



คู่มือการเปิดใช้งาน Two Factor Authentication For Zimbra Collaboration

สารบัญ

ทำความเข้าใจกับ 2FA (Two Factor Authentication)	3
การรับรองความถูกต้องด้วยสองปัจจัยของ ZIMBRA EMAIL	3
ขั้นตอนการตั้งค่า 2FA (Two-Factor Authentication) สำหรับผู้ใช้งานครั้งแรกผ่าน Webmail	4
การตั้งค่า 2FA ด้วย Third-party authenticator app	6
การตั้งค่า 2FA ด้วย By email to password recovery address	9
การเข้าใช้งานหลังเปิด Two-factor authentication	10
การเพิ่มแอปพลิเคชันที่ไม่รองรับการทำงาน Token key หลังจากเปิดใช้งาน 2FA (App a passcode)	12
การใช้งาน ZIMBRA EMAIL สำหรับอุปกรณ์ที่ไม่รองรับ Token key หลังจากเปิดใช้งาน 2FA	14
สำหรับระบบปฏิบัติการ IOS	14
สำหรับระบบปฏิบัติการ Android	17
การใช้งาน One-Time Code	19

ทำความรู้จักกับ 2FA (Two Factor Authentication)

เป็นการรักษาความปลอดภัยอีกชั้นหนึ่งเรียกว่า "การตรวจสอบหลายปัจจัย" ในการระบุตัวตนของคุณ หลังจากล็อกอินด้วยรหัสผ่านตามปกติ จะมีการยืนยันผ่านด้วยแอป Authentication เพื่อป้อนรหัสให้ตรงกัน และยืนยันตัวตน โดยรหัส OTP จะเป็นรหัสผ่านที่ใช้งานได้เพียงครั้งเดียว และมีอายุการใช้งานสั้นมาก อาจจะไม่เพียงกี่วินาที อย่างมากที่สุดที่เห็นก็ 15 นาที หากไม่ใช่เจ้าของบัญชี ไม่มี OTP หรือป้อนรหัสไม่ถูกต้องก็ไม่สามารถล็อกอินได้

การรับรองความถูกต้องด้วยสองปัจจัยของ ZIMBRA EMAIL

ZIMBRA EMAIL 2FA ช่วยป้องกันความปลอดภัยอีกชั้นหนึ่ง นอกเหนือจากรหัสผ่าน ตัวอย่างเช่น, หากไม่มี 2FA ผู้ใช้จะเข้าสู่ระบบบัญชี ZIMBRA EMAIL ด้วยชื่อผู้ใช้และรหัสผ่านอย่างเดียว วิธีนี้เสี่ยงต่อการแฮ็ก การหลอกลวงแบบฟิชชิ่งและภัยคุกคามด้านความปลอดภัยอื่นๆ ด้วย 2FA ผู้ใช้เข้าสู่ระบบด้วยรหัสผ่านและรหัสเฉพาะมีเฉพาะในสมาร์ทโฟนเท่านั้น การรักษาความปลอดภัยทำให้บัญชีถูกบุกรุกได้ยากขึ้นมากด้วย

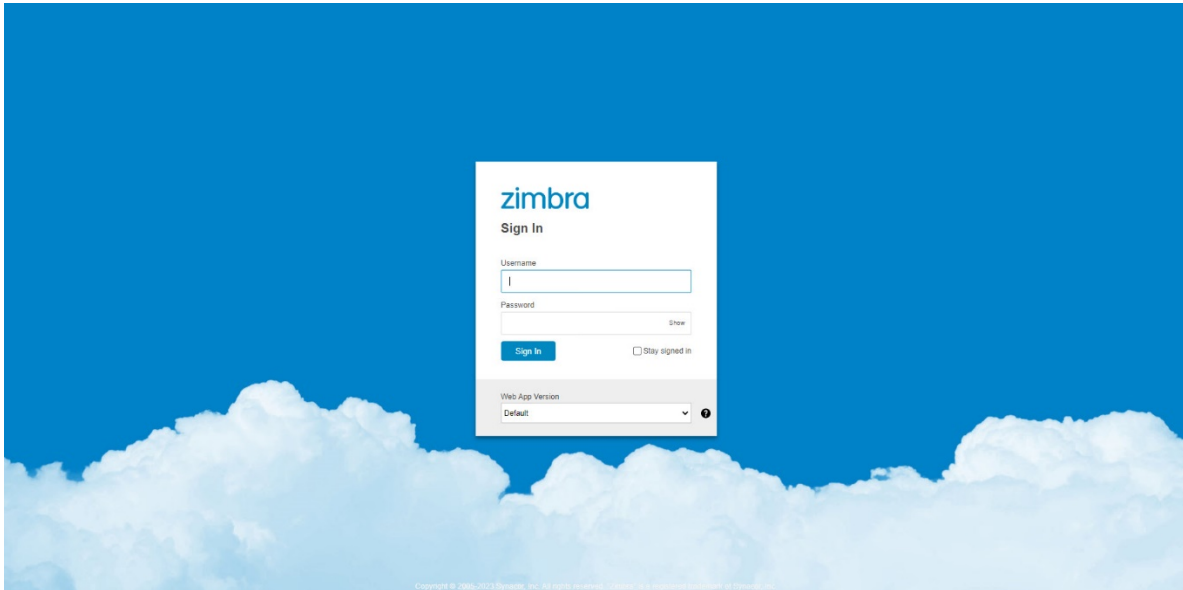
สิ่งสำคัญสำหรับการใช้งานการเข้าสู่ระบบ ZIMBRA EMAIL คือ

- ชื่อผู้ใช้งาน และ รหัสผ่าน
- อุปกรณ์สมาร์ทโฟน เช่น อุปกรณ์โทรศัพท์มือถือ อุปกรณ์แท็บเล็ต เป็นต้น

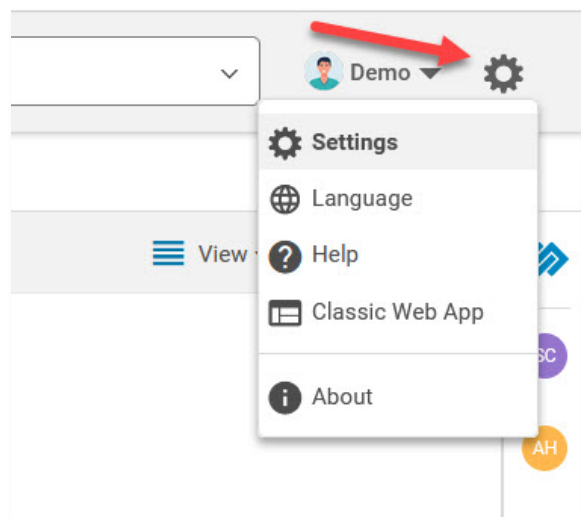


ขั้นตอนการตั้งค่า 2FA (Two-Factor Authentication) สำหรับผู้ใช้งานครั้งแรกผ่าน Webmail

