Interreg
North-West Europe
REAMIT
European Regional Development Fund

EUROPEAN UNION

Improving Resources Efficiency of Agribusiness Supply Chains by Minimising Waste Using Internet of Things Sensors (REAMIT)

Deliverable 5.4: User manual for the big data platform and the web-interface

Content

1. INTRODUCTON

1.1 Introduction to REAMIT

Reducing food waste is of the highest priority for the European Union (88Mt or € 143B wasted per year). The EU has committed to halving food waste by 2030 by focusing on all stages in the supply chain. Despite the fact that technologies to reduce food waste already exist, they have not been applied to food supply chains. The REAMIT project suggests adapting and applying already existing innovative technology to food supply chains in Interreg North-West Europe (NWE) to reduce food waste and improve resource efficiency.

REAMIT is a transnational European territorial cooperation project, implemented by 14 partner organisations from Higher Education Institutions, business support organisations, technology and food enterprises in NWE. The REAMIT consortium has brought several academics, business support organisations and industry partners closer to achieving the core objective of using Internet of Things (IoT) sensors and Big Data analytics in food supply chains to reduce food waste.

This document is a user manual that covers the detailed information on using the Big Data platform and the web-interface.

1.2 The REAMIT Big Data Server

1.2.1 Definition of REAMIT Big Data server

The REAMIT technology testing data is gathered from different pilot companies and it should be stored in the UoB Big Data Hub.

Figure 1 shows Big Data server at the University of Bedfordshire (UoB). The Data Hub is located in a secure area inside the university, and the physical access to it requires obtaining security permissions.

Figure1: Image of REAMIT Big Data server at the University of Bedfordshire

As expected, the project partners are able to connect to the REAMIT server, however, not all of them are allowed to have admin rights.

The instructions for the project partners on how to connect to the Big Data server are explained in more details in the following sections.

2. REAMIT Big Data basic concepts

2.1: External user

An external user is a user who needs to access the server from outside of the organisation that is hosting the server. External users usually do not have admin rights and use the information that is provided to them to be connected to the server remotely. The external users do not work for a company or university, but they have access to some information stored on the server.

2.2: Internal user

An internal user is a user who is employed by the server hosting organisation and can access the organisation's internal systems. They may have admin rights or they may not have admin rights, depending upon their role.

2.3: Shared instance

A shared instance, sometimes called shared database, allows internal/external users to store their documents in their relational SQL database rather than on a file system. It allows multiple users using the same synchronised storage location at any time.

2.4: Admin user

The database administrator (DBA) is **the person responsible for the design, control, and administration of the database**. The DBA must manage the information system (IS) each time the database is analysed, designed, and implemented. The person also interacts with and provides support for end users.

Figure 2 shows a DBA role to manage a database.

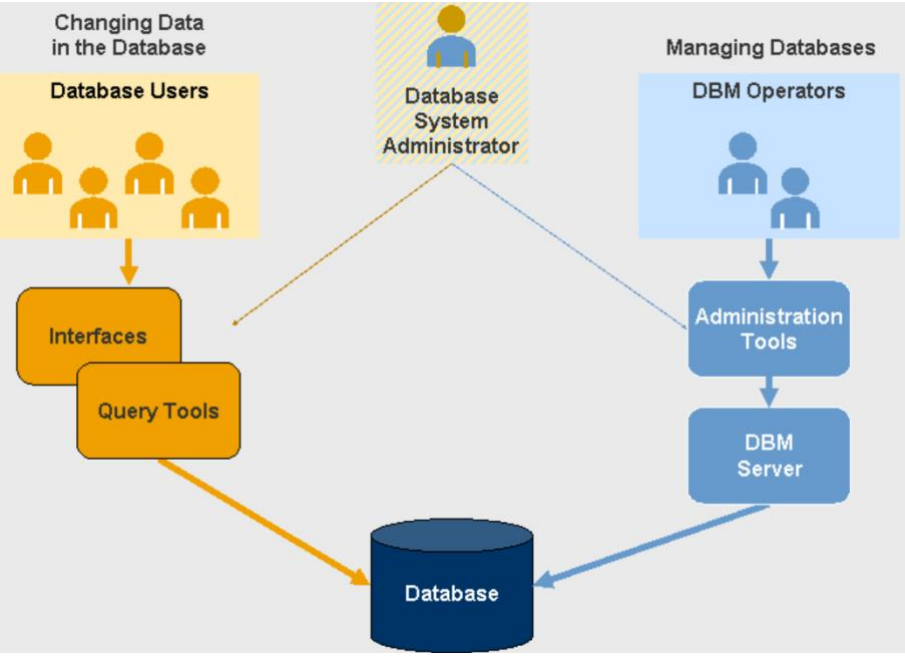


Figure 2. DBA's role in managing a database

3. Creating instances

3.1: Admin instance

There are two types of users that may request an administrative right: external and internal users.
There is a guide for both the internal and external users that should be followed before sending them out login credentials.

1. Create a Windows user account on the REAMIT server machine using the following steps for the external user. (No need to wait for completion of the first two steps before starting this step. This can be done in parallel with the first two steps.)

    a. **Start > Computer Management**
    b. Expand "**Local Users and Groups**" and double click on "**Users**". Right click on empty white space>**New User** …
    c. Enter the details of the new user (double check spellings). Make sure that you keep consistency on the username formats for all REAMIT external users. Choose a random initial password and ensure that "**User must change password on next logon**" is ticked and then click on "**Create**". You will see that a new Windows user account is created with the suggested name. If it does not appear, please refresh the website and check again.
    d. Expand "**Local Users and Groups**" and double click on "**Groups**", then double click on "**Remote Desktop Users**" and click "**Add**".
    e. Enter the tentative username and click on "**Check names**". It should complete the name by adding the server name. Click "**Ok**" twice. This will create a user account on the server with the username and initial password you have entered.

f. Share the REAMIT Windows server username and password created in the above step with the external user through the mobile phone number provided to you.

   Inform the external user that they will be prompted to change the password after the first login.

2. Send the document "**External access client setup and login instructions**" to the contact person from the external organisation and arrange for testing VPN-based remote connection.
3. Update the REAMIT server excel log sheet with a new row and new details for the external user (VPN access Login credentials; password will not be known to you) and REAMIT server user account login credentials (initial password will be known to you).

3.2: External instance

Procedure to create a MSSQL database instance with user access credentials on the REAMIT server

1. Mount the MSSQL ISO (**Right click > Mount**) –E:\Softwares\Admin\MSSQL ISO. The name of the file is "SW_DVD9_NTRL_SQL_Svr_Standard_Edtn_2019Dec2019_64Bit_English_OEM_VL_X22-22109". **Right click and mount**.
2. To add a new instance you need to run the setup from the mounted drive (Drive F). **Right click on the drive to run or install.**
3. Using the left navigation menu select "**Installation**".
4. Run the "**New SQL Server Standalone installation or add features to an existing installation**" option.
5. Step through the wizard until "**Feature Selection**".
6. Installed features: **Select SQL Server Database Engine** – other features can be added in the future if required (a full list of feature explanations can be found here: https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-version-15?view=sql-server-ver15). Note: For easier management "SQL Server Management Studio" installation recommended – can be downloaded from here: (https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?redirectedfrom=MSDN&view=sql-server-ver15
7. **Setup Named Instance**, give your name.
8. Service accounts as default.
9. Database Engine Configuration: Paths set to use E: (E:\MSSQL) by navigating to Data directories Tab.)
10. Database Engine Configuration, Server configuration tab: Use mixed mode setting an SA password. The SA account can be used to manage the instance (provide to user). The instance name is used as the ID by default. Instance information page here: (https://docs.microsoft.com/en-us/sql/sql-server/install/instance-configuration?view=sql-server-ver15#instance-configuration-page).
11. **Click on "add current user"**, wait until REAMIT-SERVER\Administrator (Administrator) appears inside the white space.
12. **Click "Next" and** then **"install"**.

13. Log an ICT service desk request by visiting in.beds.ac.uk by logging in with your staff details, click on service desk and then ICT.
14. Select service Catalogue (just below incident report) and click on **Account and E-mail request**. From the dialogue box choose firewall rule – change Access/Permissions.
15. Enter again your staff credentials to release a dedicated port number for accessing the specific instance of the database on the REAMIT server. In the request, make sure to mention the required port number (preferably in the range 14001 and afterwards, and make sure to check the REAMIT server excel log sheet to choose an unallocated number and a continuous sequence with the previous numbers), name of the database instance created in step 5 and for whom (company/organisation) the access is requested. Kindly request to direct this to Andrew Stallion (Andrew.Stallion@beds.ac.uk).
16. Once you received the confirmation from ICT BED that the access to the database has been granted on the requested port number, proceed to port configuration.
17. Ports can be assigned to the instances using the SQL Server Network Configuration in SQL Server Configuration Manager. Select the instance, **Go to Network Configuration**, **click the SQL instance** for which you want to check SQL port.
18. It opens the protocols list. Right click on **TCP/IP and properties**.
19. Click on **IP Addresses** and scroll down to IPAll group. You can see TCP dynamic SQL ports and TCP ports. From the list to configure, assign the port under the TCP/IP properties. Note: turn off dynamic ports by removing the "0" in the TCP Dynamic Ports field.
20. Once ports have been configured it is worth **restarting (right click) the service SQL server** (Instance) service in SQL Server Services in the SQL Server Configuration Manager.
21. Update the fire wall settings on the server to allow connections through the assigned port number. **Go to Windows search** and **type and click on "Windows Defender Firewall"**. **Go to Advanced Settings>Select Inbound rules** in top left corner>Select New Rule on top right corner> Select Port and click Next > Enter allocated port number in the empty white space>Follow the wizard until you reach Name. **Enter the Name** in a format consistent with other users (For example, LEVSTONE_MSSQL or MTUKERRY_MSSQL or SENX_MSSQL). **Click on "Finish"** and **close all Windows defender firewall windows screens**.
22. Communicate the port number to the external user through which they should be able to connect to the database.
23. **Update the REAMIT server excel log sheet with the MSSQL instance name**, dedicated port number and server access login details (password will be known to you) for the corresponding Windows external user.

3.3: Internal instance

4. Big Data access rights.

4.1: Admin access

The remote external access setup procedure to access REAMIT server as an ADMIN has been explained as follows:

It is the remote desktop access to the REAMIT server for a non-BED employee. Please note that this procedure will need to be followed to allow non-BED employees to access the REAMIT server and will not be needed if they only need the creation of an SQL instance to store data in the MSSQL data base, in which case, only "**Procedure to create a MSSQL database instance for a user on the REAMIT server**" should be followed.

Once a BED staff receives the request for external access, they should make sure to have the following details of the person who needs the external access:

1. name of the company/organisation the external user is employed with;
2. tentative username of the external user;
3. mobile phone number of the external user.

