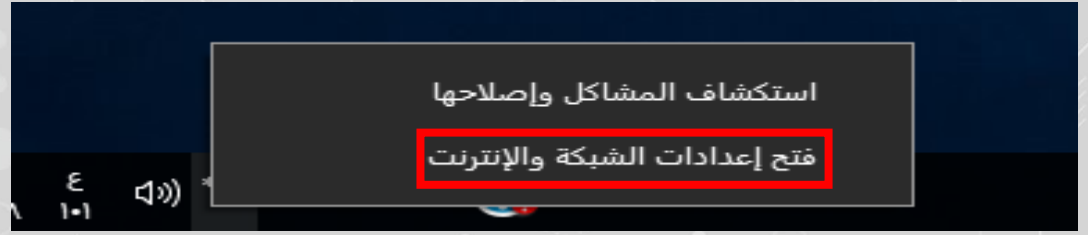
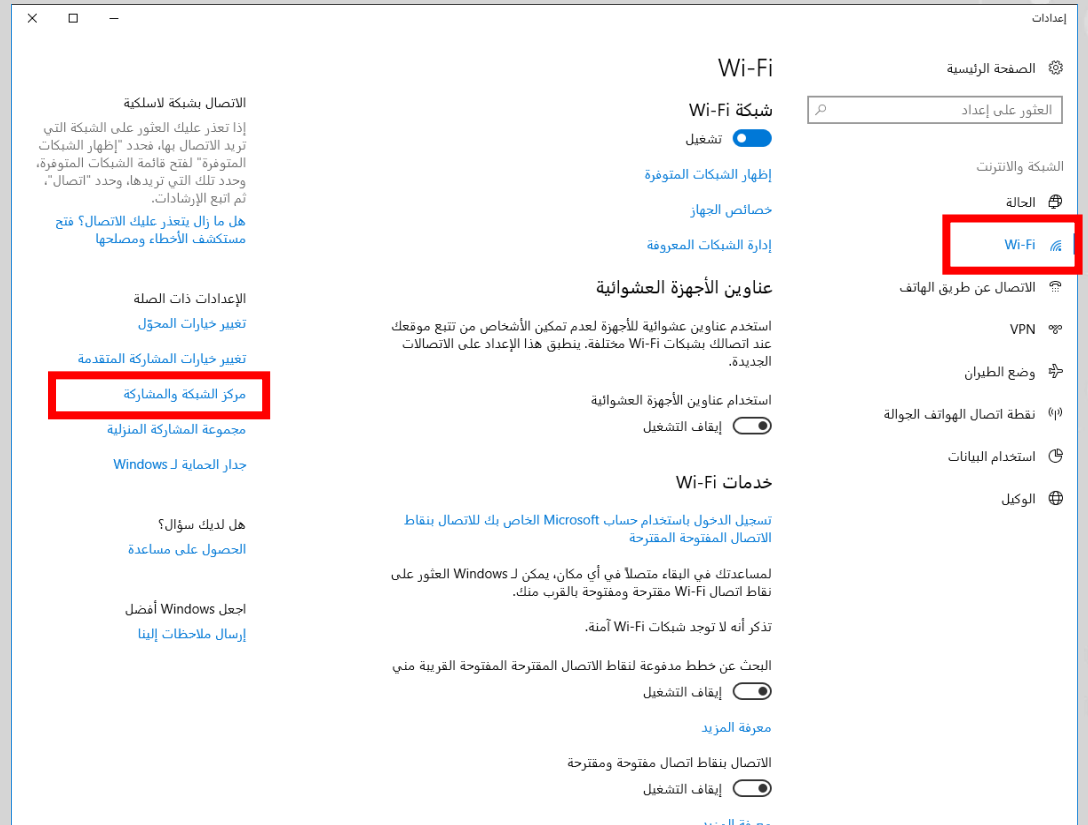


# طريقة دخول QU-WIFI لنظام Windows

1- قم بالضغط ع زر الماوس الأيمن عند أيقونة الشبكة ثم اضغط على :



2- من أيقونة ( WiFi ) اختر ( مركز الشبكة والمشاركة )



### 3- إختار ( إعداد اتصال جديد أو شبكة جديدة )

مركز الشبكة والمشاركة

البحث في لوحة التحكم

لوحة التحكم > كافة عناصر لوحة التحكم > مركز الشبكة والمشاركة

عرض معلومات الشبكة الرئيسية وإعدادات الاتصالات

الصفحة الرئيسية للوحة التحكم

عرض الشبكات النشطة

تغيير إعدادات المحول

تغيير إعدادات المشاركة المتقدمة

تغيير إعدادات الشبكة

إعداد اتصال جديد أو شبكة جديدة

إعداد اتصال واسع النطاق أو طلب هاتفي أو VPN أو إعداد موجة أو نقطة وصول.

