

CC IT Development



Network Secure Gateway

The Network Secure Gateway has been developed in partnership between Burconix Ltd and Lode Heath School High Performing Academy.

Secure Remote Access to all your IT Systems.

Simplifying IT Access

Benefits quick point

- Low cost, simple, seamless access, **remote access** to IT Systems
- Secure Access
- Using Windows Technologies
- Reduce Data Protection Issues
- Less issues with created resources not working
- Flexible working
- Increased productivity
- Reduced Costs
- Possible alternative to other systems you may have
- Simple access to everything
- Access in event of Staff absence
- Controlled Access
- Consistent Environment
- No need to copy files to the network less issues with Viruses, Trojans etc.
- Data is consistently backed up, less chance of Data loss.



Benefits of the Network Secure Gateway

Secure remote access for Staff to all their resources and systems 24 hours a day 7 days a week, if required the same as if they were at a PC in at work (**which they actually are**), The system uses HTTPS, SSL externally and uses an RDP connection internally with SSL traffic only tunnelled to this connection on a single port.

Developed to work with Windows Technologies and built to work with these seamlessly and using dual factor Authentication **where required** using an Encrypted key.

Secure Access to your systems and data means that there is no need to take data off site so reducing Data Protection issues.

Staff can work from home remotely and no issues with forgotten or lost USB flash, Portable Hard drives, laptops.

Flexible working for Staff, as they can leave on time and work from home when it suites them if they need or wish too.

In cases of Business closure due to poor weather or other circumstances Staff would still have access to IT resources and systems.

One simple way of accessing everything so reducing the number of systems you may require and can reduce compatibility issues.

Staff not able to attend work could still have access to IT systems.

Control which users can access which PC's, Resources and what times.

A Consistent Environment for the organisations systems users.

No need to copy Files onto the Network as you can work on documents live less issues with Viruses, Trojans etc.

Data is worked on and stored on the Network so data is backed up consistently using the organisations backup methods, less chance of data loss on USB sticks, Laptops etc.

Staff can use the system to demonstrate other software systems live by logging into their own environment within their organisation and demonstrating software using just an internet connection.

Network Secure Gateway how it works Quick points

Network Secure Gateway how does it work?

Uses SSL over HTTPS externally and uses an RDP connection internally with SSL traffic only tunnelled to this connection.

Staff go to the Secure Gateway and Login with their Username and Password.

Access to MIS and other systems for Staff

Certain Staff can Access resources by running an Encrypted App that can be run from USB, PC or laptop off site.

Network Secure Gateway how does it work?

The system has various layers of security that are hidden from the user, so as not to interfere with the user's seamless experience. In essence it uses SSL encryption over HTTPS similar to banks or internet secure payment sites and uses a single HTTPS port as well as other in built security. It uses an RDP connection internally with SSL traffic only tunnelled to this connection which uses only a single port.

Access to computer systems for Staff

Staff can have access to resources within the organisation, Staff will just need to go to the Secure Gateway website and login with their Network Username and Password and obviously they would only have access to the resources they would have access to normally. You can also create add an extra layer of Security by using the Encrypted App (see below)

Access to MIS systems or Specific Systems

Access for staff by using a small encrypted App that is generated for staff this does not need to be installed and can be given\copied onto a USB Memory stick, CD, DVD etc. The App can be copied by the user onto their home PC or Laptop or just run from a USB Memory Stick.

You double click the App this takes you to your Secure Gateway and Verifies the Encrypted App against the Encryption software on the Server, so first method of Authentication.

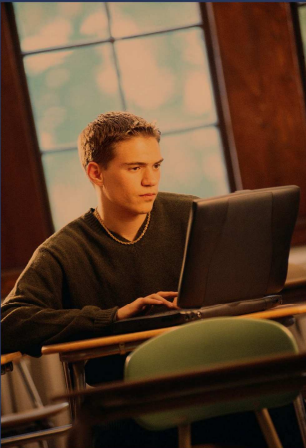
The user then signs in using their Network Username and Password and selects the Computer they wish to access and is automatically logged in as if they were in work. The username and password being the second level of Authentication, **which is all the user has to enter.**

This means using this method staff can access MIS resources\systems that standard users can't.

This means that a member of staff can securely login to a computer from anywhere in the world they have access to the internet.

Features of the System

- The system links with Active Directory, so retains all permission's, security etc.
 - The system is extremely configurable and allows you to change options easily.
 - Built-in security layers.
 - Uses SSL Encryption HTTPS, it uses an RDP connection internally with SSL traffic only tunnelled to this connection which uses only a single port.
 - Provides various reports\logs, on who has accessed the Gateway, failed logins, these can be exported to excel etc.
 - Allows you to control who has access to what and at what time.
 - You can setup the software on your own Server or purchase a preconfigured system which will be
- Auto Start-up of PC's that have Network Boot up enabled when required for remote access.
 - All of these features and much more are explained in more detail in the User guide.
 - Auto shutdown of PC's that are not being used, which is configurable, scheduling etc.
 - Auto log off of user after a certain time which is configurable.



CC IT Development

Simplifying IT Access