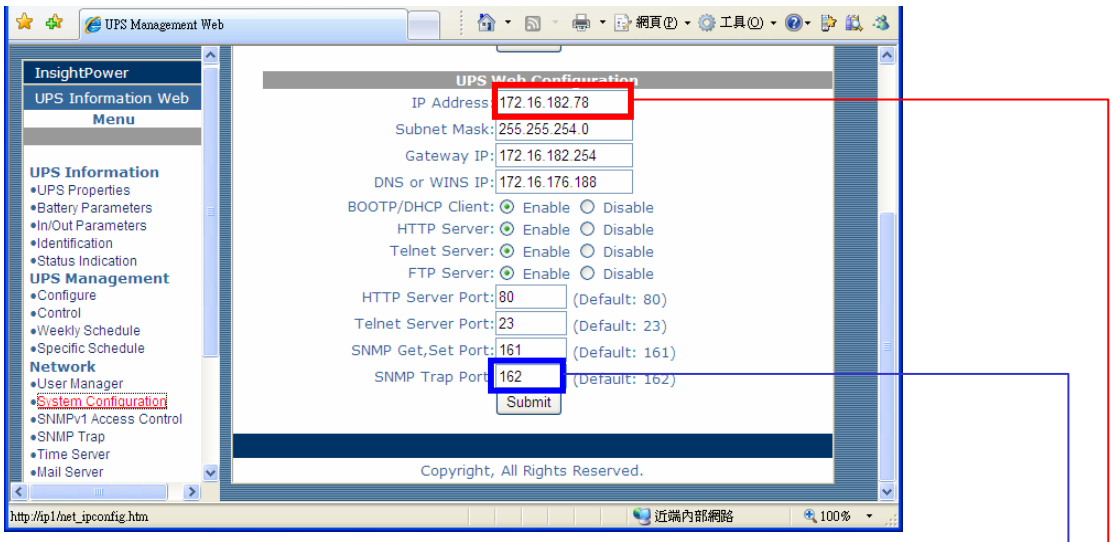
3. Press **Submit** button to update your changes.

15. Work with the SNMP Card

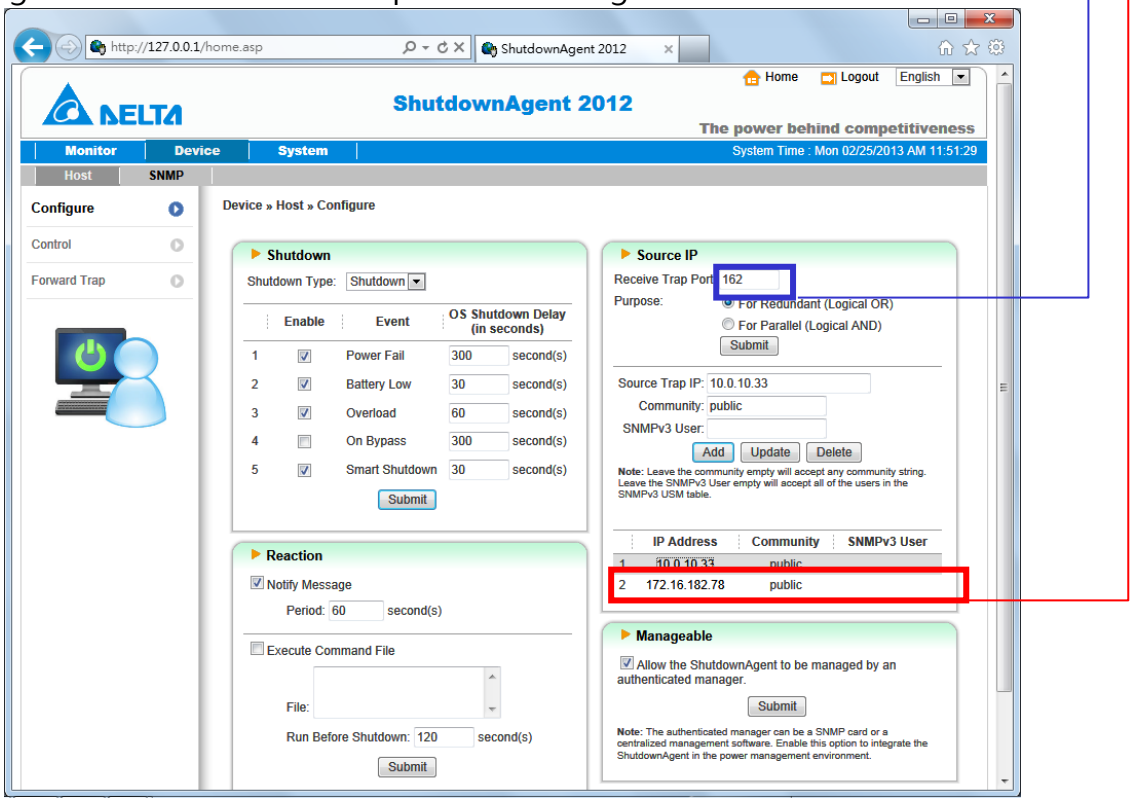
15.1 Legacy Delta InsightPower SNMP Card

