

Contents

[Practice 1: ESM Walk-Through 3](#_Toc405161625)

[Practice 2: SIEM Users and Groups 11](#_Toc405161626)

[Practice 3: Creating a Custom View 16](#_Toc405161627)

[Practice 4: Adding Data Sources 19](#_Toc405161628)

[Practice 5: Using the Syslog Parser 24](#_Toc405161630)

[Practice 6: Correlation Rules 28](#_Toc405161631)

[Practice 7: Alarms and Watchlists 34](#_Toc405161632)

[Practice 8: Reporting 38](#_Toc405161633)

[Practice 9: Update Rule 41](#_Toc405161625)

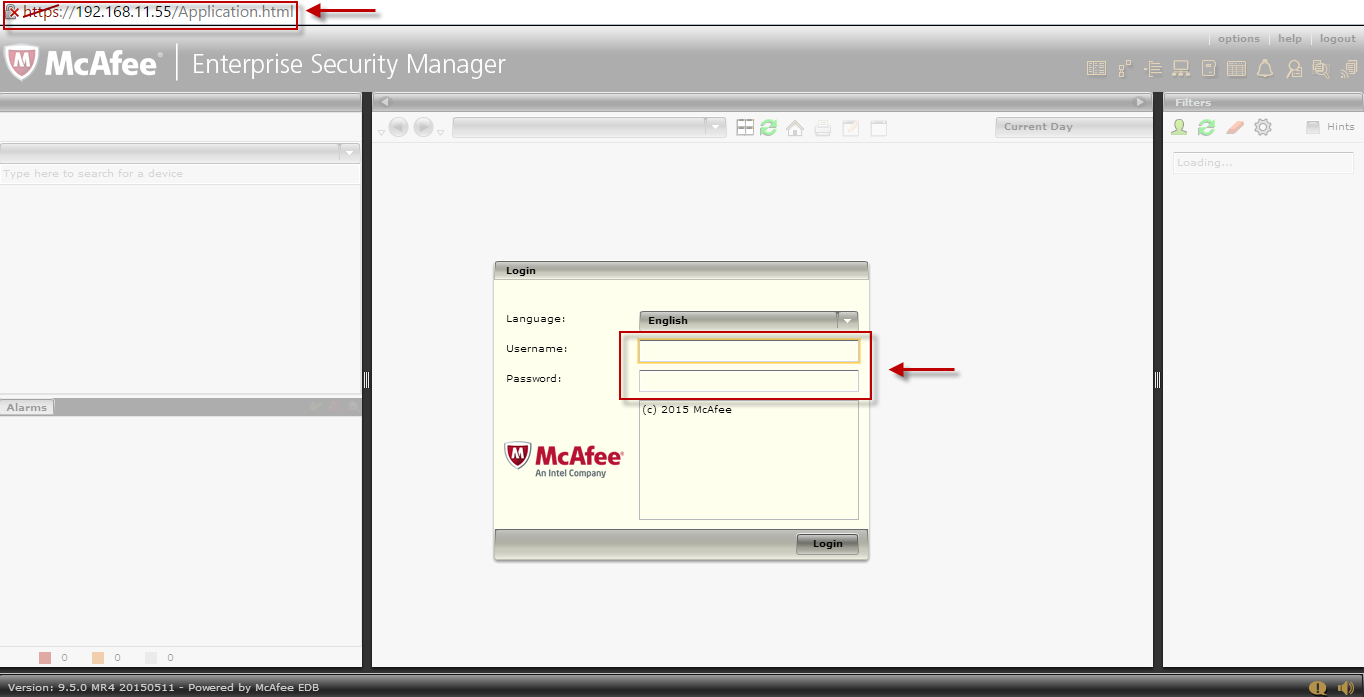
# Practice 1: ESM Walk-Through

1. การดูข้อมูล Event จาก ESM

2. Guided Tour

1. **การดูข้อมูล Event จาก ESM**
   1. เปิด browser และทำการใส่ IP : [**https://xx.xx.xx.xx**](https://xx.xx.xx.xx)
   2. พิมพ์ Username : **NGCP**

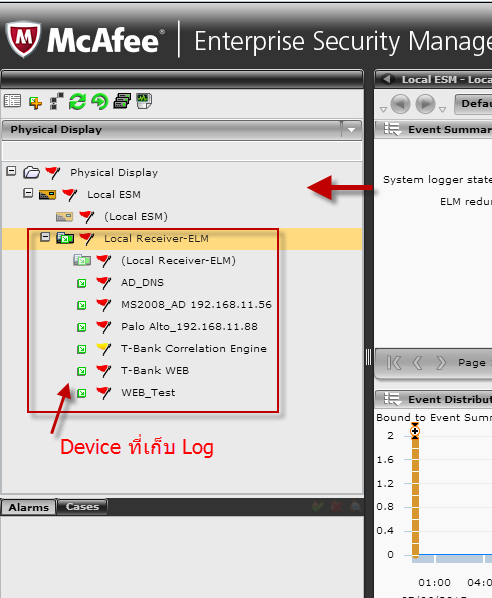
Password : **McAfee123!**



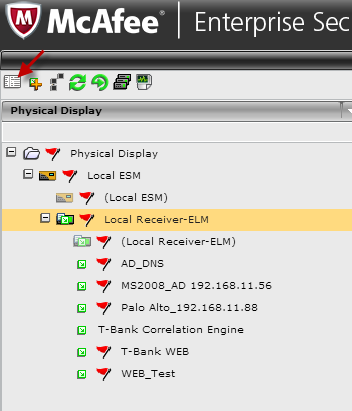
**หน้าต่างแสดงผลหลังจาก Login เข้ามาครั้งแรก**

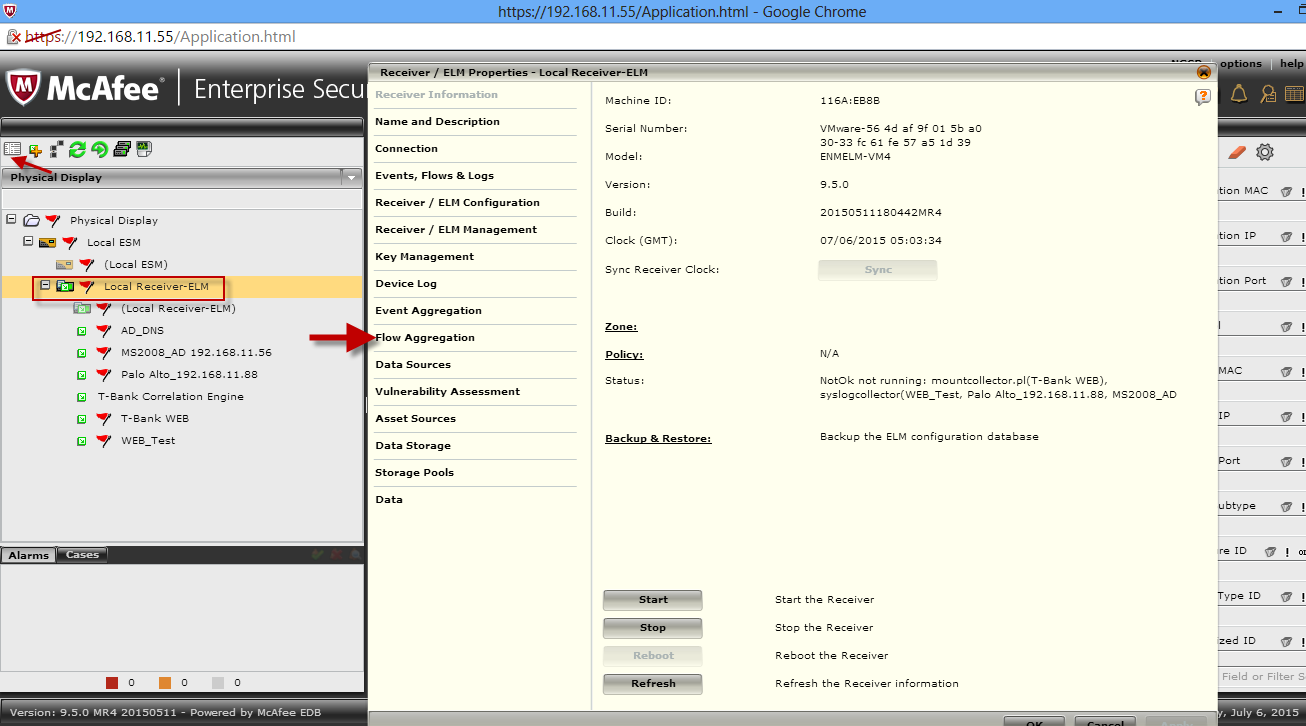


* 1. จากเมนูด้านซ้ายมือเป็นการแสดงรายละเอียดของอุปกรณ์ทั้งหมด
  2. หลังจากการแตกรายละเอียดของ Local Receiver-ELM คือรายการอุปกรณ์ที่ระบบ SIEM ทำการเก็บ Log

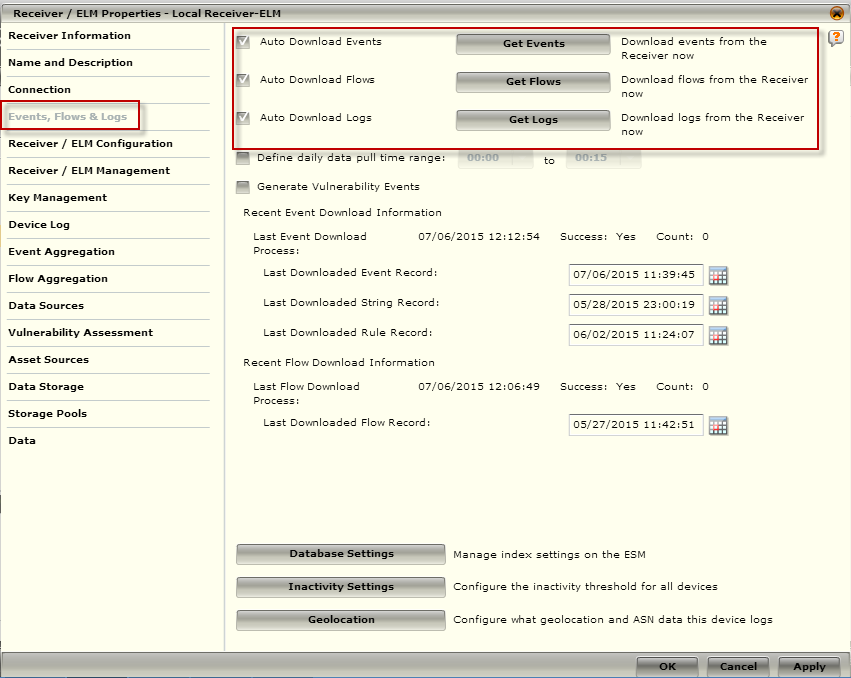


* 1. จากเมนูด้านซ้ายมือเลือก **Properties**

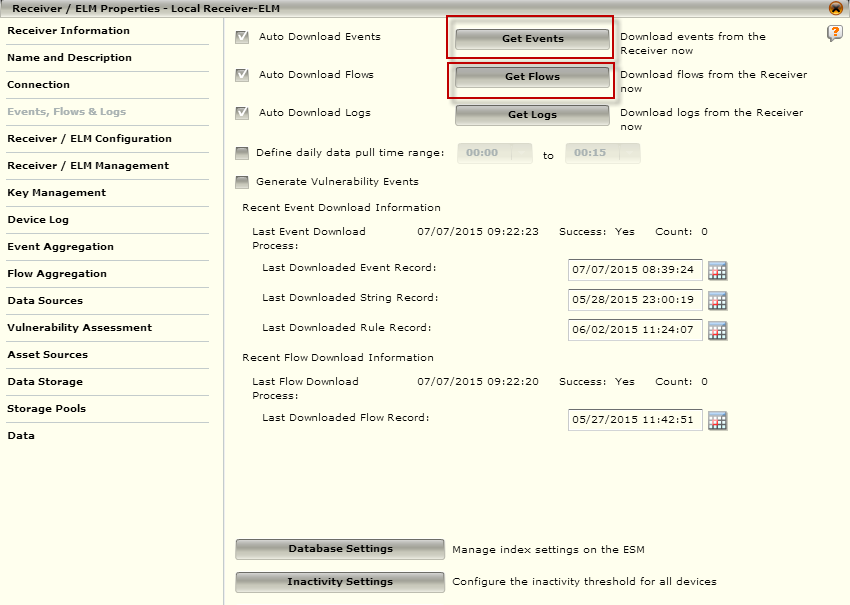


1.6 หลังจากเลือก Local Receiver-ELM > Properties จะแสดงหน้าต่างเกี่ยวกับรายละเอียดของ ELM ดังภาพด้านล่าง

