

G/On Setup and Configuration Reference

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

G/On 5.4
Document revision 1
2010-12-29

G/OnTM 5

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 Setup and Configuration
- Getting started with G/On Management
- Getting started with Field Deployment
- Getting started with Secure Desktop
- G/On Setup and Configuration Reference
- G/On Management Reference
- G/On Customization Reference

© Giritech A/S, 2010
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
Contents.....	3
Before installation.....	4
Supported Platforms.....	4
Software Dependencies.....	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.....	10
Installation Wizard.....	10
Change Wizard.....	21
Upgrade Wizard.....	22
Package Generation Wizard.....	23
Menu.....	24
File Menu.....	24
Edit Menu.....	24
Generate Menu.....	24
Help Menu.....	25
Advanced Setup Topics.....	27
Field Deployment – Advanced Setup.....	27
Backup and Restore.....	28
Initialization of Tokens.....	28
Access notification by mail.....	30
Advanced User Setup.....	30
LDAP and Active Directory plugins	31
Fail-over set-up.....	34
Troubleshooting.....	38
FAQ	39
How to change the external address or port of the G/On Gateway Server?.....	39
How to install a changed license?.....	39

Before installation

Supported Platforms

G/On Client

- Windows XP (32 bit)
- Windows Vista
- Windows 7
- Apple Mac OS X 10.4 (Tiger), on Intel based Macs
- Apple Mac OS X 10.5 (Leopard), on Intel based Macs
- Apple Mac OS X 10.6 (Snow leopard), on Intel based Macs
- 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, Windows Server 2008R2

G/On Server

- Windows Server 2003 R2 SP2, Windows Server 2008 SP2, Windows Server 2008R2

Software Dependencies

G/On Management requires Java runtime, JRE6, 32bit version. This is true, even if the OS is 64bit. When installing G/On Management as a package on a token, it is possible also to install a package containing the Java Runtime, on the token. When this has been done, G/On Management can be run from the token, no matter whether the PC has the correct JRE installed or not.

G/On Setup and Configuration requires Java runtime, JRE6, 32bit version. This is true, even if the OS is 64bit.

Client Installer. In order to be able to generate a Client Installer for field deployment, the Nullsoft scriptable install system must be installed on the G/On server. Get it here: <http://nsis.sourceforge.net/>

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

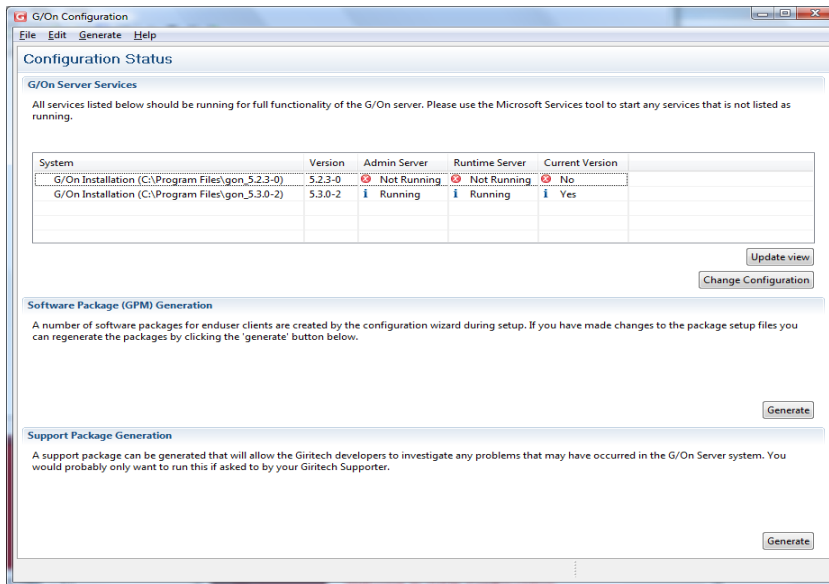
If no license is found, the Welcome Screen will look like this:



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:

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

Below the table there are two buttons:

Update View	Checks and updates the information in the table. Could for example be used after starting server services.
Change Configuration	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. Terminology notes: GPM stands for G/On Package Management. Currently, most of the packages contain software to be deployed on the client side, e.g., application clients. These packages are also referred to as Client Packages, and the Client Package Management actions in the menu of the end-user client can be used for installing, updating and deleting client packages.

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`

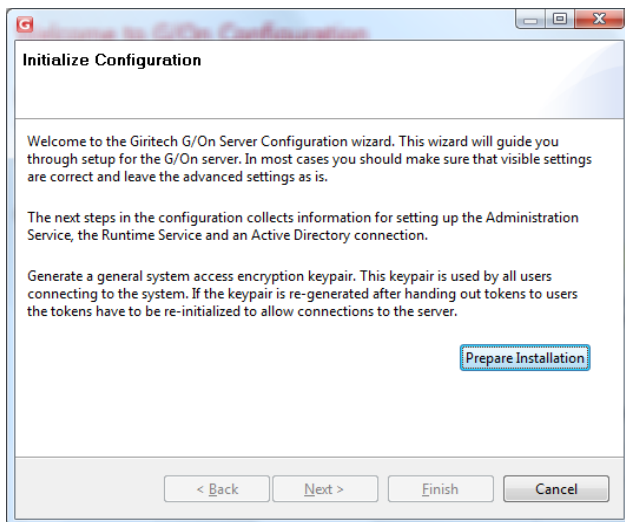
Wizards

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.

