

G/On Setup and Configuration

G/On 5.5

Document revision 1.2

2011-09-30

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:

<http://www.giritech.com/int/Support-Download/Product-Download/G-On-5.5-Product-Download>



© Giritech A/S, 2011
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

Getting started

Introduction.....	6
Before installation.....	7
Supported Platforms.....	7
Java Runtime Environment.....	7
User Directory.....	7
Preparations.....	7
Installation.....	8
Server Installation.....	8
Initial server configuration.....	9
Directory Services Configuration.....	13
Finalize Installation.....	15
Configuration Status.....	16
Using G/On Management.....	17
Changing the Server Configuration.....	17
Restarting from Scratch.....	17

Reference

Before installation.....	19
Supported Platforms.....	19
Software Dependencies.....	19
Introduction.....	20
Overview: Making New Installations and Upgrades.....	21
G/On Configuration Welcome Screen.....	21
No License.....	22
Main Status Window.....	23
G/On Management Service.....	23
Software Package (GPM) Generation.....	24
Support Package Generation.....	24
Wizards.....	25
Installation Wizard.....	25
Change Wizard.....	42
Upgrade Wizard.....	43
Package Generation Wizard.....	46

Menu.....	47
File Menu.....	47
Edit Menu.....	47
Generate Menu.....	48
Help Menu.....	48
Advanced Setup Topics.....	50
Field Deployment – Advanced Setup.....	50
Backup and Restore.....	51
Initialization of Tokens.....	52
Access notification by mail.....	54
Advanced User Setup.....	54
LDAP and Active Directory plugins	55
Installing Addition Gateway Servers with a Gateway Installer.....	58
Creating Custom Client Installers.....	63
Troubleshooting.....	66
FAQ	67
How to change the external address or port of the G/On Gateway Server?.....	67
How to install a changed license?.....	67

Getting started

Introduction

A full functioning installation consists of the following steps:

1. Preparation of the installation
2. Installing the G/On software on the G/On server
3. Configuration of the two G/On service modules, G/On Gateway and G/On Management
4. Setting up basic policies and adding users and authentication tokens

This document describes the basic preparation, installation and configuration of the G/On solution. The last step (number 4 above), of setting up basic policies and adding users and authentication tokens is described in the document: *G/On Management Client*.

Assumptions: In step 4 (*G/On Management Client*), it is assumed that the G/On server is installed on a *physical server machine, with a USB port*, which can be used for enrolling and deploying software to the first token(s). For demo/test installations, you may install on a Windows desktop OS (XP, Vista or 7). This usually works fine, even though it is not supported for production use. The only exception is the port scanning feature which does not work properly on the desktop operating systems.

Before installation

Supported Platforms

To check whether your intended platform is supported, see page 19.

Java Runtime Environment

The G/On 5 Server Configuration and G/On 5 Management requires that Java Runtime Environment (JRE) is installed. Get it here: <http://www.java.com/>

Note: The 32bit version of the JRE must be installed, even in the case where a 64bit OS is used.

User Directory

G/On can connect to three types of user directories; Active Directory, a LDAP user directory or the local Windows users on the server machine. In order for Active Directory integration to work properly the 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. See the document: G/On Setup and Configuration Reference for more details on how to choose and setup user directory.

Preparations

Before starting the installation please consider collecting the following information:

<p>Which IP address and tcp port should the clients connect to, when connecting from outside the firewall?</p> <p>Symbolic/DNS name for the IP can also be used. The IP address is part of the G/On License File, and must be specified when ordering G/On.</p>	<p>IP/DNS address and Port that the G/On client should connect to.</p> <p>The default port number is 443, even though 3945 is the official IANA allocated port-number for G/On. If possible, port 80 – or 443 are normally good choices, as these ports are open outbound in most environments. So by selecting these ports, it is even more likely, that G/On clients will be able to connect to the G/On server</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Please note, that IP address and port number(s) must be specified at ordering time – and is part of the license agreement.	
Which user directory should be used to authenticate users.	Connect to Active Directory through native Windows API or to eDirectory or Active Directory through LDAP

Installation

The installation is done using the installer, which at the end will start the G/On Configuration program. G/On Configuration includes all the basic, technical setup of server IP addresses etc.

Server Installation

Please download the latest installer from Giritech's website at

<http://www.giritech.com/int/Support-Download/Product-Download>

Store it on the server on which you want to install G/On.

Installation is done in two steps: actual installation of the G/On Server software modules – and subsequently the initial configuration of the G/On main components.



The installation requires about 400MB free disk space.

Once the installation is completed, you can continue directly with the initial configuration (recommended). Once you press finish – and if you have checked the "Run G/On Configuration Wizard" - allow some time for the wizard to start. Alternatively, you can find the G/On Configuration program in the Windows Start Menu.

Note: 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".

Initial server configuration

Initial Server Configuration is done through the configuration wizard. Before configuring the G/On server, you may wish to obtain a proper G/On license file. This file will determine the number of G/On users possible, as well as specifications regarding purchased options etc.

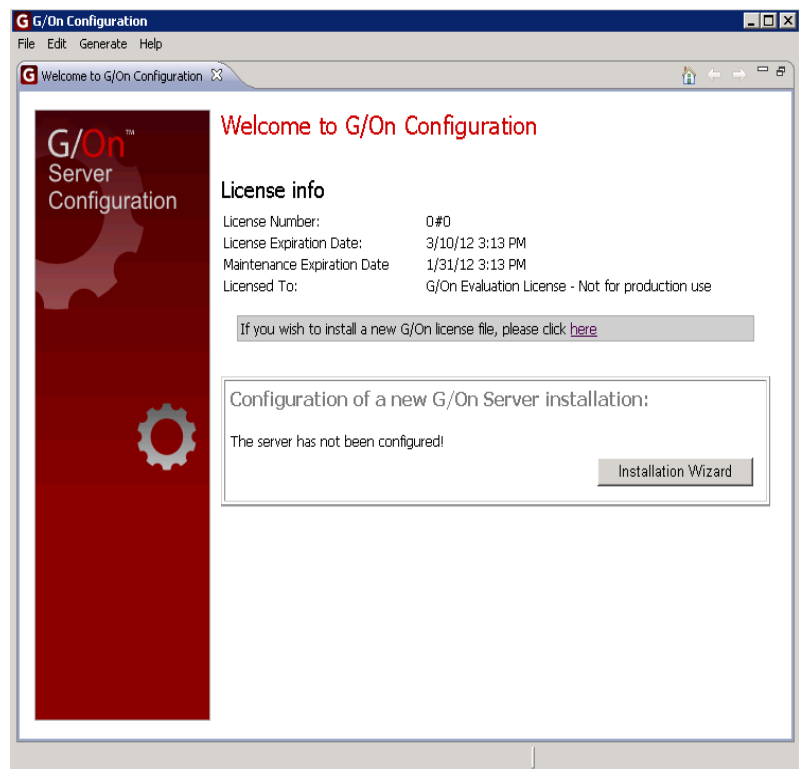
If you do not use a proper G/On license file, the installation will proceed with a so-called demo-license. This will allow you to test G/On, but not all options.

License Handling

All G/On installation options are specified in the license file. The license file is obtained as part of the purchase process for G/On. If you do need a proper G/On license file, please contact your Giritech Partner.

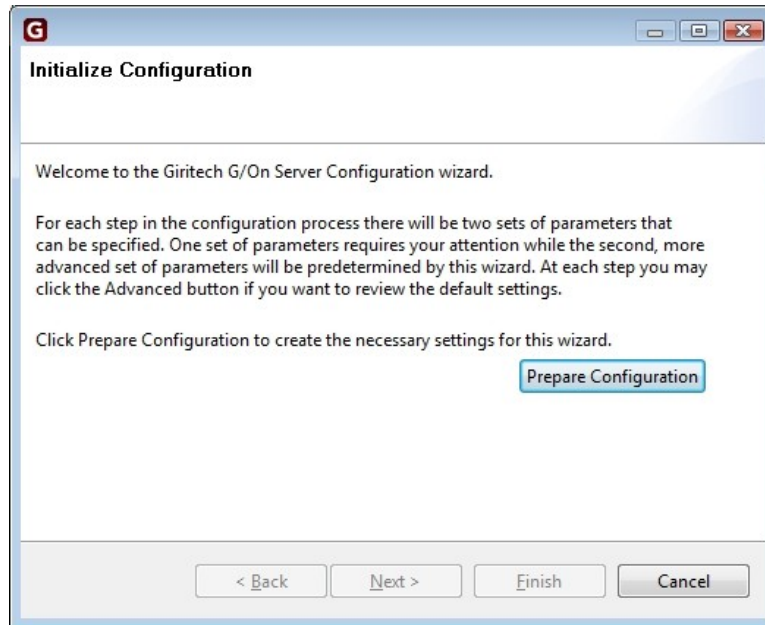
In the welcome screen to the right, you can see the current status of your license file:

If you have received a proper license file, you can install by clicking on the link in the welcome screen.



Using the Installation Wizard

Press the Installation Wizard button on the configuration welcome screen. You can also start the Wizard at a later time, from the Windows G-On program menu: "G-On Configuration". Once started the following instruction screen will be shown:



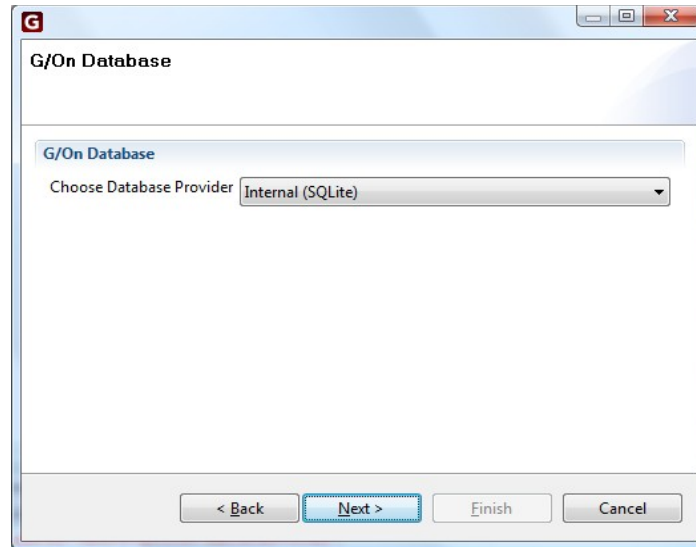
Please read, and continue by clicking Prepare Configuration - and the Configuration Wizard will generate an initial set of configuration data. Once done, click Next on the Initialize Configuration screen.

