

# Solution Guide:

## Secure Wireless Network

### Why wireless should never connect to corporate LANs

#### Executive Summary

Many wireless networks in the world are not protected and those that are can easily be hacked. This leaves thousands of corporate networks vulnerable to attacks and eavesdropping resulting in the theft of personal and commercial data.

A great number of companies are responding to this issue by banning any form of wireless access in their offices.

Without wireless connectivity user frustration goes up and productivity goes down. Companies have invested in laptops for employee mobility — but in reality there is no mobility without wireless access.

The mistake the industry is making is to use wireless networks to access corporate LANs — that is wrong. Wireless networks should only give access to the Internet.

Because G/On provides secure connectivity across any network — including wireless, companies with wireless Internet access in their office can use G/On to give their employees access to the applications they need. To become mobile in the office, employees always connect remotely — even from their own offices.

The benefit of this approach is that companies can realize the full potential of wireless networks and leverage their investment in employee laptops and mobile devices.



### Solution Highlights

#### Benefits

- Makes wireless networks useful and secure
- Users become truly mobile within corporate offices
- IT-department can pre-configure laptops

#### Recommended configurations

- Wireless access to the Internet
- Use G/On Desktop on all laptops for access to corporate applications
- Users should also have a G/On USB for remote access from other PC's.

#### Requirements

- Citrix Server or Microsoft Terminal Server
- Windows Server 2003 for the G/On Server
- A PC/Laptop with Windows XP or Windows Vista for the remote PC.



## 1. The challenge

Wireless networks are increasingly popular with users because they make PC's a lot more user friendly. The built-in receivers in laptops make it very convenient for users to be on-line without dealing with cables and finding wall plugs that work.

Wireless is also a very convenient way for companies to provide connectivity in office spaces, in shopping malls and other places where cabling is too restrictive or too expensive.

Unfortunately, wireless networks are very difficult to protect. Numerous cases around the world have shown that hackers can hack their way onto a wireless network and also further into corporate networks.

Consequently, many companies are no longer allowing the use of wireless networks and merely consider it a technology for public Internet access in hotspots, café's, airports and other places like that.

Banning wireless networks in the office is causing a lot of user pain and frustration. People are fighting for network cables in meeting rooms while stumbling around cables that are spread across floors. Visitors can't access the Internet let alone their own office. Corporate fear of wireless even goes as far as banning any form of company access that involves a wireless connection, for example an employee accessing from home.

A wireless network is a wonderful tool if it is used correctly. The mistake the industry is making with wireless networking is to use it for access to corporate LANs. By design, a wireless network cannot be forced to stay within your company walls and consequently it can be tapped into by the wrong people.

## 2. The Solution

The right way to use a wireless network is only for access to the Internet, even if you deploy it from inside your own offices. Nevertheless, your wireless network shouldn't be open for everyone's use. You should protect it to the level that fits your needs. You may want to offer visitors easy access to the Internet without making it too complicated for them to connect. On the other hand, you don't want strangers to be able to use it. However, if strangers do connect, or if "bad guys" are able to get on, you know that they only have access to the Internet. That's it.

But since your wireless network is connected to the Internet, you can use G/On for secure access to your corporate applications. G/On gives your employees the flexibility and mobility to stay connected at all time as they move around your premises.

Your employees will soon discover that it's easier to always use G/On to connect. This is how they connect from home and when they travel and it becomes a convenient way for them to get access to those specific applications they work with all the time.

If you have remote locations or offices, you no longer have to create a separate LAN for such locations. All that's needed is a wireless network with Internet access. Employees will then connect through G/On and get access to those corporate applications and tools they require. G/On in combination with wireless networks will reduce your costs considerably when you establish new offices and locations. If you set up all your wireless networks with the same network ID, encryption mode, and encryption keys, all your employees will automatically connect regardless of which of your offices and locations they visit. That saves time and removes user frustration in trying to connect to the wireless network. In fact, you can pre-configure all your laptops so employees don't even have to know the network ID and encryption keys. They just connect.



### 3. Benefits

Wireless networks are simple to install and if they only give access to the Internet there is less to worry about from a security standpoint. And the benefits are tremendous. Visitors to your office will have easy access to the Internet and they can use their own tools for remote access to their office without compromising your corporate LAN.

You use G/On to provide your employees with wireless access to your corporate applications the same way you would use G/On for remote access. Users can move around freely in your offices and be connected all the time.

If you have multiple locations and offices it is very easy to get people up and running in these facilities. Especially, if you have one common corporate configuration for all your wireless networks.

G/On and wireless Internet access is a very effective and productive for users as well as for the IT department.

### 4. More Information

The G/On USB is a combined authentication and connectivity device. It can also be used as a storage device for those application clients that the user needs to launch to connect to the corresponding application server.

One example is a Citrix client. Normally, the Citrix client needs to be physically installed (through an installation process) on the remote PC. However, in many cases, it's not an option or simply not possible to install the full Citrix client on any PC you want to use for your remote connection.

Giritech is addressing this issue by working together with Thinstall which allows us to create a special packaged version of the Citrix client fully integrated with G/On. This makes it possible to bring along with you the full Citrix client on the G/On USB and consequently turning Citrix into a true portable and secure remote access solution.

See also Giritech Solution Guides for Working from Home/Tele Commuting, External Consultants/Outsourcing, and Access to your office Desktop.

Giritech A/S | Herstedøstervej 27-29 | 2620 Albertslund | Denmark | [www.giritech.com](http://www.giritech.com) | + 45 70 277 262

Giritech reserves the right to change the information contained in this document without prior notice. Giritech™, EMCADS™ and G/On™ are trademarks of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property currently includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. © Giritech A/S 2005, 2008.