LabSheet 05:

การติดตั้งโปรแกรมส่งล๊อกไฟล์บนเซิร์ฟเวอร์ที่มีระบบปฏิบัติการ Windows (Apache Log)

Date: 8 August 2008

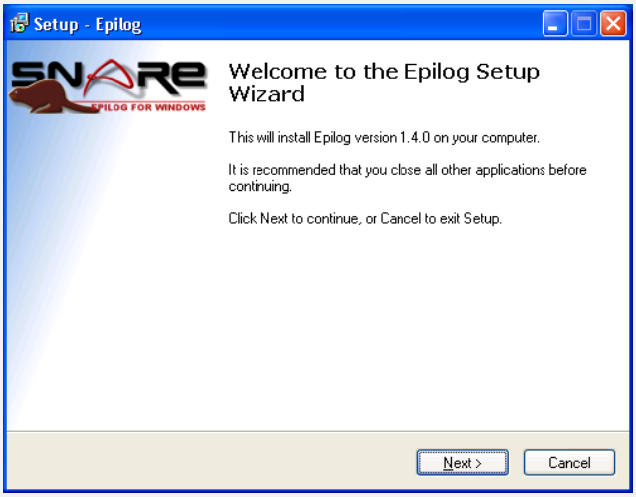
Program name: Epilog

Description: Send Apache log files to Centralized Log Server (logger.ku.ac.th)

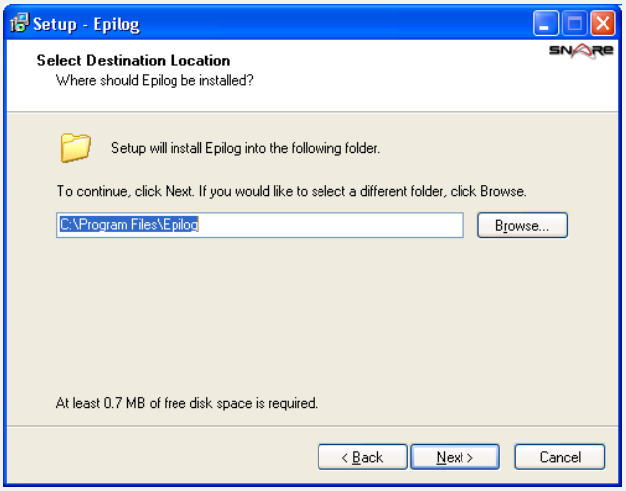
Step:

1. Download : http://ftp.ku.ac.th/pub/syslog-ng/snare/EpilogSetup-1.4.0-MultiArch.exe
2. ติดตั้งโปรแกรม

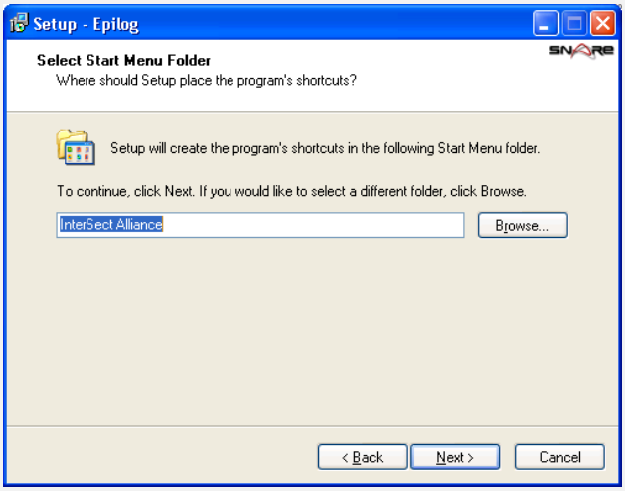
ดับเบิ้ลคลิกที่ชื่อโปรแกรม >



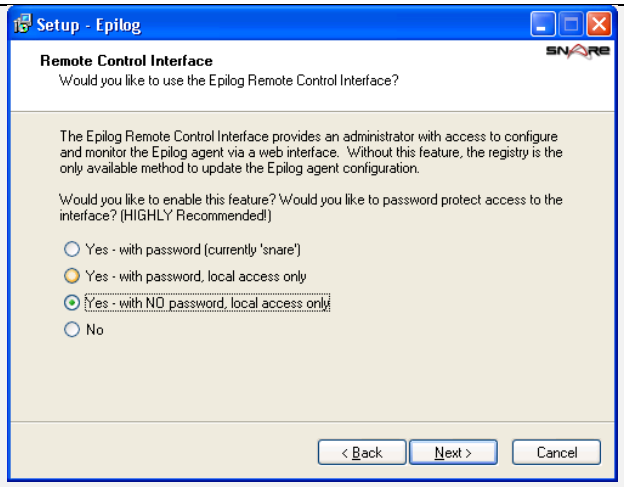
คลิกที่ปุ่ม Next >



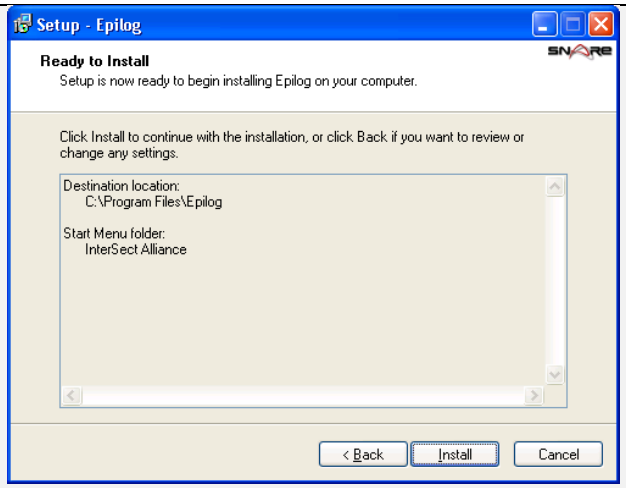
คลิกที่ปุ่ม Next >



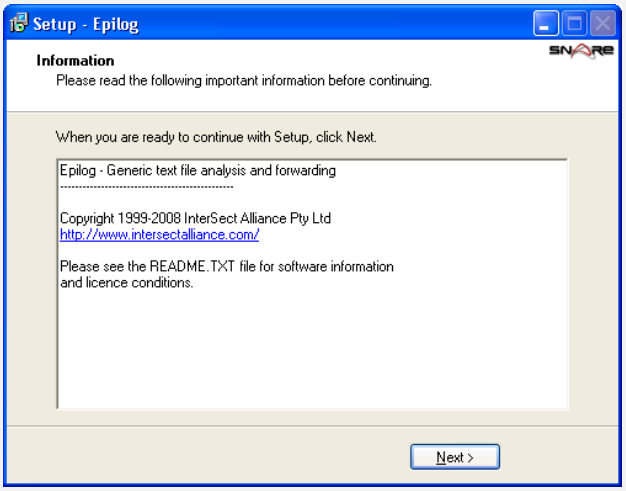
คลิกที่ปุ่ม Next >



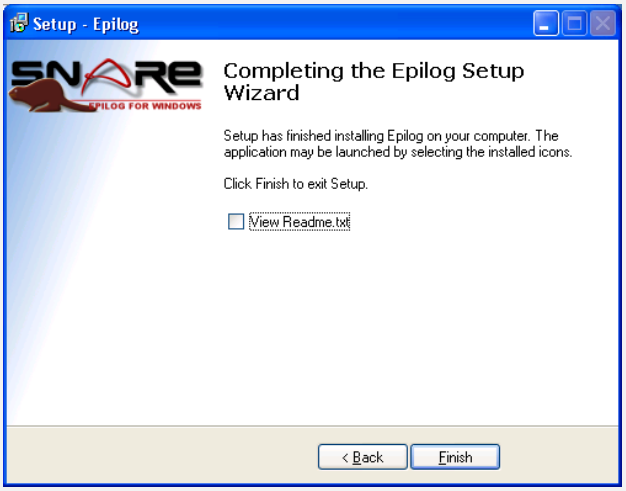
คลิกที่ปุ่ม Next >



