AlienVault 如何收集 Windows/Linux 平台資訊

1 AlienVault 如可收集 Windows 事件檢視器資料 2

2 AlienVault 如可收集 Windows 文字型 Log 10

3 AlienVault 如可收集 Linux Syslog 資訊 16

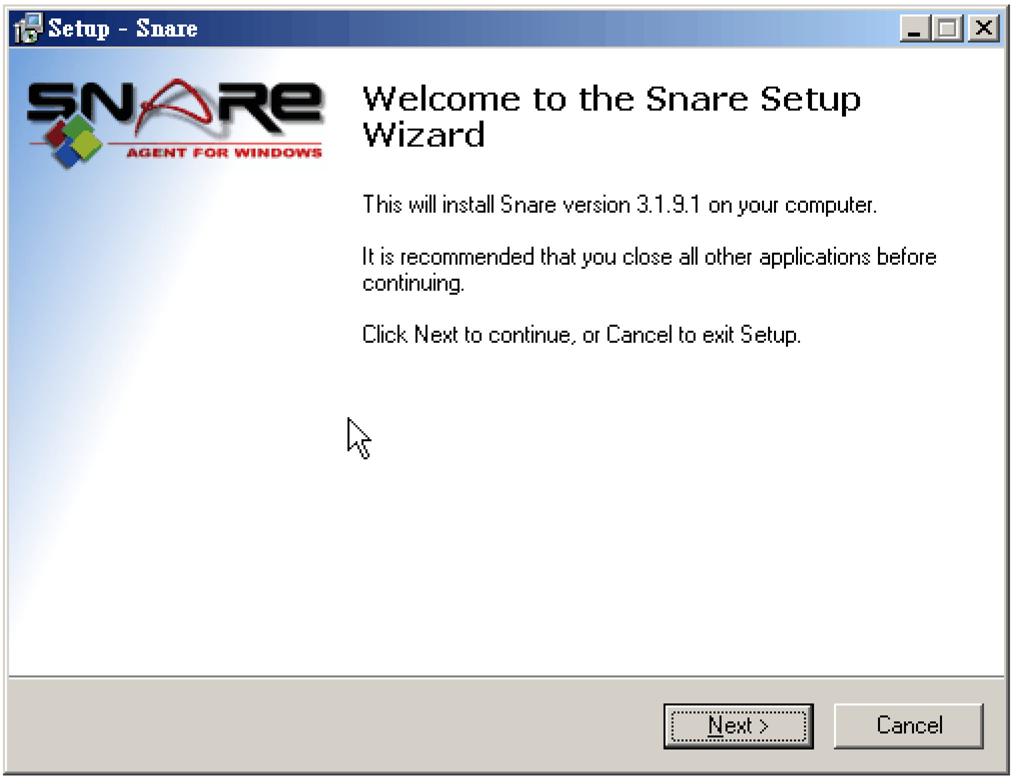
4 AlienVault 如可收集 Linux/Unix 文字型 Log 17

1 AlienVault 如可收集 Windows 事件檢視器資料

1. 下載 Snare Agent for Windows

http://www.intersectalliance.com/projects/index.html

2. 安裝 Snare Agent for Windows

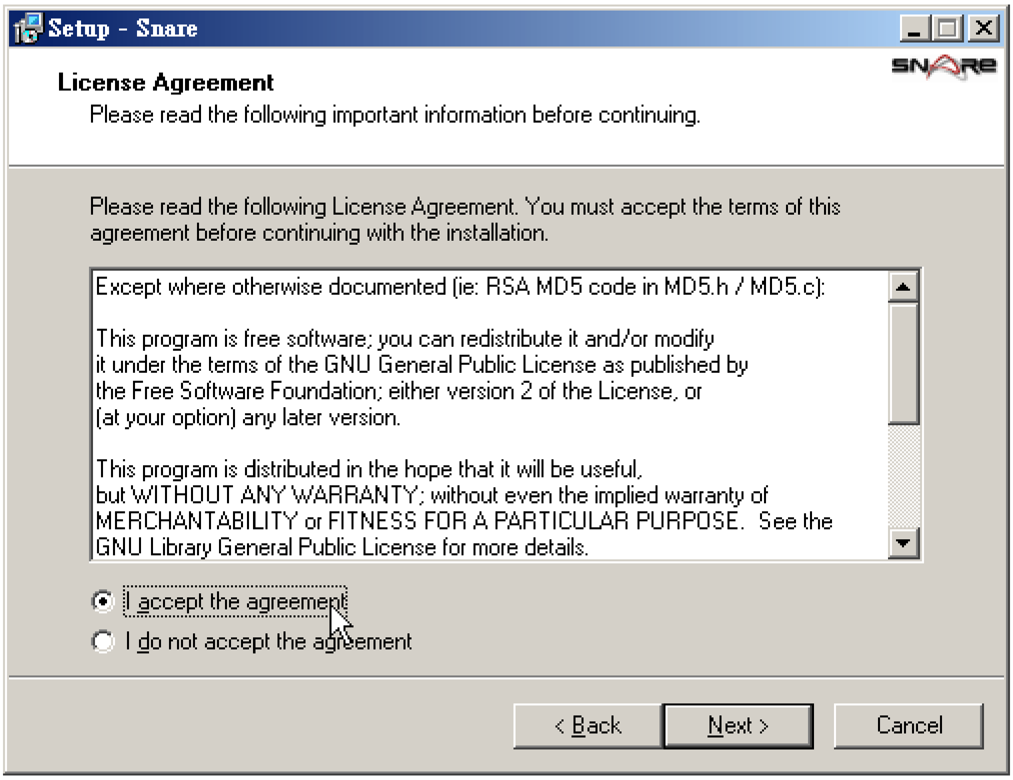


Welcome to the Snare Setup Wizard

This will install Snare version 3.1.9.1 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.



Setup - Snare

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

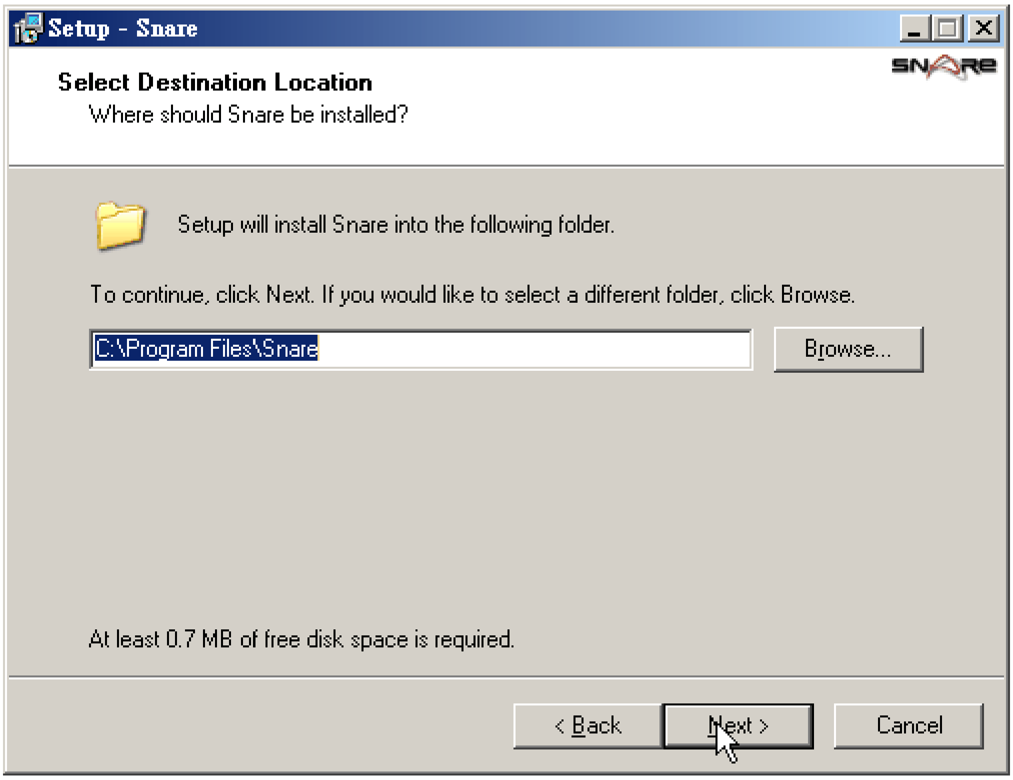
Except where otherwise documented (ie: RSA MD5 code in MD5.h / MD5.c):

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

● I accept the agreement

○ I do not accept the agreement



Setup - Snare

Select Destination Location

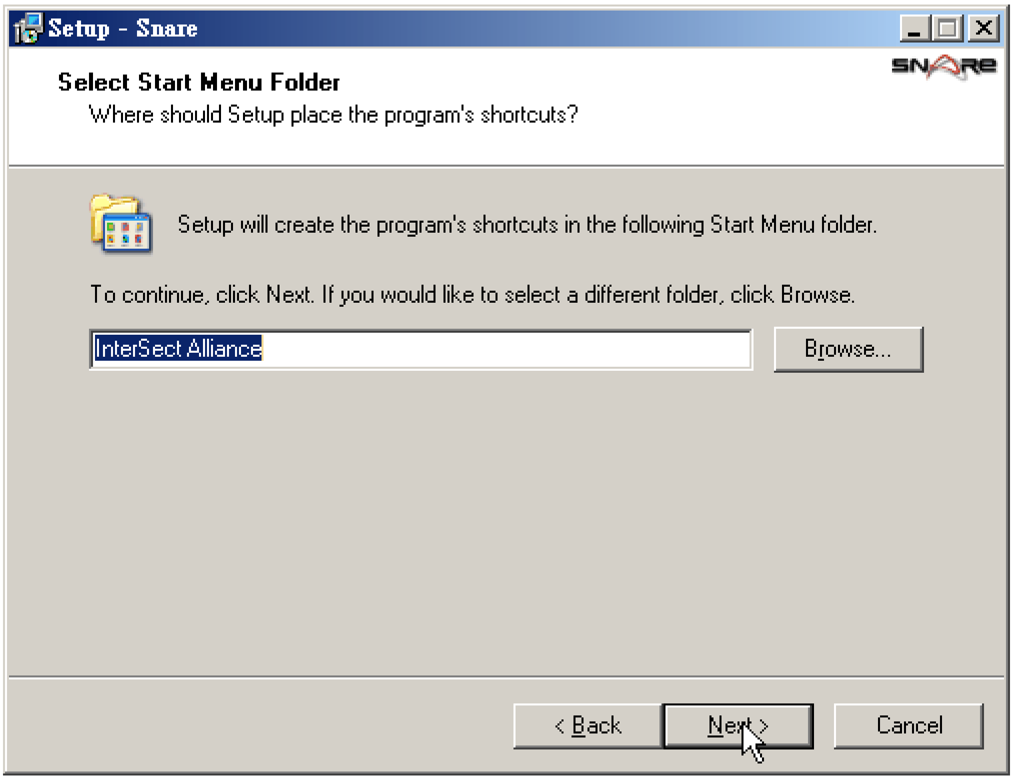
Where should Snare be installed?

Setup will install Snare into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Snare

At least 0.7 MB of free disk space is required.



