**LabSheet 10:**

การติดตั้งโปรแกรมส่งล๊อกไฟล์บนเซิร์ฟเวอร์ที่มีระบบปฏิบัติการ Windows 2008 (IIS7 Log)

Date: 27 August 2008

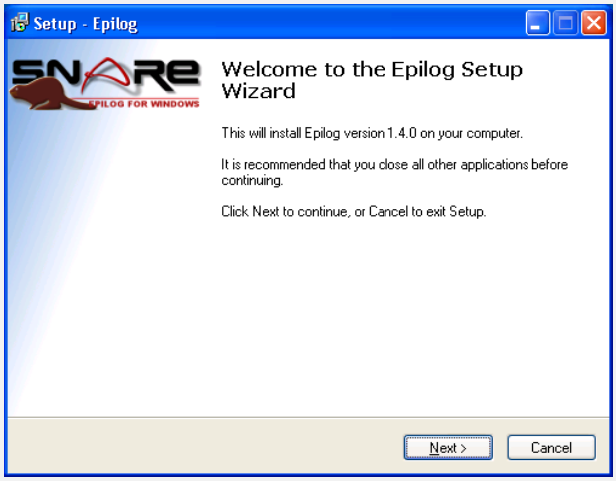
**Program name:** Epilog for Windows

**Description:** Send IIS7 log files to Centralized Log Server (logger.ku.ac.th)

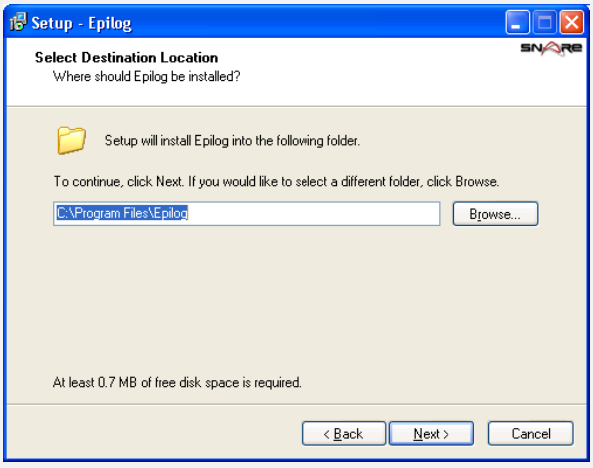
**Step:**

1. ติดตั้งโปรแกรม Epilog for Windows

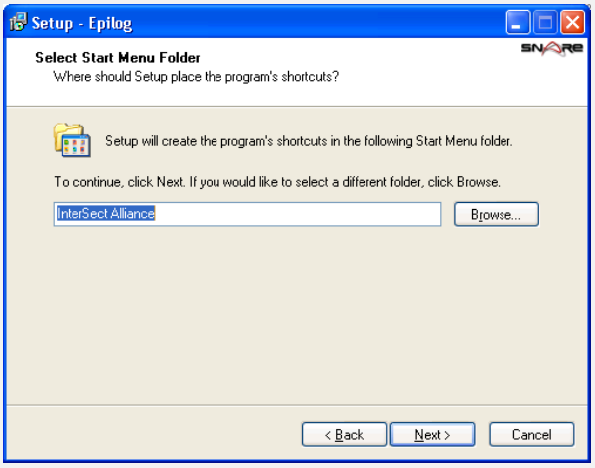
(ดาวน์โหลดได้จาก http://ftp.ku.ac.th/pub/syslog-ng/snare/EpilogSetup-1.4.0-MultiArch.exe )