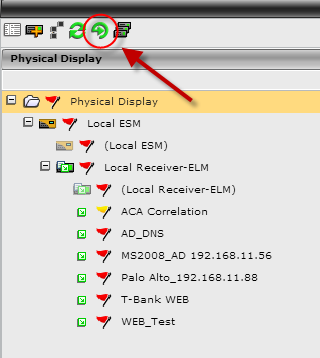
หมายเหตุ เมื่อต้องการกำหนดค่าเกี่ยวกับการรับ Log คลิกที่เมนู Events, Flows and Logs ดังภาพด้านล่าง

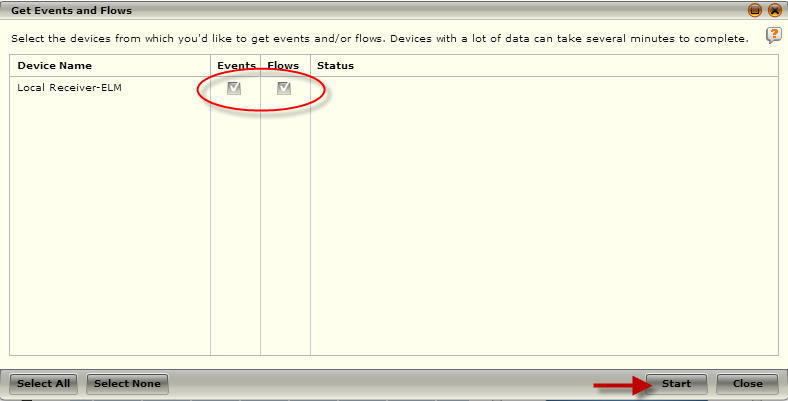


1.7 หากต้องการ Get Event และ Flows > คลิก Get Event หรือ Get Flows



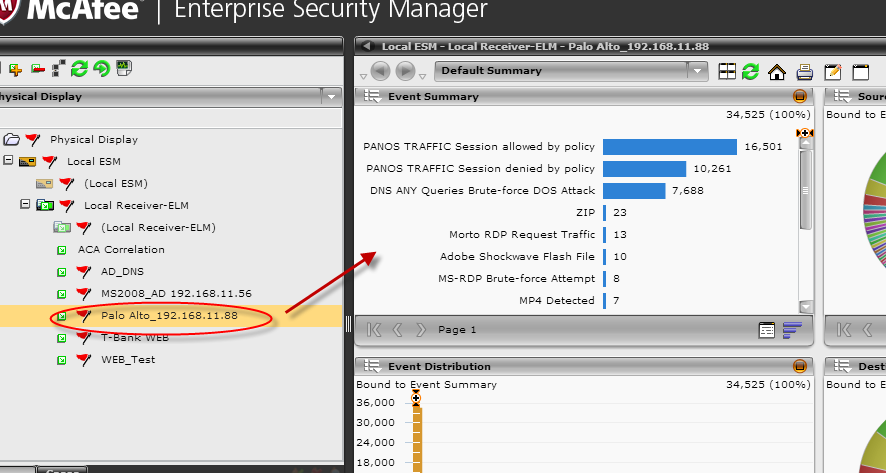
**TIP**: วิธีที่ 2 ในการดึง Event และ Flows > คลิก เมนู Get Event and Flows



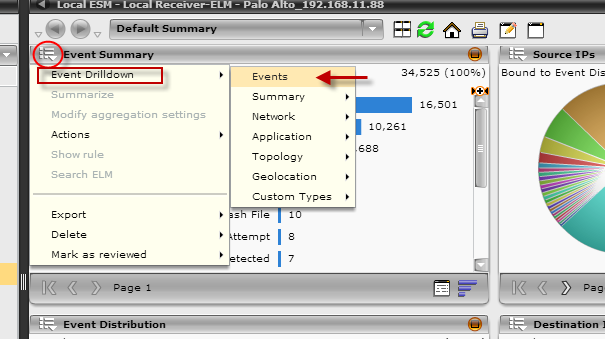


**2. Guided Tour**

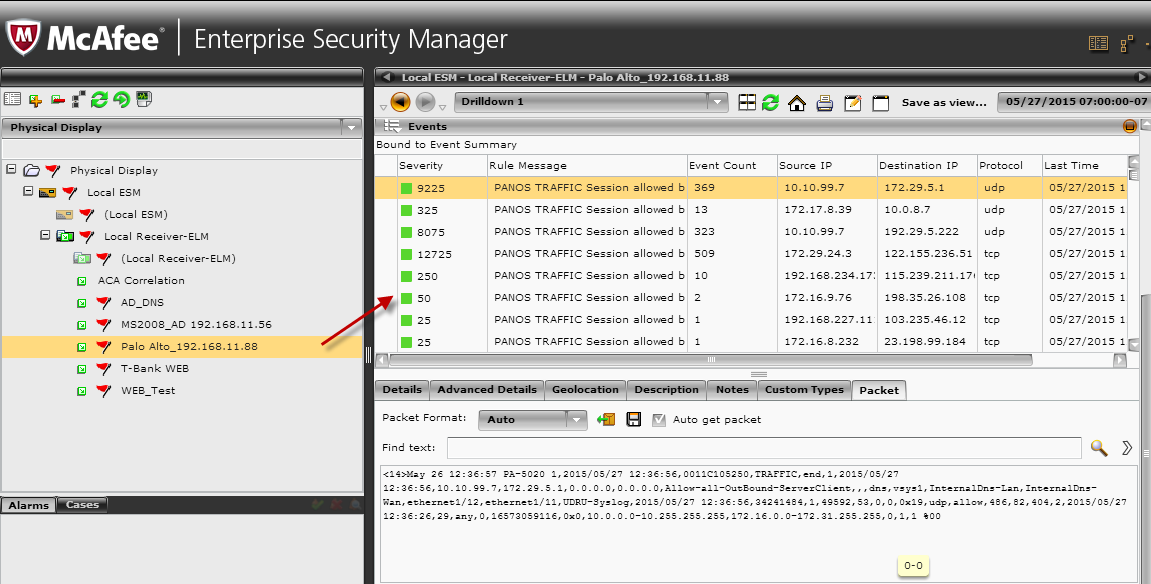
2.1. หลังจากทำการ Download Event จาก Receiver ทำการ คลิกที่อุปกรณ์ที่ต้องการดูข้อมูล



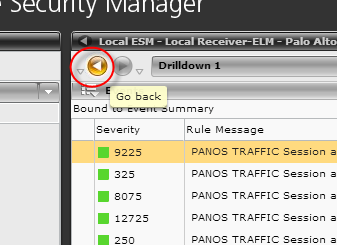
2.2. เมื่อต้องการดูรายละเอียดของเหตุการณ์สามารถคลิกที่ Event Summary



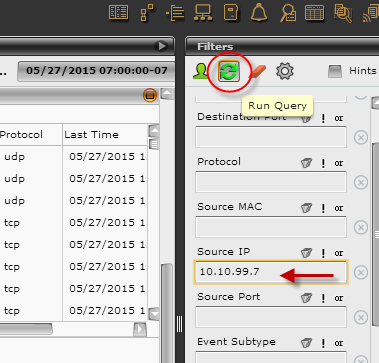
2.3. เลือก Event จะเป็นการแสดงรายละเอียดต่างๆเช่น Source IP , Potocol , Event Count



2.4. เมื่อต้องการย้อนกลับไปยังหน้าต่างแรกสามารถทำได้โดย คลิก Go back



2.6. เมื่อต้องการค้นหาสิ่งที่สนใจเฉพาะเจาะจงสามารถใช้ Filters ช่วยในการค้นหา เช่นต้องการค้นหา Source IP 10.10.99.7 > คลิก Run Query



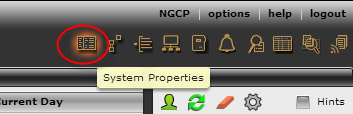
**End of Practice 1**

# Practice 2: SIEM Users and Groups

1. การสร้าง role (group)
2. การเพิ่ม user ภายใน group
3. ตรวจสอบสิทธิ์ (Verify Permissions)