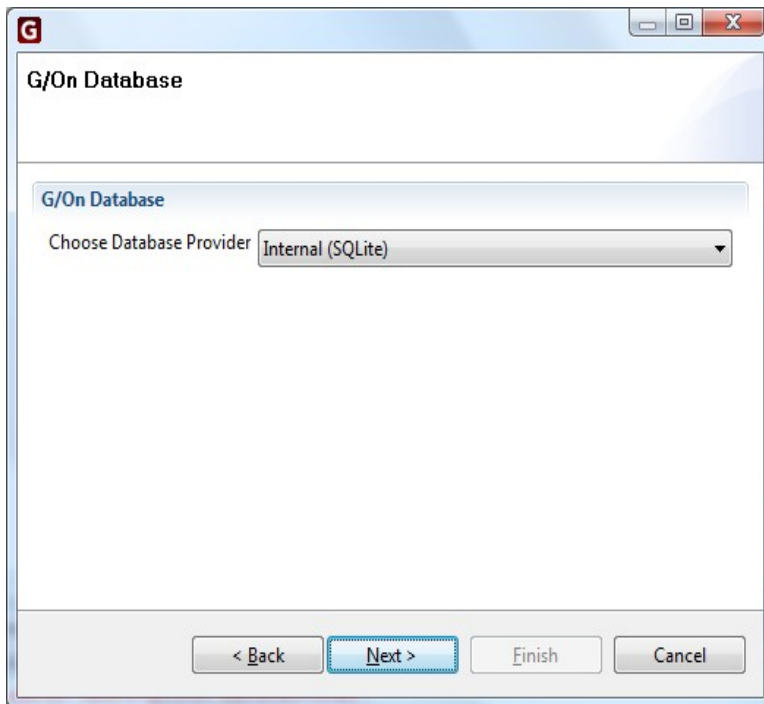
Initialize Configuration



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.

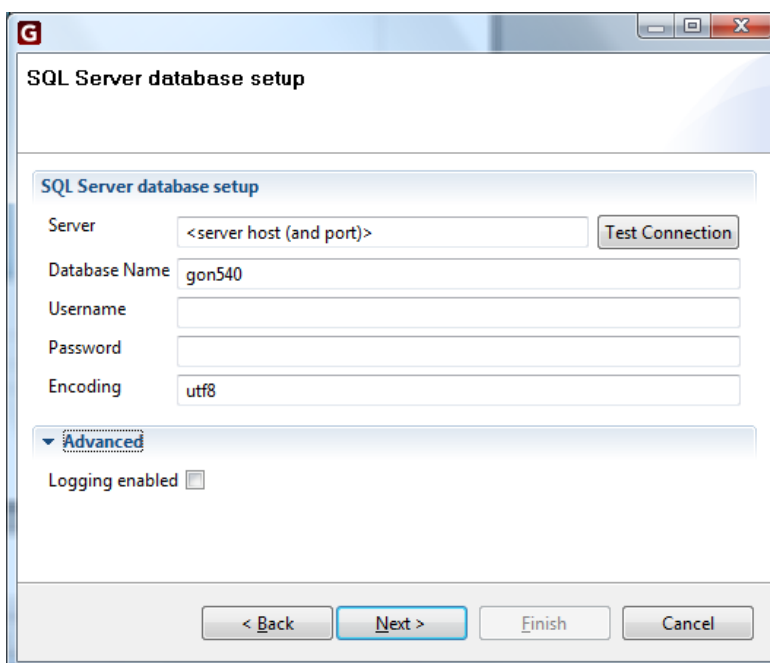
Database setup

A database is used for saving system setup.



You must choose database provider. If you want to use the default internal database then no further configuration is required. If you choose "SQL Server", a new window for entering further configuration will open when you press "Next".

SQL Server Set-up



In this window, the SQL 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:

Server	Name or IP address and port number of SQL Server host., e.g. myhost:1433
Database Name	The name of the database, which will hold G/On data
Username	User name for a database administrator for the specified database. Leave blank if NT authentication should be used.
Password	The password for the specified user.
Encoding	The database character set encoding.

OBS: The default value is “utf8” – but this will not work with SQL Server databases. It is important that the value you configure in G/On matches the value of the database, so you should check the encoding of the database and fill in the correct value in this field in G/On

You can find the encoding of the database, by SQL queries like these:

First try:

```
SELECT databasepropertyex(<database name>, 'Collation')
```

If this returns the value “NULL” try:

```
SELECT SERVERPROPERTY('Collation')
```

You should get a collation name, e.g., “Danish_Norwegian_CLAS”

Use the collation name in the query:

```
SELECT collationproperty(<collation name>, 'CodePage')
```

You should get a codepage number, e.g. “1252”.