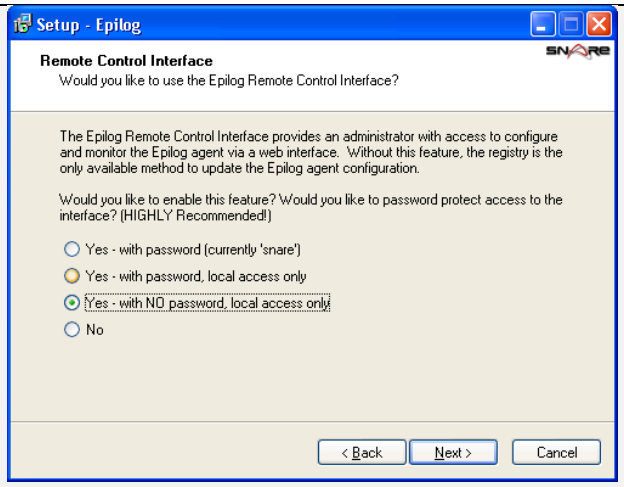

คลิกที่ปุ่ม Next >



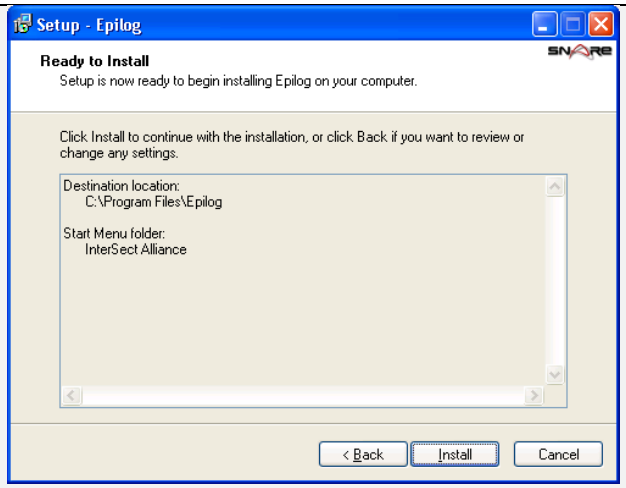

คลิกที่ปุ่ม Next >



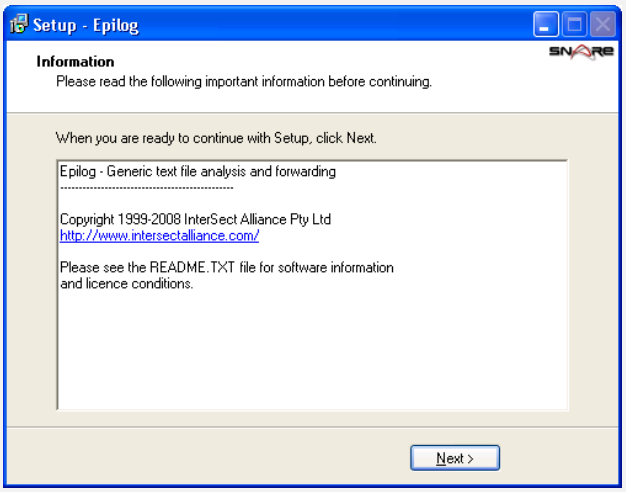

คลิกที่ปุ่ม Next >



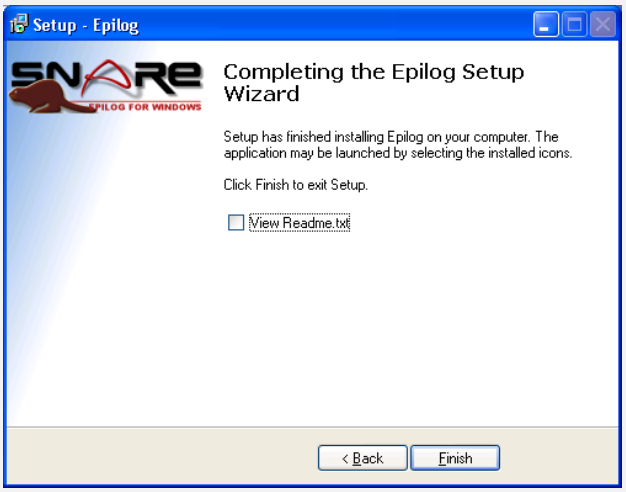

คลิกที่ปุ่ม Next >




คลิกที่ปุ่ม Install >

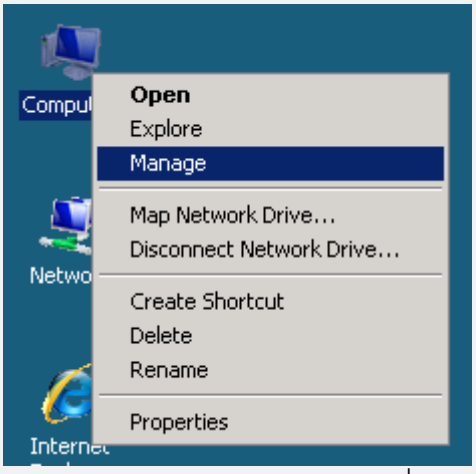