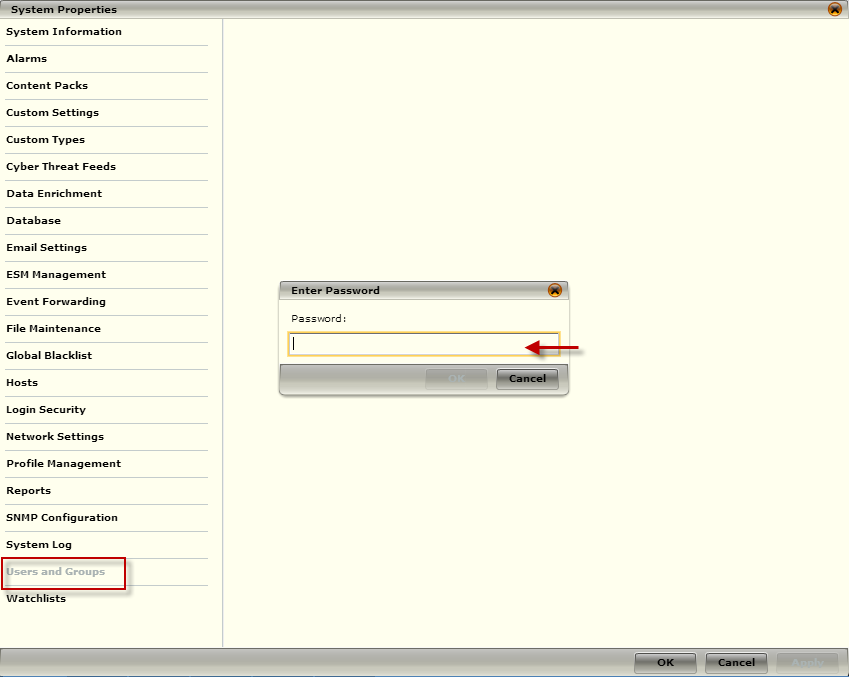
**1. การสร้าง group**

1.1. จากเมนูหลักของ ESM ด้านขวามือ เลือก System Properties

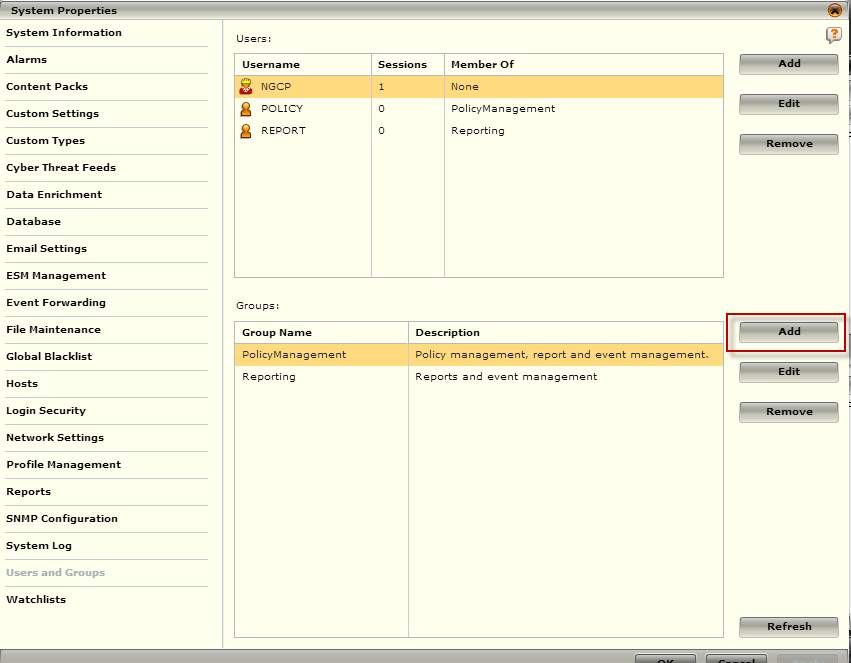


1.2. From the options list-pane, select Users and Groups.จากตัวเลือกด้านซ้ายเลือก Users and Groups

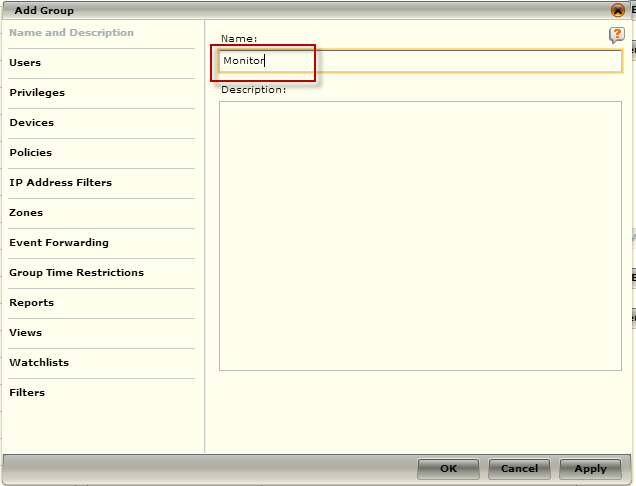
1.3. กรอก password: **McAfee123!**



1.4. คลิกที่ปุ่ม Add

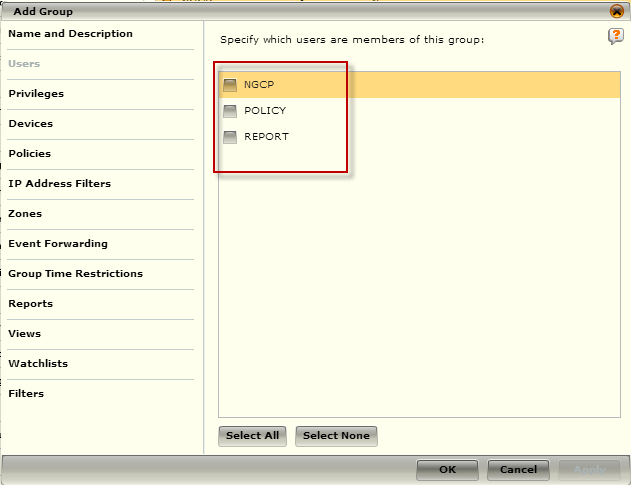


1.5. กำหนดชื่อตามต้องการ

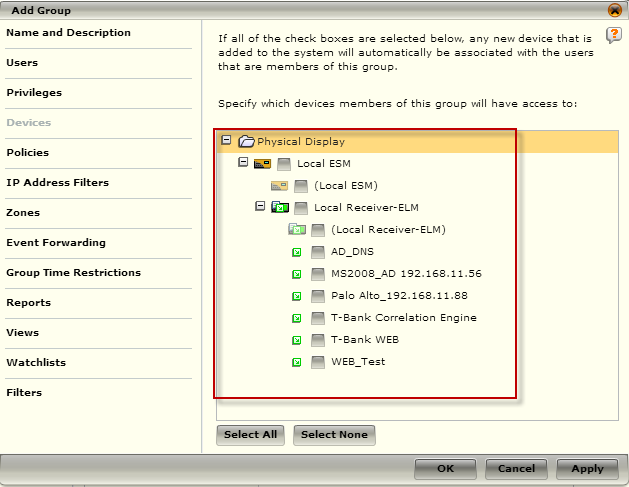


1.6. กำหนดเงื่อนไขต่างๆ สำหรับ Group

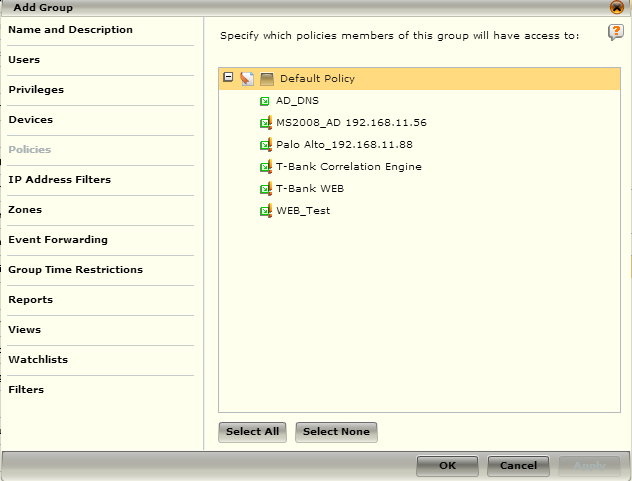
1.6.1. User : กำหนด User สำหรับ Group



1.6.2. Devices : เพิ่ม / ลบ อุปกรณ์

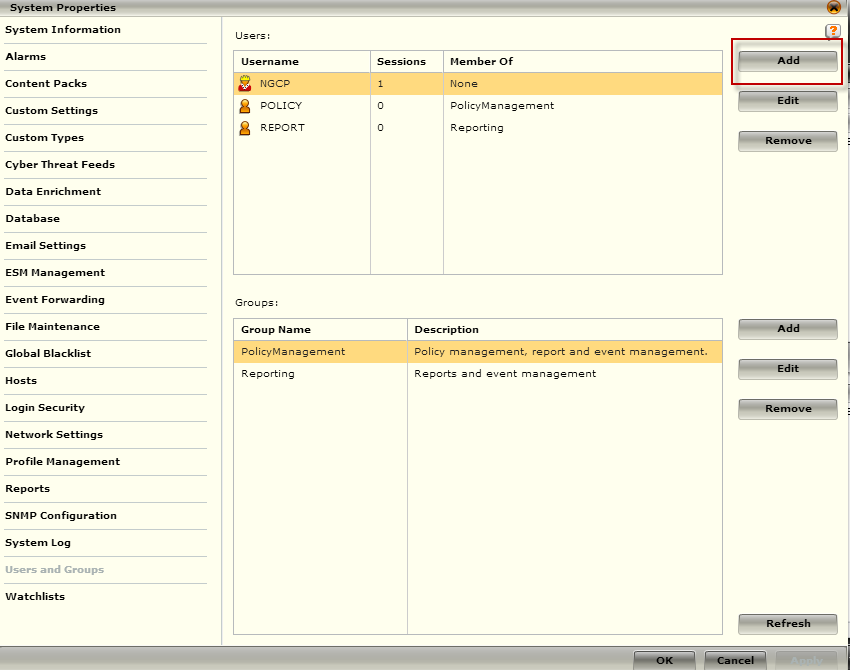


1.6.3. Policies : เพิ่ม / ลบ นโยบาย

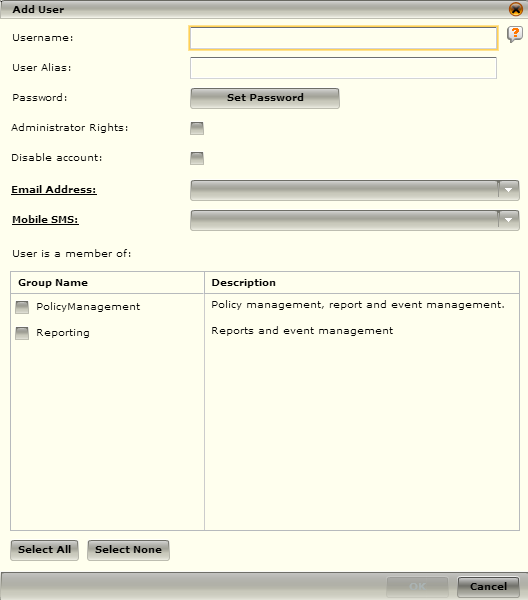


**2. การสร้าง User**

2.1. ใน Users : เลือกปุ่ม Add

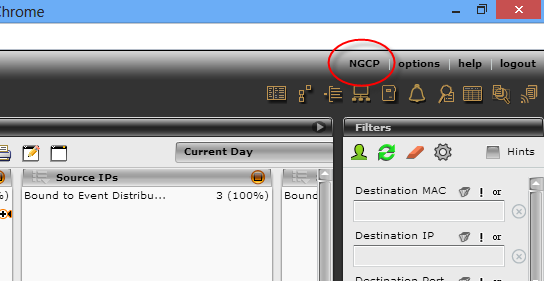


2.2. กำหนดค่าต่างๆเกี่ยวกับ User



**3. ตรวจสอบสิทธิ์ (Verify Permissions)**

3.1. การตรวจสอบสิทธิ์ สามารถดูได้จากแถบเมนูด้านขวามือบนดังภาพด้านล่าง



End of practice 2

**Practice 3: Creating a Custom View**

1. สร้างมุมมองที่กำหนดเอง

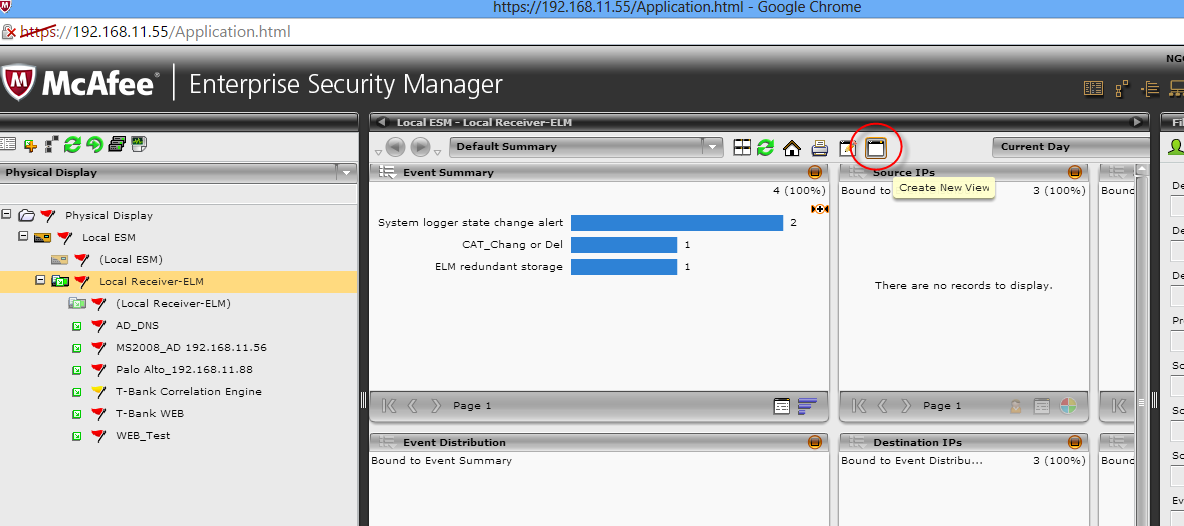
2. บันทึกมุมมองที่กำหนดเอง

3. ตั้งค่าเริ่มต้น มุมมองที่กำหนดขึ้นเอง

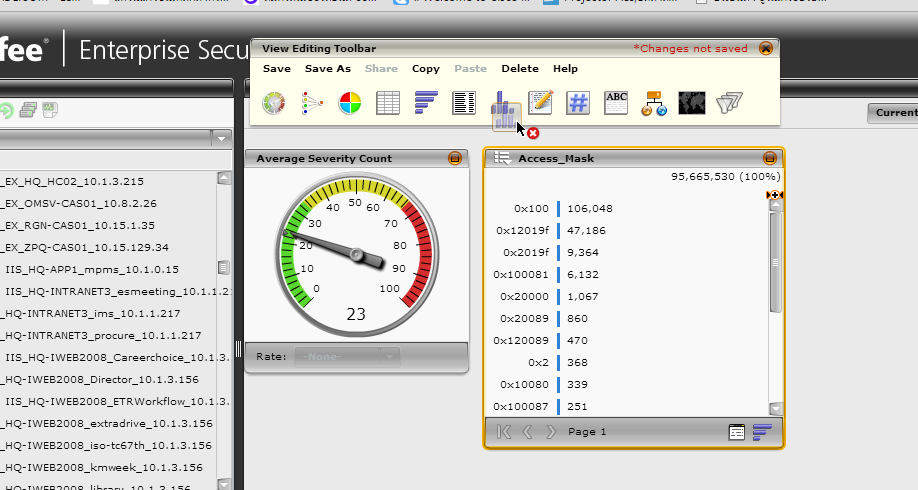
**1. สร้างมุมมองที่กำหนดเอง**

1.1. Log on ผ่านหน้า web ด้วย User **: NGCP**

1.2. จากแถบเมนู dashboard คลิก Create New View

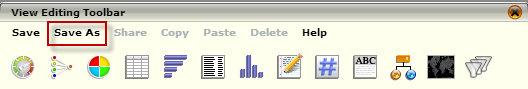


การเพิ่มองค์ประกอบและรายละเอียดของมุมมองสามารถทำได้โดยการคลิกที่ไอคอนที่ต้องการและลากไปวางในตำแหน่งที่ต้องการ