A G/On installation will normally have at least two services running -

1. **The G/On Management Server** – allowing Management of the solution (users, authentication and authorization policies)
2. **The G/On Gateway Server** – performing the actual tasks of connecting users with applications according to the policies specified.

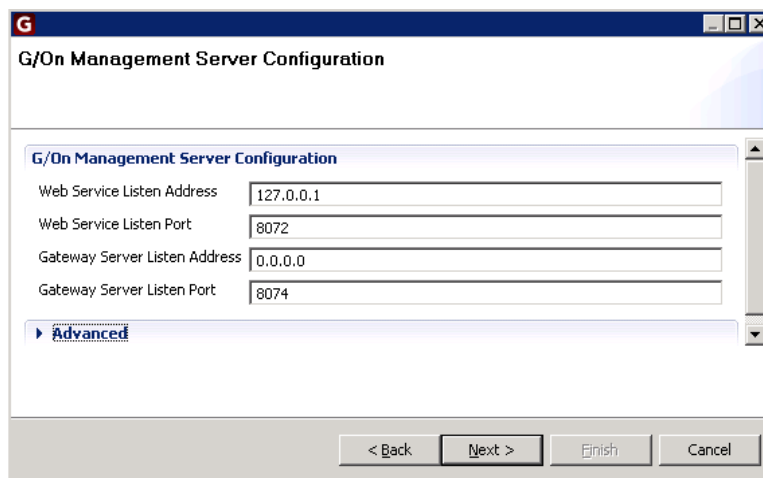
Each server/service is configured separately as described in the following.

Database Configuration



Choose the default Internal database and click Next.

Management Server Configuration



Web Service Listen Address: 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.

Web Service Listen Port: To enable the G/On Management Server, a port must be designated (default is 8072). This port is used for the G/On Management client to connect to the management Server.

Gateway Server Listen Address: IP address where the Management service should listen for connections from Gateway Servers.

Gateway Server Listen Port: TCP Port where the Management service should listen for connections from the Gateway Servers.

Note: In the default set-up, the Management Client must run on the same machine as the Management Server, in order to be able to connect to it. If you want to run the Management Client on a remote PC, define a G/On menu action for this purpose and run G/On Management through a G/On connection.

Gateway Server Configuration

G/On Gateway Server Configuration	
Listen Port	443
Client Connect Addresses	demo.giritech.com
Client Connect Ports	443
Management Server Connect Address	127.0.0.1
Management Server Connect Port	3074

▶ Advanced

< Back Next > Finish Cancel

Listen Port: The port that the Gateway Server listens on in order to accept connections from G/On Clients.

Client Connect 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.

Client Connect Ports: The default port number is 443, even though 3945 is the official IANA allocated port-number for G/On. If possible, port 80 – or 443 are normally good choices, as these ports are open outbound in most environments. So by selecting these ports, it is even more likely, that G/On clients will be able to connect to the G/On server. The port must be specified at the time of ordering G/On, and is part of the license (file). If using the demo license, any port can be specified.

Management Server Connect Address: IP address or DNS name, which the Gateway servers should use for connecting to the management server.

Management Server Connect Port: TCP Port number, which the Gateway servers should use for connecting to the management server.

Note: Remember to set up your firewall/router so it accepts connections on these ports and forwards the connections to the Listen port specified for the Gateway server (see above).

HTTP Encapsulation

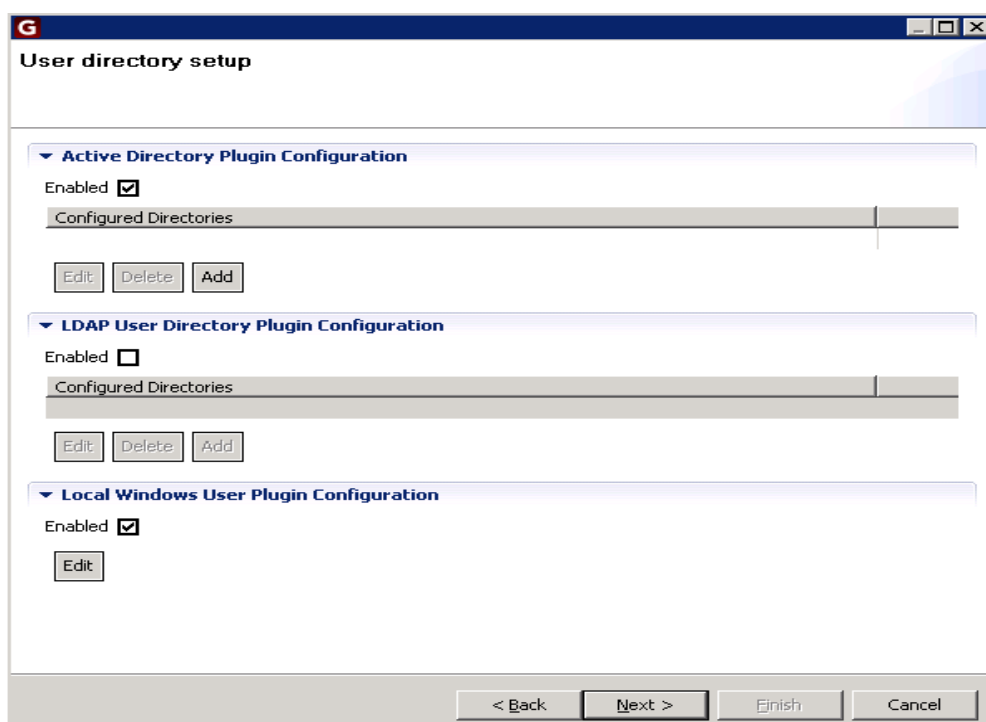
In some environments, a deep packet inspection firewall or other might block the communication between G/On clients and the G/On server. To allow connectivity in these situations, the **HTTP Encapsulation** option should be specified when ordering G/On.

If the feature is not included in your license, or you do not wish to configure it, you can skip this step.

For information on configuring this option, see the G/On Set-up and Configuration Reference.

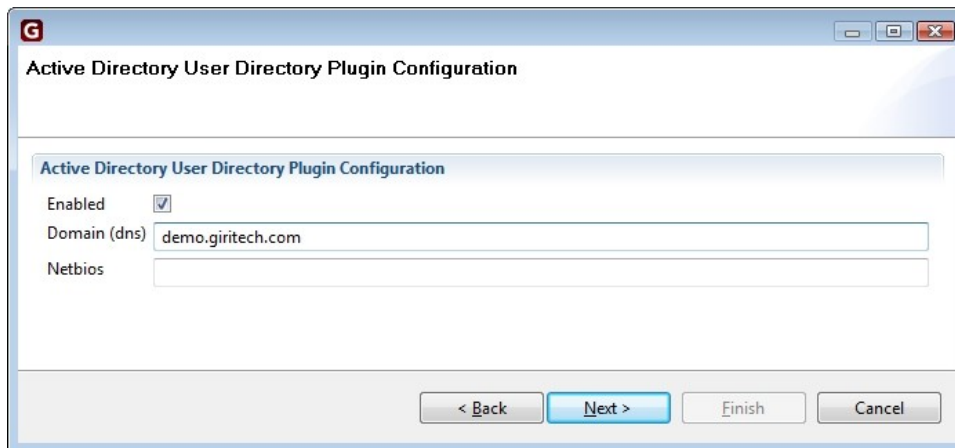
Directory Services Configuration

Identity management in G/On is through a directory service like Microsoft Active Directory (AD) – and/or LDAP (Lightweight Directory Access Protocol) – and/or local users and groups on the G/On server machine.



Each user directory type can be enabled/disabled using the “Enabled” check boxes. For Active Directory and LDAP it is possible to add any number of different directory specifications, whereas there can be only one instance of the local Windows user plugin. Choosing the “Add” or “Edit” buttons will open a new window with specifications for the user directory (type) in question.

Active Directory User Directory Plugin Configuration



On the Active Directory configuration screen, you must specify the **Domain (dns)** name of the Active Directory. Normally, the **Net bios** name is automatically filled in. If this does not happen, please fill in the Netbios name manually.

If the AD feature is not included in your license, or you do not wish to configure it, you can skip this step.

LDAP User Directory Plugin Configuration

As an alternative to Active Directory, an LDAP enabled user directory can be used. For information on configuring this option, see the G/On Set-up and Configuration Reference.

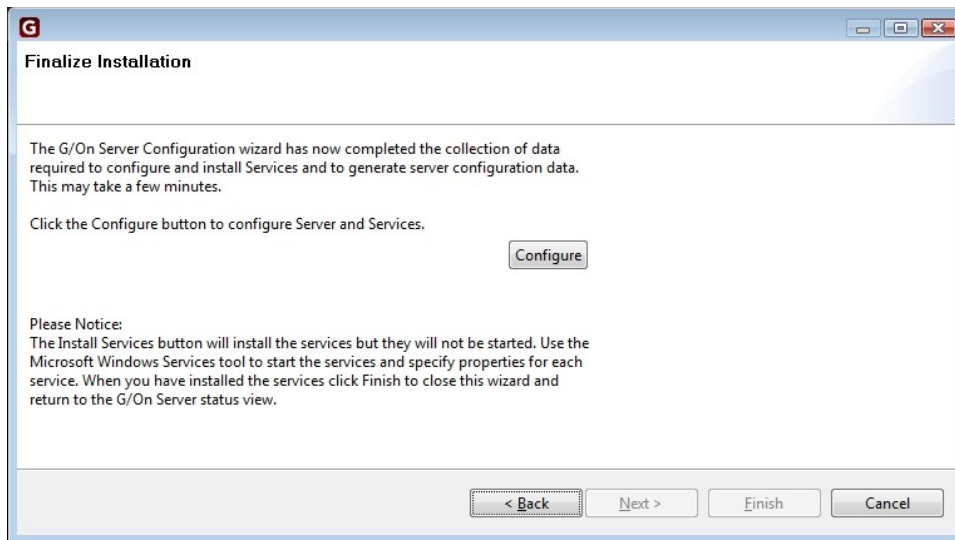
If the feature is not included in your license, or you do not wish to configure it, you can skip this step.

Local Windows User Plugin Configuration

As an alternative (or supplement) to Active Directory, G/On may be configured to use local users and groups that exist on the server machine where the G/On Gateway and Management Servers are running. If you do not wish to configure this feature, you can skip this step.

