

Secure Remote Access

As part of the comprehensive support package we provide to each of our clients, Perceptive will access the daily log files written by our software. These give us a detailed insight into operational performance, allowing us to :

1. Assess and analyse historical data for fault-finding and troubleshooting
2. Generate management reports and performance data
3. Quickly identify and resolve any queries regarding process control
4. Identify opportunities for further process optimisation and improvement

We understand that the security of your plant and processes is paramount. For your piece of mind, we have put in place a rigorous methodology for ensuring the safest possible remote access, which is used to help our clients all around the world.

First, we always adopt procedures which the client has already put in place. If no procedures yet exist, we offer detailed guidance and advice, based on many years of practical experience.

Second, remote access is provided from a **designated office** within our secure building. Only with your express permission will access be made from any other location.

Third, we gain approval from the designated customer contact **before** remote access is attempted and **before** any changes are made to our on-site system.

Here are some of the most common methodologies we adopt:

- Citrix remote applications, with **VNC** (virtual network computing)
- Citrix remote applications, with **Remote Desktop**
- **VPN** (virtual private network), such as Juniper, Cisco Systems, CheckPoint Endpoint Security
- **VPN Tunnel** - used with Radmin for remote desktop access. These VPNs typically utilise a SecureID keyfob which generates a random 6 digit passcode, providing a further level of security.
- **'Air Break'** of permanent connection via VPN. Remote access can only be achieved when the client physically connects our PC to an Ethernet router/firewall.

