

คู่มือการใช้งาน One Session Security — AcademyWebs

1. One Session Security คืออะไร

One Session Security เป็นระบบรักษาความปลอดภัยสำหรับบัญชีนักเรียน โดยมีวัตถุประสงค์หลักเพื่อช่วยจำกัดการนำ **Username / Password** ของนักเรียนหนึ่งบัญชีไปใช้งานพร้อมกันหลายคน

แนวคิดหลักคือ แม้นักเรียนจะได้รับอนุญาตให้ลงทะเบียนอุปกรณ์ได้มากกว่าหนึ่งเครื่อง เช่น Notebook และ Desktop แต่ระบบสามารถควบคุมการเข้าใช้งานจริงด้วย **Active Session** เพื่อช่วยลดการแชร์บัญชีระหว่างผู้เรียนหลายคน

ตัวอย่างเช่น นักเรียนมี Device Limit = 2 เครื่อง ได้แก่

บัญชี Student1

อุปกรณ์ที่ลงทะเบียน

└─ Notebook

└─ Desktop

ไม่ได้หมายความว่าต้องอนุญาตให้ทั้งสองเครื่องใช้งานบัญชีพร้อมกันโดยไม่มีข้อจำกัด เพราะ **Device Access** และ **Session Security** เป็นคนละระดับของการควบคุม

2. ความแตกต่างระหว่าง Device Access และ One Session Security

ส่วนนี้สำคัญมาก เพราะผู้ดูแลระบบอาจเข้าใจว่าสองระบบทำงานเหมือนกัน

Device Access Manager ใช้กำหนดว่า นักเรียนสามารถลงทะเบียนอุปกรณ์ได้กี่เครื่อง เช่น 2 เครื่อง

ส่วน **One Session Security** ใช้ควบคุมการเข้าใช้งานบัญชีในขณะนั้น หรือ **Active Login Session**

สามารถจำง่าย ๆ ได้ว่า:

Device Access = “เข้าได้จากเครื่องไหนบ้าง”

One Session Security = “ขณะนี้บัญชีนี้กำลังถูกใช้งานอยู่ที่ไหน/กี่ Session”

ตัวอย่าง:

Device Limit = 2

Student1

└─ Windows PC A ✓ Registered

└─ Windows PC B ✓ Registered

แต่ Active Session

└─ ใช้งาน Session ปัจจุบันตามเงื่อนไขของระบบ

ดังนั้น การกำหนด Device Limit 2 ไม่ได้มีความหมายเดียวกับการอนุญาตให้แชร์บัญชีสองคนใช้งานพร้อมกัน

3. จุดประสงค์ของ One Session Security

ระบบนี้เหมาะกับเว็บไซต์การเรียนออนไลน์ เพราะ Account ของนักเรียนมักมีสิทธิ์เข้าถึงเนื้อหาที่มีมูลค่า เช่น

- Video Course
- Live Class
- Zoom
- Replay
- เอกสารประกอบการเรียน
- Student Dashboard

หากไม่มีการควบคุม Session นักเรียนอาจส่ง Username และ Password ให้บุคคลอื่นนำไปใช้งานร่วมกันได้ง่ายขึ้น

One Session Security จึงเป็นมาตรการอีกขั้นหนึ่งสำหรับช่วยลดพฤติกรรมดังกล่าว

4. หลักการทำงานของ Active Session

เมื่อผู้เรียนเข้าสู่ระบบ เว็บไซต์จะสร้าง **Session** เพื่อยืนยันว่าผู้ใช้งานคนนั้น Login สำเร็จแล้ว

ตัวอย่าง:

Student1



Login



Username + Password ถูกต้อง



สร้าง Active Session



เข้าสู่ Student Dashboard

ระหว่างที่ Session ยังใช้งานได้ ผู้เรียนไม่จำเป็นต้องกรอก Username และ Password ใหม่ทุกครั้งที่เปิดหน้า Course

One Session Security จะเข้ามาช่วยตรวจสอบ Session เหล่านี้ตามกฎหมายที่ระบบกำหนด

5. กรณีนักเรียนเข้าสู่ระบบจากอีกอุปกรณ์

ตัวอย่าง นักเรียน Student1 กำลังใช้งานอยู่บน

Windows PC A — Google Chrome

จากนั้นมีการนำบัญชีเดียวกันไป Login บนอุปกรณ์อีกเครื่อง เช่น

Windows PC B — Google Chrome

ระบบ One Session Security จะใช้ข้อมูล Session เพื่อควบคุมการใช้งานตามนโยบายของเว็บไซต์

แนวคิดคือ ไม่ควรพิจารณาเพียงว่าอุปกรณ์ทั้งสองเครื่องเป็น **Registered Devices** หรือไม่ แต่ต้องตรวจสอบด้วยว่า
มี Active Session ของบัญชีเดียวกันอยู่หรือไม่