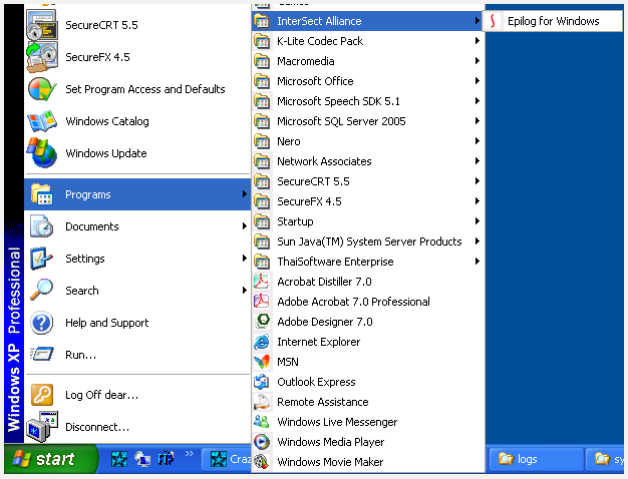
คลิกที่ปุ่ม Install



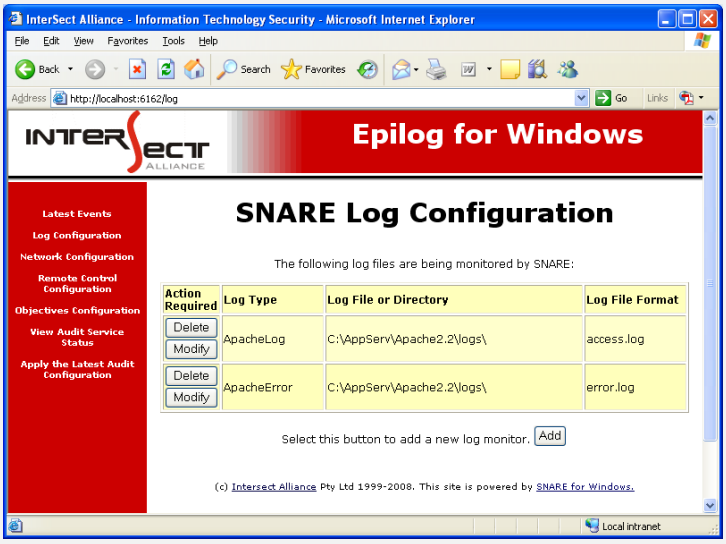
คลิกที่ปุ่ม Next >



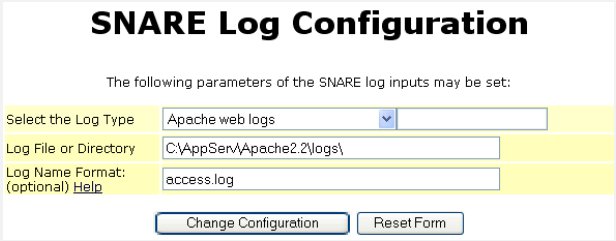
เสร็จแล้วคลิกที่ปุ่ม Finish



ปรับแต่งค่าคอนฟิก ไปที่เมนู Start > Programs > InterSect Alliance > Epilog for Windows



Apache Access Log



- คลิกที่เมนู Log Configuration > คลิกที่ปุ่ม **Add**
- กำหนดค่าต่างๆ ดังนี้

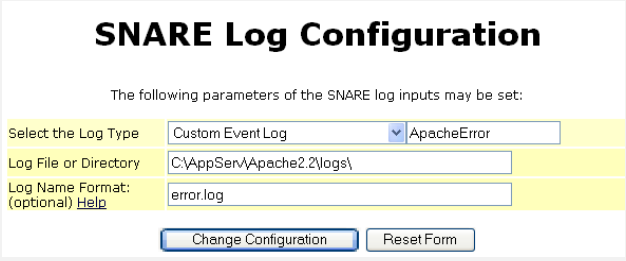
Select the Log Type: --> Apache web logs