คลิกที่ปุ่ม Next >

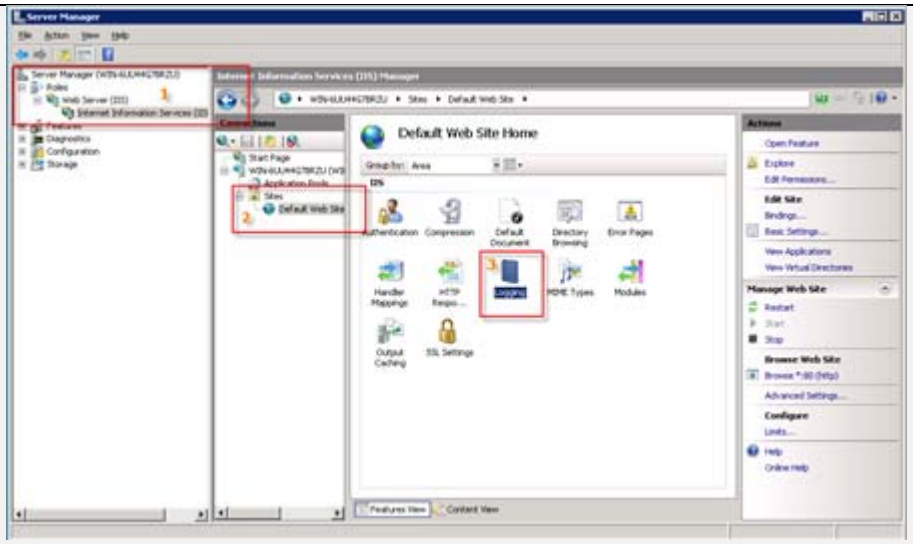



เสร็จแล้วคลิกที่ปุ่ม Finish

2. ดูตำแหน่งการจัดเก็บล๊อกไฟล์และปรับตั้งค่าของข้อมูลล๊อกไฟล์ที่ต้องการจัดเก็บ

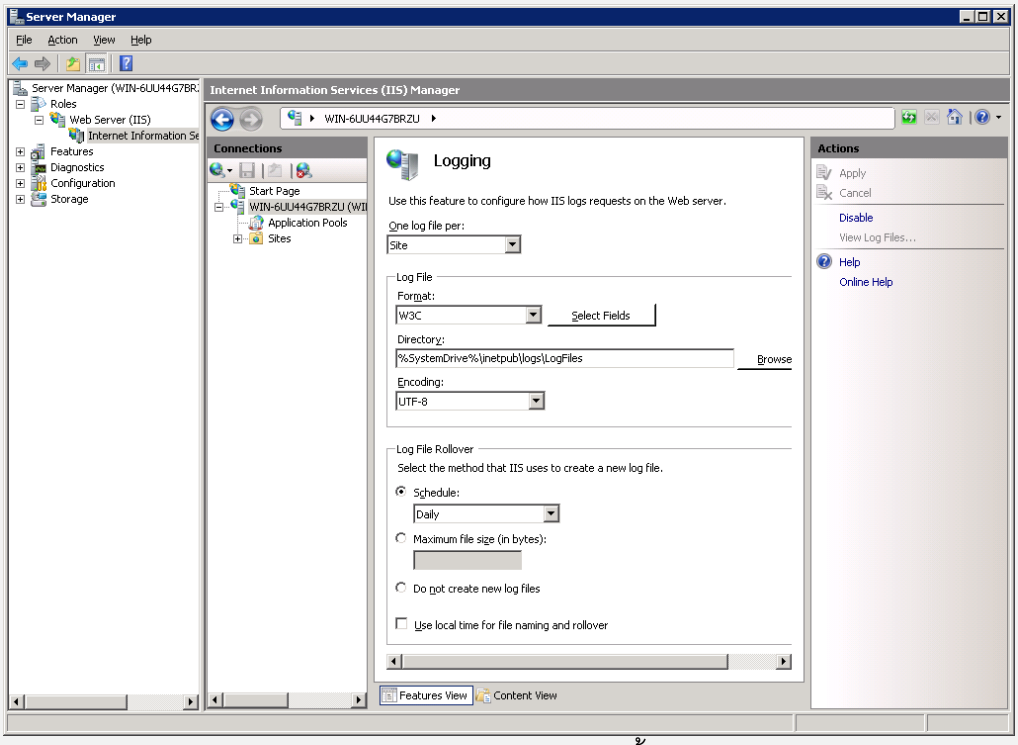



บนหน้าจอ Desktop คลิกเมาส์ขวาที่ไอคอน My Computer > เลือกเมนูย่อย Manage



จากเมนูด้านขวามือ “Server Manager”

