



# **G/On Set-up and Configuration Reference**

---

*In depth explanations and reference manual for the G/On Configuration Client*

G/On version: 5.3

Document revision: 0.97

## About this document

This document gives an in-depth description of the functionality of the G/On Configuration program.

If you do not find the information you need in this document, you may want to look in the other documents in the G/On software documentation suite:

- G/On User Guide – Getting started – Fedora
- G/On User Guide – Getting started – Windows XP
- G/On User Guide – Getting started – Windows Vista
- G/On User Guide – Getting started – Windows 7
- G/On User Guide – Getting started – Mac
- G/On User Reference
- Getting started with G/On Set-up and Configuration
- Getting started with G/On Management
- G/On Set-up and Configuration Reference
- G/On Management Reference
- G/On Customization Reference

© Giritech A/S, 2009  
Spotorno Allé 12, 2.  
2630 Taastrup  
Denmark  
Phone +45 70.277.262

### Legal Notice

Giritech reserves the right to change the information contained in this document without prior notice. Giritech® and G/On™ are trademarks and registered trademarks of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property currently includes the patented systems and methods known as EMCADS™. Other product names and brands used herein are the sole property of their owners. Unauthorized copying, editing, and distribution of this document is prohibited.

## Contents

About this document.....	2
Before installation.....	4
Supported Platforms.....	4
Introduction.....	5
Overview: Making New Installations and Upgrades.....	5
G/On Configuration Welcome Screen.....	6
No License.....	7
Main Status Window.....	8
G/On Server Services.....	8
Software Package (GPM) Generation.....	8
Support Package Generation.....	9
Wizards.....	9
Installation Wizard.....	9
Change Wizard.....	18
Upgrade Wizard.....	18
Package Generation Wizard.....	19
Menu.....	20
File Menu.....	20
Edit Menu.....	20
Generate Menu.....	21
Help Menu.....	21
Advanced Setup Topics.....	23
Backup and Restore.....	23
Initialization of Tokens.....	23
Access notification by mail.....	24
LDAP and Active Directory plugins .....	25
Fail-over set-up.....	26
Troubleshooting.....	30
FAQ .....	30
How to change the external address or port of the G/On Gateway Server.....	30

# Before installation

## Supported Platforms

### ***G/On Client***

- Windows XP (32 bit)
- Windows Vista
- Windows 7
- Apple Mac OS X 10.4 (Tiger)
- Apple Mac OS X 10.5 (Leopard)
- Apple Mac OS X 10.6 (Snow leopard)
- Linux Fedora 11 with GTK+ GUI (32 bit)

### ***G/On Management***

- Windows XP SP3, Windows Vista SP2, Windows 7
- Windows Server 2003 R2 SP2, Windows Server 2008 SP2

### ***G/On Server***

- Windows Server 2003 R2 SP2, Windows Server 2008 SP2

## Introduction

Three different programs are used for installing, configuring and managing a G/On Server:

**The Windows Installer** creates a program folder and unpacks all the necessary files to this folder, and creates entries in the Windows start menu.

**G/On Configuration** is used for basic configuration of a new installation (IP addresses etc.) and is also used for upgrading an existing version to a new version.

**G/On Management** is used for the management of authentication and authorization policies, and daily operation regarding users, tokens etc.

This document describes in detail the options available when using the G/On Configuration program. Please refer to the document: Getting Started with G/On Setup and Configuration for a quick introduction.

See the G/On Management Reference, for documentation regarding the G/On Management program.

The architecture of G/On Configuration is a client-server application where both client and server runs on the same computer (the server). The G/On Configuration client automatically starts up a G/On Configuration server process, which is the one that does the actual configuration. The G/On Configuration server program can also be used as a command line tool, for certain tasks.

**OBS:** *On Windows Server 2008, you must run the G/On Configuration program as Administrator: Find the program in the Windows Start Menu, right-click on it, and choose: "Run as Administrator".*

## Overview: Making New Installations and Upgrades

To make a new installation:

- Run the Windows Installer, G/On Configuration program and G/On Management program, in this order.

To make an upgrade of an existing installation:

1. Install the new version, by running the Windows Installer for that version. This will make a new program folder for the version, without affecting the already installed versions.
2. Run G/On Configuration for the new version. On the Welcome Screen, there will a list of the already installed versions. Choose the one, which you want to upgrade from, and complete the steps that you are guided through.
3. Now, the services of the new version are ready to be started. But before doing that, stop (and disable) the services of the old version. This is necessary, because the services of the new version listens on the same ports as the old version, and two different services cannot listen on the same ports.

**OBS:** Before starting any installation or upgrade, read the release notes, to see if there are special issues to consider.

## G/On Configuration Welcome Screen

The first time you open G/On Configuration, you will be presented with a Welcome Screen like this:



If you see a screen like this it is because the G/On configuration utility has detected that the server has not yet been configured. Configuration is done using the the installation wizard, which is described below.

The Welcome screen can also be opened from the Main Status Window by choosing Help → Welcome to the G/On Configuration in the menu.

In case one or more upgradable G/On system is already installed on the server, these systems will also be listed in the Welcome Screen.

To upgrade from a previously installed system press the “Upgrade Wizard” button for that system. The Upgrade Wizard is described below.

## No License

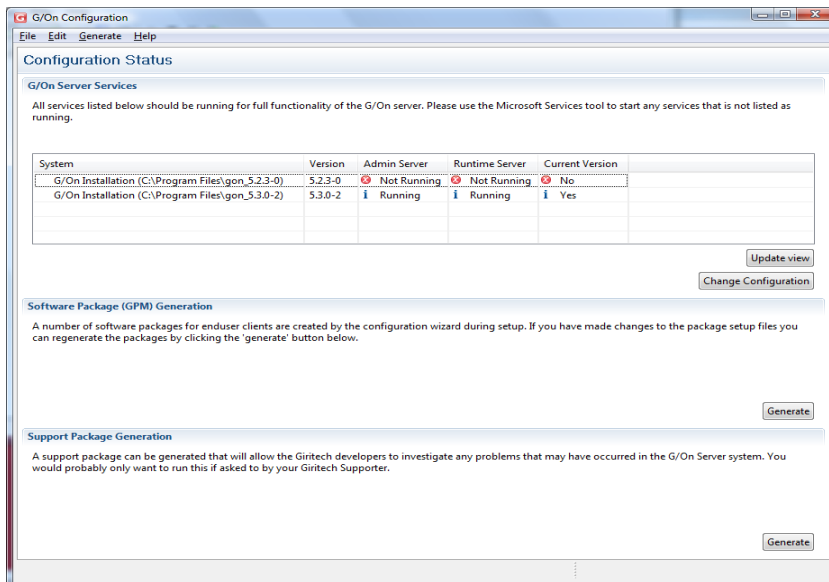
If no license is found, the Welcome Screen will look like this:



If you do not use a proper G/On license file, the installation will proceed with an evaluation license. If you have acquired a proper license file, you should place it in the folder "gon\_server\_management\_service\win\deployed".