For G/On, you must add “cp” before the code page number, to get the encoding name, e.g. “cp1252”, which you can then fill into this field.

Advanced:

Logging enabled	Enable logging
-----------------	----------------

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!

Logging enabled Enable logging

Logging verbose level	The primary purpose of logging in this context is for support reasons. 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).
Automatic Approval of Enrollment Requests	If checked, the personal token assignments created as a result of field enrollments are automatically activated. If not checked, these personal token assignments will be inactive until manually activated by an administrator.
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:

Listen Port	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.
Server DNS names or IP addresses	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.
Port the client connects to	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:

Listen IP	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).
Logging enabled	Enable logging. The primary purpose of logging in this context is for support reasons.
Logging 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).
Session logging enabled	Log each user session in a separate file
Authorization time-out	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.
GPM Concurrent Downloads	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 simultaneously do field updates or installs of the software on the tokens. If this limit is reached, the next user that attempts an installation or update will observe that the process is paused before download, and then automatically resumed at a later time, when fewer users are downloading.
Inform User before first access enabled	This option can be used to acquire user acceptance of the terms and conditions under which access is granted.
Inform user before first access message file	If the previous option is enabled, this file contains the message which the user must accept at the first time access is about to be granted. When using a relative path, note that the current working directory is: gon_server_gateway_service\win
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.

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

Standard:

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

Advanced:

HTTP Listen Address	Specify the address from which HTTP Encapsulated traffic are accepted. 0.0.0.0 (default value) defines all addresses.
HTTP Encapsulation Logging level 2 enabled	Debug logging enabled.
HTTP Encapsulation Logging level 3 enabled	Very detailed logging level of all activities. Using this level will severely impact performance – and should not

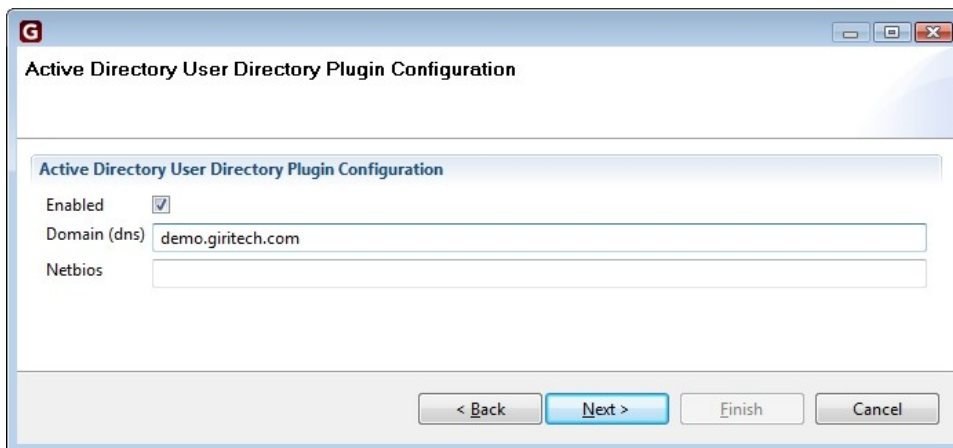
Logging level 3 enabled be used unless needed for support reasons (remember to deactivate).

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 in the Active Directory management interface, check the "Effective permissions" in the "Advanced security settings" of the account, and see if the permission "Read Group Membership" is in effect.



The screenshot shows a wizard window titled "Active Directory User Directory Plugin Configuration". The window has a blue header bar with a "G" logo. Below the header, the title "Active Directory User Directory Plugin Configuration" is repeated. The main content area contains the following fields:

- Enabled:** A checkbox that is checked.
- Domain (dns):** A text box containing the value "demo.giritech.com".
- Netbios:** An empty text box.

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

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

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.

OBS: The Active Directory configuration in the previous step of the wizard does *not* depend on configuration of LDAP. So you do not have to configure LDAP unless you really want G/On to use the LDAP protocol when communicating with the user directory. See page 31 for a discussion of issues related to AD and LDAP and which to use.

Standard:

Enabled	Enable or disable LDAP plugin.
Directory Name	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 never be changed once users and groups have been entered in the system.
Root DN	The root DN under which users, groups and ou's should be found.
Server host list	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. Example : firstserver:636, secondserver, thirdserver

Advanced:

Is Active Directory	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.
Use SSL	Check if SSL communication should be used.
SSL Certificate	Full path to Certificate file used for SSL communication.
Don't Require Server	Check if G/On server should not check the server certificate when connecting when SSL is used. Use to enable

Certificate	SSL communication without server verification.
User DN	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.
Password	Password for the user specified account
Password Change	Check if password change via G/On should be disabled.
Disabled	
Password Expiry Warning Time	Time (in number of days) before which the user is warned about password expiring. Enter '0' in order to disable warnings.

