LabSheet 03:

การติดตั้งโปรแกรมส่งล๊อกไฟล์บนเซิร์ฟเวอร์ที่มีระบบปฏิบัติการ Windows (System Log)

Date: 8 August 2008

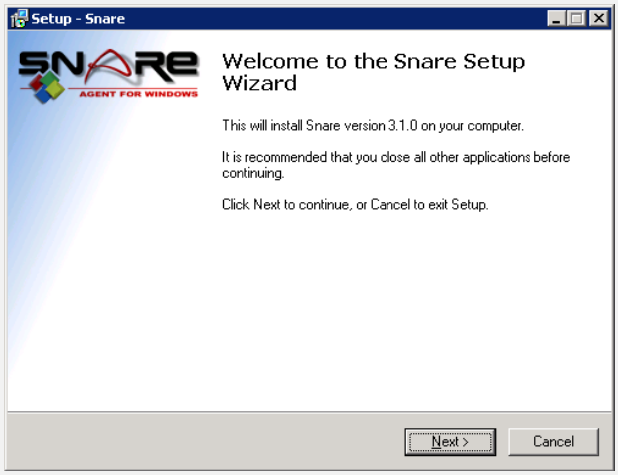
Program name: Snare for Windows

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

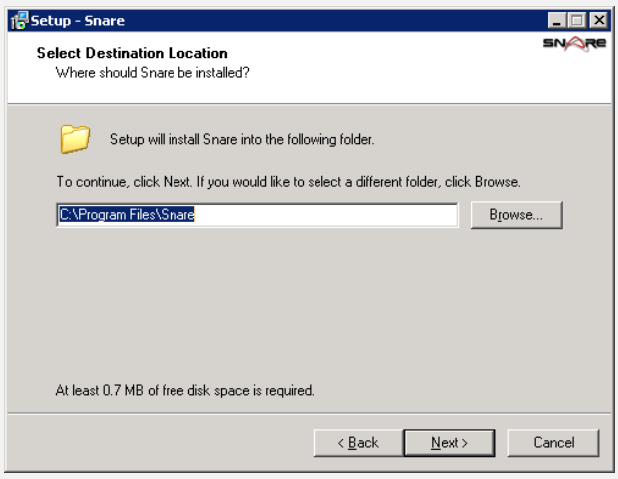
Step:

1. Download : http://ftp.ku.ac.th/pub/syslog-ng/snare/SnareSetup-3.1.0-MultiArch.exe
2. ติดตั้งโปรแกรม

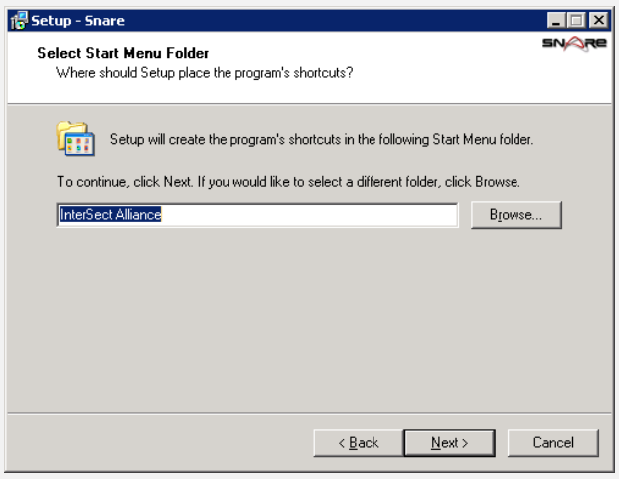
ดับเบิ้ลคลิกที่ชื่อโปรแกรม >



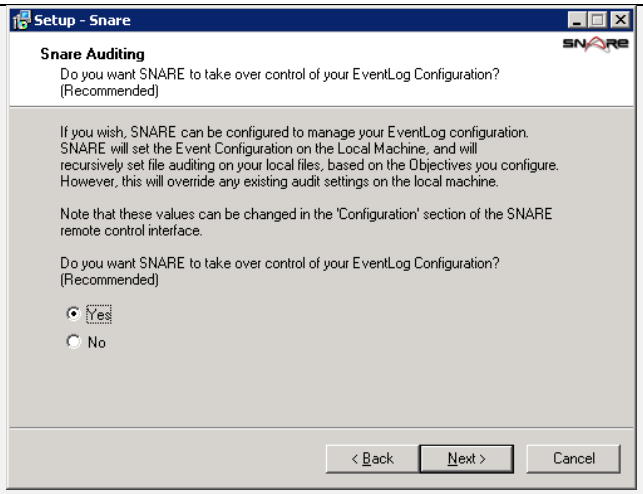
คลิกที่ปุ่ม Next >



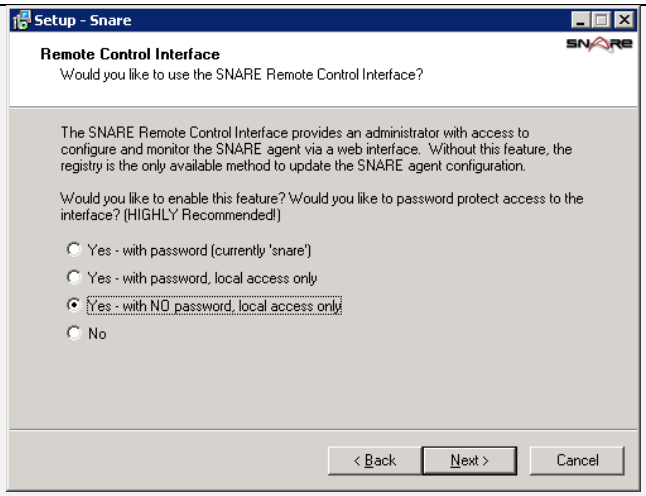
คลิกที่ปุ่ม Next >



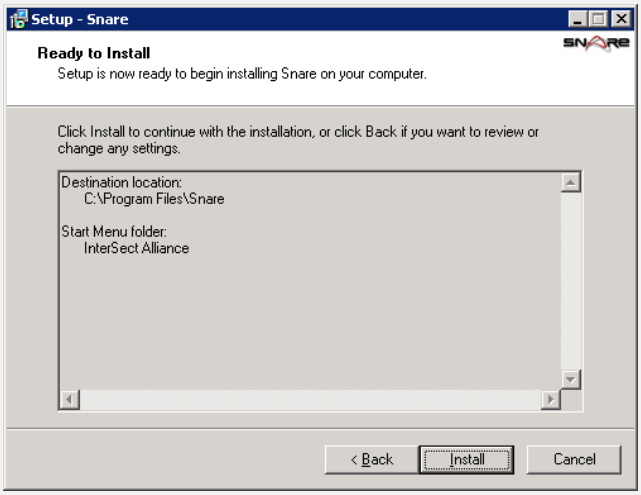
คลิกที่ปุ่ม Next >



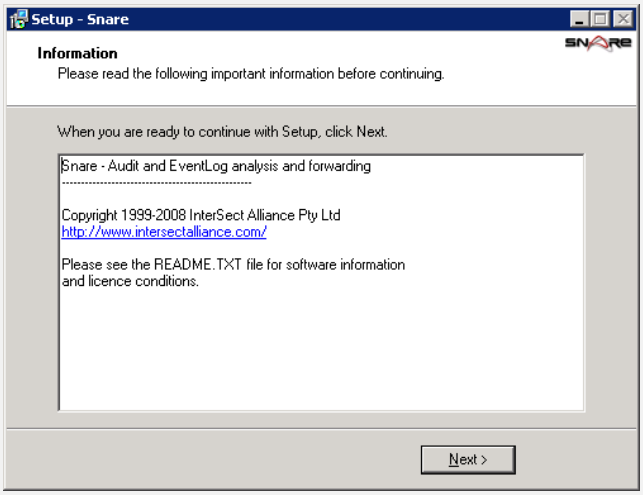
คลิกที่ปุ่ม Next >



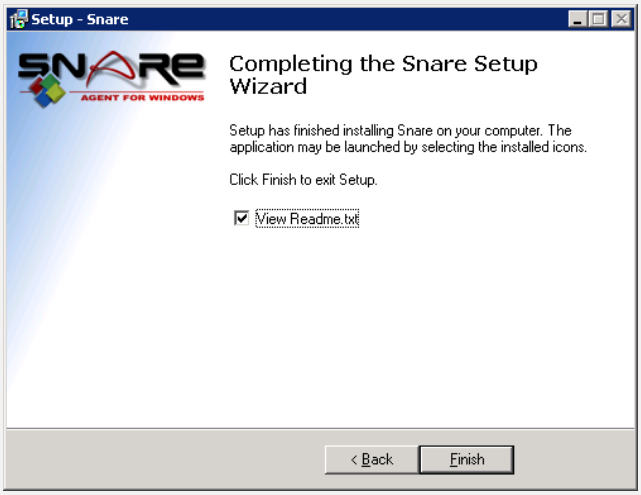
คลิกที่ปุ่ม Next >



คลิกที่ปุ่ม Install

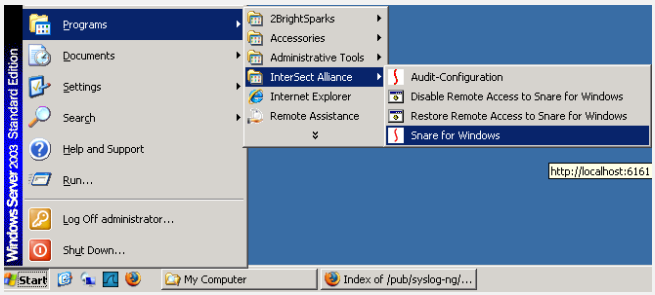


