

G/On Management Client

Manual

G/On 5.5

Document revision 1.0

2011-06-03

About this document

This document gives an introduction to the basic functionality of the G/On Management 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
Overview of the G/On Management Client.....	7
Starting G/On Management.....	8
Setting up Authorization Policies.....	10
Register a Personal Token for a User.....	12
Adding Software to the Token.....	14
Daily Use.....	15

Reference

Basic Concepts.....	17
Menu Actions.....	17
Rules and Elements.....	23
The Management Client.....	31
Preferences.....	31
License information.....	32
Introduction to perspectives.....	33
Introduction to Element lists.....	36
Introduction to Rule lists.....	38
Element: User.....	41
Element: User Group.....	43
Element: G/On User Group.....	44
Element: Token.....	45
Element: Token Group.....	47
Element: Tag.....	48
Element: Menu Action.....	50
Element: Authentication Status.....	56
Element: Personal Token Status.....	58
Element: Management Role.....	59
Element: Zone.....	61
Element: IP Range.....	62
Element: Operating System State.....	64
Element: Login Interval.....	67
Perspective: G/On User Group.....	69

Perspective: Action Authorization Policy.....	70
Perspective: User Authentication Policy.....	72
Perspective: Personal Token Assignment.....	73
Perspective: Token Software Management.....	75
Perspective: Token Group Management.....	76
Perspective: Zone Management.....	77
Perspective: Management Role Assignment.....	78
Perspective: Menu Structure Management.....	80
Perspective: Gateway Servers.....	81
Perspective: Reporting.....	85
Best Practices.....	87
Tokens.....	87
Elements.....	87
FAQ.....	89
General.....	89
Rules.....	90
Elements.....	90
Menu Actions.....	91
Tokens.....	91
Users.....	91
Messages.....	92
Menus.....	93
Predefined Menu Action Templates.....	95
FileZilla Templates.....	95
Citrix Web Interface Templates.....	96
 Index	
Index.....	99

Getting started

Introduction

This chapter on “Getting Started” describes a very basic setup using the G/On management application. It will guide the reader through setting up basic access policies, enroll Personal Tokens and adding software to Tokens. This is enough to get a basic G/On Server system running.

The G/On server uses a Rule engine to decide who gets access to what. The G/On management application is primarily used for creating Rules for that engine. Each Rule has a number of premises and one conclusion. A Rules states, that if all premises hold, then the conclusion also holds. For instance, a Rule could say:

If the Token: micro_smart_0002 is being used, and the User is bob@giritech.com, then we conclude that in the current session, there is a known User with a Personal Token

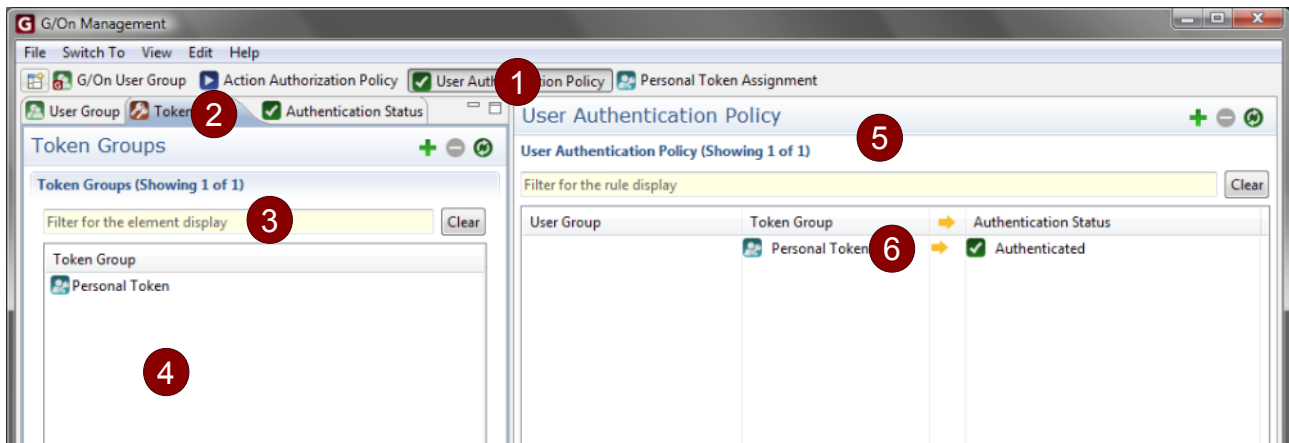
When you first open the G/On management application, you will probably not have any Rules in the Rule Views. This guide will help you set up basic Rules for User access to the application of your choice.

Assumptions: In the following, *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).* Note: 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.

More advanced topics, such as installing on a virtual server, and enrolling tokens and deploying software to Tokens in the field, are covered in separate documents.

Note: *On Windows Server 2008, Windows Vista and Windows 7, 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.*

Overview of the G/On Management Client

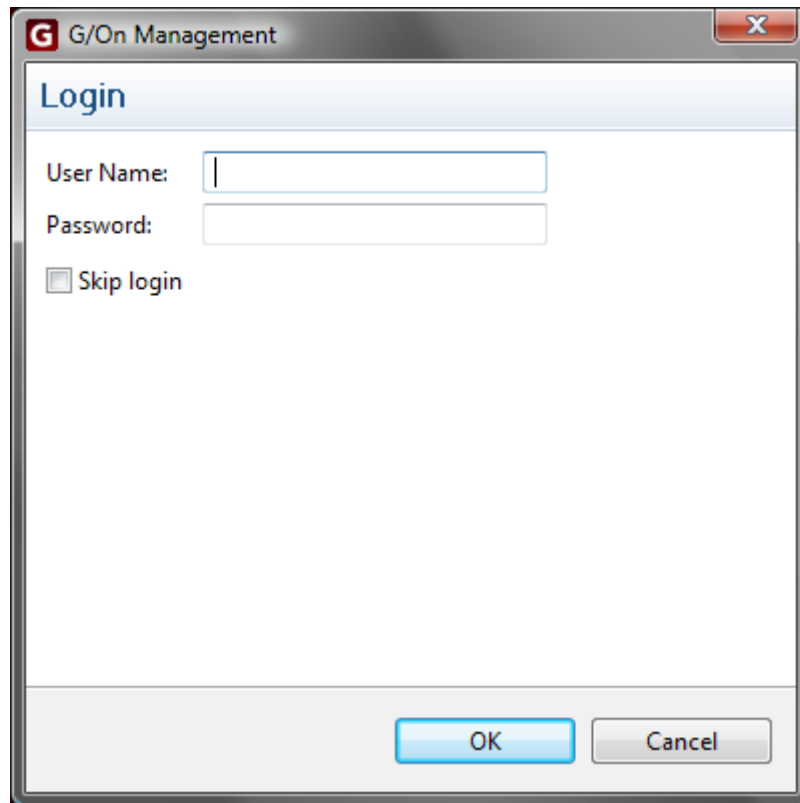


PARTS OF THE MANAGEMENT CLIENT

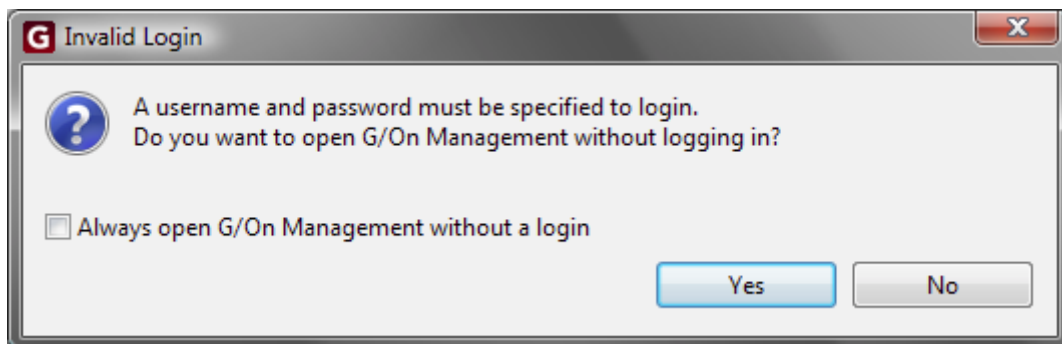
1. The **Perspective bar** is used for selecting between focus areas.
2. The **Element tabs** gives you access to the Elements that can be used in the perspective you are currently viewing. Every Element tab has a plus sign (+) in the top right, that will allow you to create new Elements. In the Element list you can see a list of all available Elements of a given type.
3. Use the **filter** to search for specific elements.
4. Right-click in the view to get a **context menu** that will let you add/remove and edit Elements.
5. The **Rule list** shows all Rules in this perspective. In the top right corner of this view you will also find a plus sign (+) that will allow you to create new Rules.
6. You can right-click on existing Rules to get a **context menu** that will let you **add/remove** and **edit** Rules.

Starting G/On Management

When you start G/On Management it will connect to the management service and a login screen will be presented to you:



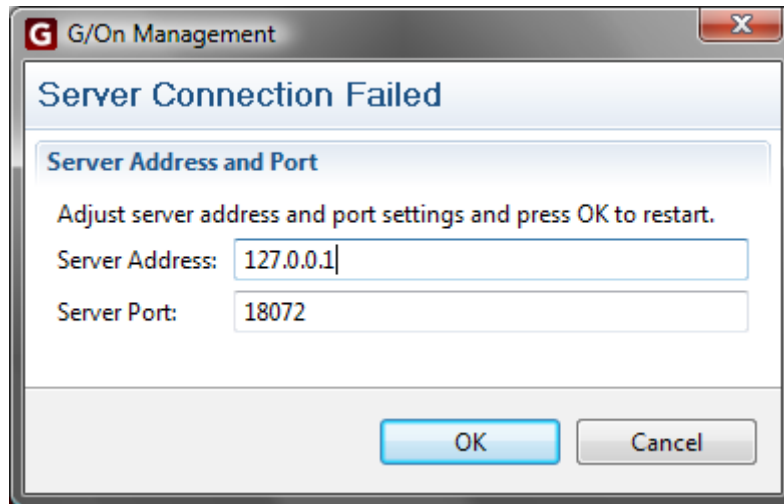
In the initial setup it is not necessary to log in, so you may either click the "Skip login" box and click "OK" or just click Ok. In the latter case you will get a confirmation dialog:



Just choose "Yes" here. Access control can be added to G/On management using the Management Role Assignment view (see page 78). If you don't want to use access control, you can change the preferences so that the login screen is not shown at start-up (or by clicking the

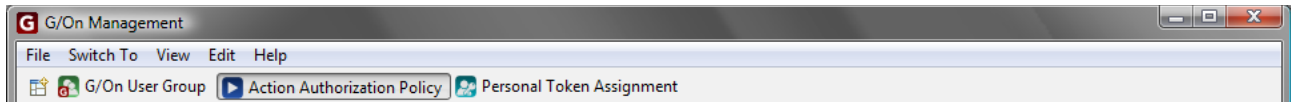
“Always open G/On Management without a login box in the message box above). See page 31 for further details.

In case a connection to the management service can not be established at start-up, you will be presented with a window, where you can edit the connection settings:



If the settings are wrong then change them and click “Ok”. If the connection settings are ok, then you should check that the management service is running and, if it is, check the management service log file for possible errors.

Setting up Authorization Policies



Action Authorization Policies are used to give the Users access to specific Menu Actions when they have authenticated themselves. Click the Action Authorization Policy button in the Perspective bar to see the perspective. The perspective contains a number of Element tabs on the left, and a Rule list on the right.

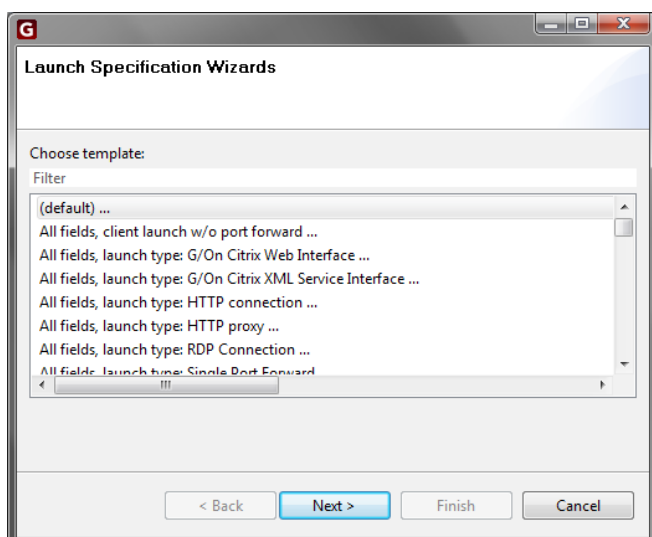
In this perspective you can use the Authentication Status, you specify in the Authentication Policy perspective.

You have the User Groups list to create Authorization Rules for separate groups of users. For instance managers may be authorized to use other applications than accountants.

The last tab contains the Menu Action list. These are the actions that will be listed in the Users menu if they are allowed to use them and if the computer they are using can handle it.

CREATE AN AUTHORIZATION POLICY

1. Open the Authorization Policy perspective.
2. From the Authentication Status list select the 'Authenticated' element and drag it into the Rule listing.
3. From the User Group list, select a group of users, and drag the Element representing them into the Rule editor.
4. From the Menu Actions list, select a Menu Action and add it to the Rule. The Menu Action will be added to the users menus if policies and Rules permit it.
5. Click Save and Close to save the new Rule.



If a Menu Action for the action you want for your Users are not available already, you can use the Launch Specifications Wizard by clicking the green plus sign (+) in the Menu Actions tab. Just follow the instructions to create a new Menu Action and name it as you see fit.

To get started with something simple, we

suggest to make a remote desktop connection to a specific machine, e.g. the machine where the G/On server is installed. In order to enable this on Windows client PCs, use the template: “Windows MSTSC, with Server Side SSO ...”, and fill in the fields in the basic section:

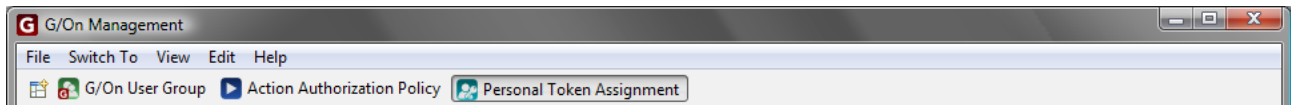
In this example (in the first three Rules) a Menu Action provides access to the end-user package manager for installing, updating and removing packages, to any Users that are Authenticated.

Authentication Status	User Group	Token Group	Menu Action
✓ Authenticated			▶ Client Package Manager, Update
✓ Authenticated			▶ Client Package Manager, Remove
✓ Authenticated			▶ Client Package Manager, Install
✓ Authenticated	Administrators		▶ (W) Remote Desktop on G/On Server

The fourth Rule states that Authenticated Administrators are allowed access to the Remote Desktop connection.

You can create as many Authorization Rules as you like, to give access to various applications.

Register a Personal Token for a User



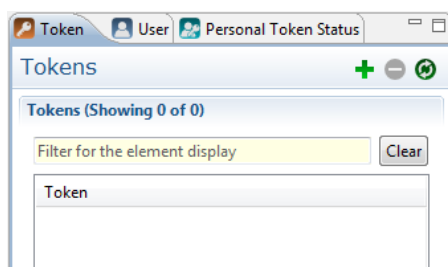
Two different perspectives are used for making the Tokens ready to hand over to users: the Personal Token Assignment perspective and the Token Software Management perspective (the latter will be described in the next part “Adding Software to the Token”).

The Personal Token Assignment perspective is used for registering in the system which Users should be identified by which Tokens. This is important because we want each User to authenticate themselves by a Token that they carry and a password that they remember. This is what is called Two-Factor Authentication. To assign a User to a Token, you first need to open the Personal Token Assignment perspective by selecting it from the Perspective Selector.

On your left hand side you will find a number of Element tabs. In this perspective you have a list of Users, a list of Tokens and a list of a Personal Token Status indication.

REGISTER A PERSONAL TOKEN

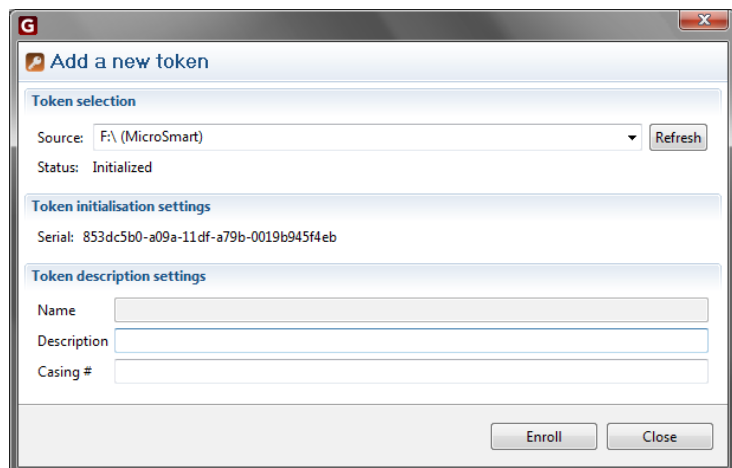
1. Open the Personal Token Assignment perspective.
2. In the Token tab click the plus sign (+) to enroll a new Token.
3. Insert the Token into your local workstation and click the Refresh button.
4. Click the Enroll button to register the Token into the system.
5. Drag the new Token from the Token list to somewhere in the Rule list
6. Drag a User from the User list to the Add Rule area. This registers that the Token should identify this User.
7. From the Personal Token Status list select the Element called Personal Token and add it to the Rule.
8. Click Save and Close to save the rule.



View the Tokens list by selecting the Token tab. You will notice that there are no Tokens yet. That’s because you have to register Tokens before they can be used. Click the plus sign (+) to add and register a new Token into the system. This is called Enrolling the Token.

If you insert a Token into your local workstation it should appear in the source drop-down after you click Refresh. To be able to tell the Tokens apart, you can add a Description and/or Casing text as you see fit.

Then click Enroll to register the Token. Repeat this step with as many Tokens as you like.



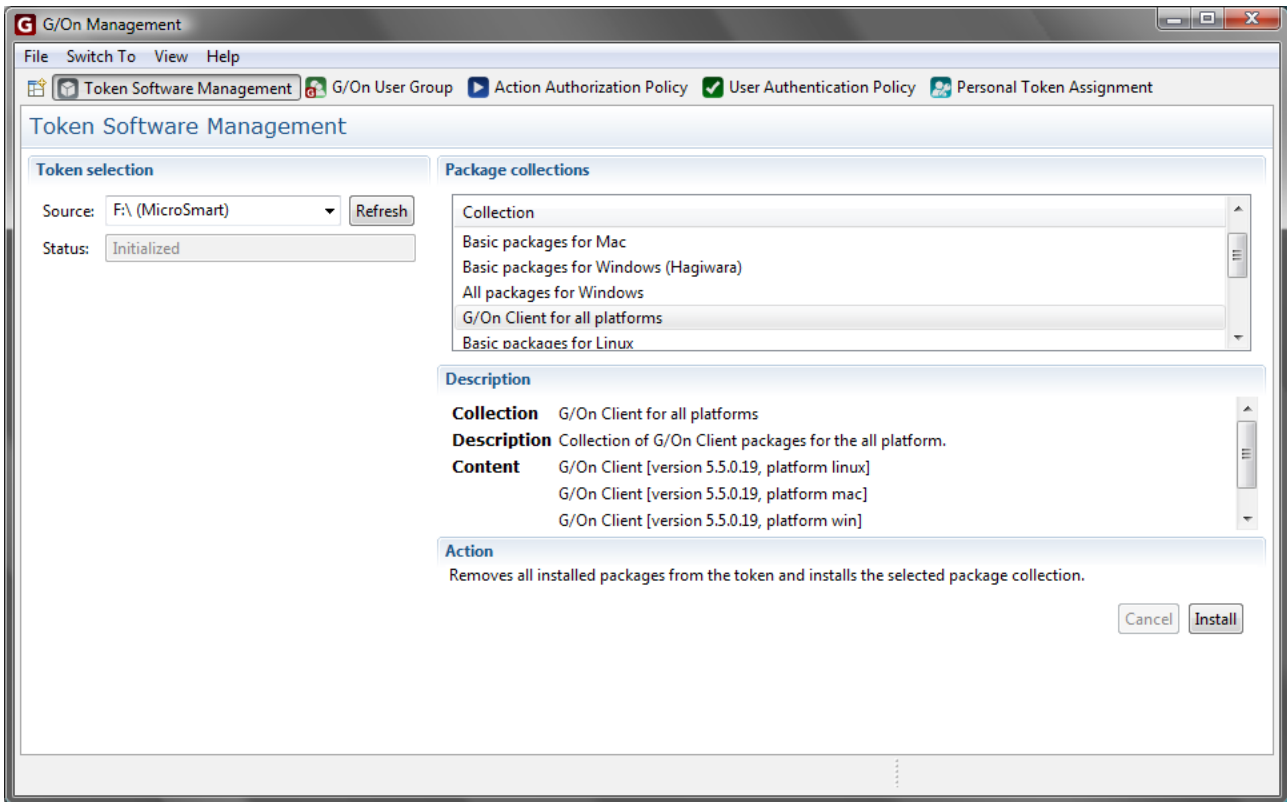
The Personal Token Status tab contains an element called “Personal Token”. This is a special Token Group that holds Tokens that are assigned to a specific User and only that specific User.