Local Windows User Plugin Configuration

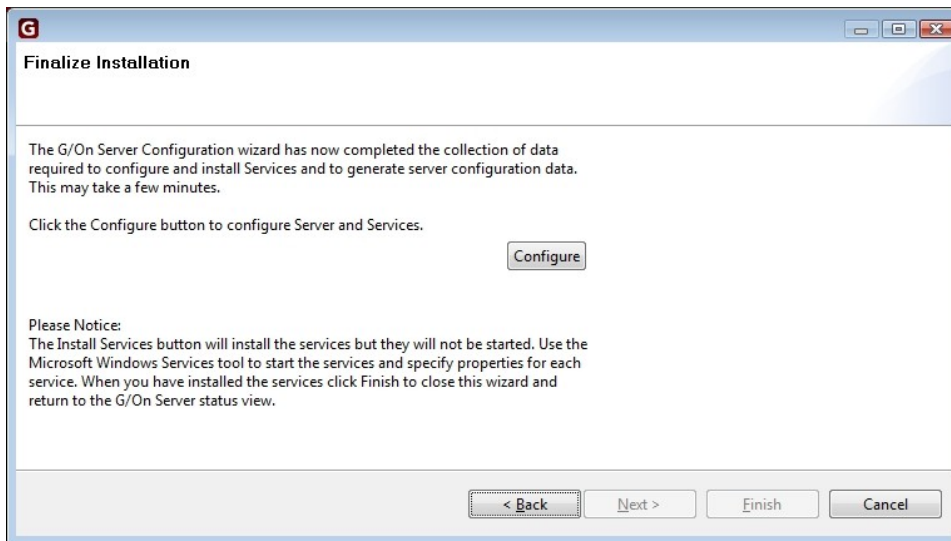
The Local Windows User plugin is used for user verification and for obtaining information about local users and groups that exist on the server machine where the G/On Gateway and Management Servers are running.

Note: In order for this to work correctly the G/On Management and Gateway Servers should run on the same machine, so they will “see” the same local users and groups.

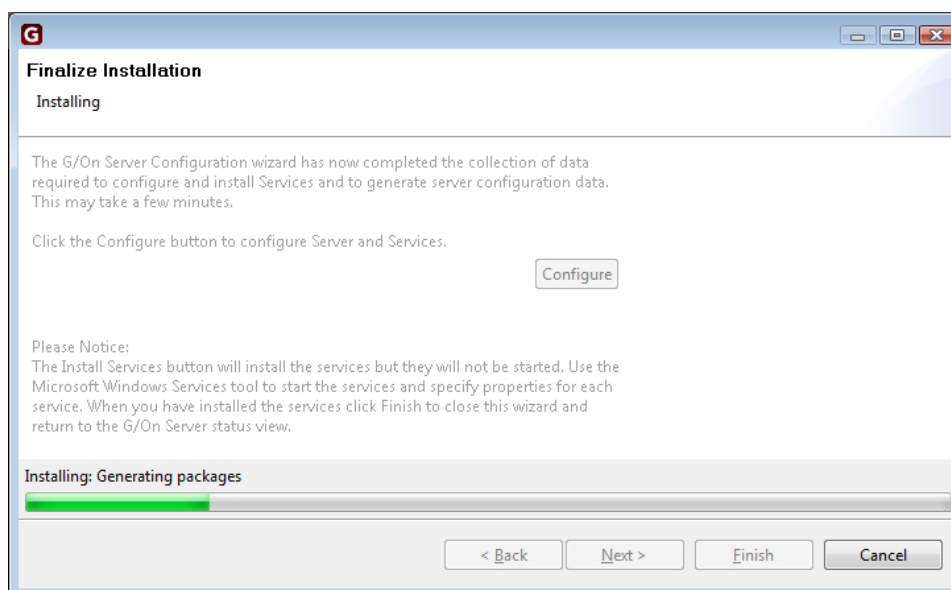
Standard:

Enabled	Enable or disable Local Windows User plugin.
Maximum Password Age (days)	When a user's password is older than this limit, G/On will ask the user to change the password. G/On cannot read the maximum password age for local Windows users, so this must be entered manually.

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.

