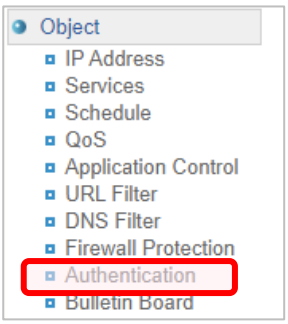
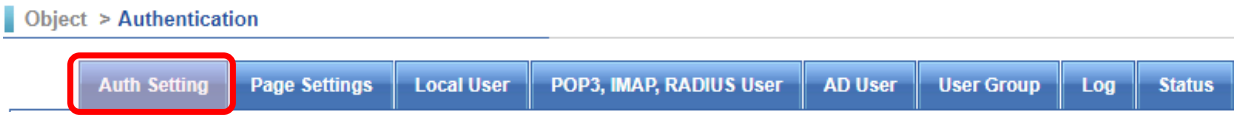
Authentication

การ Setting สำหรับระบบ Authentication มีขั้นตอนการ Setting ดังนี้

1.เปิดเมนู Object > Authentication

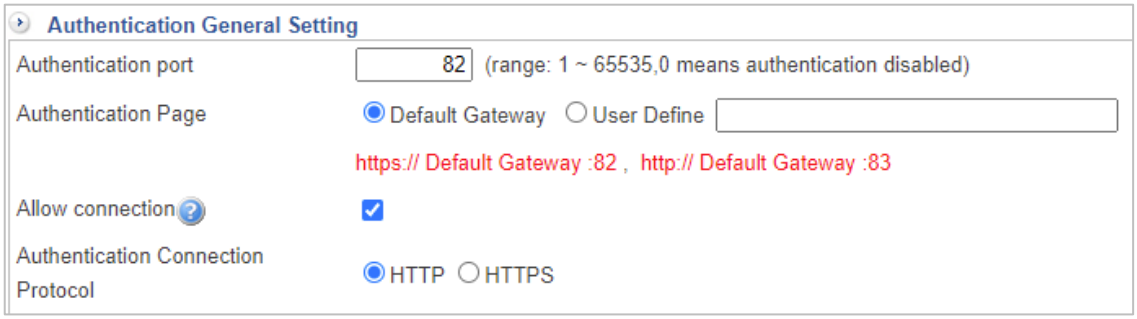


2.ให้เลือก Auth Setting เป็นการกำหนดค่าเบื้องต้นสำหรับ Authentication เรียกใช้งาน



หมายเหตุ : Authentication จะใช้สำหรับเครือข่ายภายในเท่านั้น

Support : support.th@nit.co.th
Sales : rung@nit.co.th
Mobile : 081=985-6916
Web : www.netinfortech.co.th
Line : nit.sharetech



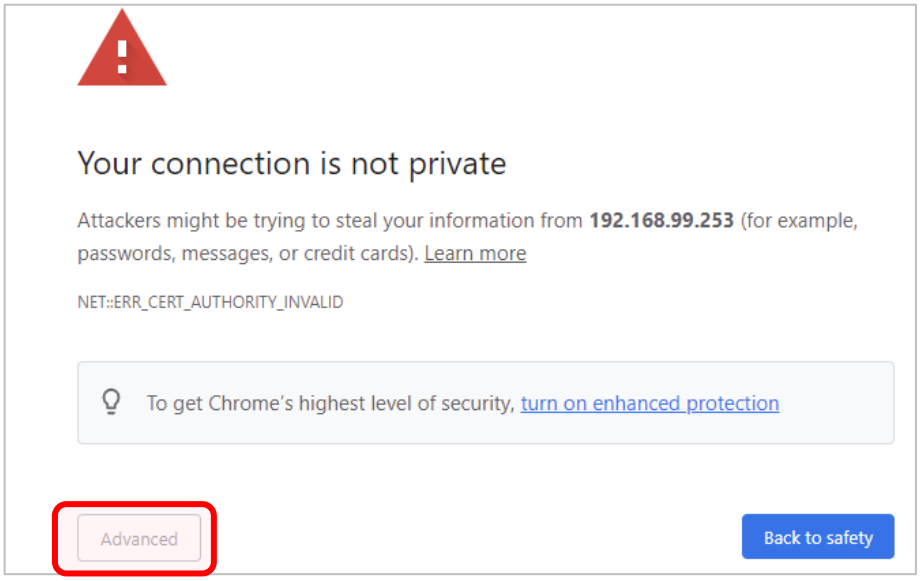
2.1 Authentication port ค่าเริ่มต้นจะเป็น 82 สามารถเปลี่ยนแปลงได้แต่ต้องไม่ซ้ำกับ Port ที่มีใช้อยู่