In the Rule view on the right hand side you can create a Rule that will assign a User to a Token. Drag a Token into the Rule list area on your right to start creating a new Rule. The Add Rule area appears at the bottom right. From the Users list on the left you can then drag a User into the Add Rule area. Finally add the “Personal Token” into the Add Rule area and click Save and close. The Rule now appears in the Rule list.

INFO ON ASSIGNING TOKENS

- **Tokens need to be enrolled** into the G/On server before they can be used in Rules.
- **Assigning a Token to a User** means to create a Rule with the User and a Token. The result should be the “Personal Token” element.

Adding Software to the Token



In order for the G/On clients to work for your users, you need to put the client software on the Tokens.

INFO ON ADDING TOKEN SOFTWARE

- Software on the Token is needed in order for Users to get access to the G/On server.
- Adding a collection of packages to a Token erases the current package content of the Token.

Open the Token Software Management perspective by clicking the button in the Perspective bar. Insert a Token into your local workstation and click Refresh until it appears in the Source list. On the right hand side you have a number of Package collections.

If you select the collection called G/On packages for all platforms, your users can run the G/On client on Windows, Mac or Linux as they choose. If you are absolutely sure they will only use a certain platform, you need only select the relevant collection, as it may save time and also space on the Token. After selecting the Package collection you want, click Install to start installation.

When installation finishes, you can hand the Token to a User and he/she can start using it.

ADDING TOKEN SOFTWARE

1. Open the **Personal Software Management** perspective.
2. **Select a Token** from the Source list.
Click Refresh if it does not show.
3. **Select a Package collection** to add to the Token depending on user's needs.
4. **Click Install** to add the collection to the Token.

Daily Use

The rules in the Action Authorization Policy perspective normally do not have to be changed very often.

Once the policies have been set up, they are in force, and you can add new users using the Personal Token Assignment perspective and the Token Software Management perspective.

DAILY USE

1. Open the **Personal Token Assignment** perspective.
2. Register a new token.
3. **Connect the token to a user** as a personal token.
4. Open the **Token Software Management** perspective.
5. **Add client software** to the token.
6. Hand the token to the user.
7. You're done

Reference

Basic Concepts

The purpose of G/On is to securely connect authenticated users to authorized applications. To prepare for this, the manager of a G/On system must define:

1. Which applications can be authorized,
2. Which Authentication Factors are sufficient for establishing the identity of a User
3. Which groups of Users can be authorized to use which applications, and
4. Under which circumstances an authorized application can be allowed to be used.

An application, which has been authorized for a given user, may appear in the menu for that user. In G/On terminology, the specification of an application is therefore called a *Menu Action*. Menu Actions are introduced below.

Which Authentication Factors are sufficient for establishing the identity of a User, and which groups of Users can be authorized to use which applications under which circumstances are defined in G/On in terms of so-called *Decision Rules*. Decision Rules are introduced below, after the introduction to Menu Actions.

Menu Actions

G/On Menu Actions are divided into the following types:

Port Forward. Creates one or more Port Forwards from the client side to the server side, and may start a client side command.

RDP Connection. Port forward with built-in RDP protocol inspection. Does single sign-on on the server side, and reacts to re-direction messages from Remote Desktop Connection Broker (Terminal Services Session Broker).

Citrix XML Interface. Enables Citrix applications, published through the Citrix XML interface, and makes them available as individual menu items in the G/On Menu, without having to install anything on the client PC.

Citrix Web Interface. Creates a http proxy connection between a browser on the client side and a Citrix Web server on the server side. The http proxy implements single sign-on the server side and launch of the Citrix client on the client side, without having to install anything on the client PC or browser.

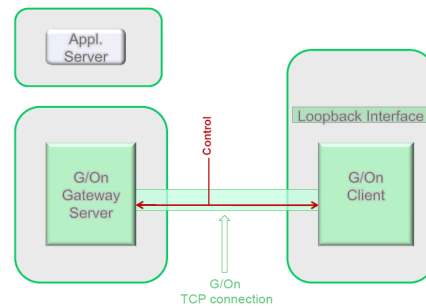
HTTP and SOCKS Proxy. Establishes a connection to the built-in proxy in the Gateway server. The proxy can handle HTTP and SOCKS proxy protocols, and can also function as a transparent

HTTP proxy. Menu actions of this type include specification of a server whitelist and may include configuration data for HTTP single sign-on.

G/On Internal. Starts the build-in G/On actions for installing, updating or removing Packages, or doing field enrollment of Tokens.

Wake-on-LAN. Sends wake-on-LAN packets from the G/On server to wake up a machine with a given network MAC address.

Each of the types is described more in detail in the following. In each description, we assume that the User has already established a session, and has been authorized to carry out the Menu Action. This means that the G/On client and G/On Gateway server have established a TCP connection between them, and through this TCP connection, the client and server exchanges control data.

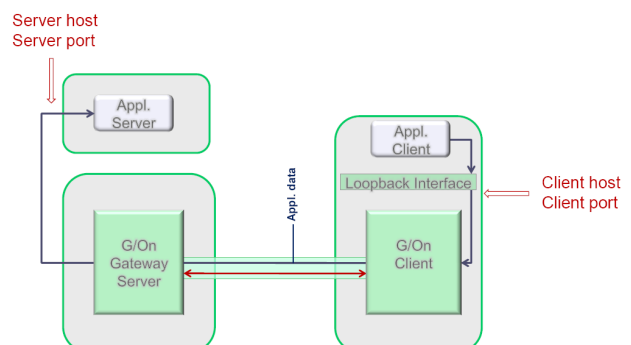
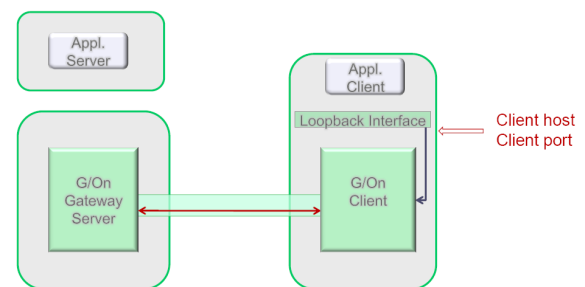


Port Forward Menu Actions

When the User selects the Menu Action, the Menu Action name is communicated from the client to the server, as control data. The server then looks up the definition of this specific Menu Action and instructs the client to do its part:

- To start listening on a given address and port (Client host, Client port).
- To start a given application client with given parameters. The parameters can, e.g., include the address and port which the client must communicate on, to reach the application server through G/On.

When the application client communicates on the given address and port, the G/On client forwards this communication through its TCP connection to the G/On server, and the G/On server forwards the communication through a



connection to the application server at an address and port, that was also defined by the Menu Action (Server host, Server port).

Citrix Web Interface Menu Actions

When the User chooses the Menu Action, the Menu Action name is communicated from the client to the server, as control data. The server then looks up the definition of this specific menu action, and contacts the Citrix Web Server at the specified address and port. The Web server responds by sending a web page with a login form, and the G/On server fills in the User Name and Password, and posts the form back to the web server.

The Citrix Web Server now initiates a User session, and sends a web page with icons for the Citrix enabled applications.

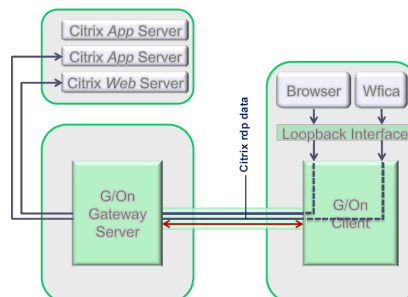
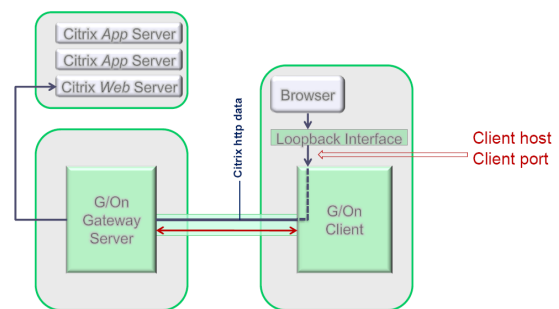
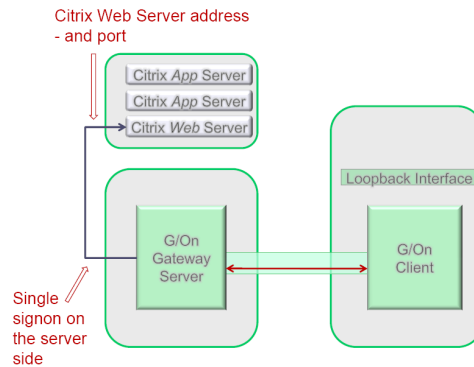
The G/On server forwards this page to the G/On client, which starts a browser. The start URL points to the G/On client itself, and allows the G/On client to serve the web page to the browser, so it can display the page to the User.

When the User clicks on one of the icons on the web page, the browser sends a request to get the .ica file, which describes how to start the corresponding application through Citrix.

The request is forwarded through the G/On client and server to the web server, which responds by sending the .ica file.

The .ica file is inspected by the G/On server in order to identify the address and port of the Citrix application server. The .ica file is then forwarded to the G/On client, which starts a Citrix client (wfica), and gives it the .ica file, however with an modified address and port, so the Citrix client will contact the Citrix Application server through G/On rather than directly.

When the Citrix client communicates on the



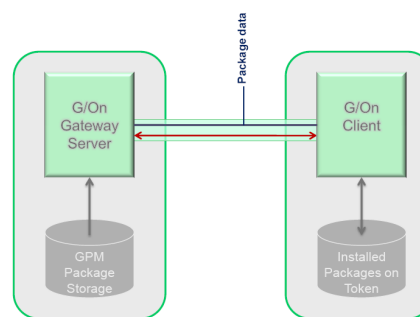
modified address and port, the G/On client and server forwards this communication to the original address and port of the Citrix application server.

G/Update Menu Actions

When the User selects the Menu Action, the Menu Action name is communicated from the client to the server, as control data.

The server inspects the GPM package storage to find out which packages are available, and this is compared with the information about which packages are currently installed on the token.

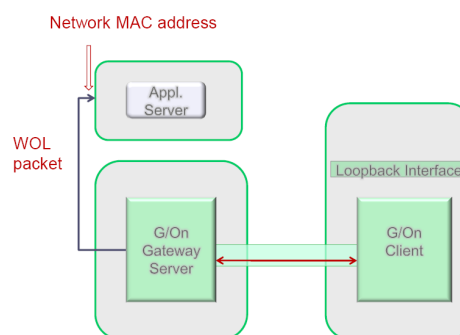
Depending on the definition of the G/Update Menu Action, the User is then presented with a wizard for either installing, updating or removing packages, and if needed, packages are downloaded from the server to the client.



Wake-on-LAN Menu Actions

When the User selects the Menu Action, the Menu Action name is communicated from the client to the server, as control data.

The server then looks up the definition of this specific menu action and then sends Wake-on-LAN packets to the device with the network MAC address, which is specified in the definition of the Menu Action.



Citrix XML Interface Menu Actions

When a User is authorized for a Menu Action of this type, the G/On server creates a connection to a Citrix XML service and logs in as this User. Each of the Citrix applications published for the User is then presented as a G/On Menu item.

When the User chooses one of these Menu items, the Menu item name is communicated from the client to the server, as control data. The server then looks up the definition of this specific Menu Action, and contacts the specified Citrix XML service, to get input for generating an .ica file that describes how to start the corresponding application through Citrix. The template for the .ica file is specified as part of the menu action.

The .ica file is then forwarded to the G/On client, which starts a Citrix client/Citrix receiver (wfica), and gives it the .ica file. The .ica file includes information about a local address and port, so the Citrix client will contact the Citrix Application server through G/On rather than directly.

When the Citrix client communicates on the local address and port, the G/On client and server forwards this communication to the original address and port of the Citrix application server, obtained from the Citrix XML service.

RDP Connection Menu Actions

When the User chooses the Menu Action, the Menu Action name is communicated from the client to the server, as control data. The server then looks up the definition of this specific Menu Action and connects to the specified Remote Desktop server (Terminal server).

The G/On server then instructs the client to start listening on a given address and port, and also to start the specified RDP client. When the RDP client communicates on the given address and port, the G/On client forwards this communication through its TCP connection to the G/On server, and the G/On server forwards the communication to the Remote Desktop server.

If the Remote Desktop server uses the Remote Desktop Connection Broker (Terminal Services Session Broker), it may respond that another server should be used. In that case, the G/On server connects to the other server.

When the Remote Desktop server asks for User Login, the G/On server provides User Name and Password on behalf of the User.

HTTP and SOCKS Proxy Menu Actions

When the User chooses the Menu Action, the Menu Action name is communicated from the client to the server, as control data. The server then looks up the definition of this specific Menu Action and instructs the client to do its part:

- To start listening on a given address and port (Client host, Client port).
- To start a given application client with given parameters. The parameters can, e.g., include the address and port which the client must communicate on, to reach the HTTP/SOCKS

proxy built into the G/On server.

When the application client communicates on the given address and port, the G/On client forwards this communication through its TCP connection to the G/On server.

If the client communicates using plain HTTP, the communication will then be routed through the transparent HTTP proxy in the G/On Server, and forwarded to an application server address and port specified in the Menu Action.

If the client communicates using the HTTP proxy protocol or the SOCKS proxy protocol, the communication will be routed to the built-in HTTP or SOCKS proxy in the server. The proxy will carry out the commands in the proxy protocol for establishing HTTP or TCP connections to given addresses and ports – however only if the addresses and ports are included in the whitelist specified in the Menu Action.

Rules and Elements

A G/On Decision Rule states that if given premises hold, then a given conclusion also holds. The Rules are written in this form (the number of premises can be 0, 1 or more):

PREMISE 1, **PREMISE 2** **⇒ CONCLUSION**

where both premises and conclusions have the form:

ELEMENT TYPE: *ELEMENT*

As an example, consider the following Rule:

TOKEN: *MICRO_SMART_0002*, **USER:** *BOB@GIRITECH.COM* **⇒** **PERSONAL TOKEN STATUS:** *PERSONAL TOKEN*

In short, it can be read as: “If the `micro_smart_0002` token is being used, and the User is `bob@giritech.com`, then we conclude that we have some known user with a Personal Token”.

Put differently, we can say that the rule registers the fact, that `micro_smart_0002` is a Personal Token of `bob@giritech.com`.

Technically, the premise: `Token: micro_smart_0002` is true, if the token `micro_smart_0002` has been verified as being plugged into the client computer.

And the premise: `User: bob@giritech.com` is true, if the User of the client computer has entered a Name and Password that, according to the User Directory (e.g. Active Directory), establishes that the User is in fact: `bob@giritech.com`.

So, technically, the conclusion of the rule expresses that the current User has been authenticated with two factors: Password verified by the User Directory and Personal Token verified by G/On.

Combining Rules to make more complex decisions

The conclusion of one Rule can be used as premise for other Rules. For example, consider these two Rules:

TOKEN: MICRO_SMART_0002, **USER:** BOB@GIRITECH.COM ⇒ **PERSONAL TOKEN STATUS:** PERSONAL TOKEN

USER GROUP: EMPLOYEES, **PERSONAL TOKEN STATUS:** PERSONAL TOKEN

⇒ **AUTHENTICATION STATUS:** AUTHENTICATED

Assuming that the conclusion of the first Rule holds, this can be used “as input” to the second Rule.

If we also assume that bob@giritech.com is a member of the User Group *Employees*, the second Rule then allows us to conclude that the current User is *Authenticated*.

Overview of the types of Elements in G/On

Token. Elements of this type are things that can be given to a User, and which the User can then present at a later time in order to confirm his or her identity. Some Tokens also have a capacity to hold client side software, such as the G/On client, application clients, and even a whole client side operating system.

User. Elements of this type are Users, registered in a User Directory.

Personal Token Status. There is only one, fixed Element of this type. The Element is called: Personal Token. It represents the fact that a known User (from a User Directory) has presented (one of) his Personal Tokens.

User Group. Elements of this type are User Groups, registered in a User Directory

Authentication Status. There is one, pre-defined Element of this type. The Element is called: Authenticated. It represents the fact that a User has been properly authenticated. Other Elements can be defined in G/On, if needed.

Token Group. Elements of this type are groups of Tokens. They are defined in G/On.

G/On User group. Elements of this type are groups of Users, defined in G/On (not in the User Directory)

Menu Action. An element of this type is a specification of an application, that may appear in the user's menu. See the overview of menu actions, above.

IP Range. An element of this type represents a range of IP addresses, as they may be observed by the G/On Gateway Server when a G/On Client connects. The range may concern either the client side or the server side address.

Operating System State. An element of this type represents observed properties of the state of the operating system, where the G/On Client is running.

Login Interval. An element of this type represents a time of day/day of week interval.

Zone. Elements of this type represent circumstances of a user session, that may be required before the user can be allowed to use given menu actions

Management Role. An element of this type represents a role that a G/On Manager may have, and the (limited) set of privileges that are needed for carrying out the management tasks of that role.