Afterwards, please follow the steps below:

4. Log an ICT service desk request (not an incident request) by visiting in.beds.ac.uk to create and enable the tentative username to access the REAMIT server through the VPN. In the request, please mention that in this regard, there will be a need to enable firewall settings for having the above access through VPN and demilitarised zone (DMZ). Finally, kindly request to direct this to Andrew Stallion (Andrew.Stallion@beds.ac.uk).
5. Please ensure that the password and username are communicated to the external user by following up with ICT. If the contact person gets back to you, they receive a request to wait until you have created a REAMIT Windows server user account for them (step 3). If you have already done this please proceed to step 4.
6. Create a Windows user account on the REAMIT server machine using the following steps for the external user. (No need to wait for completion of the first two steps before starting this step. This can be done in parallel with the first two steps and some partners who do not need Windows remote desktop access may not need to follow this step at all.)

    a. **Start > Computer Management**
    b. Expand "**Local Users and Groups**" and double click on "**Users**". Right click on empty white space>**New User** …
    c. **Enter the details of the new user** (double check spellings). Please ensure consistency with username formats for all REAMIT external users. Choose a random initial password and make sure that "User must change password on next logon" is ticked and then click on **"Create"**. You will see that a new Windows user account is created with the suggested name. If it does not appear, please refresh the website and check again.

d. Expand **"Local Users and Groups"** and double click on **"Groups"**, then double click on **"Remote Desktop Users"** and click **"Add".**
e. Enter the tentative username and click on **"Check names"**, it should complete the name by adding the server name, after this click **"Ok"** twice. This will create a user account on the server with the username and initial password you have entered.
f. Share the REAMIT Windows server username and password created in the above step with the external user through the mobile phone number provided to you.

   Inform the external user that they will be prompted to change the password after the first login.

7. Send the document "External access client setup and login instructions" to the contact person from the external organisation and arrange for testing VPN based remote connection.
8. Update the REAMIT server excel log sheet with a new row and new details for the external user (VPN access login credentials; password will not be known to you, while REAMIT server user account login credentials, initial password will be known to you).

4.2: External access

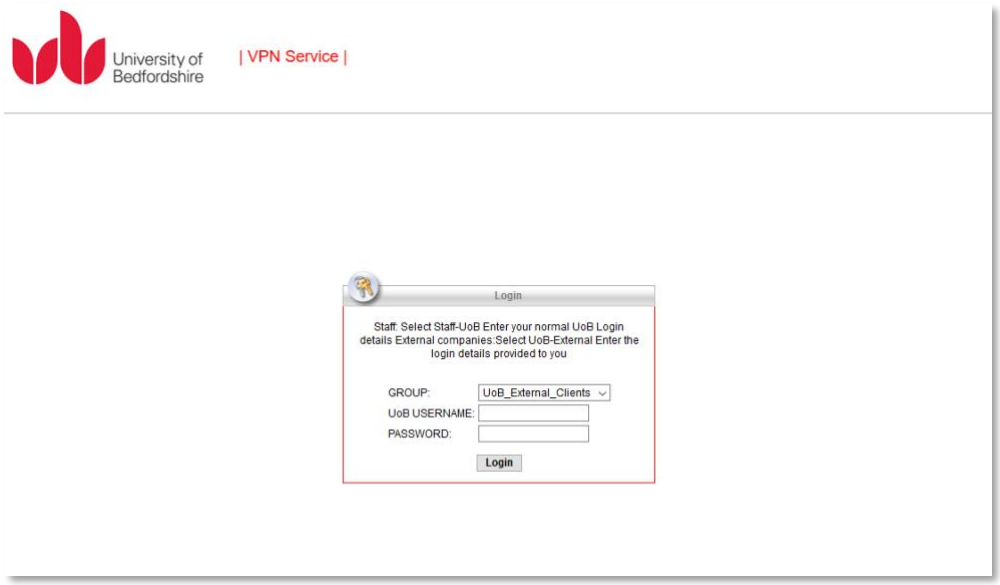
Steps to be followed by the external user for connecting with the REAMIT server through Virtual Private Network (VPN) and Remote Desktop (RDP)

1. To connect to the server, first refer to the following steps needed for the VPN connection (taken from document sent by Andrew, ICT BED on 12/01/2021 to Lohit, BED and Wayne, Levstone).

   a. Downloading the **AnyConnect Client** from vpn.beds.ac.uk

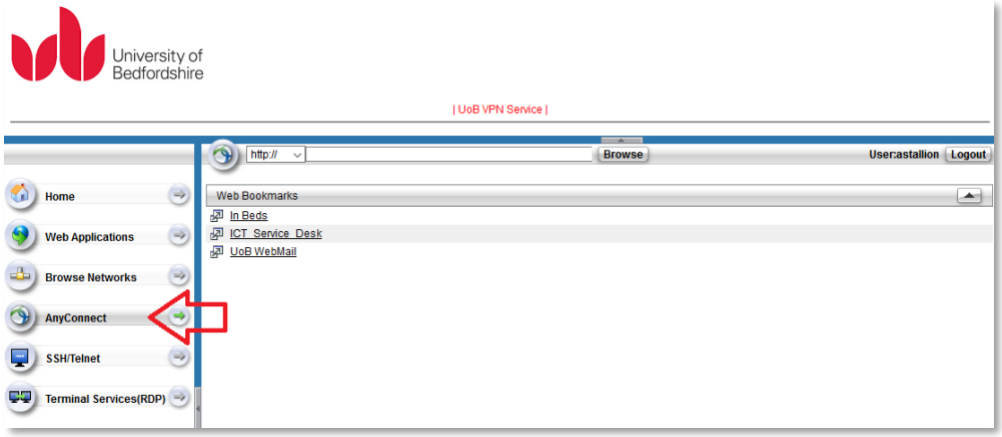
Skip this step if you have the AnyConnect software already installed

- Browse to https://vpn.beds.ac.uk



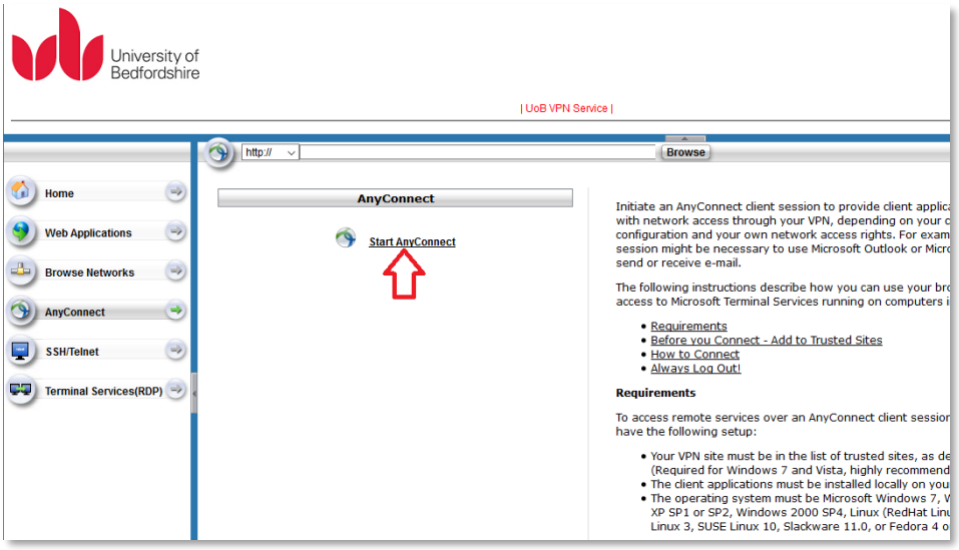
- If the GROUP field does not already show **UoB_External_Clients**, use the drop-down menu to select it.
- Enter the username and password supplied by UoB (aka BED)

The initial VPN Web-Page should now be displayed as below:



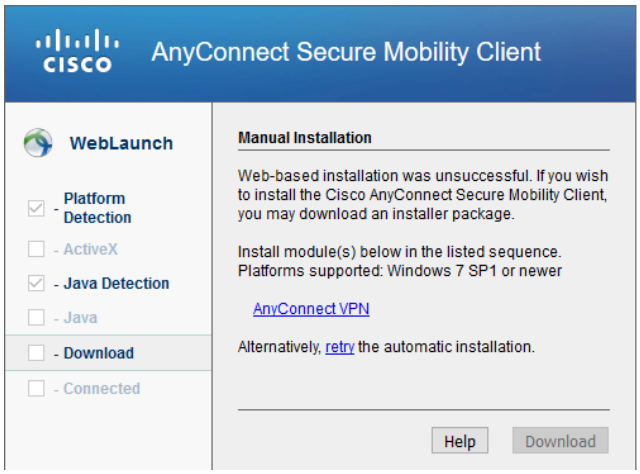
- Click on the **AnyConnect** button on the left.

The AnyConnect Web-Page should now be displayed:



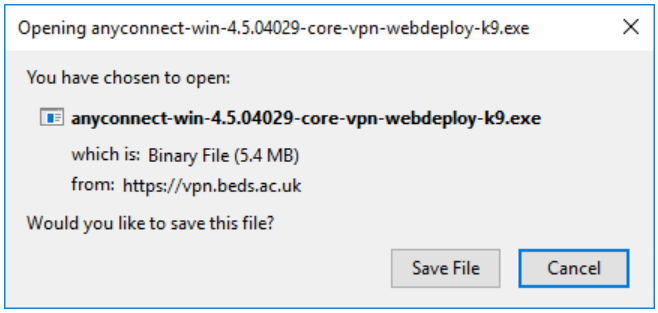
- Click on the Start AnyConnect link.

The web-launch notification window will now open. Try to download the client **AnyConnect**.



- If the download fails (as shown above), click on the **AnyConnect VPN** link.

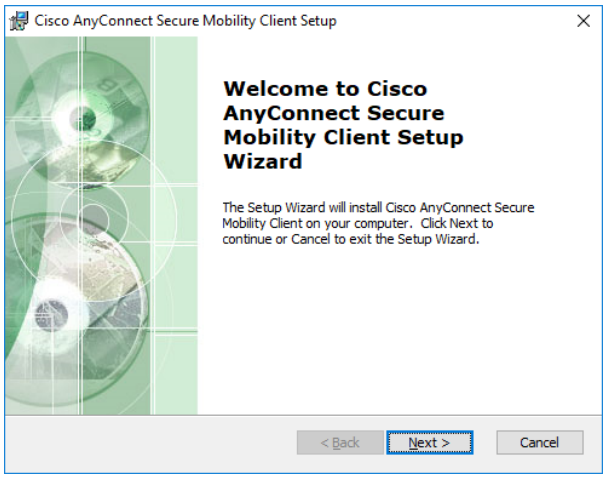
It will then try to download the installation file:



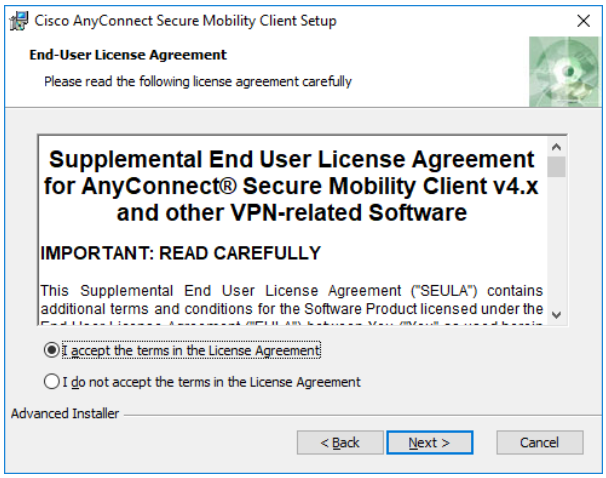
- Click **Save File.**

The file should be saved to your browser download location.