## Main Status Window

If the Installation Wizard has already been run successfully, G/On Configuration will open in the Main Status Window, which could look something like this:



The Window is divided into three parts. Each part is described below.

### G/On Server Services

In this section of the status window, you should see a table showing detected currently installed G/On Systems. The table shows the following information:

<b>System</b>	Name and location of the system
<b>Version</b>	System version
<b>Admin Server</b>	Status for Management server service
<b>Gateway Server</b>	Status for Gateway server service
<b>Current Version</b>	Whether the system is part of the same version as the Server Configuration utility

Below the table there are two buttons:

<b>Update View</b>	Checks and updates the information in the table. Could for example be used after starting server services.
<b>Change Configuration</b>	Starts the Change Configuration Wizard for the current system. The wizard is described below.

### Software Package (GPM) Generation

This section contains a description of the Software Package concept and a button which starts up the Software Package Generation Wizard.

## Support Package Generation

This section contains a description of the Support Package concept and a button for generating a Support Package. Support Packages can also be generated by choosing Generate → Generate Support Package in the menu.

A Support Package is a zip-file containing ini-files, log-files and more, that can be generated and send to Giritech Support. Notice that the database and the server part of the known secret are NOT included in the Support Package, because this information should only be shared in very special situations.

Generated support packages are placed in the folder:

```
.\gon_config_service\win\support_packages
```

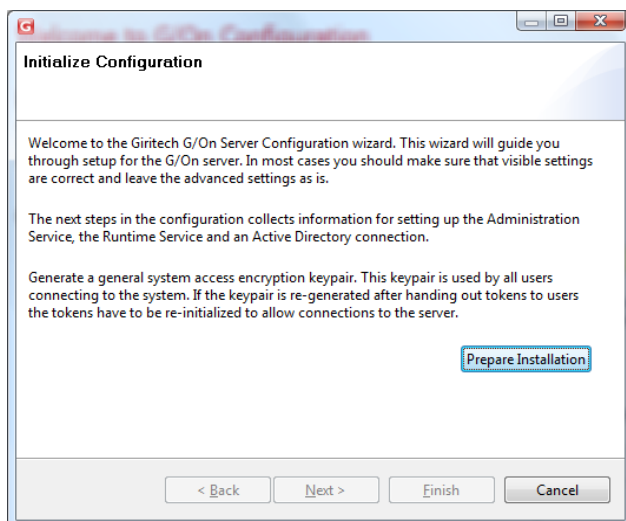
## Wizards

This section contains detailed information regarding the various Wizards in the G/On Configuration tool.

### Installation Wizard

The installation Wizard is started automatically, the first time you run G/On Configuration. It can also be started by pushing the “Start Wizard” button In the “G/On Configuration Wizard” section in the Welcome Screen. Note that the Installation Wizard should only be run once. Running it again on an installed system will erase system data and potentially invalidate the system.

#### *Initialize Configuration*



Push the “Prepare Installation” button in order to run the preparation job. If no errors occur, you will be able to push the “Next” button after the job finishes. If any errors occur they will be shown immediately after the “Initialize Configuration” title and you will not be able to continue the Wizard.

## Management Server Configuration

The Management server allows management of the solution (users, authentication and authorization policies). It accepts input from the G/On Management Client and stores the resulting policies etc. in a database, where the Gateway server can read it.

In this window, the Management Server configuration can be entered. Note that the “Advanced” pane is hidden initially, but in the screen shot above it has been opened in order to show the information fields.

### Standard:

**Listen Port** Port number

### Advanced:

**Listen IP** IP address that the Management Server should listen on. Default is 127.0.0.1 – which means that the G/On Management Server will only allow connections from the machine the Management server is running on. That way, the Management tool can only be accessed directly on the G/On server itself (through the console or a terminal server session) or through the G/On Gateway Service also running on the server.

If for some reason the Management Server should allow connections from other machines, the Listen IP address can be specified as 0.0.0.0 – which will allow access from all IP addresses on the local network. As stated above, authorization to use the G/On Management tool must then be enforced by other means, so this option should be selected carefully!

Enable logging

### Logging enabled Logging

The primary purpose of logging in this context is for support reasons.

- verbose level** Currently, there are two logging levels defined:  
 0: All warnings, errors and critical errors will be logged  
 9: Very detailed logging level of all activities. Using this level will severely impact performance – and should not be used unless needed for support reasons (remember to deactivate).
- Portscan enabled** Enable the possibility for port scanning when creating Menu Actions. Note that port scanning can violate local network security policies.
- Portscan IP ranges** When port scanning is enabled, the ranges of ports to be scanned will be the ones defined here. A range is simply defined as <startPort>-<endPort>, and more ranges can be specified by separating them with a comma.

## Gateway Server Configuration

The Gateway server does the actual “gate keeping”: it accepts connections from G/On clients, gets user names and passwords and tokens checked, and grants access to menu actions in accordance with the Authentication and Authorization policies specified in G/On Management.