Overview of the types of Rules in G/On

Personal Token Assignment Rules register the fact, that a given Token is a Personal Token of a given User. The Rules have the type:

TOKEN, USER ⇒ PERSONAL TOKEN STATES

User Authentication Policy Rules register policies for authentication. The Rules have one of the types :

PERSONAL TOKEN STATUS ⇒ AUTHENTICATION STATUS

USER GROUP, PERSONAL TOKEN STATUS ⇒ AUTHENTICATION STATUS

G/ON USER GROUP, PERSONAL TOKEN STATUS ⇒ AUTHENTICATION STATUS

TOKEN GROUP ⇒ AUTHENTICATION STATUS

USER GROUP, TOKEN GROUP ⇒ AUTHENTICATION STATUS

G/ON USER GROUP, TOKEN GROUP ⇒ AUTHENTICATION STATUS

USER GROUP ⇒ AUTHENTICATION STATUS

G/ON USER GROUP ⇒ AUTHENTICATION STATUS

Action Authorization Policy Rules register policies for giving access to Menu Actions. The Rules have one of the types:

AUTHENTICATION STATUS, USER GROUP ⇒ MENU ACTION

AUTHENTICATION STATUS, G/ON USER GROUP ⇒ MENU ACTION

USER GROUP ⇒ MENU ACTION

G/ON USER GROUP ⇒ MENU ACTION

⇒ MENU ACTION

AUTHENTICATION STATUS, USER GROUP, TOKEN GROUP ⇒ MENU ACTION

AUTHENTICATION STATUS, G/ON USER GROUP, TOKEN GROUP ⇒ MENU ACTION

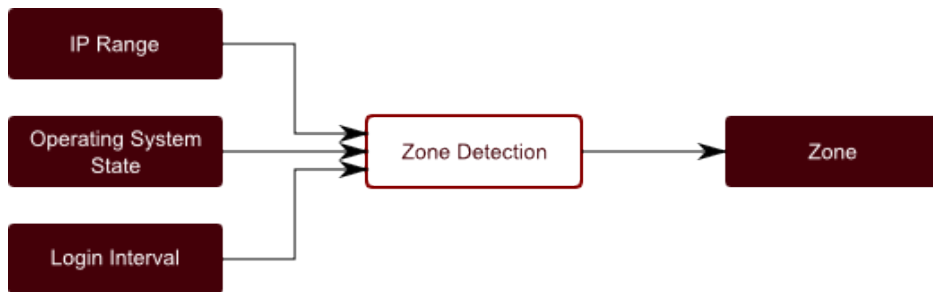
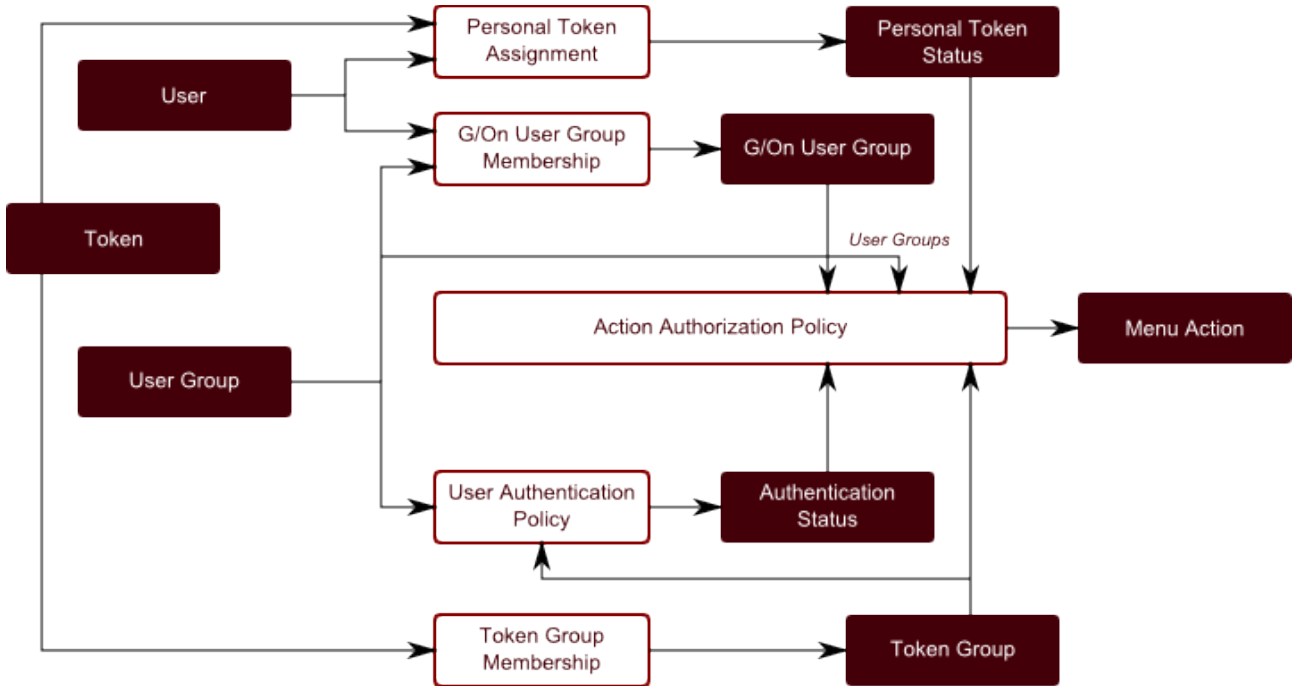
IP RANGE,

LOGIN INTERVAL ⇒ ZONE

LOGIN INTERVAL ⇒ ZONE

⇒ ZONE

Overview of the way Rules fit together in G/On



The Rule Engine

User Sessions – Deciding which Menu Actions are Authorized and Active

The G/On Rule engine is used in the Gateway Server, where it starts each time a new User session is created.

First the engine examines all the Rules, which have been entered in the G/On Management interface, and checks all the basic premises, which occur in the Rules. For instance, when there are Rules with premises of type *User*, it asks the User management layer in G/On to present a Login dialogue and verify User Name and Password in the appropriate User Directory.

Having checked the basic premises, the Rule engine then checks if any Rule has fulfilled *all* its premises. In this case, the engine registers the conclusion of the Rule. This conclusion may be the premise of other Rules, which now have all premises fulfilled, leading to new conclusions being registered, etc.

The process stops when no more new conclusions can be found. At this time, the Rule engine:

- Collects all the conclusions of type *Menu Action*, and registers them as the *Authorized Menu Actions* for the current User session.
- Collects all the conclusions of type *Zone*, and registers them as the *Active Zones* for the current User session.

Each authorized menu action is then considered:

- If it is not restricted to any Zones, the Menu Actions is marked as an *Active Menu Action*
- If it is restricted to one or more Zones, and at least one of these is an Active Zone, the Menu Actions is marked as an *Active Menu Action*
- If it is restricted to one or more Zones, and none of these is an Active Zone, the Menu Actions is marked as an *Inactive Menu Action*

All the authorized menu actions will be shown to the user, but the inactive ones will be marked as such, and the server will only carry out a menu action if it is active.

Management Sessions – Deciding which Management Roles are Active

The G/On Rule engine is also used in the Management Server, where it starts each time a new Management session is created. Here, it only works on the specified Management Role Assignments Rules, in order to determine which roles the current manager has.

The Management Client

The management client is a tool that, among other things, lets an administrator add Rules to the Rule engine and create Tokens for Users. After installation there should be a sub-menu in the windows start menu called 'G-On'. Navigate to the menu item labeled G-On Management and use this menu item to launch the Management Client.

If there are no G-On menu items, the Management Client program: `gon_client_management.exe` can be found in the folder:

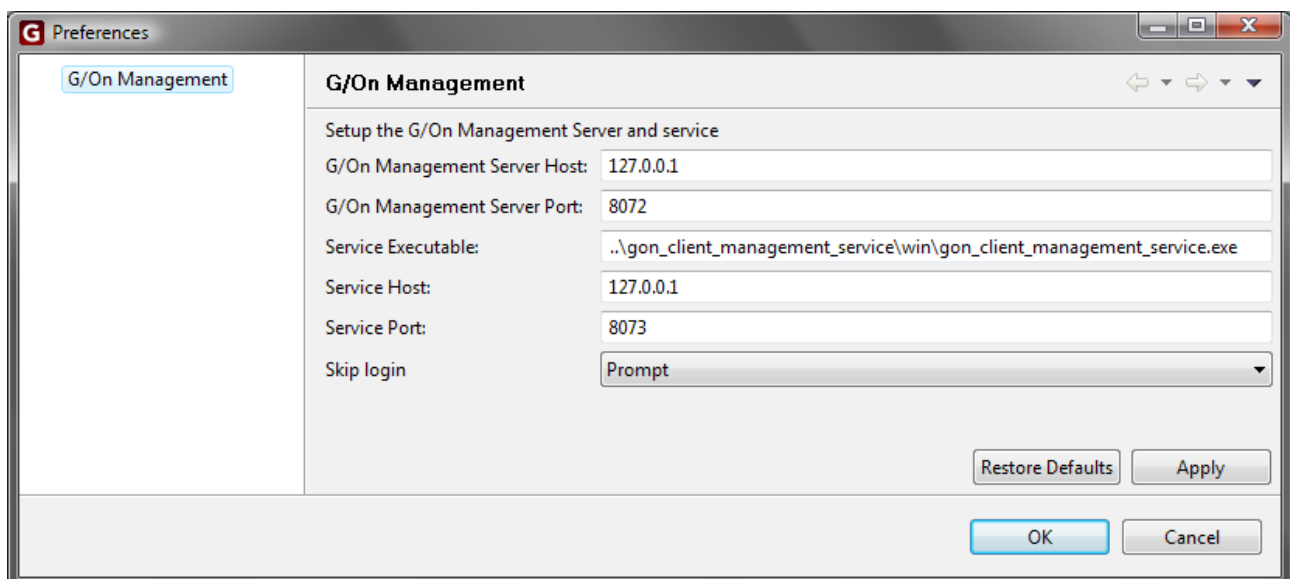
Program Files (x86) → Giritech → gon_<version> → gon_client_management

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

The Management Client is separated into a number of different perspectives. Some of these perspectives are used for creating Rules. The perspectives used for creating Rules all have the same basic functionality. Adding Elements to the Rule engine always takes place in a Rule creation perspective. Special perspectives have been created for tasks that do not create Rules for the Rule engine. For example adding software to a Token or getting Reports on system usage.

Preferences

Preferences for the Management Client are used for setting connection and login settings.



The settings are:

- **G/On Management Server Host:** IP address or DNS name of management service host

- **G/On Management Server Port:** Port number management service listens on.
- **Service Executable:** Path to local management server tool executable.
- **Service Host:** IP address for the local management service. This should only be if, for some reason, it is not possible to set up a service on 127.0.0.1.
- **Service Port:** The port number used to communicate with the local service.
- **Skip login:** Setting for the login dialog. There are four possible values:
 - **Always:** The login dialog will not be shown at start-up.
 - **Default:** The “Skip login” box in the login dialog will be checked by default.
 - **Prompt:** Default setting.
 - **Never:** It is not possible to skip login.

Note: If, for some reason, it is not possible to access G/On Management to edit the preferences, it is possible to restore the default settings by removing the folder “workspace” located in the folder containing the G/On Management executable (<installation folder>\gon_client_management on the server).

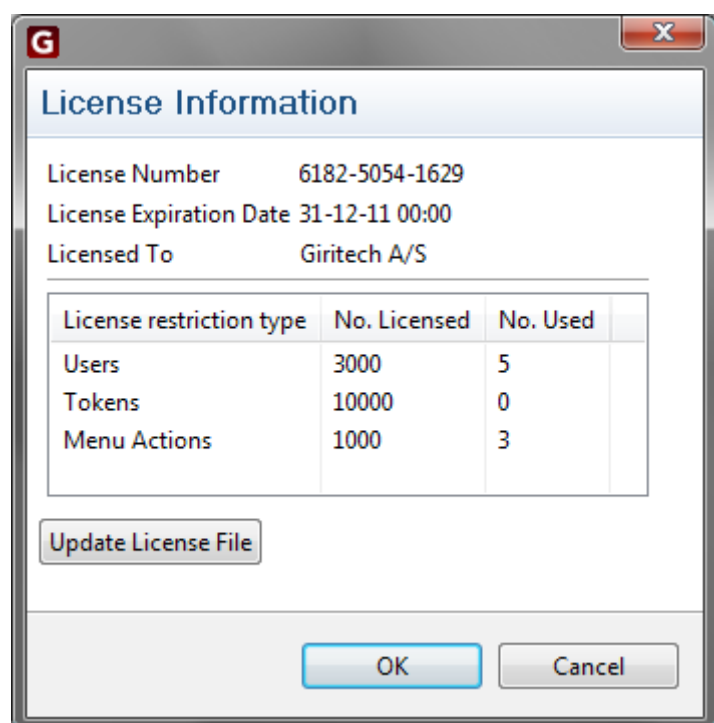
License information

The license information window is available in the “View” menu. In this window it is possible to see current license information and update the license.

By pushing the “Update License File” a file chooser will open, in which the new license file can be selected.

The license information window is only available if the user has the “Gateway server configuration” access right and updating the license file is only possible if the access right is read/write.

Note: If the current license is invalid, it will not be possible to start G/On Management. If the number of user, token or menu action licenses has been exceeded a nagging background will be shown in all rule policy perspectives.



Introduction to perspectives

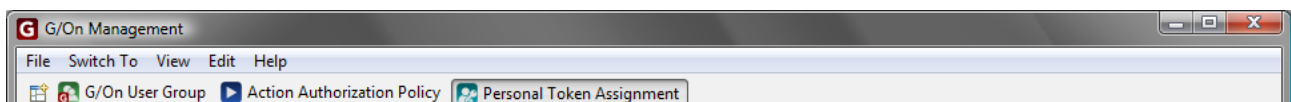
Perspectives are defined as a full window with a specific purpose. Most perspectives are used for defining Rules for the Rule engine. Additional perspectives are used for adding software to Tokens or display Reports on system usage.

The perspectives included in the Management Client are:

- **G/On User Group perspective** adds User or Groups to local G/On User Groups via Rules.
- **Action Authorization Policy perspective** sets up Authorization Policies via Rules.
- **User Authentication Policy perspective** sets up Authentication Policies via Rules.
- **Personal Token Assignment perspective** sets up User and Token links via Rules.
- **Token Software Management perspective** adds software to a Token.
- **Token Group Management perspective** adds Tokens to Token Groups via Rules.
- **Menu Structure Management perspective** orders User Menus via Tags.
- **Reporting perspective** gets information on system usage.
- **Gateway Servers perspective** manages running Gateway Servers and User Sessions.
- **Management Role Assignment perspective** defines who can do what in the Management Client.
- **Zone Management perspective** defines special circumstances that may be used to restrict access to otherwise authorized actions.

Use the perspective bar to select another perspective. The perspective bar is by default set to include the most used perspectives when first using the management client. If the wanted perspective is not in the perspective bar, use the open perspective button, in the far left of the perspective bar, to open other perspectives.

The Perspective bar



The Perspective bar is used for changing the current perspective. When the Management Client first launches it will display buttons for the three most used perspectives. These are:

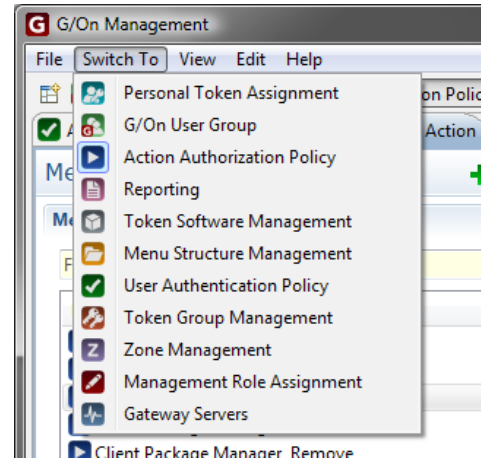
- **G/On User Group** – for defining the group of Users who are allowed to enroll a Personal Token “in the field”

- **Personal Token Management** – for activating Personal Token assignments and thereby approving field enrollment requests
- **Action Authorization Policy** - for defining which Menu Actions are authorized for use by which User Groups, under which which circumstances

Selecting other perspectives

Choose the menu Switch To and then choose the relevant perspective.

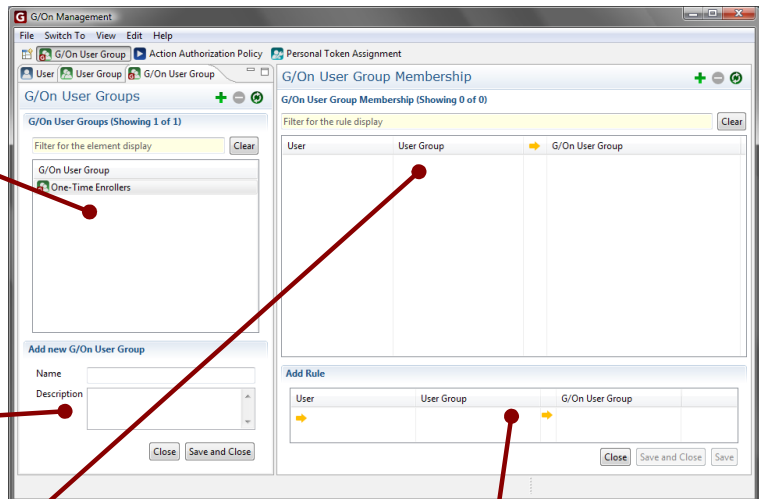
When a Perspective has been chosen in the menu, it will appear and stay in the Perspective bar. Buttons in the Perspective bar can be removed by right-clicking and choosing Close.



Perspective layout

Underneath the Perspective bar on the left hand side is number of Element tabs. The Element tabs holds a list of the existing Elements of specific types. A filter field is used for locating Elements by name.

When choosing to add or edit an Element the Add/Edit Element area appears at the bottom.



At the right hand side is a listing of Rules related to the selected perspective.

When adding or editing a Rule the Add/Edit Rule area will appear at the bottom.

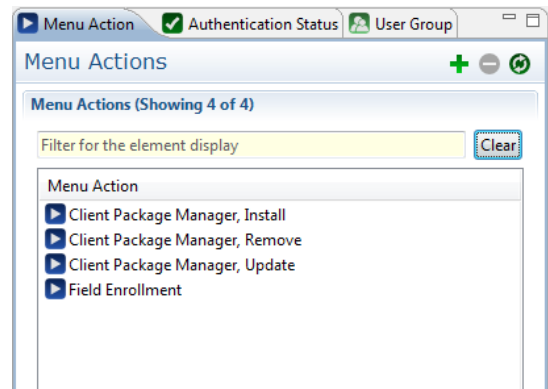
Resetting the perspective

If the perspective seems to be out of order somehow, it is possible to reset the different parts of the

perspective. In most cases this should not be needed. However to reset the perspective go to the menu and choose View > Reset Window.

Introduction to Element lists

The Elements in the Element lists are used for creating Rules that are located in the Rule lists. For each type of Element there is an Element list. The Element list available in any perspective reflects the Elements that can be used in Rule creation in that specific perspective.



Listing Elements

The list should show all the available Elements of the selected type. It is possible to refresh the Element list, thereby ensuring that all Elements are displayed:

- Click anywhere in the list area. Then choose View > Refresh in the menu.
- Click anywhere in the list area. Then press the keyboard short cut F5.

Editing Elements

Most Elements can be edited.

There are several ways of editing existing Elements:

- Double-click the Element to start the editor.
- Select the Element that should be edited and press Enter.
- Right-click on the Element the should be edited and choose Edit from the context menu.
- Select the Element that should be edited. Then press the keyboard short cut Ctrl-E.

Note that not all Element types can be edited (For instance groups retrieved from a User Directory).

The editing possibilities depend on the Element type. Please refer to the subsections on the individual Elements for details.

Creating new Elements

There are several ways of adding new Elements:

- Click the plus sign (+) in the upper right corner.

- Right-click anywhere in the list area. Then choose New from the the context menu. For some Element types, it is also possible to choose Create Copy.
- Click anywhere in the list area. Then choose Edit > New.
- Click anywhere in the list area. Then use the keyboard short cut Ctrl-N.

Click the 'Close' button to close the editor without saving. Click the 'Save and close' button to save the changes and close the editor.

Deleting Elements

There are several ways of deleting an Element:

- Right-click the Element you wish to delete. Then choose Delete in the context menu.
- Select the Element you wish to delete. Then choose Edit > Delete.
- Select the Element you wish to delete. Then press the keyboard short cut Ctrl-D.

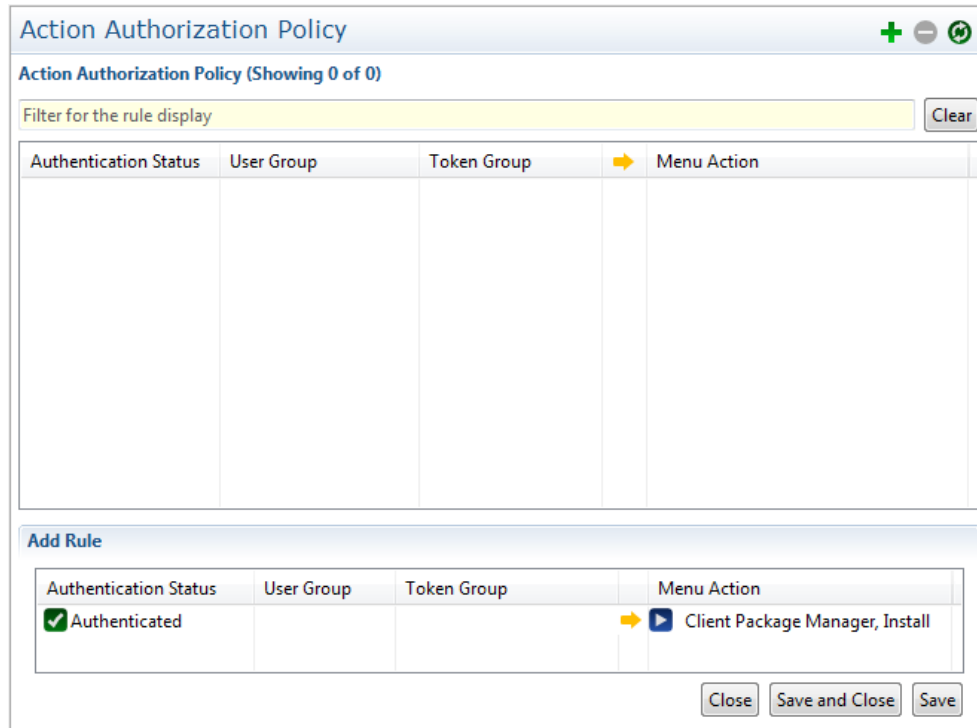
You will be asked to confirm the deletion of the selected Element.