Finalize Installation

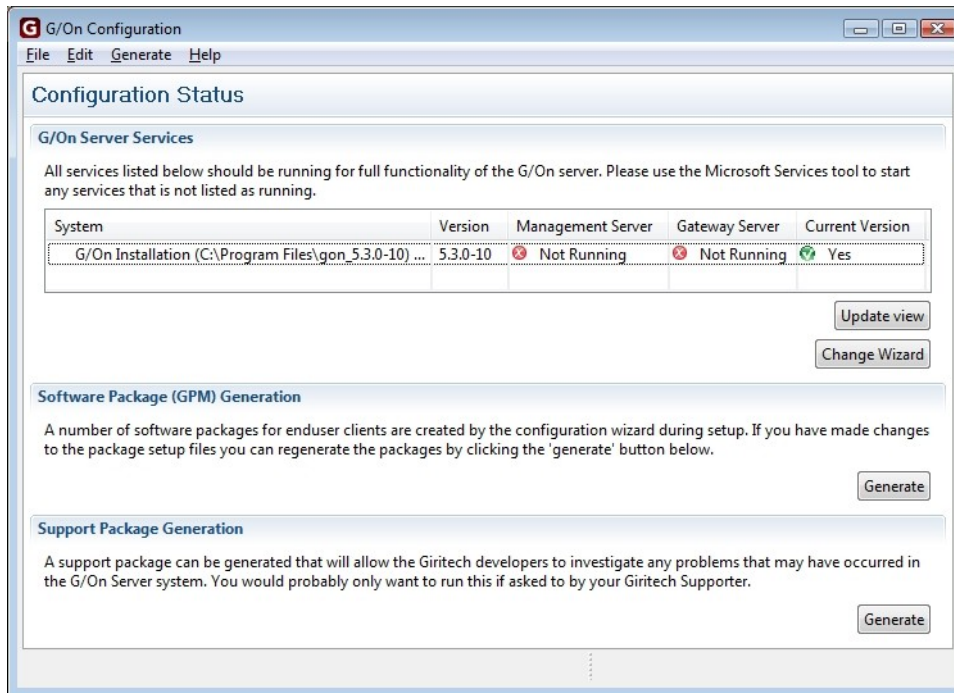
Last step in the initial installation process of the G/On server is to configure the Management and Gateway services on the G/On server. Also, the system will use the supplied configuration data to generate the initial G/On Client Software Packages.



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

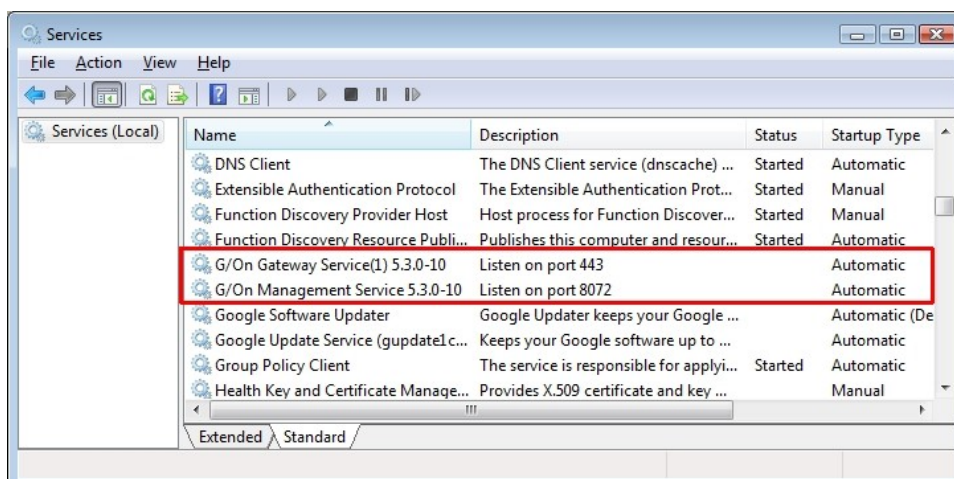
Once the configuration routine has finished, click **Finish** to go to the Configuration Status screen.

Configuration Status



The configuration Status screen allows you to see the current status of the G/On services. Note that the Management and Gateway services need to be started manually (first time).

You can start the G/On services by using the “Services” Management interface in windows. (All Programs > Administrative Tools > Services) – to see the following screen:



Locate the two installed G/On services (Management and Gateway) highlighted above – and right-click on each one in turn, and choose Start.

After starting the G/On services and clicking Update view on the G/On configuration status screen, the services will be listed as “running”.

Using G/On Management

After installation and running the G/On Configuration wizard, the program: G/On Management can be used for setting up authentication and authorization policies, preparing tokens etc. Please see the separate document: “Getting Started with G/On Management”.

Note: On Windows Server 2008, you must run the G/On Management program, as Administrator: Find the program in the Windows Start Menu, right-click it, and choose Run as Administrator.

Changing the Server Configuration

Re-configuration of the system can be done by clicking Change Wizard in the Configuration Status Window. For details, see the document: G/On Set-up and Configuration Reference.

Restarting from Scratch

Cleaning and re-doing the configuration of the system, from scratch can be done by using the wizard in G/On Configuration. Start the G/On Server Configuration program. Choose Help > Welcome to the G/On Configuration. Click Start Wizard.

Warning: All configuration and management settings are reset.

Reference

Before installation

Supported Platforms

G/On Client

- Windows XP (32 bit), Windows Vista, Windows 7
- Apple Mac OS X 10.5 (Leopard), and 10.6 (Snow leopard) on Intel based Macs
- Linux Fedora 14 with GTK+ GUI (32 bit)

G/On Management

- Windows XP (32 bit), Windows Vista, Windows 7
- Windows Server 2003 R2, Windows Server 2008, Windows Server 2008R2

G/On Server

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

All platforms mentioned, have been tested with the latest Service Packs/updates, at the time where the G/On version was released.

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, and a Gateway installer for separate Gateway installation, the Nullsoft scriptable install system must be installed on the G/On server. Get it here: <http://nsis.sourceforge.net/>

G/On Management requires Internet Explorer 8 or newer for some functions (reporting).

Introduction

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

The Windows Installer creates the *G/On Master Installation* in a program folder and unpacks all the necessary files to this folder, and creates entries in the Windows start menu. The Master Installation contains the Management Server and also includes a Gateway Server. However, use of this Gateway Server may be supplemented by or replaced by one or more other Gateway servers, which are installed on separate machines by means of the Windows Gateway Installer (see below).

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

The Windows Gateway Installer is used for installing additional Gateway Servers, replacing or supplementing the Gateway Server in the G/On Master Installation.

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.

Note: 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:

3. 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.
4. Run G/On Configuration for the new version. On the Welcome Screen, there will be 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.
5. 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.

Note: 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.

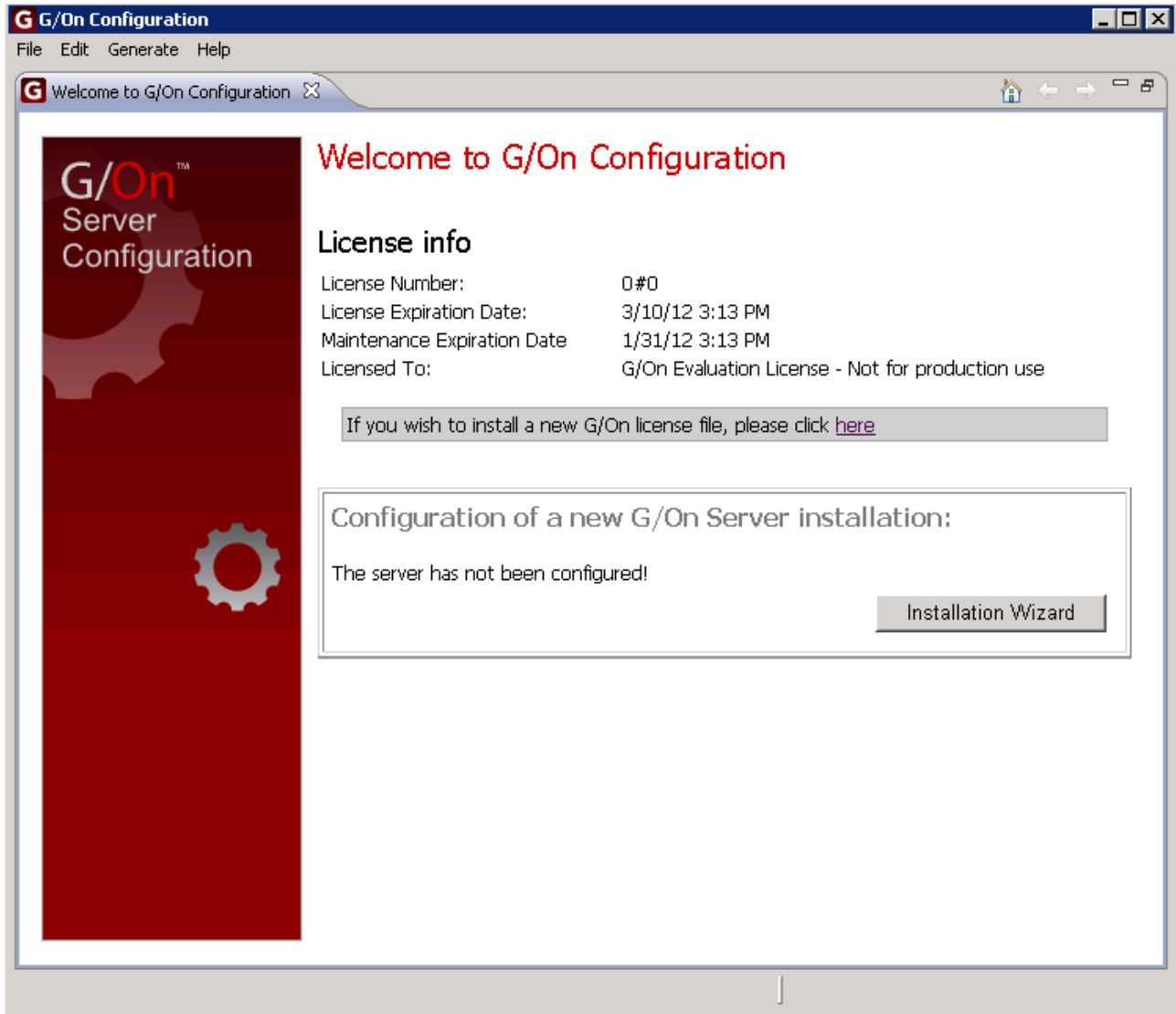
The Welcome screen can also be opened from the Main Status Window by choosing Help > Welcome to the G/On Configuration in the menu.