Setup - Snare

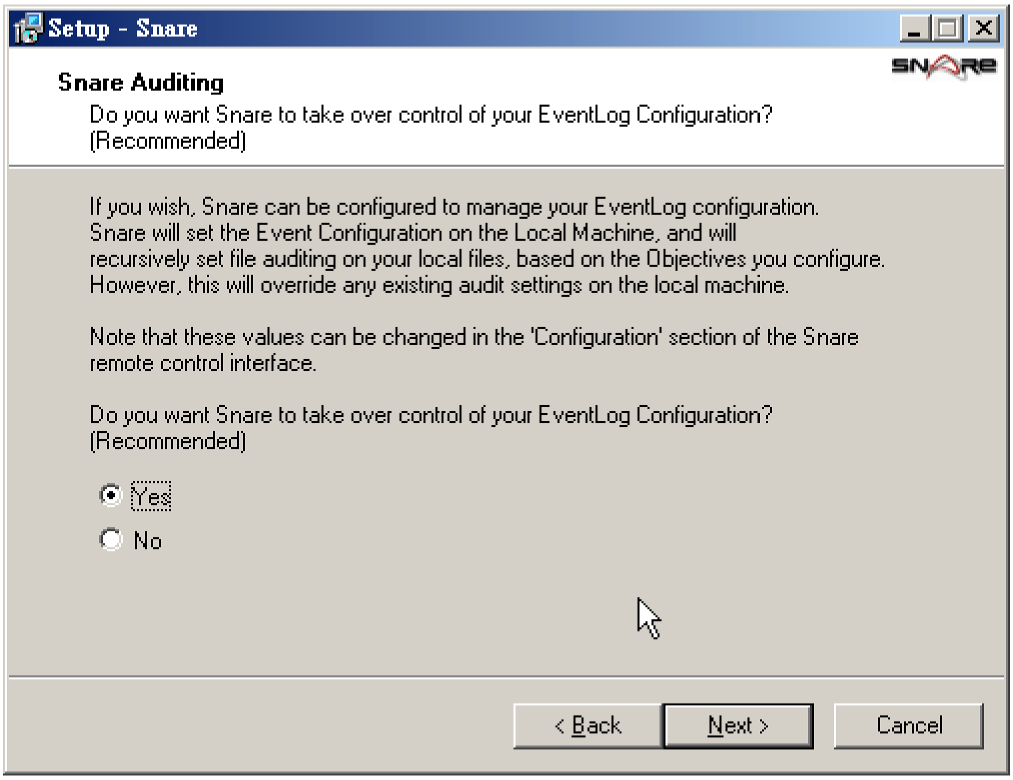
Select Start Menu Folder

Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

InterSect Alliance



Setup - Snare

Snare Auditing

Do you want Snare to take over control of your EventLog Configuration? (Recommended)

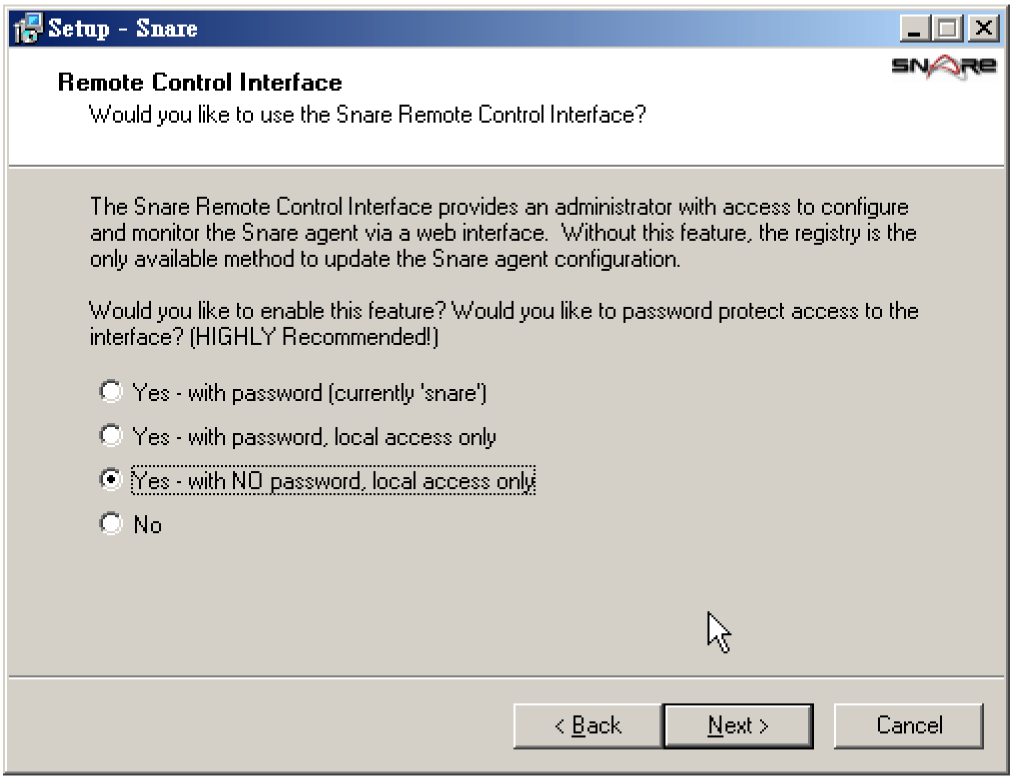
If you wish, Snare can be configured to manage your EventLog configuration. Snare will set the Event Configuration on the Local Machine, and will recursively set file auditing on your local files, based on the Objectives you configure. However, this will override any existing audit settings on the local machine.

Note that these values can be changed in the 'Configuration' section of the Snare remote control interface.

Do you want Snare to take over control of your EventLog Configuration? (Recommended)

● Yes

○ No



Remote Control Interface

Would you like to use the Snare Remote Control Interface?

The Snare Remote Control Interface provides an administrator with access to configure and monitor the Snare agent via a web interface. Without this feature, the registry is the only available method to update the Snare agent configuration.

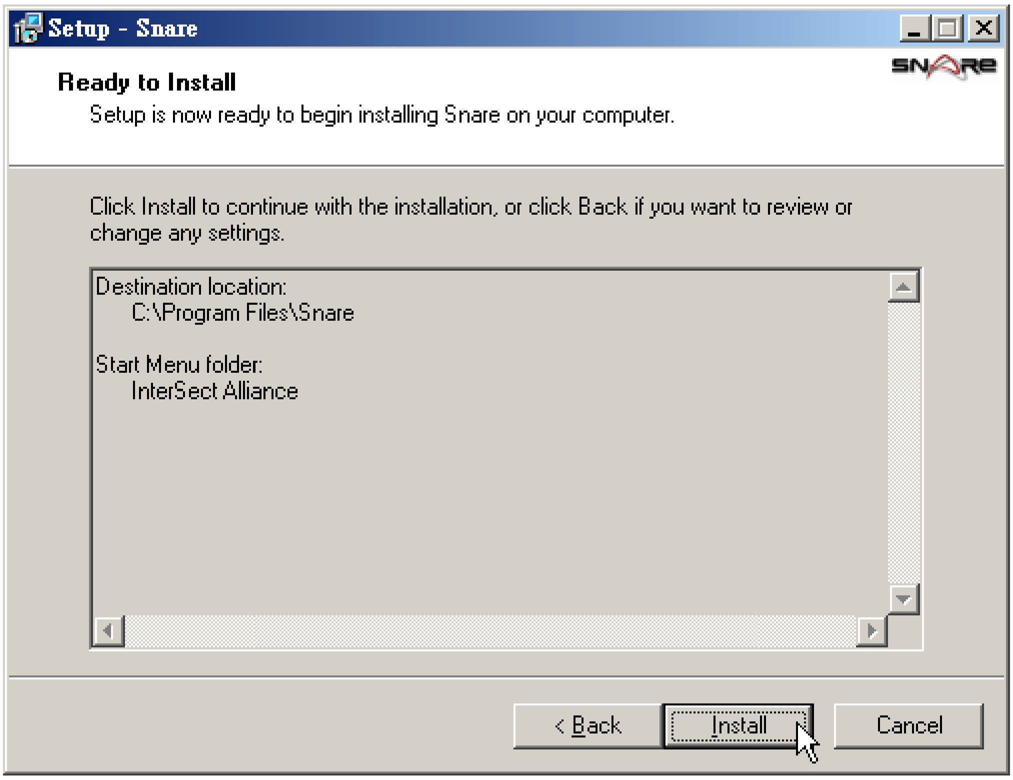
Would you like to enable this feature? Would you like to password protect access to the interface? (HIGHLY Recommended!)

○ Yes - with password (currently 'snare')

○ Yes - with password, local access only

● Yes - with NO password, local access only

○ No



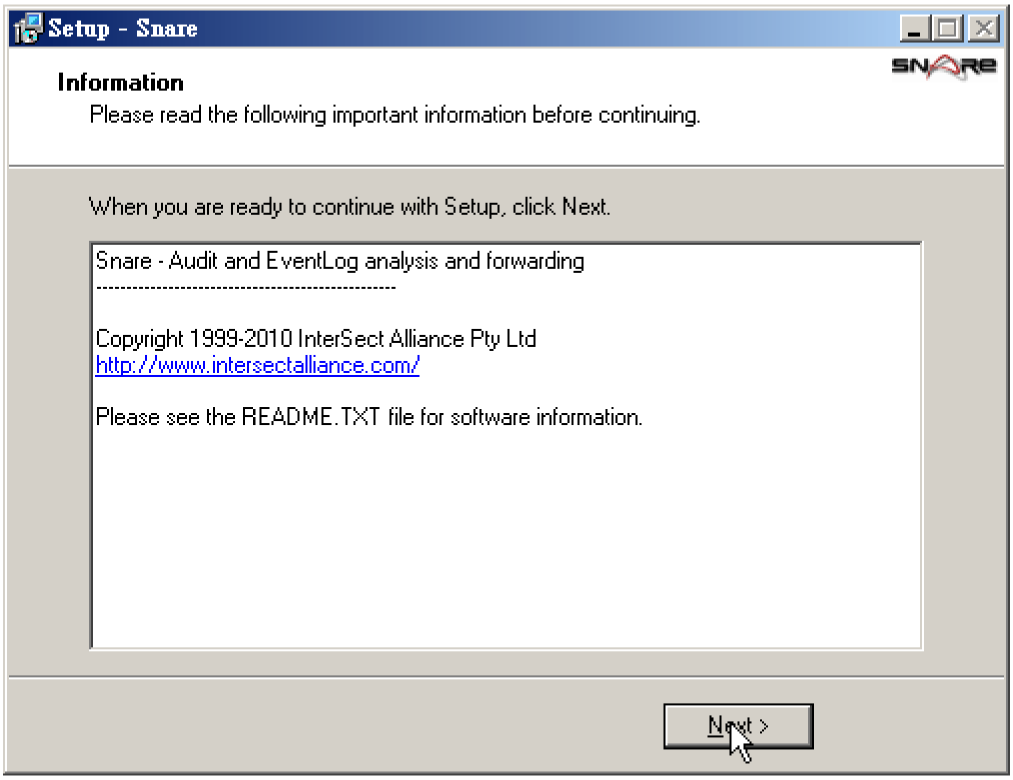
Ready to Install

Setup is now ready to begin installing Snare on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files\Snare