Filtering Elements

The Element filter is a live filter. This means that while typing in the filter input area the list adjusts to display the relevant Elements. Use the Clear button to clear the filter and display all available Elements.

Introduction to Rule lists

The Rule list shows all the Rules that correspond to a specific perspective.



Listing Rules

The Rule list should show the Rules related to the selected perspective. It is possible to refresh the Rule list, thereby ensuring that all Rules are displayed:

- Click anywhere in the Rules list. Then press the keyboard short cut F5.
- Click anywhere in the Rules list. Then choose View > Refresh.

Creating new Rules

In any of the Rule based perspectives it is possible to create new Rules. There are several ways of starting to create new Rules.

- Click the green plus sign (+) at the top right.
- Click anywhere in the Rules list. Then press the keyboard short cut Ctrl-N.
- Click anywhere in the Rules list. Then choose Edit > New.
- Right-click anywhere in the Rules list. Then choose New in the context menu.

Any of these should result in the Add/Edit Rule area appearing at the bottom of the perspective.

Editing Rules

Rules can be edited. There are several ways of editing a Rule:

- Double-click the Rule.
- Select the Rule. Then press Enter.
- Right-click on the Rule. Then choose Edit in the context menu.
- Select the Rule. Then press the keyboard short cut Ctrl-E
- Select the Rule. Then choose Edit > Edit.

Single elements can be removed from an existing rule by right-clicking the element and selecting remove from the context menu.

Deleting Rules

Rules can be deleted. There are several ways of deleting a Rule:

- Select the Rule. Then press the keyboard short cut Ctrl-D
- Select the Rule. Then choose Edit > Delete.
- Right-click the Rule. The choose Delete from the context menu.

Filtering Rules

The Rule filter is a live filter. This means that while typing in the filter input area the list adjusts to display the relevant Rules. Use the Clear button to clear the filter and display all available Rules. The filter considers all Elements in a Rule to see if something matches.

Adding Elements to a Rule

Elements are selected from the Element lists. There are several ways of adding an Element to a Rule:

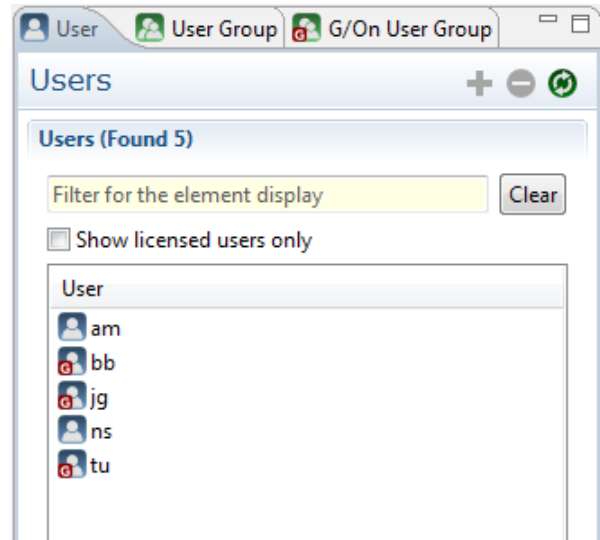
- Select the Element and drag it onto the Add/Edit Rule area.
- Select the Element and drag it into the Rule list.
- Select the Element. Then press the keyboard short cut Ctrl-A
- Right-click the Element and choose Add to rule editor from the context menu.
- Select the Element. Then choose Edit > Add to rule editor.

Adding an Element to a Rule results in that Element appearing in the Add/Edit Rules area at the location provided for that specific Element type. Adding another Element of the same type removes the existing Element and adds the new one instead.

Element: User

User Elements represents an actual User on the G/On server.

User Elements come from the User Directories, which the server is set up to connect to. This may also include local Users on the machine where the G/On Management and G/On Gateway Servers are running. User Elements may be used in the Personal Token Assignment perspective and the G/On User Group perspective. Note that there is a limit of 500 on the number of users shown in the list by default. This limit has been introduced in order for G/On Management to work with large user directories. The limit size can be changed in G/On Configuration.



New

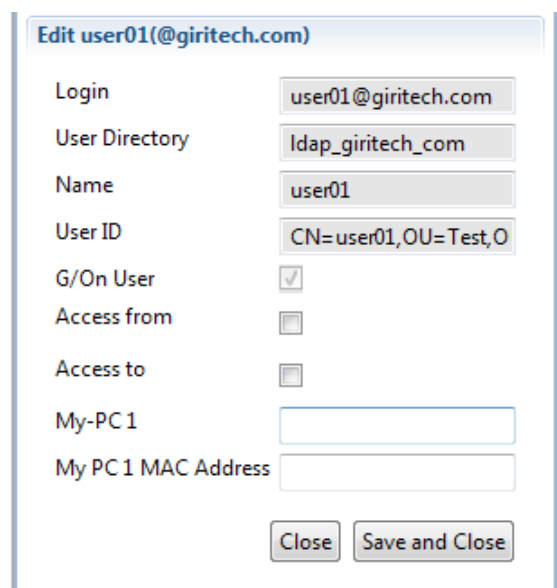
It is not possible to add new Users directly through G/On. Users should be created in one of the external User Directories.

Edit

The User Elements can be edited. See page 36 for information on how to start editing. Note that once settings have been saved, the user will be registered as a G/On user and therefore count as a licensed user. If the number of licensed users have been reached already it will not be possible to save settings for an unregistered user.

The settings that can be changed for a User are the access period and the User's personal workstation settings.

An access period can be set for a user, so that the user will only be considered a valid user during that period. Checking the "Access from" will reveal a date and a time field in which the start date of an access period can be entered. Likewise an end date and time can be entered by checking the



“Access to” box. If only one of the fields is checked it means that the access period is open-ended at one end. Leaving both unchecked means that there is no time restriction on the User's access.

The personal workstation settings (the My PCx fields) allows you to set up actions that will allow a User direct and secure access to his/her personal workstation from anywhere. Note that any number of workstations can be set up. In order to set up more than one workstations, first enter the data for the first one, save it and then edit the User again. It is now possible to add information on workstation 2 and save it. After that you can add workstation 3 and so on.

It is possible to create a Menu Action that will wake up a User's personal workstation. For this Menu Action to work properly the workstations mac address needs to be set. The Menu Actions are created in the Menu Action list. See page 50 for more information on the Menu Action list.

It is not possible to change any User Directory related settings through the G/On management client.

Delete

It is not possible to delete Users directly through G/On. Users should be deleted in one of the external User Directories.

Add as G/On user

This is a shortcut for adding a user as a licensed G/On user. A user can also be added by editing user settings or by creation of a rule containing the user.

Remove from G/On users

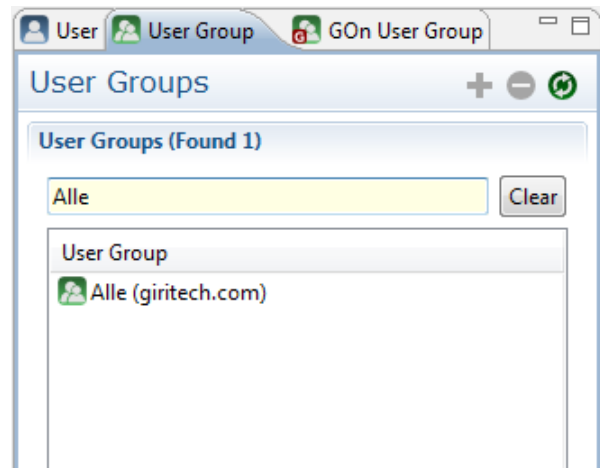
This action will remove the user from the G/On database. If the user has been assigned a personal token, it is not possible to remove. The token assignment rules containing the user must be deleted first. Memberships of G/On user groups will, however, be deleted automatically when the user is been removed.

Show licensed users only

Checking this box will change the User view so that only users registered as licensed G/On users are shown in the list. Note that a user which has been registered as a G/On user, but has been deleted from the user directory, will only appear in this list. Also note that there is no limit on the number of users shown in this list.

Element: User Group

User Group Elements come from the User Directories, which the server is set up to connect to. This may also include local groups on the Machine where the G/On Management and G/On Gateway Servers are running. It is not possible to add or remove Users from User Directory User Groups from within the G/On Management Client. User Groups are used in the Authorization and the Authentication Policy Perspectives.



Note that there is a limit of 500 on the number of users shown in the list by default. This limit has been introduced in order for G/On Management to work with large user directories. The limit size can be changed in G/On Configuration.

Note: In the perspectives: User Authentication Policy and Action Authorization Policy, the User Group list is actually a *mix* of groups from the User Directories and G/On User Groups (see below).

New

Creating a new User Group defaults to creating a new G/On User Group. If you create a new G/On User Group you should go to the G/On User Group Management Perspective to manage which Users should be part of your new group. See page 36 for information on how to create new Elements.

Edit

It is not possible to edit any settings for User Directory Groups directly through G/On. These groups should be edited in one of the external User Directories.

In the G/On User Group Management perspective it is possible to edit both the title of G/On User Groups and which Users are member of the group.

Delete

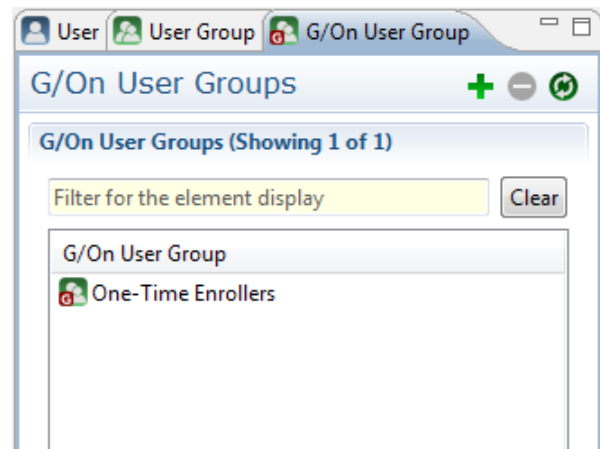
It is not possible to delete User Directory User Groups directly through G/On. These User Groups should be deleted in one of the external User Directories.

It is possible to delete G/On User Groups in the G/On User Group Management perspective. But only if they are not used in any Rule.

Element: G/On User Group

G/On User Groups can be used as an extension of the User Directory Users and Groups. If you have a number of User Directory Groups and individual Users that you wish to combine into one Group, you can use G/On User Groups for that purpose. This can significantly simplify Authorization and/or Authentication Policies.

Note: There is a special, built-in G/On User Group: One-Time Enrollers. It is intended to be used in connection with field enrollment: Users in this Group can be authorized to enroll a Token, as a action in the end-user G/On client.



New

It is possible to create new G/On User Group Elements. See page 36 for information on how to create new Elements.

Edit

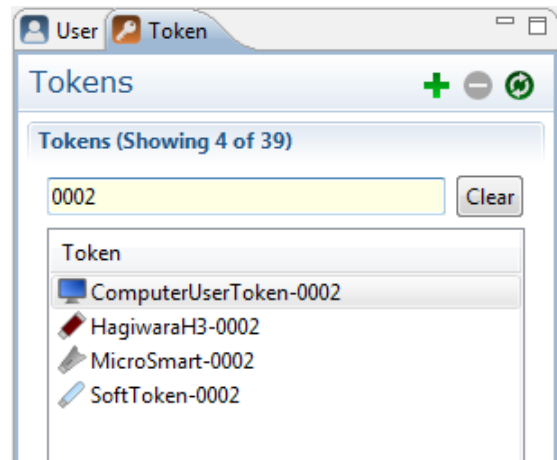
You can edit the name of any G/On User Group that is not built-in. See page 36 for information on how to start editing Elements.

Delete

It is possible to delete G/On User Groups that are not built-in or in use in any Rules. See page 37 for general information on how to delete Elements.

Element: Token

A Token is a hardware or software device that can serve as an authentication factor of the kind: "Something You Have". So a Token can be distributed to a User, and the User can then present the Token at a later time in order to confirm his or her identity. Some Tokens also have a capacity to hold client side software, such as the G/On Client, application clients, and even a whole client side operating system.

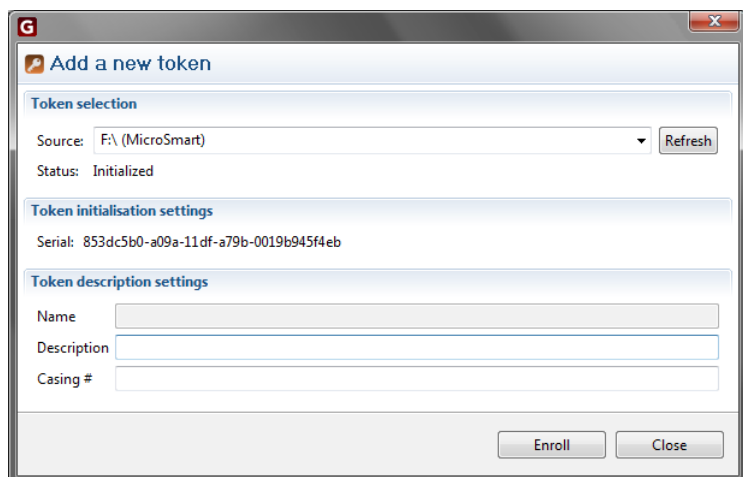


New

Token Elements are added to the system by enrolling them. See page 36 for information on how to start creating new Elements.

Creating a new Token Element results in opening the 'Add new token' dialogue.

The source drop-down shows any valid Token inserted into the local workstation.



Note: Some tokens must be initialized before they can be enrolled. See the G/On Setup and Configuration Reference, section: Advanced Setup Topics - Initialization of Tokens.

If no Token is shown in the Source drop-down try inserting another Token and click Refresh. For any Token you can add a Description and a Casing Number. Click Enroll to add the selected Token to the G/On Server. The new Tokens Serial number should now appear in the Token list.

Click Close to close the editor without saving. Click Save and close to save the changes and close the editor.

Edit

The Tokens that are enrolled into the server can be edited. See page 36 for information on how to start editing Elements.

It is possible to edit the Description and the Casing Number fields. The Serial Number is used by the G/On system and needs to be unique. Therefore it can not be changed.

Click Close to close the editor without saving. Click Save and close to save the changes and close the editor.

Delete

It is possible to delete Tokens. But only if the Token is not used in any Rules. See page 37 for general information on how to delete Elements.

Types of Tokens

SoftToken is a top level folder on a removable device with G/On software and a private key file for authentication.

MicroSmart Token is a MicroSD card with a flash drive with G/On software and a built-in Smart Card with a private key for authentication.

MicroSmart USB Token is a USB adapter with a MicroSmart Token (see above). Software which accesses the Token cannot distinguish it from Tokens of the type: MicroSmart.

Hagiwara H2/H3 USB Token has both a CD and a flash drive with G/On software and a hidden Unique ID and private key file for authentication.

Computer User Token is a computer (PC or other computing device) where a (possibly non-admin) User has "installed" a private key and the G/On software in the Users home directory/registry on a computer. The key file is typically locked to a specific computer by a screening check of the MAC addresses.

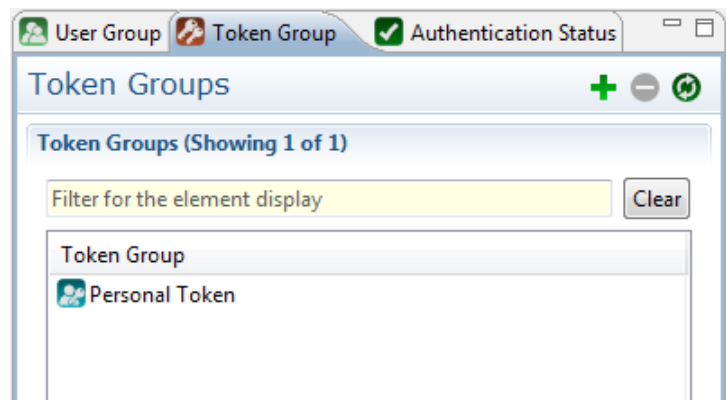
Mobile Token is a mobile device, e.g. an iPhone, where a (possibly non-admin) User has "installed" a private key and the G/On software on the device. The key file is locked to a device by a screening check of the unique ID of the device.

Smart Card Token is a private key authentication factor which can be inserted in a Smart Card Reader in a PC running the G/On software.

Element: Token Group

Token Groups are collections of Tokens that can be used when formulating User Authentication Policies or action Authorization Policies. Which Tokens are members of which Token Groups is defined in the Token Group Management perspective.

Note: In addition, there is a built-in, “dynamic” Token group called 'Personal Token' which is used for identifying the Personal Tokens of the User of the current session. This is defined in the Personal Token Assignment perspective.



New

It is possible to add new Token Group Elements. See page 36 for general information on how to create new Elements.

Edit

It is possible to change the name of Token Groups – but only in the Token Group Management perspective. See page 36 for more information on how to start editing Elements.

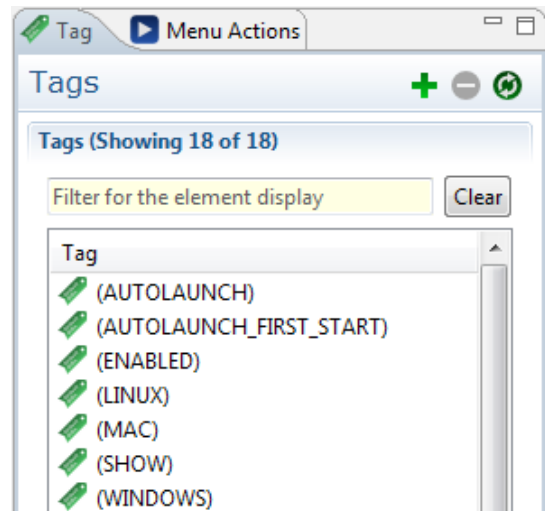
Delete

Any Token Groups that is not built in can be deleted when they are not used in any Rules - but only in the Token Group Management perspective. See page 37 for general information on how to delete Elements.

Element: Tag

The Tag Elements can be used to categorize your Menu Actions. All Menu Actions are assigned a number of Tags. A Tag can be placed in a Menu structure and then any Menu Action that has that Tag will be added in the Tag's location (But only if the User has access to that specific Menu Action). Any personalization of menu actions placement in the user menu is done by manipulating tags. Because of the dynamic nature of when Menu Actions are available to Users, the location of Menu Actions can not be done more precisely.

Note that several predefined Tags exist. See page 55.



New

It is possible to add new Tags. See page 36 for general information on how to create new Elements. Note also that new Tags can be introduced by adding them to a Menu Action – see page 55.

Edit

It is possible to edit Tags. See page 36 for more information on how to start editing Elements.

Each Tag has several settings that can be changed.

- **Name** is the Tag's name. This is the name which is used as referral in Menu Action specifications. The Tag name can only consist of alphanumeric characters and is always in upper case (lower case letters entered will be converted when the Tag is saved)
- **Caption** is used for naming a folder in the User menu that will contain Menu Actions with this Tag.
- **Show in menu** is used for deciding whether or not this Tag should be shown as a folder in the User menu. Some Tags should not. For instance tags can be used to decide whether some Menu Actions should be displayed at all.
- **Parent Tags** are listing the parents to this Tag in the menu structure. A Tag can have any number of parent Tags. Note that parent Tags can only be edited by dragging the Tag onto the menu tree.

- **Max items to show** are used for limiting the number of items displayed in the menu folder with Menu Actions with this Tag. This is useful for e.g. creating top 3 most used menu folders. If the value is 0, all items are displayed.
- **Sort option** is used alone or in combination with the “Max items to show” functionality to find the order of items shown. Possible values are most used, last used or plain alphabetically.
- **Override item show** can be set in order to always see all Menu Actions in the menu even though other factors (e.g. client platform) prevents it from being shown. Useful for checking that a Menu Action has been authorized for a User.
- **Automatically add to all items** is used for adding this tag dynamically to all Menu Actions. This is used for creating an “All Programs” menu or a “Top <X> Most Used” folder for the Users.

Delete

It is possible to delete Tags. See page 37 for general information on how to delete Elements.

Element: Menu Action

The Menu Action Elements are the Elements that correspond to the Menu items that may end up in the end-users menu if they are authorized to use it. See the introduction in the section: “Menu Actions“, on page 17.

New

It is possible to add new Menu Actions. See page 36 for general information on how to create new Elements. Note that it is possible to start creating a new Menu Action, based on a copy of an existing Menu Action: right-click and choose Create New.