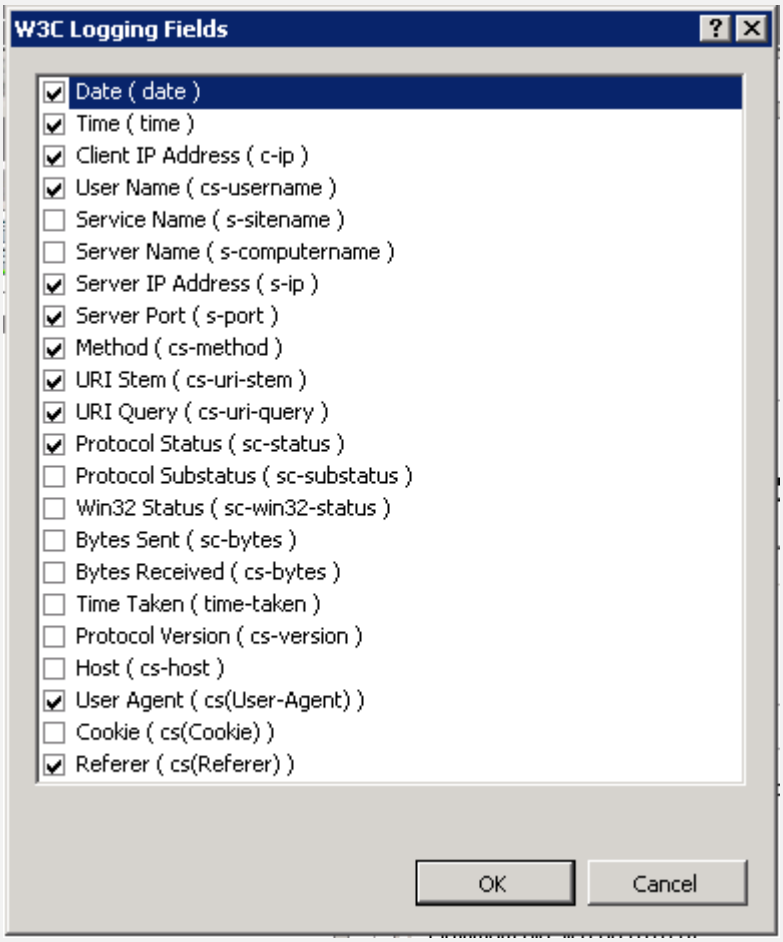
1. คลิกเมนูย่อย Roles > Web Sites (IIS) > Internet Information Services (IIS) Manager
2. จากหน้าจอย่อย “Internet Information Services (IIS) Manager” ให้คลิกชื่อเครื่อง > Sites > Default Web Sites
3. คลิกไอคอน “Logging” จากหน้าจอด้านขวามือ




จะปรากฏหน้าจอ Logging ให้ปรับแต่งค่าดังนี้

- One log File per: Site
- Log File
  - Format: W3C และคลิกปุ่ม “Select Fields” เพื่อกำหนดข้อมูลที่จะจัดเก็บ และให้คลิ๊กเลือก field ดังต่อไปนี้