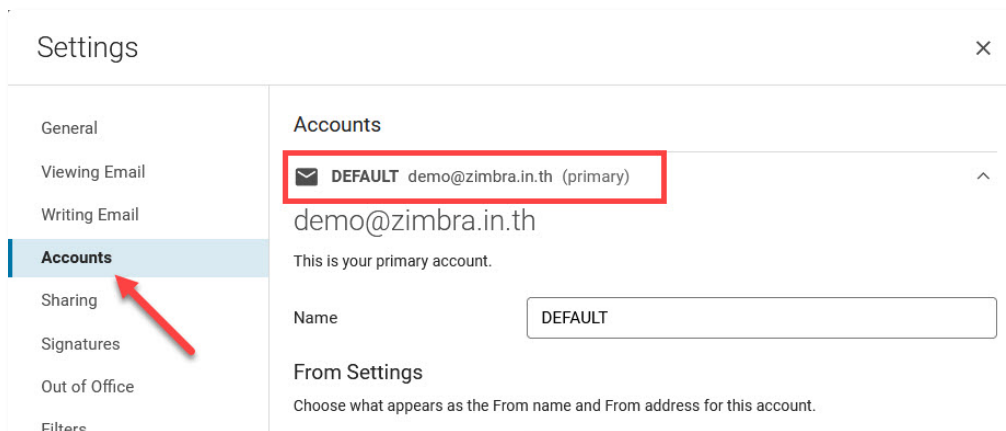
1. Login เข้าใช้งานระบบ ZIMBRA EMAIL ที่ URL ของท่าน



2. เมื่อเข้าสู่ระบบแล้วไปที่รูป “ฟันเฟือง ⚙” จากนั้นไปที่เมนู การตั้งค่า (Setting)



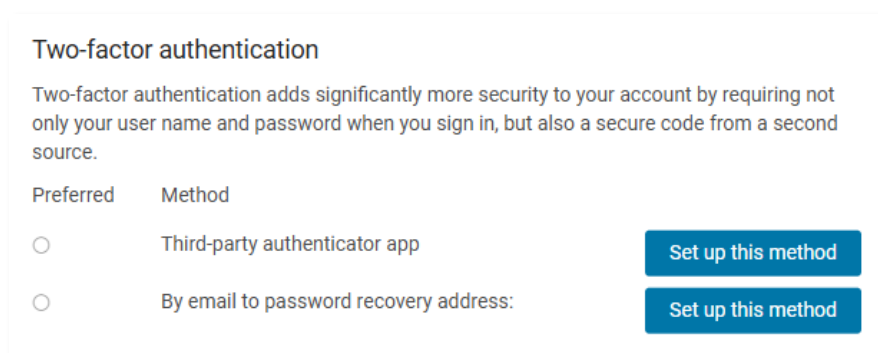
3. ไปที่แถบ บัญชี (Accounts) จากนั้นคลิกที่ ชื่อบัญชีของท่าน



4. ไปที่แถบ การรับรองความถูกต้องด้วยสองปัจจัย (Two-factor authentication)

คุณสามารถเลือกการตั้งค่าได้ 2 แบบ

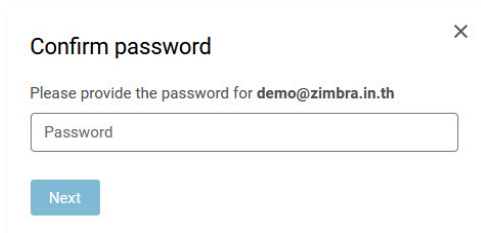
- Third-party authenticator app (สำหรับผู้ใช้งานที่ต้องการใช้งาน 2 FA authenticator app)
- By email to password recovery address (สำหรับผู้ใช้งานที่ต้องการใช้งานอีเมลส่วนตัว)



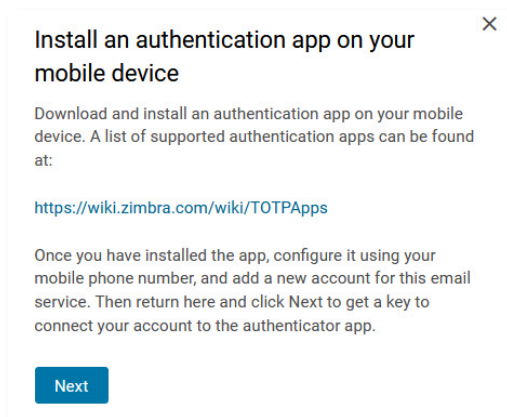
คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

การตั้งค่า 2FA ด้วย Third-party authenticator app

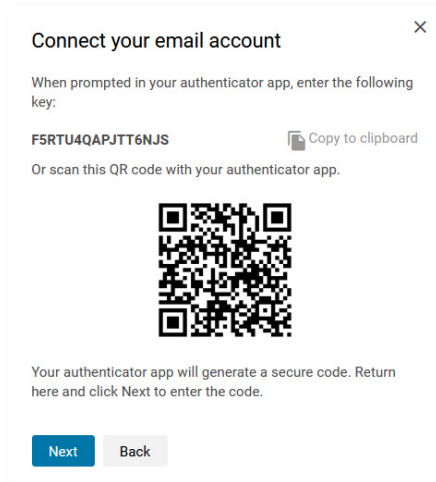
1. หลังจากที่คุณเลือกการตั้งค่าด้วย แอปตรวจสอบสิทธิ์บุคคลที่สาม (Third-party authenticator app) ระบบจะให้ป้อนรหัสผ่าน จากนั้นคลิกปุ่ม ถัดไป (Next)



2. ระบบจะขึ้นข้อความแนะนำแอปพลิเคชันที่รับรองความถูกต้อง เราแนะนำ “Google authenticator” จากนั้นคลิก ถัดไป (Next)



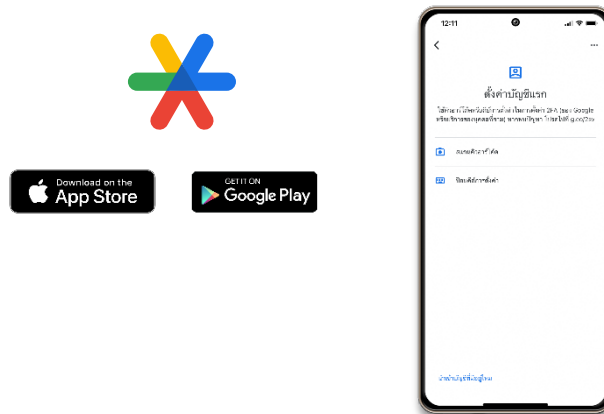
3. ระบบจะสร้างคีย์และ QR Code นำคีย์ที่ได้รับไปป้อนในแอปพลิเคชัน “Google authenticator” หรือนำโทรศัพท์ที่ติดตั้งแอปพลิเคชันแล้วมาสแกน จากนั้นคลิก ถัดไป (Next)