2.2 Authentication Page เป็นการกำหนด IP Address เมื่อเรียกหน้าจอ Login โดยค่าเริ่มต้นจะเลือก Default Gateway คือ LAN IP Address บน Firewall แต่ถ้ามีหลาย LAN บน Firewall และต้องการให้ใช้ IP Address อื่นๆที่ไม่ใช่ Gateway เพื่อหลีกเลี่ยงการโจมตี Gateway ให้ใส่ IP Address ที่ User Define

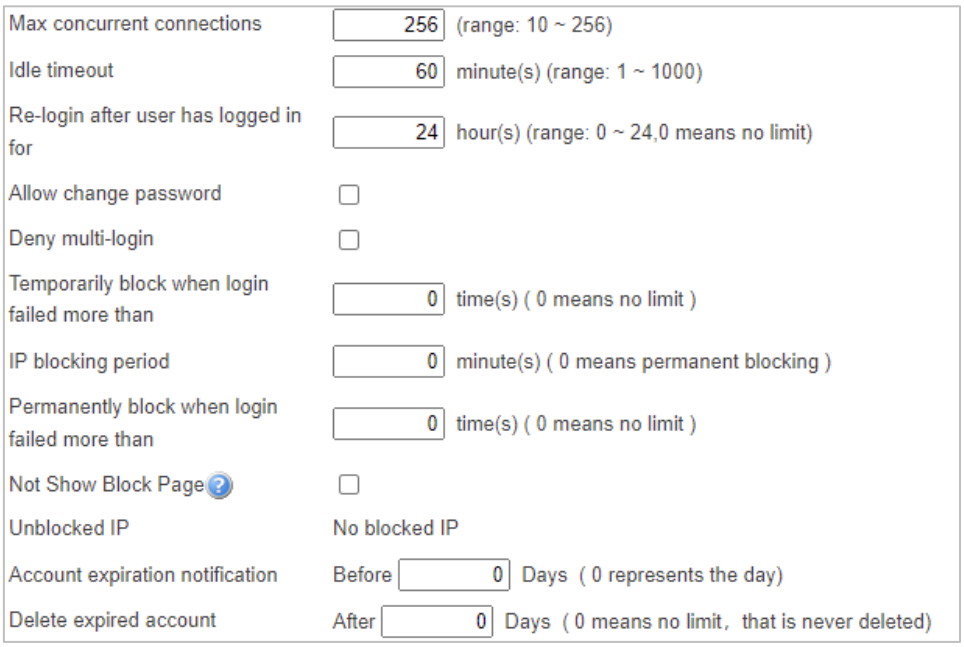
! หมายเหตุ : เมื่อใส่ IP แล้วจะแสดงตัวอย่างสีแดงด้านล่าง

2.3 Allow connection ให้เอาเครื่องหมายถูกออก ถ้ามีการใส่ไว้ ความหมาย คือเป็นการอนุญาตให้ IP Address ที่อยู่นอกลุ่ม Authentication สามารถเรียกหน้าจอ Login ได้ เช่น http://192.168.99.253:83

2.4 Authentication Connection Protocol มีให้เลือก HTTP และ HTTPS เมื่อเรียกหน้าจอ Login ให้เลือกตามความเหมาะสม ซึ่งถ้าเลือก HTTPS เวลาเปิดหน้าจอ Login จะถามเรื่อง Certificate ทุกครั้ง