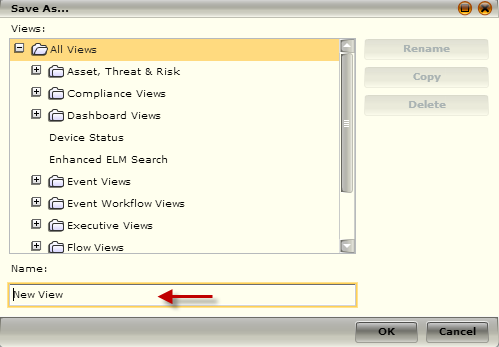


**2. บันทึกมุมมองที่กำหนดเอง**

2.1.คลิก Save As ที่ View Editing Toolbar

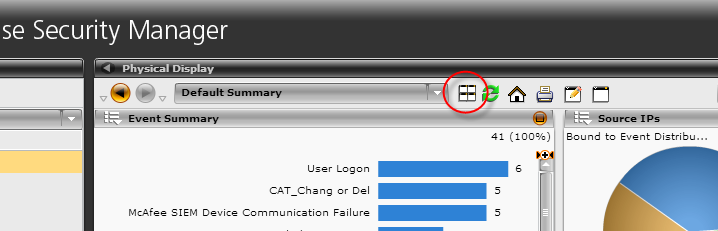


2.2. พิมพ์ชื่อตามต้องการ > OK

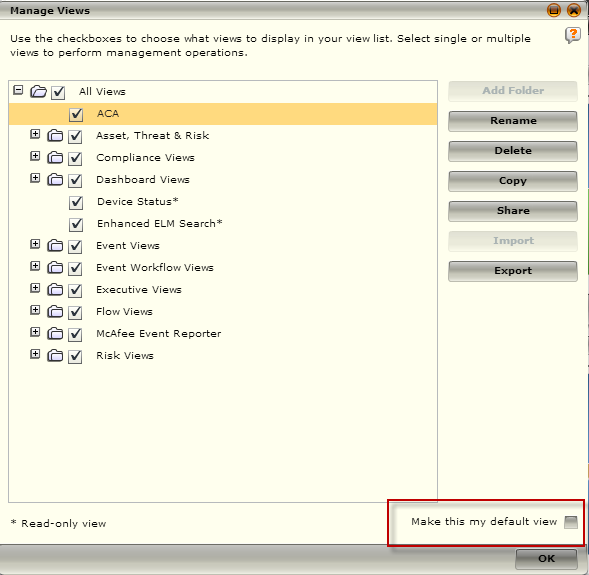


3. ตั้งค่าเริ่มต้น มุมมองที่กำหนดขึ้นเอง

3.1. จากแถบเมนูเลือก Manage views icon



3.2. เลือกมุมมองที่ต้องการตั้งค่าเป็นหน้าแสดงผลเริ่มต้น >ติ๊กถูกที่ Make this my default view มุมขวามือด้านล่าง



End of Practice 3

# Practice 4: Adding Data Sources

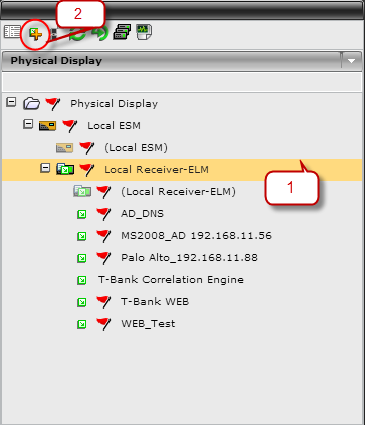
1. WMI Data Source

2. Firewall Data Source

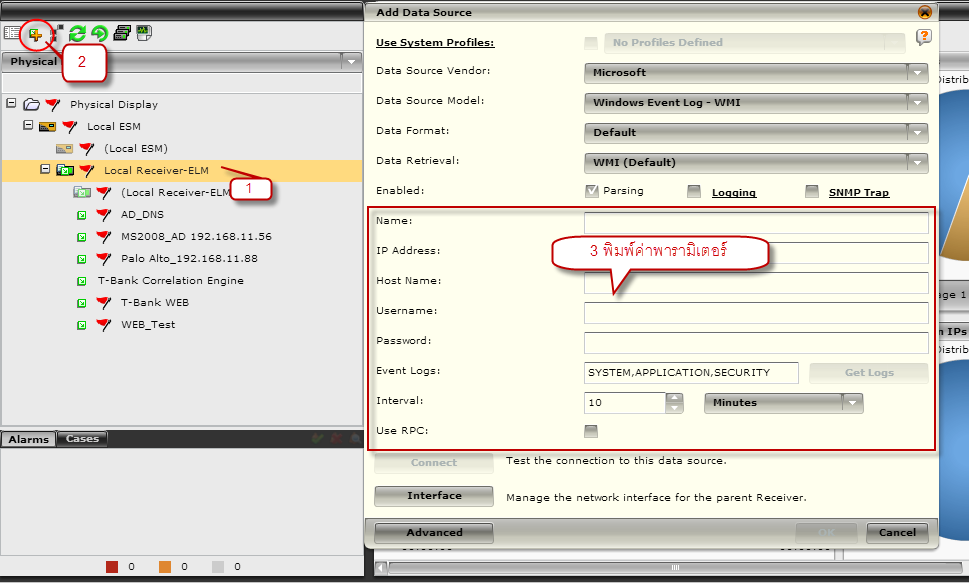
3. Web Gateway Data Source

4. Write the Data Sources to the Receiver

การเพิ่ม Data source สามารถทำได้โดยการเลือกที่ Local Receiver-ELM คลิก Add Data source

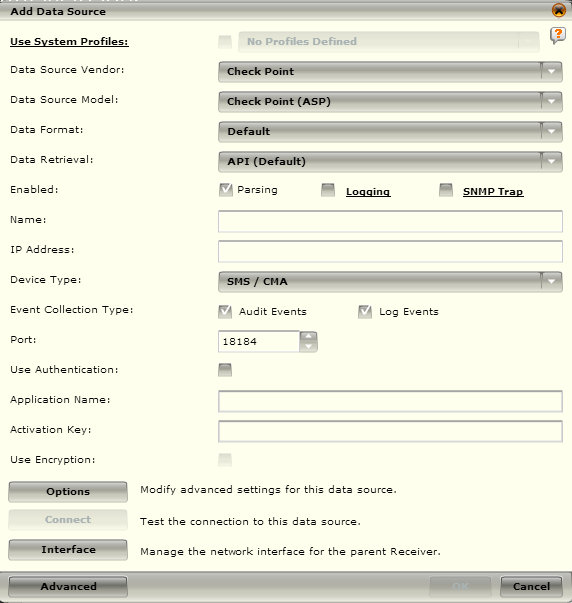


**1. WMI Data Source**

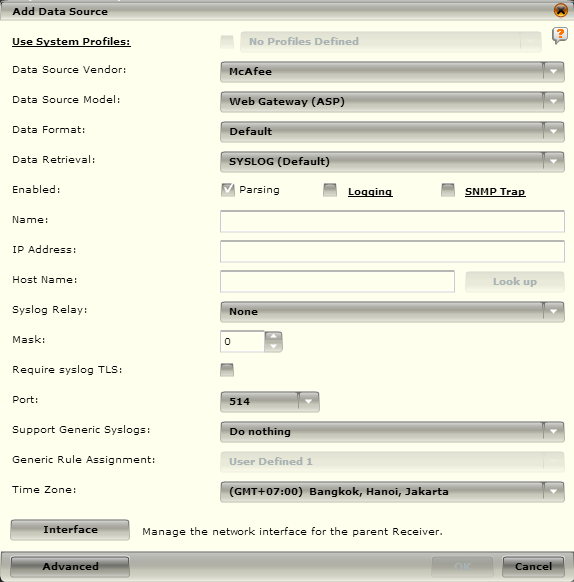


**2. Firewall Data Source**

****

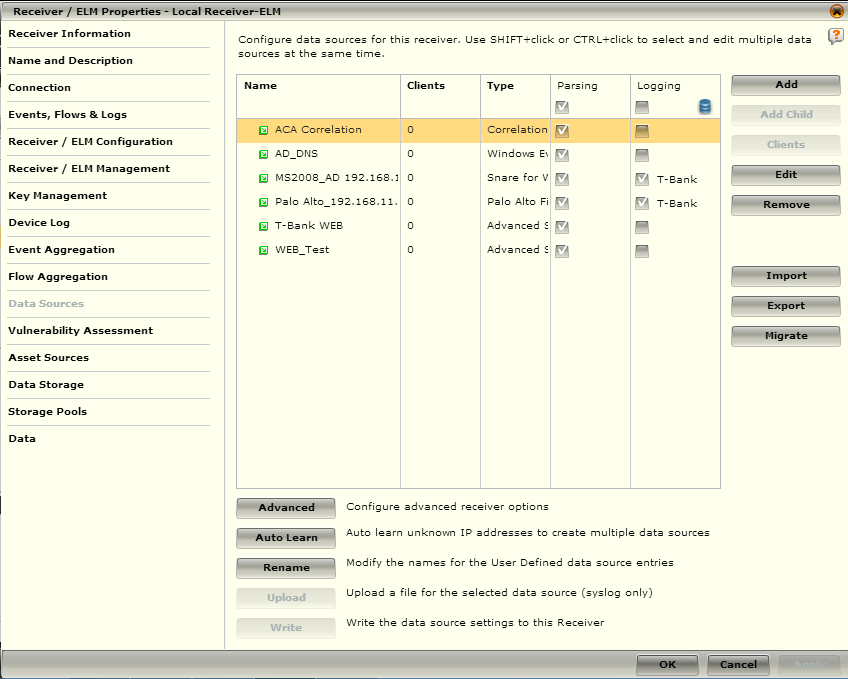


**3. Web Gateway Data Source**

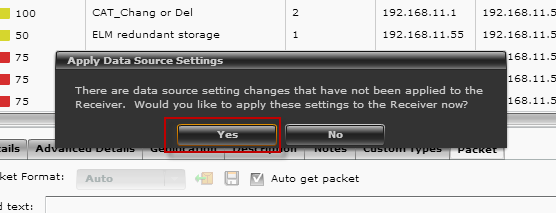


**4. การสั่งเขียน Data Sources ไปยัง Receiver**

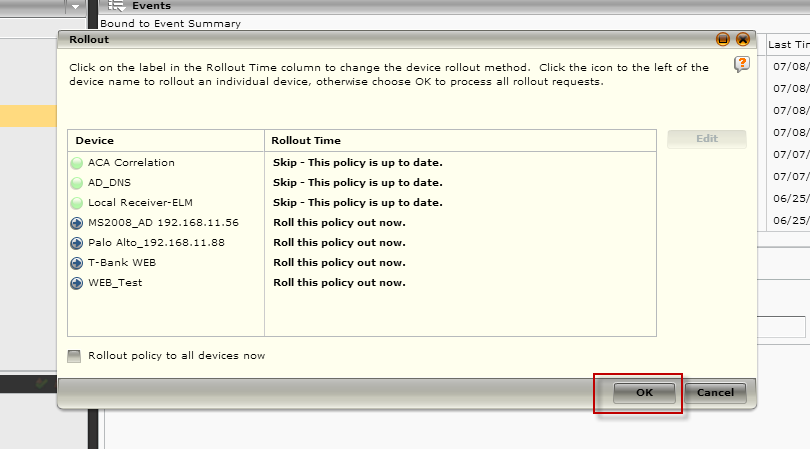
4.1.หลังจากทำการเพิ่ม Data source ใน Receiver/ELM คลิก เขียนจากปุ่มดังภาพด้านล่าง > OK



4.2.แสดงหน้าต่าง Apply Data source Setting > Yes



4.3. เมื่อมีการเปลี่ยนแปลงค่าต่างๆจะต้องมีการ Update policy คลิก Rollout Now ดังภาพด้านล่าง



