## คู่มือการตั้งค่า Authentication LAN บน Windows 10

1.ไปที่ Search (รูปแว่นขยายด้านล่าง) หลังจากนั้น พิมพ์ Services แล้วเลือก



2. กด Start ที่ Service Wired AutoConfig จนขึ้น status Running (คลิกที่ Wired AutoConfig หมายเลข 1 จากนั้น กดที่ Start หมายเลข 2 )

	0,		Services				×	ſ
	File Action View	Help						1
:	🗢 🔿   💼   🖾	3 🛃 🛛 📷 🕨 🔲 II ID						
,	Services (Local)	Services (Local)						ĺ
		Wired AutoConfig	Name	Description	Status	Startup Type	Log ^	
		Start the service 2 Description: The Wired AutoConfig (DOT3SVC) service is responsible for performing	Windows Media Player Net Windows Modules Installer Windows Presentation Fou Windows Remote Manage	Shares Win Enables inst Optimizes p Windows R	inning Running	Manual (Trig Automatic Manual Manual Manual Manual	Loc Loc Net Loc Loc	
		IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to petwork	Windows Search Windows Store Service (WS Windows Time Windows Update	Provides co Provides inf Maintains d Enables the WinHTTP i	Running	Automatic (D Manual (Trig Manual (Trig Manual (Trig Manual	Loc Loc Loc Loc	
		resources. Wired networks that d	🖏 Wired AutoConfig	The Wired		Manual	Loc	
e a		not enforce 802.1X authentication a unaffected by the DOT3SVC service.	Wireless PAN DHCP Server WLAN AutoConfig WMI Performance Adapter Work Folders Workstation WWAN AutoConfig มริการ ช่าวอัพเดต Google (gu ปริการ ช่าวอัพเดต Google (gu	The WLANS Provides pe This service Creates and This service โปรดอัปเดตซ่ โปรดอัปเดตซ่	Running Running	Manual Automatic Manual Automatic Manual Automatic (D Manual	Loc Loc Loc Loc Loc Loc Loc Loc V	
1							_	

3.ไปที่หน้า Network and Sharing Center > คลิก Change adapter setting



#### 4.คลิกขวาที่ Ethernet



## 5.คลิกที่ Authentication tab

Configure	t Connection 1218-LM	Intel(R) Etnemet	<u>.</u>
Configure			
	he following items:	connection uses t	his co
^	osoft Networks	Client for Mich	
	je Protocol	VMware Bridg	
dea	JIS 6.3 Packet Filter Div	FortiClient ND	
IKS	Scheduler	BOoS Packet S	
ocol	work Adapter Multiplexo	<ul> <li>Microsoft Netv</li> </ul>	
¥	P Protocol Driver	- Microsoft LLD	<ul> <li></li></ul>
>			<
	Uninstall	Install	
Properties			
Properties	C	cription	Desc
Properties	er to access resources o	scription ows your compute twork.	-Desc Allov netw
>	Scheduler work Adapter Multiplexo )P Protocol Driver	<ul> <li>QoS Packet S</li> <li>Microsoft Network</li> <li>Microsoft LLD</li> <li>Install</li> </ul>	

6.Enable IEEE 802.1x authentication > คลิก Setting

	Ethernet 4 Properties	1
: ar	Networking Authentication Sharing	or
)ia	Select this option to provide authenticated network access for this Ethemet adapter.                 ■ Enable IEEE 802.1X authentication                  Choose a network authentication method:                 Microsoft: Protected EAP (PEAP)                 Remember my credentials for this connection each time I'm logged on                 Fall-back to unauthorised network access                 Additional Settings	ual apt
	OK Cancel	