**G/On Gateway Server Configuration**

Listen Port: 443

Client Connect Addresses: artst01.demo.giritech.com

Client Connect Ports: 443, 80, 3945

**Advanced**

Listen Address: 0.0.0.0

Logging enabled:

Logging verbose level: 0

Session logging enabled:

Session logging enabled by remote:

Authorization timeout (sec): 60

CPM Concurrent downloads:

Inform user before first access enabled:

Inform user before first access message file: /gon\_message\_on\_first\_access.txt

Inform user before first access, close on cancel:

< Back   Next >   Finish   Cancel

Standard:

<b>Listen Port</b>	The port that the Gateway Server listens on in order to accept connections from G/On Clients. Only one port can be specified here. Note: The G/On clients can be configured to try connecting to several ports (see the field: "Port the client connects to"). In this case, there must be a firewall/router in front of the G/On Gateway server, which maps all these "external" ports to the port that the server is actually listening on.
<b>Server DNS names or IP addresses</b>	This is the IP address (DNS name or number), that the G/On clients will use to connect to the G/On server. Please note, that when using a proper license, this address is fixed, and must be determined at the time of ordering G/On, as the connection address is part of the license (file). If using the demo license, any address can be specified.
<b>Port the client connects to</b>	Although 3945 is the official IANA allocated port-number for G/On – other port-numbers can be used. Port 80 – or 443 are recommended, as these ports are open outbound in most environments. So by selecting these ports, the G/On clients will be able to connect to the G/On server under all normal circumstances. The port(s) must be specified at the time of ordering G/On, and is part of the license (file). If more ports are to be used, all ports must be specified at the time of ordering – and the "Multiport" Option must be part of the license. If using the demo license, any port can be specified.

Advanced:

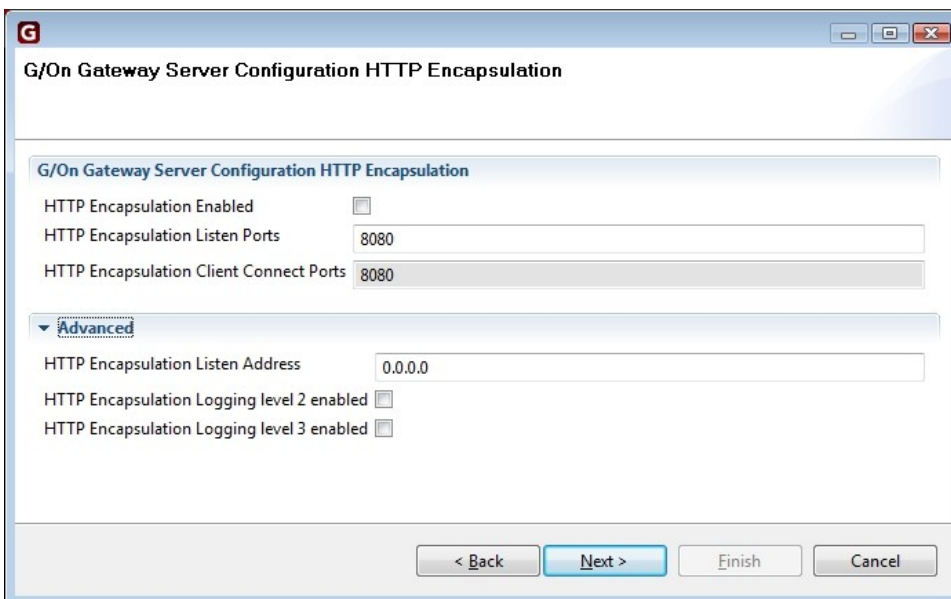
<b>Listen IP</b>	This is the internal address that the G/On Gateway will listen on to accept connections from G/On clients. 0.0.0.0 will enable connections on all the network interfaces of the Gateway Server machine (default).
<b>Logging enabled</b>	Enable logging. The primary purpose of logging in this context is for support reasons.
<b>Logging verbose level</b>	Currently, there are two logging levels defined: 0: All warnings, errors and critical errors will be logged 9: Very detailed logging level of all activities. Using this level will severely impact performance – and should not be used unless needed for support reasons (remember to deactivate).
<b>Session logging enabled</b>	Log each user session in a separate file
<b>Authorization time-out</b>	This is the time users have to complete the authentication process (specify user-id and password) from a connection is established. If the user does not log on during the specified time, the connection is terminated.
<b>GPM Concurrent Downloads</b>	To avoid performance impact, the number of concurrent downloads of GPM packages can be limited by setting this field. This controls how many users can do field updates or installs of the software on the tokens.
<b>Inform User before first access enabled</b>	This option can be used to acquire user acceptance of the terms and conditions under which access is granted.
<b>Inform user</b>	If the previous option is enabled, this file contains the message which the

**before first access message file** user must accept at the first time access is about to be granted.

**Inform user before first access, close-on-cancel check box** If this is checked, the G/On connection will be closed, unless the user clicks Accept, when shown the message.

## HTTP Encapsulation

In some environments, a deep packet inspection firewall or other might block the communication between G/On clients and the G/On server. To allow connectivity in these situations, the **HTTP Encapsulation** option should be specified when ordering G/On. This optional feature enables the G/On client to encapsulate the G/On data stream in http packages, thereby using G/On in "web communications" mode. This will allow the G/On client to connect from virtually all environments, where a web browser can be started successfully.



The screenshot shows a Windows-style dialog box titled "G/On Gateway Server Configuration HTTP Encapsulation". The dialog has a blue header bar with a "G" logo on the left and standard window controls (minimize, maximize, close) on the right. Below the header, the title "G/On Gateway Server Configuration HTTP Encapsulation" is repeated. The main area contains several configuration options:

- "HTTP Encapsulation Enabled" with an unchecked checkbox.
- "HTTP Encapsulation Listen Ports" with a text box containing "8080".
- "HTTP Encapsulation Client Connect Ports" with a text box containing "8080".
- An "Advanced" section, indicated by a downward arrow and the word "Advanced" in blue, which is expanded to show:
  - "HTTP Encapsulation Listen Address" with a text box containing "0.0.0.0".
  - "HTTP Encapsulation Logging level 2 enabled" with an unchecked checkbox.
  - "HTTP Encapsulation Logging level 3 enabled" with an unchecked checkbox.

At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Finish", and "Cancel". The "Next >" button is highlighted in blue.