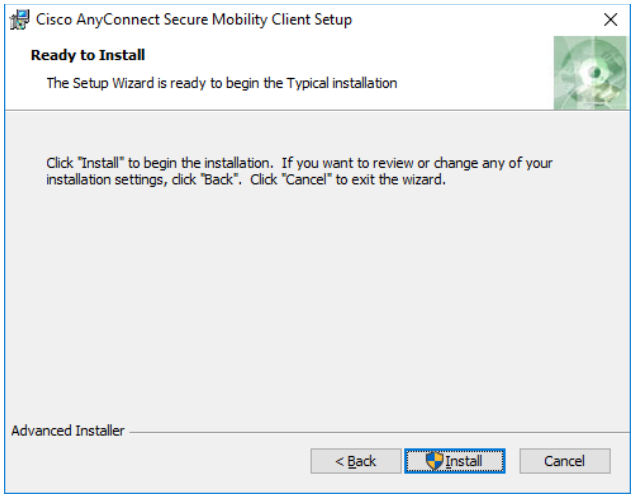
- Open the install executable by double clicking on it.



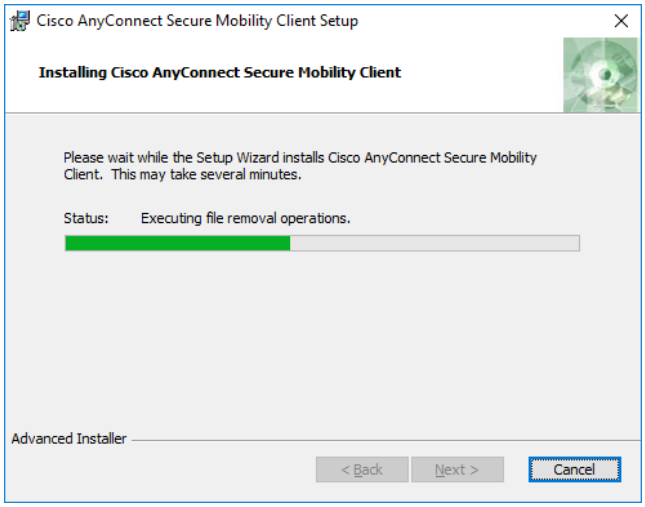
- Accept the Licence Agreement and click on **"Next".**



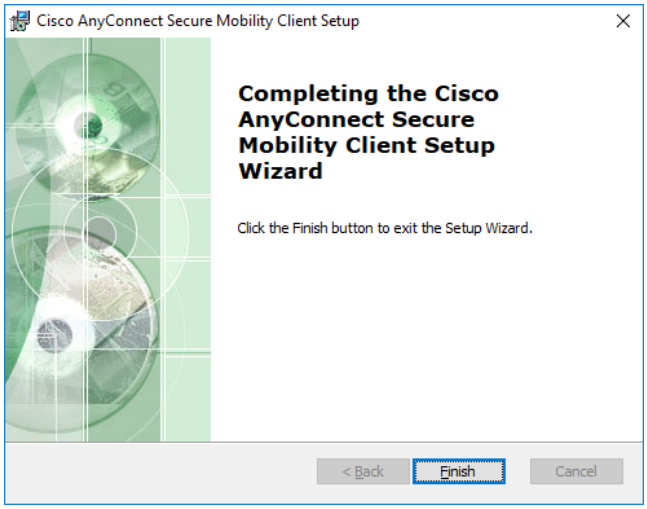
- Click the **"Install"** button.



The installation progress will now be displayed.



- Click on **"Finish"** to complete.



- You can now close the browser window.

The software should now be installed on your computer – the location will depend on what version of Windows you have.

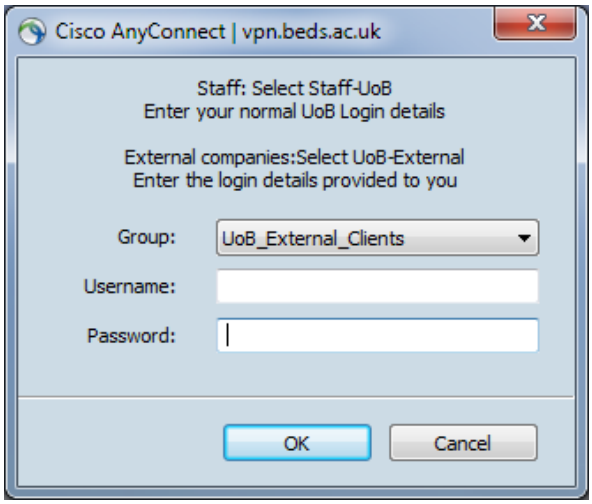
For Windows 10, for example, the application (Cisco AnyConnect Mobility Client) will appear as a drop-down for Cisco Software.

b. Running the Cisco AnyConnect Mobility Client

- Launch the AnyConnect client software.
- Enter **vpn.beds.ac.uk** in the destination box and click the **"Connect"** button.

The **vpn.beds.ac.uk** connection window should now be displayed.

- Select **UoB_External_Clients** from the drop-down **Group** box (if it's not already displayed).



- Enter the **username** and **password** already provided by UoB (aka BED) for VPN access and click the **"OK"** button.
- Click on the "**Accept"** button when the authorisation window is displayed.

You are now connected to the internal local area network of the University of Bedfordshire, with an IP address in the range 10.2.0.200 – 10.2.0.249. You should have access to the required internal resources.

2. After this step, to connect with RDP, the user needs to open **"Remote Desktop Connection"** app on Windows and enter in the IP address (194.80.213.19) then click "**Connect"**.

3. After a successful remote desktop connection to the server, a login screen will be prompted for accessing the REAMIT server. You can log in with the login credentials (username and password) provided by BED for REAMIT server remote desktop access. During the first login, you will be asked to change the password.

4.3: Internal access

Remote Internal access client setup procedure and login instructions to access REAMIT server

Internal access to REAMIT server: it is the remote desktop access to the REAMIT server for a BED employee either from inside or outside the BED campus. At present the internal access is only available to the Administrator. Anyone who has the admin credentials can login remotely from any computer device. There are four ways an admin user can access the server remotely:

1. using a university desktop computer which is connected to the internet through the University LAN wire (**to be tested after University reopens**);
2. using a personal laptop which is connected to the internet through the University LAN wire (**to be tested after University reopens**);
3. using a personal laptop which is connected to the internet through the University wi-fi (for example through eduroam);
4. using a laptop or a computer which is connected to the internet through a non-BED internet connection (for example, to connect remotely from home using a computer/laptop which uses a home network connection).

For the first case, you will have to follow the steps below:

1. login to the University computer with your BED staff username and password in the same way as you login to any University system. Make sure your system is connected to the University LAN wire.
2. open the Windows Remote Desktop Client App by accessing it through the search bar.
3. in the "General" tab, Enter the IP address: "194.80.213.19" in the "Computer" field and use the username: "MicrosoftAccount\Administrator".
4. click "Connect" and click "Yes" on the next Screen which will take you to the server login window.
5. Enter the Admin password given to you for logging in to the REAMIT server and click **"OK".**

For the second case, once you have logged in to your laptop and ensured that it is connected to the University LAN wire, please follow steps 2 to 5 as described for the first case.

For the third case, log an ICT service desk request by visiting in.beds.ac.uk to enable the firewall settings to connect to the REAMIT server through the University wi-fi using your BED

staff username. Next, once you have a confirmation from ICT saying that your request is completed, please follow steps 2 to 5 as described for the first case.

For the fourth case, a Multi Factor Authentication (MFA) will be used to connect to the REAMIT server from outside the University network. First, log an ICT service desk request by visiting in.beds.ac.uk to enable the firewall settings to connect to the REAMIT server through non-University internet using your BED staff username. In the email, explain the need and request it to be directed to Andrew Stallion (andrew.stallion@beds.ac.uk). Once you have received a confirmation from ICT BED saying the request is completed, the following procedure will allow for a successful connection from home using the Microsoft Authenticator App (MFA) with Cisco AnyConnect for BED staff.

Step 1

You will need to:

- download the app to the phone you will be using to 'authenticate' yourself;
- set-up your UoB login to use MFA;
- and you can now connect to the UoB network over VPN using the UoB_Staff++ connection – this allows you to use RDP. Standard connections are not allowed RDP.

Step 2

If you want to RDP to REAMIT from your laptop from home:

- make sure you are connected to the Internet (for example, via home wi-fi);
- have your phone ready with the MFA app running;
- run the Cisco AnyConnect Client – Instructions are available here: https://in.beds.ac.uk/ict/guides/cisco-anyconnect/.

Step 3

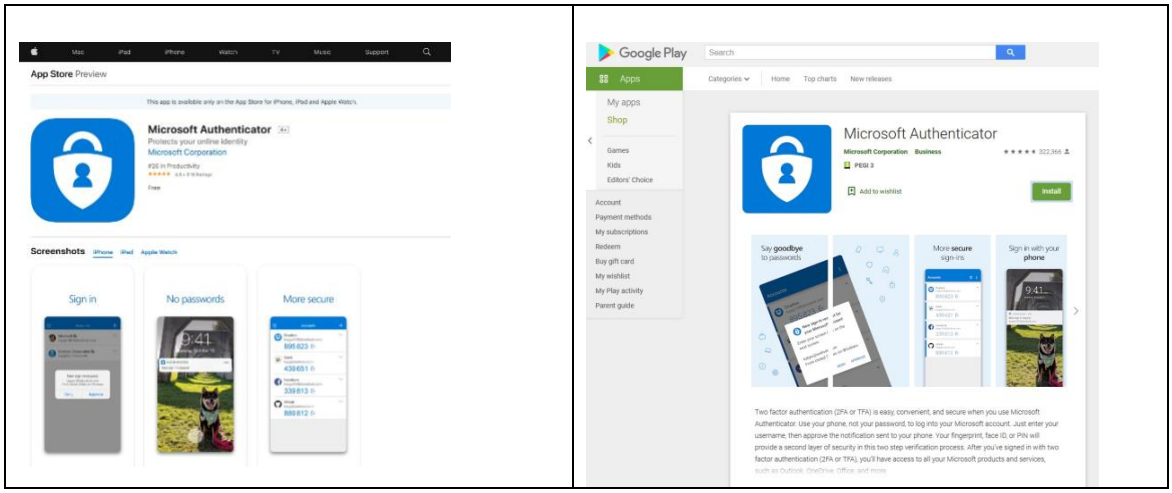
- Authenticate your login attempt to login to the UoB network on the mobile phone.
- You will now be connected directly/connected to the UoB network.
- Run the RDP client on your laptop to connect to the REAMIT server (Steps 2-5 as shown for the first case).