استكشاف المشاكل وإصلاحها

تشخيص مشاكل الشبكة وإصلاحها، أو الحصول على معلومات حول استكشاف الأخطاء وإصلاحها.

راجع أيضاً

أدوات Intel® PROSet/Wireless

الأضعة تحت الحمراء

جدار حماية Windows Defender

خيارات الإنترنت

مجموعة المشاركة المنزلية



4- اختر ( الاتصال يدويًا بشبكة لاسلكية ) ثم اضغط التالي :

إعداد اتصال أو شبكة →

### تحديد خيار الاتصال

الاتصال بالإنترنت  
قم بإعداد اتصال واسع النطاق أو اتصال طلب هاتفى بالإنترنت.

إعداد شبكة جديدة  
إعداد موجه جديد أو نقطة وصول جديدة.

**الاتصال يدويًا بشبكة لاسلكية**  
الاتصال بشبكة مخفية أو إنشاء ملف تعريف شبكة لاسلكية جديد

الاتصال بمساحة العمل  
إعداد اتصال الطلب الهاتفى أو VPN بمساحة العمل.

إلغاء الأمر | التالي

5- قم بادخال ( اسم الشبكة QU-WIFI ) وتأكد من تغيير ( نوع الأمان الى WPA2-Enterprise ) ثم اضغط التالي

الاتصال يدويًا بشبكة لاسلكية →

### إدخال معلومات عن الشبكة اللاسلكية التي تريد إضافتها

اسم الشبكة: QU-WIFI

نوع الأمان: WPA2-Enterprise

نوع التشفير: AES

مفتاح الأمان:

بدء هذا الاتصال تلقائيًا

الاتصال حتى في حالة توقف الشبكة عن البث  
تحذير: إذا تم تحديد هذا الخيار، فقد تتعرض خصوصية الكمبيوتر للخطر.

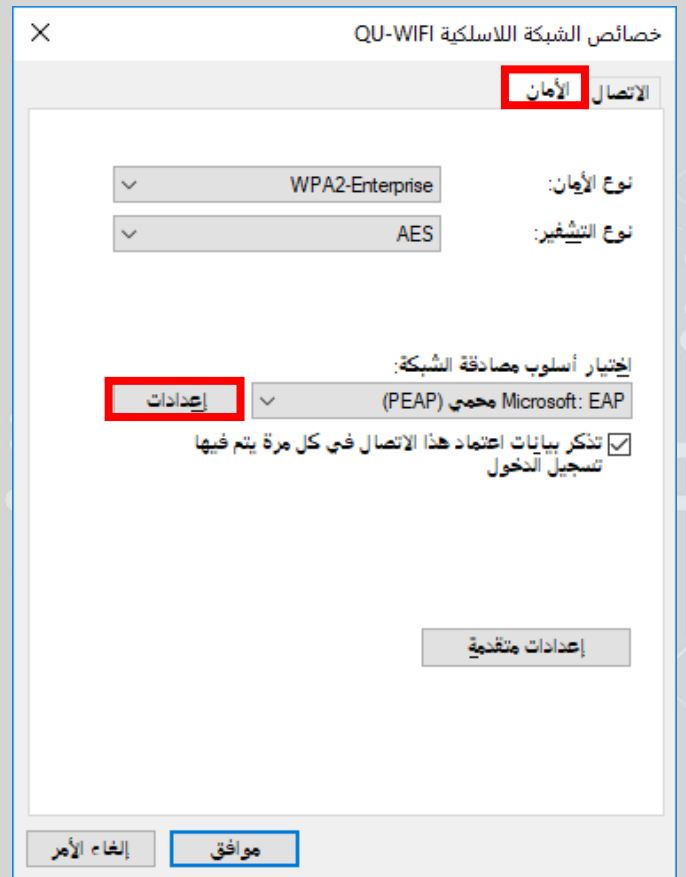
إلغاء الأمر | التالي



6- اضغط ( تغيير إعدادات الاتصال )