If the HTTP Encapsulation option has been specified when ordering G/On, you can enable and configure this feature as follows:

**Standard:**

<b>HTTP Encapsulation Enabled</b>	Enable or disable use of HTTP encapsulation.
<b>HTTP Encapsulation Listen port</b>	specifies the port on which the Gateway Server will listen for HTTP Encapsulated G/On traffic, on the inside of the firewall.
<b>HTTP Encapsulation Client Connect Port</b>	specifies the ports, that G/On clients will use on the outside when sending HTTP encapsulated data streams.

**Advanced:**

<b>HTTP Listen Address</b>	Specify the address from which HTTP Encapsulated traffic are accepted. 0.0.0.0 (default value) defines all addresses.
<b>HTTP Encapsulation Logging level 2 enabled</b>	Debug logging enabled.
<b>HTTP Encapsulation Logging level 3 enabled</b>	Very detailed logging level of all activities. Using this level will severely impact performance – and should not be used unless needed for support reasons (remember to deactivate).

***Active Directory User Directory Plugin Configuration***

The Active Directory plugin is used for user verification and for obtaining information about users and groups in G/On Management.

Note: In order for Active Directory integration to work properly the following conditions must be met:

- Installation must be done on a computer which is either on the Active Directory domain or on a domain with which a trust relationship has been established.
- The account used for running the Gateway and Management server services (by default Local System Account) must have access to see group membership for all users. Notice that the default Active Directory settings allow for all users to see other users group membership. To verify this permission, check the "Effective permissions" in the "Advanced security settings" of the account, and see if the permission "Read Group Membership" is in effect.

**Active Directory User Directory Plugin Configuration**

Active Directory User Directory Plugin Configuration

Enabled

Domain (dns)

Netbios

< Back   Next >   Finish   Cancel

**Standard:**

- Enabled** Enable use of the AD plugin
- Domain (dns)** Enter dns name of the AD domain, e. g. mycompany.com
- Netbios** Normally, the Netbios name of the AD domain is automatically filled in by the system. If this does not happen, please fill in the Netbios name, manually.

**LDAP Plugin Configuration**

**LDAP User Directory Plugin Configuration**

LDAP User Directory Plugin Configuration

Enabled

Directory name

Root DN

Server host list

**Advanced**

Is Active Directory

Use SSL

SSL Certificate

User DN

Password

Password Change Disabled

Password Expiry Warning Time

< Back   Next >   Finish   Cancel

The LDAP plugin is used for user verification and for obtaining information about users and groups against an LDAP enabled User Directory such as Novell eDirectory or Active Directory.

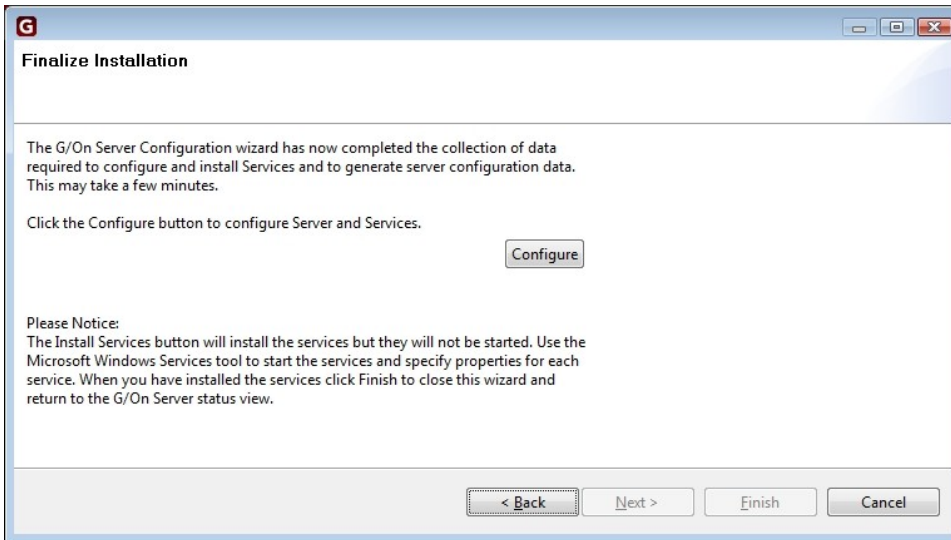
**Standard:**

<b>Enabled</b>	Enable or disable LDAP plugin.
<b>Directory Name</b>	Enter a name for the directory. This name will be used to link users to this LDAP Directory and for reference in reports and log files. This name should <b>never</b> be changed once users and groups have been entered in the system.
<b>Root DN</b>	The root DN under which users, groups and ou's should be found.
<b>Server host list</b>	A comma-separated list of servers for the LDAP directory. Add more servers to get fail-over if first server is down. Port number is assumed to be 389 unless specified. <b>Example</b> : firstserver:636, secondserver, thirdserver