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 something like this:



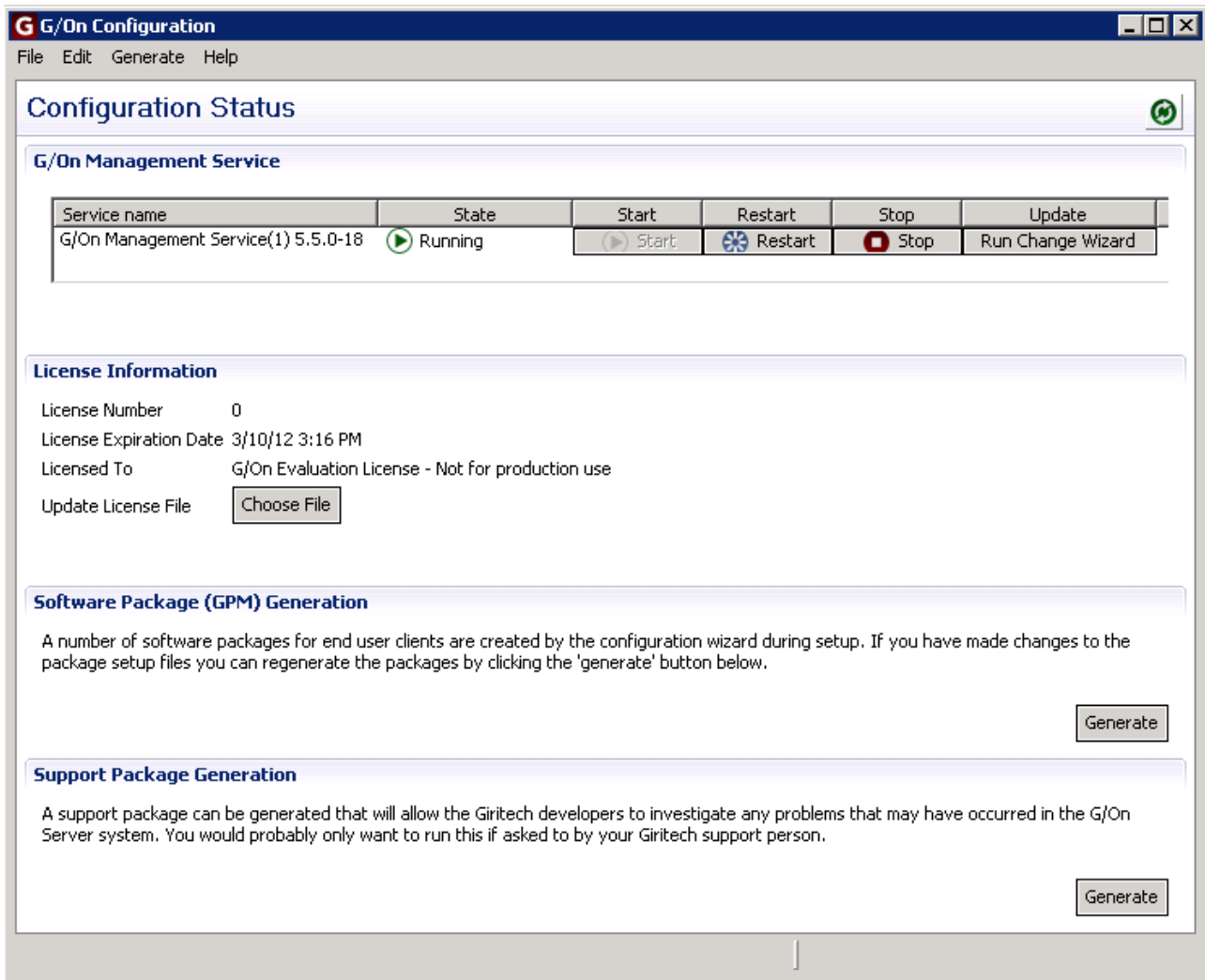
If you do not use a proper G/On license file, the installation will proceed with an evaluation license. If you have acquired a proper license file, you can place it in the folder

```
\config\deployed
```

or you can simply click on the link in the window. This will open a file chooser, in which you can choose the license file and install it.

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 Management Service

In this section of the status window, you should see status of the installed G/On management service. The following information/functionality is available:

- **Service name:** The name of the management service.
- **State:** Current state; Running, Restarting or Stopped.
- **Start:** Starts the service.

- **Restart:** Restarts the service.
- **Stop:** Stops the service.
- **Run Change Wizard:** Starts the Change Wizard (see 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.

After completion a file chooser will open in which you can choose where to put the generated zip file.

Wizards

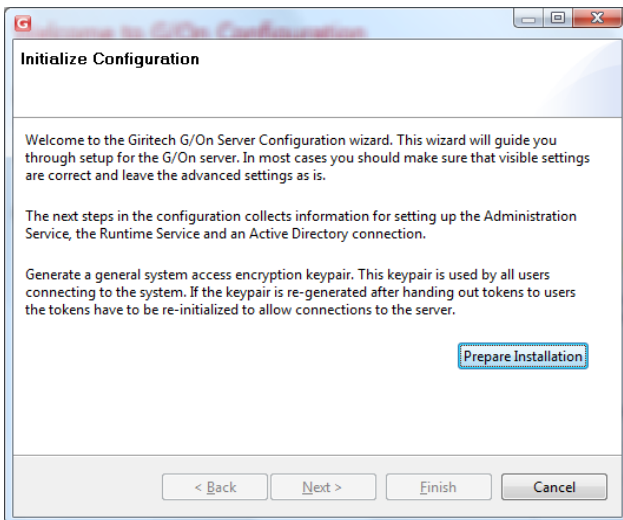
This section contains detailed information regarding the various Wizards in the G/On Configuration tool.

Installation Wizard

The installation Wizard is started automatically, the first time you run G/On Configuration. It can also be started by clicking the Start Wizard button In the “G/On Configuration Wizard” section in the Welcome Screen.

Note: the Installation Wizard should only be run once. Running it again on an installed system will erase system data and potentially invalidate the system.

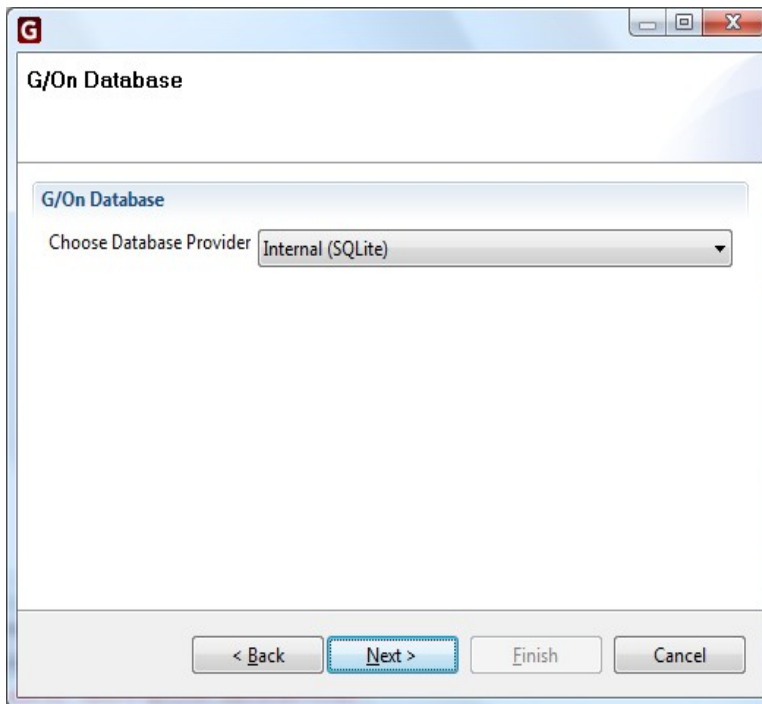
Initialize Configuration



Click Prepare Installation in order to run the preparation job. If no errors occur, you will be able to Click 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 select database provider. If you want to use the default internal database then no further configuration is required. If you select SQL Server, a new window for entering further configuration will open when you click 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.
Gateway Server user name	Optional user login for the gateway server. The gateway server only needs read permission to the database, so it can make sense in some set-ups to

	<p>use another account for database access on gateway servers.</p> <p>Leave blank in order to use same authentication as the config and management services.</p>
Gateway Server password	The password for the Gateway server user account.

Advanced	
Port	The port number used for communication. Leave blank if you want the port number to be negotiated by the ODBC client.
Options	A comma separated list of extra options for the ODBC connection. Can be used for a failover setup. Example: "Driver={SQL Native Client}, Failover_Partner=SomeServerName"
Logging enabled	Enable logging

The button "Check connection" will check whether the connection to the database is ok and create and delete a temporary table in order to test that the connection has the rights necessary for creating the database.

The "Create database" button will try to create the database specified. Use this if the database has not already been created in the SQL Server Management tool.

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	
Web service listen address	<p>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.</p> <p>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 – winch</p>

	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!
Web service listen port	TCP Port where the Management service should listen for connections from the Management Client.
Gateway server listen address	IP address where the Management service should listen for connections from Gateway Servers.
Gateway server listen port	TCP Port where the Management service should listen for connections from Gateway Servers.

Advanced

Logging enabled	Enable logging
Logging verbose level	<p>The primary purpose of logging in this context is for support reasons. Currently, there are two logging levels defined:</p> <p>0: All warnings, errors and critical errors will be logged</p> <p>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).</p>
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.

Standard	
Listen Port	<p>The port that the Gateway Server listens on in order to accept connections from G/On Clients. Only one port can be specified here.</p> <p>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.</p>
Client Connect Addresses	<p>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</p>

	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.
Client Connect Ports	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.
Management Server Connect Address	IP address or DNS name, which the Gateway servers should use for connecting to the management server.
Management Server Connect Port	TCP Port number, which the Gateway servers should use for connecting to the management server.