Start Menu folder:
InterSect Alliance



Information

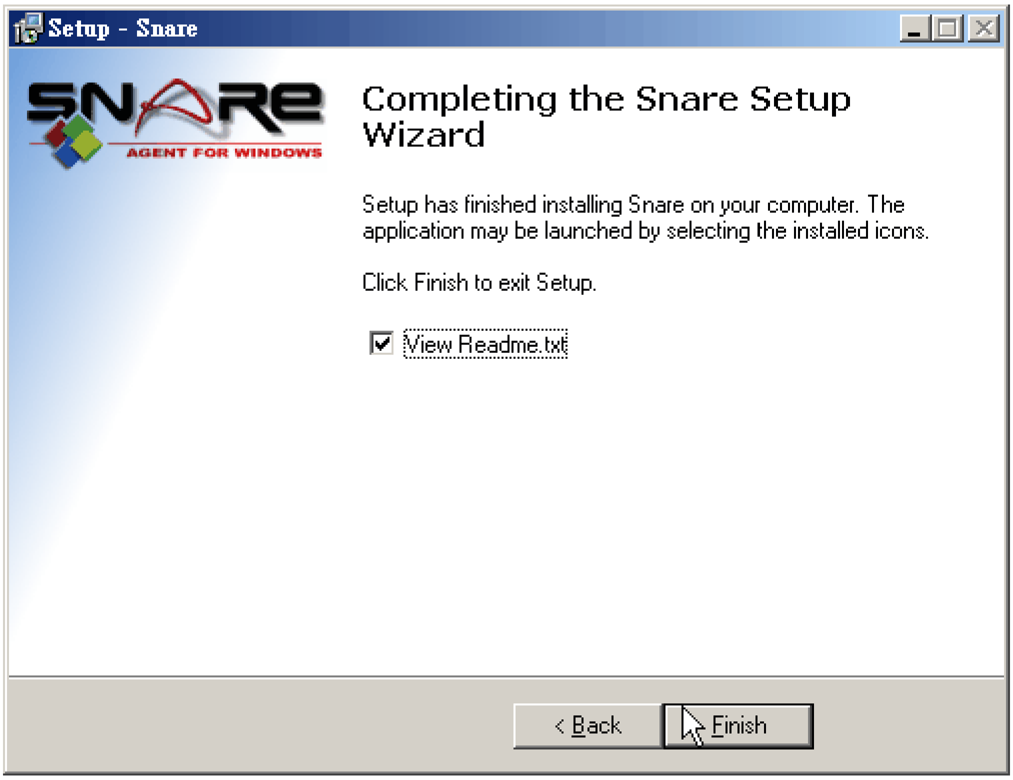
Please read the following important information before continuing.

When you are ready to continue with Setup, click Next.

Snare - Audit and EventLog analysis and forwarding

Copyright 1999-2010 InterSect Alliance Pty Ltd
http://www.intersectalliance.com/

Please see the README.TXT file for software information.



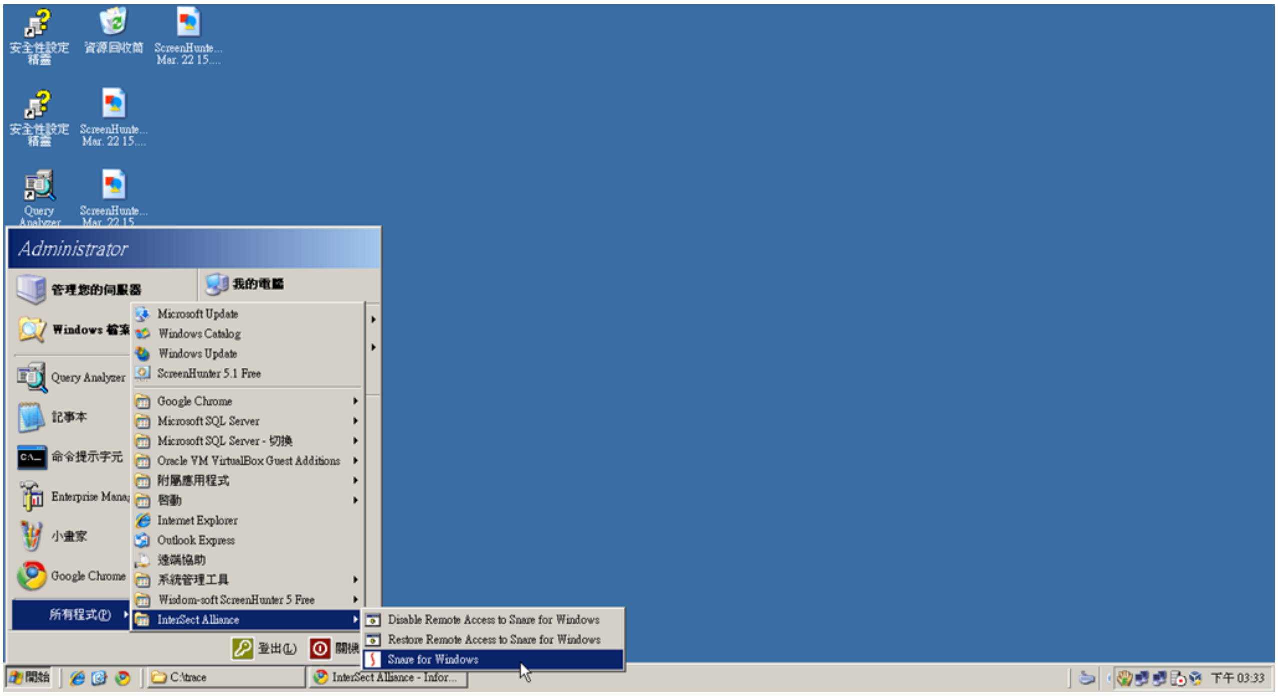
Completing the Snare Setup Wizard

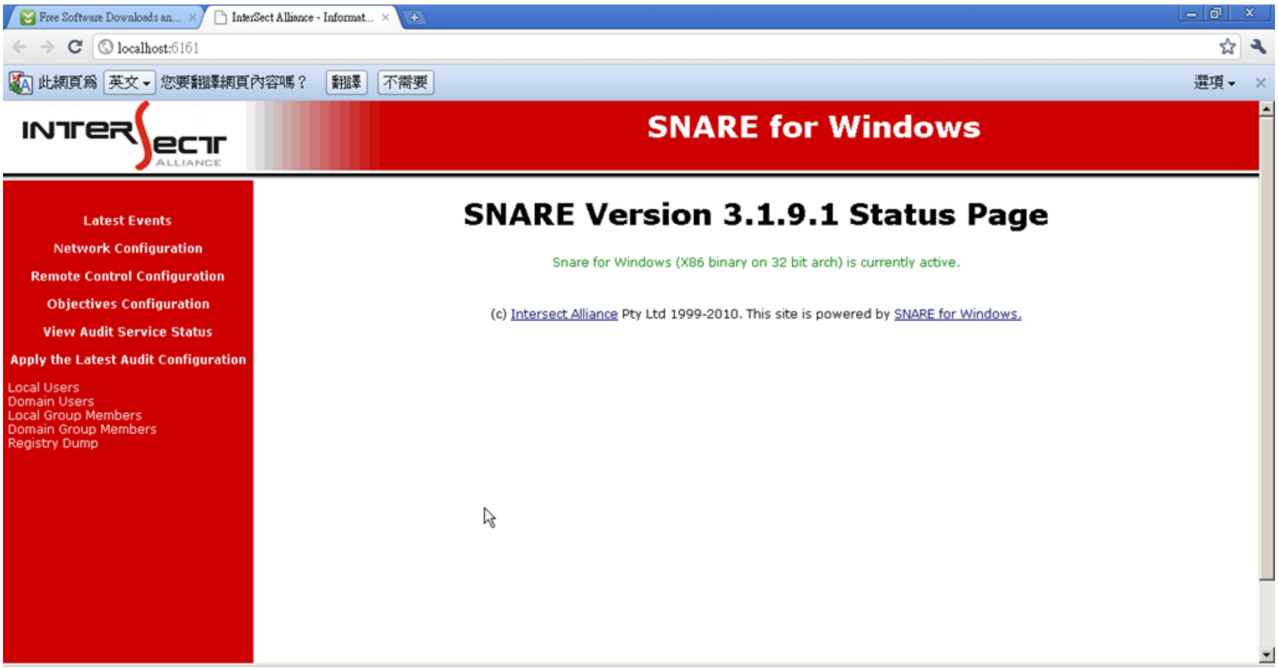
Setup has finished installing Snare on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ View Readme.txt

3. 設定 Snare Agent 參數




Free Software Downloads an...
InterSect Alliance - Informat...
localhost:6161
此網頁為 英文 您要翻譯網頁內容嗎？ 翻譯 不需要
選項
INTERSECT ALLIANCE

SNARE for Windows

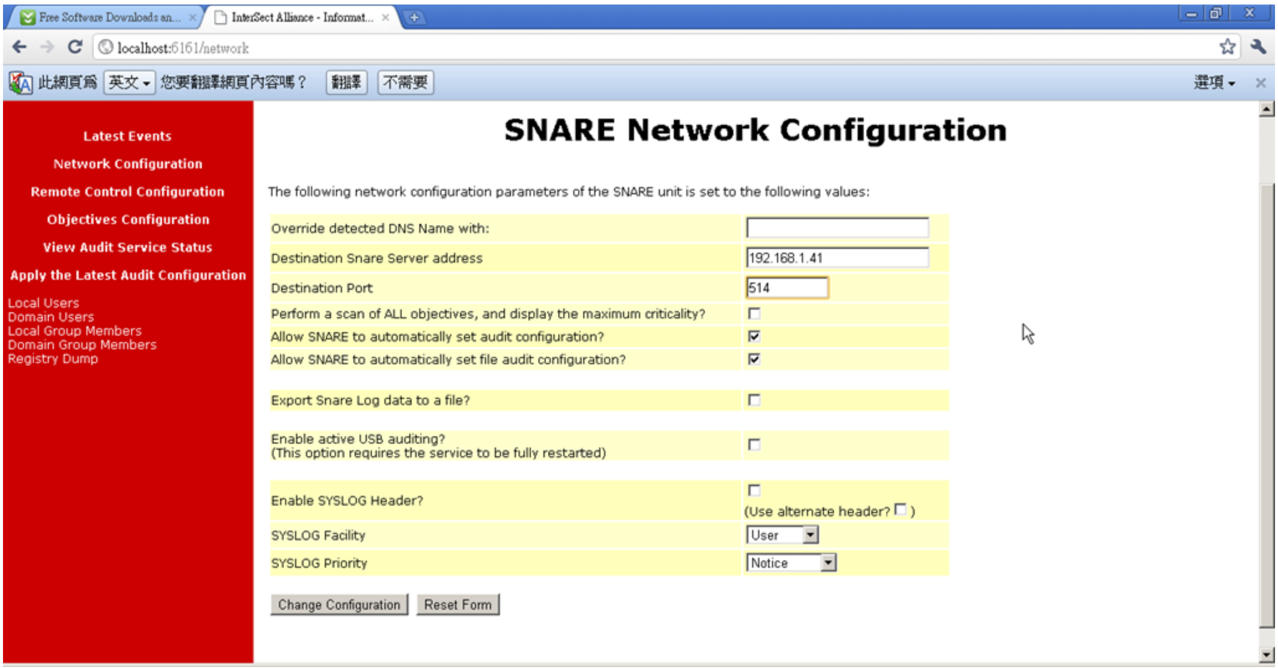
Latest Events
Network Configuration
Remote Control Configuration
Objectives Configuration
View Audit Service Status
Apply the Latest Audit Configuration

Local Users
Domain Users
Local Group Members
Domain Group Members
Registry Dump

SNARE Version 3.1.9.1 Status Page

Snare for Windows (X86 binary on 32 bit arch) is currently active.

(c) Intersect Alliance Pty Ltd 1999-2010. This site is powered by SNARE for Windows.