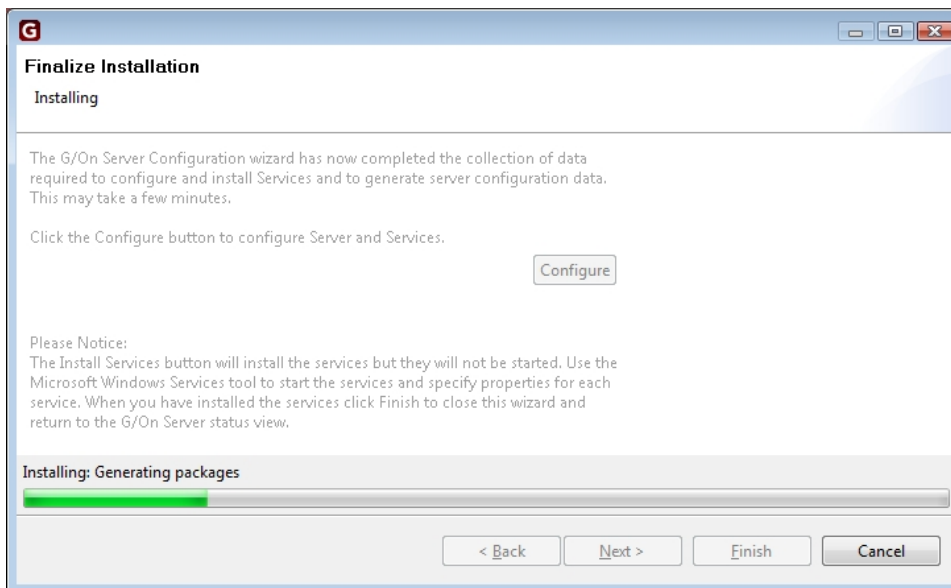
**Advanced:**

<b>Is Active Directory</b>	Check if connecting to Active Directory via LDAP. Some functionality such as password change and group membership differs from standard LDAP, when using the LDAP protocol to access AD.
<b>Use SSL</b>	Check if SSL communication should be used.
<b>SSL Certificate</b>	Full path to Certificate file used for SSL communication.
<b>Don't Require Server Certificate</b>	Check if G/On server should not check the server certificate when connecting when SSL is used. Use to enable SSL communication without server verification.
<b>Username</b>	Name (dn) of user account used for connecting to LDAP in order to search for information. Leave blank if anonymous access is enabled in the User Directory. Note: AD does not allow anonymous access.
<b>Password</b>	Password for the user specified account
<b>Password Change Disabled</b>	Check if password change via G/On should be disabled.
<b>Password Expiry Warning Time</b>	Time (in number of days) before which the user is warned about password expiring. Enter '0' in order to disable warnings.

## Finalize Installation



Press the **Configure** button to start configuration and services and generation of G/On Client Software packages.



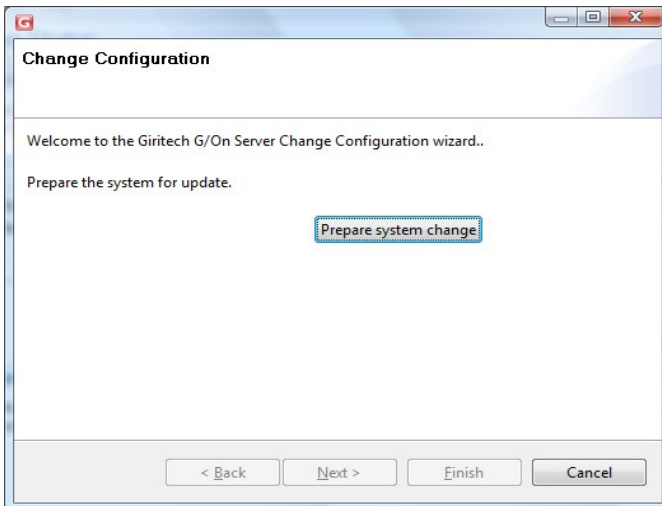
If no errors occur, you will be able to click the “Finish” button to exit the Wizard and go to the Configuration Status screen. If any errors occur they will be shown immediately after the “Finalize Installation” title.

OBS: Note that the Wizard only creates the G/On Services. The services have to be started manually. You can start the G/On services by using the “Services” Management interface in windows. (**All Programs**→**Administrative Tools**→**Services**)

## Change Wizard

The Change Wizard is used for changing information for the currently installed system. The Wizard is started by pushing the “Change Configuration” button in the Main Status Window.

The Change Wizard has the same structure as the Installation Wizard: On the first page a “Prepare Change” job has to be run, on the following pages configuration information is entered and on the final page the change is finalized. Here is a screen shot of the first page:



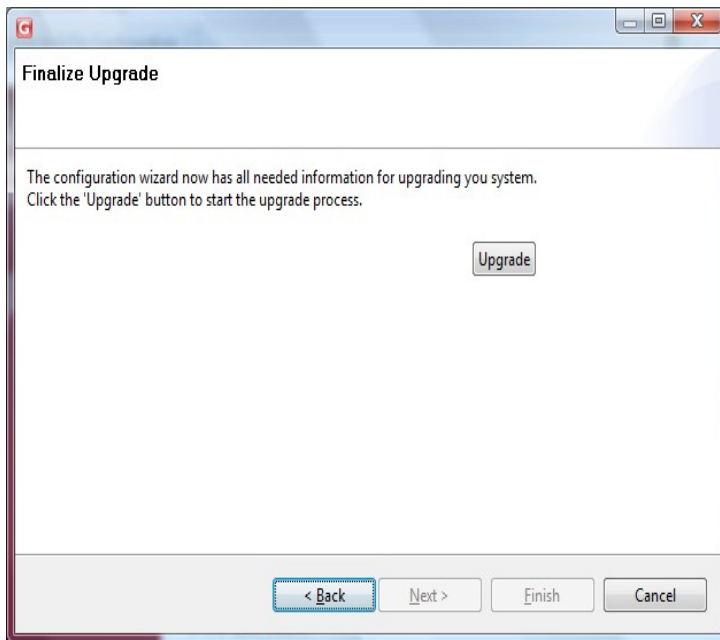
All pages following this are the same as or similar to those of the Installation Wizard, so please refer to the Installation Wizard Section for information about these pages.

**NOTE:** The last step in the Change Wizard will stop both the Management and Gateway services, and re-install them. So do not do this, while there are users on the system,

## Upgrade Wizard

The Upgrade Wizard is used for upgrading a previously installed G/On System to the version of the Sever Configuration tool.

The Upgrade Wizard has the same structure as the Installation Wizard: On the first page a “Prepare Upgrade” job has to be run, on the following pages configuration information is entered and on the final page the upgrade is finalized. Note that depending on the upgrade there may not be any pages between the “Initialize” and “Finalize” page. Here is a screen shot of the first page:



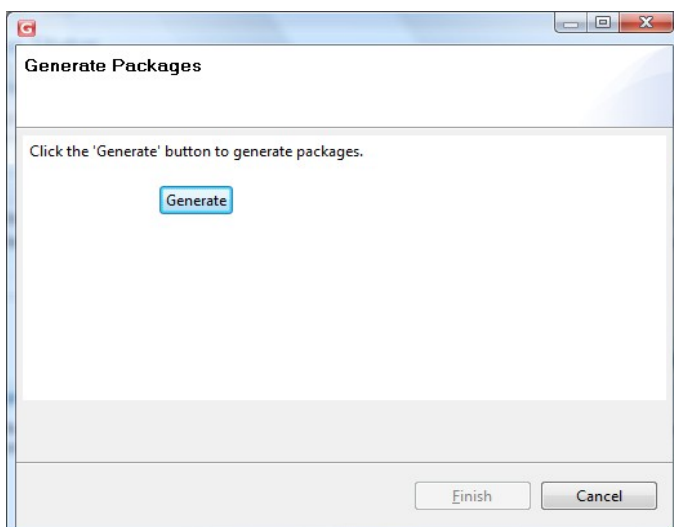
Note that during the upgrade, the system from which the upgrade is made will not be changed. You will need to stop the services of the “old” version manually, and uninstall it manually, if you desire to remove it.