This will start a Menu Action creation wizard that will guide you through the set up of the most commonly used Menu Actions. If you need to create a Menu Action that is more specialized you can use the default wizard.

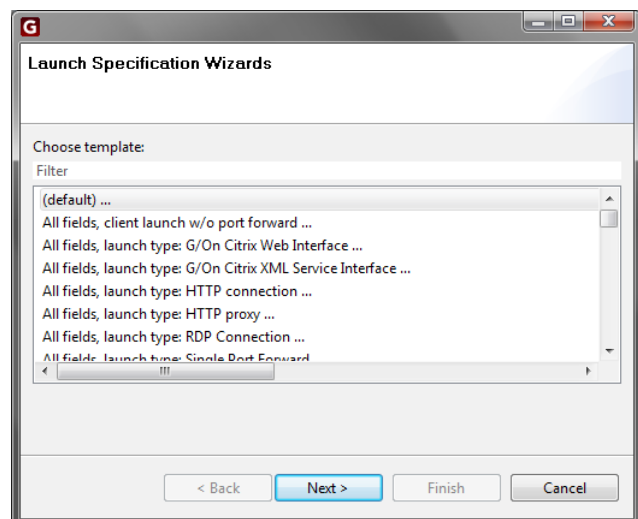
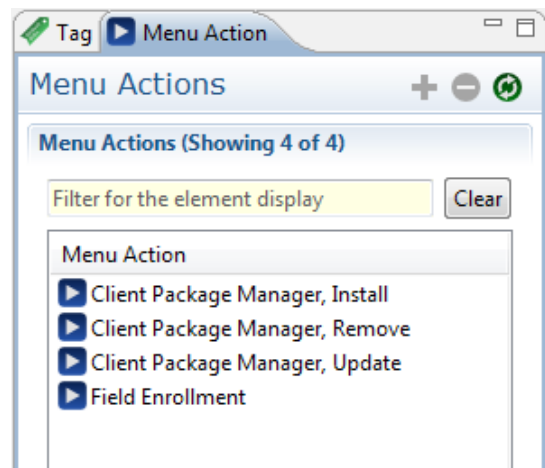
Click next and fill in the required information until you can click Finish and the Menu Action appears in the Menu Action list.

Some Menu Actions require information about specific User's workstation settings. These settings are added in the User's information editor. See page 41 for more information on editing User settings.

Some Menu Actions require a special setup of an application server. These are documented on page 95.

Properties

It is possible to edit a Menu Actions. The editor resembles the wizard pages for the specific Menu Actions. See page 36 for information on how to start editing Elements.



Delete

It is possible to delete Menu Actions that are not used in any Rules. See page 37 for general information on how to delete Elements.

Create Copy

Create a new Menu Action based on an existing one.

View

View the Menu Action using the default wizard in read-only mode.

Add/Remove zone restrictions

Add or remove Zone restrictions to/from a Menu Action. See page 61 for further description of the Zone concept.

General Features of Menu Actions

The different Menu Action templates have different fields, but there is a basic set of fields, which are used in many templates. These fields and their meanings are described in the following.

Note: For an introduction to the notion and types of Menu Actions, see the section: “Menu Actions“, on page 17.

Fields for identifying the Menu Action

Each Menu Action has a unique name and a title and optionally an image (icon). The unique name is internal, only visible to the administrators. The title is used in the menu presented to end-users; it need not be unique across all menu actions. For instance, the title: “Remote desktop” can be used both for a menu action for Windows client, and a menu action for the Mac client, which provide access to the same terminal server:

- Name
- Menu Title
- Menu Image ID (currently only used on iPad/iPhone)

Fields for defining port forward(s)

Menu Actions of the type: "Port Forward" can define 1 or more port forwards. Each port forward is defined by the listening address and port on the client side and the address and port on the server side:

- Client Host (default value: 127.0.0.1)
- Client Port (default value: 0, which means: pick any unused port)
- Server Host
- Server Port

This works much like a port/address translation in a router:

1. An application on the client PC can connect to the *client port* at the *client host* address
2. This connection will be translated (forwarded) to the *server port* at the *server host* address, on the network where the G/On server is located.

Fields for defining client-server connectivity with RDP and Citrix connections

When a menu action of type: "RDP Connection", "Citrix XML Interface" or "Citrix Web Interface" has been started, the G/On client will listen for connections from the application client (RDP client, ICA client or browser) on a specified address and port:

- Client Host
- Client Port

On the server side, connection to an RDP or Citrix server is specified by server address and port:

- Server Host
- Server Port

In order to support fail-over and load sharing functionality, a list of hosts can be specified in the Server Host field. If the initial connection to one host fails, there will be fail-over to another one in the list. Note, however: there is no "hot" fail-over - connected users must reconnect after failure.

Entries in the list of hosts must be separated by space. Optionally, a port can be added to each entry, separated by a colon. If there is no port added to an entry, the port specified in the separate field: Server Port is used.

Special tags can be specified at the start of the list of hosts, separated by space:

- Specify: `#random` to share the load among the servers. This is the default.
- Specify: `#failover` to start with the first host and fail-over on failure.

- The number of seconds before a host should time out and considered a failure can be specified as: `#timeout=3` (which is the default).

Examples:

- `#failover #timeout=2 primary.server.com secondary.server.com`
- `#random fw.com:112 fw.com:911`

In addition to the explicitly defined addresses and ports, menu actions of types: “RDP Connection”, “Citrix XML Interface” and “Citrix Web Interface” may automatically create other connections as described above in the section: “Menu Actions“, on page 17.

Fields for defining client-server connectivity with HTTP and SOCKS proxy connections

When a menu action of type: “HTTP and SOCKS Proxy” has been started, the G/On client will listen for connections from the application client (e.g. a browser) on a specified address and port:

- Client Host
- Client Port

If the client communicates using plain HTTP, the communication will be routed through the transparent HTTP proxy in the G/On Gateway Server, and forwarded to the specified application server address and port:

- Server Host
- Server Port

If the client communicates using the HTTP proxy protocol or the SOCKS proxy protocol, the communication will be routed to the built-in HTTP or SOCKS proxy. The proxy will carry out the commands in the proxy protocol for establishing HTTP or TCP connections to given addresses and ports – however only if the addresses and ports are included in a specified whitelist:

- 1. Permitted Server Address
- 1. Permitted Server Port
- 2. Permitted Server Address
- 2. Permitted Server Port
- etc.

Fields for defining the client side program to start

A Menu Action can start a program on the client PC, and can also generate a parameter file with

data for the program. Both are optional. The parameter file is automatically deleted after a specified life time has expired, or when the program exits, whichever comes first:

- Command
- Working directory
- Parameter file name
- Parameter file lifetime (0 and -1 have special meaning – see details in the Customization Reference)
- Parameter file template

Field for defining what to do when ending a menu action

When a menu action ends, either because of “Close with process” (see below) or because the G/On Client exits, a command may be executed:

- Close Command

This can in some cases be used to perform some kind of clean-up.

Fields for defining ties between port forwards and client side programs

The following fields are used for specifying which programs can use a port forward, and what to do if the port forward closes, or the program exits:

- Close with process (closes the port forwards, if the program exits)
- Kill process on close (kills the program, if one of the port forwards closes; currently this can only happen if the G/On client closes)
- Lock to process PID (Only the launched command may use the port forward)
- - or its sub processes (Also allow subprocesses of the launched command to use the port forward - requires lock_to_process_pid)
- Lock to process name (Only processes with this name are allowed to use the port forward - conflicts with lock_to_process_pid)

Note: Some programs behave in a way which makes it impossible to use the above fields. For instance, some applications hand over control to another process immediately after they have been started, and then exits. This is the case for commonly used browsers. It is also the case for the Microsoft Terminal Services Client (mstsc), when used on 64 bit versions of Windows Vista and Windows 7.

Fields for specifying User convenience properties by means of Tags

The following fields are used for controlling the appearance of the Menu Action in the menu, and whether the Menu Action should be automatically started, when first appearing in the menu:

- Dialog Tags
- Dialog Tag generators

Any Tag can be put on a Menu Action by simply adding the Tag to the field: Dialog Tags.

Thereafter, it will be available a basis for defining menus and sub-menus. See page 48 and 80.

For instance, you can put a tag “ERP” on some menu actions – this will enable that the menu actions can be presented in a separate sub-menu.

You can use the special tag: **_MENU_ROOT** for enabling that a menu action be shown in the root of the user's menu.

In addition, the following Tags have special meaning:

SHOW

Must be present for the Menu Action to be shown. Is automatically added to all Menu Actions that have (or get) the Tag ENABLED. Can also be added manually, in order to show Menu Actions that are not enabled.

ENABLED

Is automatically added to all Menu Actions that have (or get) both the Tags: CLIENTOK and SERVEROK.

CLIENTOK

Must be present for the Menu Action to get the Tag ENABLED. Can be generated dynamically by a Tag generator of the form:

```
client_ok::IfPlatformIs("...")
```

SERVEROK

Must be present for the Menu Action to get the Tag ENABLED. In future versions, there may be Tag generators for automatically generating this, e.g. based on the availability of a server etc.

AUTOLAUNCH

If specified, the Menu Action will be automatically started, when it becomes available in a User's menu – provided that it also has the Tag ENABLED.

AUTOLAUNCH_FIRST_START

If specified, the Menu Action will be automatically started, when it becomes available in a User's menu – provided that it also has the Tag ENABLED, and provided that this is this first time the client is running after it was installed.

Tag generators

There are currently two types of Tag generators:

```
client_ok::IfPlatformIs("os")
```

where os is either win, mac, linux, iOS, iOS-iPhone, iOS-iPad, or iOS-iPod.

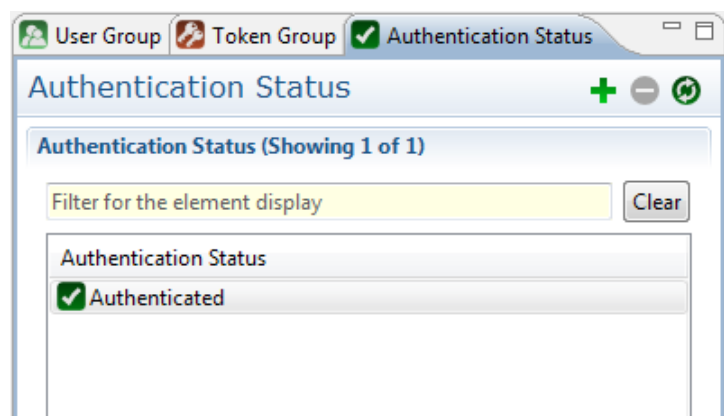
If this is specified, and the G/On Client is running on a computer with the given OS, the Tag CLIENTOK is automatically generated.

```
package::CheckPackage("name", "os")
```

If this is specified, the Tag: PACKAGE_CHECK is automatically generated. Moreover, if the G/On Client is running in an environment where the given package is installed, in the highest version available from the server, the Tag: PACKAGE_INSTALLED is also automatically generated. If the package is not installed in the highest version available, the Tag: Package("name", "os") is generated. Currently, this is used for providing feedback, when a User chooses a Menu Action, where the necessary package has not been installed.

Element: Authentication Status

The Authentication Status list has a built-in Element called 'Authenticated'. This can be used to indicate when proper authentication has been achieved. For a simple set-up use this as the only indicator for proper authentication.



New

It is possible to add new Authentication Status Elements. See page 36 for general information on how to create new Elements.

Edit

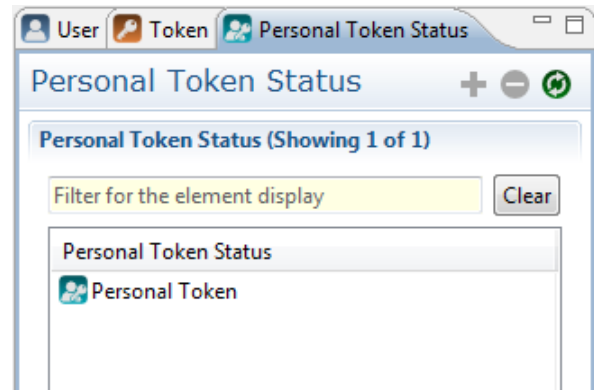
It is possible to edit the name of the Authentication Status Elements. See page 36 for information on how to start editing Elements.

Delete

It is possible to delete Authentication Status Elements that are not built-in or in use in any Rules. See page 37 for general information on how to delete Elements.

Element: Personal Token Status

The Personal Token Status Element is used as an indicator of when a User can be said to be using a Personal Token. In the Personal Token Status list is a built in Element named Personal Token. This Element is used as a result Element in the Personal Token Assignment Rules. The Token Assignment Rules register individual Tokens to be authentication factors for individual Users. So if it follows from evaluation of the Rules, that Personal Token Status is Personal Token, we know that a known User with a Personal Token is using the system..



The Personal Token Status Element can also be viewed as a dynamic Token Group, which depends on the current User: for a given User, the Token Group, Personal Token, contains the Personal Token(s) of that User. Therefore, in the Authentication Policy perspective, the Token Group list also contains “Personal Token” as a special Token Group.

New

It is *not* possible to add new Personal Token Status Elements.

Edit

The built in Personal Token Status Element called Personal Token can not be edited.

Delete

The built in Personal Token Status Element can not be deleted.

Element: Management Role

A Management Role Element represents a role that a G/On Manager may have, and the (limited) set of privileges that are needed for carrying out the management tasks of that role. By using Management Roles it is possible to define exactly which access a user or user group should have to information and functions in the Management Server. The assignment of roles to users and groups is made in the perspective: Management Role Assignment.

There are two built-in Management Roles: “Administrator” and “Token Manager”. The Administrator role has access to all functionality, whereas the Token Manager role is a sample role dedicated to the management of tokens and their assignment to users.

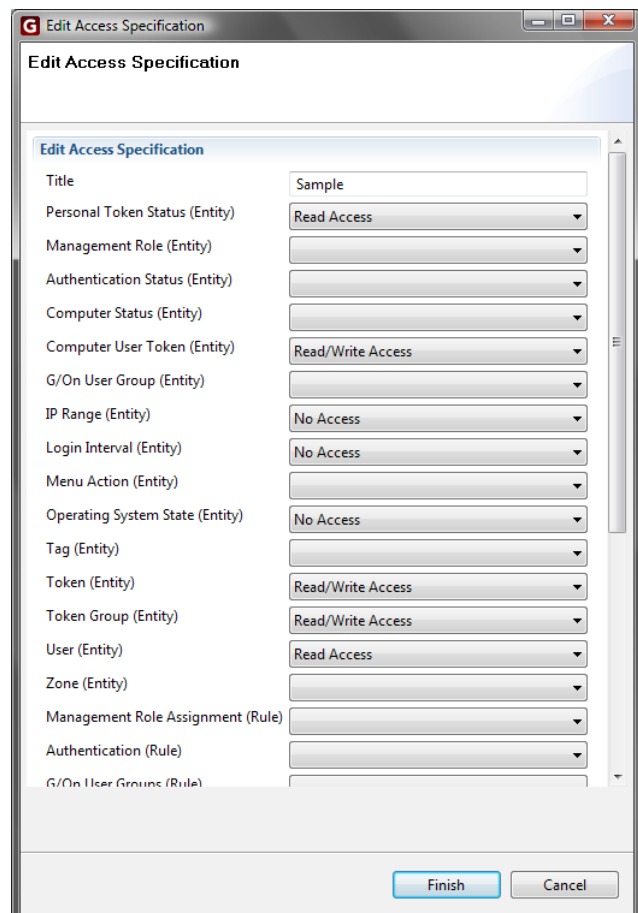
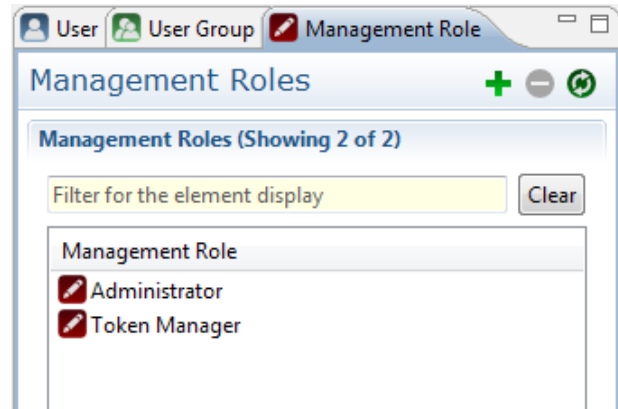
Each role specifies access rights to elements, rules, reports and special functionality.

For each Entity type (Users, Tokens, Menu Actions, etc). it is possible to give Read or Read/Write access.

For each Rule type (Personal Token Assignment, Action Authorization Policy, etc.) it is possible to give Read or Read/Write access.

For each Report it is possible to give Read access.

A special “Gateway server configuration” access right can be given in order to enable the Gateway Servers perspective. This also controls whether a user can install a new license.



New

Create a new Management Role

Properties

View/Edit a Management Role. Note that the built-in roles cannot be edited.

Delete

Delete a Management Role. Note that the built-in roles cannot be deleted.

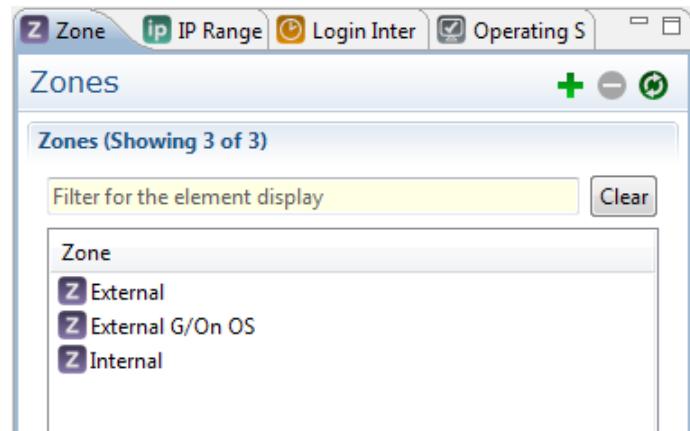
Create Copy

Create a new Management Role based on an existing role. This means that the new role will be pre-filled with the access rights from the existing role. Note that for built-in roles, the copy will have “Built-in” set when the window is opened. That will change once the rule has been saved.

Element: Zone

The Zone elements each represent a set of circumstances which may be detected at the start of a user session. Zone detection rules are defined in the “Zone Management” perspective. A set of allowed Zones can be specified for a Menu Action, and this has the consequence that the Menu Action can only be launched if at least one of the allowed Zones has been detected for the current user session. If

none of the allowed zones have been detected, the Menu Action will still appear in the client menu, but it will be marked with a special “disabled” icon and launching it will result in an error message specifying the reason why it cannot be launched.



New

It is possible to add new Zone Elements. See page 36 for general information on how to create new Elements. To create a Zone a unique name must be specified. It is also possible to specify a User Message. If the User Message is filled in, then this message will be shown to users trying to launch a Menu Action, which has been disabled by this zone. If the User Message is left blank the user message will be “Zone restriction <zone name> not met”

Properties

It is possible to edit Zone Elements. See page 36 for information on how to start editing Elements.

Delete

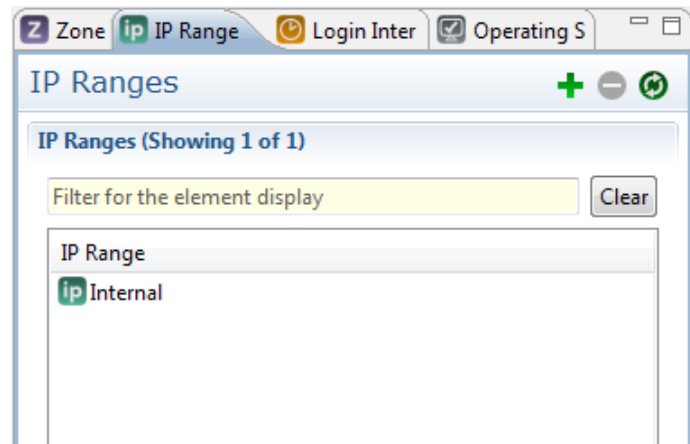
It is possible to delete Zone Elements that are not used in any Rules. See page 37 for general information on how to delete Elements.

Element: IP Range

An IP Range Element represents a range of IP addresses, as they may be observed by the G/On Gateway Server when a G/On Client connects. The range may concern either the client side or the server side address.

Both IPv4 and IPv6 addresses can be specified.

An IP address range may consist of just a single IP address.



