



TECHNICAL FACT SHEET

G/On

G/On is a client/server application based on Giritech's EMCADS technology.

The G/On Server is a small footprint Windows server application. It is typically installed on a dedicated server behind the main perimeter firewall together with the network's application servers. It's primary tasks are to:

- Authenticate G/On clients ("something you have")
- Verify users (based on username and password - "something you know")
- Encrypt and decrypt data (using 256-bit AES as default)
- Push out menus to users
- Connect clients to applications

The G/On Server includes a comprehensive set of tools for connecting to different applications, and defining precisely how each user can access those applications based on different parameters.

Installation

It is recommended that the G/On Server be installed on a dedicated server behind the main perimeter firewall.

After inserting the G/On Server USB token provided by Giritech in the server, the installation CD-ROM is used to install the application.

Only one port (configured in through mode on the firewall, directed to the EMCADS listen tcp port) needs to be opened.

Setup

Once installed, a GUI tool called G/On Builder is used to set up the G/On Server. This involves working through 5 tabs, specifying details about the server, the user directory, the G/On client and how to update them, and Active Directory synchronization. Once this has been done, the G/On Server license can be activated, upgraded or renewed.

Configuration

The G/On Server is now ready to be configured for operation. This involves using G/On Admin to:

- Import users and groups from Microsoft Active Directory into the G/On Server.
- Create Zones i.e. rules that specify which menu a user is provided with depending on where they log on from (IP address with subnet mask) and/or the device they are using (based on unique identifiers about that PC or USB key).
- Create the application strings used to launch applications

and programs on either the server or the client

- Create the menu actions specifying server names and other necessary parameters for the applications you want users to be able to launch.
- Assign menus to groups, test them and deploy them.

Application Connectivity

The range of applications that G/On can connect users to is broad and includes:

- Directly to users' Windows Desktop on their own office PC
- Server-based computing platforms such as Microsoft Terminal Services, Citrix and mainframes
- Client/server applications such as Navision, SAP and Lotus.
- Web Browser based applications
- Any other application that uses TCP/UDP traffic

(Note: Configuring the G/On Server to access these applications can require minor modifications which Giritech's Certified Partner can assist you with.)

The G/On Clients

There are two G/On Clients: the Desktop Client and the USB Client. From the administrator view point they are basically the same and can be treated as such, when it comes to deploying applications and menus.

G/On USB offers maximum mobility and can be used from any Windows PC that meets the basic technical specifications, and has a tcp port open to the Internet. It can carry its own versions of the needed clients, and is made to autolaunch when inserted, making it very user-friendly.

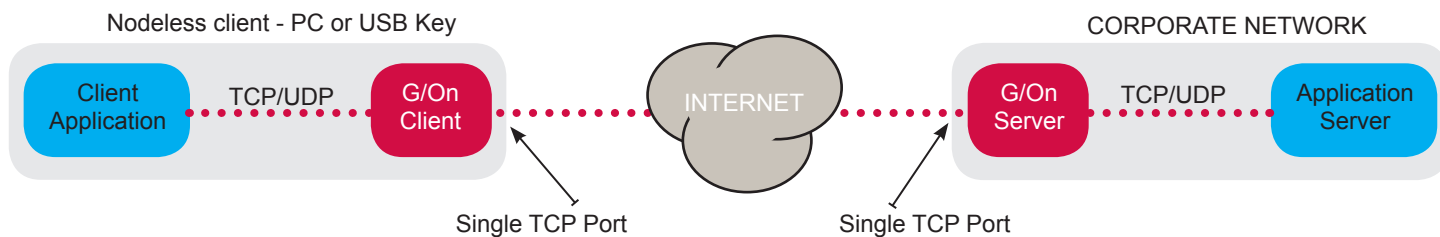
G/On Desktop is installed on the PC hard drive as a normal application, and places an icon on the desktop for the users to activate when they want to access a remote application.

G/On USB offers maximum flexibility and productivity, enabling users to connect from virtually any Windows PC. The G/On Desktop client is an economical alternative for users who always connect from the same PC.

Deploying the Clients

The G/On USB keys can be distributed by post or in person. G/On Desktop clients can be sent by email or pre-installed on corporate PCs.

The first time users log on, the IT administrator must confirm the connection and register that they are now part of the system. This one-time only "adoption" process is essential for ensuring the validity of G/On's 2-factor user authentication.



This diagram illustrates the minimal requirements needed for G/On connectivity. Only one TCP port needs to be opened on any firewall between the G/On client and the G/On Server. The device

hosting the connection never becomes part of the network where the G/On server is located.

The G/On Connection Process

The G/On Server has one TCP port open for incoming connections and forwards the relevant parts of incoming connections to the applications on the network that it is configured to use. This only occurs once a connection has been established.

The G/On Server first authenticates the G/On client - either G/On USB or G/On Desktop - based on the unique USB serial number or various unique identifiers about the PC that the G/On Desktop client is installed on. It then checks for connection rules, allowing or denying access to that client.

If it can confirm that the G/On client belongs to its "family", the G/On Server then authenticates the user, either against Microsoft Active Directory (AD) or if AD is not used, G/On's own internal user directory (called EDMS), based on the user's network username and password. The AD is not queried until the G/On Server verifies that the user exists in the EDMS. The AD is never exposed, and the passwords are never stored outside the AD.

Depending on the AD groups that the user belongs to and the zones that the connection matches, specific menus with applications and/or gateways are presented to the user. The administrator can also make menu items auto-launch when the connection is established.

Deployment and Upgrades

Upgrading the client software involves using the G/Update client, deployed as part of the G/On client package.

The G/On Server can be configured to "force" an update i.e. the user is not allowed to connect until they have received the

latest software. Alternatively, the G/On client can be allowed to check for updates and download them when suitable.

Dynamic Menus

Changes to user's rights and privileges are typically enforced within 60 seconds of them being made in G/On Admin or after synchronization with Active Directory.

This means new applications can be made available on-the-fly with no user intervention – even during a session.

G/On Zones

G/On uses Zones to help regulate which applications users can access as well as the level of access based on where they are logging in from (i.e. their IP address) as well as which PC they are using to host the connection.

This means, for example, that when people connect from "trusted" networks and/or PCs it makes sense to give them full access. If they log on from an Internet Hot Spot i.e. an "unknown" zone, you can configure the G/On Server to only let them read their email in a terminal session, for example.

There's no limit to the number of Zones that can be defined, or the number of rules used to define them.

Logon Security Features

To enhance the security of the authentication process, the G/On Server can also be configured to enforce different features designed to hinder scripted log on attacks.

These include an onscreen keyboard, randomly positioning the logon dialog box on the screen, disabling the ability to tab from the username field to the password entry field and making the Cancel button the "OK" button.