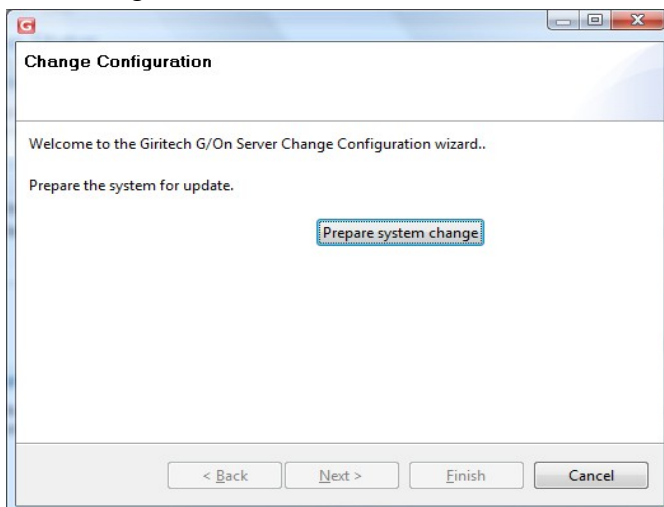
OBS: Note that the Wizard only creates the G/On Services. The services have to be started manually. You can start the G/On services by using the “Services” Management interface in windows. (**All Programs**→**Administrative Tools**→**Services**)

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 much the same structure as the Installation Wizard. On the first page, a “Prepare Change” job has to be run. The “Prepare Change” job reads the current settings from ini-files, so they can be presented in the following steps of the wizard.

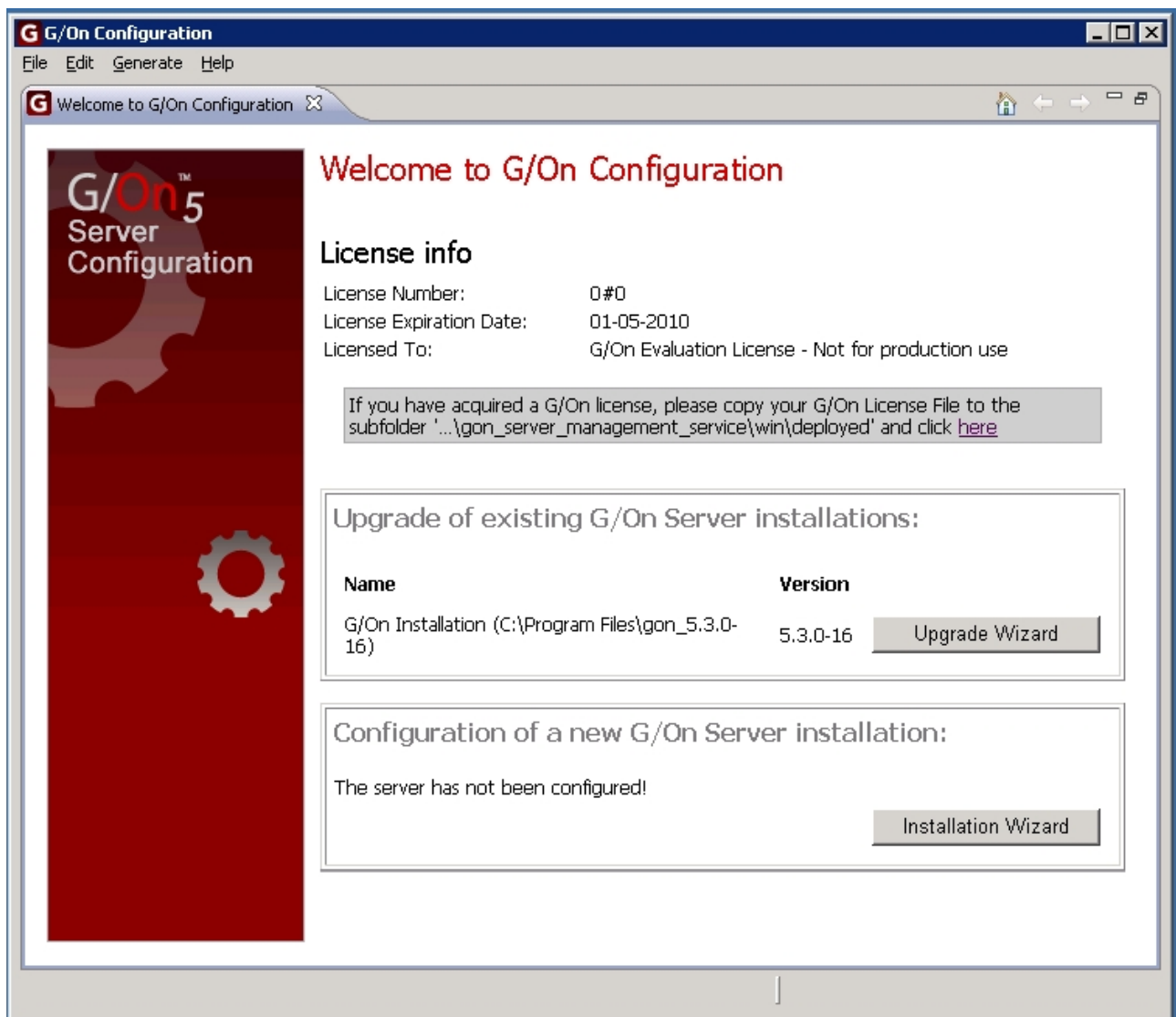
On the following pages, configuration information can be entered and on the final page, the change is finalized. Here is a screen shot of the first page:



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.