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

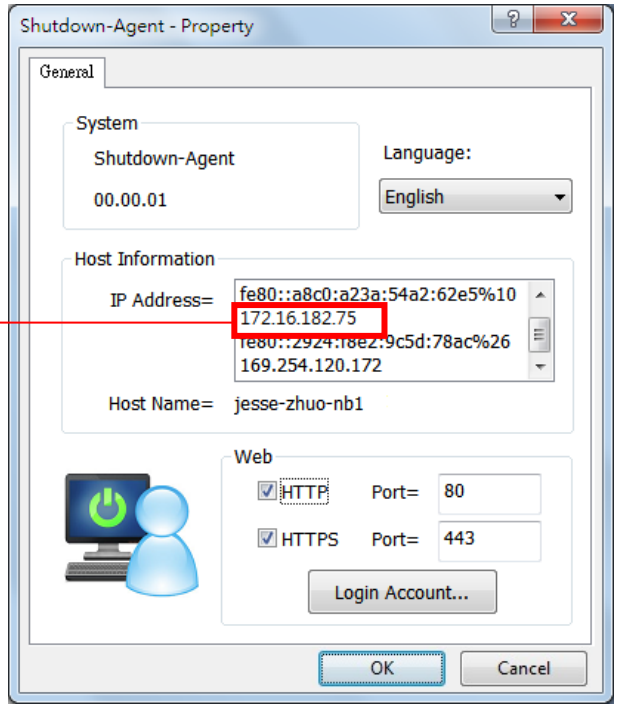
2. Record the IP address and SNMP Trap Port in the System Configuration web page.



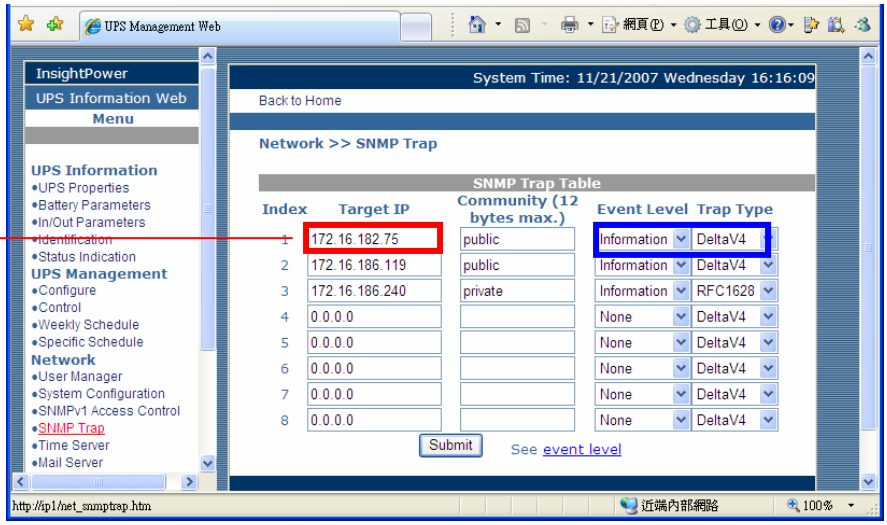
3. Add the SNMP IP address and the trap port to ShutdownAgent as the following to receive the SNMP trap from the InsightPower SNMP Card.