7- من إيقونة الأمان قم بالدخول على ( إعدادات )



8- تأكد من عدم وجود علامة صح عند ( التحقق من هوية الخادم ... ) ثم اضغط ( تكوين )

خصائص EAP المحمية

عند الاتصال:

للتحقق من هوية الخادم عن طريق التحقق من صحة الشهادة

الاتصال بهذه الخوادم (أمثلة: srv1.srv2:.\*\srv3\com):

مراجع الشهادات الجذرية الموثوقة:

- AddTrust External CA Root
- Altus Local client Certificate Authority
- Baltimore CyberTrust Root
- Certum CA
- Certum Trusted Network CA
- Class 3 Public Primary Certification Authority
- COMODO Certification Authority

إعلامات قبل الاتصال:

إعلام المستخدم إذا تعذر التحقق من هوية الخادم

تحديد أسلوب المصادقة:

كلمة المرور المؤمنة (EAP-MSCHAP v2)   تكون...

تمكين إعادة الاتصال السريع

قطع الاتصال إذا لم يقدم الخادم الربط المشفر TLV

تمكين خصوصية الهوية

9- تأكد من عدم وجود علامة صح ( عند استخدام اسم تسجيل الدخول ... ) ثم اضغط موافق

خصائص EAP MSCHAPv2

عند الاتصال:

استخدام اسم تسجيل الدخول إلى Windows وكلمة المرور تلقائياً (والمجال إن وجد).



10 – من أيقونة الأمان قم باختيار ( إعدادات متقدمة )

خصائص الشبكة اللاسلكية QU-WIFI

الاتصال الأمان

نوع الأمان: WPA2-Enterprise

نوع التشفير: AES

اختيار أسلوب مصادقة الشبكة:

إعدادات EAP Microsoft محمي (PEAP)

تذكر بيانات اعتماد هذا الاتصال في كل مرة يتم فيها تسجيل الدخول

إعدادات متقدمة

إلغاء الأمر موافق

11 – تأكد من وجود علامة صح عند ( تحديد وضع المصادقة ) واختيار ( مصادقة المستخدم )

إعدادات متقدمة

إعدادات 802.1X إعدادات 802.1X

تحديد وضع المصادقة:

مصادقة المستخدم

حفظ بيانات الاعتماد

حذف بيانات الاعتماد ليكافة المستخدمين

يمكن تسجيل الدخول الأحادي لهذه الشبكة

التنفيذ قبل تسجيل دخول المستخدم مباشرة

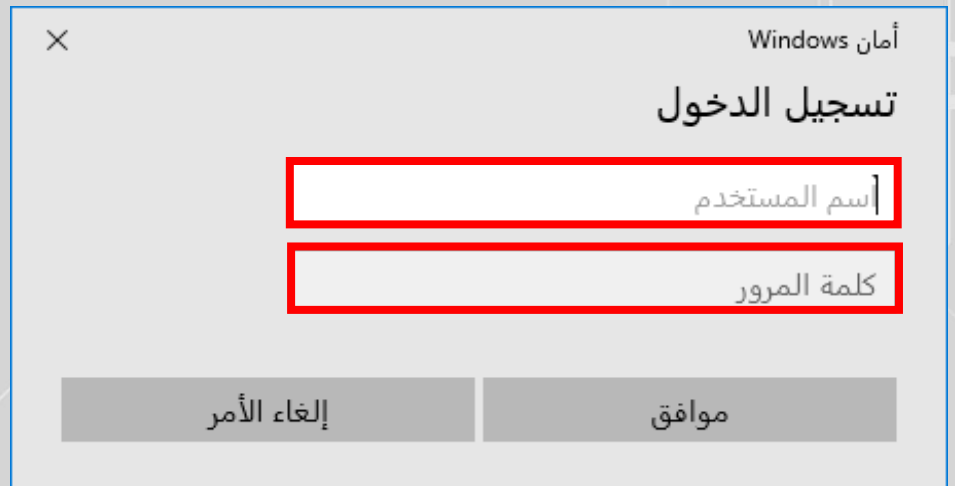
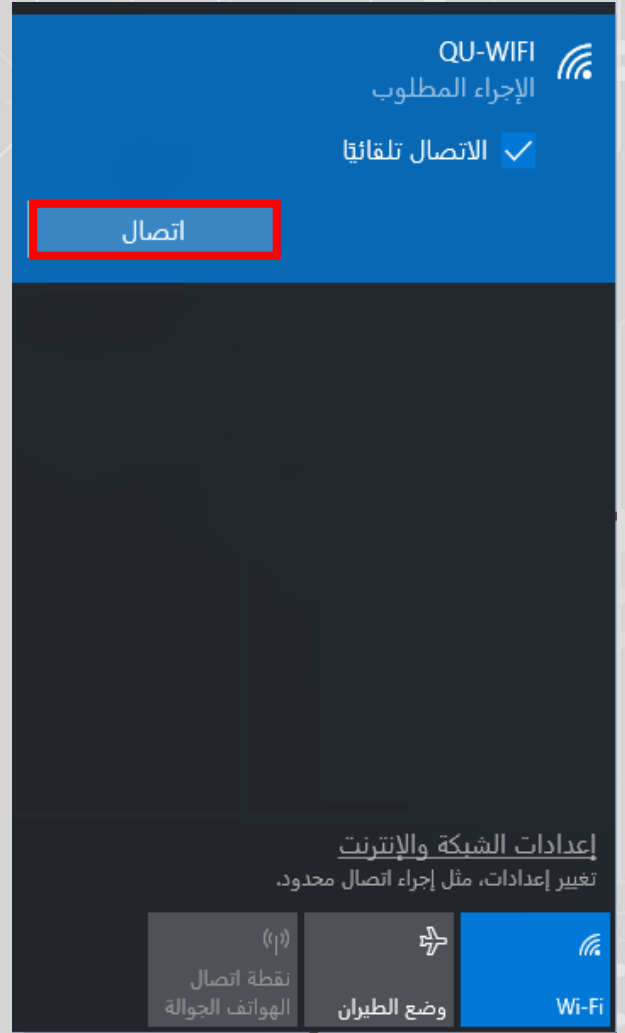
التنفيذ بعد تسجيل دخول المستخدم مباشرة