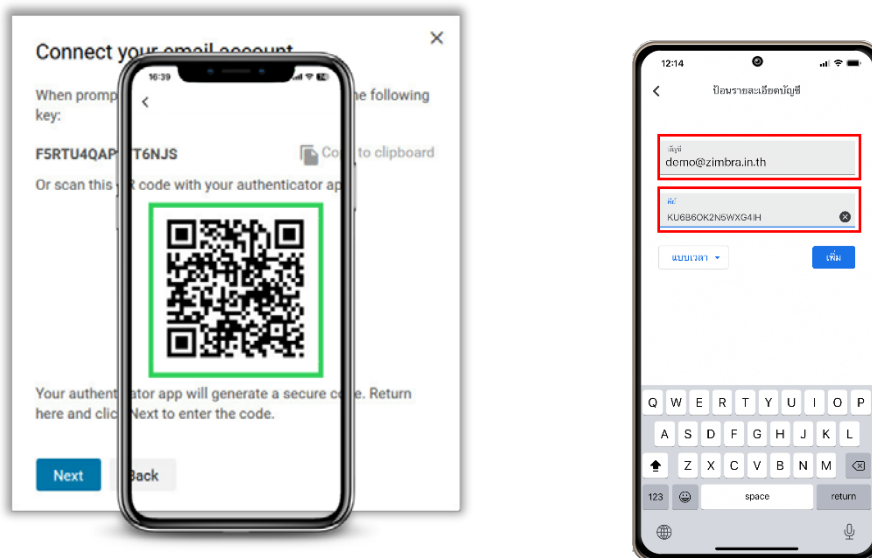
* กรณีที่มีการใช้บัญชีอีเมลร่วมกัน และต้องการเปิดใช้แอปพลิเคชัน “Google authenticator” พร้อมกับฟังก์ชัน 2FA ของ Zimbra บนอุปกรณ์โทรศัพท์มือถือหลายเครื่อง ให้คุณบันทึกการรหัสผ่านชุดนี้ไว้ (Capture หน้าจอ เก็บไว้) และนำ Key ไปป้อนในแอปพลิเคชัน “Google authenticator” บนอุปกรณ์ใหม่เพื่อยืนยันการเชื่อมต่อบัญชีอีเมล คุณก็จะสามารถเชื่อมบัญชีอีเมลของคุณได้กับหลายอุปกรณ์

คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

- ติดตั้งแอปพลิเคชัน“Google authenticator” นำคีย์ที่ได้รับไปป้อนในแอปพลิเคชัน“Google authenticator” หรือนำโทรศัพท์ที่ติดตั้งแอปพลิเคชันแล้วมาสแกน

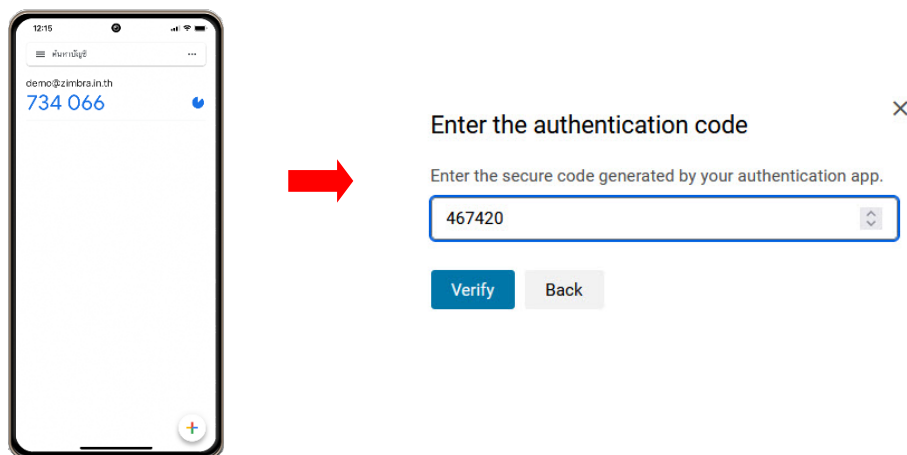


- นำมือถือมาสแกน QR Code หรือเพิ่มคีย์ (จากข้อ 7)



คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

6. (จากข้อ 5) ให้คลิกปุ่ม **ถัดไป (Next)** ระบบจะแสดงหน้าใส่รหัสเพื่อยืนยันการตั้งค่า ให้นำรหัสตัวเลข 6 ตัวที่ได้รับจากแอปพลิเคชัน “Google authenticator” มากรอกในระบบ ZIMBRA EMAIL จากนั้นคลิกปุ่ม **ถัดไป (Next)**



7. คลิกปุ่ม **ถัดไป (Next)** เพื่อสิ้นสุดการตั้งค่าการรับรองความถูกต้องแบบสองขั้นตอนสำเร็จ (Two-Factor Authentication)

Two-factor authentication

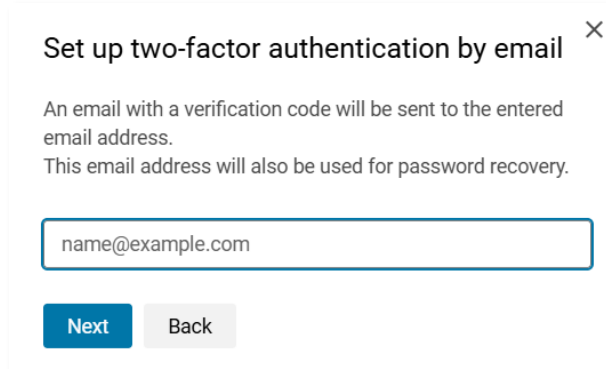
Two-factor authentication adds significantly more security to your account by requiring not only your user name and password when you sign in, but also a secure code from a second source.

Preferred	Method	
☒	Third-party authenticator app	<button>Remove this method</button>
☐	By email to password recovery address:	<button>Set up this method</button>

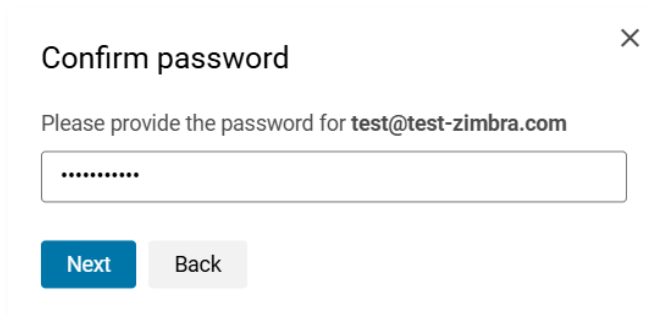
คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

การตั้งค่า 2FA ด้วย By email to password recovery address

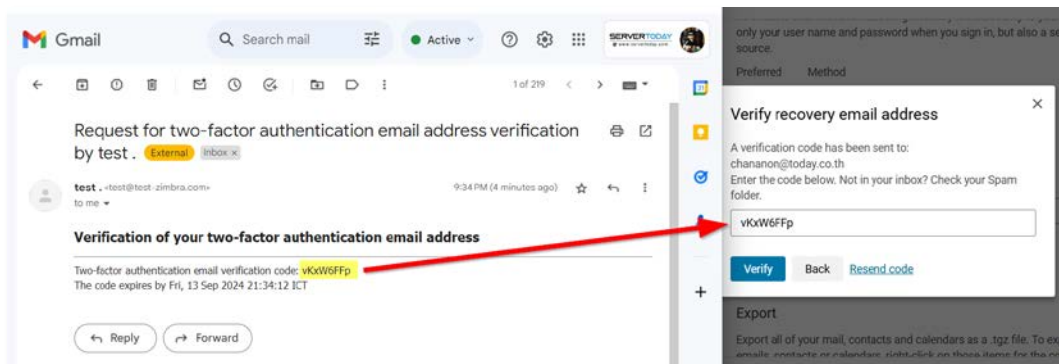
1. หลังจากที่ได้เลือกการตั้งค่า ทางอีเมลไปยังที่อยู่การกู้คืนรหัสผ่าน (By email to password recovery address) ระบบจะให้ลงทะเบียนด้วย อีเมลส่วนตัว จากนั้นคลิก ถัดไป (Next)