Using the Microsoft Authenticator App with Cisco AnyConnect

1. Download & install the Microsoft Authenticator App

- You will need a smartphone (iPhone or an Android phone) and a relevant login for the Apple App Store or Google Play.
- Download and install the relevant app for your phone.

iPhone	Android



2. Configure the Microsoft Authenticator App

The app makes sure that your UoB account is linked to the app on your phone. The two are linked together initially using a **QR code** – your UoB account is used to generate it, and the phone app accesses the camera on the phone to scan this code.

1. Setting up your UoB account

Connect to the URL: http://aka.ms/mysecurityinfo

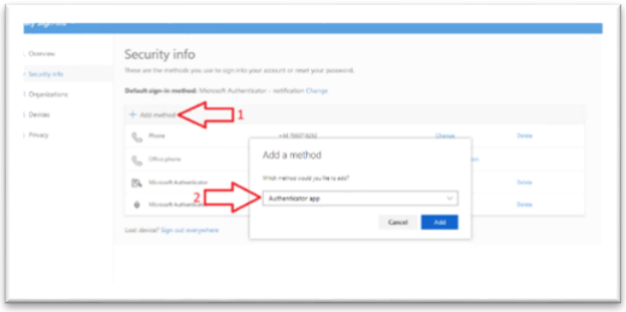
Note: this is a direct link to the relevant page, although you can access this via the web-mail page (Office 365, view account, security info).

Log in at the UoB Single Sign On Page if prompted.

Once logged in it should display the **Security info** page for your account.

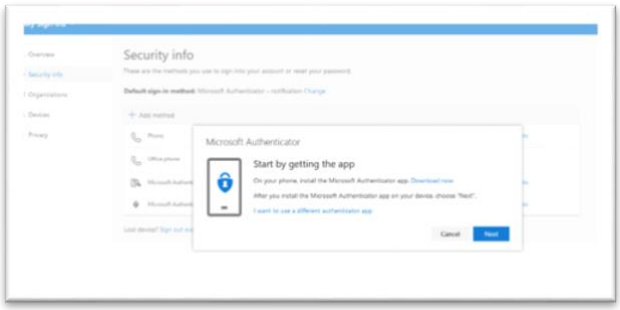
Click on:

1. **+ Add a method;**
2. select **Authenticator App** from the drop-down.

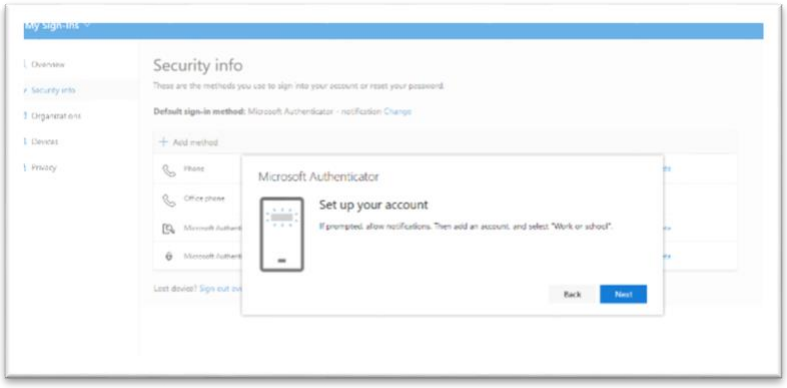


It will now prompt you to download and install the Microsoft Authenticator app for your phone.

You should have already done this (as described above), so click "**Next".**



We are now ready to link the Microsoft Authenticator phone app with your UoB account.



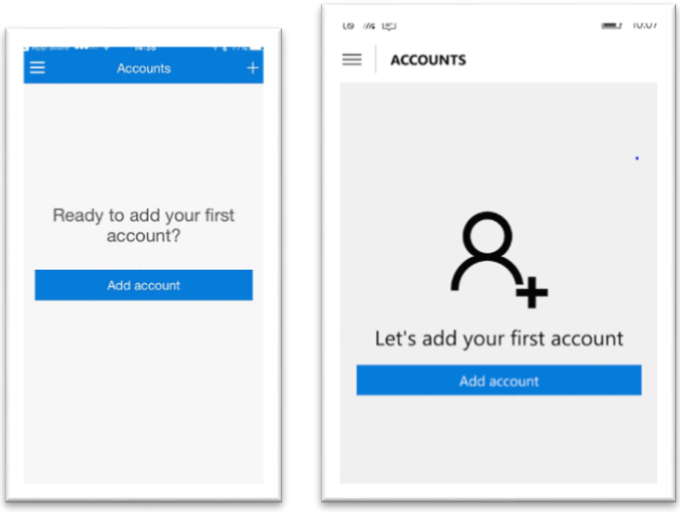
When the **Set Up Your Account** window is displayed, click **"Next".**

This page displays the QR code needed by your phone to link the mobile app to your UoB account.

Keep this page open, and go to your mobile phone.

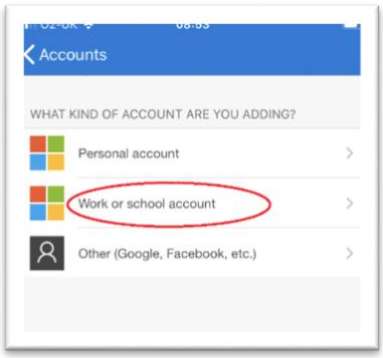
3. Linking the Account with the app

Open the Microsoft Authenticator App on your phone.



Click "**add an account".**

Now select "**Work or school account".**



This should open your phone's camera.

Point the camera at the QR code on the web-page, centring with the red-cross or the blue corners.

The mobile app should now read the code and link it to your UoB account.

You should now be able to complete the set-up.

4. Connecting to AnyConnect

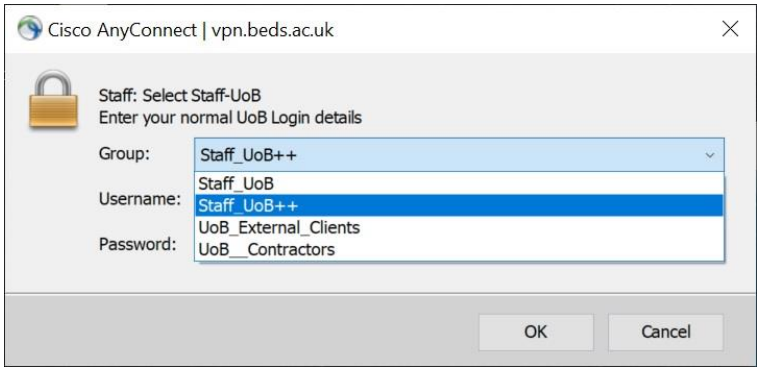
There is a new 'Group' now defined on vpn.beds.ac.uk, which will use Multifactor Authentication.

When you log in, it checks your username and password, and then uses the UoB MFA set-up to get you to authenticate your login via the Microsoft Authenticator App.

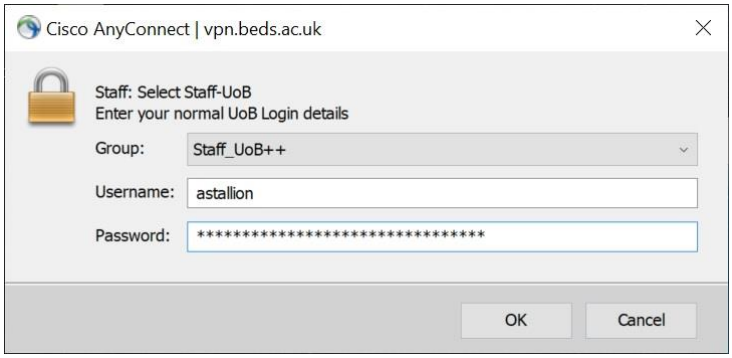
Make sure you have you phone turned on. It saves time if you have the Authenticator already running too.

Connect to vpn.beds.ac.uk as normal:

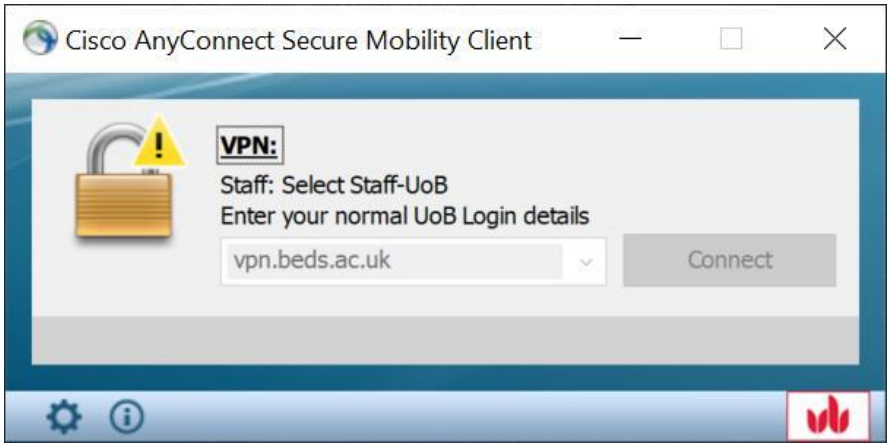
Where you normally type in your username and password change the 'Group' from Staff_UoB to the new Group called **Staff_UoB++.**



Now enter your username and password as normal:



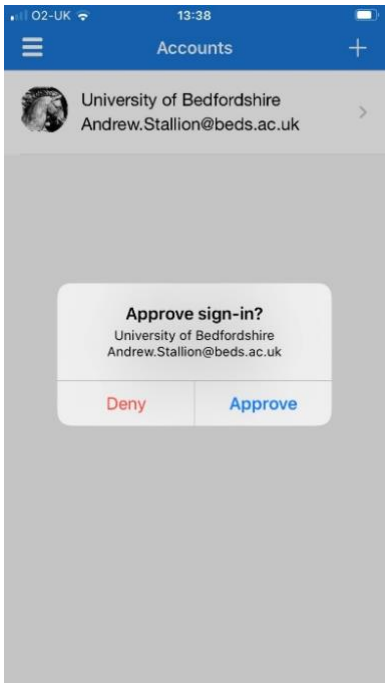
The Cisco login box will display and alert while it waits for the authentication to be approved:



5. Microsoft Authenticator App

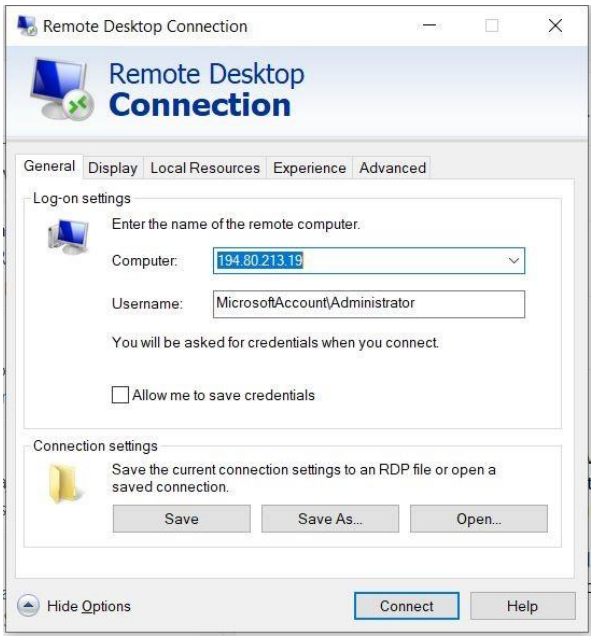
You should get the authenticator asking you to approve the login. This may require your finger/thumb etc before you click on the **"Approve"** option on the phone.