! ให้คลิก Advanced และเลือกยอมรับความเสี่ยงเพื่อเปิดหน้า Login



2.5 Max concurrent connections คือ อนุญาตให้ผู้ใช้งานสามารถติดต่อกับ Auth Server ได้สูงสุด 256 Connections ต่อ ผู้ใช้งาน

2.6 Idle timeout คือ เมื่อ Login สำเร็จแล้วไม่การรับส่งข้อมูล ผ่าน Firewall หรือปล่อยเครื่องคอมพิวเตอร์ทิ้งไว้ไม่มีการเคลื่อนไหวของ Mouse ระบบ Auth จะทำการตัดการเชื่อมต่อและให้ ผู้ใช้งานทำการ Login ใหม่ หน่วยที่ใส่จะเป็น นาที

2.7 Re-login after user has logged in for ความหมายคือ ถ้าผู้ใช้งาน Login สำเร็จและจะอนุญาตให้ใช้งาน ไปกี่ชั่วโมงแล้วระบบจะตัดการเชื่อมต่อ เพื่อให้ Login ใหม่ หน่วยเป็น ชั่วโมง (0-24, 0 คือไม่มีการตัดการเชื่อมต่อ)

! หมายเหตุ : เหมาะสำหรับป้องกันผู้ที่เปิดเครื่องแล้วโหลดงานทิ้งไว้

2.8 Allow change password ถ้าคลิกถูกระบบจะมีปุ่ม Change password ให้ผู้ใช้งานสามารถเปลี่ยน Password เองได้ ที่หน้า Logout

2.9 Deny multi-login ถ้าคลิกถูกผู้ใช้งานจะ Login ได้เครื่องคอมฯ เครื่องเดียวเท่านั้น

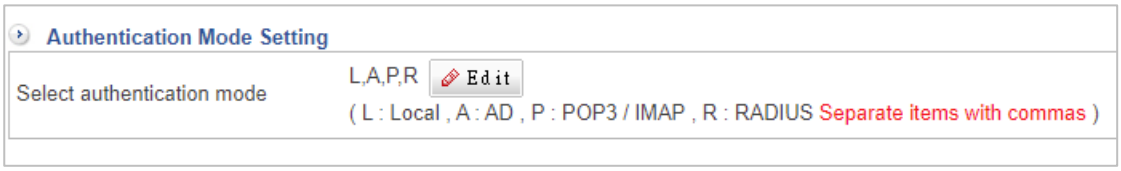
2.10 Temporarily block when login fail more than เป็นการตรวจเช็คการ Login ผิดจำนวนกี่ครั้งแล้วทำการ Block ถาวร หรือ เป็นนาทีได้

2.11 IP blocking period การ Block เป็นนาทีเมื่อ login ผิดครบตามจำนวนครั้งที่กำหนด

2.12 Permanently block when login failed more than เป็นการ Block แบบถาวรจนกว่า Admin จะทำการคลาย Block ในหัวข้อ Unblocked IP

2.13 Account expiration notification ความหมายคือจะแจ้งก่อนกี่วันที่จะ Disable ผู้ใช้งาน ถ้ามีการกำหนด Expiration Date ไว้