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



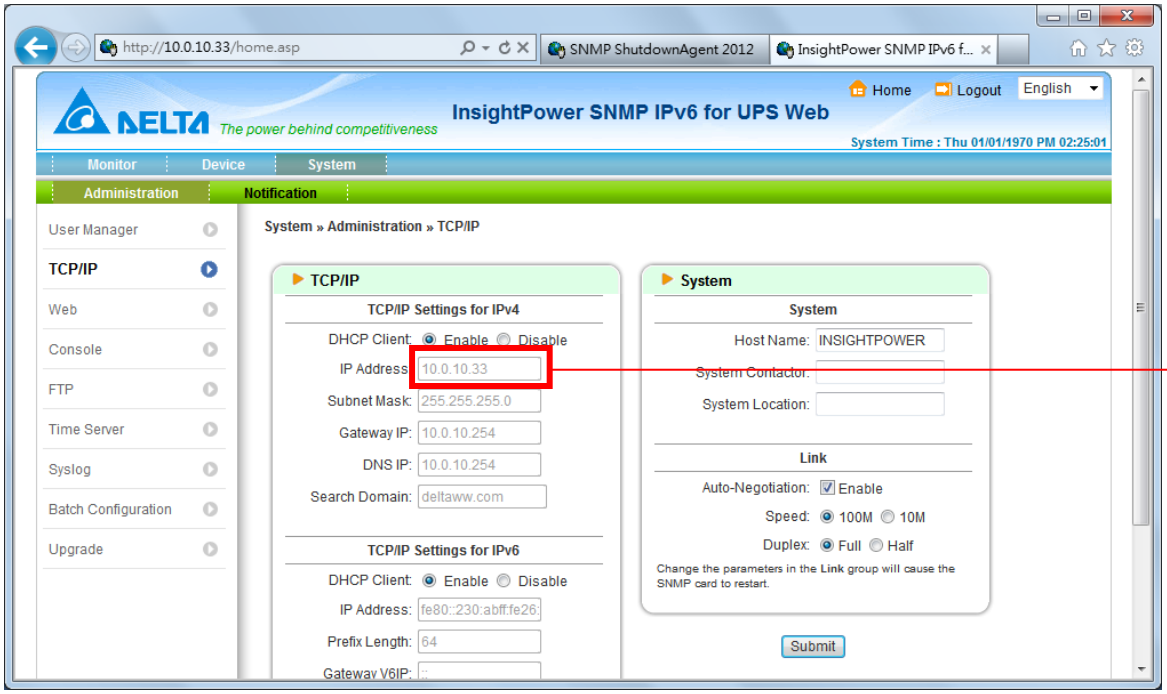
5. Add ShutdownAgent IP address to the SNMP Trap table in the InsightPower SNMP Card. Please select the "Information" for the Event Level and DeltaV4 as the Trap MIB Type.