Example from an iPhone:

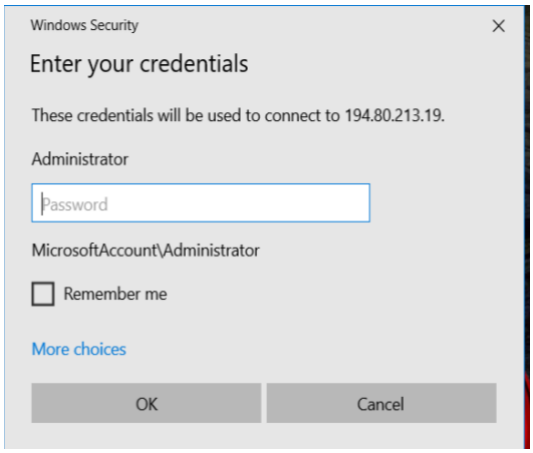


The AnyConnect login should change to *establishing VPN – activating VPN adapter*. You should be connected.

After completing the above steps, you will need to login remotely using remote desktop connection client (just type remote desktop in your Windows search bar, you will find it) and enter credentials as shown in the remote desktop login screen below. For a non-Administrator account, enter the user name provided by the REAMIT server Admin.



Note: you will know that you have a made a successful connection from home if you can see the server login screen as attached in the Figure below. This will let you input a secured password that will be sent to you by the Administrator, Server Login Screen.



5. Data route

5.1: Connecting to Data Sources

Steps to be followed by the internal user for setting up Multifactor Authentication for homeworking

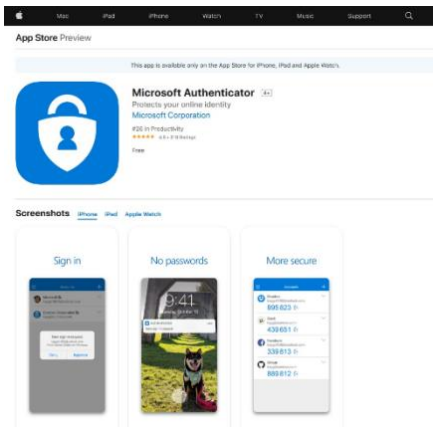
If you are working from home using internet not provided by the university, please follow the procedure below to install the MFA settings on your computer and link your mobile to the Cisco AnyConnect mobility client. This is a prerequisite to connect to REAMIT server from home network. If you are on the University campus and are using the University internet, then ignore this step and proceed to next heading in bold on page 5.

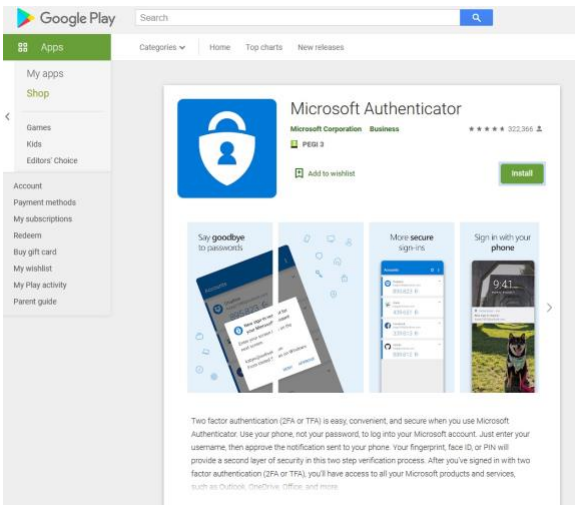
Using the Microsoft Authenticator App with Cisco AnyConnect

Download & an Android phone) and a relevant login for the Apple App Store or Google Play

- Download and install the relevant app for your phone.

iPhone	Android





Configure the Microsoft Authenticator App

This ensures your UoB account is linked to the app on your phone. The two are linked together initially using a **QR code** – your UoB account is used to generate it, and the phone app accesses the camera on the phone to scan this code.

2. Setting up Your UoB account

Connect to the URL: http://aka.ms/mysecurityinfo

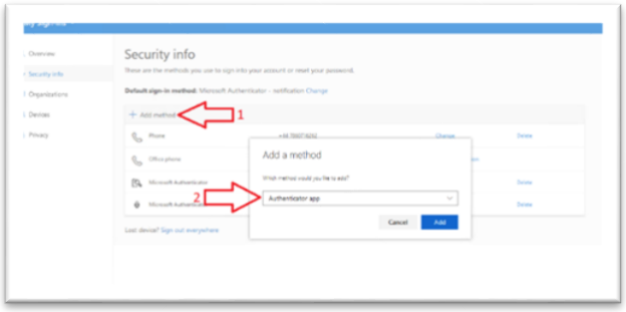
Note: this is a direct link to the relevant page, although you can access this via the web-mail page (Office 365, view account, security info).

Log in at the UoB Single Sign On Page if prompted.

Once logged in it should display the **Security info** page for your account.

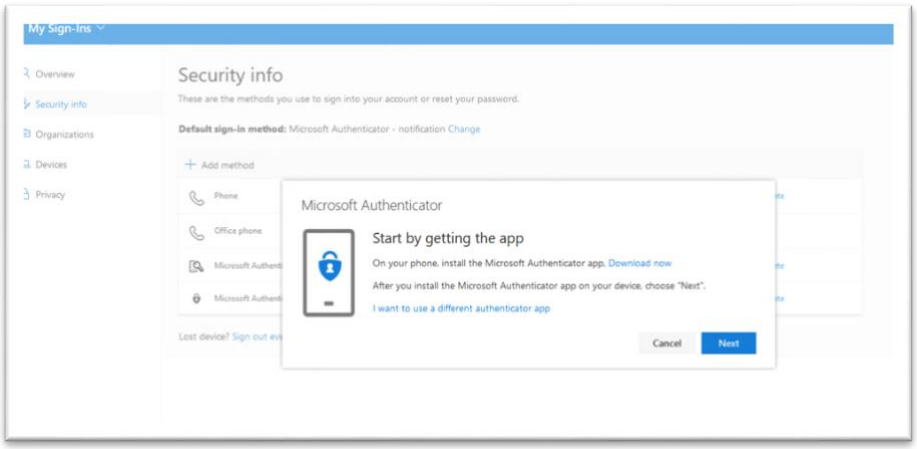
Click:

6. + **Add a method;**
7. select **Authenticator App** from the drop-down.

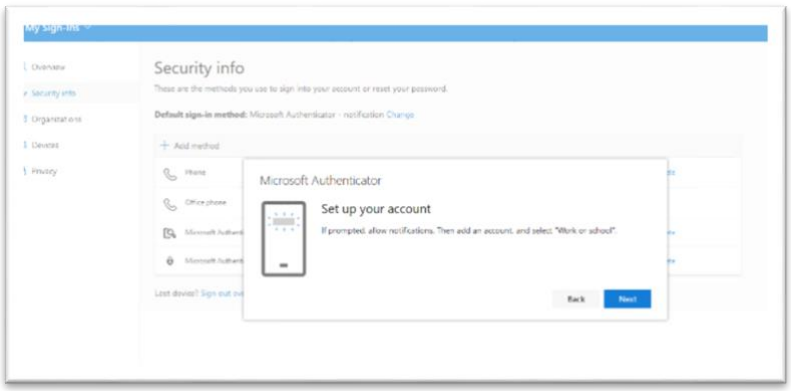


It will now prompt you to download and install the Microsoft Authenticator App for your phone.

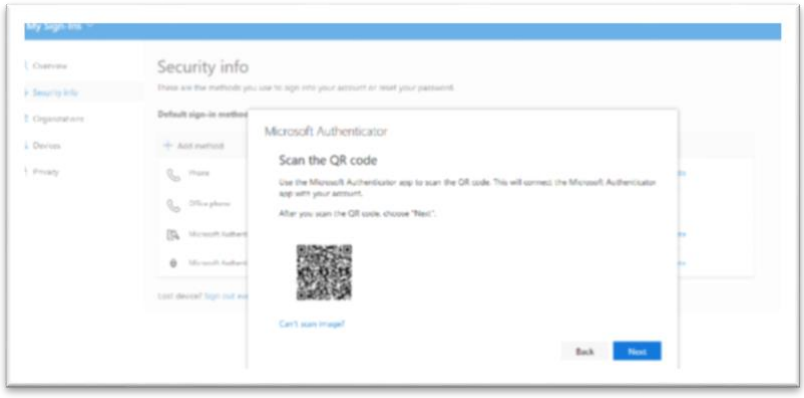
You should have already done this (as described above), click "**Next".**



We are now ready to link the Microsoft Authenticator App with your UoB account.



When the **Set Up Your Account** window is displayed, click "**Next".**

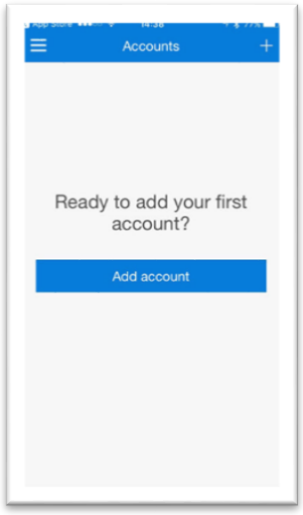


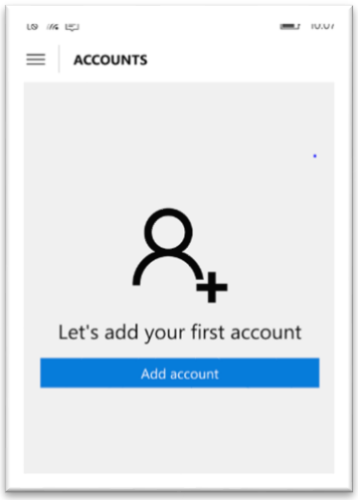
This page displays the QR code needed by your phone to link the mobile app to your UoB account.

Keep this page open and go to your mobile phone.

3. Linking the Account with the App

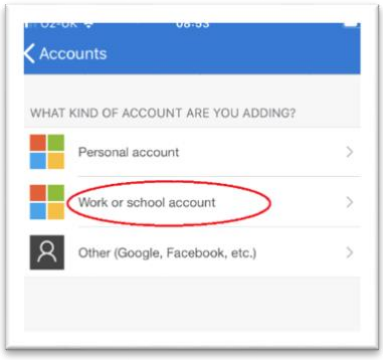
Open the Microsoft Authenticator App on your phone.



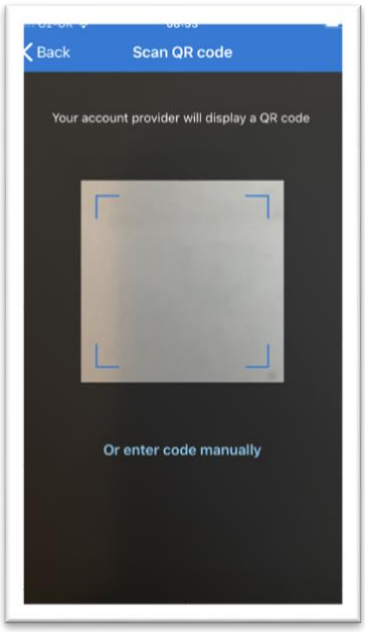


Click "**add an account".**

Now select "**Work or school account".**



This should open your phone's camera.