2.14 Delete expiration account ระบบจะเก็บผู้ใช้งานที่หมดอายุ ไว้ตามจำนวนวันที่กำหนดถึงทำการลบออกจากระบบ



2.15 จะเป็นกำหนดว่า Auth สามารถดึง Username / Password จากที่ไหนบ้าง

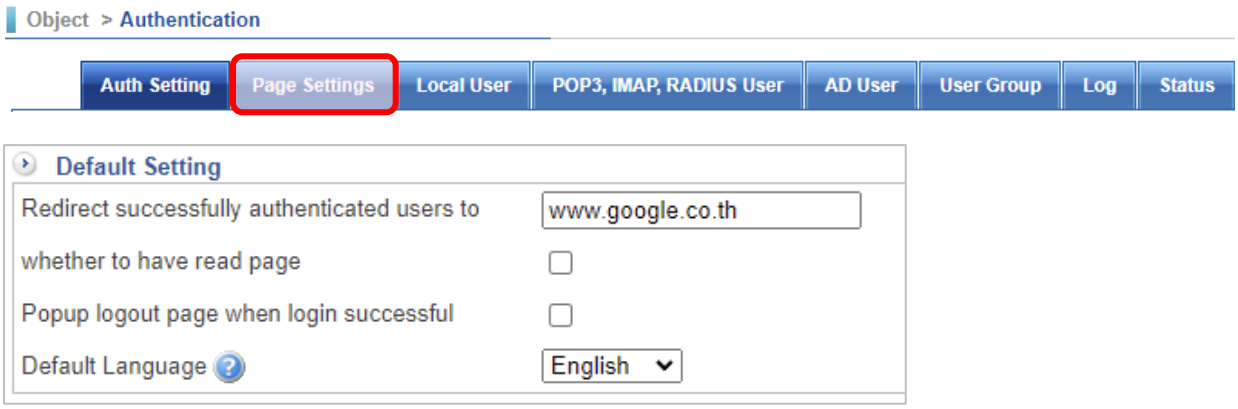
- L คือ Local users database จะเก็บอยู่บนอุปกรณ์ Firewall
- A คือ Microsoft Active Directory หรือเรียกว่า AD
- P คือ ดึงจาก POP3 / IMAP ที่ Mail Server
- R คือ Radius server ใช้สำหรับเก็บ Username / Password

สามารถเลือกได้มากกว่า 1 ชนิด และตอนเช็คจะไล่จาก ซ้าย ไป ขวา เช่น L, A จะเช็คที่ Local ก่อนถ้าไม่พบก็จะไปเช็คที่ A ต่อ

