

Security Token

If this is your first time using the remote access login, you will have to register your security token before login. You will only need to do this once and will require you to connect to the company network or contact the IT Service Desk.

- Requesting a security token
- Registering your security token
- Using your security token
- How does it work
- Contact the IT Service Desk

Requesting a security token

By accessing the "Order a Product or Service" service available from your company intranet, you will be able to request any of the available types of security tokens:

- Defender token
Global Remote Access (Defender GO-6) 2)
- Soft token
Can be installed on a suitable mobile device (either personal or company issue), replacing the need to carry a separate security token. The current choices are:
 - Global Remote Access (iPhone Token) - requires iOS 5.0 or later
 - Global Remote Access (Android Token)
 - Global Remote Access (SMS Token) - can be used with "non-smart" mobile phones to receive unique codes sent via SMS to remotely access our systems

Once you have requested a token, you will be sent an email containing instructions on how to register it.

Registering your security token

Before your security token can be used it must be registered on our system; you will only need to do this once.

To register a physical token you'll need your token with you, if you are registering a "soft" token you will need your mobile device with you; you'll also need to be connected to our network. We recommend you register your token while in the office, it will then be ready to use when you need it.

To begin the registration process launch your company intranet, click on the Tools menu, then click on the Security Token Self Registration System option.

You will then be guided through the registration process. Registration takes several minutes, and once registered your token can be used to access our network. During the registration process you'll be asked to set a PIN code, please remember this PIN and do not disclose it to anyone.

If you experience any problems during registration, or would like us to do this for you please contact the IT Service Desk (details can be found below).

After registering your security token you will be able to use your security token.

Using your security token

If you're using a company laptop you can use the relevant VPN software along with your security token to make a secure connection to the office.

If you're going away for the first time it is always a good idea to call the IT Service Desk and ask them to check to make sure your VPN software is configured correctly. This could save you a lengthy telephone call to the IT Service Desk at a later time. If you're not using a company laptop, or if VPN is not supported at your location you can use an internet enabled PC to connect to Citrix or access your email via Outlook Web Access.

All you need to do is visit your company internet site and click on the Remote Access Login link in the top right hand corner. Once connected to this page you'll see several options depending on your location, select the most suitable.

How does it work?

Two-factor authentication is an approach to authentication which requires the presentation of "two or more" of the three authentication "factors" ("something the user knows", "something the user has", and "something the user is").

The first factor is your PIN number - "Something you know". The second factor is the token itself, the code it generates is - "something you have". This combination helps us verify your identity. To generate the code just press the button on the front of the token and a code will be displayed for several seconds. If you miss it just press the button again.

You'll notice that the code will change frequently. There's no need to turn off the token it will turn off automatically after several seconds.

You'll be prompted to supply your user ID, password and Security Token code. Enter your user ID and network password as normal and your Security Token PIN and the code it generates. The user guides may be helpful the first time you login.

Multiple attempts to login without success will disable your security token. You will then need to call the IT Service Desk for assistance.