Log File or Directory --> C:\AppServ\Apache2.2\logs\

Log Name Format: --> access.log

- เสร็จแล้ว คลิกที่ปุ่ม Change Configuration
- ตั้งค่าเสร็จแล้ว คลิกที่เมนู Apply the Latest Audit Configuration

Apache Error Log



- คลิกที่เมนู Log Configuration > คลิกที่ปุ่ม **Add**
- กำหนดค่าต่างๆ ดังนี้

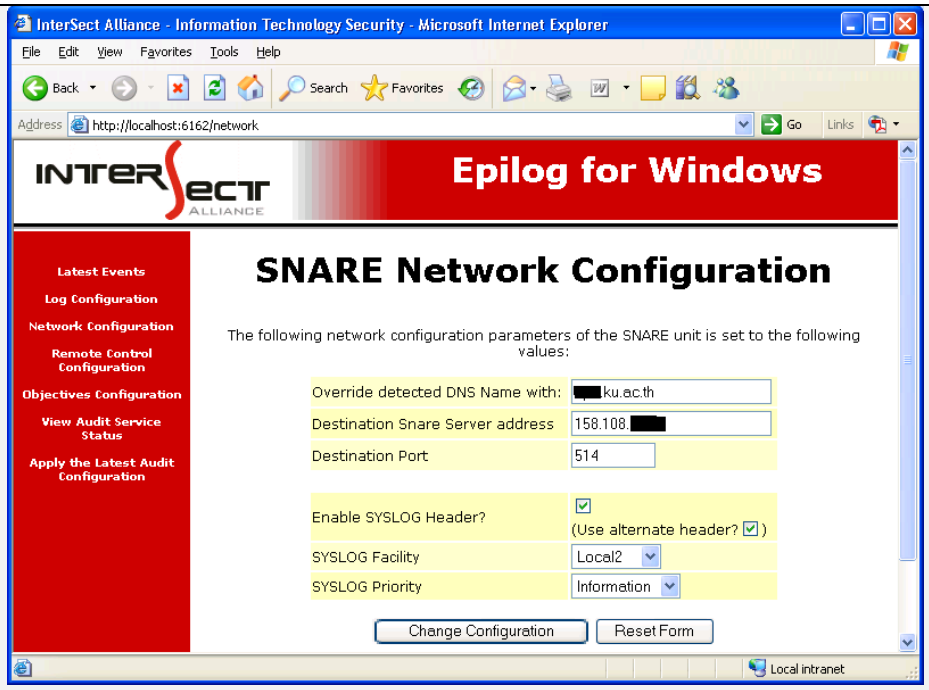
Select the Log Type: --> Custom Event Log

--> ApacheError

Log File or Directory --> C:\AppServ\Apache2.2\logs\

Log Name Format: --> error.log

- เสร็จแล้ว คลิกที่ปุ่ม Change Configuration
- ตั้งค่าเสร็จแล้ว คลิกที่เมนู Apply the Latest Audit Configuration



- คลิกที่เมนู Network Configuration
- กำหนดค่าต่างๆ ดังนี้

ที่ช่อง Override detected DNS Name with: --> hostname (ตัวอย่าง wsus.ku.ac.th)

Destination Snare Server address --> IPAddress Log Server(158.108.5.154)

Destination Port --> Port กำหนดเป็น 514

Enable SYSLOG Header? --> คลิกถูก

Use alternate header? --> คลิกถูก

SYSLOG Facility --> เลือก Local2

SYSLOG Priority --> เลือก Information

- เสร็จแล้ว คลิกที่ปุ่ม Change Configuration
- เมื่อตั้งค่าเสร็จแล้ว คลิกที่เมนู Apply the Latest Audit Configuration