# 7.ติ๊ก Verify ออก > คลิก Configure

When connecting:         Verify the server's identity by validating the certificate         Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):         Trusted Root Certification Authorities:         AddTrust External CA Root         Baltimore CyberTrust Root         Certum CA         Certum CA         Certum Trusted Network CA         Class 3 Public Primary Certification Authority         DigiCert Assured ID Root CA         <         Notifications before connecting:         Tell user if the server's identity cannot be verified         Select Authentication Method:         Secured password (EAP-MSCHAP v2)         Pinable Fast Reconnect         Enforce Network Access Protection         Disconnect if server does not present cryptobinding TLV         Enable Identity Privacy	s ×
Verify the server's identity by validating the certificate         □ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):         □ Trusted Root Certification Authorities:         □ AddTrust External CA Root         □ Baltimore CyberTrust Root         □ Certum CA         □ Certum CA         □ Certum CA         □ Cortum CA         □ CondDO RSA Certification Authority         □ DigiCert Assured ID Root CA         <         >         Notifications before connecting:         Tell user if the server's identity cannot be verified         Select Authentication Method:         Secured password (EAP-MSCHAP v2)         □ Disconnect if server does not present cryptobinding TLV         □ Insconnect if server does not present cryptobinding TLV	
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):  Trusted Root Certification Authorities:  AddTrust External CA Root Baltimore CyberTrust Root Certum Trusted Network CA Catas 3 Public Primary Certification Authority COMODO RSA Certification Authority DigiCert Assured ID Root CA Composed Cataget Composed Cataget Composed Cataget Composed Cataget	tificate
Trusted Root Certification Authorities:         AddTrust External CA Root         Baltimore CyberTrust Root         Certum CA         Cass 3 Public Primary Certification Authority         CMODO RSA Certification Authority         DigiCert Assured ID Root CA            Notifications before connecting:         Tell user if the server's identity cannot be verified         Select Authentication Method:         Secured password (EAP-MSCHAP v2)         Enable Fast Reconnect         Enforce Network Access Protection         Disconnect if server does not present cryptobinding TLV         Enable Identity Privacy	;.*\.srv3\.com):
Trusted Root Certification Authorities:          AddTrust External CA Root         Baltimore CyberTrust Root         Certum CA         Certum Trusted Network CA         Class 3 Public Primary Certification Authority         DigiCert Assured ID Root CA         V         Notifications before connecting:         Tell user if the server's identity cannot be verified         Select Authentication Method:         Secured password (EAP-MSCHAP v2)         Enable Fast Reconnect         Enforce Network Access Protection         Disconnect if server does not present cryptobinding TLV         Enable Identity Privacy	
AddTrust External CA Root Baltimore CyberTrust Root Certum CA Certum CA Certum Trusted Network CA Class 3 Public Primary Certification Authority COMODO RSA Certification Authority DigiCert Assured ID Root CA < Notifications before connecting: Tell user if the server's identity cannot be verified  Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	
Baltmore Cyber Irust Root     Certum CA     Certum CA     Cass 3 Public Primary Certification Authority     DigiCert Assured ID Root CA     Composed Cass and the server's identity cannot be verified     Select Authentication Method:     Secured password (EAP-MSCHAP v2)     Configure     Enable Fast Reconnect     Enforce Network Access Protection     Disconnect if server does not present cryptobinding TLV     Enable Identity Privacy	^
Certum Trusted Network CA Class 3 Public Primary Certification Authority COMODO RSA Certification Authority DigiCert Assured ID Root CA < Notifications before connecting: Tell user if the server's identity cannot be verified  Select Authentication Method: Secured password (EAP-MSCHAP v2)  Configure  Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	
Class J Public Primary Certification Authority COMODO RSA Certification Authority DigiCert Assured ID Root CA  Notifications before connecting: Tell user if the server's identity cannot be verified Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure Endole Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	
DigiCert Assured ID Root CA Notifications before connecting: Tell user if the server's identity cannot be verified Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	
Notifications before connecting:     Tell user if the server's identity cannot be verified     Select Authentication Method:     Secured password (EAP-MSCHAP v2)     Configure     Enable Fast Reconnect     Enforce Network Access Protection     Disconnect if server does not present cryptobinding TLV     Enable Identity Privacy	~
Notifications before connecting: Tell user if the server's identity cannot be verified Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	>
Tell user if the server's identity cannot be verified Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure Configure Configure Configure Configure Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	
Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure Penable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	~
Secured password (EAP-MSCHAP v2) Configure	
Enable Fast Reconnect     Enforce Network Access Protection     Disconnect if server does not present cryptobinding TLV     Enable Identity Privacy	✓ Configure
Enforce Network Access Protection     Disconnect if server does not present cryptobinding TLV     Enable Identity Privacy	
Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	
Enable Identity Privacy	ng TLV
OK Cancel	Cancel

8.ติ๊ก Automatically ออก

ifi	EU LAD C	×
	Protected EAP Properties	×
	EAP MSCHAPv2 Properties	
When	connecting:	
	Automatically use my Windows log-on name and password (and domain if any).	3\.com):
	OK Cancel	^
	ertum CA ertum Trusted Network CA Jass 3 Public Primary Certification Authority OMODO RSA Certification Authority JigiCert Assured ID Root CA	~
Notifica	ations before connecting:	
Tell us	ser if the server's identity cannot be verified	~
Select A	uthentication Method:	
Secureo	d password (EAP-MSCHAP v2) V	Configure
Enab Disco	le Fast Reconnect rce Network Access Protection onnect if server does not present cryptobinding TLV ole Identity Privacy	
	OK	Cancel

#### 9.คลิก Additional Settings

1	Ethernet 4 Properties	
ar	Networking Authentication Sharing	or
)ia	Select this option to provide authenticated network access for this Ethemet adapter. Enable IEEE 802.1X authentication	ua
	Choose a network authentication method:          Microsoft: Protected EAP (PEAP)       V       Settings         Remember my credentials for this connection each	ne
	time i m logged on ✓ Fall-back to unauthorised network access	
	Additional Settings	
	OK Cancel	

10. เลือก Specify authentication mode>เลือก User or computer authentication

ng	Autrenication Shanng
	Advanced settings
:t th :the	802.1X settings
٦ab	Specify authentication mode
se	User or computer authentication 💙 Save credentials
osc	Delete credentials for all users
em ne	Enable single sign on for this network     Ore Perform immediately before user log-on
əll-b	Perform immediately after user log-on
	Maximum delay (seconds):
lditi	Allow additional dialogues to be displayed during single sign on
	This network uses separate virtual LANs for machine and user authentication
	OK Cancel

11. จากนั้นเสียบสาย LAN จะมีหน้าต่างให้ Sign in ให้ใส่ username และ password ที่อยู่บน AD (รหัส เดียวกันกับ Intranet และ Wi-Fi)

