GOV.UK

Guidance

BYOD Guidance: Excitor G/On OS

Published 6 October 2014

Contents

This guidance is applicable to G/On OS, running from G/On USB tokens that use a built-in smartcard. This guidance was developed following testing performed with G/On Server 5.6 and G/On OS 19.2, and applies up to Server version 5.7 and OS version 21.

1. Usage scenario

G/On OS is a customised build of Fedora that runs the G/On client application from a USB token. This enables organisations to deploy a corporately-managed desktop to:

- corporately-owned end user devices (EUDs), including those of another trusted organisation
- personally-owned EUDs, such as an end user’s home PC

Organisations should consider the common risks of using unmanaged devices in addition to specific risks highlighted in this guidance.

In either scenario, G/On OS will be used to remotely connect to corporate services over any network bearer, including Ethernet, Wi-Fi and 3G, using a secure tunnel. This enables a variety of remote working approaches such as:

- accessing OFFICIAL intranet web applications, including webmail

- accessing OFFICIAL remote desktop services

2. Summary of platform security

This platform has been assessed against each of the 12 security principles, and that assessment is shown in the table below. Explanatory text indicates that there is something related to that principle that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See How the platform can best satisfy the security recommendations for more details about how each of the security principle is met.

Security principle	Rationale
Assured data-in-transit protection	[!] G/On uses a proprietary protocol for connectivity between G/On clients and the G/On gateway. This has not been independently assured to Foundation Grade.
Assured data-at-rest protection	
Authentication	End users do not authenticate to the G/On client. G/On OS does not have a screen lock.
Secure boot	Secure boot is not supported on this platform.
Platform integrity and application sandboxing	[!] There is no integrity protection of files on the USB token.
Application whitelisting	Users can run applications from unapproved sources.
Malicious code detection and prevention	There is no malicious code detection.
Security policy enforcement	Users can bypass some locally-configured policies.
External interface protection	
Device update policy	[!] Patches and updates for G/On OS are not released regularly. Administrators need posession of USB tokens to apply these.
Event collection for enterprise analysis	[!] There is no facility for collecting logs remotely from a device, forensic log information is not persistent.
Incident response	

2.1 Significant risks

In addition to the common risks of unmanaged hardware the following risks have been identified:

- G/On uses a proprietary protocol, known as EMCADS, to create a secure tunnel between an EUD and the corporate network. This has not been independently assured to Foundation Grade, and does not support some of the mandatory requirements expected from assured VPNs. Without assurance in the VPN there is a risk that data transiting from the device could be compromised.
- There is no screen lock mechanism. A local attacker can access a user session and any remote corporate resources they have access to.
- Without secure boot, data-at-rest protection and no integrity protection of files on the USB token, an attacker who can write to the USB token can modify G/On OS and locally-enforced security policies to gain persistent remote access to corporate resources. Procedural controls are necessary to protect USB tokens and prevent end users inserting them into untrusted or malicious devices.
- End users have permission to execute files downloaded through a web browser or added to a USB token manually. These files could contain malicious code.
- There is no malicious code detection and organisations cannot install additional software to support this.
- There are no controls to disable physical ports on a device. Many devices which can run G/On OS have external interfaces which permit Direct Memory Access (DMA) from connected peripherals. This presents an opportunity for a local attacker to exfiltrate sensitive data.
- G/On OS is composed of a number of software packages, many of which come from other developers. These packages often receive security patches that fix known vulnerabilities. However, as updates for G/On OS are released on a 6-monthly basis, these security patches will not be available on G/On OS for up to 6 months. A network attacker can exploit publicly known vulnerabilities during this time. In order to apply these updates, a USB token needs to be returned to an administrator.

3. How the platform can best satisfy the security recommendations

This section details the configuration required to meet the security recommendations for this platform.

3.1 Assured data-in-transit protection

The native G/On VPN client is enabled by default and protects all device traffic between the EUD and the corporate network. There are no configurable settings.

3.2 Assured data-at-rest protection

G/On OS does not encrypt data-at-rest as it is designed as a thin-client platform and limits the storage of user application data. Minimise the amount of sensitive configuration data stored on the device, such as Wi-Fi passphrases.

3.3 Authentication

The user has a strong 9-character passphrase to authenticate themselves to the G/On Gateway. Each USB token also has a unique key, stored on the token smartcard, used to authenticate the token to the G/On Gateway.

The user closes the connection to the G/On Gateway server when leaving the device unattended. An inactivity timeout on the G/On Gateway forces idle connections to terminate.

3.4 Secure boot

There is currently no secure boot mechanism in G/On OS. Procedural controls should be present in the user security procedures to prohibit USB tokens being inserted into a device not approved for use by the organisation.

Set a UEFI/BIOS password to make it more difficult for an attacker to modify the boot process.

3.5 Platform integrity and application sandboxing

There are no configurable platform integrity or application sandboxing mechanisms in G/On OS.

Files on the G/On USB token, including the OS and configuration files, are not integrity protected. Users should not leave their G/On USB token unattended or insert it into untrusted devices.

3.6 Application whitelisting

Procedural controls prevent users installing applications on their USB token.

Access to corporate applications is granted to users from the G/On Management Server, based on user and group permissions.

3.7 Malicious code detection and prevention

There are no configurable malicious code detection and prevention mechanism in G/On OS. Content-based attacks can be filtered by scanning capabilities in the corporate network.

3.8 Security policy enforcement

The G/On Gateway server is used to enforce access to corporate resources and cannot be modified by the end user.

Procedural controls prevent user modification of the firewall rules and security policies configured in gon_os_config.txt.

3.9 External interface protection

Direct Memory Access is possible from peripherals connected to some external interfaces including FireWire, eSATA, and Thunderbolt. It is advisable to use USB tokens with devices which do not have DMA interfaces present, or devices which allow such interfaces to be disabled in the UEFI/BIOS.