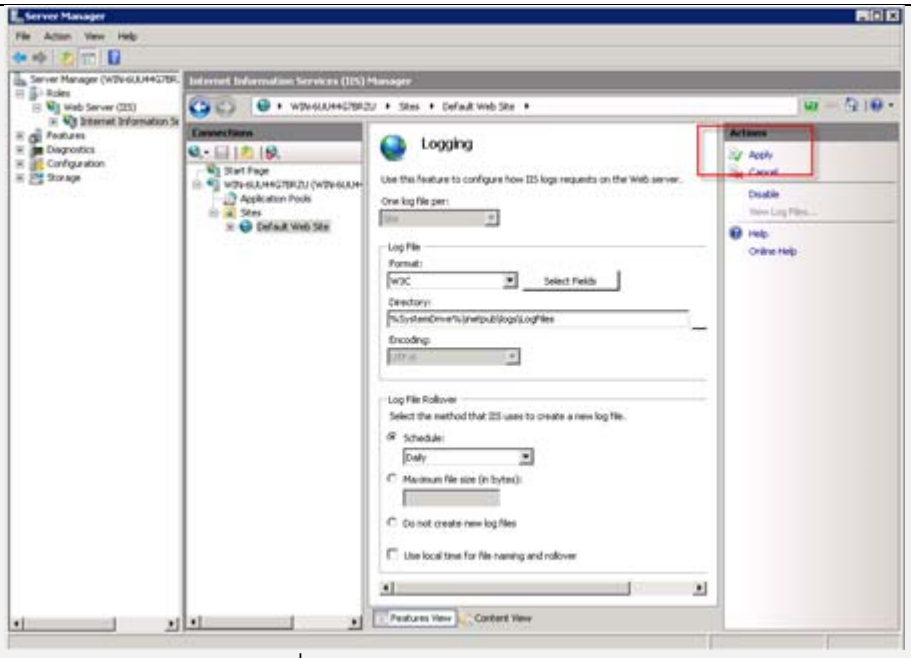
แล้วคลิกปุ่ม OK



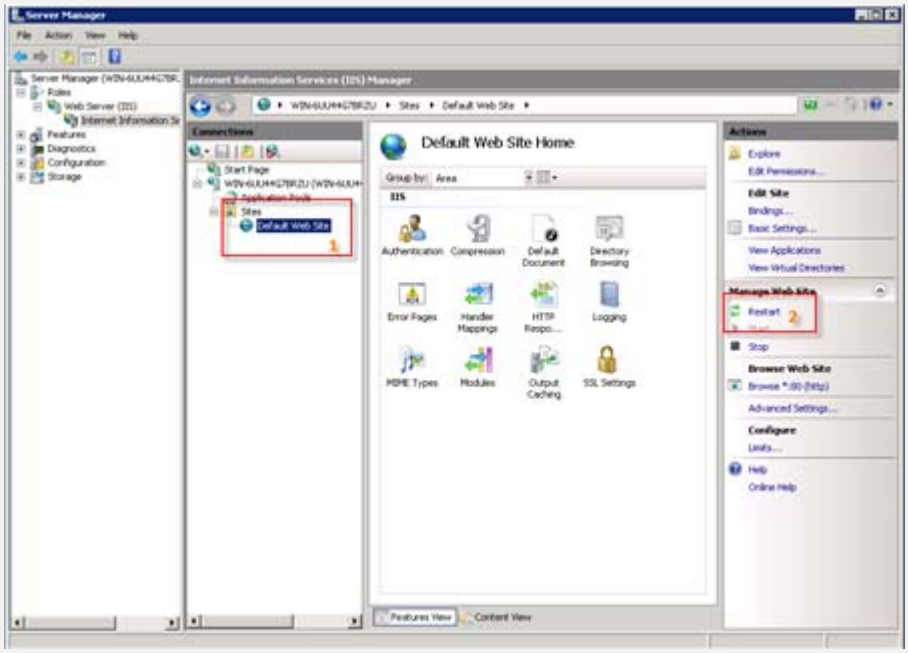

- Date
- Time
- Client IP Address
- User Name
- Server IP Address
- Server Port
- Method
- URI Stem
- URI Query
- Protocol Status
- User Agent
- Referer

- Directory: %SystemDrive%\inetpub\logs\LogFiles
- Encoding: UTF-8

- Log File Rollover : Schedule "Daily"



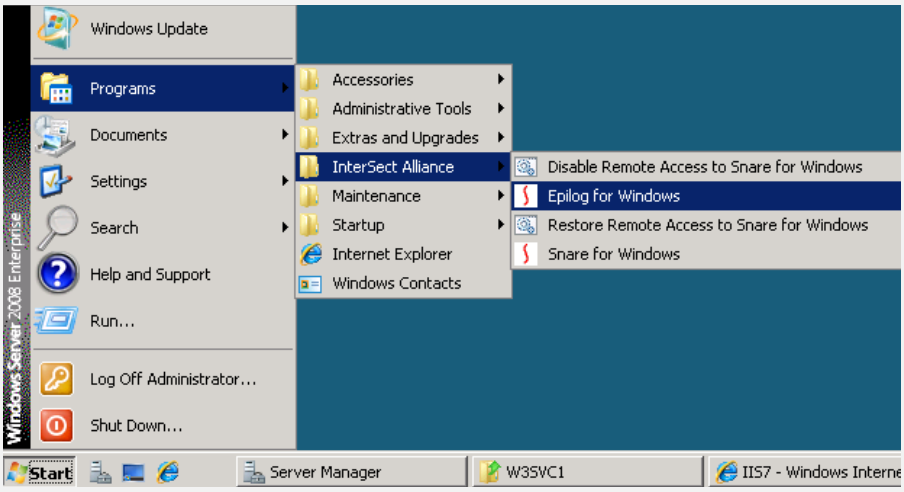

คลิก Actions “Apply” เพื่อบันทึกการแก้ไขข้อมูล >




จากหน้าจอ Internet Information Services (IIS) Manager ให้คลิกเมนู “Default Web Site” แล้วจากเมนูด้านขวามือ “Manage Web Site” ให้คลิกเมนูย่อย Restart