2. ระบบจะคุณป้อนรหัสผ่านของอีเมล Zimbra เพื่อยืนยันตัวตน จากนั้นคลิก ถัดไป (Next)

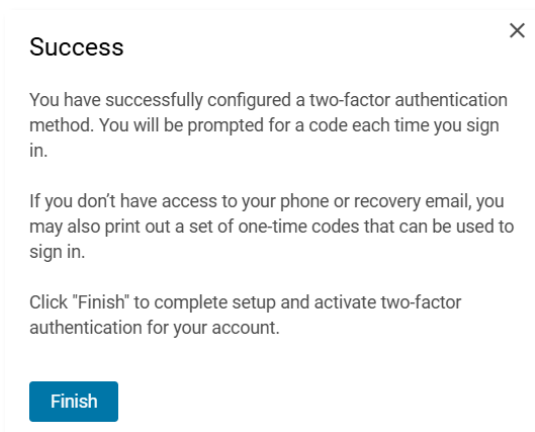


3. ตรวจสอบอีเมลใน Inbox ของอีเมลส่วนตัว(อีเมลที่ลงทะเบียนไว้ในข้อ 1) ค้นหาอีเมล Subject: **ขอการยืนยันที่อยู่อีเมลสำหรับการตรวจสอบสิทธิ์แบบสองปัจจัย (Request for two-factor authentication email address verification)** และนำ verification code จากอีเมลส่วนตัวมา ยืนยันตัวตนบนระบบ Email Zimbra อีกครั้ง จากนั้นคลิก **ตรวจสอบ (Verify)**



คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

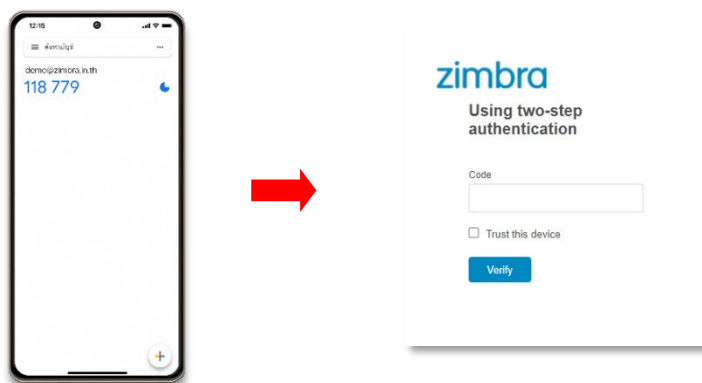
4. คลิก **เสร็จสิ้น (Finish)** เสร็จสิ้นการตั้งค่าการรับรองความถูกต้องแบบสองขั้นตอนสำเร็จ (Two-Factor Authentication)



การเข้าใช้งานหลังเปิด Two-factor authentication

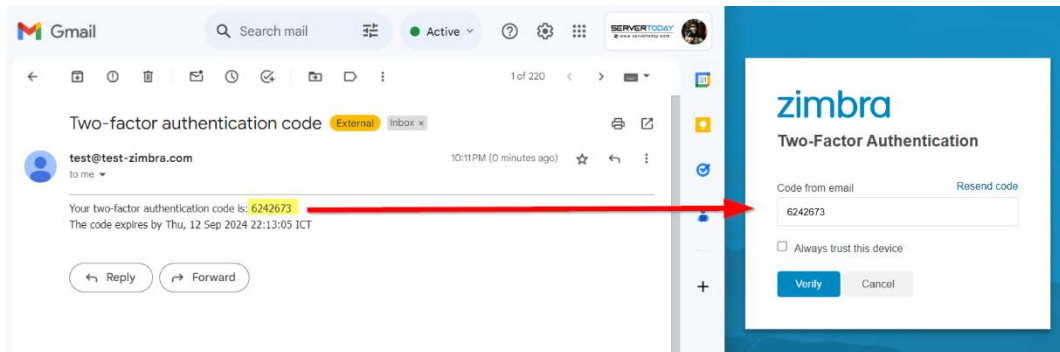
เมื่อ Login เข้าสู่ระบบ ZIMBRA EMAIL ครั้งถัดไป หลังจากการกรอกชื่อผู้ใช้งานและรหัสผ่าน จะพบหน้าต่างให้กรอกรหัส Token key

หากท่านเปิดใช้งานด้วย **Third-party authenticator app** ให้แอปพลิเคชัน Google authenticator บนมือถือระบบจะแสดงหรือ จากอีเมลส่วนตัวที่ลงทะเบียนไว้ ให้นำรหัสตัวเลข Token key 6 ตัว นำไปป้อนที่ระบบ ZIMBRA EMAIL ซึ่งรหัส Token key จะเปลี่ยนทุกๆ 30 วินาที



คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

หากท่านเปิดใช้งานด้วย **By email to password recovery address** ให้ตรวจสอบที่อีเมลส่วนตัวที่ลงทะเบียนไว้ ค้นหาอีเมล Subject: **Two-factor authentication code**ให้นำรหัสตัวเลข Token key 6 ตัว นำไปป้อนที่ระบบ ZIMBRA EMAIL ซึ่งรหัส Token key จะมีอายุ 3 นาที



ท่านสามารถกำหนด Primary methods ที่ใช้งานอยู่เป็นประจำเพื่อให้ใช้งานได้ง่ายขึ้น

- Third-party authenticator app (สำหรับผู้ที่ต้องการใช้งาน 2 FA authenticator app)

zimbra
Two-Factor Authentication

Code from authenticator app

☐ Always trust this device

Use other method

Two-factor authentication

Two-factor authentication adds significantly more security to your account by requiring not only your user name and password when you sign in, but also a secure code from a second source.

Preferred	Method	
☒	Third-party authenticator app	Remove this method
☐	By email to password recovery address: chananon@today.co.th	Remove this method

One-time codes 10 unused codes

- By email to password recovery address (สำหรับผู้ที่ต้องการใช้งานอีเมลส่วนตัว)

zimbra
Two-Factor Authentication

Code from email

☐ Always trust this device

Use other method

Two-factor authentication

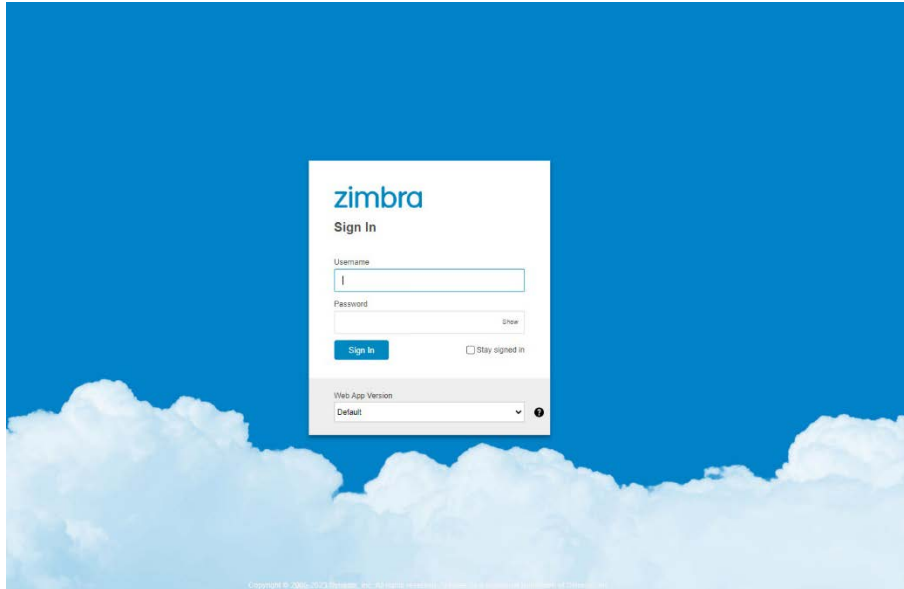
Two-factor authentication adds significantly more security to your account by requiring not only your user name and password when you sign in, but also a secure code from a second source.