จึงช่วยลดกรณี:

Student1 Account

คน A → เรียน Biology

คน B → เรียน Math

คน C → เปิด Live Class

พร้อมกันด้วย Username เดียวกัน

6. One Session Security ทำงานร่วมกับ Device Access Manager

ในระบบ AcademyWebs สามารถมองการรักษาความปลอดภัยเป็นหลายชั้นได้

Username / Password



Device Access Manager

ตรวจสอบว่าอุปกรณ์ได้รับอนุญาตหรือไม่



One Session Security

ตรวจ Active Session



Student Access

ตรวจว่านักเรียนมีสิทธิ์ Course หรือไม่



เข้าเรียน

ดังนั้นแต่ละระบบมีหน้าที่ของตัวเอง

Device Access ป้องกันการใช้อุปกรณ์เกินจำนวนที่กำหนด

One Session Security ช่วยควบคุมการใช้งาน Session ของบัญชี

Student Access ตรวจสอบสิทธิ์ว่า User สามารถเข้า Course หรือ Live Class ได้

Content Protection ช่วยลดการ Copy, Print, Capture หรือการนำเนื้อหาออกไป

การใช้ทั้งระบบร่วมกันจะมีประสิทธิภาพมากกว่าการใช้เพียงฟังก์ชันใดฟังก์ชันหนึ่ง

7. ความสัมพันธ์กับการเปลี่ยน Password

จากระบบ Device Access Manager ที่ติดตั้งอยู่ มีข้อความเกี่ยวกับ **Active Session** และการเปลี่ยน Password ซึ่งเป็นจุดที่ควรอธิบายในคู่มือด้วย

ในกรณีที่ **Administrator** สงสัยว่าบัญชีถูกแฮกหรือถูกบุคคลอื่นนำไปใช้งาน การปลด Device อย่างเดียวอาจไม่ใช่การจัดการ Session ที่กำลังเปิดอยู่ทั้งหมดทันที

แนวทางที่ควรพิจารณาคือ

Reset Device + จัดการ Active Session + เปลี่ยน Password

โดยเฉพาะกรณีที่เจ้าของบัญชีไม่ทราบว่าใครมี Password อยู่

ตัวอย่าง:

สงสัยว่าบัญชีถูกแฮก



ตรวจ Device Access



Remove / Reset Devices



ยุติ Session ตามระบบ



เปลี่ยน Password



ให้นักเรียน Login ใหม่

8. ตัวอย่างสถานการณ์ใช้งาน

สมมติ Student1 ได้รับสิทธิ์ให้ใช้งานสูงสุด 2 อุปกรณ์

Device Limit = 2

และมี Registered Devices:

Device 1

Windows PC — Google Chrome

Device 2

Windows PC — Microsoft Edge

นี่เป็นสถานะที่ถูกต้องในมุมมองของ Device Access

แต่ One Session Security จะพิจารณาเพิ่มเติมเรื่อง **Session** ปัจจุบันของบัญชี

จึงสามารถอนุญาตให้นักเรียนมีอุปกรณ์ประจำได้หลายเครื่องตามนโยบาย แต่ยังคงควบคุมการใช้งานบัญชีพร้อมกัน เพื่อช่วยป้องกัน Account Sharing ได้

9. กรณีนักเรียนเปลี่ยนเครื่อง

หากนักเรียนซื้อ Notebook ใหม่ แต่มี Registered Devices ครบ Limit แล้ว ให้ Administrator เข้า

Device Access Manager

ค้นหานักเรียน จากนั้นตรวจสอบเครื่องเก่าแล้วใช้

Unlock / Remove Device

เมื่อมีพื้นที่ว่าง นักเรียนจึงสามารถลงทะเบียนเครื่องใหม่ได้

ส่วน One Session Security จะยังทำหน้าที่ควบคุม Session ตามปกติ

จึงไม่จำเป็นต้องปิด One Session Security เพียงเพราะนักเรียนเปลี่ยนอุปกรณ์

10. กรณีนักเรียนเปลี่ยน Browser

ควรทราบว่า Browser อาจถูกระบบมองเป็นรายละเอียดหนึ่งของ Device/Session

ตัวอย่าง เครื่องเดียวกันอาจมี

Windows PC — Chrome

และ

Windows PC — Edge

ดังที่ปรากฏในหน้า Device Access Manager

ดังนั้น หากนักเรียนแจ้งว่า “ใช้คอมพิวเตอร์เดิมแต่เปลี่ยน Browser แล้วเข้าไม่ได้” Administrator ควรตรวจสอบทั้ง

Registered Devices

และ

Active Session

ก่อนสรุปว่าบัญชีมีปัญหา

11. กรณีนักเรียนลืม Logout

อีกสถานการณ์หนึ่งที่พบได้คือ นักเรียน Login ไว้บนอุปกรณ์หนึ่งแล้วไม่ได้ Logout จากนั้นไป Login จากอีกเครื่อง