New

It is possible to add new IP Ranges. See page 36 for general information on how to create new Elements.

Each IP Range has the following settings.

- **Name** is the IP Range name. This is the name which is used as referral in Zone Detection Rule specifications.
- **Description** is a description which can be used for reference.
- **Client IP Ranges** is a list of IP ranges for the client side of the connection between the G/On Client and G/On Gateway Server. IP Ranges should be separated by a comma, e.g. "127.0.0.1 – 127.0.0.2, 192.168.0.0/24.

Note: If the client is behind a NAT router, these ranges relate to the externally observable address of the router.

Exception: In G/On 5.5.0, the actual client side IP is always reported as: 127.0.0.1, if the client has connected by use of HTTP encapsulation.

- **Server IP Ranges** is a list of IP ranges for the network interfaces on the server, specified in the same way as Client addresses. This is only relevant when the G/On Gateway Server(s) have more than one network interface.

Properties

It is possible to edit IP Ranges. See page 36 for more information on how to start editing Elements.

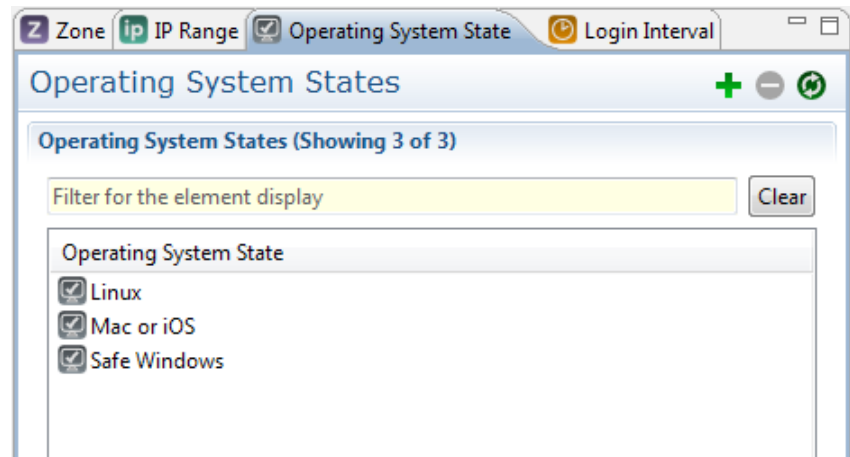
Delete

It is possible to delete IP Ranges, which are not used in any rules. See page 37 for general information on how to delete Elements.

Element: Operating System State

An Operating System State element represents observed properties of the state of the operating system, where the G/On Client is running.

The properties may concern the client Operating System type, version and security status. Currently version and security settings check is available for Windows only.



New

It is possible to add new Operating System States. See page 36 for general information on how to create new Elements.

Each Operating System State has the following settings.

- **Name:** This is the name which is used as referral in Zone Detection Rule specifications.
- **Description** is a description which can be used for reference.
- **Linux Allowed:** Connection from linux is allowed
- **Windows Allowed:** Connection from Windows is allowed
- **G/On OS Allowed:** Connection from G/On OS is allowed
- **Mac Allowed:** Connection from a Mac is allowed
- **iOS Allowed:** Connection from iPhone or iPad is allowed

If Windows OS is allowed it is also possible to specify version and security checks on a separate page. Push the “Next” button in the wizard to reveal this page. The following options are available:

Click “Check Version” if version check should be in effect. The following versions are available:

- **Windows XP**
- **Windows Vista**
- **Windows 7**

and for each version a service pack requirement can be added. In the drop-down list it is possible

to choose the service packs available at the release of the current G/On version. In order to specify a service pack which has been released since the G/On release, the version number can be entered in the field manually. Check Giritech support for further details on what should be entered for a given service pack.

Click “Check Security” if security should be checked. The following checks are available:

- **Firewall**
- **Anti virus**
- **Windows Auto Update**
- **All important updates installed**

All except the last check are gathered from Windows Security Center. The possible values are “Poor” and “Good” relating to the values returned by Windows Security Center. Please check [“http://msdn.microsoft.com/en-us/library/bb432506%28v=vs.85%29.aspx”](http://msdn.microsoft.com/en-us/library/bb432506%28v=vs.85%29.aspx) for further details on the precise definition of the used API. Testing shows that the “Poor” value is always met, so setting the check for an option to be “Poor” is in practice the same as checking whether Windows Security Center returns a valid value. The value “Good” means the following:

- **Firewall:** a firewall is installed and enabled
- **Anti virus:** Anti virus is installed and up-to-date.
- **Windows Auto Update:** Windows is set to download and install updates automatically. Any other setting will result in the value “Poor”

Note that on Windows XP there is no Windows Security Center API. Therefore G/On uses WMI and registry lookup on Windows XP, in order to get the information necessary to behave in a similar manner as on the newer operating systems.

The “All important updates installed” check performs a call to Windows Update to check if there are any updates available, which are marked as required. Put in another way it checks for updates which will be automatically installed if Windows Auto Update is set to install automatically. Note that this check can be time consuming (normally in the range of 5-15 seconds, but it can be more), which means that Menu Actions depending on this check may be disabled at start-up and then enabled later when the check has passed.

Properties

It is possible to edit Operating System States. See page 36 for more information on how to start editing Elements.

Delete

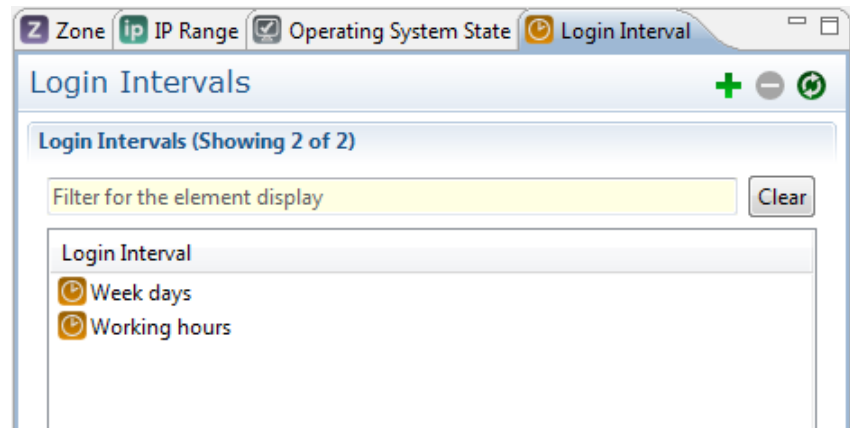
It is possible to delete Operating System States, which are not used in any rules. See page 37 for general information on how to delete Elements.

Element: Login Interval

Login Interval Elements are definitions of allowed login intervals on a weekly basis. It is possible to specify login hours on each day of the week. The following limitations apply:

- The login time is the server time. Time zone is the server time zone.
- The check is only made at login time. So if a user session expands outside any given login interval it has no consequences.

Note: For individual users, it is also possible to specify a (possibly open-ended) date/time interval where the user is considered valid. See page 41 for further details.



New

It is possible to add new Login Intervals. See page 36 for general information on how to create new Elements.

The following general settings are available.

- **Name:** This is the name which is used as referral in Zone Detection Rule specifications.
- **Description** is a description which can be used for reference.

Furthermore there are settings for each week day:

- **All:** Access all day, i.e. from 0:00 to 24:00
- **None:** No access that day
- **Time::** A time interval in which access is allowed.

Note that it is allowed for the time interval to pass midnight, e.g. go from 9 PM to 9 AM. Also note that this means that it is possible to enter contradictory information. If, for example, access on Monday is set to be from 9 PM to 9 AM and access on Tuesday is disabled, then access on Tuesday morning is both allowed and forbidden. In such a case the interpretation will be that the positive access definition wins, i.e. logging in Tuesday morning before 9 AM is allowed.

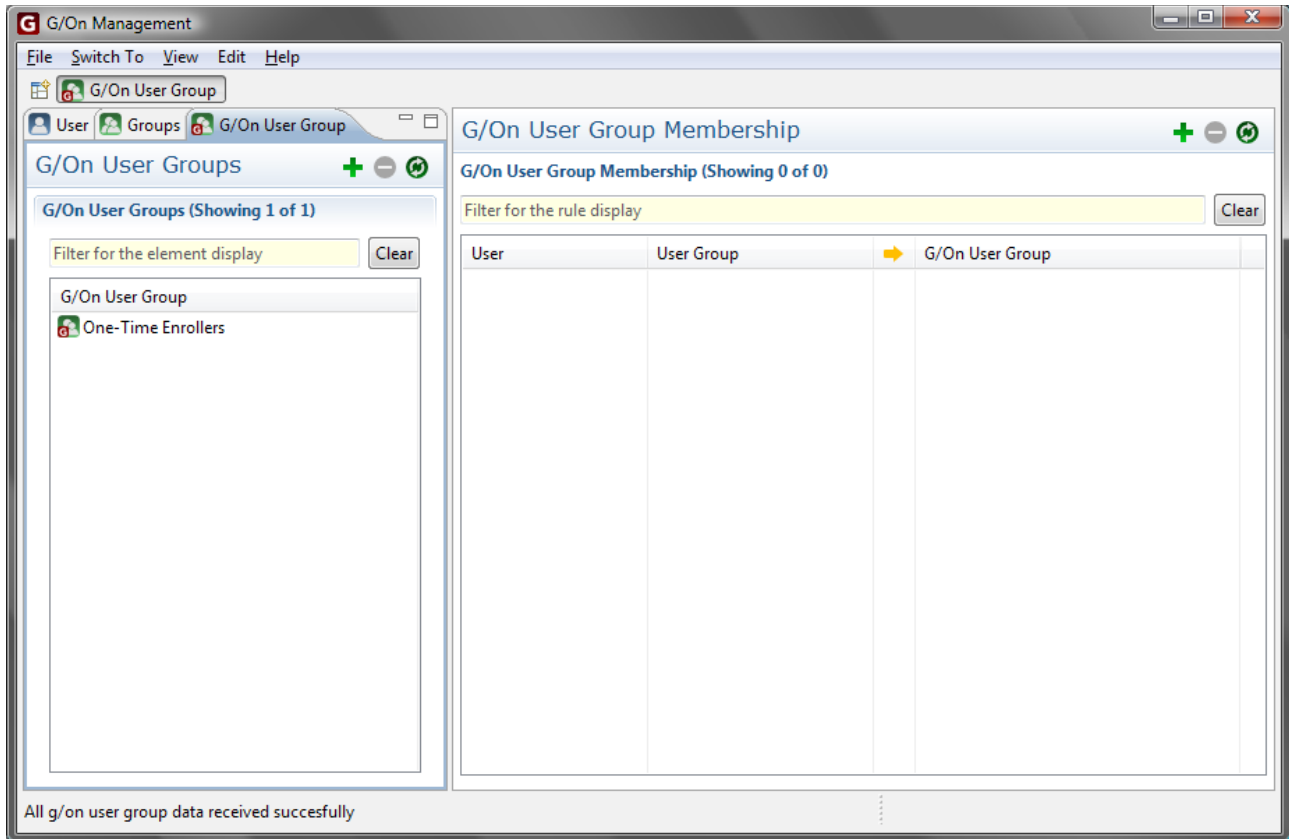
Properties

It is possible to edit Login Intervals. See page 36 for more information on how to start editing Elements.

Delete

It is possible to delete Login Intervals, which are not used in any rules. See page 37 for general information on how to delete Elements.

Perspective: G/On User Group



The G/On User Group perspective is used for adding Users that are retrieved from a central User Directory to a G/On User Group that can be created for that purpose. It is also possible to add entire groups from a User Directory to G/On User Groups. G/On User Groups adds a convenient way off creating local groups for use with the G/On services.

Note: There is a built-in G/On User Group: One-Time Enrollers, which has special properties:

1. By default, there is an Action Authorization Rule which authorizes members of One-Time Enrollers to do Field Enrollment
2. When a User has succeeded in doing a field enrollment, this User is automatically removed from the group One-Time Enrollers. However, for this to work, Users have to be added *individually* to One-Time Enrollers, i.e., there must be one Rule in the G/On user group perspective for each User. The automatic removal will not work, if the User is *indirectly* a member of One-Time Enrollers, through a Rule that adds an entire group from a User Directory to One-Time Enrollers.
3. To make this easier, right-click the User Group and choose Add members to One-Time-Enrollers. This will add all the Users in the User Directory group to the One-Time Enrollers

group, as *individual members*.

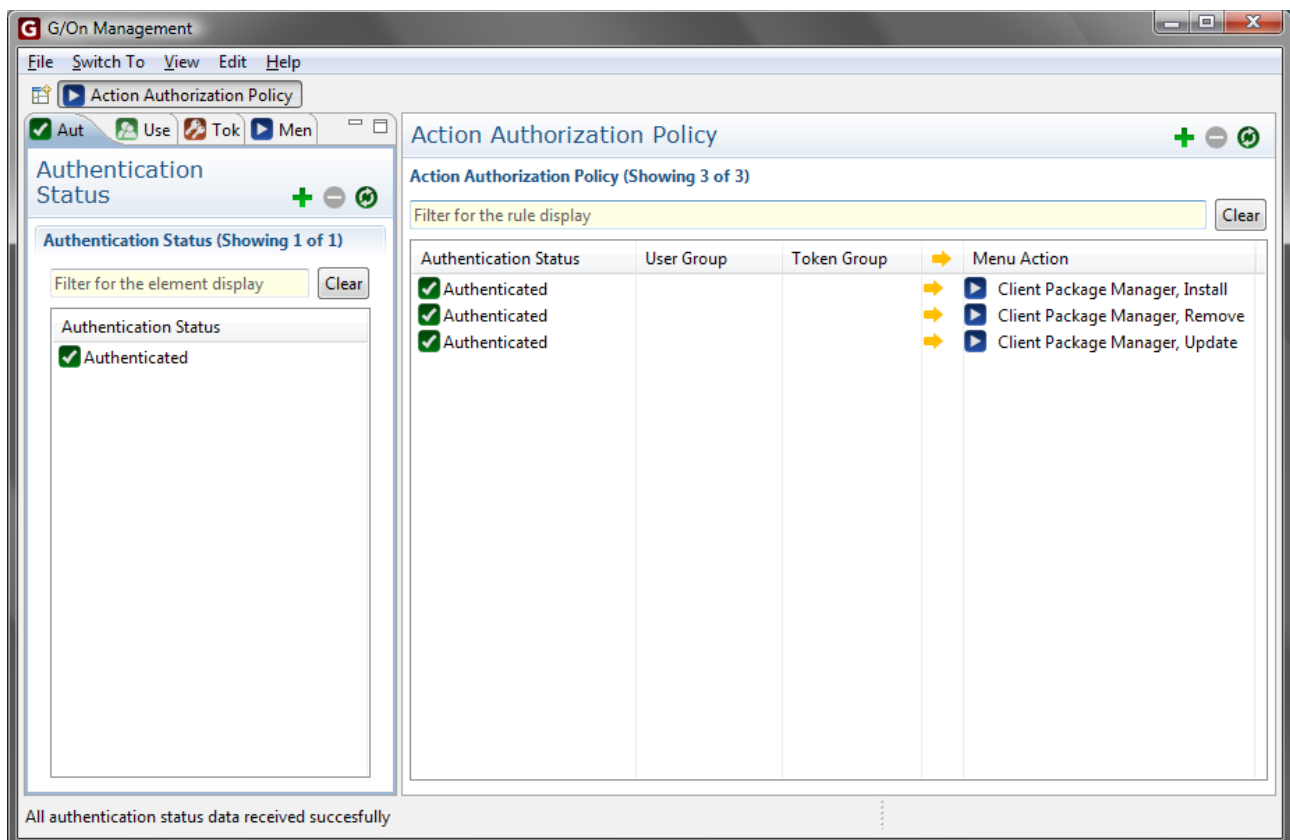
Rule Elements

The User and User Group Elements come from a central User Directory. The G/On User Groups are the result Elements of the Rules in this perspective. This means that for each Rule any User or User Group on the left hand side means they are placed in the G/On User Group at the right hand side.

Usage

Rules can be added, edited and deleted. See page 38 and onwards for general information on how to do this. For general information on how to add Elements to a new Rule or to an existing Rule, see page 39.

Perspective: Action Authorization Policy



The Action Authorization Policy perspective is used for creating Rules specifying when to authorize the use of specific Menu Actions. The authorization may depend on the Authentication Status and the User Group membership of the current User. It may also depend on the presence of a Token in

a given Token Group.

Rule Elements

The Authentication Status Elements are possible results of User Authentication Policy Rules, that have been set up in the User Authentication Policy perspective.

The User Group Elements come from one of the User Directories that G/On has been configured to work with - or the G/On User Groups defined in the G/On User Group Management perspective. The Groups can be used for giving different groups of Users access to different Menu Actions. For example, management-users may need access to different applications than guest-users.

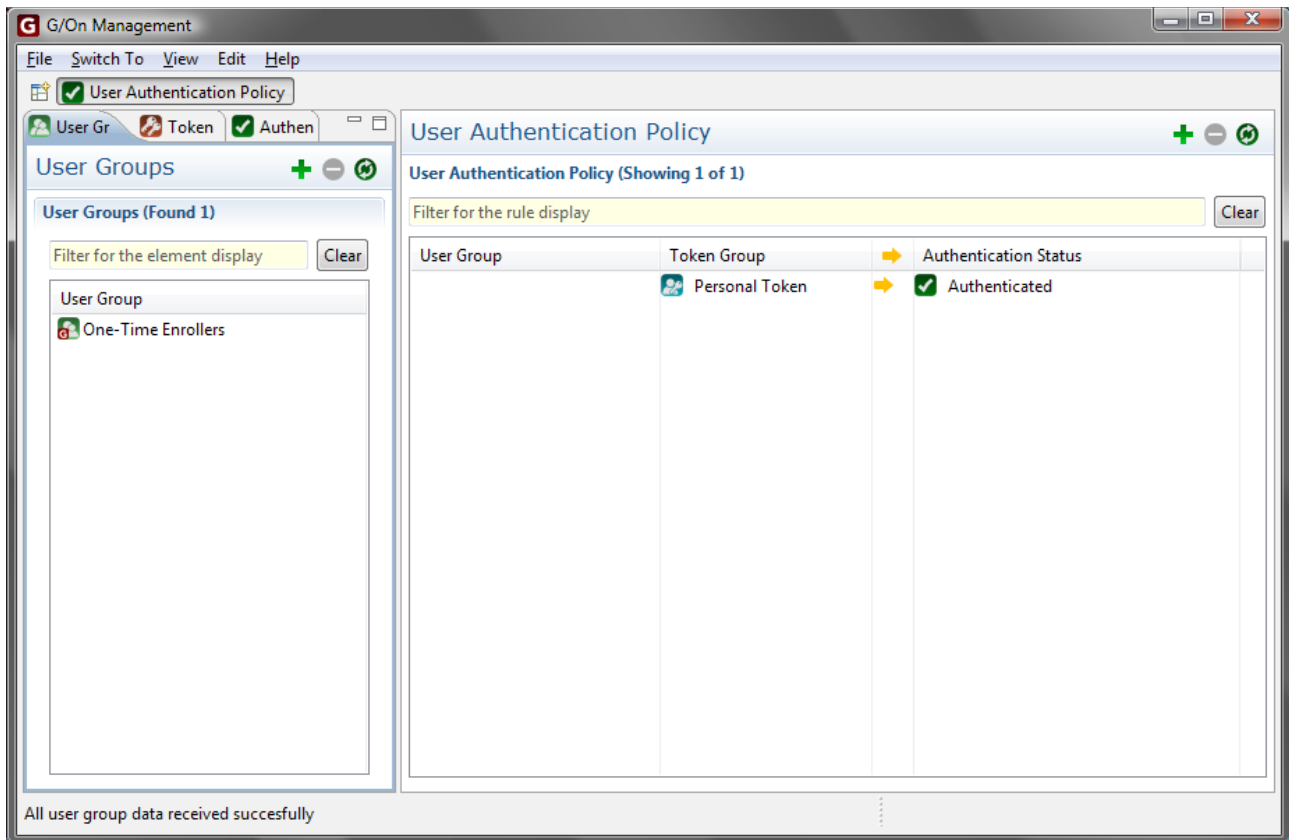
The Token Group Elements are defined in the Token Group Management perspective. In Authorization Rules, Token Groups can be useful as a way of identifying groups of PCs which must be used, in order for certain actions to be authorized. For instance, the PCs could each have a MicroSmart Token or a smart card inserted in a build-in reader or they could each have a Computer User Token installed, which could then be used to identify them.