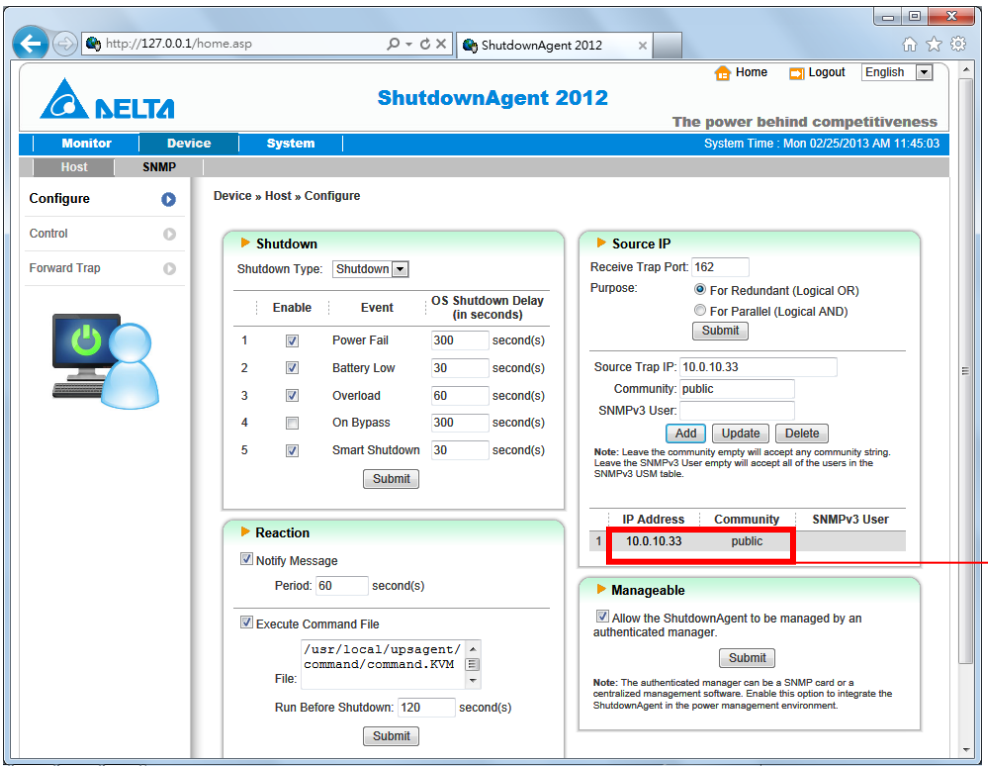
15.2 Delta InsightPower SNMP IPv6 Card

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

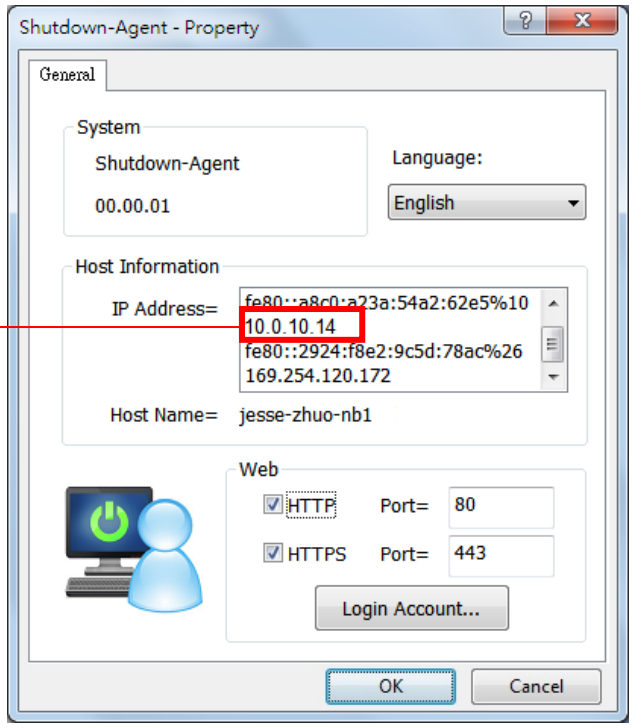
2. Record the IP address in the System Configuration web page. The SNMP Trap is assigned in the SNMP Trap web page individually.