3.10 Device update policy

Configure the G/On Gateway server to prevent old versions of G/On OS accessing corporate resources.

When an update is available, USB tokens should be returned to an administrator and reprovisioned with the latest software versions.

3.11 Event collection for enterprise analysis

G/On OS does not support remote event collection for enterprise analysis of security incidents.

The G/On Gateway and Management servers should be configured to log failed device login attempts and other security events.

3.12 Incident response

Access to the corporate network can be prevented by revoking the USB token from the

G/On Server Management Client. The user’s passphrase should be reset if it could have been compromised.

Change any credentials stored on the USB token that are used for shared services, such as corporate Wi-Fi.

4. Network architecture

The following network diagram describes the recommended architecture for this platform. It is based on the BYOD Architectural Approaches and the Walled Garden Architectural Pattern.

Excitor G/On OS network architecture diagram

Recommended architecture for deployments of Excitor G/On OS

5. Deployment process

To prepare the corporate network for hosting a deployment of these devices, follow these steps:

1. Deploy and configure the requisite network components as described above.
2. Deploy the G/On Management and Gateway servers, using the recommended configuration settings.
3. Configure the default Management Role Assignment such that only authorised administrators are assigned this role.
4. Add the recommended policies from the G/On Management client.
5. Configure the default gon_os_config.txt policies on the G/On Management server.
6. Create policies and grant access to applications for users and groups in accordance with organisational policy.

6. Provisioning steps

To enrol and provision each USB token in preparation for end users, follow these steps from the G/On Server Management client:

1. Enrol the USB token and assign it to a user from the Personal Token Assignment panel.
2. Install the G/On OS package onto a USB token from the Token Software Management panel.

Where practical, configure the UEFI/BIOS of machines where the token is likely to be used; disable unused hardware interfaces, enable Secure Boot and set the boot order to prioritise booting from USB devices. Set a BIOS password to prevent unauthorised changes being made.

7. Configuration settings

7.1 G/On Server Configuration Wizard

These settings should be applied during the install wizard or using the configuration change wizard. Other settings (e.g. server address) should be chosen according to the relevant network configuration, or left as their default values.

G/On Management Server Configuration (Advanced)	
Logging enabled	Enabled
Logging verbose level	1
Automatic Approval of Enrollment Requests	Disabled
Port scan enabled	Disabled
G/On Gateway Server Configuration	
Show last login name at login	Disabled
Show last user directory at login	Disabled
G/On Gateway Server Configuration (Advanced)	
User session timeout	10 (minutes)
Authorization timeout	60 (seconds)
User directory setup panel	
Disable unused user authentication plugins (for example the 'Local Windows User' plugin)	

7.2 G/On Management client

Using the G/On Management client:

- add and configure the ‘Verify G/On OS version’ menu action from the Action Authorization Policy panel to prevent older versions of G/On OS being allowed to connect to corporate resources
- add the ‘Change Password’ menu action from the Action Authorization Policy panel to allow authorised users to change their account passphrase

7.3 gon_os_config.txt

On the G/On Management server, modify the following client configuration settings in `C:\Program Files(x86)\Giritech\gon_5.6.2-3\config\deployed\gon_os_config.txt`.

Setting	Reason
persistent_networks = False	Prevents Wi-Fi passphrases being stored on a USB token
auto_shutdown = 30	Terminates client connections to the G/On Gateway after a period of inactivity (in minutes)
sandboxed_browser = False	Prevents users bypassing the firewall from the sandboxed Firefox application

8. Enterprise considerations

The following points are in addition to the common enterprise considerations and contain specific issues for G/On deployments.

8.1 Device appropriateness

A number of the 12 security principles are reliant on both the security posture of G/On OS and the hardware that it runs from. Since G/On OS runs from a USB token that can be used with any device, it is important to set organisational policy on which devices it is appropriate for end users to use their G/On USB tokens with.

Restricting the use of G/On OS to devices which are managed by a competent entity, such as the organisation or another trusted organisation, reduces the risks of malware subverting the protections offered by G/On OS.

8.2 Remote patching

G/On OS does not support remote patching; devices must be recalled and updated by an administrator. Organisations should ensure they have a plan for implementing their patching policy and how this will cope when security-critical patches need to be applied to a whole fleet of USB tokens.

8.3 Proprietary remote access protocol

The G/On OS secure tunnel is a proprietary set of technologies which operate differently to the remote access functions of other platforms in this guidance set. As such, organisations wishing to deploy G/On OS in conjunction with other remote access solutions may need to consider how to integrate the 2 disparate solutions into the same network architecture.

8.4 RDP client applications

G/On OS supports the FreeRDP and rdesktop client applications. Organisations should note that FreeRDP supports Network Level Authentication (NLA), which may be required by the corporate network and can provide increased security, whereas rdesktop does not. When configuring menu actions for end users, consider which application is appropriate.

Legal information

CESG: This guidance is issued by CESG, the UK's National Technical Authority on Information Assurance. One of the roles of CESG is to provide advice to UK government entities and organisations providing services to UK government. The guidance found here is provided and intended for use by this audience. It is provided 'as-is' as an example of how specific requirements could be met. It should be used to help inform risk management decisions on the use of the products described, but it should not be used for procurement decisions; it is not intended to be exhaustive, it does not act as an endorsement of any particular product or technology, and it is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take appropriate technical and legal advice in using this and other guidance published by CESG. This guidance is provided without any warranty of any kind, whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, content, quality, or fitness for purpose of all or any part of it. CESG cannot, then, accept any liability whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it. This guidance is UK Crown Copyright. All Rights Reserved.

CPNI: Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.