Point the camera at the QR code on the web-page, centring with the red-cross or the blue corners.

The mobile app should now read the code and link it to your UoB account.

You should now be able to complete the set-up.

Connecting to AnyConnect

There is a new 'Group' now defined on vpn.beds.ac.uk, which will use Multifactor Authentication.

When you log in, it checks your username and password, and then uses the UoB MFA set-up to get you to authenticate your login via the Microsoft Authenticator App.

Make sure you have your phone turned on. It saves time if you have the authenticator already running too.

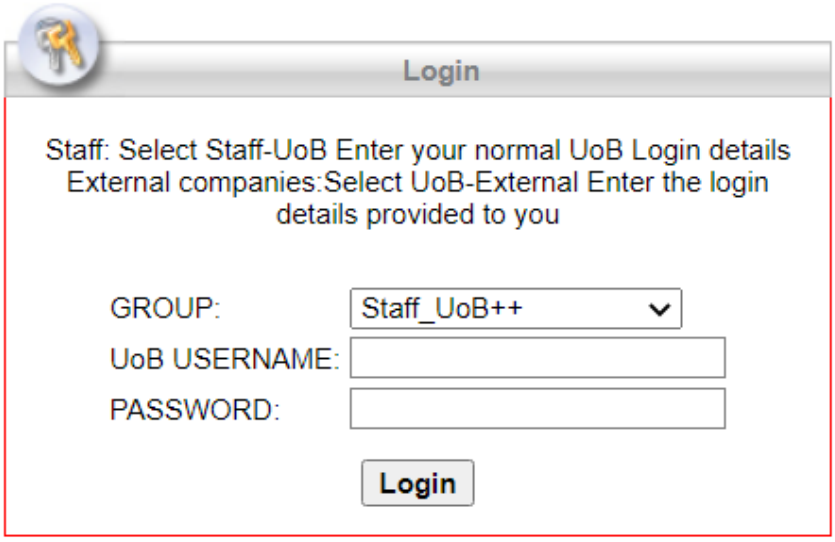
Steps to be followed by the internal user for connecting to BED University network through Virtual Private Network (VPN):

4. **If you are already using the Cisco AnyConnect mobility client**, please note that you will have to do two things differently here while you use the Cisco AnyConnect client; **1. Login using UoB++ account instead of UoB account; 2. Use MFA to approve your login.** You can then directly jump to the next heading in bold on Page 11.
5. **If you do not have Cisco AnyConnect mobility client installed** then, please follow steps as shown below:

    c. Downloading the **AnyConnect Client** from vpn.beds.ac.uk.

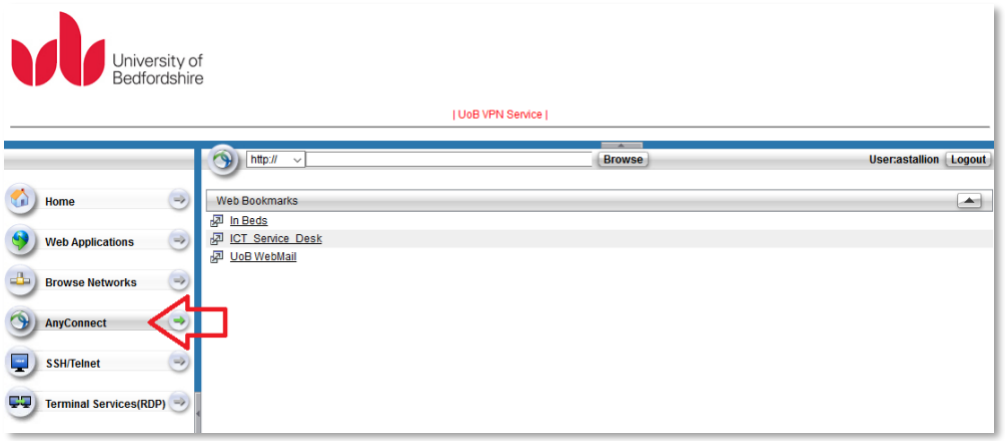
Skip this step if you have the AnyConnect software already installed

- Browse to https://vpn.beds.ac.uk



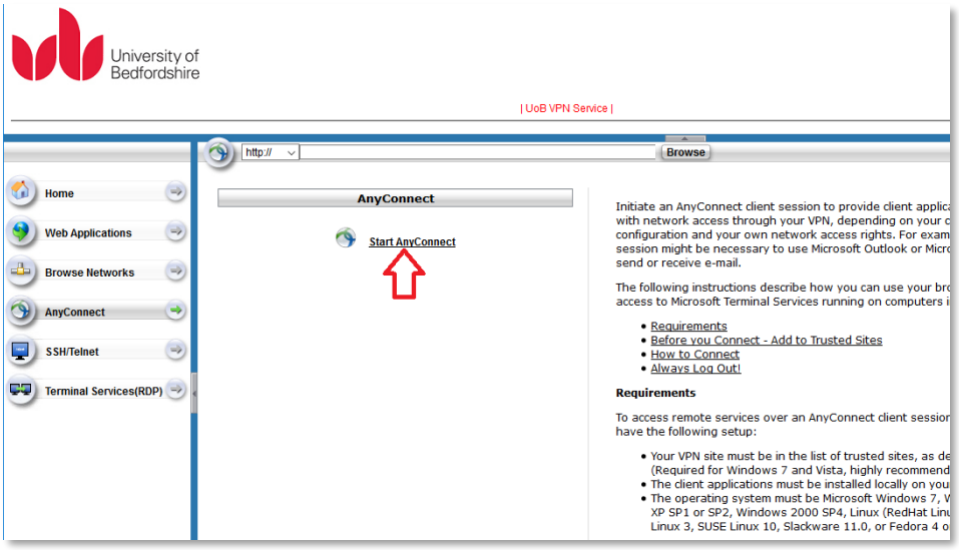
- If the GROUP field does not already show **Staff_UoB++**, use the drop-down menu to select it.
- Enter the staff login details and login.

The initial VPN Web-Page should now be displayed:



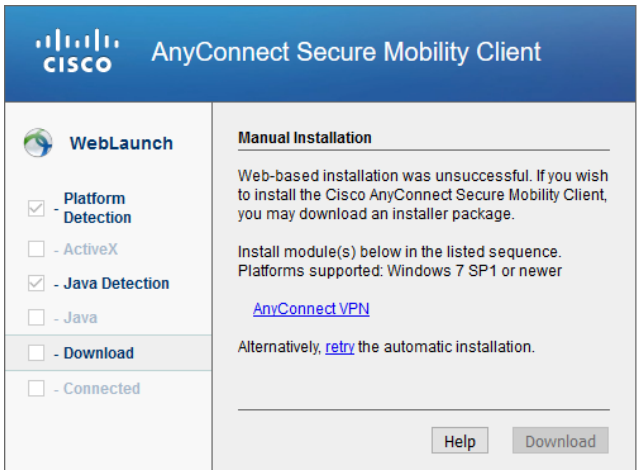
- Click on the **AnyConnect** button on the left.

The AnyConnect Web-Page should now be displayed:



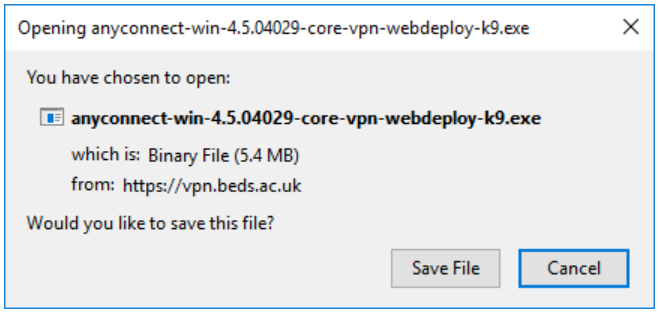
- Click on the Start AnyConnect link.

The web-launch notification window will now open and try to download the client.



- If the download fails (as shown above), click on the **AnyConnect VPN** link.

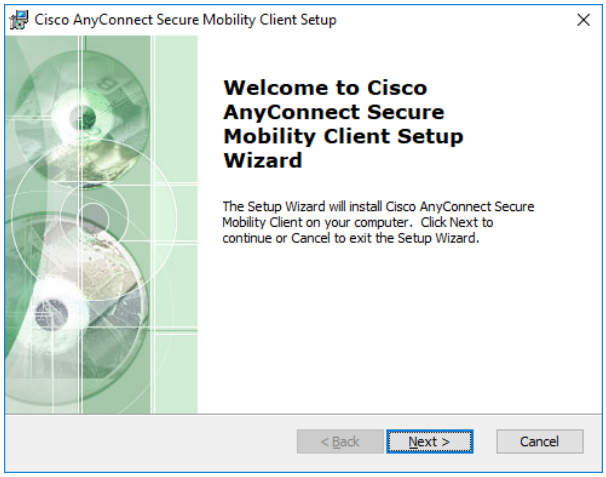
It will then try to download the installation file (as shown below):



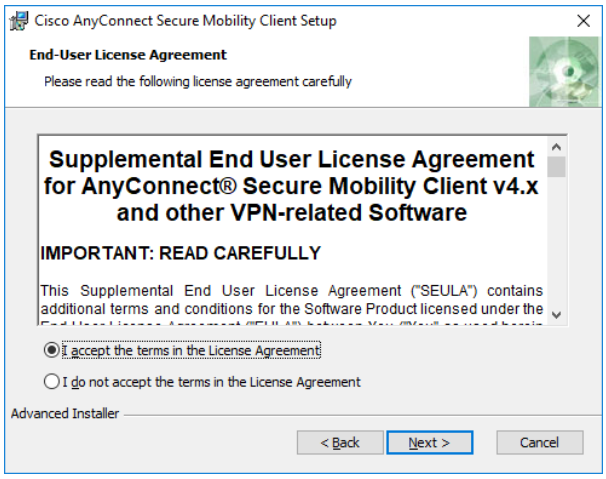
- Click **"Save File".**

The file should be saved to you browsers download location

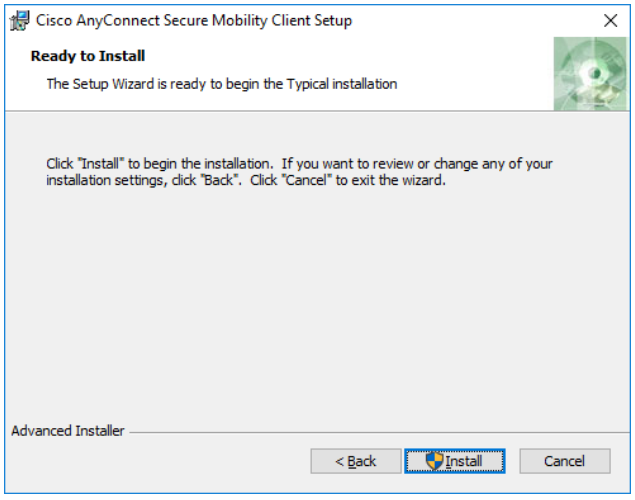
- Open the install executable by double clicking on it.