Upgrade Wizard

The Upgrade Wizard is used for upgrading a previously installed G/On System to the same version as that of the G/On Server Configuration tool being used. When starting the Server Configuration tool, it scans the machine for existing G/On installations, and if any are found, they are presented on the Welcome page, each with a button to start an upgrade from that version:



The Upgrade Wizard has much 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.

If the system being upgraded from uses an SQLserver database, the default during upgrade is to make a new database instance, named after the G/On version, e.g. gon540. However, the upgrade wizard allows the administrator to choose another name or even the name of the old database instance, which in this case will be overwritten.

Note, that during the upgrade, the system from which the upgrade is made will not be affected (except when it is deliberately chosen to re-use an existing database instance). You will need to stop the services of the “old” version manually, and uninstall it manually, if you desire to remove it.

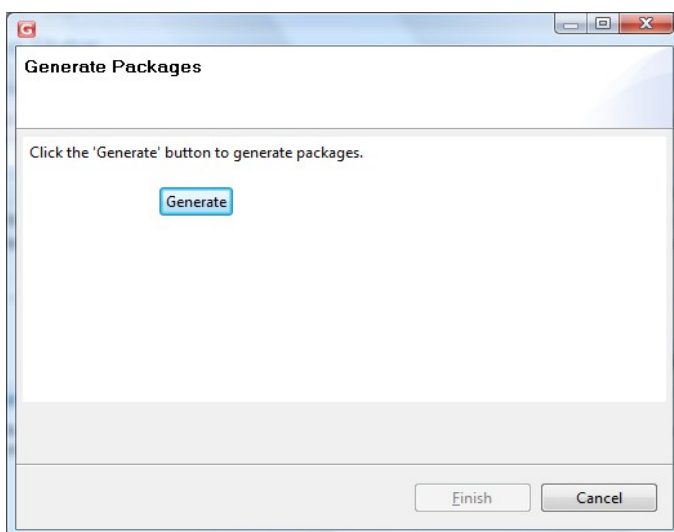
OBS: Note also, that additional GPM files that may have been added to the previous version after it was installed are not automatically copied to the new version during an upgrade. This includes, e.g., the package with the secure desktop linux image, and also other packages, which the customer or partner has added.

Package Generation Wizard

This wizard generates GPM packages. Packages are also generated as part of the Installation Wizard, so this Wizard need only be run if package sources or definitions or package collections 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

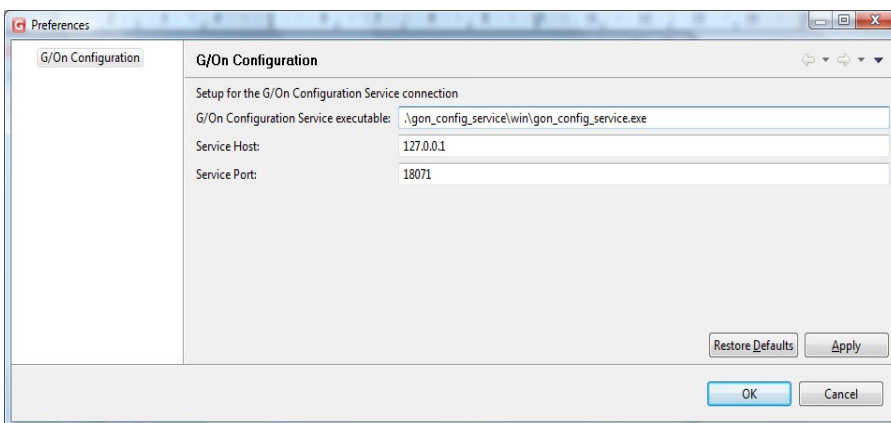
Quit G/On Configuration

Quits the program

Edit Menu

Preferences

Opens the preferences window:



The following options are available:

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

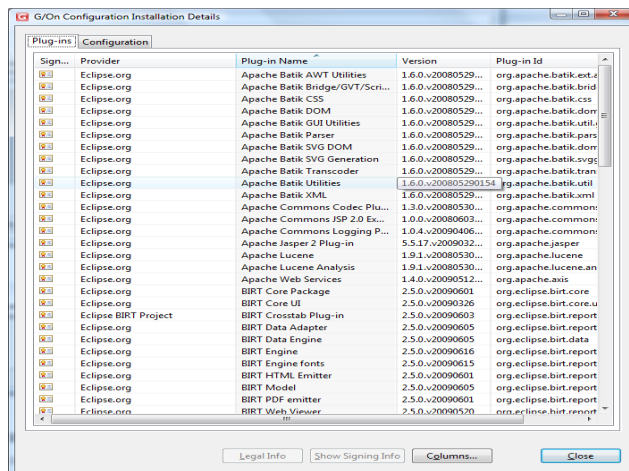
Open the “About” Window. Apart from version and copyright information, you can access the Server Configuration client error log from here by following the steps below. Note that this log only pertains to the client (GUI) part of the Server Configuration Utility.