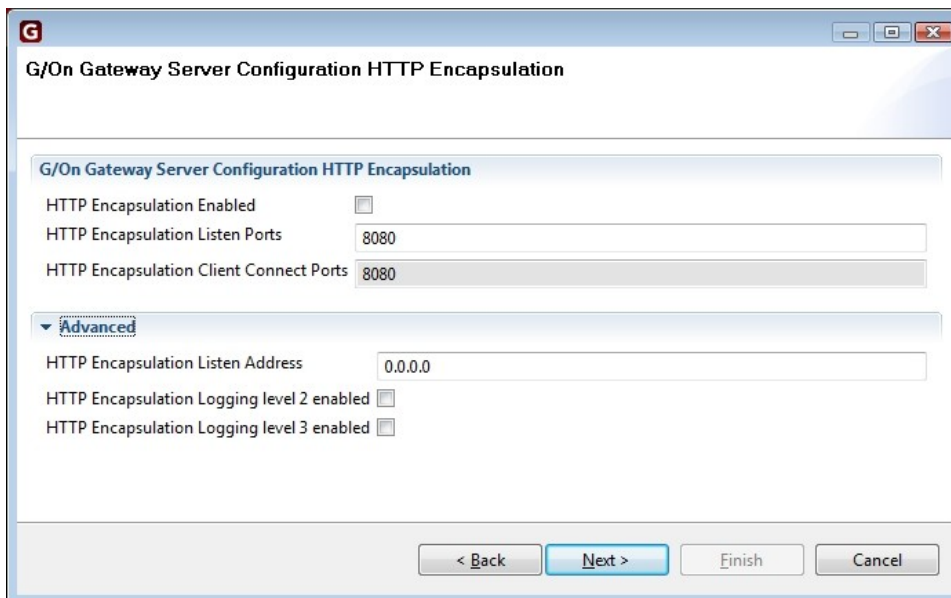
Advanced	
Listen address	This is the internal address that the G/On Gateway will listen on to accept connections from G/On clients. 0.0.0.0 will enable connections on all the network interfaces of the Gateway Server machine (default).
Logging enabled	Enable logging. The primary purpose of logging in 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
Session logging enabled by remote	Enables possibility for session logging controlled by client. If this option is set you can get session logging for a specific client by specifying it in the client's configuration file.
User session timeout (minutes)	Timeout to stop sessions, which has been idle for more than the specified period. Set to 0 in order to disable session timeout.
Authorization timeout (seconds)	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.
Mobile, offline user credentials timeout (minutes)	The time period credentials are saved on mobile devices (iPad, iPhone). In order to improve usability, credentials are saved on mobile devices in the specified number of minutes.
Mobile, close when entering background	Controls whether G/On should disconnect from the server on mobile devices (iPad, iPhone), when the G/On app is entering background, i.e. when you switch to another app or to the main menu. Note that disconnecting means that port forwards (e.g. for mail clients) are disabled
Welcome message before first access enabled	This option can be used to acquire user acceptance of the terms and conditions under which access is granted.
Welcome message 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

Welcome message before first access, close-on-cancel	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:

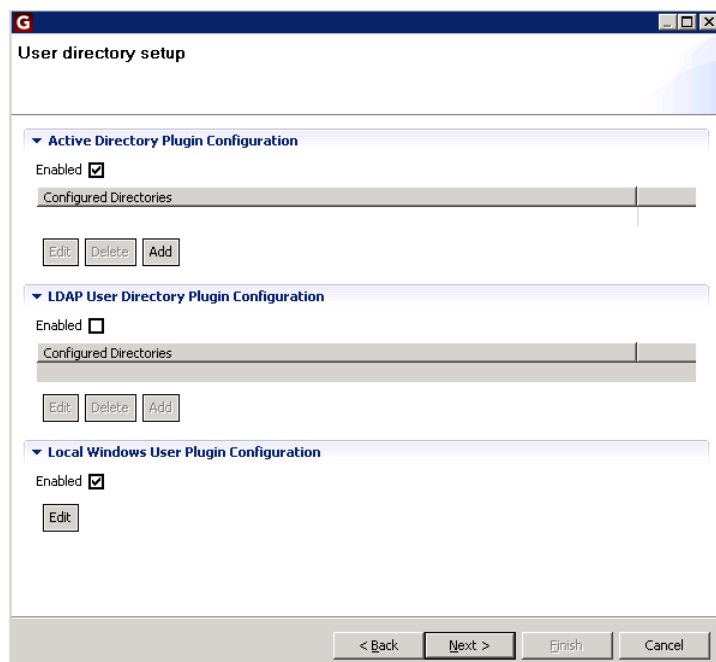
Standard	
HTTP Encapsulation Enabled	Enable or disable use of HTTP encapsulation.
HTTP Encapsulation Listen port	specifies the port on which the Gateway Server will listen for HTTP

	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 be used unless needed for support reasons (remember to deactivate).

User Directory Configuration

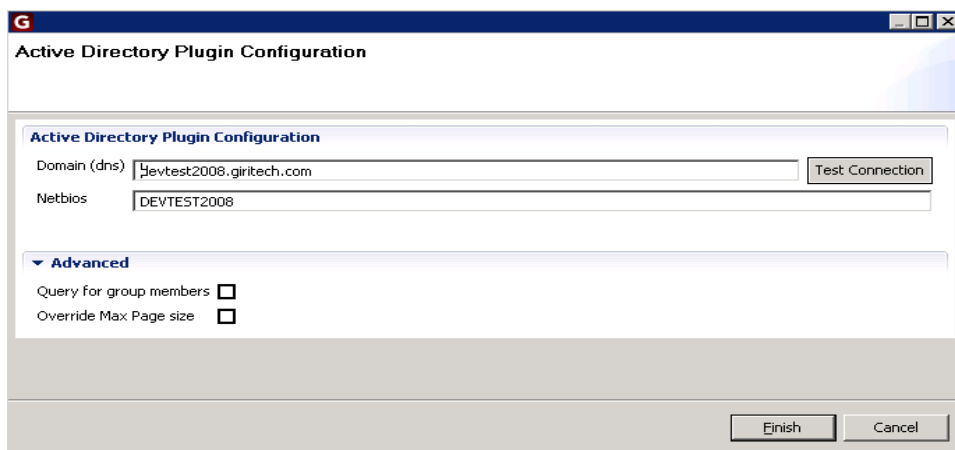
On this page it is possible to add (and remove) user directories used for user verification. There are currently three types of user directories: Active Directory, LDAP and Local Windows User (note that LDAP is a license feature and therefore may not be available).



Each user directory type can be enabled/disabled using the “Enabled” check boxes. For Active Directory and LDAP it is possible to add any number of different directory specifications, whereas there can be only one instance of the local Windows user plugin. Choosing the “Add” or “Edit” buttons will open a new window with specifications for the user directory (type) in question. These windows are described below.

Active Directory User Directory Plugin Configuration

The Active Directory plugin uses the Windows API to connect to Active Directory. In order for Active Directory integration to work properly the 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.

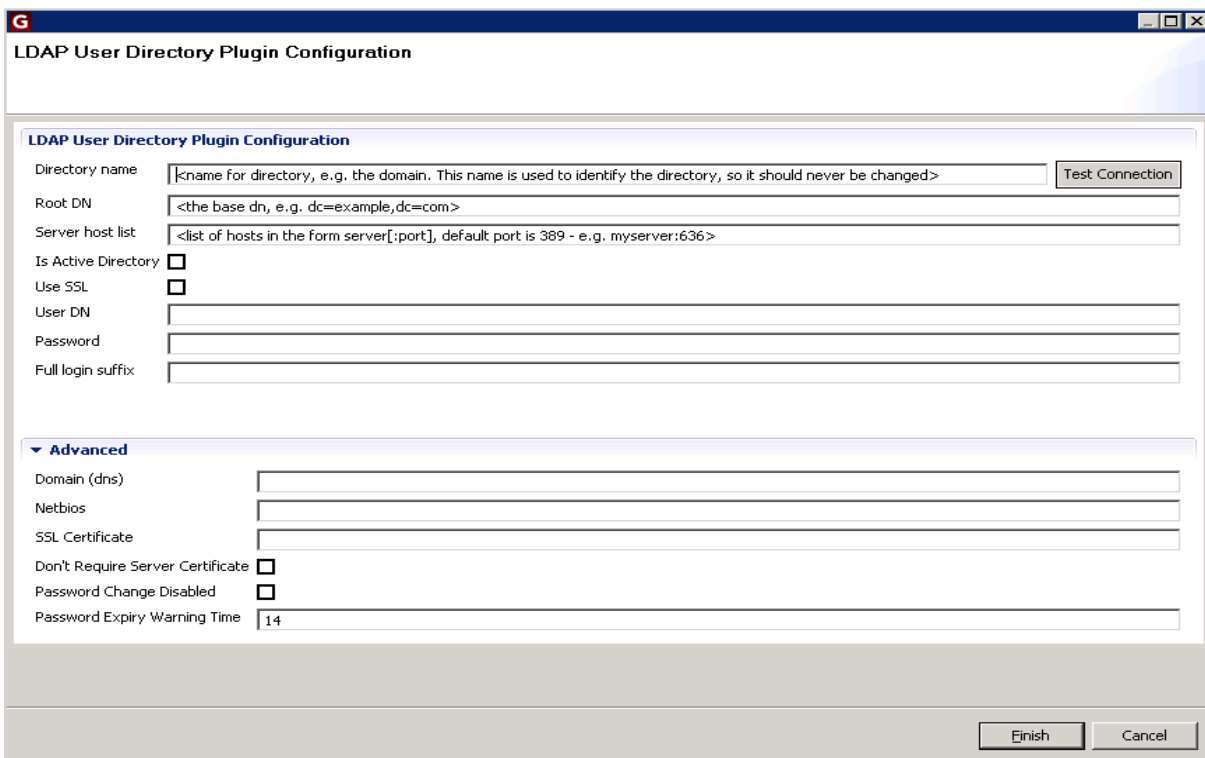


Standard	
Domain (dns)	Enter dns name of the AD domain, e. g. mycompany.com.
Netbios	The Netbios name of the AD domain.
Query for group members	Enables an alternative method for finding group memberships. The standard way does not include most domain local groups on remote trusted domains and most built-in domain local groups on the local domain (e.g. Remote Desktop Users). Note however, that the alternative method has been seen to fail on some installations, probably because of inadequate access rights – it has not been possible so far to pinpoint the exact reason.
Override Max Page Size	Overrides the Max Page Size limit so that all entries can be fetched in a query. Queries to Active Directory will by default only return a limited number of entries. The limit is controlled by a constant called MaxPageSize, which by default is 1000 (it can be changed using the “Ntdsutil.exe” utility program). The limit can be overridden in the query itself and enabling this option will cause G/On to do so.