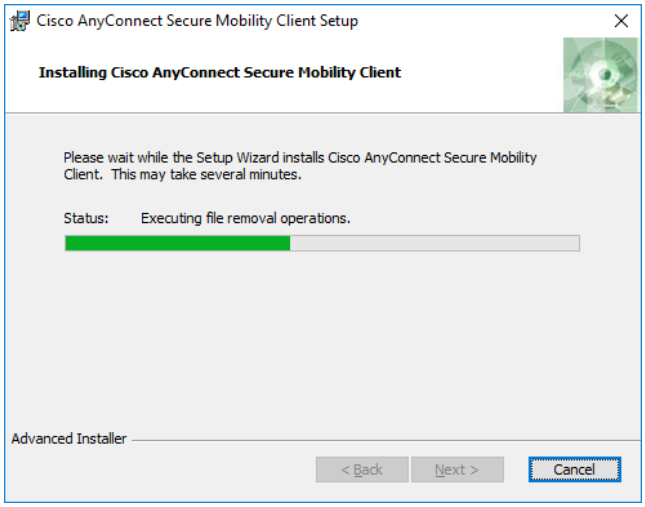
- Accept the Licence Agreement and click **"Next".**



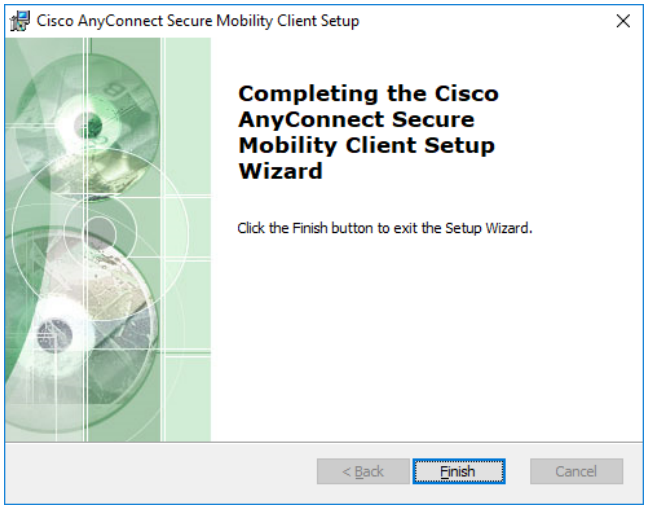
- Click the **"Install"** button.



The installation progress will now be displayed (as shown below):



- Click on **"Finish"** to complete.



- You can now close the browser window.

The software should now be installed on your computer – the location will depend on what version of Windows you have.

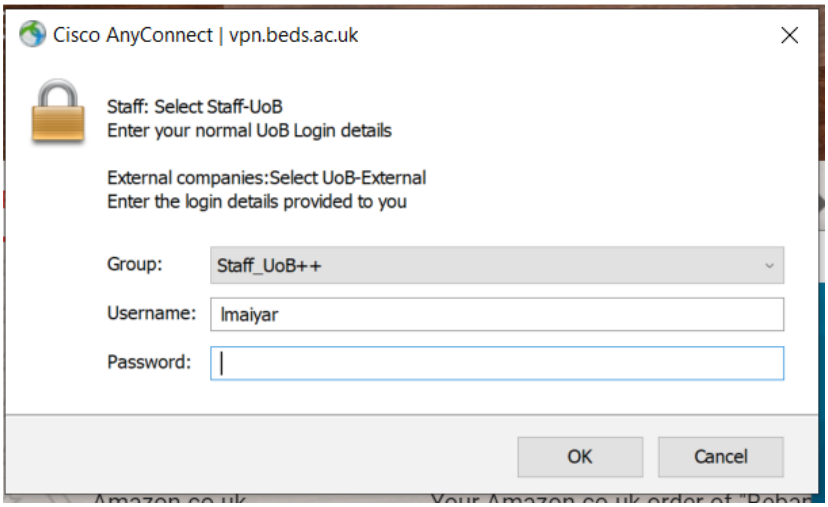
For Windows 10, for example, the application (Cisco AnyConnect Mobility Client) will appear as a drop-down for Cisco Software.

d. Running the Cisco AnyConnect Mobility Client

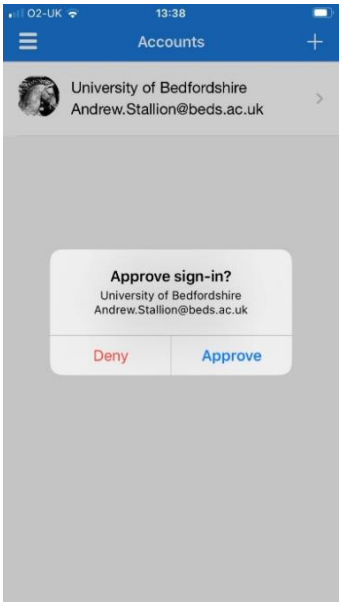
- Launch the AnyConnect client software.
- Enter **vpn.beds.ac.uk** in the destination box and click the **Connect** button.

The **vpn.beds.ac.uk** connection window should now be displayed

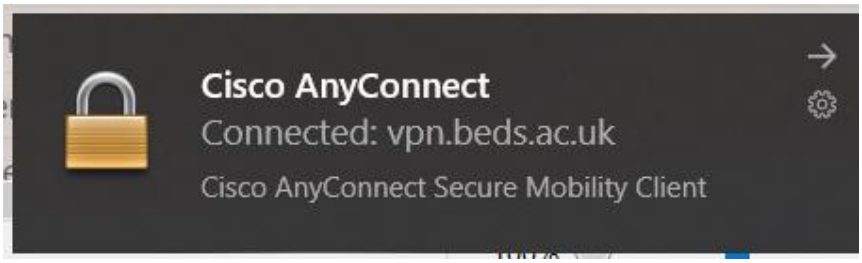
- Select **Staff_UoB++** from the drop-down **Group** box (if it is not already displayed).



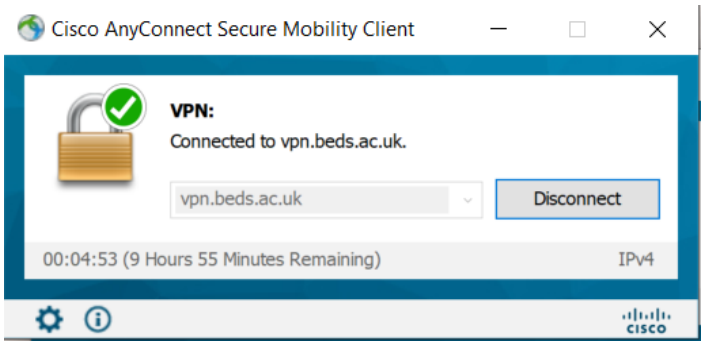
- Enter the **username** and **password** from you staff login and press **"Ok"**.
- Click on **"Approve"** when you receive a notification on the mobile for the **Multi Factor Authentication**.



- You will receive a notification that you are connected via Cisco AnyConnect on your computer if you have notifications turned on.



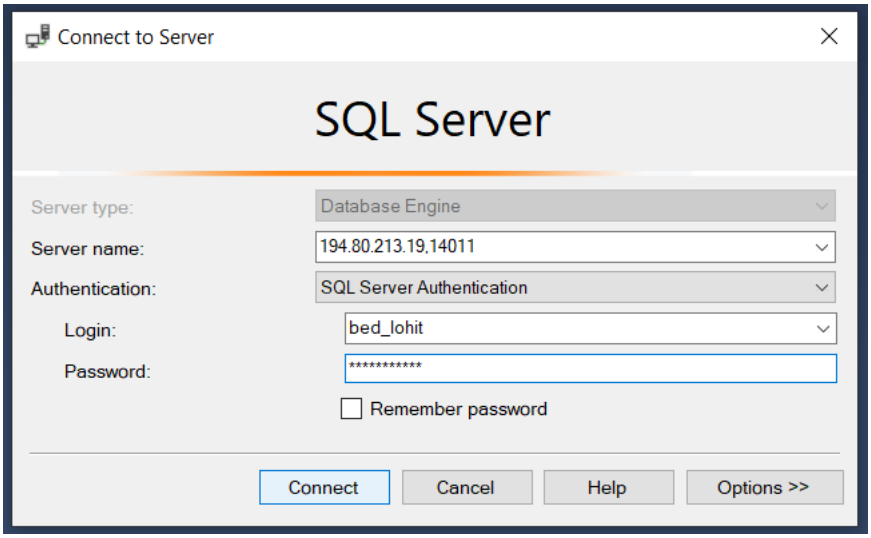
You can also have the successful connection confirmed from the following appearance of the Cisco AnyConnect window.



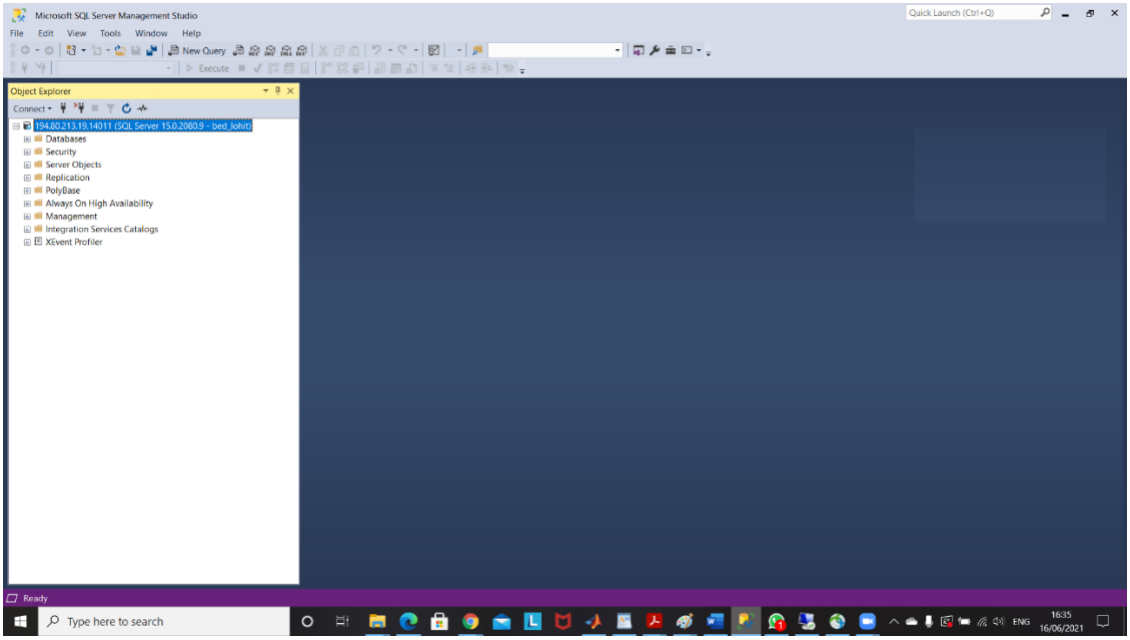
You should have access to the required internal resources from now on.