หาก One Session Security ตรวจพบ Session เดิม ระบบจะจัดการตามกฎ Session ที่ติดตั้งไว้ในเว็บไซต์

ในเชิงการใช้งาน ผู้ดูแลระบบควรแนะนำให้นักเรียน

Logout เมื่อเลิกใช้งานเครื่องสาธารณะหรือเครื่องที่ไม่ใช่ของตนเอง

เพื่อช่วยลดปัญหา Session ค้างและลดความเสี่ยงที่ผู้อื่นจะเข้าถึง Course ด้วยบัญชีของนักเรียน

12. ข้อดีของ One Session Security

One Session Security ช่วยเพิ่มการควบคุมบัญชีผู้เรียน โดยเฉพาะเว็บไซต์ที่จำหน่าย Course แบบรายบุคคล

ประโยชน์หลักคือช่วยลดโอกาสของ

การแชร์ Username / Password, การใช้งานบัญชีเดียวกันพร้อมกันหลายคน และการนำบัญชีไปแจกให้ผู้อื่นเข้าเรียน

เมื่อใช้ร่วมกับ Device Access Manager จะสามารถควบคุมได้ทั้งระดับ อุปกรณ์ และ Session

13. ข้อจำกัดของ One Session Security

One Session Security เป็นมาตรการช่วยลด Account Sharing แต่ไม่ควรมองว่าเป็นระบบที่สามารถป้องกันการแชร์บัญชีได้ 100%

ตัวอย่างเช่น เจ้าของบัญชียังสามารถให้ผู้อื่นใช้อุปกรณ์เครื่องเดียวกัน หรือให้ผู้อื่นควบคุมเครื่องผ่านวิธีอื่นได้

ดังนั้นระบบที่เหมาะสมควรใช้หลายมาตรการร่วมกัน เช่น

One Session Security + Device Access + Student Access + Content Protection + Activity Log

เพื่อเพิ่มระดับการควบคุมโดยรวม

14. แนวทางสำหรับ Administrator

เมื่อมีนักเรียนแจ้งปัญหาเกี่ยวกับการ Login หรือ Device ไม่ควร Reset ทุกอย่างทันที

ควรตรวจสอบตามลำดับ:

ตรวจสอบ Student → ตรวจ Registered Devices → ตรวจ Device Limit → ตรวจ Session → ตรวจ สิทธิ Student Access → จึงดำเนินการ Reset/Remove ตามความจำเป็น

วิธีนี้ช่วยลดโอกาสการเกิดจุด และยังช่วยให้ Administrator แยกได้ว่าปัญหาเกิดจาก

Device Limit, Session Security, Password หรือ Course Access

กรณี นักเรียนลืม Password

กรณี นักเรียนลืม Password แนะนำให้แยกเป็น 2 สถานการณ์ครับ เพราะจะเกี่ยวกับการ Login และระบบ One Session / Device Access

ถ้านักเรียน ยังจำอีเมลที่ใช้สมัครได้ ให้ใช้เมนู **Lost your password?** / ลืมรหัสผ่าน ที่หน้า Login แล้วกรอก Username หรือ Email จากนั้นระบบจะส่งลิงก์สำหรับตั้ง Password ใหม่ไปยังอีเมลของนักเรียน เมื่อเปลี่ยน Password สำเร็จแล้ว ให้กลับมา Login ใหม่อีกครั้ง

ถ้านักเรียน เข้าอีเมลไม่ได้ หรือ **Reset** เองไม่ได้ ให้ Administrator เข้าไปที่ WordPress Admin แล้วไปที่ **Users → All Users → เลือกนักเรียน → Edit** จากนั้นเลื่อนลงไปในส่วน **Account Management** แล้วใช้ **Set New Password** เพื่อ กำหนด Password ใหม่ให้กับนักเรียน จากนั้นแจ้ง Password ใหม่ให้ผู้เรียน และแนะนำให้ผู้เรียนเปลี่ยนเป็นรหัสของตนเองภายหลัง

สำหรับระบบ **One Session Security** ถ้าหลังเปลี่ยน Password แล้วนักเรียนยังมีปัญหาเข้าไม่ได้ เพราะมี Session เก่าค้างอยู่ ผม แนะนำให้ตรวจสอบ **Device Access Manager** ร่วมด้วย โดยดู Registered Devices และ Active Session ของบัญชีนั้น ถ้าจำเป็นค่อยใช้ **Reset All Devices** หรือปลดอุปกรณ์เก่าออก แล้วให้นักเรียน Login ใหม่ด้วย Password ใหม่

ลำดับที่เหมาะสมที่สุดคือ:

ลืม Password → Reset Password → ตรวจ Session/Device ถ้ายังเข้าไม่ได้ → Login ใหม่