LDAP Plugin Configuration

The LDAP plugin uses the LDAP protocol for user verification and for obtaining information about users and groups available. It can, in principle, be used against any LDAP enabled User Directory, but has only been tested against Novell eDirectory and Active Directory.

So among the uses of the LDAP plugin is another way of connection to Active Directory. See page 55 for a discussion of issues related to Active Directory and LDAP and which plugin to use.



Standard	
Directory Name	Enter a name for the directory. This name will be used to identify users and groups from this LDAP Directory. 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. Example: dc=mydomain,dc=com
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
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.
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. Example: cn=myuser,ou=myorgunit,dc=mydomain,dc=com
Password	Password for the user specified account
Full login suffix	The login suffix that distinguishes users from this directory from another one. If more than one user directory is specified, then there may be name clashes on the login names. If this is the case users must enter a <i>full</i> login, which is the normal login succeeded by a "@" and the Full login suffix (e.g. username@mydirectory). If left blank the Directory name is used as suffix.

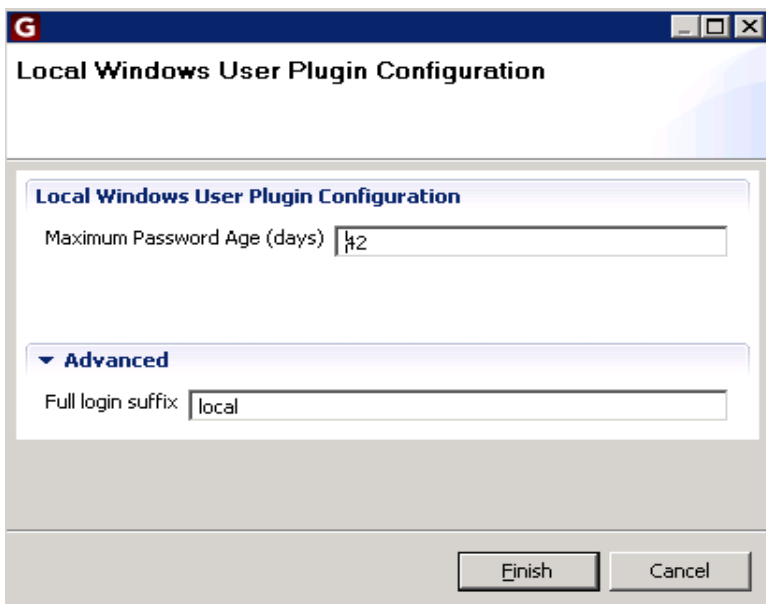
Advanced	
Domain (dns)	The domain DNS name used when launching menu actions using the <i>user.domain</i> variable.
Netbios	The domain Netbios name used when launching menu actions using the <i>user.netbios</i> variable.
SSL Certificate	Full path to Certificate file used for SSL communication.
Don't Require Server Certificate	Set this if the Gateway server should not check the server certificate when connecting using SSL. In other words this enables SSL communication

	without server verification.
Password Change Disabled	Check if password change via G/On should be 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 on the local server..

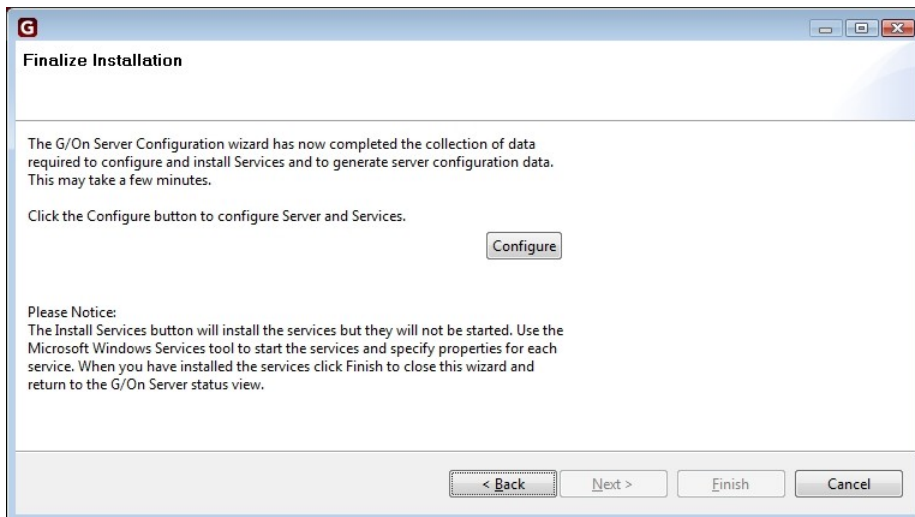
Note: In order for this to work correctly the G/On Management and all Gateway Servers should run on the same machine, so they will “see” the same local users and groups.



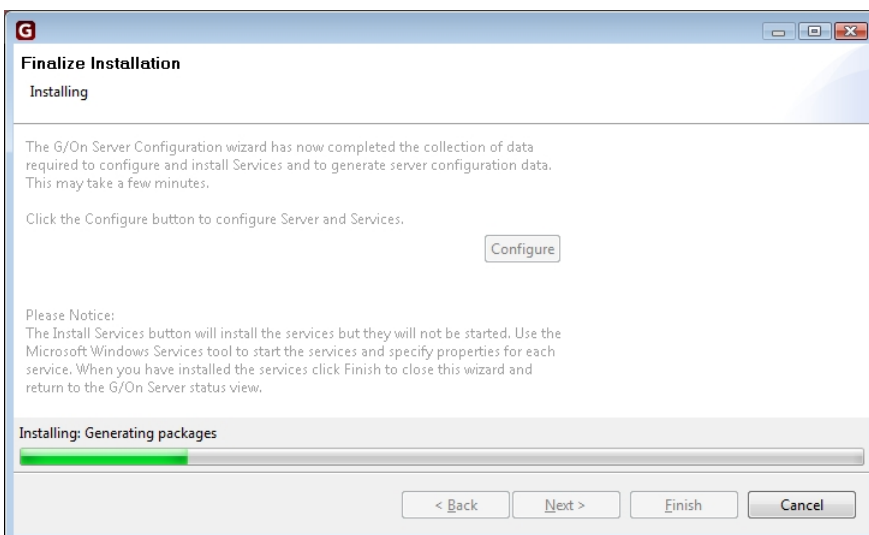
Standard	
Maximum Password Age (days)	When a user's password is older than this limit, G/On will ask the user to change the password.

Advanced	
Full login suffix	The login suffix that distinguishes users from this directory from another one. If more than one user directory is specified, then there may be name clashes on the login names. If this is the case users must enter a <i>full</i> login, which is the normal login succeeded by a “@” and the Full login suffix (e.g. <code>username@local</code>). If left blank the value “local” will be used.

Finalize Installation



Click Configure to save the configuration and generate database and G/On Client Software packages.



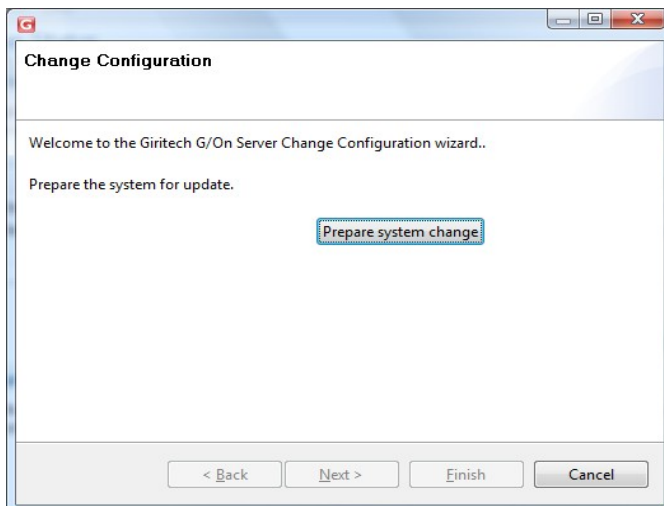
If no errors occur, you will be able to click Finish to exit the Wizard and go to the Configuration Status screen. If any errors occur they will be shown immediately after the “Finalize Installation” title.

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:



The following pages are the same as or similar to those of the Installation Wizard, so only differences from that wizard is described in this section. Please refer to the Installation Wizard Section for the remaining information