2.16 กดปุ่ม Save

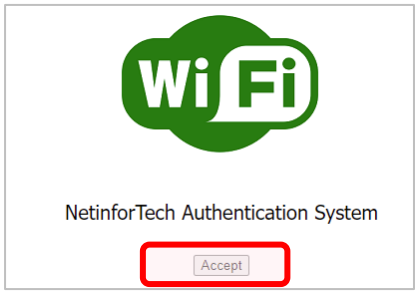
2.17 ไปขั้นตอนถัดไป

3. คลิกที่เมนูย่อย Page Settings เป็นการปรับแต่งหน้าจอ Login

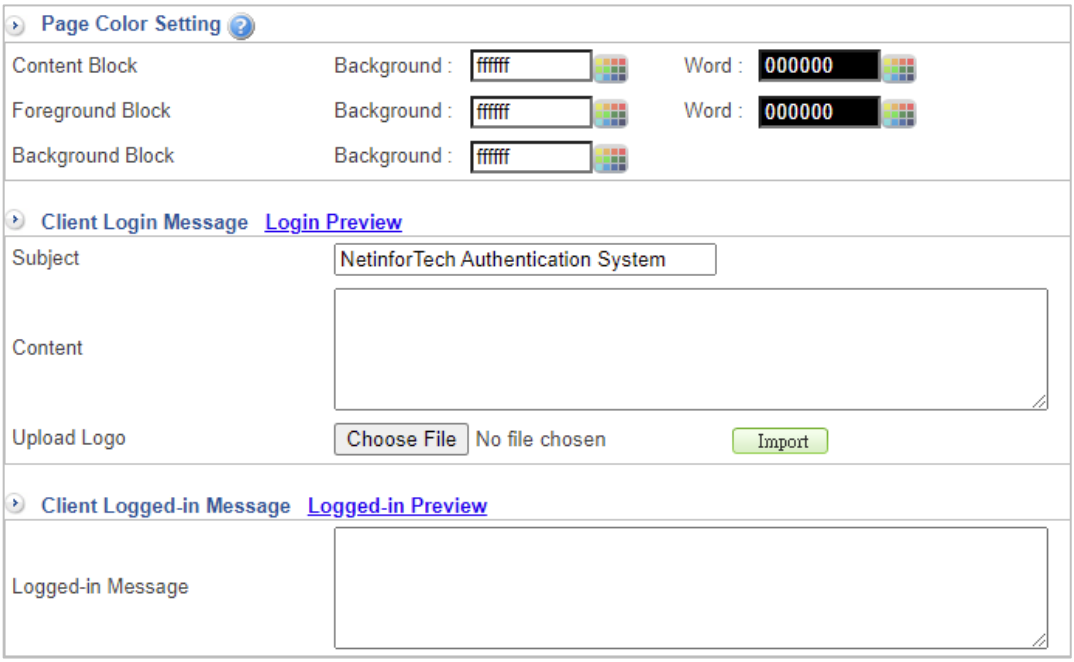


3.1 Redirect successfully authenticated users to คือถ้าผู้ใช้งาน Login สำเร็จ ต้องการให้ Redirect ไปหน้าเว็ปอะไร ตามตัวอย่างจะไปที่ www.google.co.th

3.2 whether to have read page ถ้าคลิกถูกจะต้องอ่านข้อความที่ต้องการแจ้งก่อน ถึงจะเข้าไปหน้าจอ login โดยต้องกดปุ่ม Accept แนะนำให้ข้ามขั้นตอนนี้



3.3 Popup logout page when login successful ให้คลิกเครื่องหมายถูก เพราะเมื่อ Login สำเร็จ ระบบจะ Automatic เปิดหน้าจอ Logout ไว้เพื่อ Logout ออกเมื่อเลิกใช้งาน



3.4 Page Color Setting เป็นการแก้ไข สีของหน้า Login และ Logout

3.5 Client Login Message เป็นการใส่ข้อความในหน้าจอ Login สามารถดูตัวอย่างที่สร้างโดยคลิกที่ Logged-in Preview

3.5.1 Subject คือหัวข้อของ Auth จะอยู่ใต้ Logo

3.5.2 Content คือข้อความที่ไว้แจ้งข่าวสารหรือช่องทางการติดต่อ สามารถใส่เป็น HTML TAG ได้

Content

```
<div style="outline: 1px ; width:50%; height:200px;align:left; font-
size:14px; line-height:190%;font-family: Arial, Helvetica, sans-serif;
background-color: #fff;" ><font size="middle"><b>ระบบพิสูจน์ตัวตนเพื่อใช้งาน
อินเทอร์เน็ต</b></font><div align="center"><table border="0">คำแนะนำ</u>
<li>ระบบพิสูจน์ตัวตนเพื่อใช้งานอินเตอร์เน็ต ตาม พรบ.ความผิดคอมฯ ปี 2550
<li>เพื่อตรวจสอบการเข้าใช้งานอินเตอร์เน็ทให้คีย์  http://login.comouter ที่
Browser(IE,Chrome,Microsoft Edge,Firefox)
<li>หากพบปัญหาในการใช้งานกรุณาติดต่อ ศูนย์คอมพิวเตอร์</td></tr></table>
</div>
```

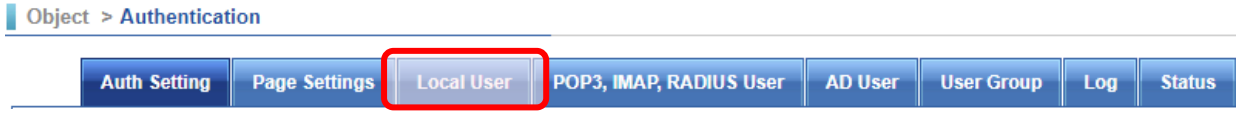
3.5.3 Upload Logo เป็นการใส่ Logo ให้หน้าจอ Login ให้กด Choose File แล้วกดปุ่ม Import