และออกจากหน้าจอ “Server Manager” ให้คลิกเมนู File > Exit

3. ปรับตั้งค่าการจัดส่งล๊อกไฟล์ของโปรแกรม Epilog for Windows




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


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

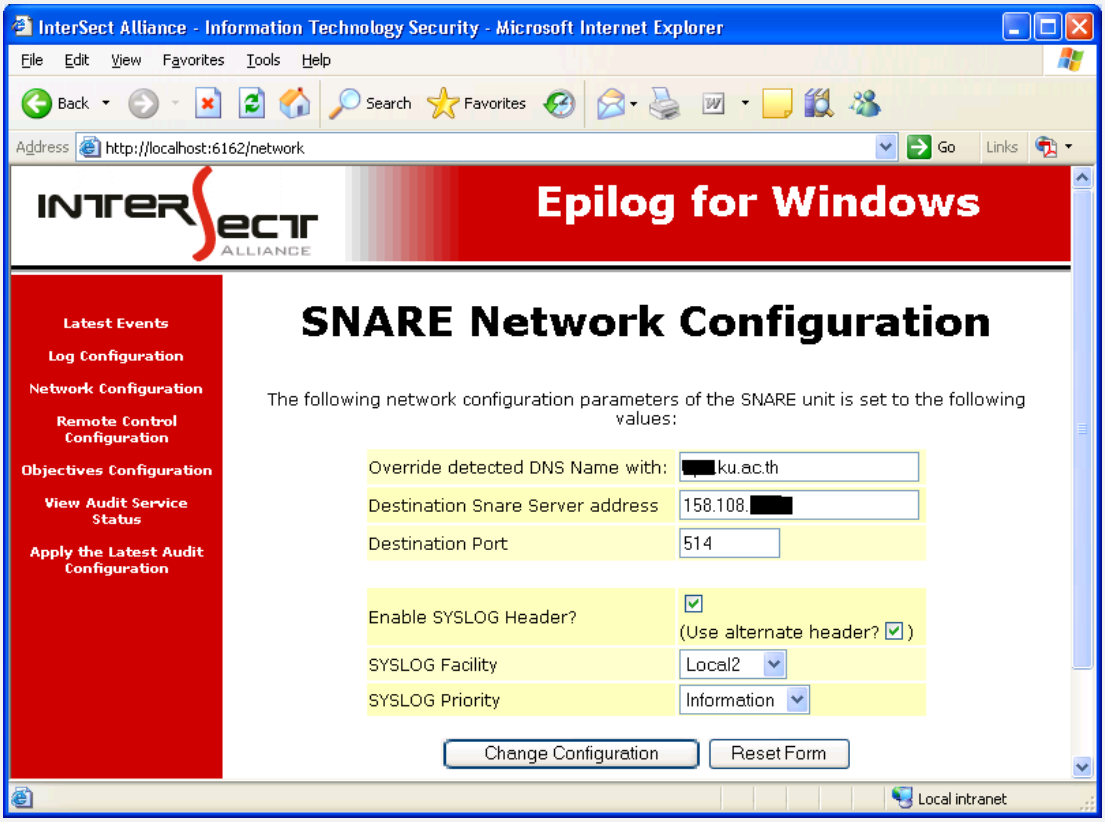
  Select the Log Type: --> Microsoft IIS web server logs

  Log File or Directory --> C:\inetpub\logs\LogFiles\W3SVC1\

  Log Name Format: --> u_ex*.log

- เสร็จแล้ว คลิกที่ปุ่ม Change Configuration

ตั้งค่าเสร็จแล้ว คลิกที่เมนู Apply the Latest Audit Configuration




- คลิกที่เมนู Network Configuration
- กำหนดค่าต่างๆ ดังนี้

ที่ช่อง Override detected DNS Name with: --> hostname

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