



FEATURES AND BENEFITS

Feature	Description	Benefit
2 client options - G/On USB - G/On Desktop	G/On clients can be deployed either on USB keys provided by Giritech or on a Windows PC. Supported platforms are: <ul style="list-style-type: none">• Windows XP SP1• Windows XP SP2 (with Hotfix KB884020)• Windows 2000 SP4	Gives customers the choice between high mobility and cost-effective convenience.
256-bit AES of all data	G/On uses the Advanced Encryption Standard (AES) to encrypt all data that it carries. Nothing is transmitted in plain text – the system is simply incapable of sending anything that isn't encrypted. (Note: This is the default encryption scheme. G/On is prepared for using other encryption schemes but this would require customization.)	AES offers a good balance between the CPU power needed to do the encryption and the need to have real time communication between clients and servers.
Account lockout on failed login attempts	If a user logs in incorrectly 5 times (default) they will be locked out of the system. The setting can be between 0 (no lockout) to a maximum of 25 failed attempts.	Improves logon security by making it harder to use dictionary attacks to "guess" a user's password.
Active Directory support	G/On can interface with Microsoft Active Directory, enabling IT administrators to use this existing registry of users and groups for setting up their G/On users.	Speeds up installation and configuration process. Reduces operational workload by only requiring IT admins to make changes in one system
Application Access	Only connects users to specific applications – not the network i.e. this is true virtual connectivity.	Minimizes risk to network if an unauthorized user does manage to find an EDC + username and password. Restricts what an authorized user can do if they want to do something on the network that they're not explicitly authorized to do.



Application Creator	<p>G/On comes with “default” connectivity for standard applications i.e. Citrix, Microsoft TS and Navision.</p> <p>Application Creator (and the Application String Editor) are G/On Admin tools that partners can use to make other applications on a customer’s network available to remote users.</p> <p>These can include, but is not limited to, server-based computing apps (e.g. mainframe), browser-based “services” (e.g. Intranet / Extranet / Portals), and client/server apps (e.g. SAP).</p>	An administration tool for extending the range of applications that a G/On system can connect to.
Client has “no serviceable parts”	Users cannot modify or tamper with the G/On client – there are no “moving parts”.	Minimizes user error and need for troubleshooting
Device Adoption	<p>Ability to bind a generic client to a unique piece of hardware, thereby transforming it into a token that must be present during logon (i.e. “something you have”). Together with the user’s domain userID and password (i.e. “something you know”), this makes up G/On’s strong 2-factor user authentication model.</p> <p>This is also a key part of the EMCADS patent.</p>	Eliminates need for secure tokens, by enabling any device to be turned into a token, based on unique identifiers.
Disable TAB to input fields	This feature means users can’t use the Tab key to move from the login name to the password field, forcing them to use the mouse. (Default is ON)	Improves logon security by making it harder to script logon exploits.
E-client	E-client is an application in the G/On client that calls the server and interprets its commands.	A simple, fast and highly efficient executable that helps make G/On’s “magic” happen.
EDMS	EMCADS Data Management System is used to store users, groups, applications, and all other information that relates to the G/On solution.	Built-in database removing the need to develop interface to third-party database. Also reduces cost by not forcing the customer to invest in third-party database.



EMCADS	Our patented core technology that allows data to be transmitted over an encrypted, resilient connection.	This is Giritech's own technology which makes development, maintenance, and bug fixing an in-house task.
Enable G/On's On Screen Keyboard (OSK)	IT administrators can give users the option of entering their login name and password using their mouse instead of their keyboard. (Default is OFF). See also "Force OSK".	Improves logon security by making it harder to use keyboard sniffers,
Force OSK (On Screen Keyboard)	Forces users to login via the OSK. (Default is OFF)	Improves logon security by making it harder to use keyboard sniffers,
G/On Builder	Part of G/On Admin, this tool is used to configure the G/On Server once it has been installed. It features a GUI with 5 tabs that let administrators specify settings for the server, user directory, client update, AD sync and clients. Once these have been defined, the administrator uses G/On Builder to activate or renew the license.	A user-friendly tool for quickly configuring the G/On Server.
G/On can run applications on a USB key and/or the local PC	G/On can be configured to enable just about anything that communicates via TCP/UDP. This means the range of applications that G/On allows users to access is <u>not</u> limited to thin clients (e.g. SBC), or other 3 rd party client software stored on G/On USB. It can, for example run client software installed a specific location on the local PC e.g. Outlook, apps that use a web browser, client/server apps etc	<p>Gives IT administrators a greater range of connectivity options by allowing them to run even "large" clients stored on the local PC. (This also reduces need to invest in bigger USB keys).</p> <p>It also improves the user experience as processing speeds are typically increased with the bandwidth available today.</p>
G/On Server	The engine that handles authentication and encryption processes, delivers the menu to G/On client, tells the client what local applications to start, and what ports to open.	All intelligence in the G/On solution resides on the server side. G/On client and is a slave to the G/On Server, and can only perform actions initiated by the G/On Server.