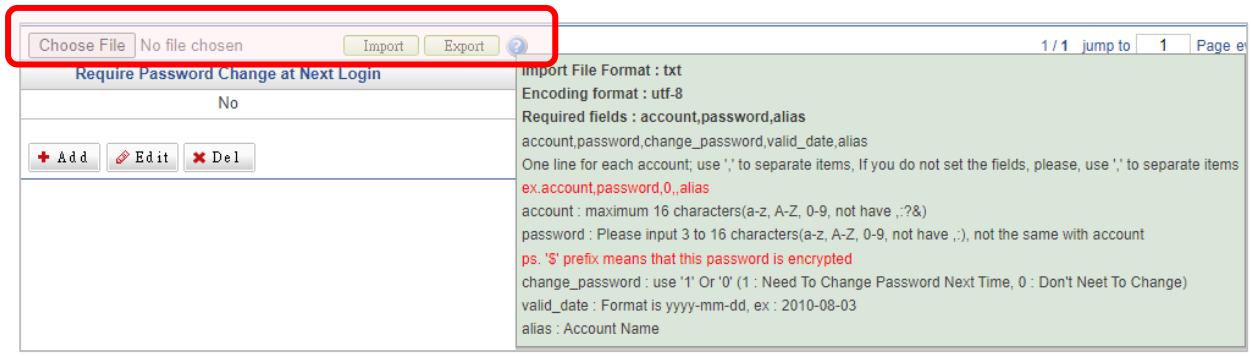
3.6 Client Logged-out Message เป็นการใส่ข้อความในหน้าจอ Logout สามารถดูตัวอย่างที่สร้าง โดยคลิกที่ Logged-in Preview

3.7 กดปุ่ม Save

3.8 ถัดไปทำการสร้าง Username / Password ที่ Local Users

4. เลือกเมนู Local Users





4.1 Username / Password สามารถสร้างที่เป็น TXT ไฟล์ที่มี Encoding format : utf-8 รูปแบบ username, password, change_password, valid_date, alias

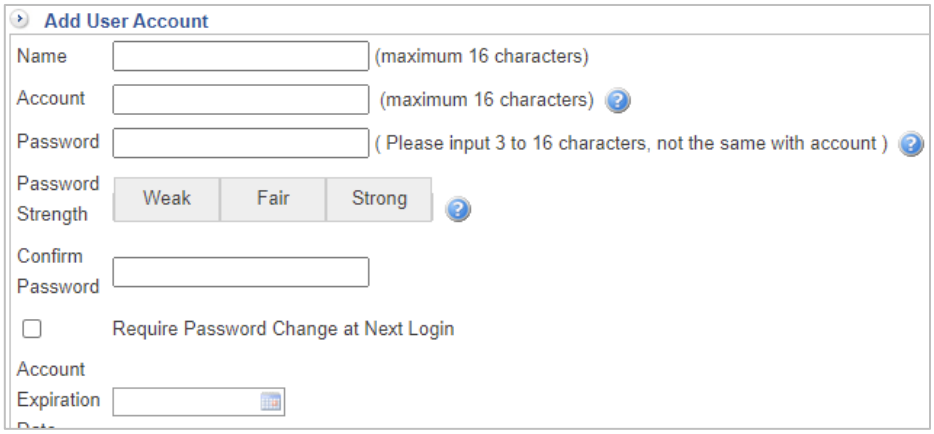
- change_password = 0 (ไม่เปลี่ยนรหัสผ่าน), 1 (สามารถเปลี่ยนรหัสผ่าน)
- valid_date = วันที่หมดอายุ
- alias คือ ชื่อและนามสกุล

ตัวอย่าง peter, 12345678, 0,,peter man

! หมายเหตุ ให้ใส่ 1 username ต่อ 1 บันทัด

4.2 Choose File ที่สร้างจากหัวข้อ 4.1 แล้วกดปุ่ม Import

4.3 หลังจาก Import เสร็จแล้วให้ข้ามไปทำหัวข้อ User Group แต่ถ้าต้องการสร้าง Username /Password ทีละชื่อให้กดปุ่ม Add



4.3.1 Name คือ ชื่อและนามสกุล

4.3.2 Account คือ Username ใน Firewall จะใช้คำว่า Account แทน Username

4.3.3 Password คือ รหัสผ่าน ต้องใส่ไม่น้อยกว่า 3 ตัวอักษรและไม่เกิน 16 อักษร

4.3.4 Password Strength เป็นการบอกเราว่า รหัสที่เราสร้างเข็มแข็งหรือไม่

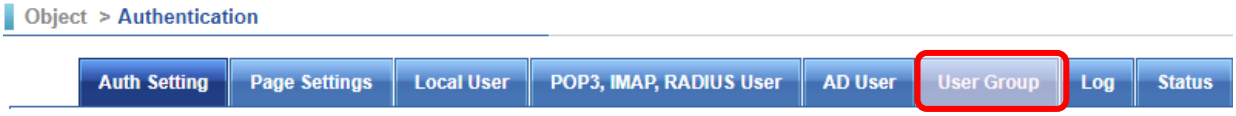
4.3.5 Confirm Password คือ ให้ใส่รหัสผ่านซ้ำอีกครั้งเพื่อยืนยันความถูกต้อง