Preferred	Method	
☐	Third-party authenticator app	Remove this method
☒	By email to password recovery address: chananon@today.co.th	Remove this method

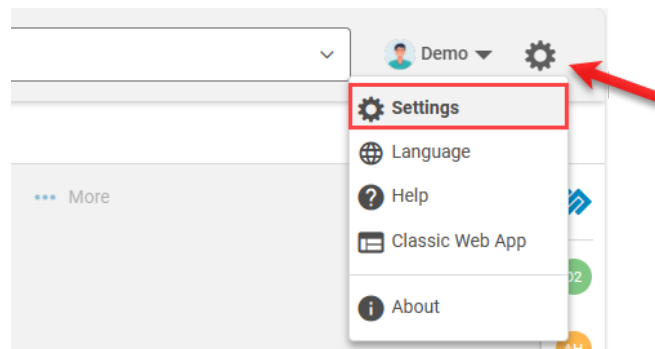
One-time codes 10 unused codes

การเพิ่มแอปพลิเคชันที่ไม่รองรับการทำงาน Token key หลังจากเปิดใช้งาน 2FA (App a passcode)

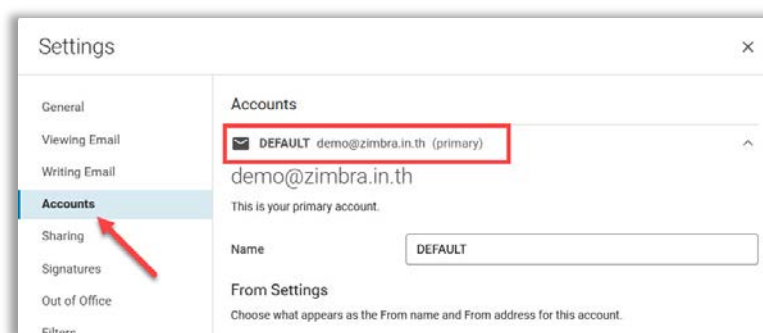
1. Login เข้าใช้งานระบบ ZIMBRA EMAIL ที่ URL ของท่าน



2. เมื่อเข้าสู่ระบบแล้วไปที่รูป “ฟันเฟือง ⚙” จากนั้นไปที่เมนู “Setting”

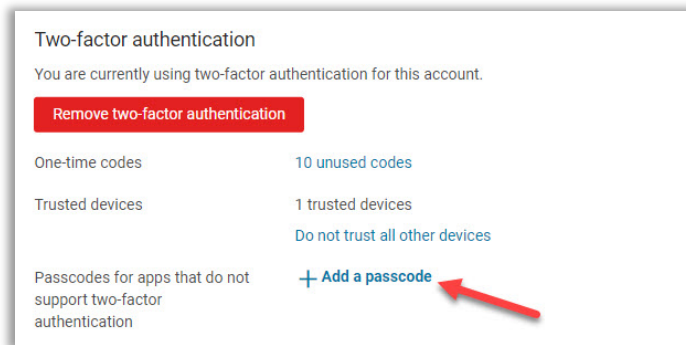


3. ไปที่แถบ “Accounts” จากนั้นคลิกที่ ชื่อบัญชีของท่าน

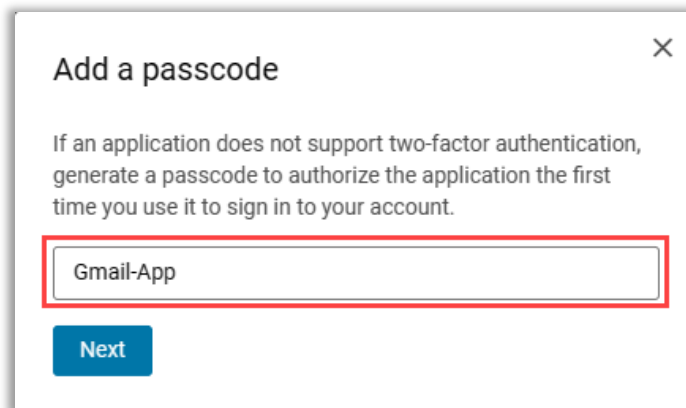


คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

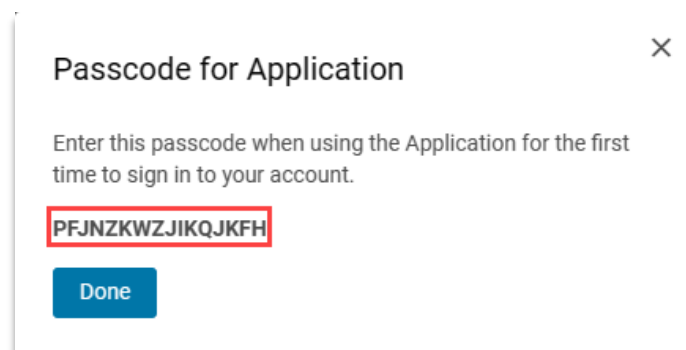
4. ไปที่แถบ “Two-factor authentication” จากนั้นคลิกที่ “Add a passcode”



5. ตั้งชื่อแอปพลิเคชันของท่านแล้วคลิก ถัดไป



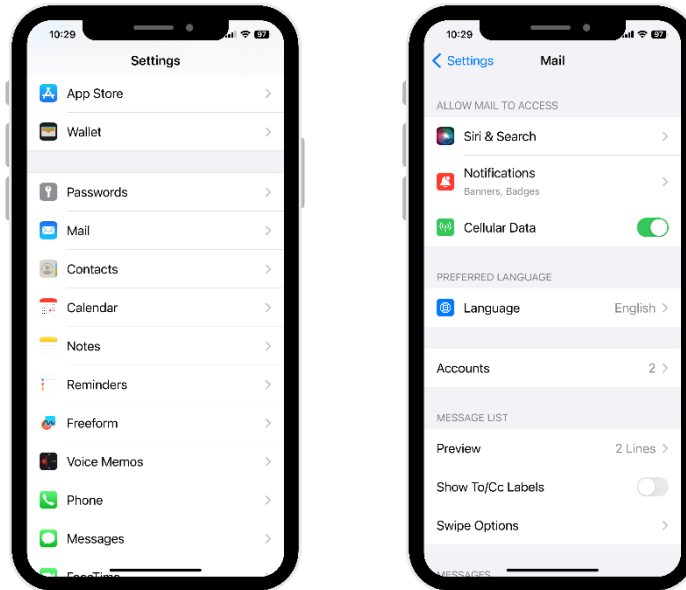
6. ระบบจะสุ่มรหัสผ่านสำหรับแอปพลิเคชันของท่าน (รหัสต่อ 1 แอปพลิเคชัน)