G/On USB leaves no data trail	<p>Any application launched from G/On USB key will not leave a trail on the host PC.</p> <p>NOTE: This does NOT apply when, for example, users run the locally installed version of, say Outlook or Internet Explorer.</p>	For G/On USB users, this eliminates risk of any subsequent user of that host PC being able to find or contact the G/On Server.
G/On Zones	<p>Ability to define which applications and level of interaction that a user can have. Setting up Zones is a way to control which types of applications are running depending on the trust level of the client. You may want to allow a user to run a local Outlook client on a trusted machine, but only run Terminal Services on an untrusted machine. Levels of trust can be built using the following parameters from the client:</p> <ol style="list-style-type: none">1. EDC (USB Key): Serial number/Manufacturer/Firmware/Class /Interface /Media Class.2. Device (PC that USB or Desktop Client is used on)3. Volume Serial Number or Label.4. G/On Client: Version, Client Network IP, CRC.5. EDC Host (client machine): Operation System, OS Major version, OS Minor Version, Host Class (cpu), Host Machine Name, Host Machine Domain and primary MAC Address on where they are connecting from (client type, domain, IP range)	Enables IT administrators to tailor level of access to individual users according to different scenarios.
G/OnAdmin	<p>This is THE tool for managing G/On. It includes modules for setting up and configuring the G/On Server, creating applications strings, action items and menus, defining groups and zones and managing login security settings.</p>	User-friendly interface for operating G/On Server.
Logging	<p>Logging is standard W3C log file format.</p>	Lets customers use their existing logging analysis tools and network optimization tools that they use to determine provisioning levels and whether customers are under dimensioned re concurrent users.



Nodeless connection	Unlike IPsec VPNs, the G/On Server does not assign an IP address to the device hosting the connection. This means the device does NOT become part of the network.	Avoids risk of viruses being replicated into the network. It also reduces network traffic and limits the number of ports that need to be opened in the firewall.
Opt-in bug report feature	Customers can choose to send bug reports to Giritech. The default setting is INACTIVE. Note: Only system relevant data is transmitted.	On a day-to-day basis, this means better customer service because we'll know if a system has gone down and can be ready to help them. Long term, this feature also ensures a better product because it gives us a clear picture of the type and frequency of the problems customers are encountering, thereby enabling us to prioritize development resources appropriately.
Random positioning for Client Logon screen	This feature means the login window opens in a random location on the user's screen, instead of always being centered in the middle of the screen. (Default is OFF)	Improves logon security by making it harder to script logon exploits.
Remote client update	Using G/Update, the G/On client can download updates from the G/On Server. By using Zone Rules, it is also possible to force G/Update to run at logon, allowing seamless upgrades of the client, or adding new functionality.	A convenient and cost-effective way for updating software and giving users access to new functionality. This significantly lowers the TCO of remote connectivity.
Resilient connections	G/On connections are highly resilient. This is because G/On Server creates keeps the connection to the application alive even if its connection to the G/On client is interrupted.	Improves the user experience by not requiring them to reconnect if the link goes down. This is especially valuable for mobile users where connectivity is sporadic (e.g. in



		aircraft).
Secure Key Exchange (SKE)	<p>As part of the initial connection process, G/On uses Elliptic Curve Cryptography (ECC) to generate a 163-bit signing pair when the client introduces itself to the G/On server. No 3rd party certificates are used in this process.</p> <p>NOTE: This is an integrated part of Giritech's patented EMCADS technology (i.e. it is not a separate component.)</p>	<p>This is a fast efficient method of initiating connections between the G/On Server and the G/On client.</p> <p>It also eliminates need (and risk) for installing certificates on the host device and buying and maintaining a certificate server on network.</p>
Server doesn't broadcast	The G/On Server doesn't broadcast – it only responds to requests from authentic G/On clients.	Ensures G/On is a discrete service that doesn't call unnecessary attention to itself.
T-client	A part of the G/On client that lets partners configure G/On to support connectivity to server-based computing (SBC), client/server applications and intranet/extranet/portals apps, that are based on TCP and UDP protocols	Increases range of applications that G/On can connect users to.
Use Cancel button instead of OK	Typically you click "OK" in a dialog box to accept / activate the data you've entered. This option makes "Cancel" the default key command in the login dialog box instead. This means when you've entered your username and password you click "Cancel" to confirm these entries instead of "OK". (Default is OFF).	Improves logon security by making it harder to script logon exploits.
Zero install for G/On USB	After the initial registration of the client/device (EDC) in the system, the user doesn't have to do anything to make the client work except plug in the USB key or click the desktop icon.	Simple, user-friendly experience
What G/On Does Not Do		
G/On cannot access network drive letters	G/On connects users to applications – not the network. The only way they can access network drive letters is if they access an application that lets them do this e.g. Citrix.	The administrator has full control over who gets network access.



<p>G/On is not malware/spyware proof</p>	<p>Malware on a PC can be used to remotely launch and operate a G/On connection.</p> <p>For this reason it is important that G/On Desktop users install antivirus software and keep it updated.</p> <p>It is also important that G/On USB users remove their USB key from the PC when they leave the PC.</p>	<p>Malicious programs will only get access to the applications published to the specific user and never the network itself. It will never be able to connect to the internal on any other ports than the ones published with the applications.</p>
<p>G/On can not be installed on "any" server.</p>	<p>G/On can only be installed on the server platforms specified in the G/On Product Announcement. Further it should only be installed according to the latest Best Practices guidelines.</p>	
<p>G/On does not work with biometric USB keys</p>	<p>G/On only works with the USB keys provided by Giritech. To date we have not identified any biometric keys that actually provide a responsible level of security.</p>	<p>Removes false sense of security.</p>
<p>G/On does not work with every USB device</p>	<p>G/On only works with the USB keys provided by Giritech.</p>	<p>Only USB Keys made to Giritech's specifications contain the special unique identifier needed to make the USB key useful as a token.</p>