Free Software Downloads an...
InterSect Alliance - Informat...
localhost:6161/network
此網頁為 英文 您要翻譯網頁內容嗎？ 翻譯 不需要 選項
Latest Events
Network Configuration
Remote Control Configuration
Objectives Configuration
View Audit Service Status
Apply the Latest Audit Configuration
Local Users
Domain Users
Local Group Members
Domain Group Members
Registry Dump

SNARE Network Configuration

The following network configuration parameters of the SNARE unit is set to the following values:

Override detected DNS Name with:	
Destination Snare Server address	192.168.1.41
Destination Port	514
Perform a scan of ALL objectives, and display the maximum criticality?	□
Allow SNARE to automatically set audit configuration?	☑
Allow SNARE to automatically set file audit configuration?	☑
Export Snare Log data to a file?	□
Enable active USB auditing? (This option requires the service to be fully restarted)	□
Enable SYSLOG Header?	□ (Use alternate header? □)
SYSLOG Facility	User
SYSLOG Priority	Notice

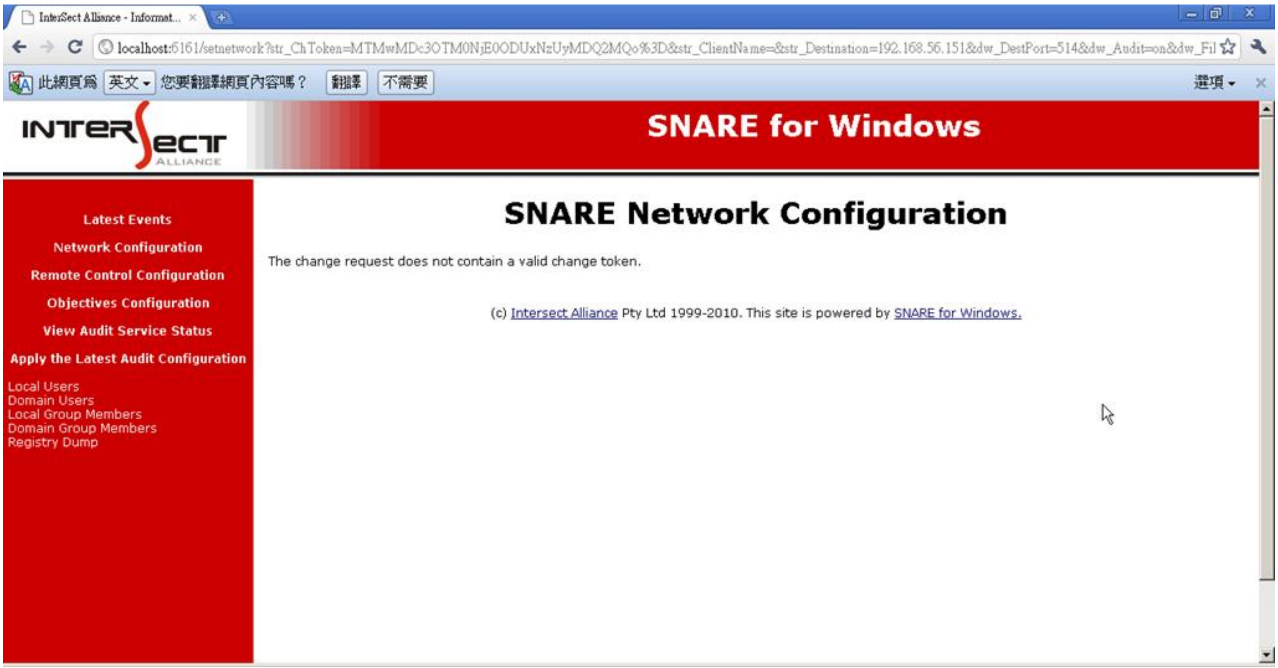
Destination Snare Server Address : 請設定為 AlienVault 主機 IP

Destination Port :請設定為 514 Port

SYSLOG Facility:依各單位需求設定或採用預設值

SYSLOG Priority:依各單位需求設定或採用預設值

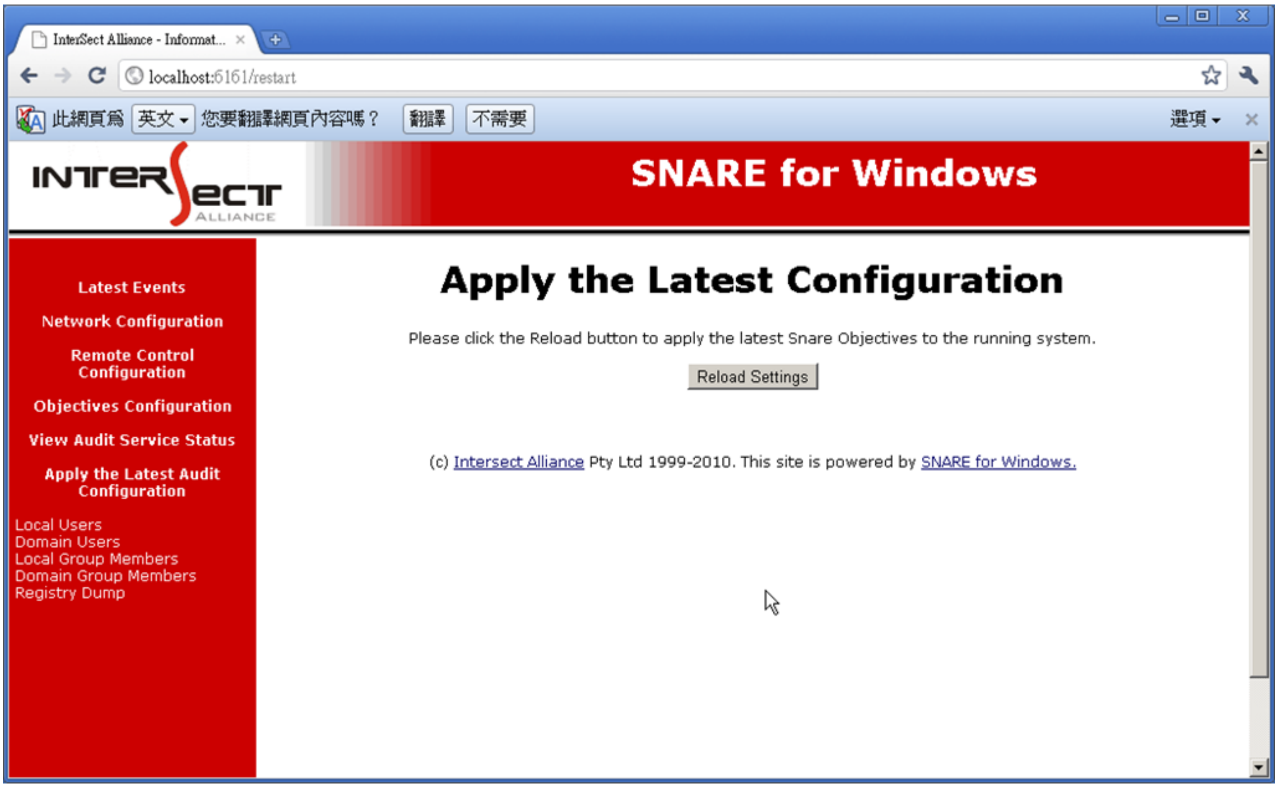
請按下:Change Configuration 完成設定


InterSect Alliance - Informat...
localhost:6161/setnetwork?str_ChToken=MTMwMDc3OTM0NjE0ODUxNzUyMDQ2MQo%3D&str_ClientName=&str_Destination=192.168.56.151&dw_DestPort=514&dw_Audit=on&dw_Fil
此網頁為 英文 您要翻譯網頁內容嗎？ 翻譯 不需要 選項
INTERSECT ALLIANCE
SNARE for Windows
Latest Events
Network Configuration
Remote Control Configuration
Objectives Configuration
View Audit Service Status
Apply the Latest Audit Configuration
Local Users
Domain Users
Local Group Members
Domain Group Members
Registry Dump

SNARE Network Configuration

The change request does not contain a valid change token.

(c) Intersect Alliance Pty Ltd 1999-2010. This site is powered by SNARE for Windows.



Apply the Latest Configuration

Please click the Reload button to apply the latest Snare Objectives to the running system.

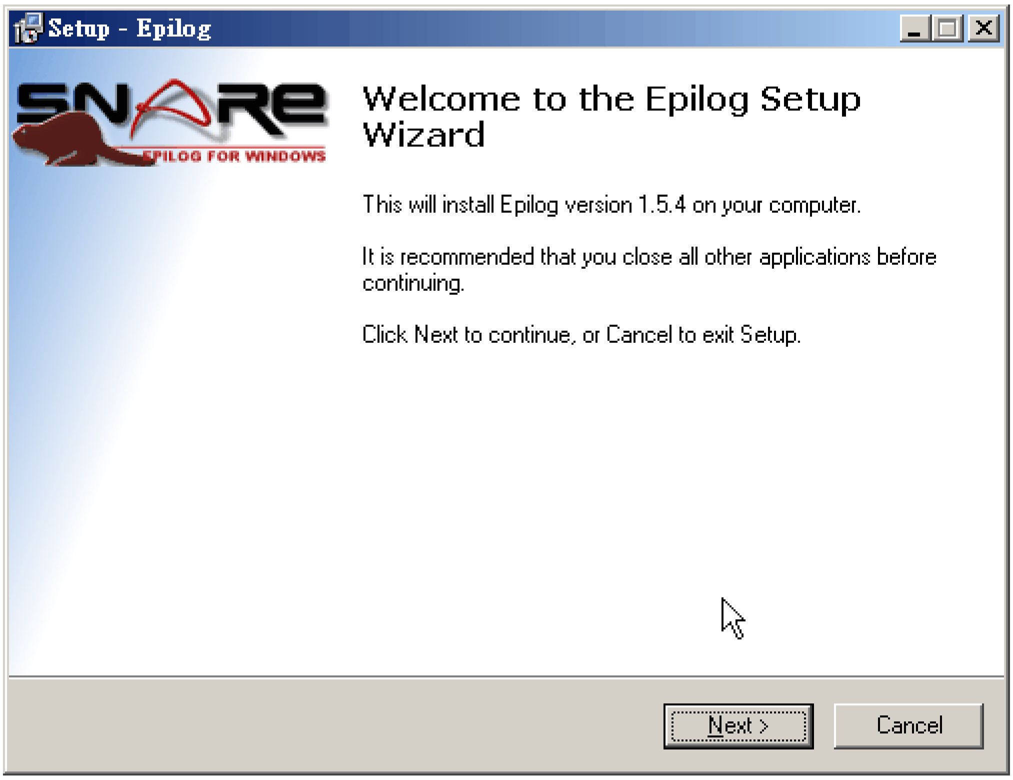
(c) Intersect Alliance Pty Ltd 1999-2010. This site is powered by SNARE for Windows.