The error log is fetched like this:

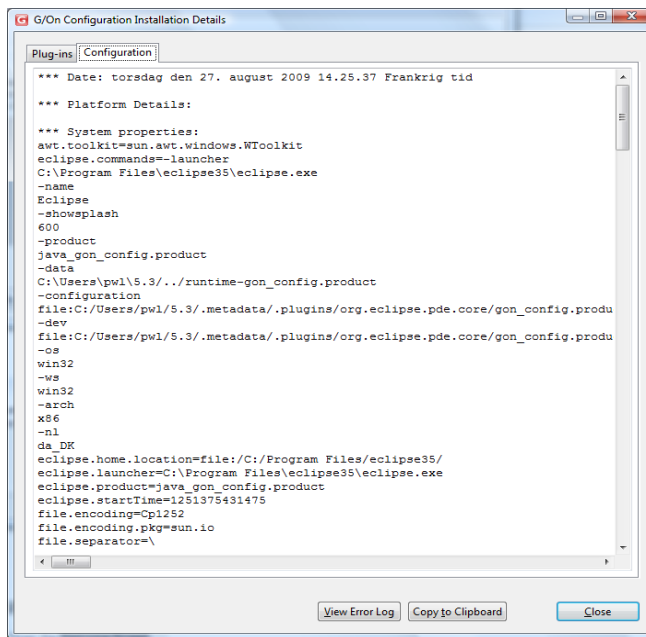
1. In the About Window:



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

Field Deployment – Advanced Setup

For an introduction to field deployment, including how to generate a client installation program, see the separate document: “Getting started with Field Deployment”. The following subsections only cover a few, more advanced topics related to field deployment.

Including additional packages to be installed by the client installation program

When generating the client installation program, the packages in the following folder are automatically included:

```
.\distribution\gon_client_installer\win\nsis\gpm
```

It is possible to manually copy packages to this folder and then generate the client installation program as described in “Getting started with Field Deployment”.

However, it is also possible to make sure that the newest versions of the desired packages are always copied automatically to this folder. To ensure this, edit the following package collection, and add the names of the desired packages:

```
.\gon_server_management_service\win\gpm\gpmcdefs\dist_client_installer_win.gpmcdef.xml
```

See the separate document “G/On Customization Reference” for a general description of Package Collections.

Controlling where the client installation program offers to install

By default, the client installation program offers the end-user a choice of installation destination: either on a (new) computer user token, or on one of the hardware tokens inserted in the PC, if any.

However, it is possible to make two variants of the installation program: One will only offer to install on a computer user token, the other will only offer to install on a hardware token.

To make one of these variants, edit the following ini-file:

```
.\gon_client_installer\win\gon_client_installer.ini
```

In this file, change the setting for `desktop_enabled` to `False`, in order to disable computer user tokens as the installation destination:

```
desktop_enabled = False
```

Similarly, change the setting for `token_enabled` to `False`, in order to disable hardware tokens as the installation destination:

```
token_enabled = False
```

After changing the ini-file, generate the client installation program as described in “Getting started with Field Deployment”.

Automatic Approval of Field Enrollment Requests

In the Management Server Configuration (see page 13 and onward in this document) there is an advanced setting, which enables automatic approval of field enrollment requests.

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_5.4.0-16_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 sub-folder). 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 soft 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 MicroSmart (USB) Tokens

Before the G/On Management Client can use a G/On MicroSmart (USB) 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.

Initialization of Computer User Tokens

Normally, Computer User Tokens are enrolled by using the procedure for field enrollment. But it is also possible to enroll a Computer User Token by running the G/On Management Client on the PC where the Computer User Token has been installed.

Before the G/On Management Client can use a Computer User Token, the token has to be installed by using a G/On Client Installer program. How to generate such an installer program is explained in the separate document: "Getting started with Field Deployment". When the installer program has finished the installation task, it offers to options: "Launch" or "Exit" – choose "Exit". At this point, the Computer User Token has been installed, so it will be recognized by the G/On Management Client.

No Initialization of Hagiwara Tokens

It is *not* necessary to initialize a Hagiwara token before the G/On Management Client can use it. However, the token must be formatted so it contains both a CDROM and a normal flash storage device.

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.

Advanced User Setup

Users are drawn from the user directory plugins, i.e. the AD, LDAP or local Windows plugins. Each user must have a unique login in G/On. This fully qualified login is constructed as <login>@<directory name>, where *login* is the users login name or initials and *directory name* is a (unique) name from each plugin: For AD it is the domain DNS, for LDAP it is the specified directory name and for local Windows users it is always *local*. It is by default possible to log in using only the login part, provided that there is not a user in another directory with the same login. In the latter case a fully qualified login is necessary for the user to log in.