## Package Generation Wizard

This wizard generates GPM packages. Packages are generated as part of the Installation Wizard, so this Wizard need only be run if packages have been updated, added or removed.

The Wizard is started by either pushing the “Generate” button in the “Software Package (GPM) Wizard” section of the Main Status Window or by choosing Generate → Generate Software Packages (GPM) in the menu.

The Wizard consists of a single window:



Push the “Generate” button in order to start the task which generates the packages. If no errors occur, you will be able to push the “Finish” button to exit the Wizard. If an error occurs it will be shown immediately after the window title.

## Menu

This section describes the options available in the menu.

### File Menu

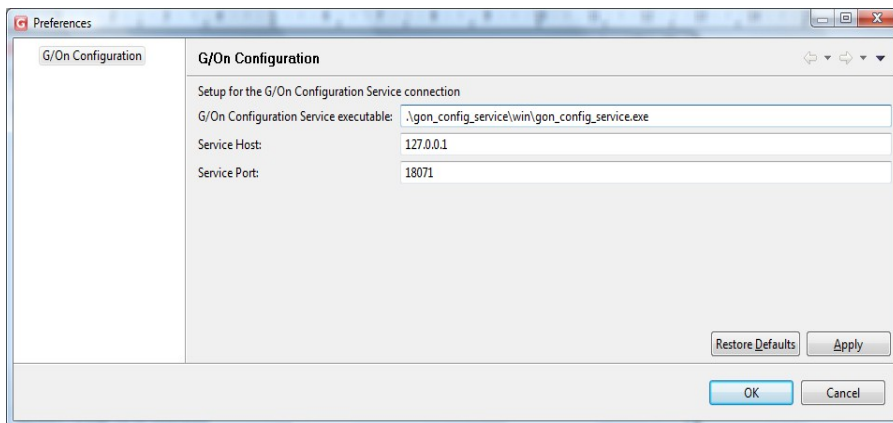
#### *Quit G/On Configuration*

Quits the program

### Edit Menu

#### *Preferences*

Opens the preferences window:



The following options are available:

**G/On Configuration Service Executable** Path to the underlying server program, which does the actual configuration.

**Service Host** The server name or IP address.

**Service Port** The port used to communicate

Usually there is no need to change these settings, except perhaps the port number, if the default port number is unavailable for some reason.

## Generate Menu

### *Generate Software Packages*

Generates software packages. See Package Generation Wizard.

### *Generate Support Package*

Generates a support package. See Support Package Generation

## Help Menu

### About G/On Configuration

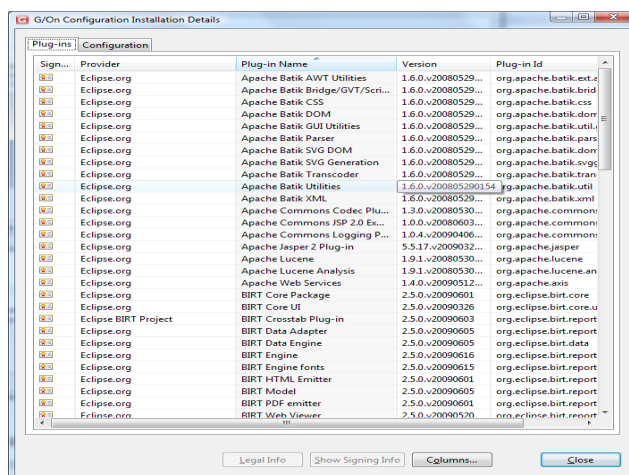
Open the “About” Window. Apart from version and copyright information, you can access the Server Configuration client error log from here by following the steps below. Note that this log only pertains to the client (GUI) part of the Server Configuration Utility.

The error log is fetched like this:

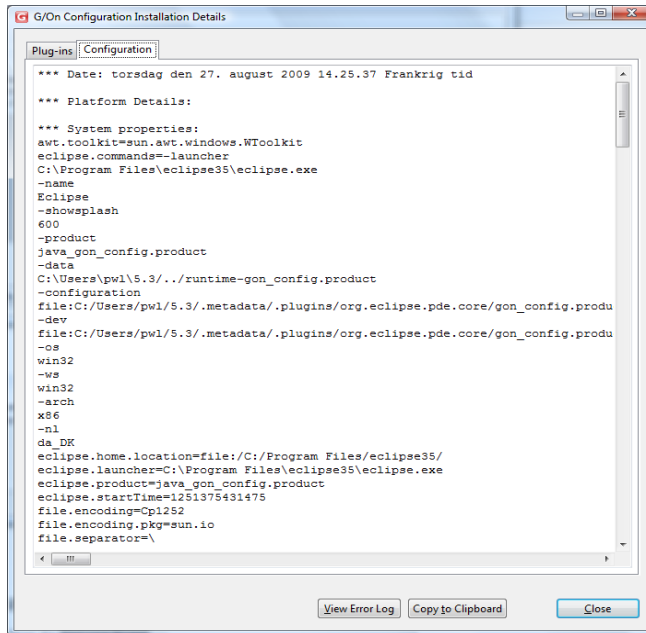
1. In the About Window:



2. Push the Installation “Details button”. You should get a window like this:



3. Select the “Configuration” Tab. The Window should change to something like this:



4. Click the "View Error Log" button. The error log should open or you will get a window in which you can choose which program you want to use to open it. A browser like Internet Explorer or Firefox is usually a good choice for viewing. If you want to save the log, then open it in an editor like Notepad.

*Welcome to the G/On Configuration*

Opens the G/On Configuration Welcome Screen.

## Advanced Setup Topics

### Backup and Restore

All the configuration and operational data in a G/On installation can be backed up to a folder. This folder can then be used as input for restoring the G/On installation to the state that was backed up. It can also be used for moving the installation to a different location.

The backup folder includes both ini files and other configuration files.