請按下:Reload Settings 確認設定生效

2 AlienVault 如可收集 Windows 文字型 Log

1. 下載 Epilog Agent for Windows
http://www.intersectalliance.com/projects/index.html

2. 安裝 Epilog Agent for Windows

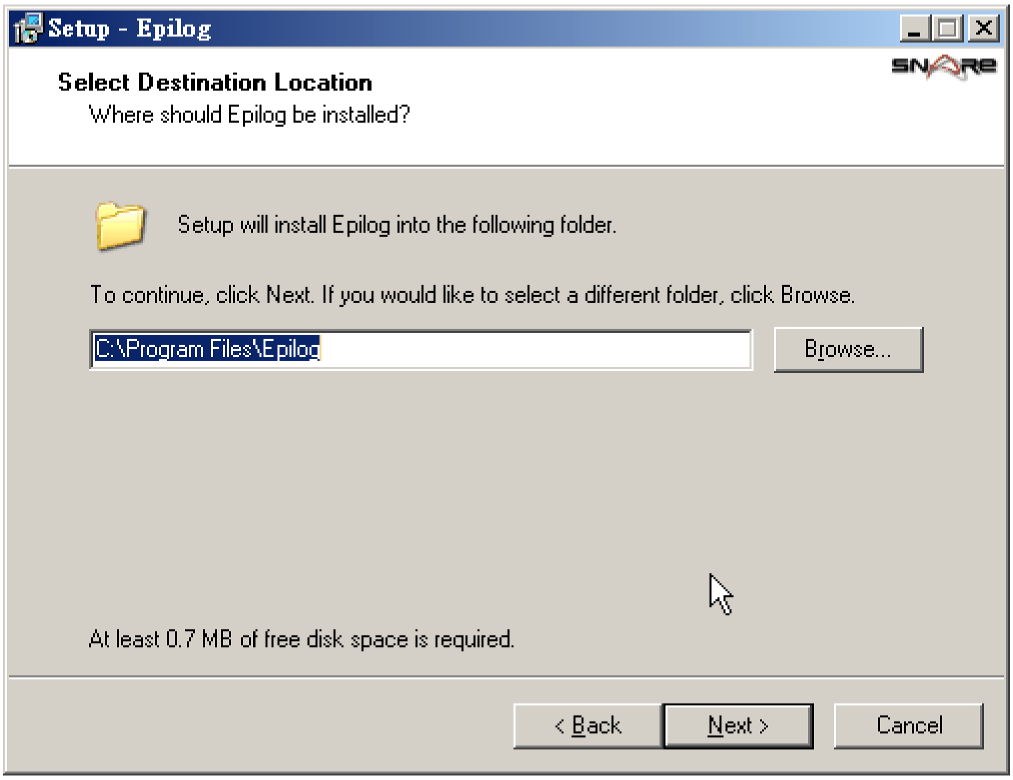


Welcome to the Epilog Setup Wizard

This will install Epilog version 1.5.4 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.



Select Destination Location

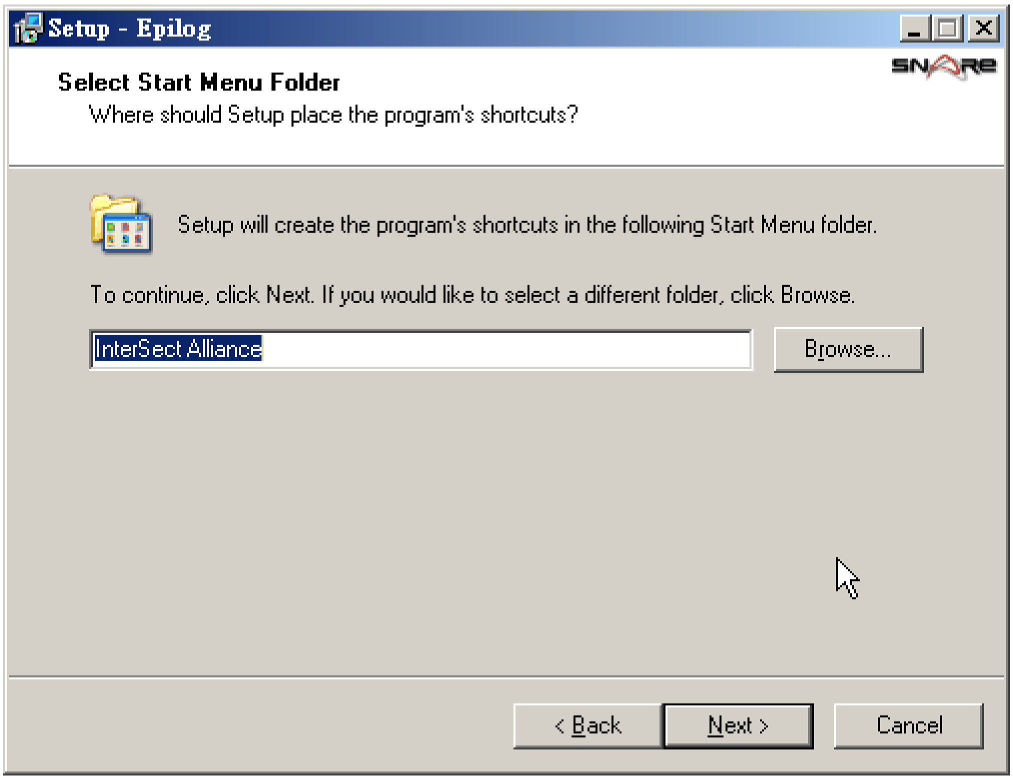
Where should Epilog be installed?

Setup will install Epilog into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Epilog

At least 0.7 MB of free disk space is required.



Setup - Epilog

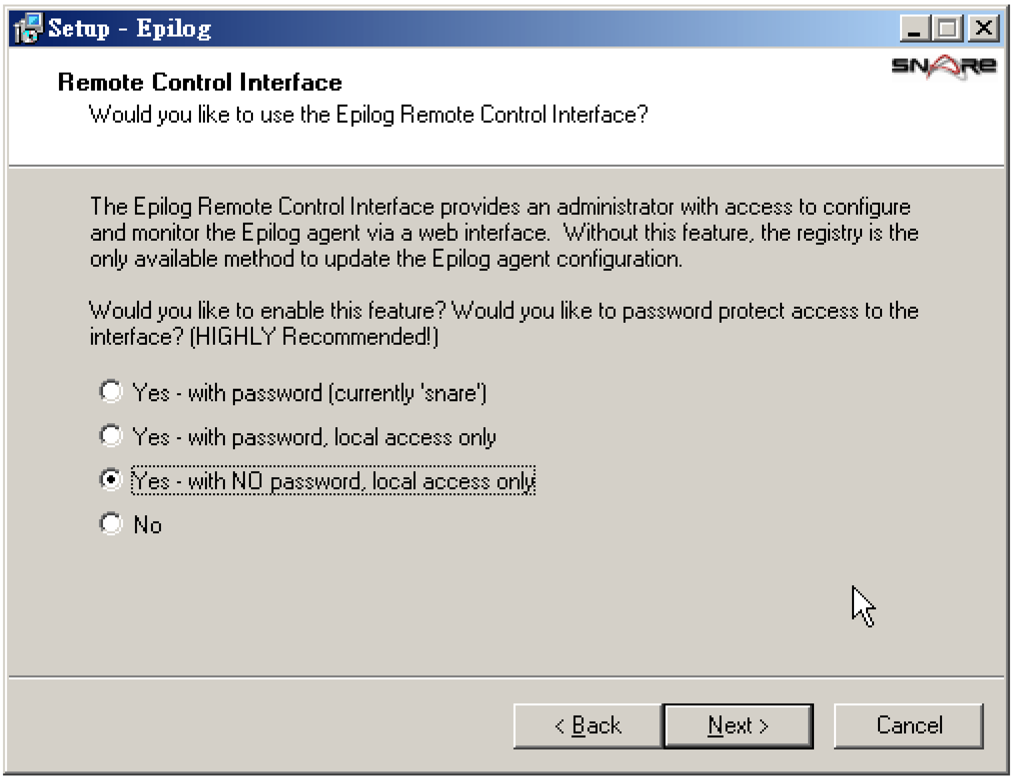
Select Start Menu Folder

Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

InterSect Alliance



Setup - Epilog

Remote Control Interface

Would you like to use the Epilog Remote Control Interface?

The Epilog Remote Control Interface provides an administrator with access to configure and monitor the Epilog agent via a web interface. Without this feature, the registry is the only available method to update the Epilog agent configuration.

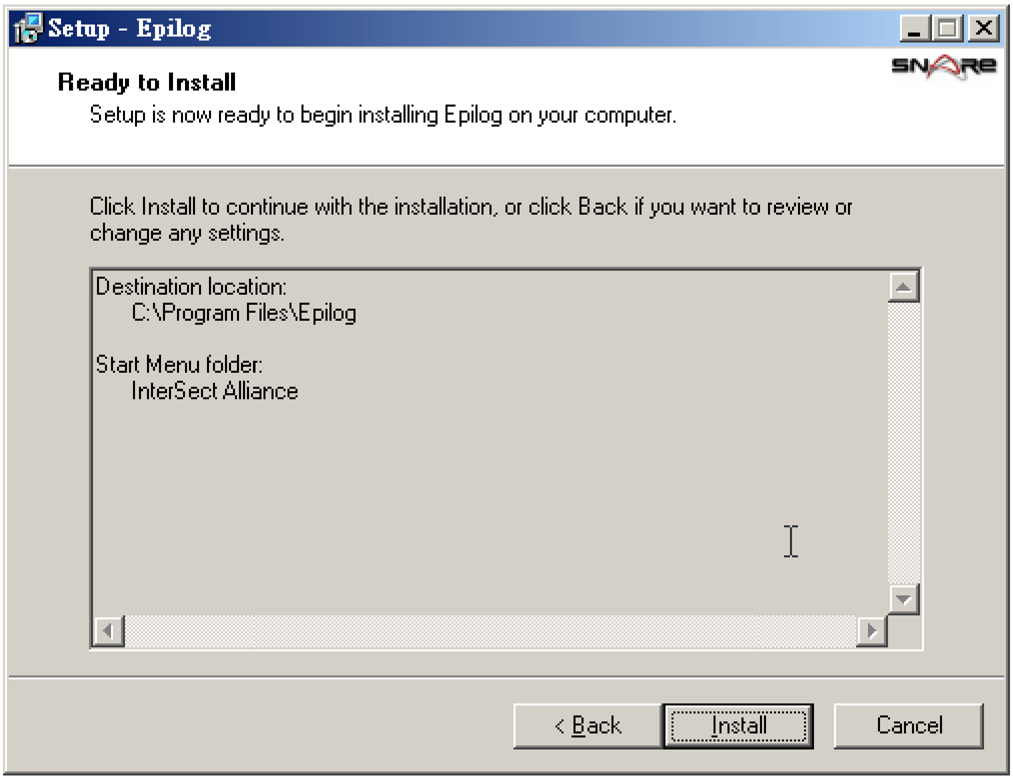
Would you like to enable this feature? Would you like to password protect access to the interface? (HIGHLY Recommended!)