Menu Actions are the result Element in the Rules in this perspective. This means that if all the specified parameters on the left hand side of a Rule are true, then the User will get access to the Menu Action on the right hand side of the Rule.

Usage

Rules can be added, edited and deleted. See page 38 and onwards for general information on how to do this. For general information on how to add Elements to a new Rule or to an existing Rule, see page 39.

Perspective: User Authentication Policy



The User Authentication Policy perspective is used for creating Rules specifying when to conclude that the current User has a given Authentication Status. The conclusion may depend on the User Group membership of the current User. It may also depend on the presence of a Token in a given Token Group.

For example a Rule can say that all Users are properly authenticated if they are using a Personal Token. The use of a Personal Token implies that the User has also logged in. So this Rule says that a User who is logged in and is using his/her Personal Token is authenticated. Another Rule could say that any User in the “Production” User Group is authenticated if using any Token from the “Production” Token Group.

Rule Elements

User Group Elements are either from a User Directory or are G/On User Groups created in the G/On User Group Management perspective. These Elements can be used to give different groups of Users different means of authentication.

Token Group Elements are either the built in Element Personal Token or any Token Group created in the Token Group Management perspective. The Personal Token group is dynamic, in the sense

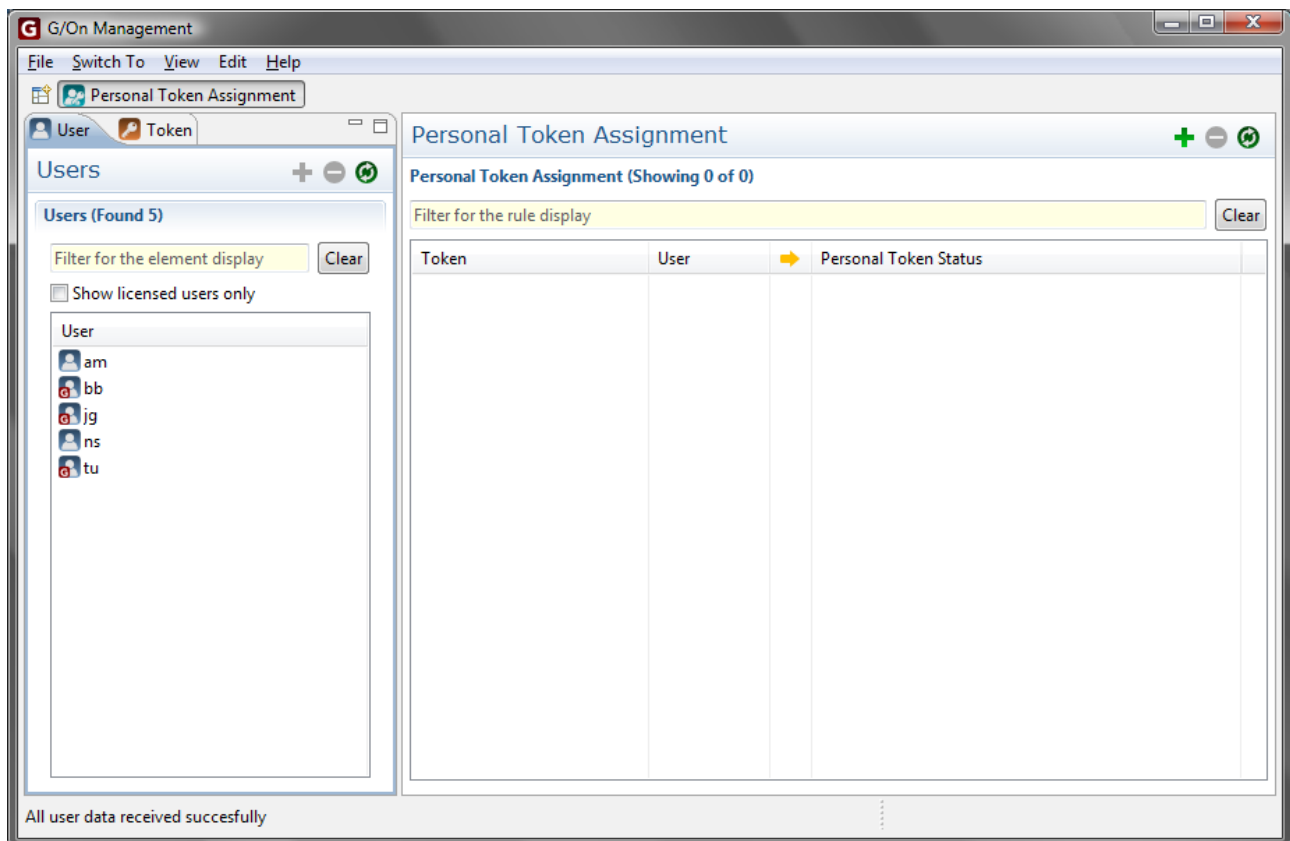
that it depends on the current User.

Authentication Status Elements are the result Elements in the Rules in this perspective. If all the specified Elements on the left hand side of a Rule are true, then the Authentication Status Element on the right hand side is also considered to be true. It is possible to create new Authentication Status Elements to get a more fine grained notion of authentication. However, in most cases this would be an unnecessary complication, because it would result in a combinatorial explosion of the number of Action Authorization Rules.

Usage

Rules can be added, edited and deleted. See page 38 and onwards for general information on how to do this. For general information on how to add Elements to a new Rule or to an existing Rule, see page 39.

Perspective: Personal Token Assignment



The Personal Token Assignment perspective is used for creating Rules that link a Token to a unique User so that it becomes the User's Personal Token.

Rule Elements

Token Elements are created by enrolling each individual Token. After enrollment, the Token may be entrusted with a specific User, for use as a second authentication factor. For the Rule engine to know which User has which Token, a Personal Token assignment Rule has to be created. A Token cannot be the Personal Token of more than one User (then it would not be personal).

User Elements come from a User Directory.

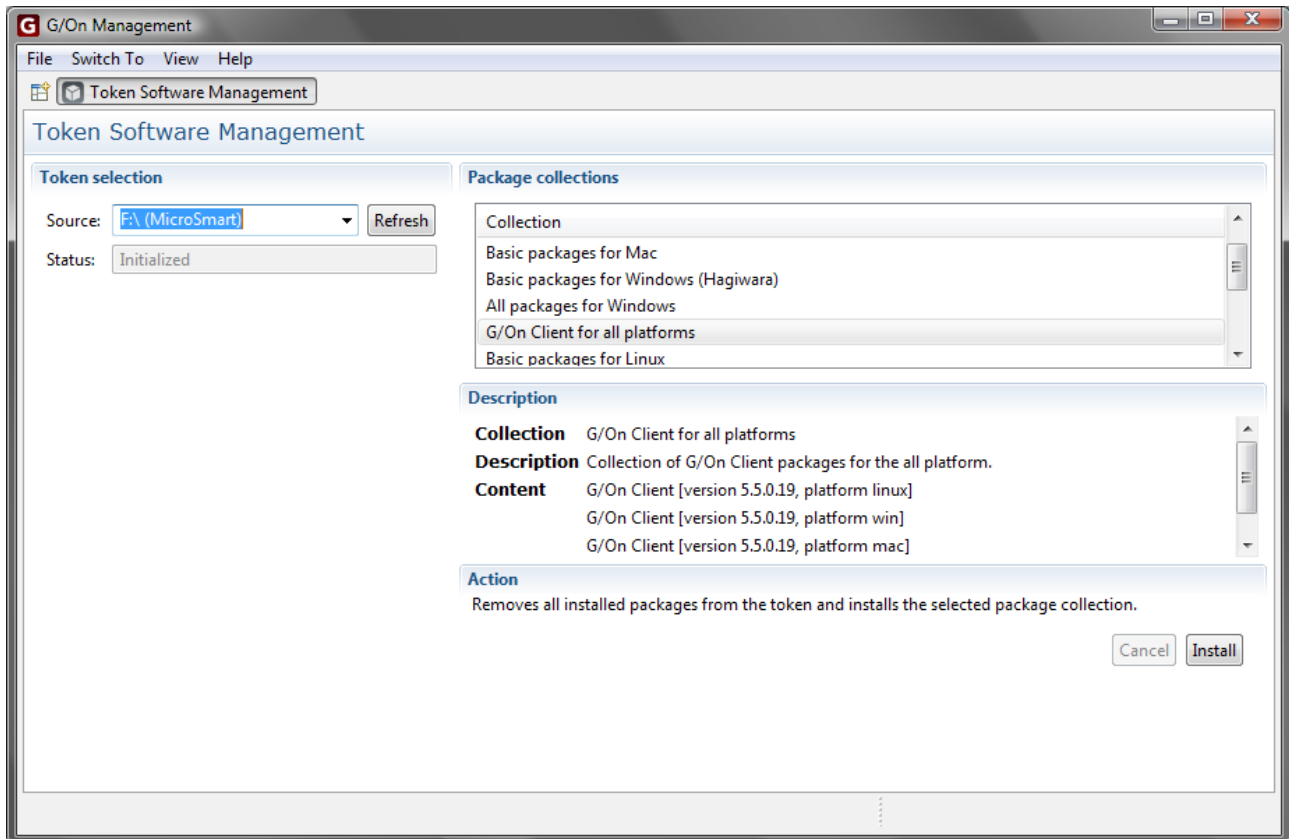
Personal Token Status Elements are the result Element of the Rules in this perspective. It is *not* possible to create other Personal Token Status Elements.

It is not possible to have empty fields in these kind of Rules.

Usage

Rules can be added, edited and deleted. See page 38 and onwards for general information on how to do this. For general information on how to add Elements to a new Rule or to an existing Rule, see page 39.

Perspective: Token Software Management

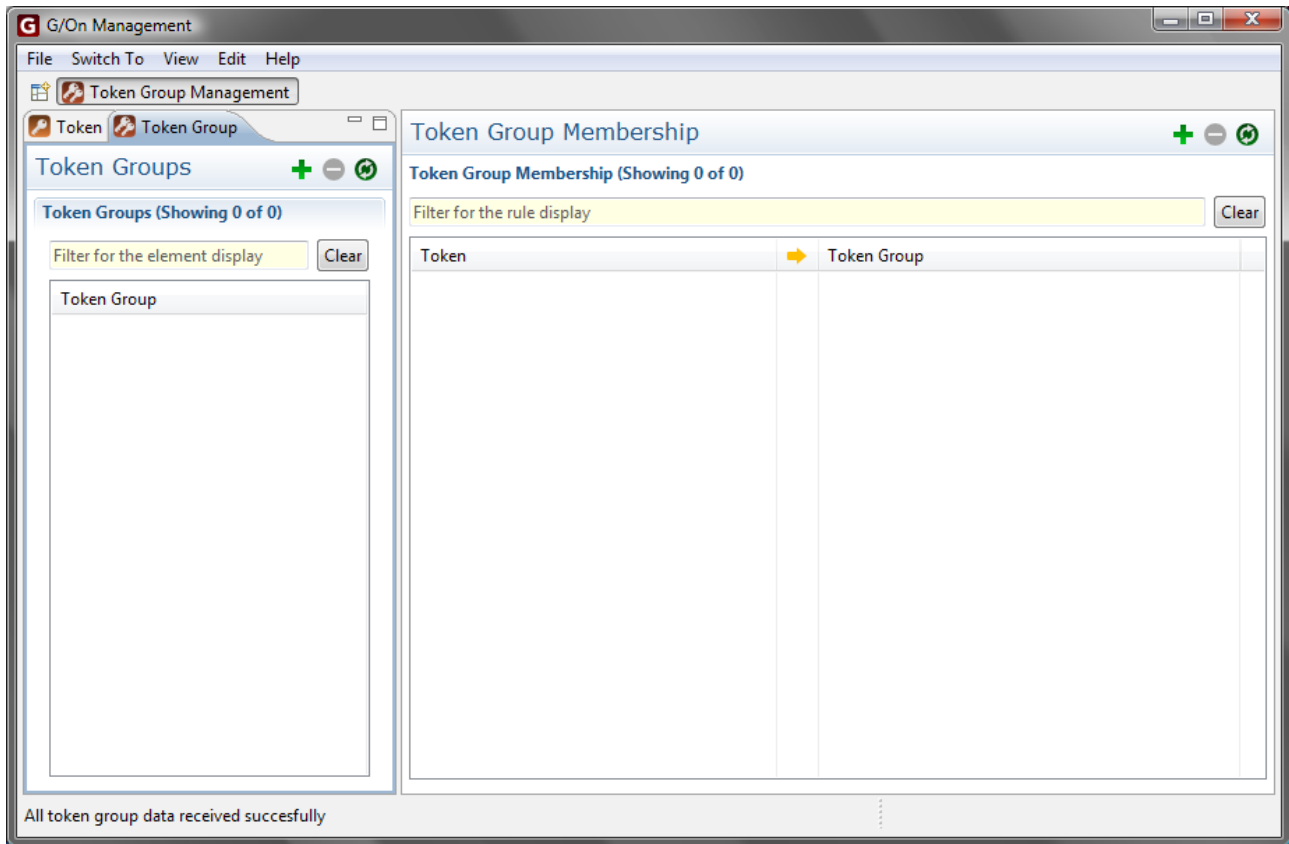


The Token Software Management perspective is used for installing software package collections to Tokens before handing them to the Users. The Tokens in the source list are the Tokens inserted in the USB ports of the local workstation.

Note: Installing a package collection will overwrite the contents of the Token: Existing files will not be deleted but may be replaced. Files unrelated to G/On will be untouched.

Also note: After the installation of a package collection, it will appear to G/On client as if only the packages in the given package collection are on the Token – even if there are in fact files on the Token, from packages that were installed earlier.

Perspective: Token Group Management



The Token Group Management perspective is used for adding Tokens to Token Groups. A newly created Token Group is empty and the way to add Tokens to that Token Group is by creating a Rule for each Token saying that it is a part of a particular Token Group.

Token Groups can be useful for identifying specific sets of PCs, assuming that they each have a fixed Token in/on them. They can also be used for identifying, e.g., a set of guest Tokens that are not personal.

Rule Elements

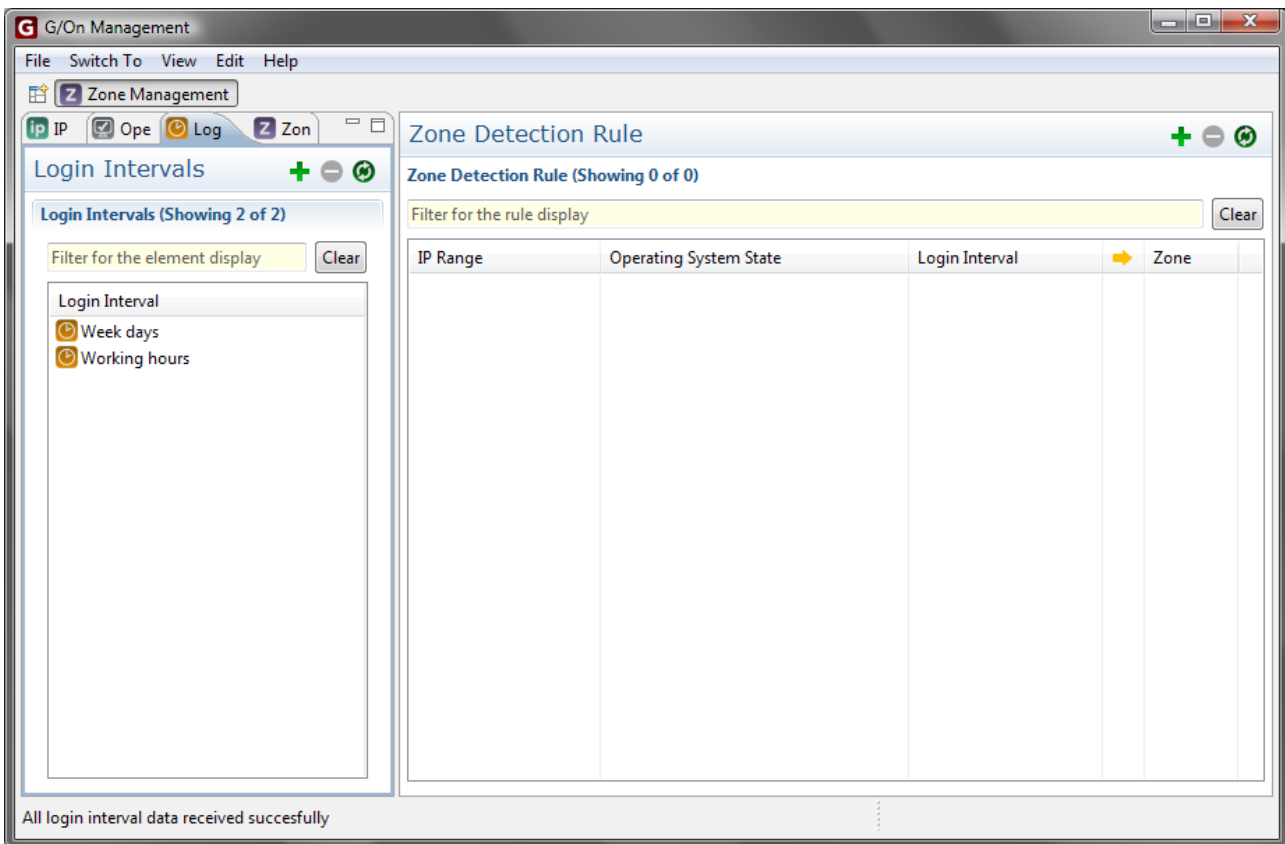
Tokens are created by enrolling each individual Token into the G/On server. Once a Token has been enrolled, it can be added to an existing Token Group. Token Group Elements are the result Elements of the Rules in this perspective. Each Rule says that a given Token is a member of a given Token Group.

Usage

Rules can be added, edited and deleted. See page 38 and onwards for general information on how to do this. For general information on how to add Elements to a new Rule or to an existing Rule, see page 39.

Perspective: Zone Management

The Zone Management perspective is used for creating Zones and Zone detection rules.



Zone detection rules is defined using IP ranges, Operating System States and Login Intervals. A Zone can be attached to a Menu Action, thereby creating the restriction that the Menu Action can only be launched if the circumstances of the Zone are fulfilled.

Zone restrictions is a more soft type of authorization, where access to the menu is not denied, but access to launching Zone restricted actions may be denied. The user is therefore able to see that under the right circumstances the action would be available.

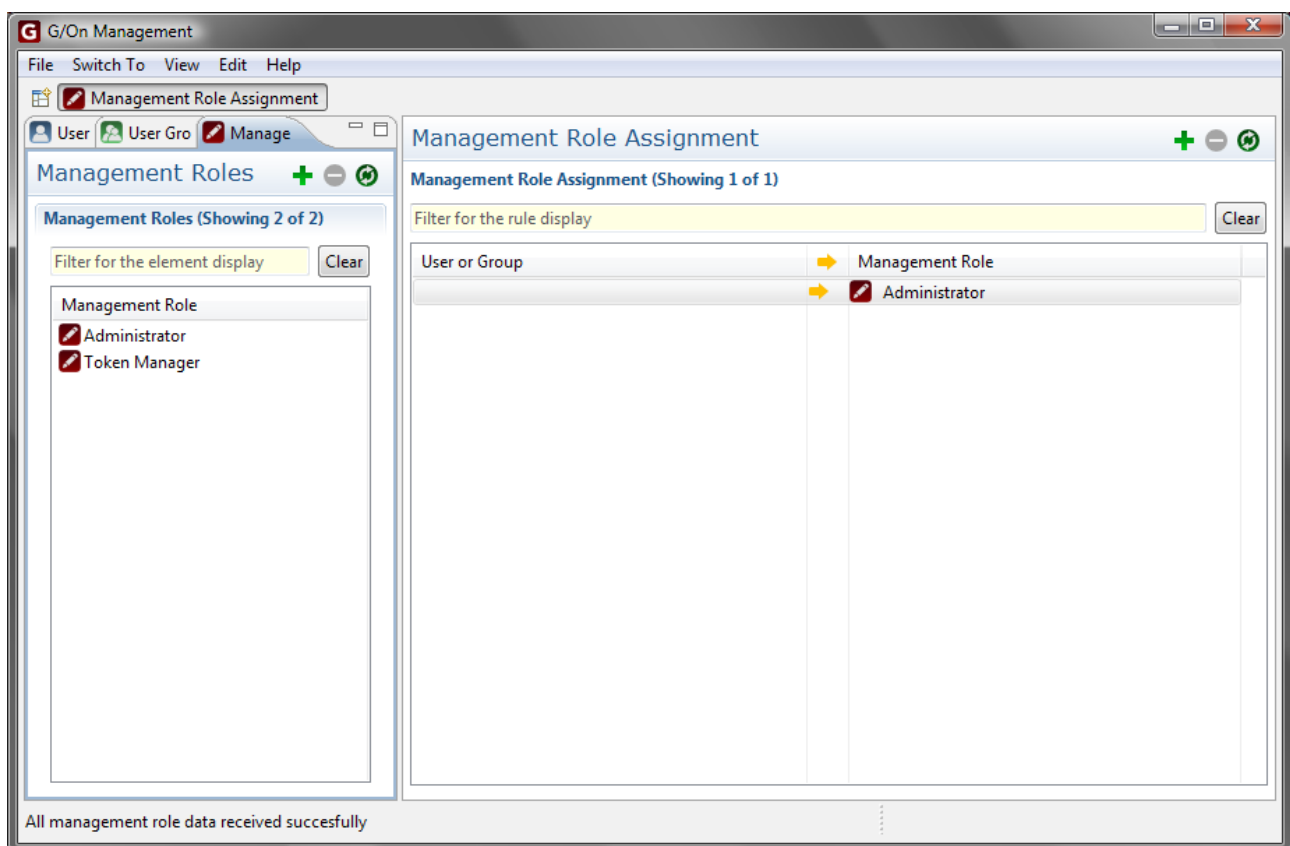
Rule Elements

Rule elements are IP Ranges (page 62), Operating System State (page 64) and Login Interval (page 67).