The backup folder also includes xml dumps of the database tables.

#### **Backup**

To make a backup, run the command:

```
.\gon_config_service\win\gon_config_service.exe --backup
```

This will by default generate a folder like this, with all the backup files:

```
.\gon_config_service\win\backup\backup_5.3.1-5_2010-01-05_083639.507000
```

The name of the folder will indicate the G/On version, and data and time of the backup.

The following options can be used, together with the `--backup` option:

```
--backup_do_not_create_sub_folder  
--backup_path=PATH
```

The first of these will place the backup files in `.\gon_config_service\win\backup` (not in a subfolder). The second will place the backup files in the folder indicated (*PATH*).

#### **Restore**

To make a restore, run the command:

```
.\gon_config_service\win\gon_config_service.exe --restore --restore_backup_path=PATH
```

where *PATH* is the full path to the folder containing the backup.

The following option can be used, together with the `--restore` option:

```
--restore_create_schema
```

This will force a restore of the database schema, in addition to restoring the data.

### Initialization of Tokens

#### **Initialization of Soft Tokens on USB-Key**

Before the G/On Management Client can use a USB-key as a soft token it has to be initialized. This can be done by creating the folder

```
.\gon_client\gon_init_soft_token
```

in the root of the USB-Key.

### ***Initialization of Soft Tokens on HD***

It is possible to prepare a soft token in a folder on the HD, and then afterwards copy it to a USB-Key. To do this, create a sub-folder of

```
.\gon_client_management_service\win\soft_token_root
```

containing the folders

```
gon_client\gon_init_soft_token
```

and it will appear in the G/On Management Client, just like a token, that can be enrolled, copied software packages to, etc.

The following example shows the folder structure needed for three certificate tokens:

```
.\gon_client_management_service\win\soft_token_root\key_a\gon_client\gon_init_soft_token
```

```
.\gon_client_management_service\win\soft_token_root\key_b\gon_client\gon_init_soft_token
```

```
.\gon_client_management_service\win\soft_token_root\key_c\gon_client\gon_init_soft_token
```

When the soft token has been enrolled, and the desired software packages have been installed, it can be copied to the root of a USB-Key, and it will appear as if the token had been enrolled and installed directly.

### ***Initialization of G&D Mobile Security Cards Key***

Before the G/On Management Client can use a G/On MicroSmart card as a token it has to be initialized. This can be done by creating the folder

```
.\gon_client\gon_init_micro_smart
```

in the root of the key.

### ***Volume Label on Tokens***

The linux “shortcut” (desktop icon) for starting the G/On client will only work if the volume label of the token is: G-ON. The same is true for the linux autostart feature.

### ***Access notification by mail***

A feature exists that sends a mail to the user's mailbox when he/she logs in. This feature has been disabled by default, but can be configured and enabled by modifying the

```
[access_notification]
```

section in the ini-file

```
.\gon_server_management_service\win\plugin_modules\ad\server_management\config.ini
```

The G/On Management Server need to be restarted in order for the configuration to be activated.

## LDAP and Active Directory plugins

G/On supports User Directory connections using LDAP and Windows API to Active Directory (AD). In this section the requirements to supported User Directories are described along with a section regarding which plugin to use for connecting to AD.

### ***LDAP to eDirectory***

#### ***Requirements:***

- IP or DNS address to an eDirectory server.
- User DN and password for an eDirectory user with browse rights OR
- Anonymous access set-up in eDirectory with a proxy user having browse rights
- Using SSL communication is highly recommended if the communication between the G/On and eDirectory server is visible from other machines. SSL communication requires a server certificate. A description on how to create a certificate can be found [here](#).

### ***LDAP to AD***

#### ***Requirements***

- IP or DNS address to an AD server.
- User DN and password for an AD user
- AD users should have permission to see their group memberships
- In order to enable password change, SSL communication must be used. SSL communication requires a server certificate. There are several descriptions from Microsoft on how to create such a certificate. One can be found here: <http://support.microsoft.com/default.aspx?scid=kb:en-us:321051>. Note even without password change, using SSL is highly recommended if the communication between the G/On and AD server is visible from other machines.

#### ***Limitations***

- By default, a maximum of 1000 users/groups can be fetched by an LDAP query to AD. This means that a maximum of 1000 users/groups will be available in G/On Management. The limitation is caused by the AD property "MaxPageSize", which can be altered using the "ntdsutil.exe" tool. See <http://support.microsoft.com/?kbid=271088> for a description on how to change an AD property using this tool.

### ***Native AD***

#### ***Requirements:***

- The server belongs to the domain OR
- The server belongs to another domain from which an outgoing trust has been set up to the domain. The trust type can be both forest or external.

- AD users should have permission to see their group memberships

Note that in order to create an outgoing trust, the trust has to be verified as an incoming trust in the other domain by a domain administrator. This can either be done by providing domain administrator credentials for the other domain during creation or by creating an incoming trust in the other domain using a shared trust password. Check Active Directory documentation for further details.

## ***LDAP AD vs. Native AD***

Since you can connect to AD using both an LDAP and a native plugin, the question of which one to use naturally arises. In order to help with this question we give a list of pros and cons of using the plugins.

### ***LDAP pros and cons***

#### **Pros**

- Server does not need to be on the domain
- Possible to connect to multiple unrelated AD's.
- Runs on Linux server

#### **Cons**

- Probably needs SSL communication, which complicates the configuration phase.
- Default query limitation to 1000 users/groups
- Subject to changes by Microsoft of LDAP support in AD.

### ***Native pros and cons***

#### **Pros**

- Easily configured if G/On server is on the domain
- Performs "real" AD login using Windows API's, which we may be able to use for extending functionality in the future, like e.g. Kerberos Single Sign On.

#### **Cons**

- Requires that G/On server belongs to the domain.
- Dependent on trust relationships in order to support multiple AD's

## **Fail-over set-up**

In this section we describe how to set up a G/On Installation with fail-over, i. e. with more than one Gateway Server machine. Note that this setup requires access to a SQL Server database. The setup is partially done manually, and thus requires some technical know-how.