**End of Practice 4**

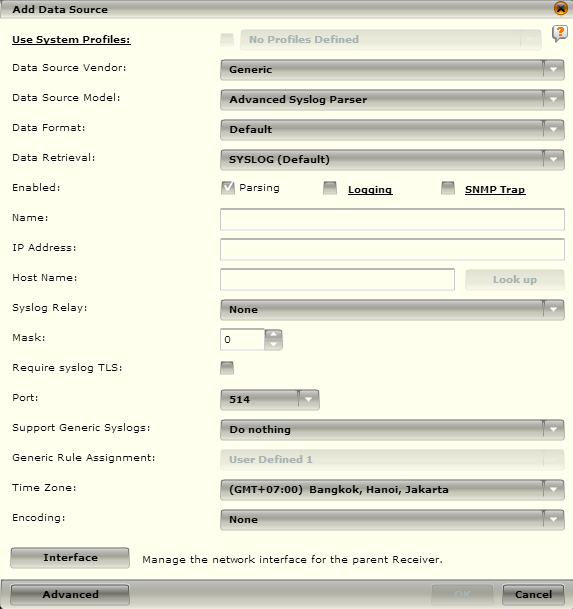
# Practice 5: Using the Syslog Parser

1. สร้าง syslog data source

2. สร้าง Advanced Syslog Parser Rule

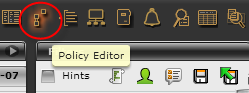
**1. สร้าง Syslog data source**

1.1. สร้าง Data Source เลือกข้อมูลดังรายละอียดภาพด้านล่าง

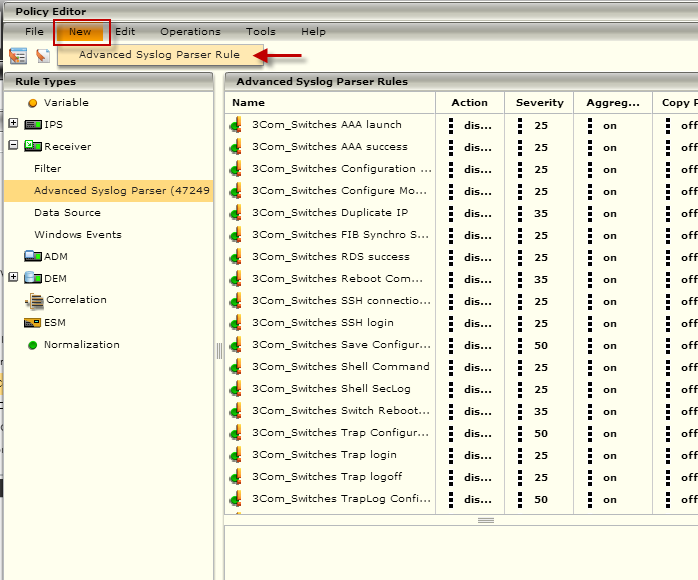


**2.Create Advanced Sys-log Parser Rule**

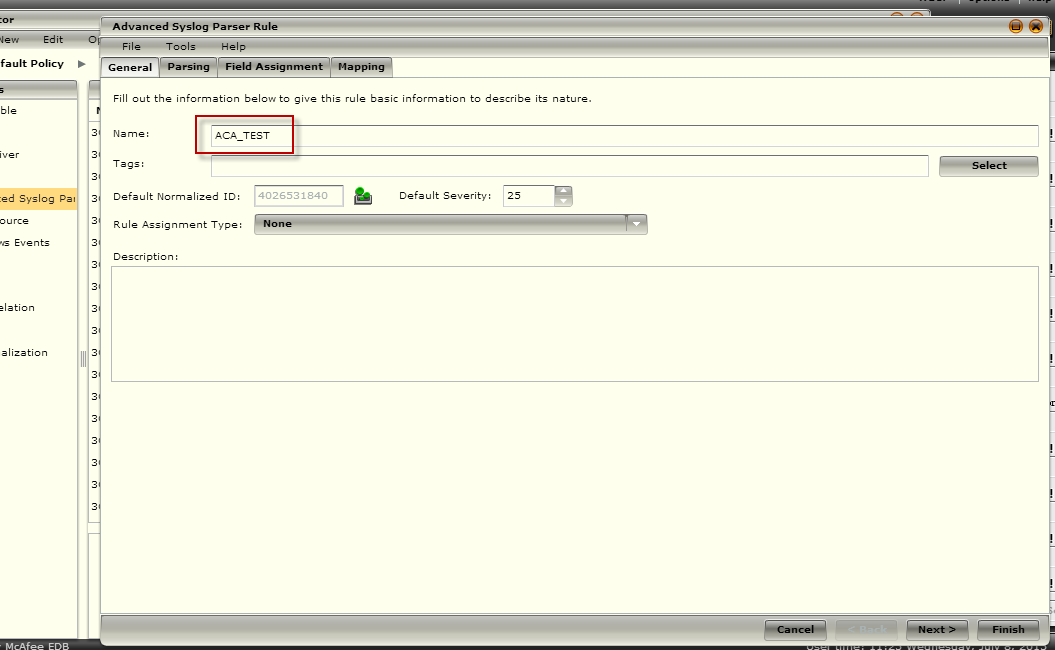
2.1. คลิกที่เมนู Policy Editor



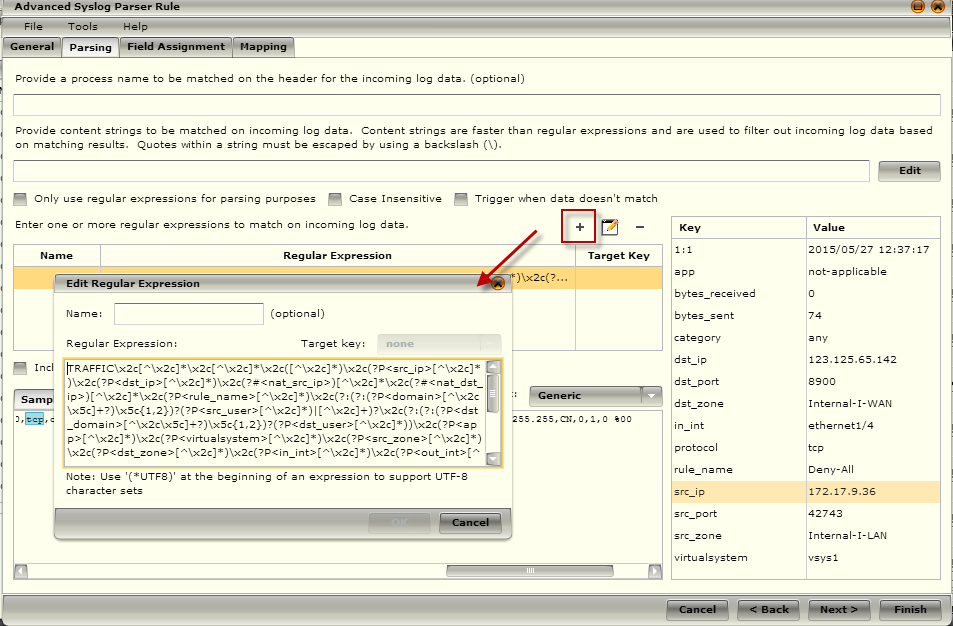
2.2. คลิก New > Advanced Syslog Parser Rule



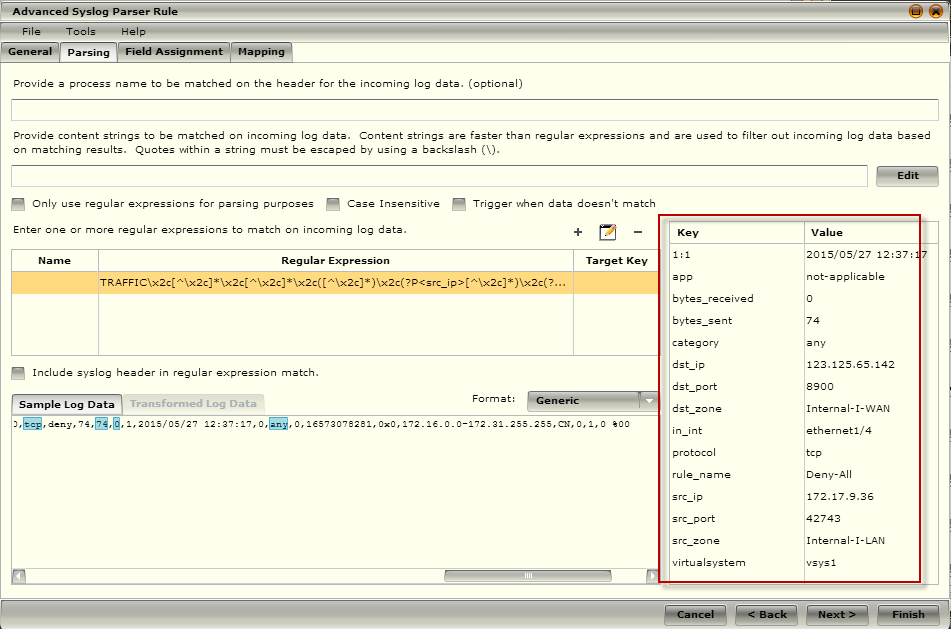
2.3. พิมพ์ชื่อตามต้องการ



2.4. ที่แถบ Parsing กดเครื่องหมายบวก > พิมพ์ Regular Expression ดังภาพด้านล่าง



2.5. เมื่อใส่ค่า Regex เรียบร้อยจะปรากฎหน้าต่างการจัดการของ Field > Next > Finish



**EX\_Log :**

<14>May 26 12:37:18 PA-5020 1,2015/05/27 12:37:17,0011C105250,TRAFFIC,drop,1,2015/05/27 12:37:17,172.17.9.36,123.125.65.142,0.0.0.0,0.0.0.0,Deny-All,,,not-applicable,vsys1,Internal-I-LAN,Internal-I-WAN,ethernet1/4,,UDRU-Syslog,2015/05/27 12:37:17,0,1,42743,8900,0,0,0x0,tcp,deny,74,74,0,1,2015/05/27 12:37:17,0,any,0,16573078281,0x0,172.16.0.0-172.31.255.255,CN,0,1,0 %00

**Regex:**

TRAFFIC\x2c[^\x2c]\*\x2c[^\x2c]\*\x2c([^\x2c]\*)\x2c(?P<src\_ip>[^\x2c]\*)\x2c(?P<dst\_ip>[^\x2c]\*)\x2c(?#<nat\_src\_ip>)[^\x2c]\*\x2c(?#<nat\_dst\_ip>)[^\x2c]\*\x2c(?P<rule\_name>[^\x2c]\*)\x2c(?:(?:(?P<domain>[^\x2c\x5c]+?)\x5c{1,2})?(?P<src\_user>[^\x2c]\*)|[^\x2c]+)?\x2c(?:(?:(?P<dst\_domain>[^\x2c\x5c]+?)\x5c{1,2})?(?P<dst\_user>[^\x2c]\*))\x2c(?P<app>[^\x2c]\*)\x2c(?P<virtualsystem>[^\x2c]\*)\x2c(?P<src\_zone>[^\x2c]\*)\x2c(?P<dst\_zone>[^\x2c]\*)\x2c(?P<in\_int>[^\x2c]\*)\x2c(?P<out\_int>[^\x2c]\*)\x2c[^\x2c]\*\x2c(?#unlisted date)[^\x2c]\*\x2c(?:0|(?P<session\_id>[^\x2c]\*))\x2c[^\x2c]\*\x2c(?P<src\_port>[^\x2c]\*)\x2c(?P<dst\_port>[^\x2c]\*)\x2c(?#<nat\_src\_port>)[^\x2c]\*\x2c(?#<nat\_dst\_port>)[^\x2c]\*\x2c[^\x2c]\*\x2c(?P<protocol>[^\x2c]\*)\x2cdeny\x2c(?#<bytes\_total>)[^\x2c]\*\x2c(?P<bytes\_sent>[^\x2c]\*)\x2c(?P<bytes\_received>[^\x2c]\*)\x2c[^\x2c]\*\x2c[^\x2c]\*\x2c[^\x2c]\*\x2c(?P<category>[^\x2c]\*)\x2c

End of Practice 5

# Practice 6: Correlation Rules

1. เพิ่ม Correlation Engine Data Source

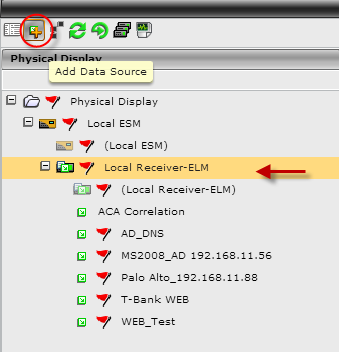
2. แก้ไข Correlation Rule

3. เพิ่ม Correlation Rule

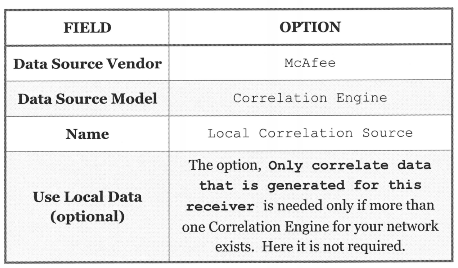
**1. เพิ่ม Correlation Engine Data Source**