الحد الأقصى للتأخير (بالشواني): 10

السماح بعرض مربعات الحوار الإضافية أثناء تسجيل الدخول الأحادي

تستخدم هذه الشبكة شبكات LAN ظاهرية منفصلة للجهاز ولمصادقة المستخدم

إلغاء الأمر موافق





14- سيتم تحويلك الى هذه الصفحة قم بتحميل ( مكافح الفيروسات ) و ( عميل فاحص الأمان )

# QASSIM UNIVERSITY

VSCMG\_HJ  
2023/30  
The Department of Information Systems  
Faculty of Computer Science  
Qassim University

جامعة القصيم  
Qassim University

مرحباً بك في شبكة جامعة القصيم

Welcome to Qaseem University Network

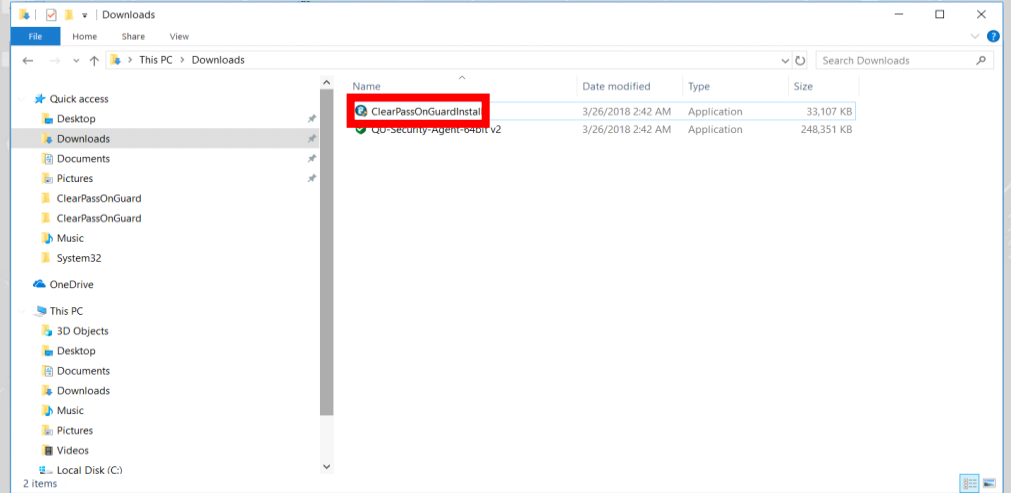
Log In

في حالة وجود مشكلة في عملية الدخول بالشبكة الرجاء  
التأكد من عمل الخطوات التالية  
تركيب نظام **مكافح الفيروسات الخاص بالجامعة**  
ثم تركيب **عميل فاحص الأمان**  
بعد تركيب مكافح الفيروسات وفاحص الامان الرجاء  
قم بتحميل **الإعدادات** ثم قم بفتح المجلد و تشغيل الملف  
Setup.exe