○ Yes - with password (currently 'snare')

○ Yes - with password, local access only

● Yes - with NO password, local access only

○ No



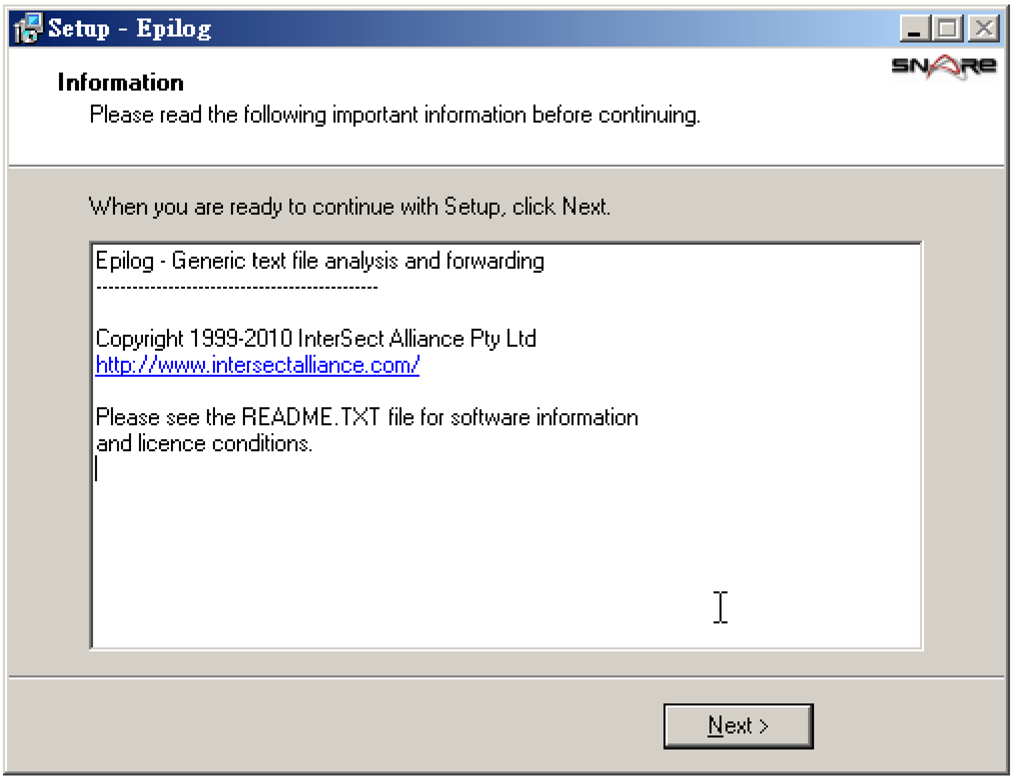
Ready to Install

Setup is now ready to begin installing Epilog on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
      C:\Program Files\Epilog

Start Menu folder:
      InterSect Alliance
```



Information

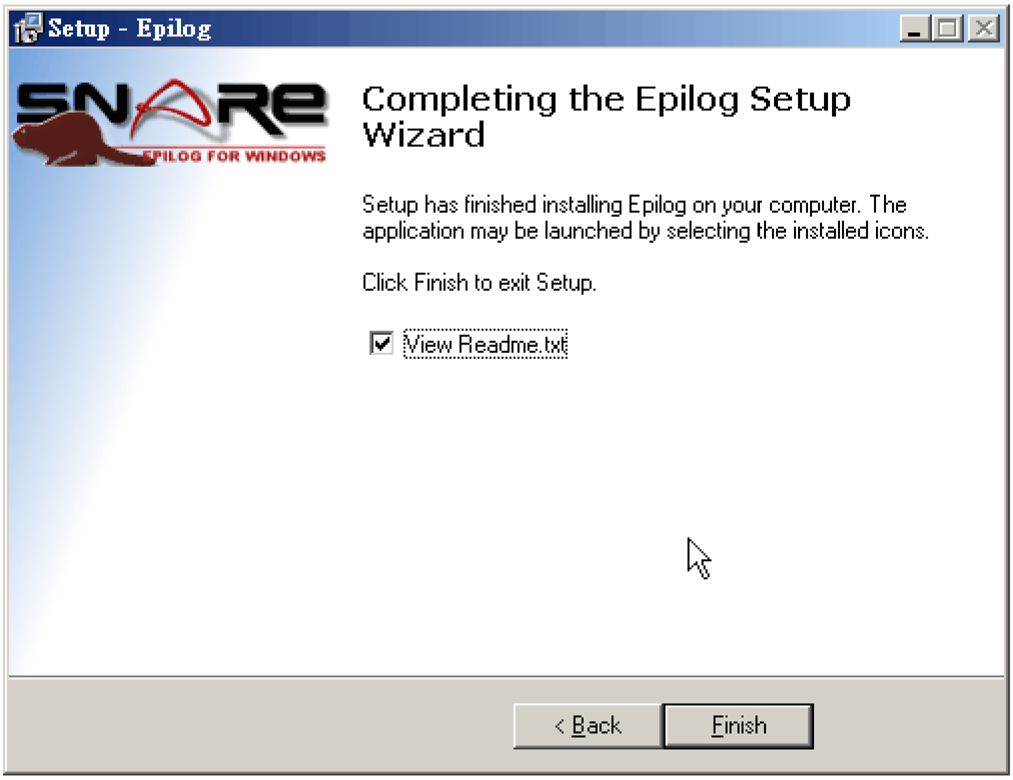
Please read the following important information before continuing.

When you are ready to continue with Setup, click Next.

```
Epilog - Generic text file analysis and forwarding
------------------------------------------------