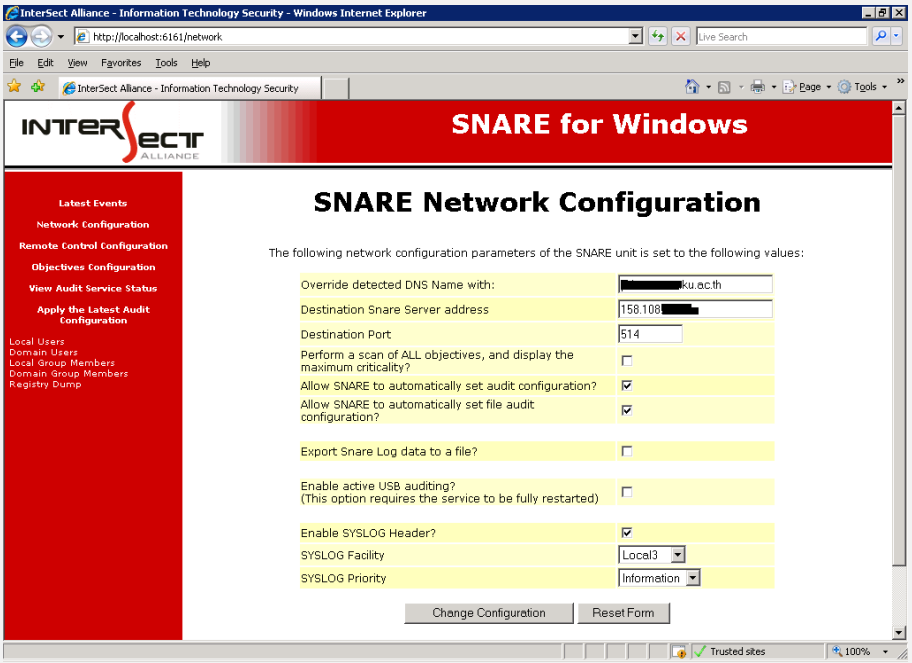
คลิกที่ปุ่ม Next >



เสร็จแล้วคลิกที่ปุ่ม Finish

3. ปรับแต่งค่าคอนฟิก ไปที่เมนู Start > Programs > InterSect Alliance > Sanre for Windows





- คลิกที่เมนู Network Configuration
- กำหนดค่าต่างๆ ดังนี้

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

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

Destination Port --> Port กำหนดเป็น 514

Enable SYSLOG Header? --> คลิกถูก

SYSLOG Facility --> เลือก Local3

SYSLOG Priority --> เลือก Information

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