4.3.6 Require Password Change at Next time ให้ข้ามถ้าไม่ต้องการให้เปลี่ยนรหัสผ่านที่ Login ครั้งแรก

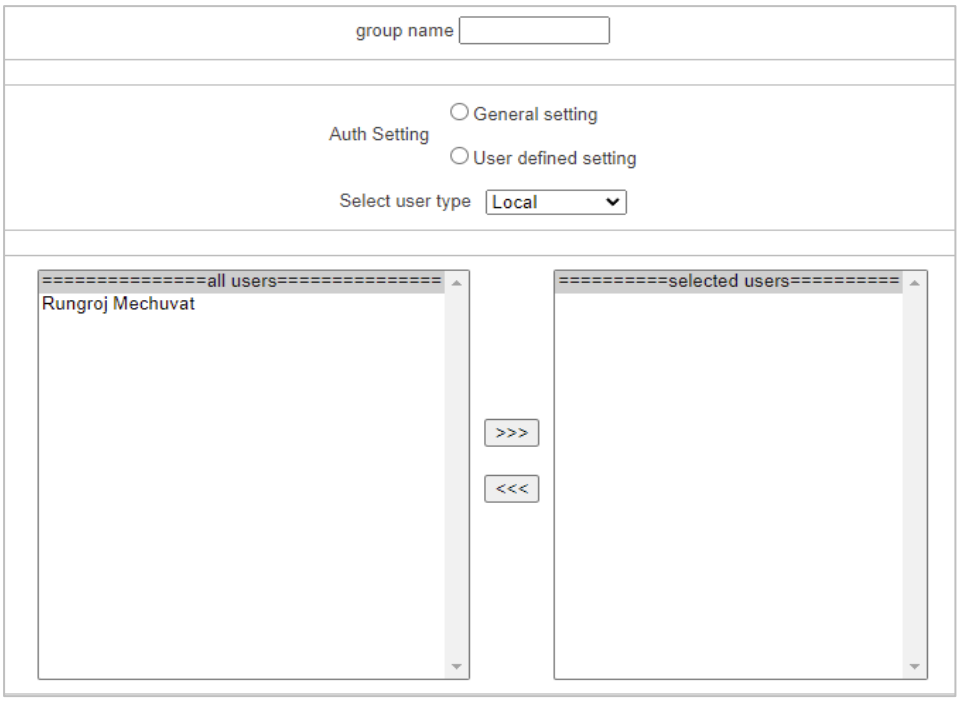
4.3.7 Account Expiration Date ถ้าไม่กำหนดวันหมดอายุของ Users นี้ให้ข้าม