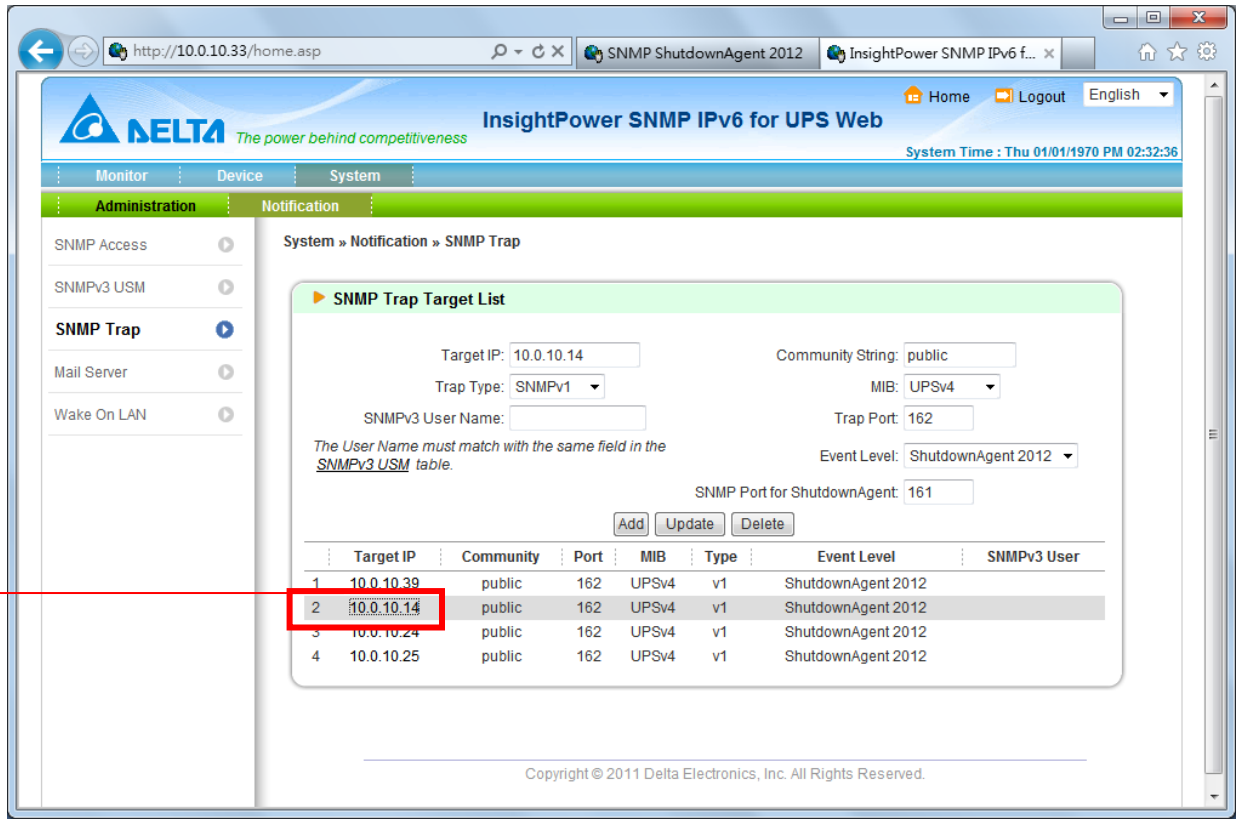
3. Login to ShutdownAgent web and add the SNMP IP address and the trap port as the following to receive the SNMP trap from the SNMP Card.