Copyright 1999-2010 InterSect Alliance Pty Ltd
http://www.intersectalliance.com/

Please see the README.TXT file for software information
and licence conditions.
```



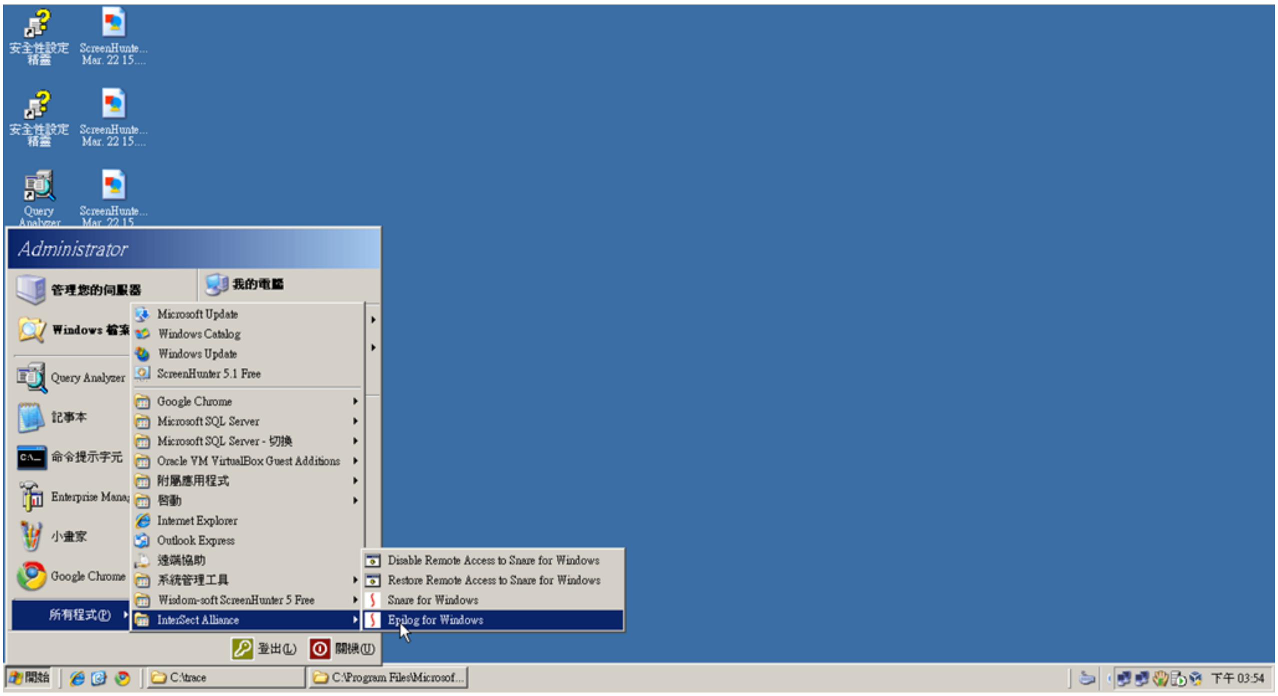
Completing the Epilog Setup Wizard

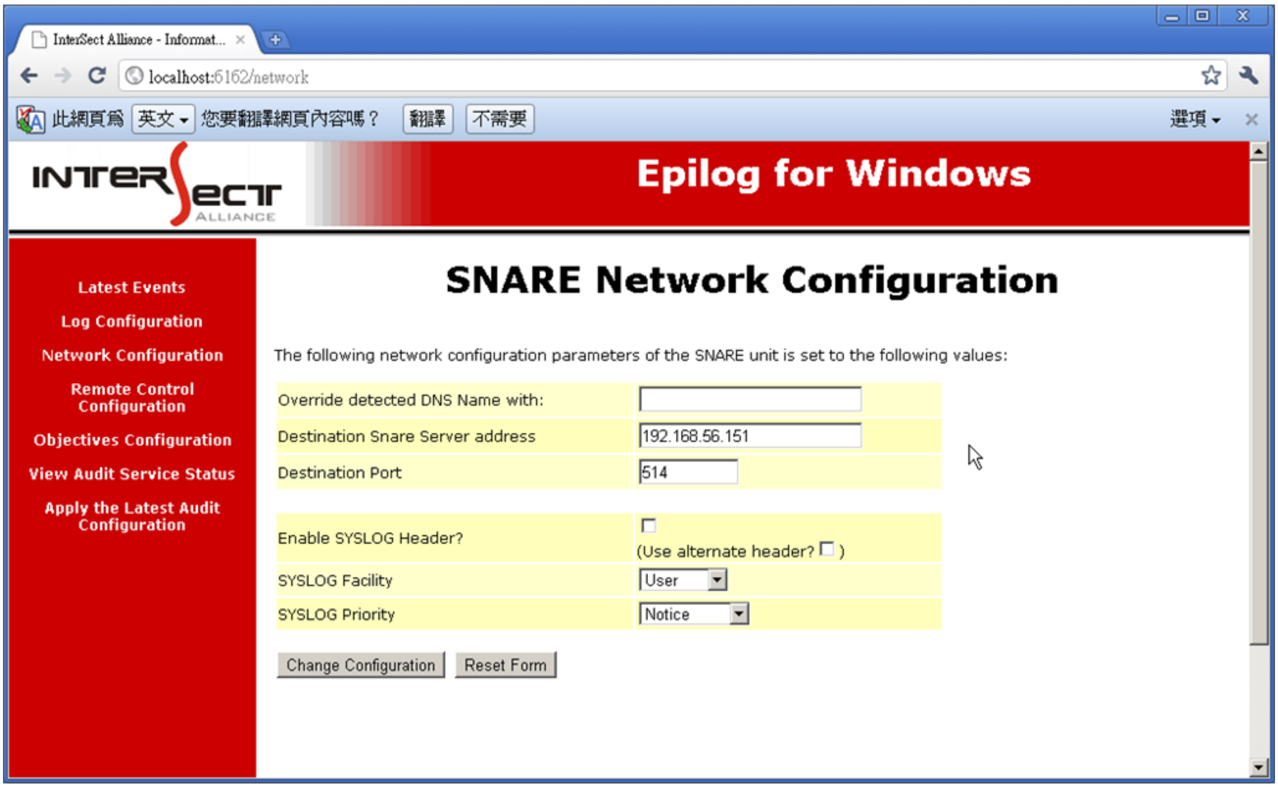
Setup has finished installing Epilog on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ View Readme.txt

3. 設定 Epilog Agent for Windows





Epilog for Windows

SNARE Network Configuration

The following network configuration parameters of the SNARE unit is set to the following values:

Override detected DNS Name with:	
Destination Snare Server address	192.168.56.151
Destination Port	514
Enable SYSLOG Header?	□ (Use alternate header? □)
SYSLOG Facility	User
SYSLOG Priority	Notice

Change Configuration　Reset Form

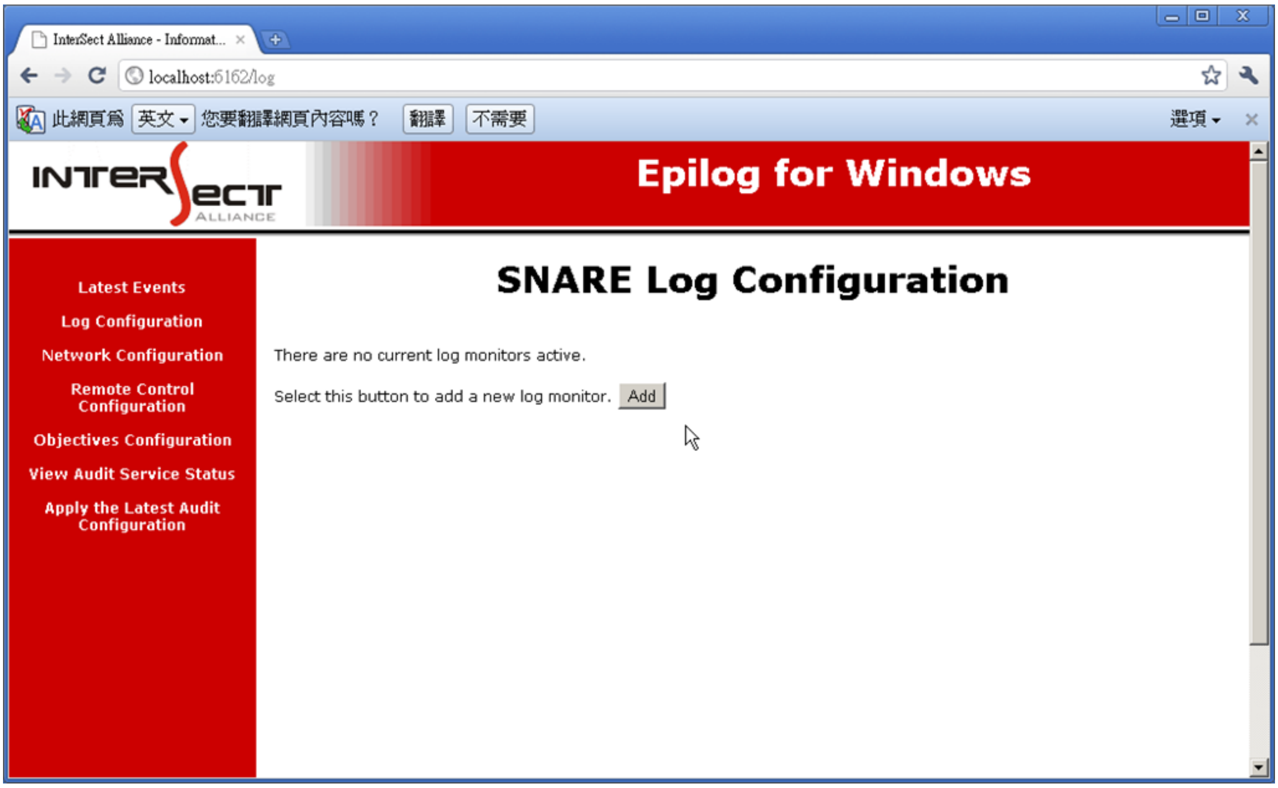
Destination Snare Server Address : 請設定為 AlienVault 主機 IP

Destination Port :請設定為 514 Port

SYSLOG Facility:依各單位需求設定或採用預設值

SYSLOG Priority:依各單位需求設定或採用預設值

請按下:Change Configuration 完成設定

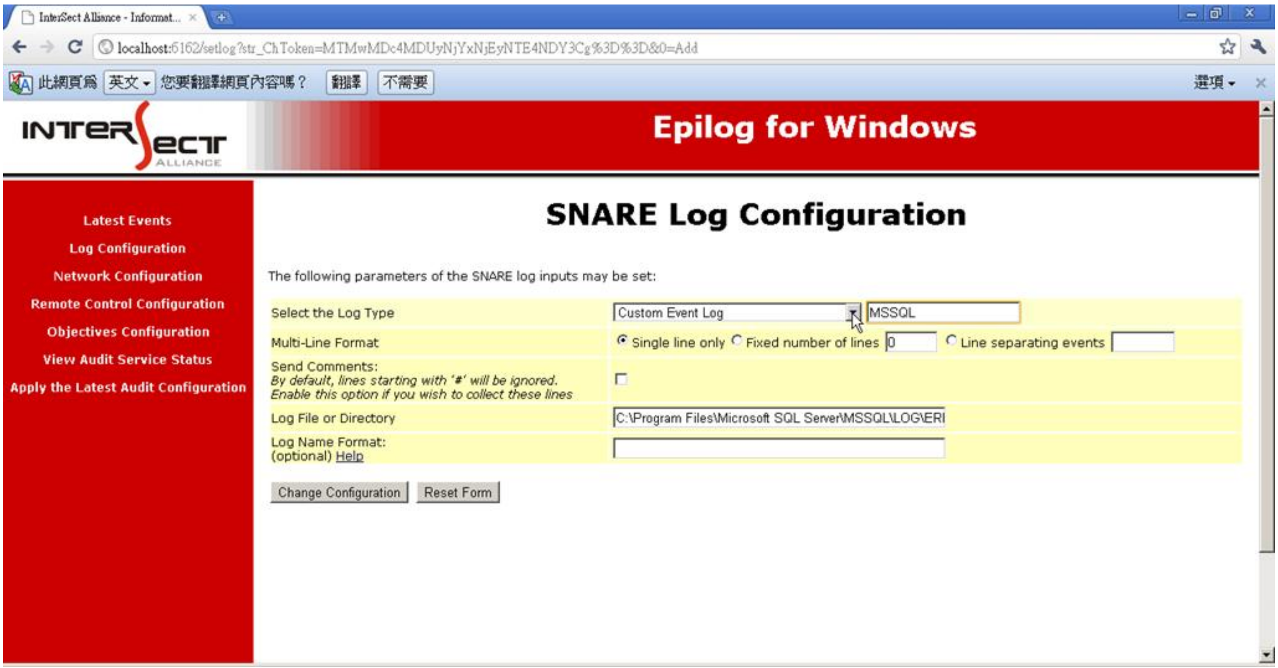


Epilog for Windows

SNARE Log Configuration

There are no current log monitors active.

Select this button to add a new log monitor. Add


InterSect Alliance - Informat...
localhost:6162/setlog?str_ChToken=MTMwMDc4MDUyNjYxNjEyNTE4NDY3Cg%3D%3D&0=Add
此網頁爲 英文 您要翻譯網頁內容嗎？ 翻譯 不需要 選項
INTERSECT ALLIANCE
Epilog for Windows
Latest Events
Log Configuration
Network Configuration
Remote Control Configuration
Objectives Configuration
View Audit Service Status
Apply the Latest Audit Configuration

SNARE Log Configuration

The following parameters of the SNARE log inputs may be set:

Select the Log Type	Custom Event Log MSSQL
Multi-Line Format	● Single line only ○ Fixed number of lines 0 ○ Line separating events
Send Comments: *By default, lines starting with '#' will be ignored.* *Enable this option if you wish to collect these lines*	□
Log File or Directory	C:\Program Files\Microsoft SQL Server\MSSQL\LOG\ERI
Log Name Format: (optional) Help	

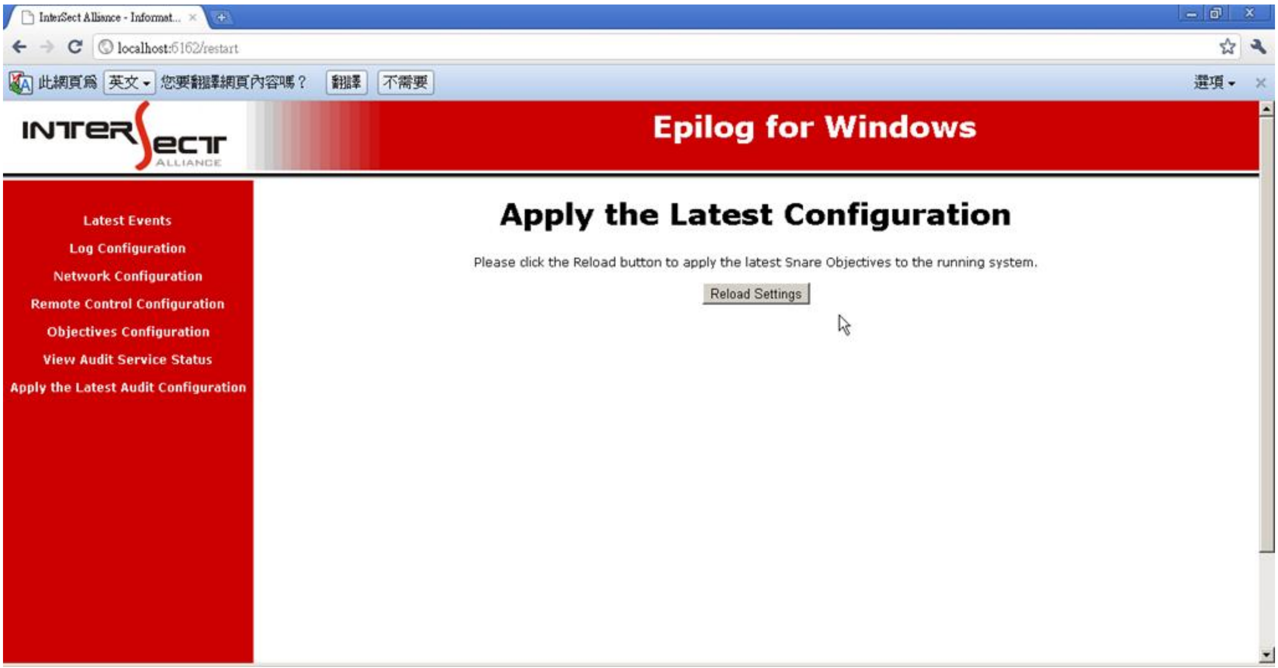
Change Configuration　Reset Form

Select the Log Type :Custom Event Log 輸入應用程式名程(請用數字及字母,不要用特殊字符)

Log File or Directory: 請輸入文字檔位置

Log Name Format : 依需求設定,如無特定需求請保持空白

請按下:Change Configuration 完成設定


InterSect Alliance - Informat...
localhost:6162/restart
此網頁爲 英文 您要翻譯網頁內容嗎？ 翻譯 不需要 選項
INTERSECT ALLIANCE
Epilog for Windows
Latest Events
Log Configuration
Network Configuration
Remote Control Configuration
Objectives Configuration
View Audit Service Status
Apply the Latest Audit Configuration
Reload Settings

Apply the Latest Configuration

Please click the Reload button to apply the latest Snare Objectives to the running system.

請按下:Reload Settings 確認設定生效

3 AlienVault 如可收集 Linux Syslog 資訊

1. Ubuntu /Debain 平台,於/etc/rsyslog.conf 中新增以下內容

1. 將所有資訊傳送至 AlienVault 主機,本機不保留 Log

```
*.*                    @ALIENVAULT_IP:514
ex.
*.*                    @192.168..41:514
```

2. 將所有資訊傳送至 AlienVault 主機,本機同時保留 Log

```
*.*                    @ALIENVAULT_IP:514
ex.
*.*                     @@192.168.1.41:514
```

2. CentOS 平台/etc/syslog.conf

1. 將所有資訊傳送至 AlienVault 主機,本機不保留 Log

```
*.*                    @ALIENVAULT_IP
ex.
*.*                    @192.168..41:514
```

2. 將所有資訊傳送至 AlienVault 主機,本機同時保留 Log(部分 **CentOS** 只有第一個方式)