Steps to be followed by the internal user for connecting with the MSSQL shared database instance on the REAMIT server:

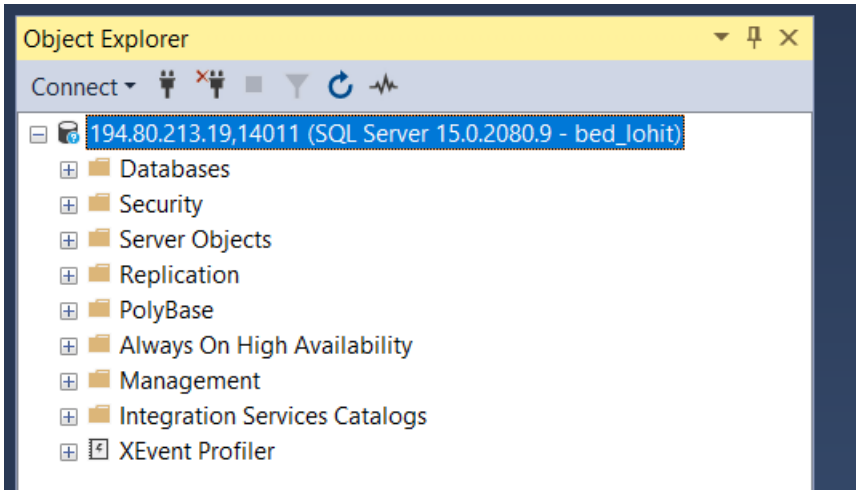
1. Connect to the BED network by logging in through the VPN client access provided by BED.
2. Open **Microsoft SQL server management studio 18**. You can find this by typing this in your Windows search bar if you already have it installed. (If you do not have it installed on your computer, you can download and install the software from https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?redirectedfrom=MSDN&view=sql-server-ver15). Feel free to use the server management software of your choice. For example, if you are comfortable with Azure Data Studio (found default in all Windows systems), please kindly proceed with this and use the appropriate login credentials. The steps enlisted here are based on a tested connection protocol using Microsoft SQL server management studio 18, that is used more often.
3. In the “Connect to Server” login window:
   Select the Server type: “Database Engine”
   Enter Server name: 194.80.213.19,Allocated_Port_number
   Select the Authentication: “SQL Server Authentication”
   Login: <<<name of the user provided to you by the REAMIT server system Admin>>>
   Password: <<<Would have been shared to you via text message by REAMIT server system Admin >>>



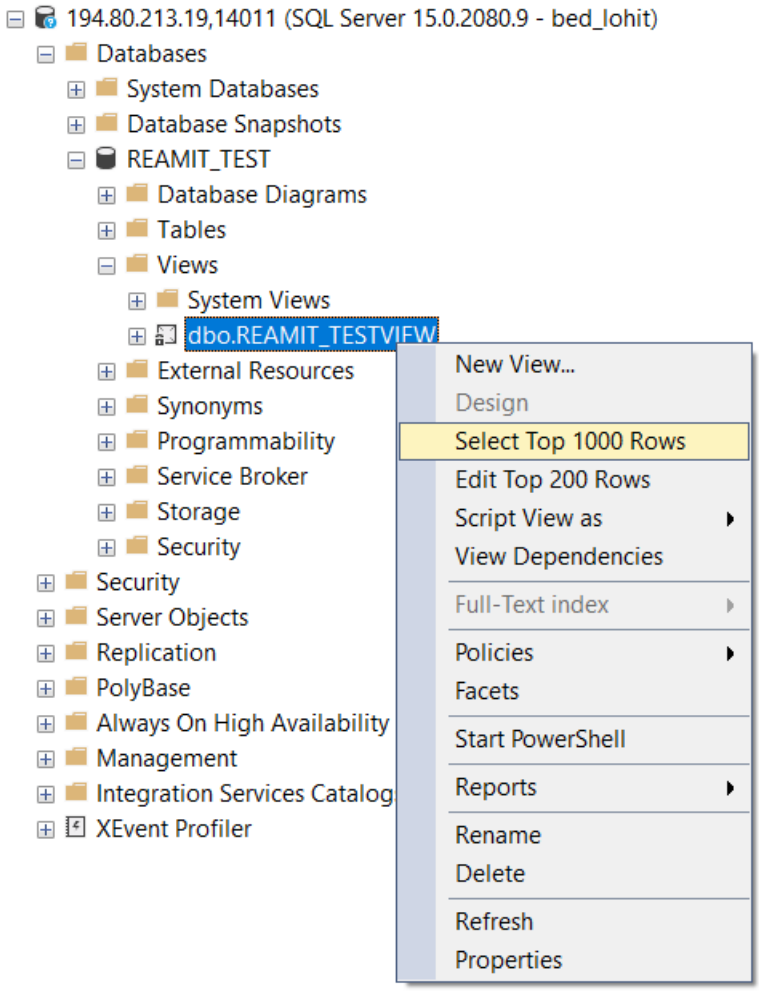
4. Click **Connect**. You will be asked to change your password. **Please change the password as soon as after the first login when prompted on the screen.**
5. Once you establish a connection the database engine connection window must disappear and take you to the below screen that provides read and download access to the REAMIT_SHARED instance on the top left corner of the MSSQL studio interface.



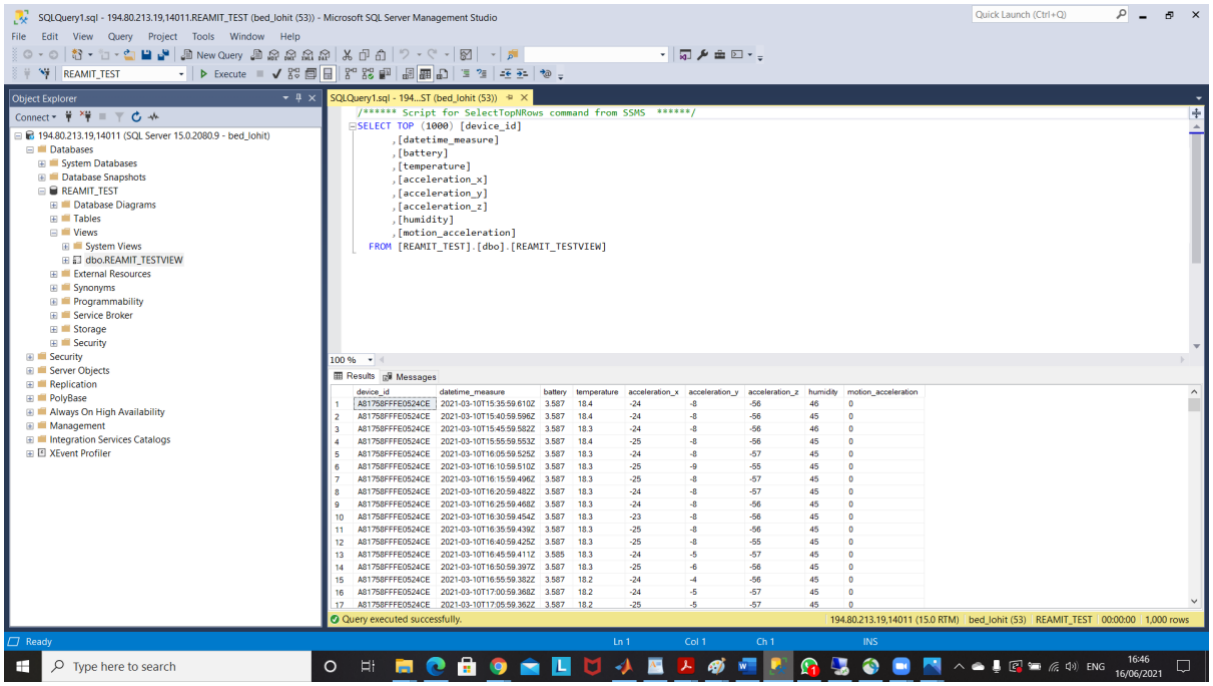
6. The object explorer on the top left will look as below:



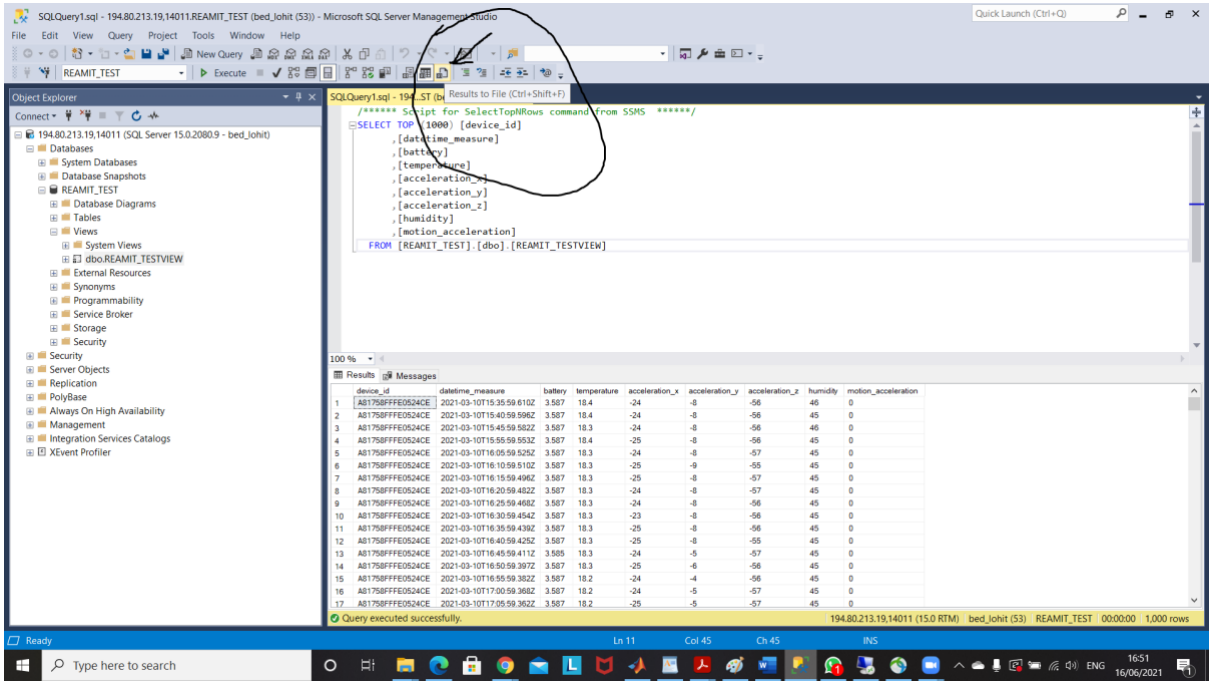
7. To view sample data, please go to **Database>REAMIT_TEST>Views>Select Top 1000 Rows** as shown below:



You should be able to see the below screen showing first 1000 rows of data available to view (as below):



8. To download the data to your laptop or computer, click **Results to File symbol** on the top of the screen as shown in the below picture. Follow the onscreen instructions to download the data in the required format.



Disclaimer: *This document was prepared by XXX (email) to the best of xxx knowledge, in association with the REAMIT project team. All information provided in this document are verified and found correct at the time of publication – June 2023.*