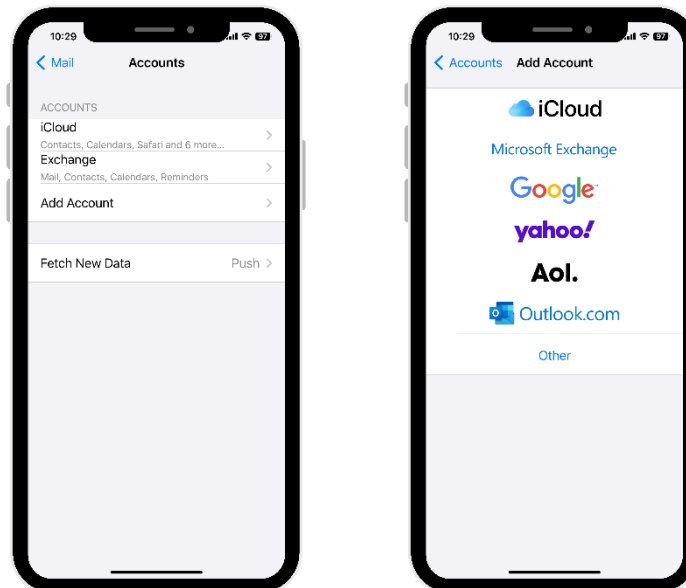
คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

การใช้งาน ZIMBRA EMAIL สำหรับอุปกรณ์ที่ไม่รองรับ Token key หลังจากเปิดใช้งาน 2FA สำหรับระบบปฏิบัติการ IOS

1. ไปที่การ ตั้งค่า  → ที่เมนู เมล → ไปที่ Account

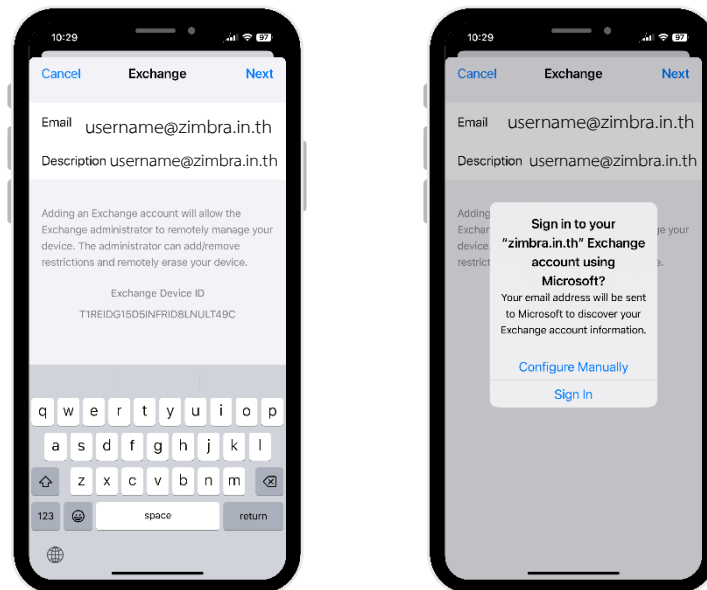


2. เลือก Add Account → เลือกการตั้งค่าแบบ Microsoft Exchange



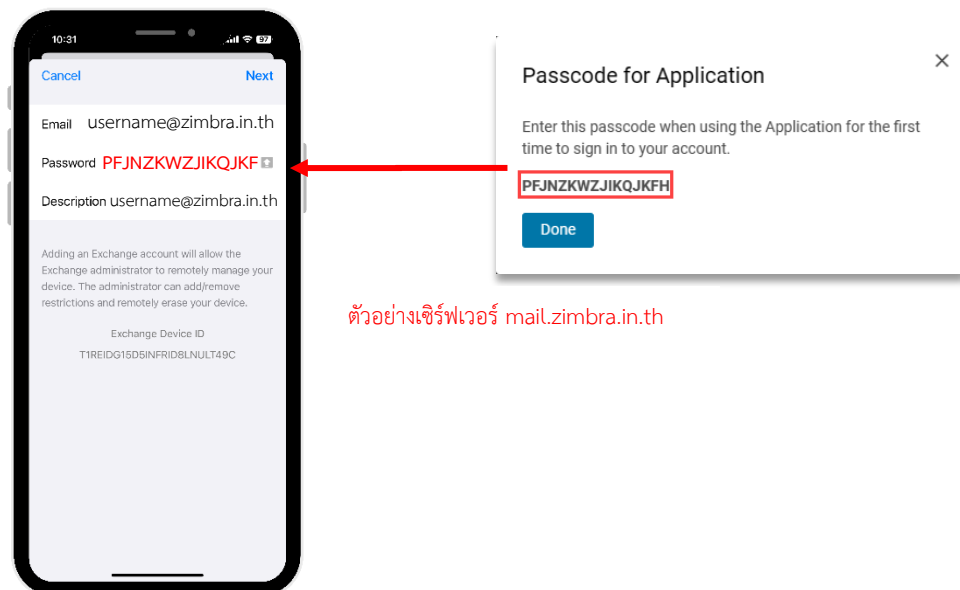
คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

3. ป้อนอีเมลที่ต้องการตั้งค่า → กำหนดการตั้งค่าด้วยตัวอย่าง “Configure Manually”



ตัวอย่างเซิร์ฟเวอร์ mail.zimbra.in.th

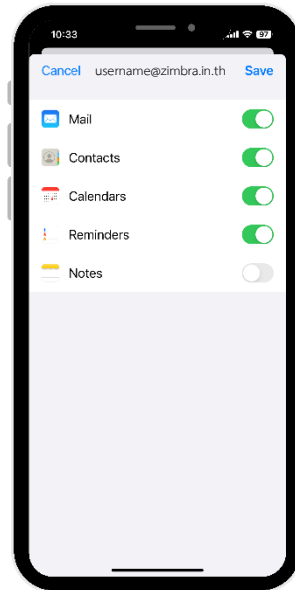
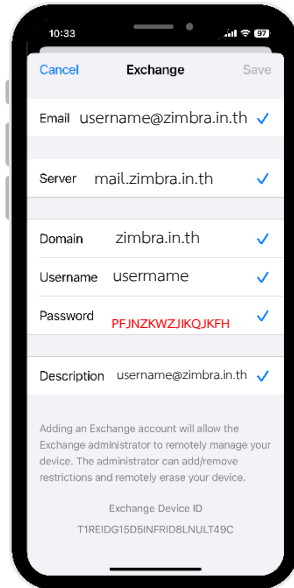
4. นำ Passcode จากเว็บเมล Zimbra มาใช้แทนรหัสผ่านเดิม



ตัวอย่างเซิร์ฟเวอร์ mail.zimbra.in.th

5. “ป้อนค่าเซิร์ฟเวอร์” และ “ชื่อผู้ใช้งาน” จากนั้นเลือก “Save”