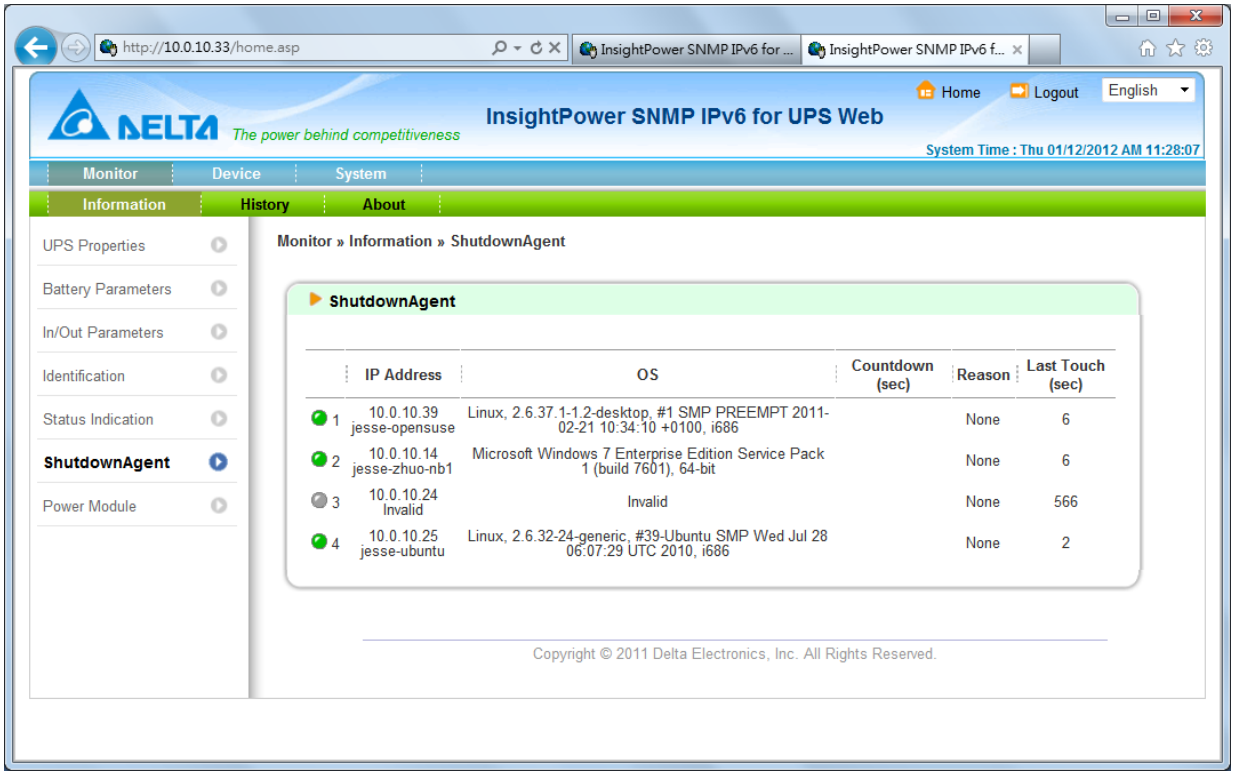
4. Open ShutdownAgent property from Windows task bar to get the IP address of the server.



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.



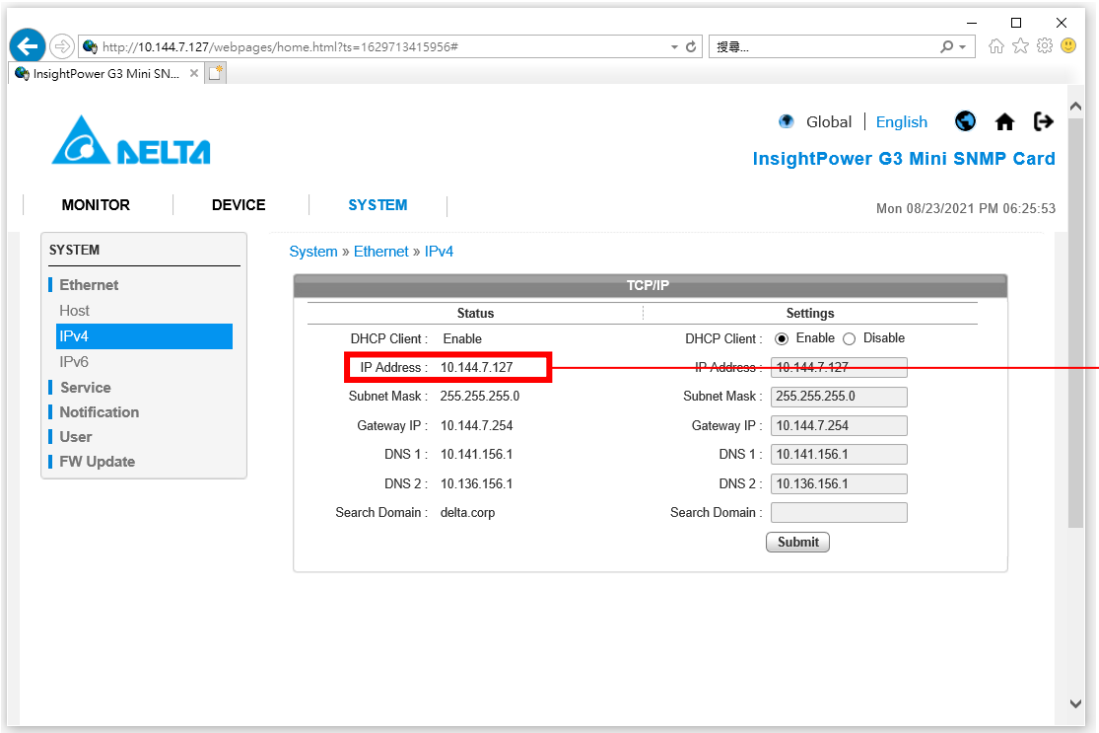
6. If you enable the manageable option in ShutdownAgent then you can observe all of the shutdown status, countdown timer and shutdown reason from the InsightPower SNMP IPv6 card. The web page is on the Monitor >> Information >> ShutdownAgent.