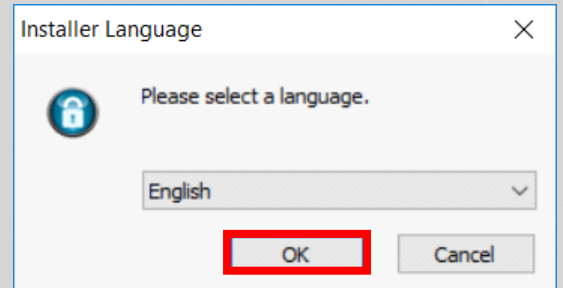
If you are facing any difficulty connecting to the network  
make sure that the **University Antivirus** is installed  
Then install the **Onguard agent**  
after installing the Antivirus and Onguard agent, install  
the **setings** by opening the NAC folder and run Setup.exe



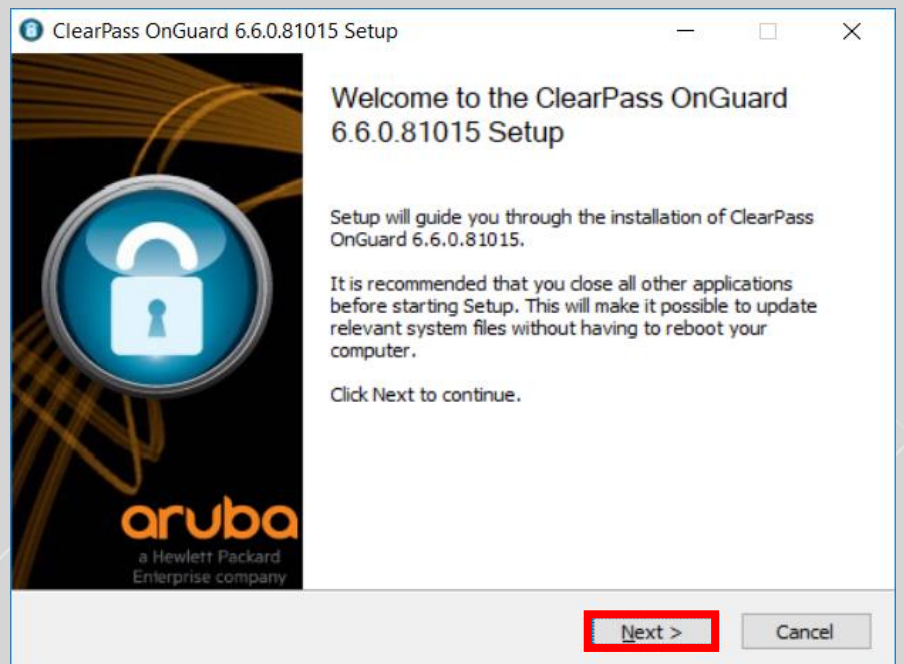
15 – اذهب الى قائمة التنزيلات وابدأ عملية التنصيب للبرامج