ตัวอย่างเซิร์ฟเวอร์ mail.zimbra.in.th

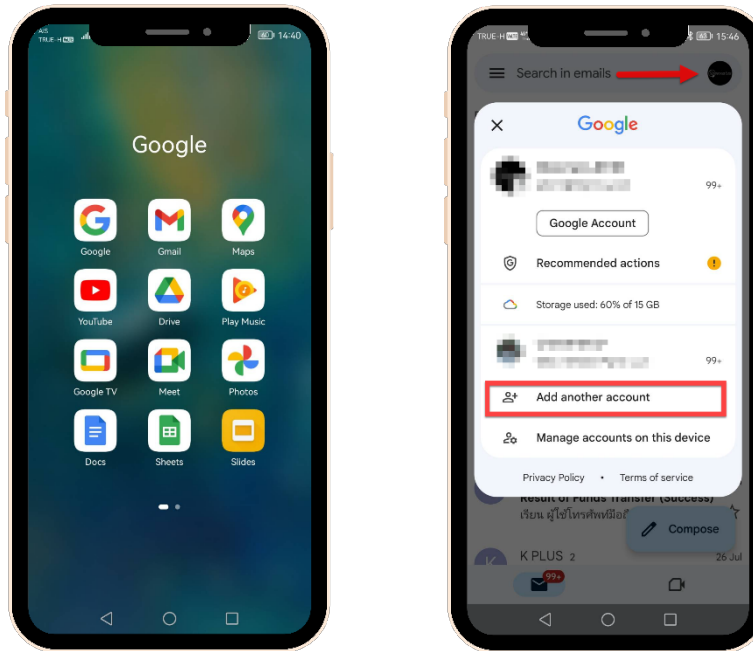


คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

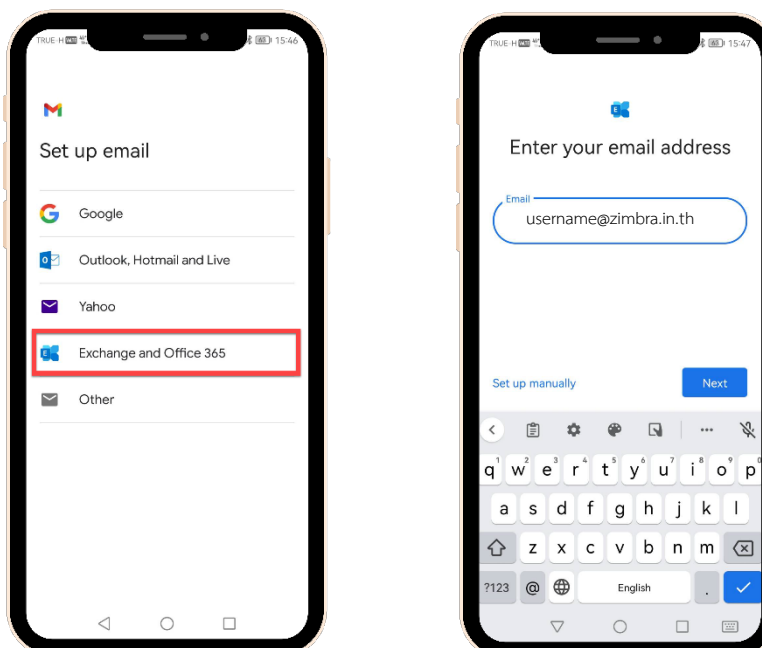
สำหรับระบบปฏิบัติการ Android

สำหรับ Gmail App

1. ไปที่การ “App gmail”  ไปที่โปรไฟล์ (มุมบนขวา) เลือกเมนู Add another account

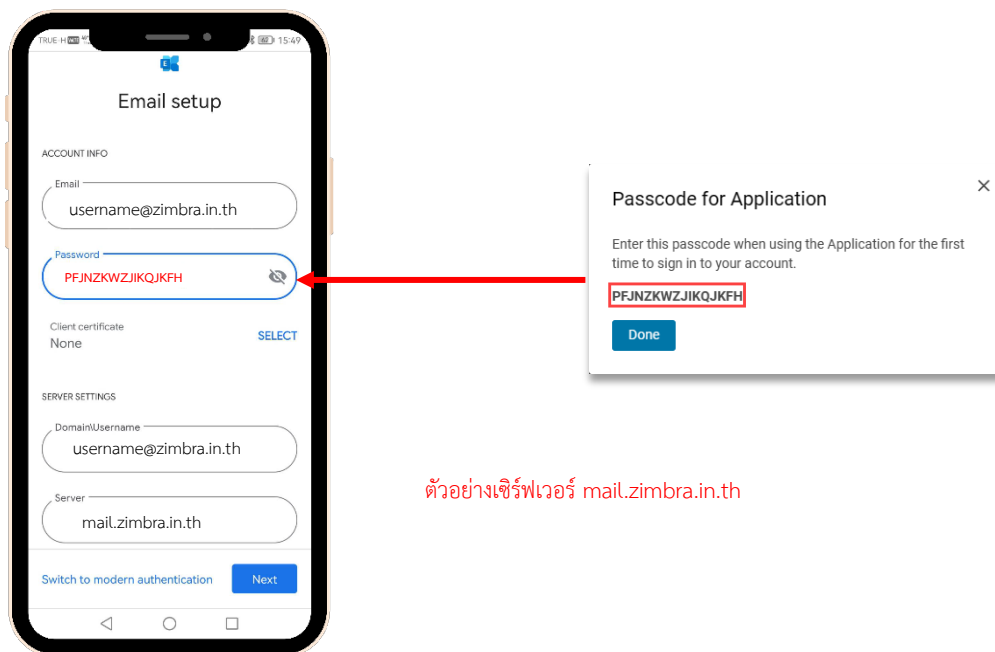


2. เลือกเมนู “Exchange และ Office 365” → ป้อนอีเมลของท่าน จากนั้นให้เลือกที่ Set up manually



คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

- นำ Passcode จากเว็บเมล Zimbra มาใช้แทนรหัสผ่านเดิม และ “ป้อนค่าเซิร์ฟเวอร์” จากนั้นเลือก Next



- เมื่อตั้งค่าเรียบร้อยแล้วระบบจะแสดงข้อความ “บัญชีของคุณพร้อมใช้งานแล้ว” เมื่อเสร็จสิ้นเลือก “เสร็จ”

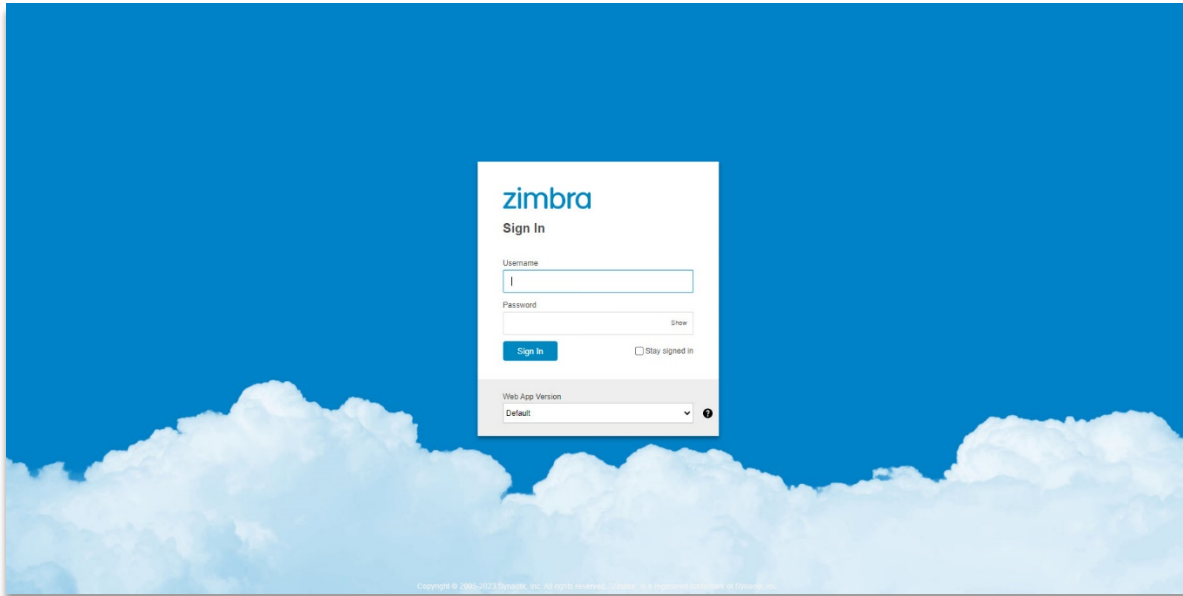


คู่มือการตั้งค่า 2FA (Two-Factor Authentication)