4.3.8 กดปุ่ม Save ให้สร้างจนครบแล้วไปที่เมนู User Group

5. คลิกที่เมนูย่อย User Group



5.1 กดปุ่ม  เพื่อสร้างกลุ่มผู้ใช้งานที่ต้องการ Authentication

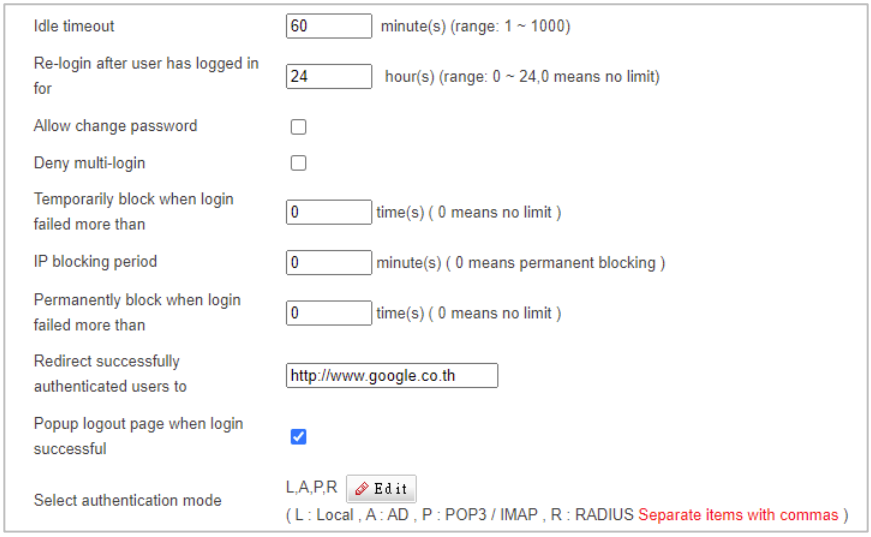


5.2 ใส่ชื่อของ Group name จะถูกนำไปเรียกใช้ที่ Policy

5.3 Auth Setting มีให้เลือก 2 Mode

5.3.1 General Setting จะเป็นการเลือกค่าที่สร้างในหัวข้อ Auth setting มาใช้งาน โดยไม่ต้อง Setting ใดๆทั้งสิ้น เนื่องจากมีการ Setting ที่เป็นพื้นฐานไว้แล้ว จากนั้นข้ามไปเลือก user type

5.3.2 User defined setting เป็นการตั้งค่าแยกตามกลุ่ม การตั้งค่าจะเหมือนข้อ 1



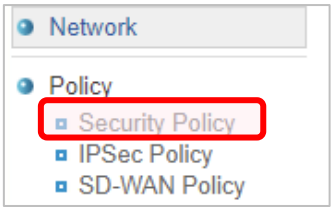
5.4 Users type ให้เลือก Local เพราะใช้ Local User Database

5.5 ย้าย Username จากจารางซ้ายมาตารางขวา

5.7 กดปุ่ม 

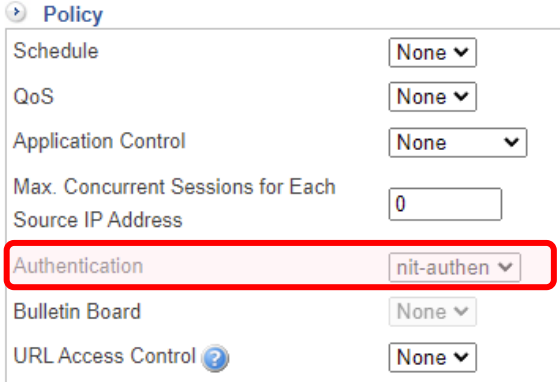
ต่อไปเข้าเมนู Policy เพื่อเปิดใช้งาน Authentication

6.8 คลิกที่เมนู Policy > Security Policy



6.8.1 เลือกเมนย่อย Outgoing

6.8.2 เข้าไป edit ที่ Policy ที่ต้องการเปิดใช้งาน Auth โดยกดปุ่ม 



6.8.3 ที่หัวข้อ Policy ตรงหัวข้อ Authentication ให้เลือก User Group ที่สร้างไว้ ให้เปิด Auth ทุกๆ Policy (80, 443, ALL) ของกลุ่ม IP ที่ต้องการตรวจสอบสิทธิ

6.8.4 กดปุ่ม 

6.9 ทดสอบการใช้งาน

หมายเหตุ : ถ้าทดสอบกับระบบที่ได้รับ IP Address จาก DHCP จะขึ้นหน้าจอ Login โดยอัตโนมัติ แต่ถ้าไม่ขึ้นหน้าจอ Login ให้กรอก URL เป็น http://login.computer หรือ URL HTTP อื่นๆก็ได้ แต่ถ้ากรอก URL ด้วย Facebook, google จะไม่ได้เพราะไม่ได้ใช้ TCP 443 แต่ใช้ UDP 443 ซึ่งระบบ Auth ไม่ยอมรับ