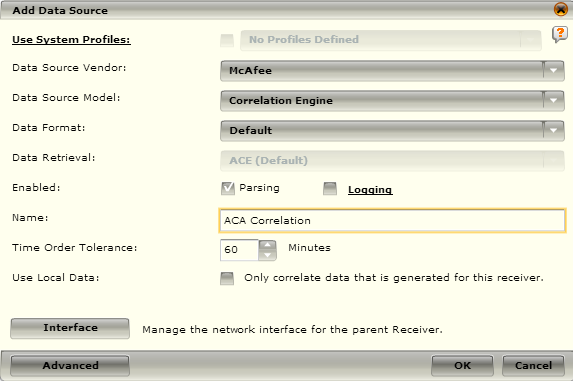
1.1. Login เข้าใช้งาน ESM ด้วย User : **NGCP**

1.2. คลิก Local Receiver – ELM > Add Data Source

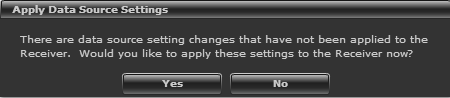


1.3. ป้อนข้อมูลต่อไปนี้ลงในหน้าต่างดังภาพด้านล่าง

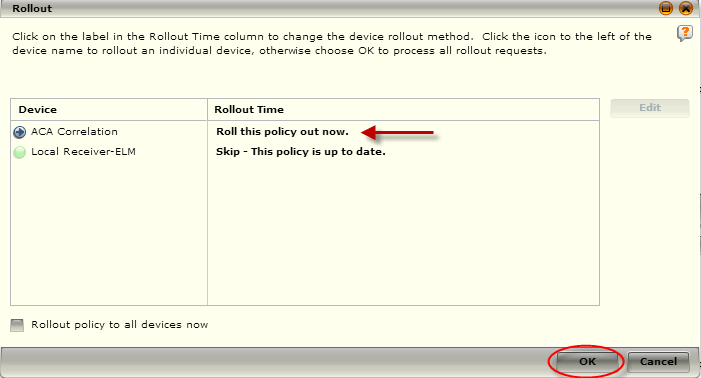




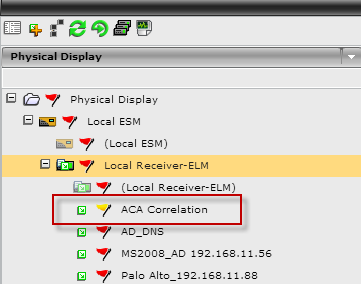
1.4. คลิก OK > Yes



1.5. ทำการ rollout policy

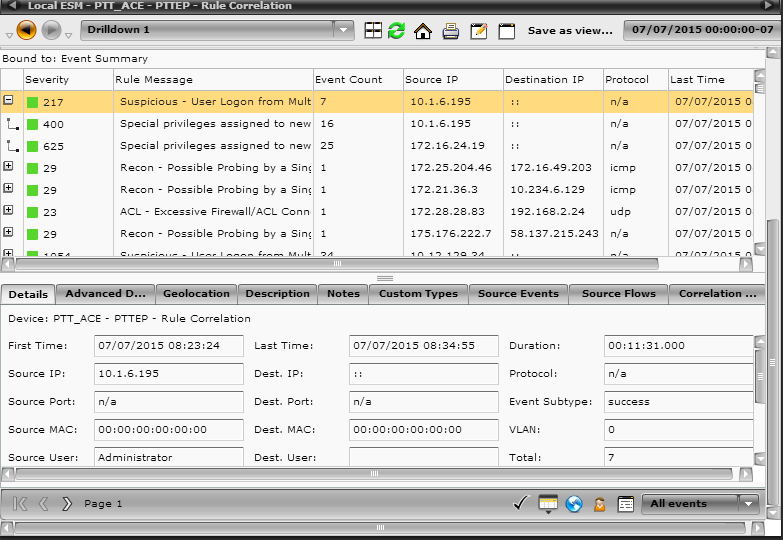


1.6. Correlation Device ปรากฎที่หน้าต่างแสดง Device

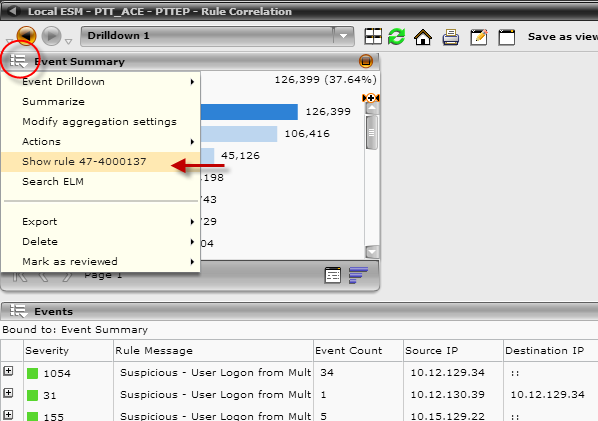


**2. แก้ไข Correlation Rule**

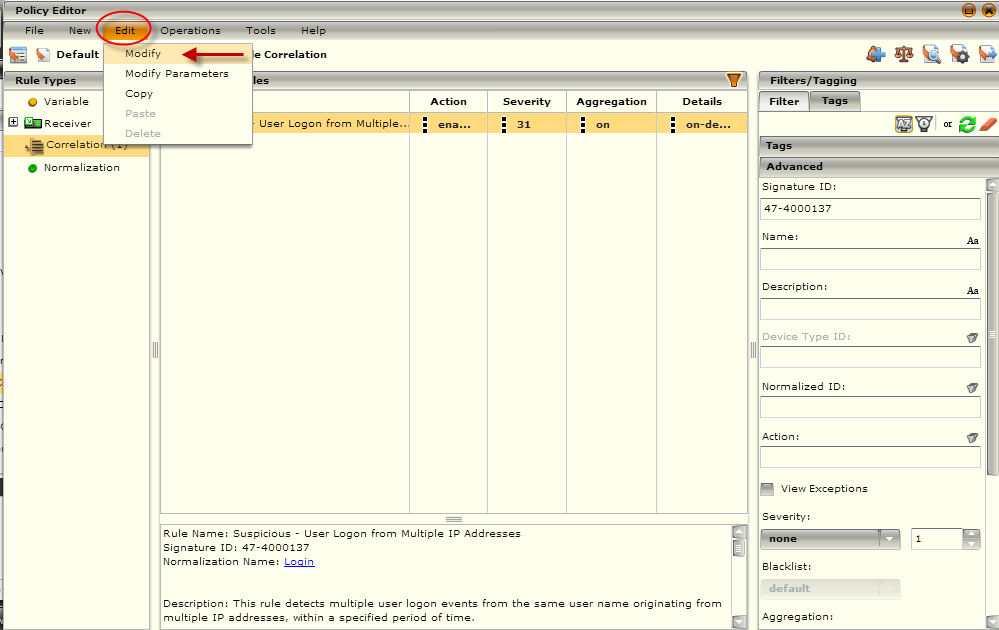
จากภาพด้านล่างจะแสดงให้เห็นความสัมพันธ์ของ Event



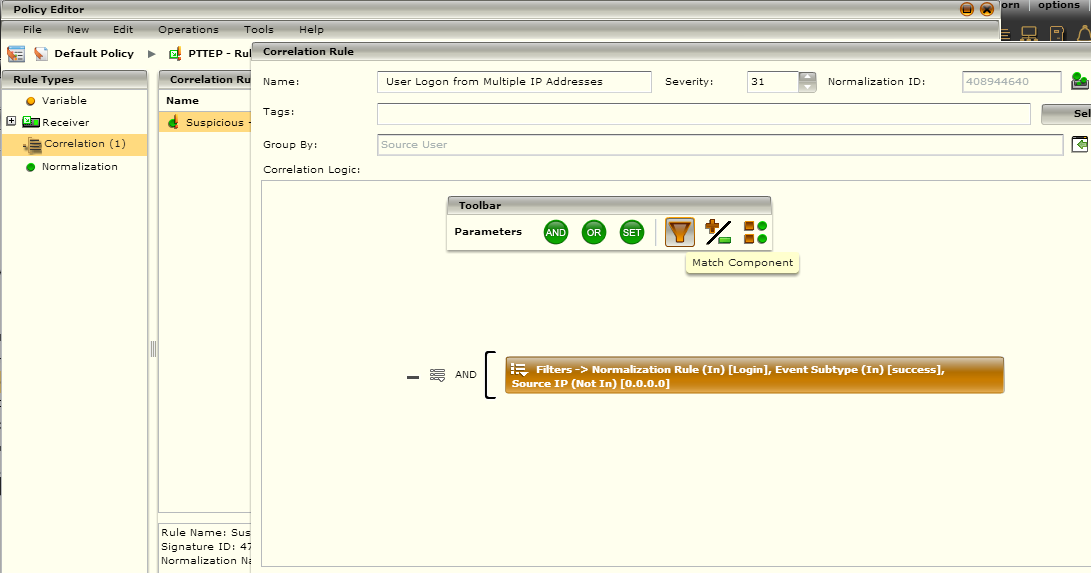
2.1. เลือกเหตุการณ์ที่ต้องการคลิกเมนู Show rule 47-4000137 ดังภาพด้านล่าง



2.2. จากเมนูคลิก Edit > Modify



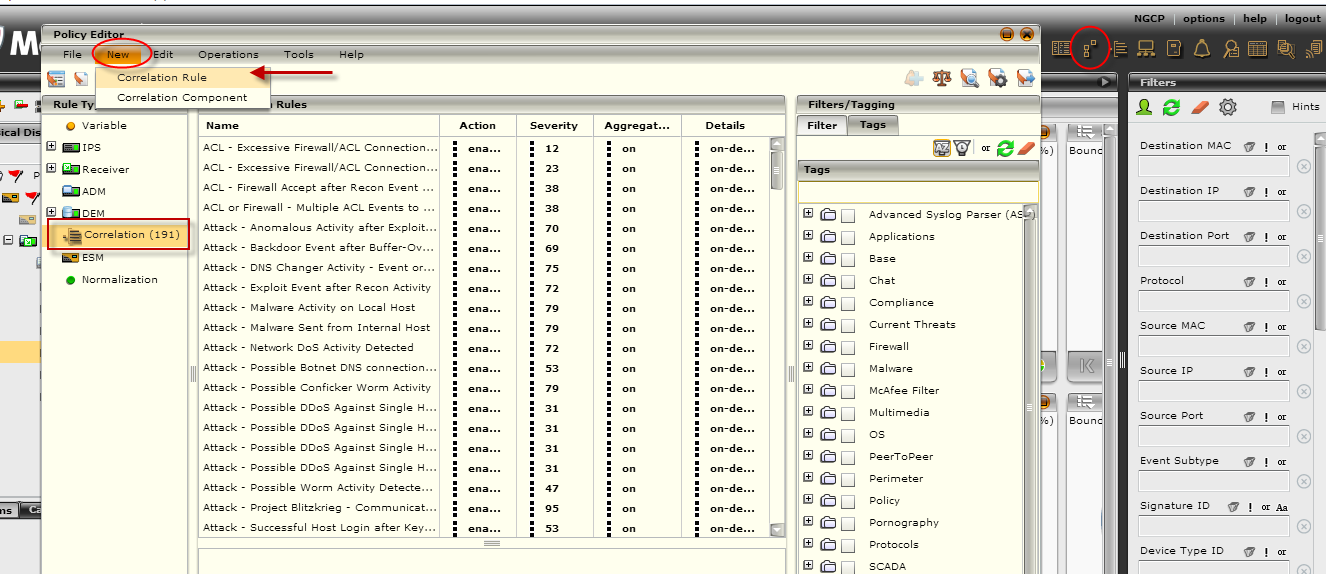
2.3. หลังจากคลิก Modify จะปรากฎหน้าต่างแสดงหน้างต่างแสดงความสัมพันธ์ของเหตุการณ์