The set-up described covers a specific fail-over configuration with:

- One G/On Management Service

- Two G/On Gateway Services, one running on the same machine as the Management Service and the other running on a separate machine (physical or virtual)

The Database Server should run on in its own fail-over set-up (presumably on different server machines).

### **Platform requirements**

Server OS: Windows Server 2003

DBMS: SQL Server 2005

### **Set-up instructions for a new installation**

In the following, “Server1” and “Server2” refer to the names of the servers on which the fail-over installation should be made.

1. On Server1, use the G/On installer and Server Configuration tool to install and configure the G/On System in the standard fashion.
2. Open the folder in which G/On was installed. In the sub folder \gon\_server\_management\_service\win, open the file “gon\_server\_management.ini” for edit.
3. In the ini file, find the following section:

```
#[db]
# encoding = utf8
# connect_string = sqlite:///./gon_server_db.sqlite
```

and change it to:

```
[db]
encoding = <db_encoding>
connect_string = mssql://<user>:<password>@<host>/<db>
```

where:

host = SQL Server host dns or IP

db = name of database

user = user name to connect as (must have administration rights on database)

password = password for user

db\_encoding = The encoding used in the database<sup>1</sup>

The specification of user and password may be omitted if the accounts used for running the Management and Gateway Server services have access rights to the database (Windows Authentication). In that case the connect string should look like this:

```
connect_string = mssql://@<host>/<db>
```

---

<sup>1</sup> By default the encoding used on the host.

4. In the ini file, find the following section:

```
#[message_queue]
# enabled = True
```

and change it to:

```
[message_queue]
enabled = False
```

5. Open the folder in which G/On was installed. In the sub folder `\gon_server_gateway_service\win` open the file “gon\_server\_gateway.ini” for edit. Repeat step 3. and 4. for this file.
6. Open the folder in which G/On was installed. In the sub folder `\gon_config_service\win` open the file “gon\_config\_service.ini” for edit. Repeat step 3. for this file.
7. Start a command prompt in the G/On installation folder. Run the following in order to create setup data:  

```
.\gon_config_service\win\gon_config_service.exe --generate_setupdata
```
8. The system should now be fully configured on Server1. You should now start the Management and Gateway Services, start G/On Management and set access for a user in order to check that the system works properly. Check that you can connect to the Gateway Server and start an application. When you are convinced that the system works properly proceed to step 9.
9. Copy the entire G/On installation folder from Server1 to Server2.
10. On Server 2, open the folder which G/On was copied to. In the sub folder `\gon_server_gateway_service\win` open the file “gon\_server\_gateway.ini” for edit.
11. In the ini file, find the following settings:

```
[service]
# title = G-On Gateway Server 1
# id = 1
```

and change them to:

```
[service]
title = G-On Gateway Server 2
id = 2
```

12. On Server2, install the G/On Services: Open a command prompt in the G/On installation folder and run the following command  

```
.\gon_config_service\win\gon_config_service.exe --install_services
```
13. On Server2, start the Gateway Server service. You can test it by temporarily stopping the Gateway Server service on Server1 and then try to connect. Note that in the Windows management console for Services, the Gateway Service will have a name ending with: (1), even if the id is 2.
14. On Server2 ,disable the Management Server service (it is never to be used).
15. In order that the Management Server service, running on Server1 can accept connections from Management clients, connecting though the G/On Gateway Server on Server2, the Management Server must be configured to listen on 0.0.0.0

instead of 127.0.0.1. However, this will allow connections to the Management service from any machine on the LAN, so it is recommended that a firewall is set up to only allow connections to the Management server's port on Server1, if the connections come from Server2.

In order to add another fail-over server, repeat steps 9.-14. above. Make sure that SQL Server accepts remote connections. In order to check this you can try creating an ODBC connection to the server. In SQL Server 2005 remote connection is enabled by starting the "SQL Server Surface Area Configuration" tool, click on the " Surface Area Configuration for Services and Connections" link and in the tool that opens enable remote connections for the server and possibly also start the "SQL Server Browser" service and set it to start up automatically, if this has not already been done. You should also check the SQL Server instance properties, on which remote connections can also be disabled.

### **Set-up instructions when migrating from SQLite**

In the following, "Server0" refers to the name of the server where there already is a G/On installation, using the SQLite DBMS.

"Server1" and "Server2" refer to the names of the servers on which the fail-over installation should be made. Server1 may be the same as Server0.

- A. On Server0, stop the G/On services, and do a backup (see the instructions regarding backup on page 23).
- B. *If Server1 is the same as Server0*, copy the entire G/On installation folder to a safe location, so it can be copied back, if something goes wrong in the following steps.
- C. *If Server1 is different from Server0*, use the G/On installer to install the G/On System in the standard fashion, but do *not* run the installation wizard in the Server Configuration tool. Instead, the server should be configured manually using the following steps:
  1. Install the G/On Services:  

```
.\gon_config_service\win\gon_config_service.exe --install_services
```
  2. If the system uses GPM packages that were not included in the installation, then copy these packages from *Server0* to *Server1*.
  3. Install the GPM packages:  

```
.\gon_config_service\win\gon_config_service.exe --generate_gpms
```
- D. Modify the backup: Edit the ini files, *which are all located in the backup folder*, in the same way as described above in "Set-up instructions for a new installation", steps 2.-6. Note that all ini files are located in the same folder under *config/ini* in the backup folder.
- E. Restore the modified backup on Server1 (see the instructions regarding restore on page 23).
- F. Installation on *Server1* is now complete. Do the remaining steps (8.,...), described above in "Set-up instructions for a new installation" in order to install to *Server2*.

## Troubleshooting

Error "Unable to connect to local service" shown at start-up	The underlying server program has not been started correctly. Check that the preferences (Edit → Preferences) are set up correctly. Check the log file <code>.\gon_config_service\win\gon_config_service.log</code> for any errors.

## FAQ

### How to change the external address or port of the G/On Gateway Server

Q: I have set up the server using the wizard in the G/On Server Configuration program. But the client connect address/port that I specified for the G/On Gateway Server was not correct. How can I change that?

A: If you are using a demo license, the fields are open so you can change these settings. If you are using a proper license, please obtain a new license with the desired address and port. **Note, however, in both cases, all tokens have to be re-adopted, after a change of client connect addresses/ports.**