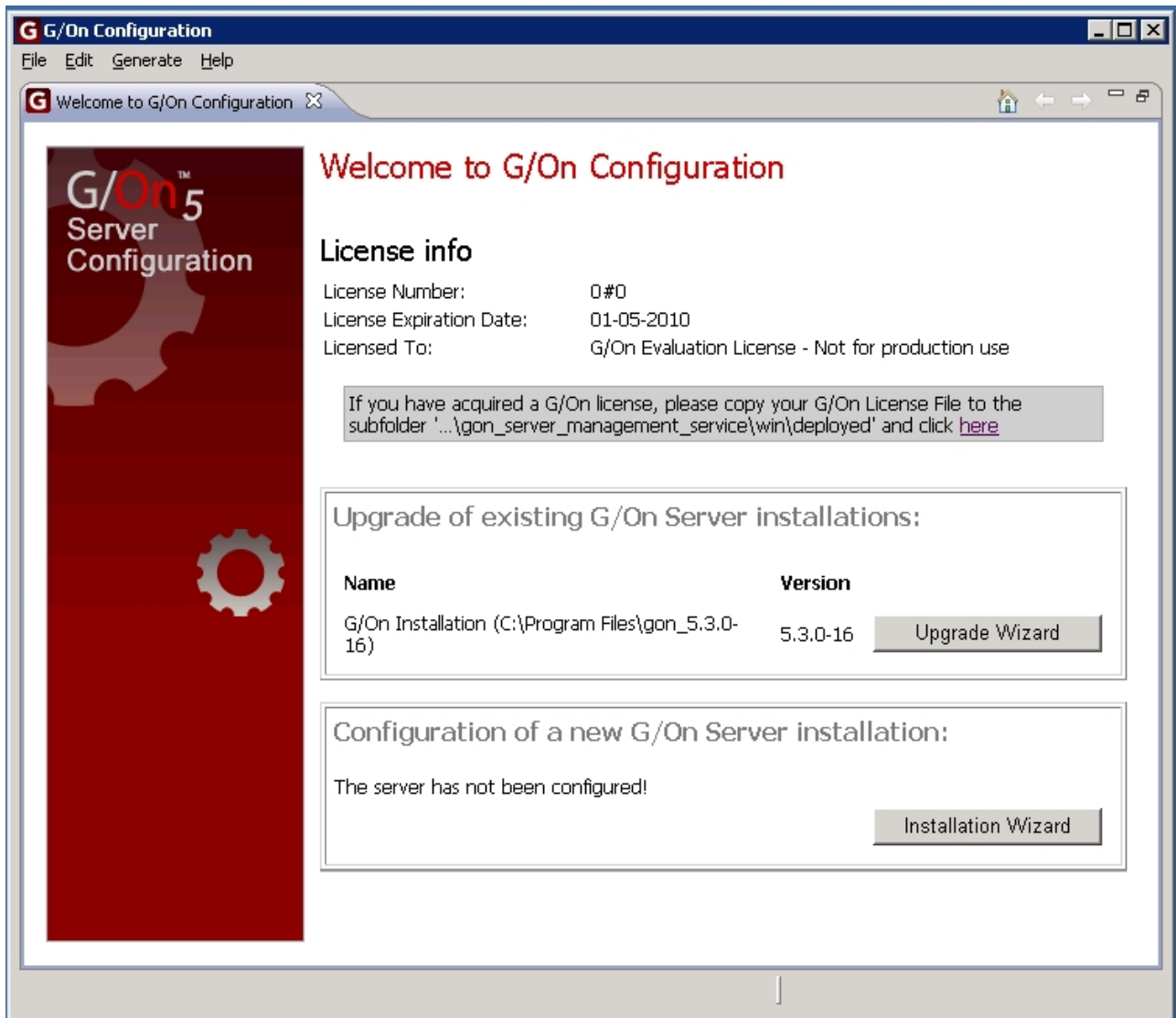
SQL Server Set-up

In the SQL server set-up an extra *encoding* field is available. The database encoding is detected and set automatically during installation but it can be changed here if necessary.

Note also that it is not possible to create a new database using the Change Wizard. The database entered in the *database* field is assumed to be a previously installed G/On database. Entering the name of an empty database will result in a database missing essential set-up data.

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. gon550. 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.

Note: 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.

Upgrade memory issue

Upgrading to 5.5.0 has caused problems in some installations where the memory usage of the server during upgrade caused the server to crash. This problem has been fixed in 5.5.1, but upgrade may still cause problems in some installations, because the configuration server in the old version is used to make a backup of the system as part of the upgrade. If you have problems upgrading to 5.5.1 or newer versions from 5.5.0 or earlier versions, please use the following steps.

Try creating a backup of the old system manually

If it is possible to create a backup manually you can upgrade from that. Follow the procedure described in “G/On Setup and Configuration” to create a backup of the old version. If creation of the backup is successful, then you should copy or move the folder containing the backup from the backup folder of the old system to the backup folder of the new system. Then restart G/On configuration and the backup should appear as one of the systems usable for upgrade. Choose the backup and follow the standard procedures for an upgrade.

Prune the database

The main reason for the memory usage failure are database tables containing access log information. With the release of 5.5.0 we have also released an SQL script, which will remove access log entries older than a specified period of time (e.g. 3 months). If you want to keep these entries in the old system, then you can backup your database or create a copy before running the script. If you want to keep the entries in the upgraded version, then this solution is not applicable. Whether or not pruning the database will solve the problem is of course dependent on how much data is deleted, which again is dependent on the length of the period from which access log data are kept and the amount of user activity in that period.

Create backup using the new system.

In 5.5.1 a special command line option has been added to the G/On configuration server, which enables the server to create a backup of a previous version without memory usage issues. However, in order for the backup to work as a foundation for an upgrade, some manual steps

needs to be performed first. Use the following procedure in order to upgrade using this method:

1. Edit configuration files: In the old system some default settings needs to be specifically set in the configuration files in order for the new configuration server to use them. As a safety precaution you should create a copy of the files before editing them. Note that you may need administrative rights to edit the files. Open the files *gon_server_config.ini* and *gon_server_management.ini* in an editor. In each file you should uncomment settings not explicitly set. Here is an example:

```
[log]
# enabled = True
enabled = True
# rotate = True
# type = text
# verbose = 1
verbose = 0
# file = gon_server_management.log
```

```
#[license]
# filename = ./deployed/gon_license.lic
```

All '#' and blank spaces at the beginning of lines should be removed, except for the settings which are already there, like e.g. the "verbose" setting in the example above. The example above should look like this after editing:

```
[log]
enabled = True
rotate = True
type = text
# verbose = 1
verbose = 0
file = gon_server_management.log
```

```
[license]
filename = ./deployed/gon_license.lic
```

2. Backup old system: Open a command prompt (as administrator) and go to the subfolder *gon_config_service\win* in the new system. Here you should start the following command:

```
gon_config_service.exe -backup_other_installation
--backup_other_installation_path <path>
```

where *path* is the path to the old system root folder, e.g. "C:\Program Files\Giritech\gon_5.4.1-6". The command should produce a backup in the new system

backup folder (*gon_config_service\win\backup*). Please check the log *backup_log.txt* in the backup folder to ensure that there were no errors during backup.

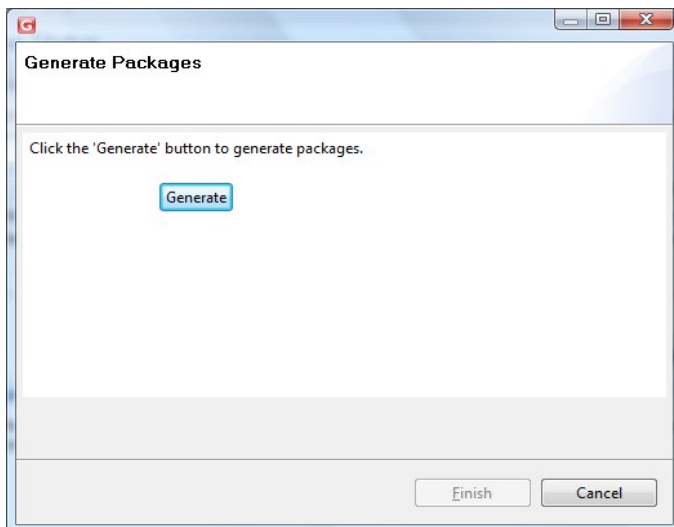
3. Start G/On Configuration in the new system. The backup should appear as one of the systems usable for upgrade. Choose this backup and follow the standard procedures for an upgrade.

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:



Click Generate in order to start the task which generates the packages. If no errors occur, you will be able to click Finish 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

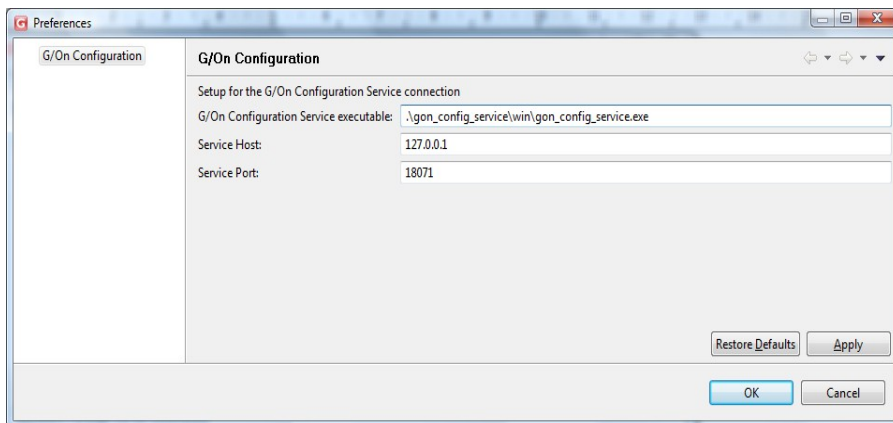
Quit G/On Configuration

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

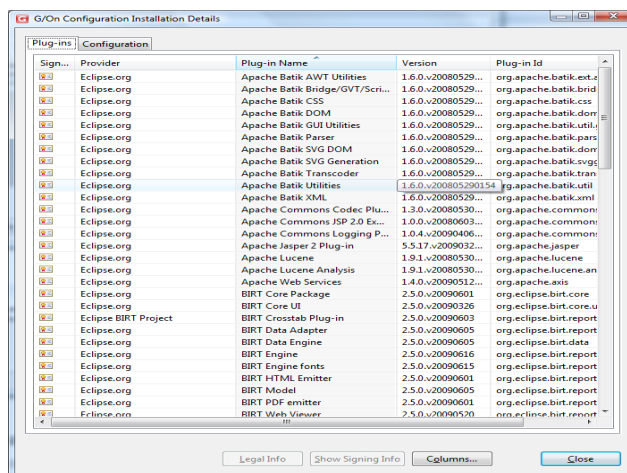
Open the “About” Window. Apart from version and copyright information, you can access the Server Configuration client error log from here by following the steps below. Note that this log only pertains to the client (GUI) part of the Server Configuration Utility.

The error log is fetched like this:

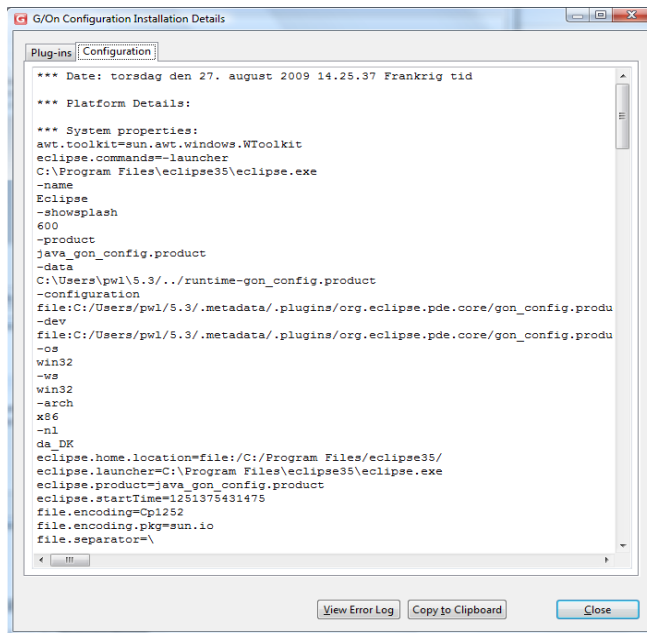
1. In the About Window:



2. Click Installation Details. A window like this opens:



3. Select the Configuration tab. The Window changes to something like this:



4. Click View Error Log. The error log opens 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\gpms
```

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 “G/On Field Deployment”.

Automatic Approval of Field Enrollment Requests

In the Management Server Configuration (see page 29 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: "G/On 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 needs 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 user's 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:
http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itame.doc_6.0/rev/am60_install167.htm

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 in the AD plugin configuration (see page 36).

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

Installing Addition Gateway Servers with a Gateway Installer

In this section we describe how to install additional Gateway Servers. Note that there is a license restriction on the number of Gateway servers and Client Connect Addresses,. Also note that this setup requires use of SQL Server database. The setup is partially manual, and thus requires some technical know-how.

Minimum Platform requirements

Server OS: Windows Server 2003

DBMS: SQL Server 2005

Before you start

First make sure that you have completed the following preparations:

1. Install the Nullsoft scriptable install system on the G/On server. Get it here:
<http://nsis.sourceforge.net/Download>
2. Specify the client connect port and server addresses using the Change Wizard, if this has not already been done.

3. Make sure that SQL Server accepts remote connections and that it is reachable from the machine on which you want to make the installation. 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.

Create Gateway Server installer

Use the Nullsoft installer (NSIS) to generate the G/On client installation program, as follows:

On Windows Server 2003, do not start the NSIS program. Simply right-click on:

```
distribution\gon_server_gateway_service_installer\win\nsis\gon_server_gateway_service_installer.nsi
```

and select Compile NSIS Script.

On Windows Server 2008, start the NSIS program with Run as administrator. Then choose Compile NSI scripts and File > Load Script... and then specify:

```
distribution\gon_server_gateway_service_installer\win\nsis\gon_server_gateway_service_installer.nsi
```

The resulting client installation program is placed here:

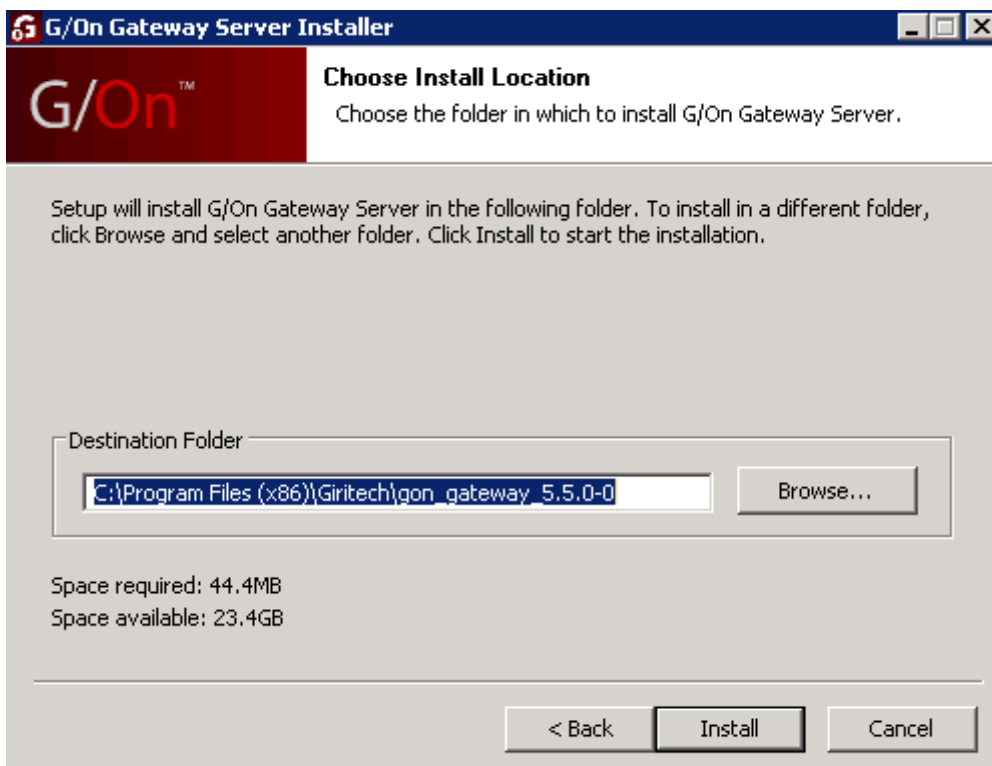
```
distribution\gon_server_gateway_service_installer\win\gon_server_gateway_service_installer.exe
```

Install Gateway Server

Copy the Gateway Server installer to the server machine on which it should be installed. Start the installer. You should see the following window:



Choosing “Next” brings you to a page where you should agree to the License Agreement. After that you should choose installation location:



Choose the destination folder of your choice and press “Install”. The installation will begin. When the installation is finished a final window will appear. Just click “Finish” to end installation.

Completing installation.

After running the Gateway Server installer there are a few steps (some optional) that needs to be performed manually.

- 1. Edit the Port number:** If the gateway server has been installed on the same server machine as the standard Gateway Server or another installed Gateway Server you need to change the port number on which the server listens for client connections. The server is installed with the same port number as the standard Gateway Server. In order to change the port number you should open the file *gon_server_gateway_local.ini* in the folder *<installation folder>\gon_server_gateway_service\win* in Notepad or another editor of your choice. Depending on the operating system and installation folder you may need to run the editor as Administrator. Add the following two lines to the file:

```
[service]
port = <port number>
```

and save the file.

- 2. Name the server (optional):** In order better to distinguish servers in the “Gateway Servers” view in G/On Management it is possible to give each Gateway Server a name. In order to do so you should open the file *gon_server_gateway_local.ini* in the folder *<installation folder>\gon_server_gateway_service\win* in Notepad or another editor of your choice. Depending on the operating system and installation folder you may need to run the editor as Administrator. Add the following two lines to the file:

```
[service]
title = <my title>
```

and save the file.

- 3. Start the service:** Open the “Services” console in Windows. A new Gateway Server service should be available. Start the service. Open G/On Management and check that the new server appears in the “Gateway Servers” view.

Note that once the service is started it is possible to restart it using G/On Management. A stopped service must , however, be started using the Windows Services console.

Upgrade of Separately Installed Gateway servers

During upgrade of a G/On Master Installation to a newer version, only the Gateway Server in the Master Installation is upgraded. Separately installed Gateway Servers must be re-installed using the steps described above, with one exception: After the Gateway server has been installed using

the Gateway installer, in stead of editing the `gon_server_gateway_local.ini` file, you should simply copy it from the old Gateway server installation. Also remember to stop the old service before starting the new one.

Set-up instructions when migrating from SQLite

The following is a description on how to migrate from using the internal SQLite database to SQL Server..

1. Create the database you want to migrate to in the SQL Server Management tool (or another tool of your preference).
2. Stop the G/On services, and do a backup (see the instructions regarding backup on page 51).
3. Open the file `.\gon_server_management_service\win\gon_server_management.ini` in an editor (e.g. Notepad). If the server is Windows 2008 or newer you have to run the editor as Administrator. Now, find the following:

```
[db]
...
type = sqlite
```

and change it to:

```
[db]
...
type = mssql
```

4. Start G/On Server Configuration and start the Change Wizard. On the first configuration page (after the "Prepare system" page) you should get a SQL Server database setup page.
5. Enter the database specification details. Note that you need to specify the database encoding. If you don't know what encoding to use then check the section below. Finish the wizard (without making further changes). Close G/On Server Configuration.
6. Create a new backup. Copy all the files in the folder `.\database` from the backup created in step 2. to the new backup (overwrite the existing files).
7. Restore the new modified backup (see the instructions regarding restore on page 51).

- Restart the G/On server services.

Finding database encoding

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_CI_AS"

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".

Alternatively you can install a (temporary) G/On server and run the installation wizard. After running the installation, start the Change Wizard. On the Database setup page you will find the encoding which has been automatically detected during installation.

Creating Custom Client Installers

In the document "G/On Field Deployment", it is described how to make a basic client installation program, that can be used for installing Computer User Tokens on Windows PCs. In the following, some options are described, that may be used when creating client installers for other purposes.

Changing which Packages are included in the Client Installer

All the gpm packages in the following folder are included when the installer is generated by the Nullsoft program:

```
distribution\gon_client_installer\win\nsis\gpms
```

In order to get a package included in the installer, you can simply copy the gpm file to this folder. Alternatively, you can add the name of the package to the following package collection:

```
dist_client_installer_win.gpmcdef.xml
```

All packages in this collection are automatically copied to the `nsis\gpms` subfolder, whenever

packages are generated.

Options for the Client Installer

The Nullsoft program includes the following ini-file when it builds the client installer:

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

When a users starts the client installer, it behaves according to options in this ini-file. The options and their default values are:

```
[discover]
desktop_enabled = True
token_enabled = True

[keys]
generate_keypair_enabled = True
```

The option `desktop_enabled` controls whether the user will be presented with a choice of installing (and re-installing) Computer User Tokens.

The option `token_enabled` controls whether the user will be presented with a choice of installing (and re-installing) USB tokens (MicroSmart, Hagiwara, Soft Tokens).

The option `generate_keypair_enabled` controls whether a new keypair is generated when (re-)installing a token. Set this to `False`, if you want to make an installer for updating the software and connect information on a token, without giving the token a new identity. This can, e.g., be used for upgrading the software (and connect info) of a selected group of tokens.

Changing which address the installed client connects to (the connect info)

The Nullsoft program includes the following file when it builds the client installer:

```
config\deployed\gon_client.servers
```

This file describes the addresses that the installed client will connect to. If you follow the steps

described in the following, you can change this file temporarily, and generate a client installer including this changed file. *But you must complete all the steps, as described.* Otherwise you run the risk of other tokens also getting their connect addresses updated to match the changed file, and you will lose the automatic synchronization of client connect addresses with the contents of the license file. The steps are:

1. Stop the management server service
2. If there is a gateway server service running on the same machine as the management service, stop this gateway server service. Note that this will mean that any user session on this gateway service will be terminated, and no users can connect to this gateway service.
3. Make a copy of the file `gon_client.servers`
4. Make the desired changes to the file `gon_client.servers`, using a text editor
5. Generate the client installer
6. Restore the file `gon_client.servers` from the copy that you made in step 3
7. Start the management server service and the gateway server service

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</p> <pre>.\gon_config_service\win\gon_config_service.log</pre> <p>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?

Question: 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?

Answer: 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: G/On version 5.5 and later can push out changes in client connect addresses to the client, which can then update the token. However, this requires that the client can still connect to the old address. So the Gateway Server should be kept listening on the original address, until all tokens have been updated.

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.

OBS: If you have changed client connect addresses and/or ports, you also need to:

1. Generate packages
2. Regenerate the Client installer and Gateway installer (if you are using these)