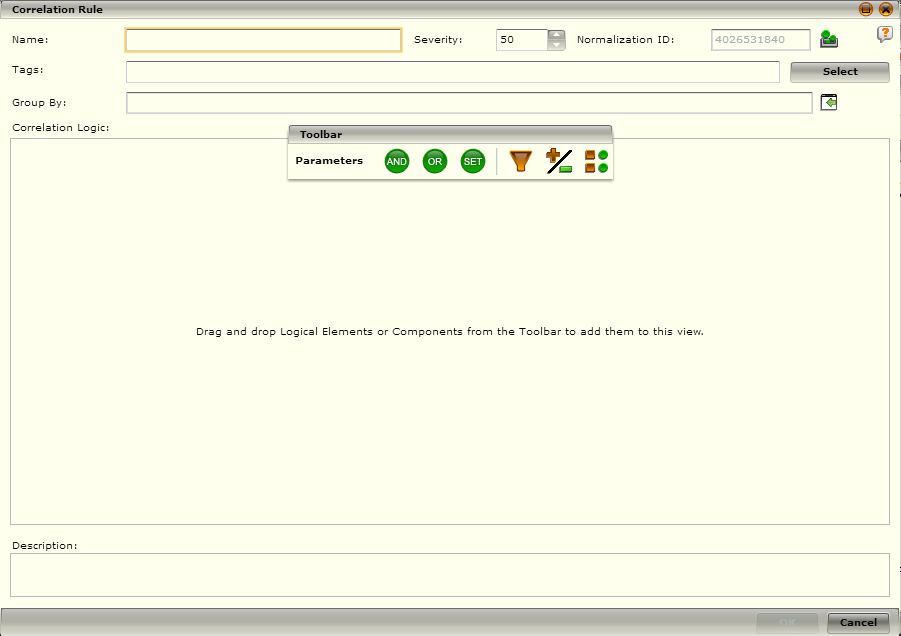
2.4. เปลี่ยนชื่อและเปลี่ยน Group ของกฎตามต้องการ > OK