```
*.*                    @@ALIENVAULT_IP
ex.
*.*                     @@192.168.1.41
```

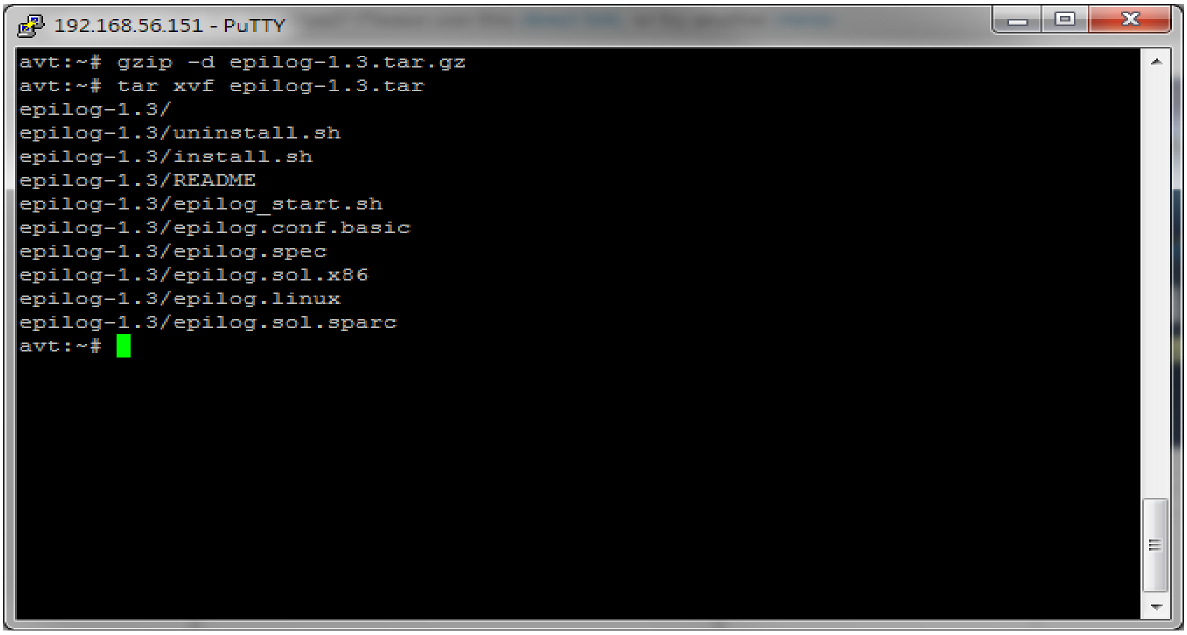
4 AlienVault 如可收集 Linux/Unix 文字型 Log

3. 下載 Epilog Agent for Unix (script)

http://www.intersectalliance.com/projects/index.html

4. 安裝 Epilog Agent for Unix

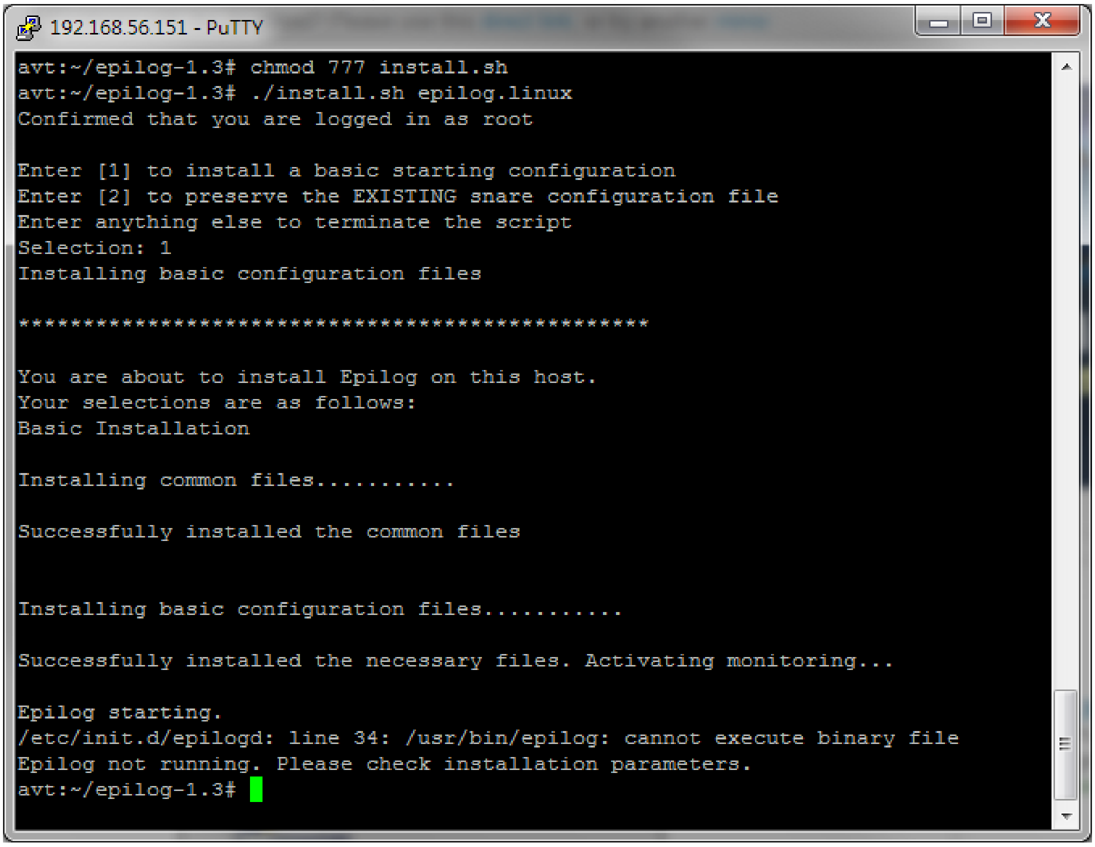
解壓縮 epilog 檔



```
avt:~# gzip -d epilog-1.3.tar.gz
avt:~# tar xvf epilog-1.3.tar
epilog-1.3/
epilog-1.3/uninstall.sh
epilog-1.3/install.sh
epilog-1.3/README
epilog-1.3/epilog_start.sh
epilog-1.3/epilog.conf.basic
epilog-1.3/epilog.spec
epilog-1.3/epilog.sol.x86
epilog-1.3/epilog.linux
epilog-1.3/epilog.sol.sparc
avt:~# 
```

1.改 script 為可執行

2.安裝 snare (參數有 epilog.sol.sparc / epilog.sol.x86 / epilog.linux)



```
avt:~/epilog-1.3# chmod 777 install.sh
avt:~/epilog-1.3# ./install.sh epilog.linux
Confirmed that you are logged in as root

Enter [1] to install a basic starting configuration
Enter [2] to preserve the EXISTING snare configuration file
Enter anything else to terminate the script
Selection: 1
Installing basic configuration files

*************************************************

You are about to install Epilog on this host.
Your selections are as follows:
Basic Installation

Installing common files...........

Successfully installed the common files


Installing basic configuration files...........

Successfully installed the necessary files. Activating monitoring...

Epilog starting.
/etc/init.d/epilogd: line 34: /usr/bin/epilog: cannot execute binary file
Epilog not running. Please check installation parameters.
avt:~/epilog-1.3# 
```

如果在安裝時有問題請下載 source code 版安裝

修改 config

vi /etc/snare/epilog/epilog.conf

請修改 Output ,Input 及 Remote 兩參數

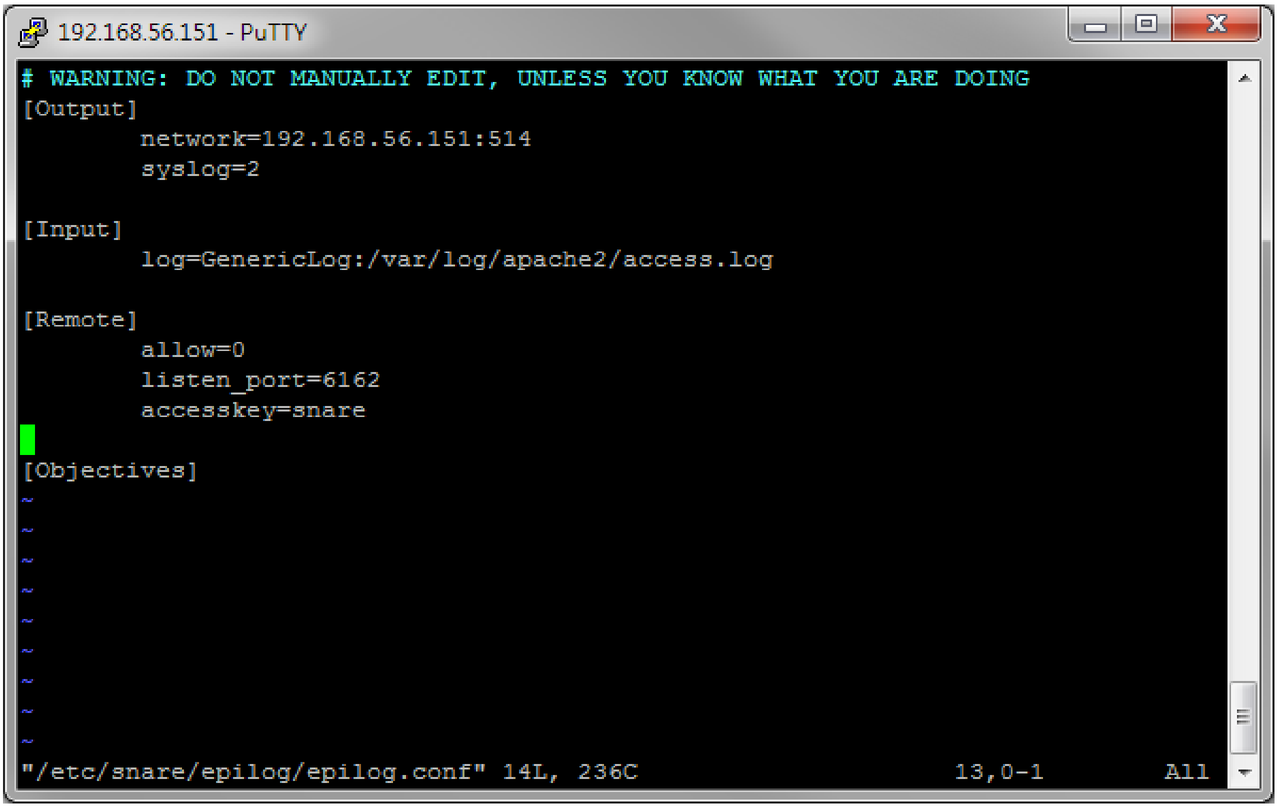
[Output]

Network 為 alienvault 主機及接收 syslog 的 port

[Input] 為要監控的檔案,可為多行

[Remote]

allow 請設為0 (不可遠端控制 snare)



```
# WARNING: DO NOT MANUALLY EDIT, UNLESS YOU KNOW WHAT YOU ARE DOING
[Output]
        network=192.168.56.151:514
        syslog=2

[Input]
        log=GenericLog:/var/log/apache2/access.log

[Remote]
        allow=0
        listen_port=6162
        accesskey=snare

[Objectives]
~
~
~
~
~
~
~
~
~
"/etc/snare/epilog/epilog.conf" 14L, 236C                    13,0-1        All
```

重啟 snare 服務,進行傳送 log

/etc/init.d/epilogd restart

如何加入開機自動執行 snare(此方式依不同之 linux or unix 略有不同)

# 確認主機使用那個 runlevel (本範例為 2)

vi /etc/inittab

檔案內容:

# The default runlevel.

id:2:initdefault:

於 runlevel 2 中加入自動執行

ln -s /etc/init.d/epilogd /etc/rc2.d/epilogd