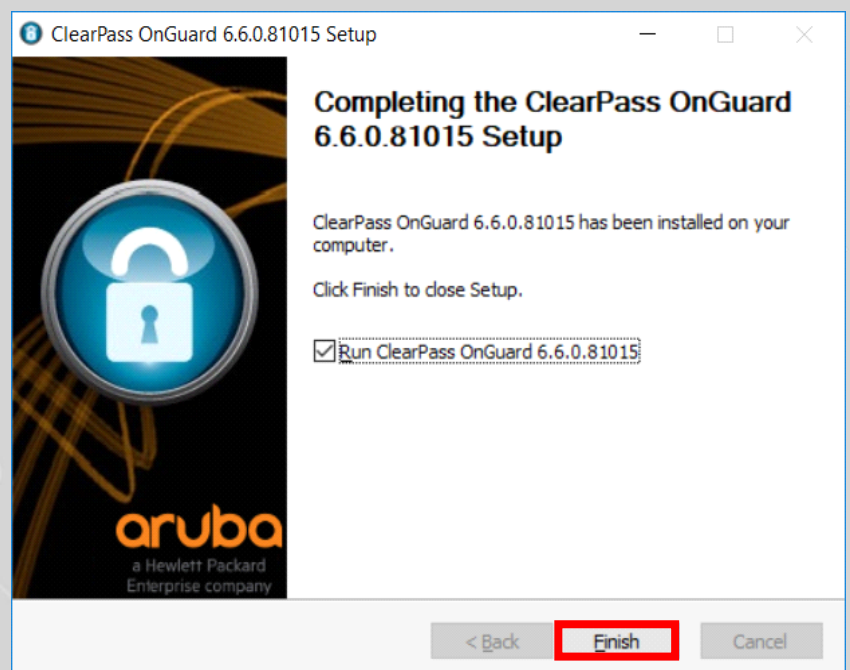
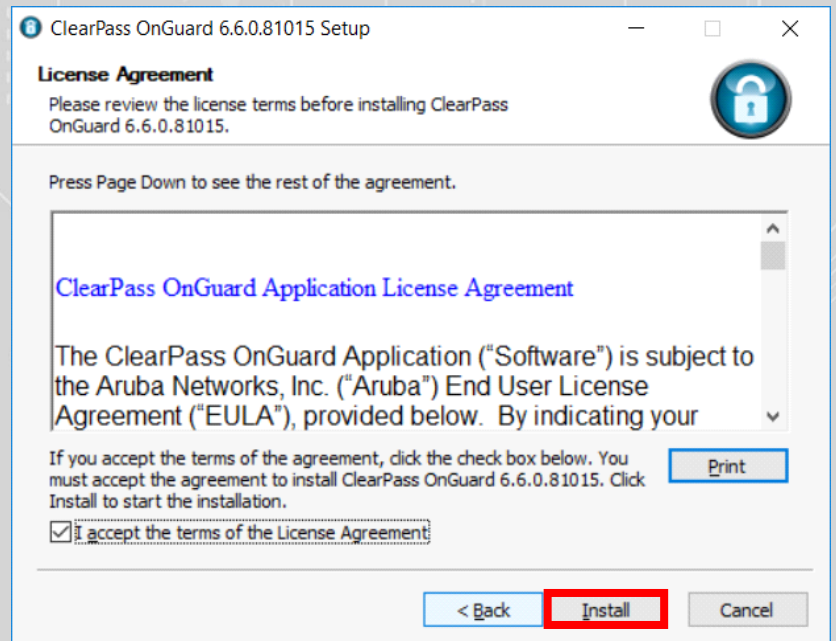


16 – قم بالضغط على ( OK )



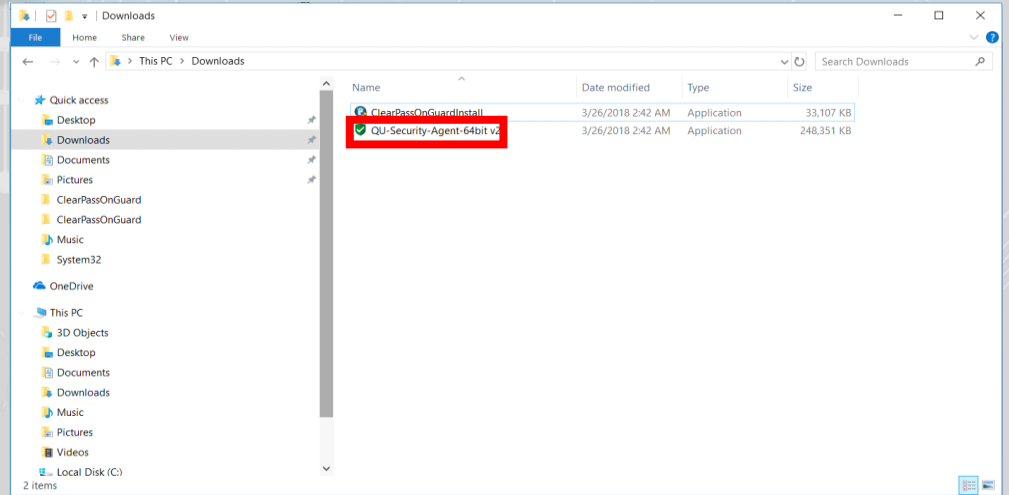
17 – قم بالضغط على ( Next )







20 – من قائمة التنزيلات قم بتحميل البرنامج الثاني



21 – قم بالضغط على ( Install )