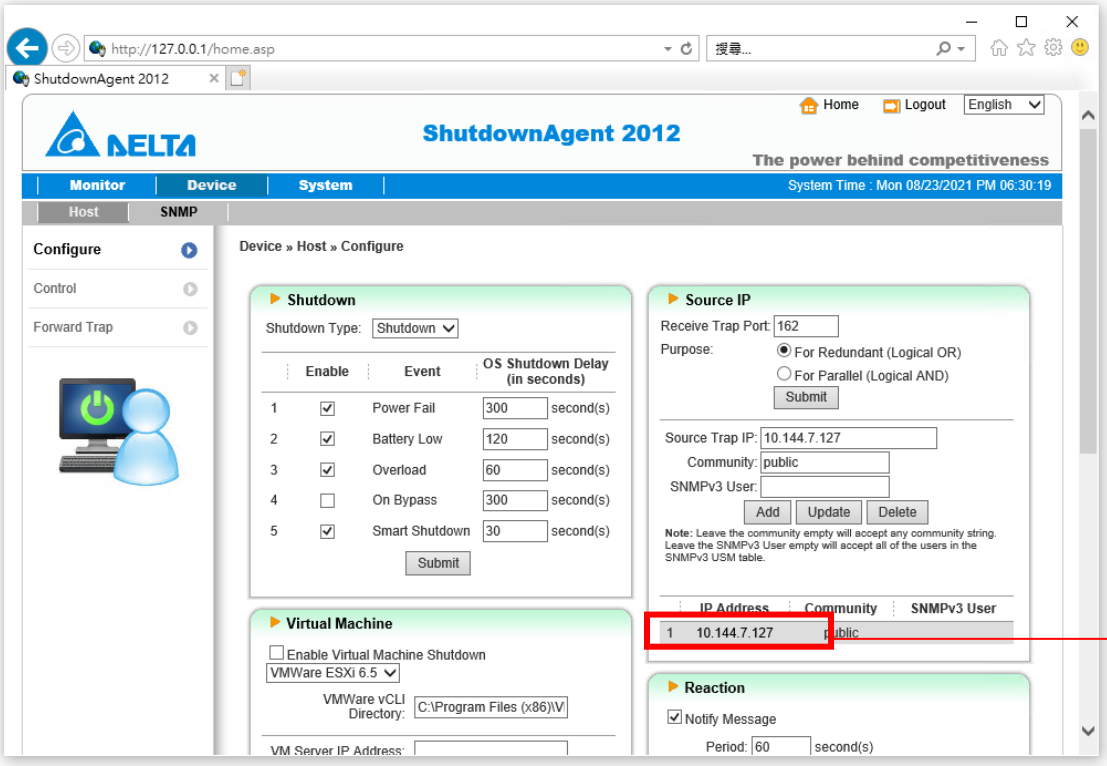
15.3 New Delta InsightPower G3 Mini SNMP Card