**3. เพิ่ม Correlation Rule**

3.1 คลิกที่แถบ Policy Editor > New > Correlation Rule



2.2. ตั้งชื่อและตั้งค่าความสัมพันธ์ของเหตุการณ์



End of Practice 6

# Practice 7: Alarms and Watchlists

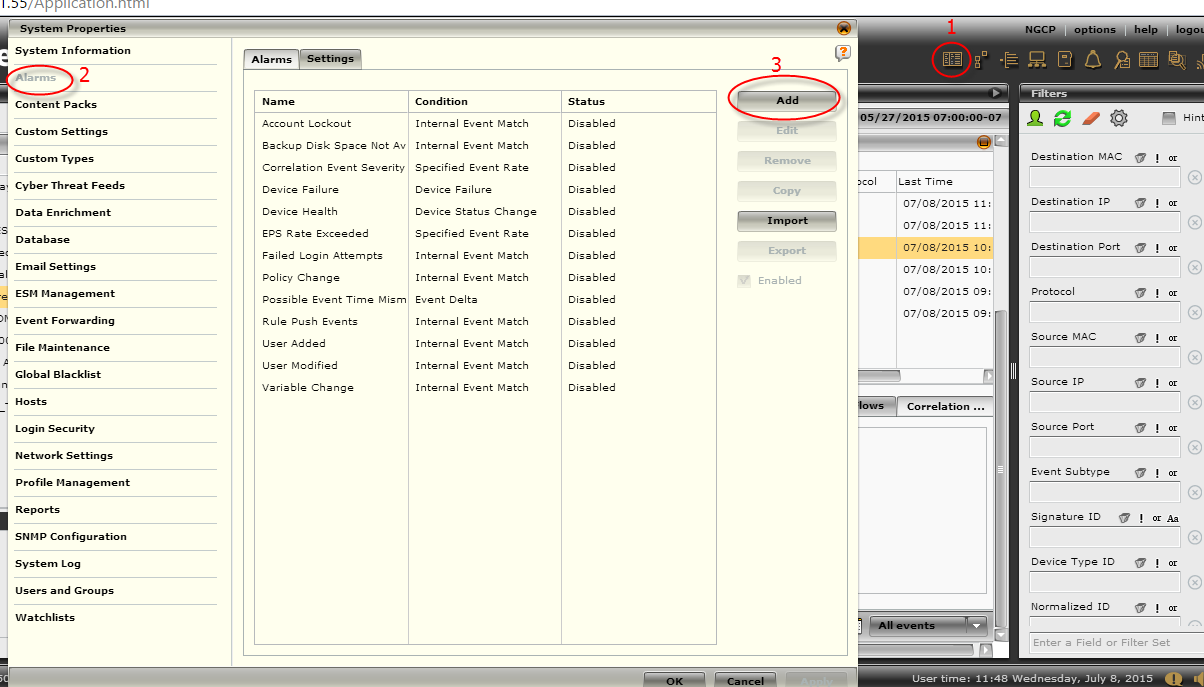
1. สร้าง Alarm

2. สร้าง Watchlist

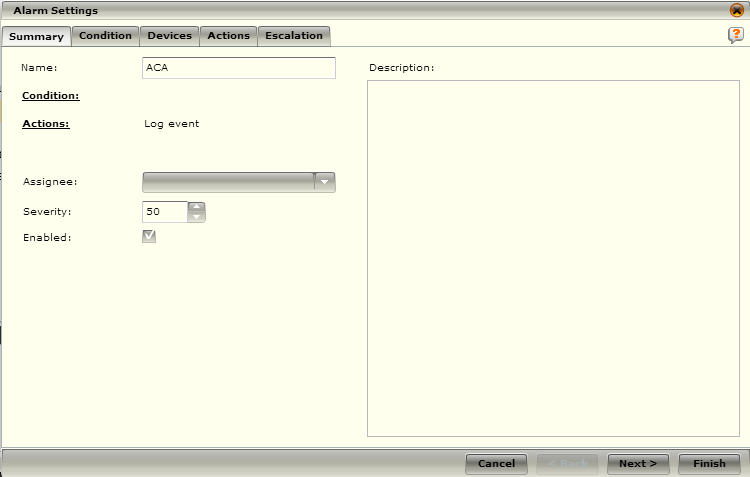
**1. สร้าง Alarm**

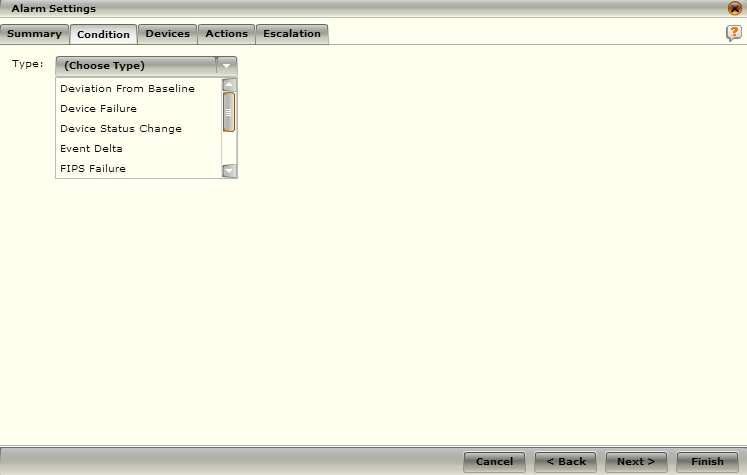
1.1. คลิกที่แถบเมนู System Properties

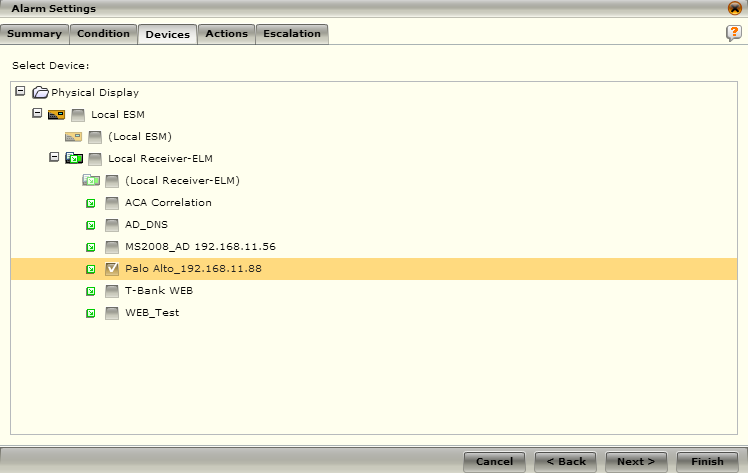
1.2. คลิก Alarms > Add

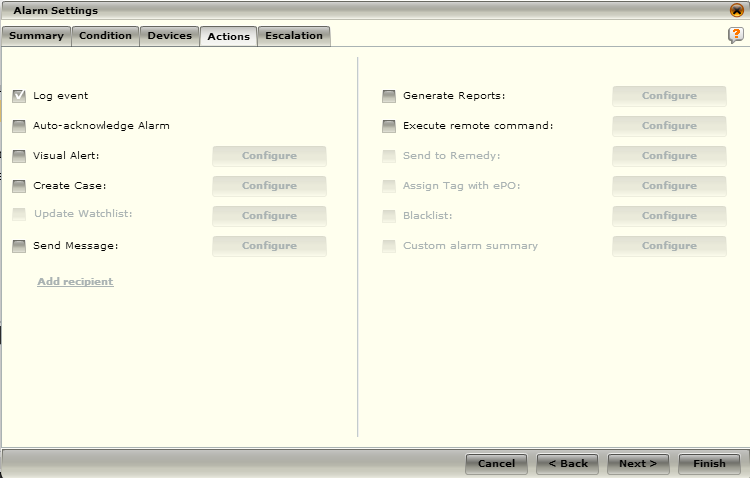


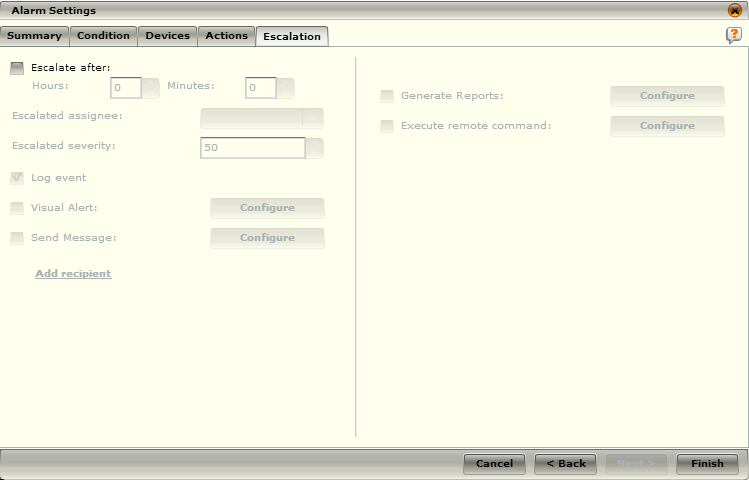
1.3. ปรากฎหน้าต่างการกำหนดค่าต่างๆ









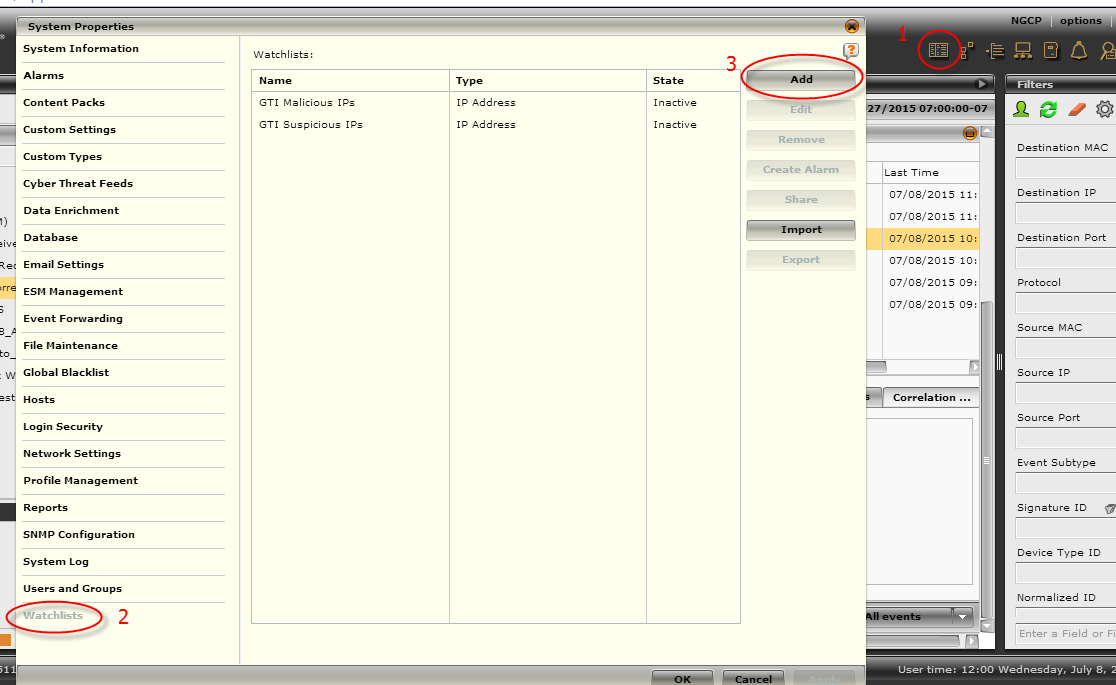


1.4. หลังจากกำหนดค่าต่างๆตามต้องการ คลิก Finish

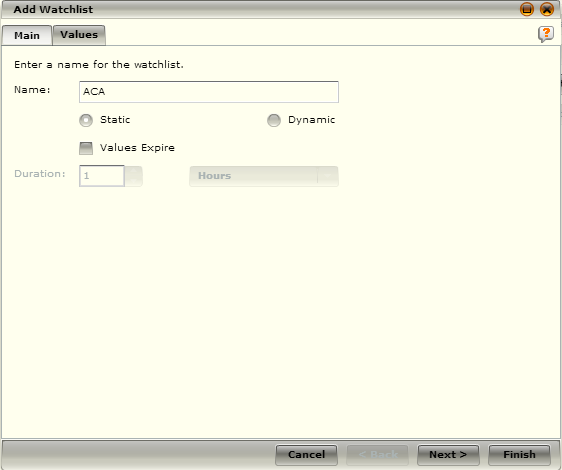
**2. สร้าง Watchlist**

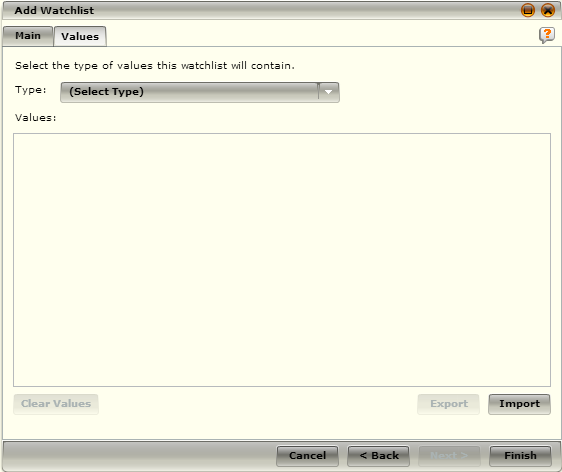
2.1. คลิกที่แถบเมนู System Properties

2.2. คลิก **Watchlist** > Add



2.3. ปรากฎหน้าต่างการกำหนดค่าต่างๆ





2.4. หลังจากกำหนดค่าต่างๆตามต้องการ คลิก Finish

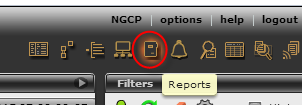
End of Practice 7

# Practice 8: Reporting

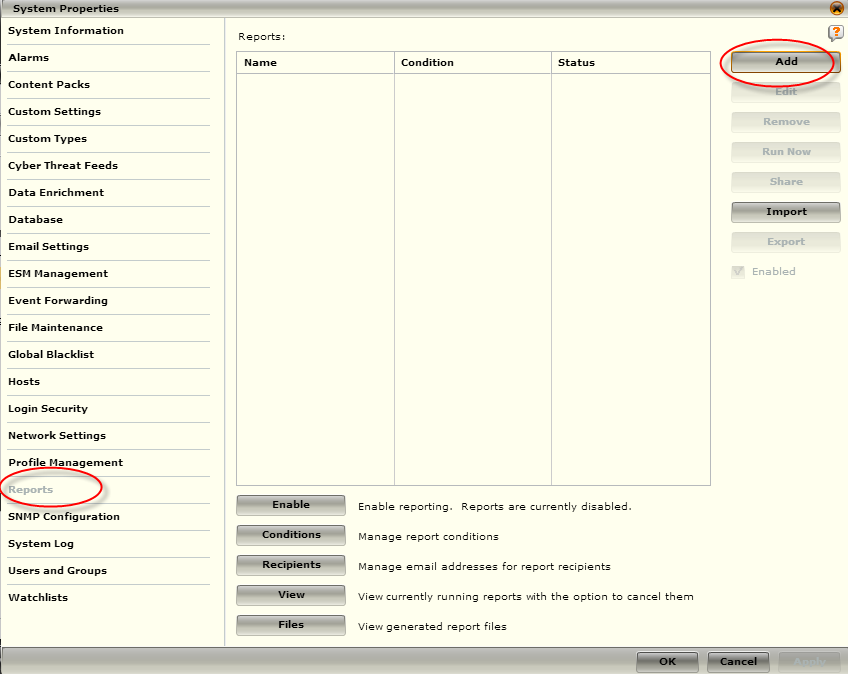
1. สร้าง Report ด้วย out-of-the-box
2. การสั่ง Run Report

**1. สร้าง Report ด้วย out-of-the-box**

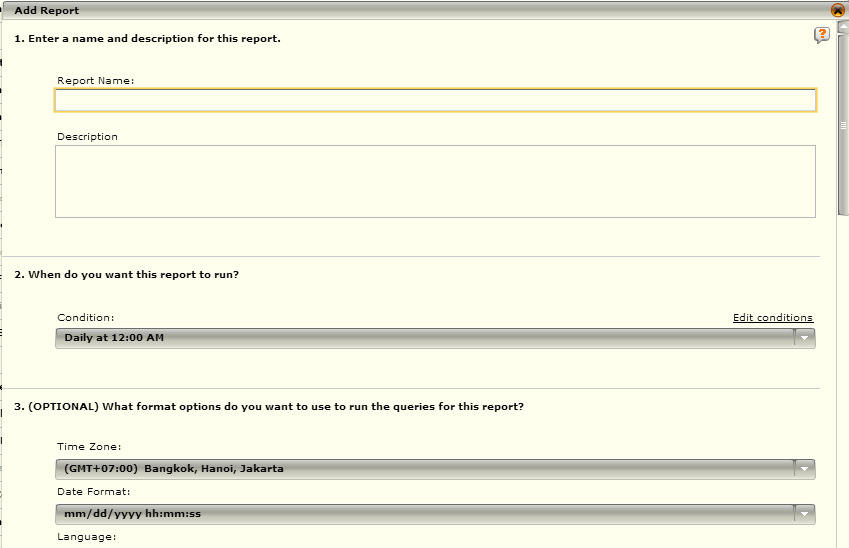
* 1. จากแถบเมนูเลือก Report

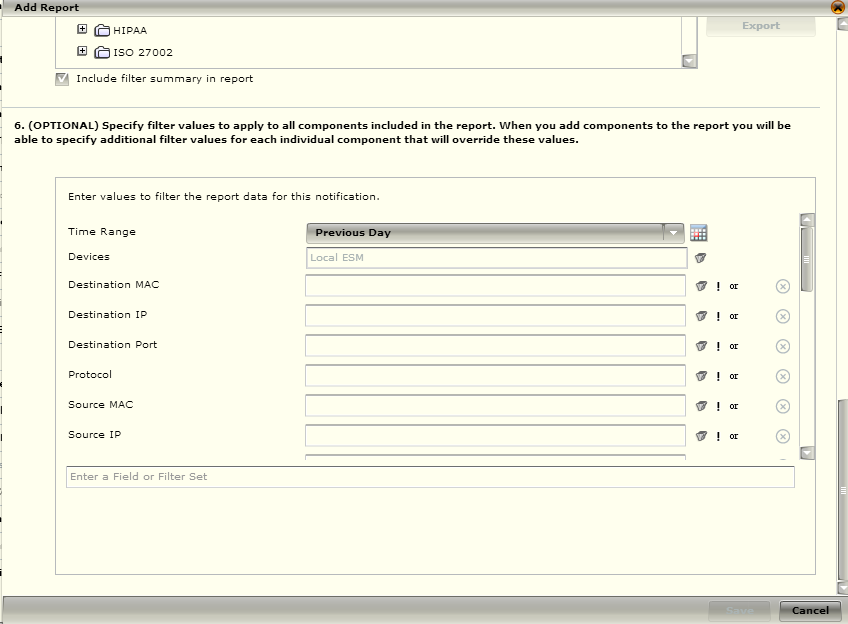


1.2 เลือก List : Report > Add



1.3 ปรากฎหน้าต่างการกำหนดค่าต่างๆ





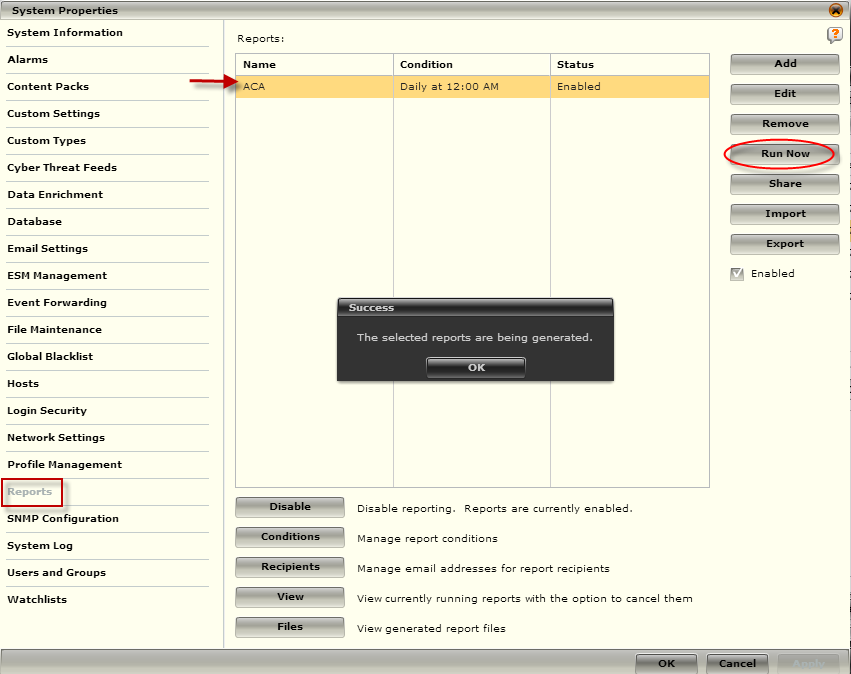
1.4 คลิก Save > OK

**2. การสั่ง Run Report**

2.1 คลิกที่แถบเมนู System Properties > Report

2.2 เลือก Report ที่ต้องการ Run

2.3 เลือก Run Now



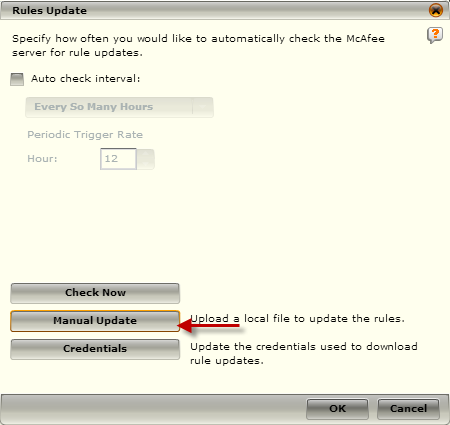
End of Practice 8

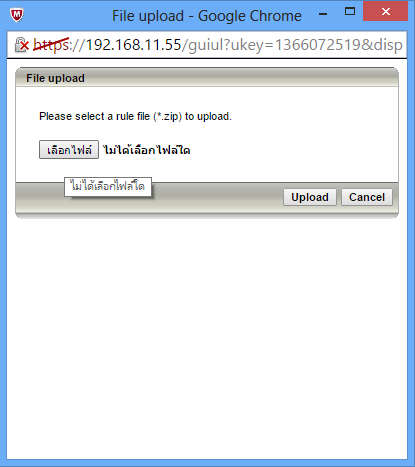
# Practice 9: Update Rule

1. คลิกที่แถบเมนู System Properties
2. เลือก System Properties
3. คลิก Rules Update



1. เลือก Manual Update > เลือก File ที่ต้องการ Update > Upload





End of Practice 9