User and group limit in G/On Management

In order to improve performance in G/On management there is a limit on how many users/groups are retrieved from the server. These limits can be configured manually by editing the *gon_server_management.ini* file. The options are called *users_returned_limit* and *groups_returned_limit* and has a default value of 500. Setting the limit to 0 is interpreted as no limit. Setting the limit to a negative number means that no users/groups are fetched initially, when the user/group pane is opened. When a search string is entered a the (positive) value of the setting is used as a limit for how many elements to show.

Note that the user directory may also have a limit on how many users/groups that can be fetched in one query (see the section on AD and LDAP plugins). The limits for G/On Management should always be set to something less than this limit in order for searches in G/On Management to work properly.

Require fully qualified login

It is possible to configure the Gateway server to always require a fully qualified login. This can be useful in a multi user directory setup, where user login in one directory should be independent of any users with the same name in other directories.

The option must be set manually by editing the `gon_server_gateway.ini` file. Add the line:

```
require_full_login = True
```

in the `authorization` section in order to require fully qualified login.

If the option is set and a user enters a login without a '@' in it, he/she will be presented with a new login prompt demanding a fully qualified login.

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 is available in G/On Management. You can however use the search/filter functionality in G/On Server Management in order to find the users/groups you are looking for. 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.
- Locking out a user after a number of failed login attempts (usually 3) does not work when logging in to AD using LDAP.

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.

By default this plugin has the same 1000 users/groups limitations as described in the the LDAP to AD section. This limit can be overridden by editing the file

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

Add the line :

```
override_max_page_size = True
```

in the domain section(s).

On some installations it has been observed that the local system account running the Server Gateway service did not have sufficient privileges for reading user group memberships. A new, but not fully tested, way of finding group memberships has been developed for 5.4.1, which should address this issue. In order to activate it the following line must be added to the

```
gon_server_gateway_service\\win\\plugin_modules\\ldap\\server_gateway\\config.ini file:
```

```
use_query_for_group_members = False
```

in all relevant domain section(s)

LDAP to other directories.

There are many LDAP directories apart from the ones described here (e.g. Apache, OpenLDAP, Siemens DirX,...), which probably work with G/On as well. We have, however, not conducted thorough testing against these directories, and therefore cannot include them in supported LDAP directories. Note also that property names and property usage can vary from one directory to another, so in order to connect to one these directories, some of the property names and queries used may have to be changed. This is also possible, but requires manual edit of LDAP configuration files. Please contact Giritech support for more information about this.

LDAP and SSL

In order to use SSL communication between the G/On server and LDAP directory server you only need to:

1. Make sure your LDAP server supports SSL communication (for AD this requires a certificate installation)
2. Check the "Use SSL" box in LDAP configuration.

However, if you want the G/On server to verify the LDAP server as well, you have to create a client certificate and specify the path to it in LDAP configuration. Whether this is necessary depends on how the servers connect, more specifically it depends on whether the G/On server can trust that it is talking to the right LDAP directory.

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 may complicate 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.
- Better error messages.

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 use of 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. Remember to choose SQLserver as the database management system.
2. In the ini file, find the following section:

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

and change it to:

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

OBS: Make sure that the number sign is removed from both lines

3. 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 2. for this file.
4. 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 5.
5. Copy the entire G/On installation folder from Server1 to Server2.
6. 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.
7. 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
```

OBS: Make sure that the number sign is removed from both lines

8. 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
```
9. 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.
10. On Server2, disable the Management Server service (it is never to be used).
11. 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 5.-10. 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 28).
- 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 all the server ini files, *which are all located in the backup folder*, in the following way:

1. 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>
```

OBS: Make sure that the number sign is removed from all three lines

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 database¹

¹ By default the encoding used on the host.

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>
```

2. Skip this step for *gon_config_service.ini*. Find the following section:

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

and change it to:

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

OBS: Make sure that the number sign is removed from both lines

- E. Restore the modified backup on Server1 (see the instructions regarding restore on page 28).
- F. Installation on *Server1* is now complete. Do the remaining steps (4,...), described above in "Set-up instructions for a new installation" in order to install to *Server2*.

Troubleshooting

<p>Error "Unable to connect to local service" shown at start-up</p>	<p>The underlying server program has not been started correctly.</p> <p>This typically happens on Windows server 2008, if G/On Configuration has not been started with "Run as administrator".</p> <p>Also 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.</p>
<p>"Error: Unable to generate checksum for ..."</p>	<p>If the G/On Management client is running on the server, Software Packages (GPM) Generation in the G/On Configuration client will give the following error:</p> <p>"Error: Unable to generate checksum for ..."</p> <p>It happens because one of the packages to be generated contains the Management client files, and one of these gets locked, when the Management client is running.</p> <p>Workaround: Exit G/On Management client (if running on the server), before generating packages.</p>

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-enrolled, after a change of client connect addresses/ports.**

How to install a changed license?

If you have acquired a changed license file, you should place it in the folder "`\gon_server_management_service\win\deployed`". Thereafter, you may want to start and complete the Change Wizard, in order to take advantage of the changes in your new license file, e.g., to use new/changed client connect addresses.