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

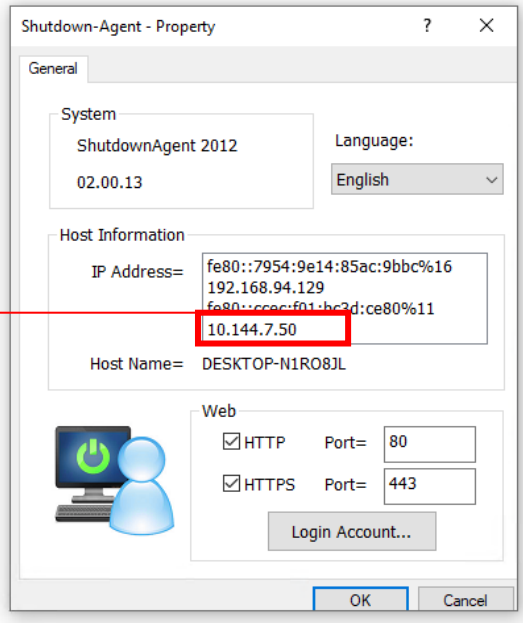
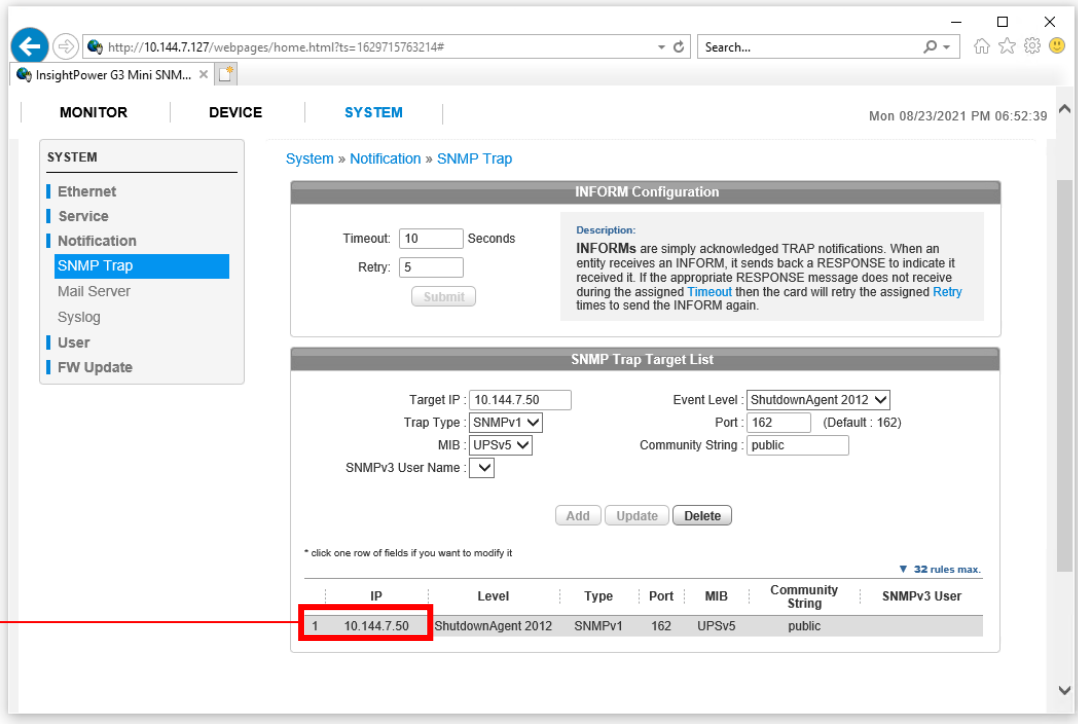
2. Record the IP address in the System Configuration web page. The SNMP Trap is assigned individually.



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



4. Go 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.