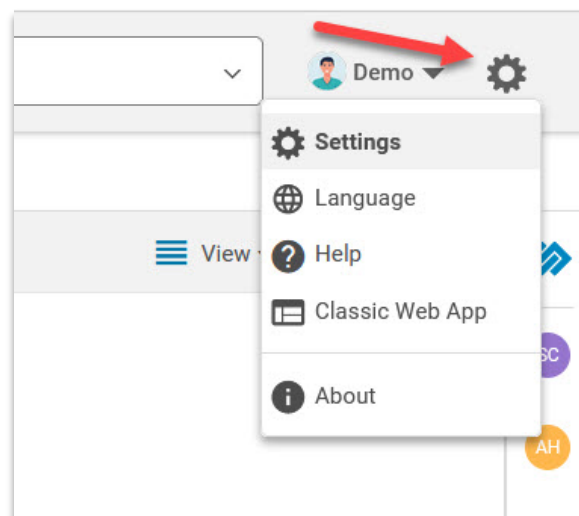
การใช้งาน One-Time Code

คือรหัสผ่านสำหรับใช้ทดแทนกรณีที่ไม่ได้ใช้รหัสจากแอปพลิเคชัน Authenticator สามารถใช้ One-Time Code หรือรหัสสำหรับการเข้าใช้งานได้ 1 ครั้ง ที่สร้างจากระบบ ZIMBRA EMAIL ได้ โดยมีการตั้งค่า ดังนี้

1. Login เข้าใช้งานระบบ ZIMBRA EMAIL ที่ URL ของท่าน

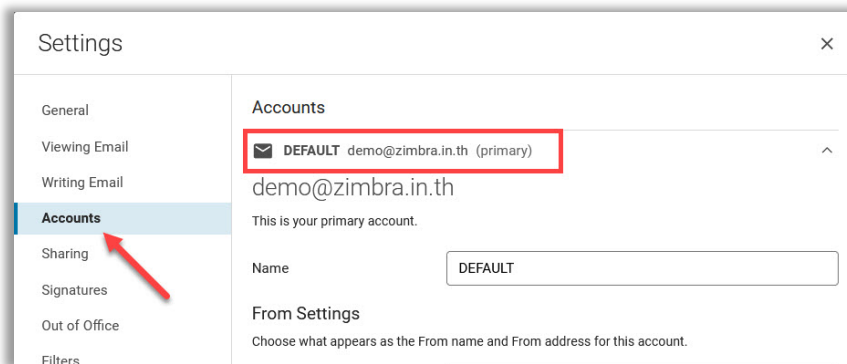


2. เมื่อเข้าสู่ระบบแล้วไปที่รูป “ฟันเฟือง ⚙” จากนั้นไปที่เมนู “Setting”

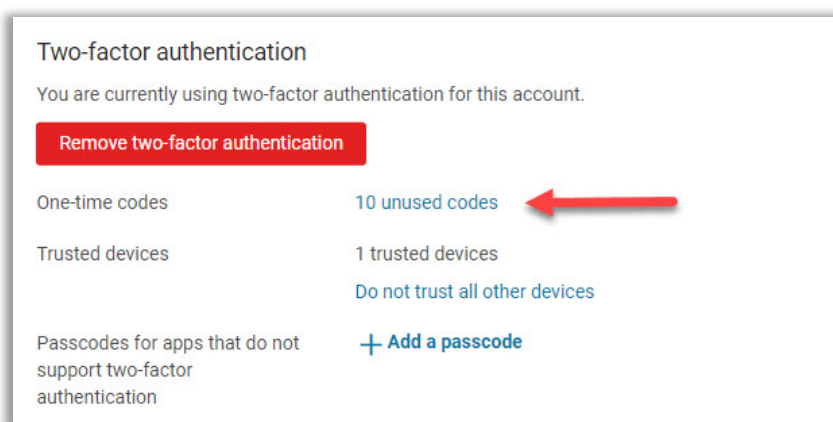


3. ไปที่แถบ “Accounts” จากนั้นคลิกที่ ชื่อบัญชีของท่าน

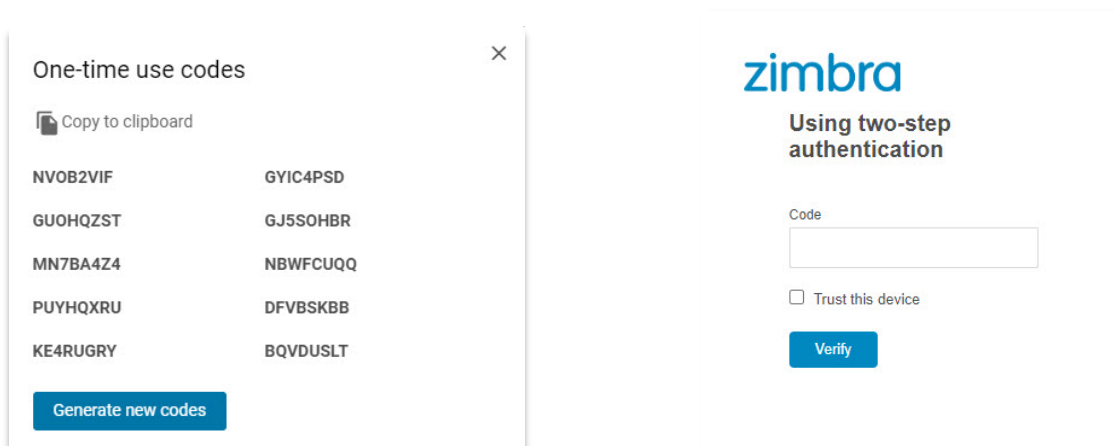
คู่มือการตั้งค่า 2FA (Two-Factor Authentication)



4. ไปที่แถบ “Two-factor authentication” จากนั้นคลิกที่ “10 Unused codes”



5. ระบบจะแสดงรหัสผ่านแบบใช้งานครั้งเดียว จำนวน 10 ชุด สามารถสั่งพิมพ์ออกมาเป็นกระดาษ หรือ บันทึกเป็นไฟล์ PDF เก็บไว้สำหรับใช้เป็น One-Time Code สำหรับเข้าใช้งานระบบครั้งถัดไป



6. เมื่อ Login เข้าสู่ระบบครั้งถัดไป หลังจากการกรอกชื่อผู้ใช้งานและรหัสผ่าน จะพบหน้าต่างให้กรอกรหัส One-Time Code ที่สร้างจากระบบ ให้นำรหัสจาก(ข้อ2)