Usage

Rules can be added, edited and deleted. See page 38 and onwards for general information on how to do this. For general information on how to add Elements to a new Rule or to an existing Rule, see page 39.

Perspective: Management Role Assignment



The Management Role Assignment perspective is used for creating management Access Roles and assigning them to users. Each Management Role defines a set of access rights for management functionality. Using the Management Role Management it is possible to delegate responsibility for different tasks in G/On Management and only giving people access to the functionality they actually need for the task. A sample “Token Manager” role is provided, which provides access to the perspectives and views necessary to manage tokens, i.e. enrollment, assignment and software deployment of tokens.

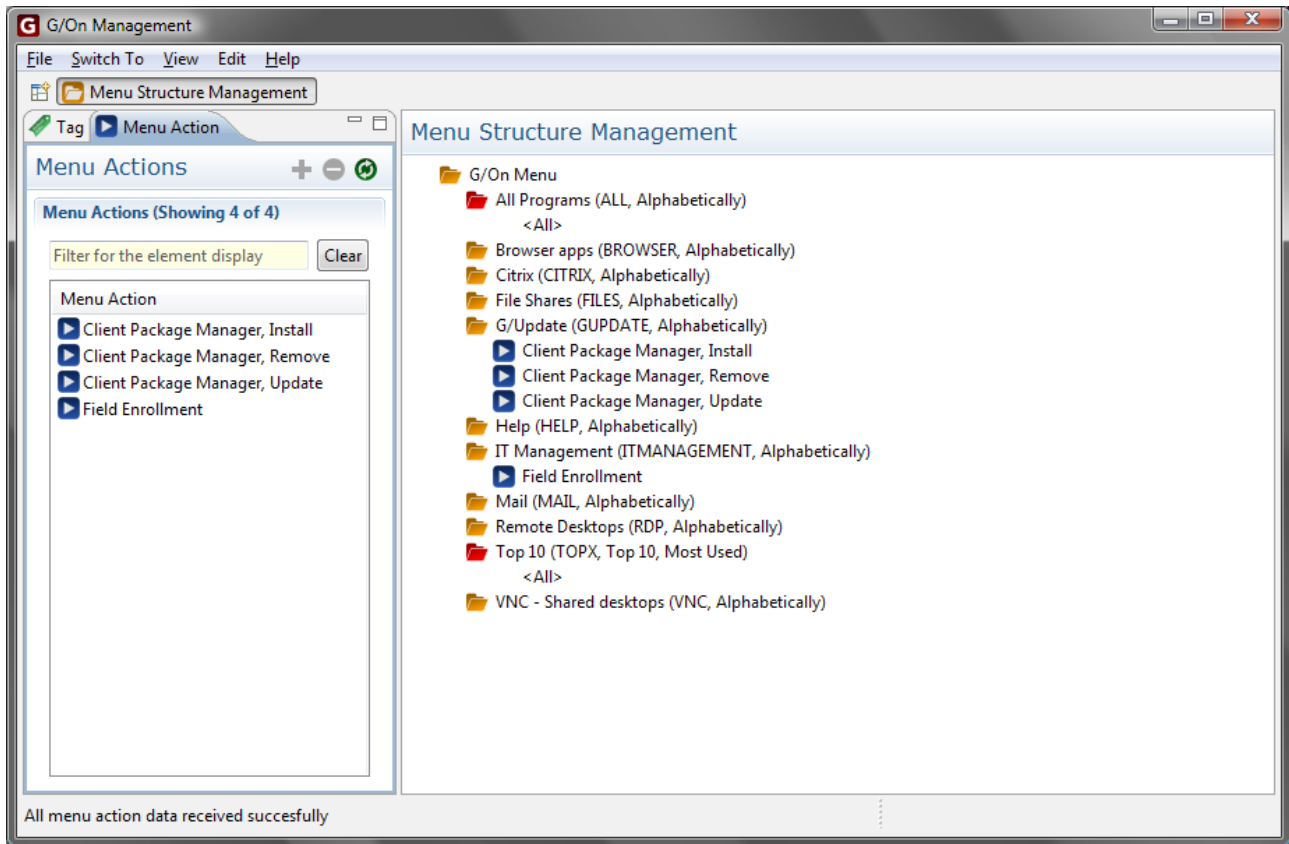
Rule Elements

The role members can be individual users or user groups, including G/On User Groups. The users, which can log in to the G/On Management are drawn from the same user directories which are defined for access via G/On Client. A Role condition can also be left blank, meaning that anyone has that role. The initial setup is that everyone has the Administrator Role, thus it is not necessary to login. If a user is member of more than one role, the user will get the union of access from both roles, i.e. if access to e.g. Users is read-only in one role and read/write in the other then the user will have read/write access to Users.

Usage

Rules can be added, edited and deleted. Note however that as a special precaution there must always be at least one active rule defining access to the Administrator Role. Thus it is not possible to delete or change the result of a rule giving access to the Administrator Role if this rule is the only one doing so. The reason for this restriction is to minimize the risk for accidentally locking yourself out of editing Management Roles. See page 38 and onwards for general information on how to edit and delete rules.

Perspective: Menu Structure Management



The Menu Structure Management perspective is used for structuring the content of end-user's menus. Each Menu Action has a number of Tags associated to it. For example, a Tag named "BROWSER" may be associated with the Menu Action "Mercurial intranet site" that launches an intranet site using Windows Explorer. If this Tag is added to the menu structure, the Tag acts like a folder containing any Menu Action that is associated with the Tag. Because a Menu Action can have any number of Tags associated with it, the Menu Action can appear several places in the menu structure.

Elements

Tags can be created by entering them in the Tags field of a Menu Action. They can also be created by the New operation in the Tag list. Tags have a number of settings. One of the settings decide whether the Tag generates a menu folder that can be used as a container for Menu Actions. See the Tag Elements description for more information.

Usage

Tags are added to the folder structure by dragging and dropping. Tags can be dragged onto other Tags in the menu structure in order to create sub-menus.

Menu Actions can be created and edited in the Action Authorization Policy perspective. Do not try to add Menu Actions to a specific location in the menu structure. Instead, you should add Tags to the individual menu actions in the Action Authorization perspective and then let the Tag system handle locations.

To create a new folder in the menu structure start by creating a new Tag. The new Tag has a name and that name should be added to the Tag list in the Menu Actions that should go into the folder that the Tag generates. Notice that Tags can be added to Menu Actions in the Action Authorization Policy perspective.

Note: Menu Actions cannot be created in the Element list in this perspective. Use the Action Authorization perspective when you want to create Menu Actions.

Perspective: Gateway Servers

The screenshot displays the G/On Management Client interface with two main panels: Gateway Servers and Gateway Sessions.

Gateway Servers Panel:

- Includes a menu bar with File, Switch To, View, and Help.
- Has a toolbar with a Refresh icon and a Gateway Servers button.
- Contains a checkbox for "Automatic update" which is checked.
- Displays a table with the following data:

Server name	IP	Port	Sessions	Status
GatewayServer 1...	127.0.0.1	13945	0	Running

Gateway Sessions Panel:

- Includes a menu bar with File, Switch To, View, and Help.
- Has a toolbar with a Refresh icon and a Gateway Sessions button.
- Contains a checkbox for "Automatic update" which is checked.
- Includes a "Show:" dropdown menu set to "All" and a "User Search:" input field.
- Displays "Showing 0 of 0" above an empty table with the following headers:

User login	User name	Server name	Client IP	Sess

A status bar at the bottom of the window reads: "All Gateway Session data received successfully".

In the Gateway Servers perspective it is possible to monitor and control Gateway servers and the users sessions running on them. The perspective consists of two parts: Left is a view of Gateway Servers and their status and right is a view of Gateway Sessions. These views are described below.

Gateway Servers

This view contains a list of running gateway servers and their status. The following fields are shown for each server:

- **Server name** is the title of the gateway server defined in the *gon_server_gateway_local.ini* file or “Not defined” if no title has been defined.
- **IP** is the IP address of the gateway server host.
- **Port** is the port on which the Gateway server listens.
- **Sessions** is the current number of user sessions.
- **Status** is the server status, which would normally be “Running”. It can be changed by choosing server actions, see below for details

Above the list is a check box titled “Automatic update”. If this box is checked then the gateway server list will be automatically updated each 30 seconds.

In the “Gateway Servers” header there is a number of buttons which can manipulate the servers and the view:

- **Stop** will send a signal to the chosen gateway to stop immediately. Any user sessions on the server in question will be disconnected.
- **Restart** will send a signal to the chosen gateway to restart immediately. Any user sessions on the server in question will be disconnected.
- **Stop when no users** will send a signal to the chosen gateway to stop as soon all current user sessions has stopped. This will also block the chosen gateway server from receiving any new client connections.
- **Restart when no users** will send a signal to the chosen gateway to restart as soon all current user sessions has stopped. This will also block the chosen gateway server from receiving any new client connections.
- **Refresh** will refresh the gateway servers view.

The first four actions will result in the gateway server Status field changing to “Stopping”, “Restarting”, “Stop when ready” and “Restart when ready” respectively. The actions are also

available in the right-click menu.

Gateway Sessions

This view contains a list of gateway (user) sessions.. The following fields are shown for each session:

- **User login** is the (full) user login of the user logged in to this session or blank if no user has logged in yet.
- **User name** is the registered name of the user logged in to this session or blank if no user has logged in yet.
- **Server name** is the name of the Gateway server the session belongs to (see description under Gateway Servers above).
- **Client IP** is the IP address of the G/On client
- **Session start** is the date and time the session was initiated.

Above the list are som options:

- **Automatic update:** If checked the session list will be automatically updated each 30 seconds.
- **Show:** Choose to show all sessions or only those belonging to the selected Gateway Server in the Gateway Server list.
- **User search:** Find sessions for which the user name or login contains the content of the search field.

In the Gateway Sessions header the following actions are available:

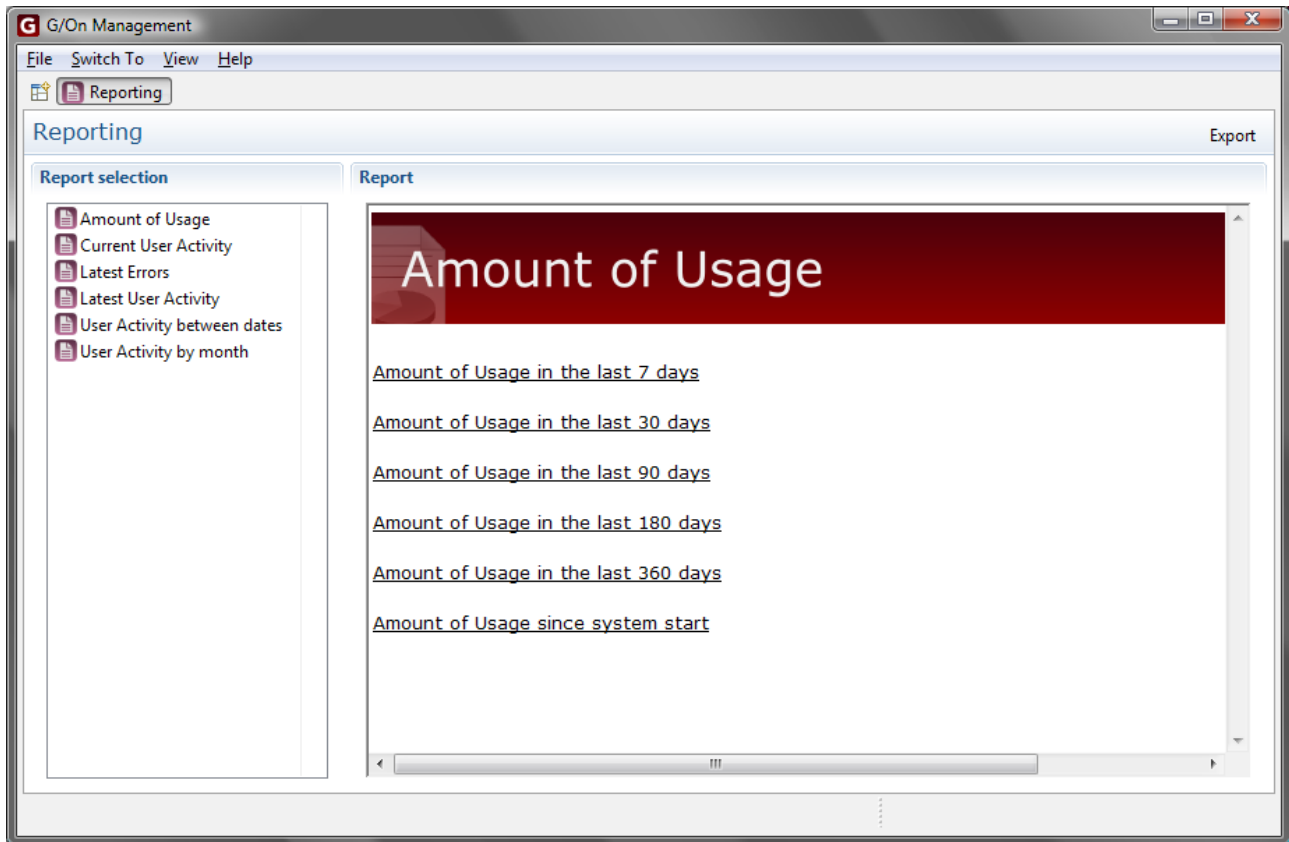
- **Stop Session** will send a signal to stop the selected session immediately.
- **Recalculate Menu** will cause the client menu to be recalculated. This functionality is described below.
- **Refresh** will refresh the list
- **Cancel Updating** will stop fetching more sessions from server (only available if there are more than 50 sessions).

These actions are also available in the right-click menu.

Menu Recalculation

The menu recalculation feature makes it possible to force a recalculation of the menu for a running G/On session. It is mainly a tool for an administrator to be able to test authorization and menu action setup, without having to restart a G/On client and log in constantly. Therefore the recalculation is not a full recalculation in the respect that all the basic authentication factors like user login, token identity, computer properties, IP address, etc. are assumed to be the same. It is the possible new authorization based on these premises, which is calculated. For example, if a new rule is added giving access to a new Menu Action for a user, then a recalculation should result in that the new Menu Action is part of the users menu. However if a new token has been enrolled and assigned to a user, a recalculation will not give further access, since the token identity was not established at login time.

Perspective: Reporting



The report perspective can be used for retrieving information about the usage of the system. Double click on any of the reports listed in the report selection list too see the selected report in the report viewer on the right hand side.

Reports

A number of reports are available to the G/On management client user:

- **Amount of usage** provides a list of users and their complete online time. Choose between 7, 30, 90, 180, 360 days, or usage since the system was started.
- **Current user activity** shows the users currently online. Click on details to get more information on a single user session.
- **Latest Errors** provided a list (and details) of errors the last 3 days. This can be useful if someone can't log in and don't know why.
- **Latest user activity** shows a list of users and their last online session, including current sessions. Click on details to get more information on a single user session.

- **User Activity between dates** provides a list of user sessions between (and including) two dates. Click on details to get more information on a single user session.
- **User Activity by month** is the same as between dates, except this quickly provides the list for a full month. Click on details to get more information on a single user session.

Export reports

It is possible to export any of the reports to a document formatted as a PDF file. At the top right of the window is a button the says 'export'. Click this button to start exporting the currently visible document.

Best Practices

Tokens

What is the best practice for handing out Tokens?

Users should not share Tokens. For the most secure setup, Tokens should be personal, so a User has to present a Personal Token, in order to prove his or her identity – not just any token, that could have been used by a number of other people. This practice also provides grounds for better usage reporting.

That being said, it is possible to create a Token that should be used by a group of Users. This feature should primarily be for “guest tokens” or Tokens handed out to a group of Users with less strict requirements for secure, individual authentication, such as a group of Users working for a contractor. Create a Token Group and call it, for example, 'guest tokens' and add the Token to this Token Group. Then create an Authentication Policy stating that Users from the Active Directory group 'guests' can be authenticated using the Tokens from the 'guest tokens' Token Group.

Elements

What is the best practice for using the built in Personal Token Status Element called Personal Token?

The Personal Token defines a special Token Group that evaluates to true when a specific Token and a specific User is active in using the G/On client. In most cases it is practical to link each Token to a specific User, so it becomes a Personal Token for this User. In the Authentication Policy perspective a Rule can be created, saying that when a Personal Token Element is validated, then User is properly authenticated.

The reason for this seemingly extra step is to allow for the creation of Authentication Policy Rules using Token Groups which contain specific Tokens. This will allow for a slightly looser authentication concept combining Token pools and User Groups from a central User and Groups Directory.

What is the best practice for using the built in Authentication Status Element called Authenticated?

Use the built in Authentication Status Element called Authenticated for labeling when a User can be considered to be properly authenticated. Do not introduce different level of authentication strength unless it is really needed. Set up a policy for when Users are properly authenticated and use this

notion in Authorization Policies. The Authorization Policies are the proper place for distinguishing which Menu Actions different groups of Users should be allowed to use. Introducing different levels of authentication in many cases adds unnecessary complexity to the Rule engine and in particular to the Authorization Policy Rules.

FAQ

General

How is it enforced that traffic from a client-side application hits the right server on the right ports?

The explanation is quite simple: The menu items shown to the User contain nothing but a name. So when a User chooses a Menu Action, the name is sent to the server, which decides what application server addresses and ports to connect to.

Going into more details, this is an overview of G/On Server behavior with focus on how the server controls access from the G/On Client to application servers:

1. The G/On client connects to the G/On server and authenticates the server and they establish an encrypted communication channel
2. At this point, the server accepts nothing from the client, except info regarding authentication and authorization factors: username, password, responses to challenges to authenticate Tokens, etc.
3. Based on the authentication and authorization information received from the client, the server computes which actions the user is authorized to do, and sends out a menu to the client. Each menu item is simply a title and the name of the associated action – there is no information sent out to the client about the meaning of the Menu Actions.
4. At this point the server now also accepts information about the names of Menu Actions, that the User has chosen – but only the ones that were authorized by the server itself.
5. The User chooses a Menu Action, and the client sends the name of that Menu Action to the server.
6. Based on the Menu Action name, the server looks up the definition of the Menu Action, and establishes a port forward as specified in the definition. The port forward is established by setting up a component on the G/On server and one on the G/On client, with a communication channel between them. The port forward component on the server will – when receiving traffic from the client part – open a connection to the application server address and port, as specified in the Menu Action definition. So the client has no control over which addresses and ports that the server connects to.

How to run the G/On Management Client remotely?

In many cases it is not convenient to run the G/On Management client on the server machine. For

instance, it is often not practical to enroll tokens, by physically having to plug them into a USB port on the server machine. If you wish to run the G/On Management client remotely, through a G/On connection, do the following:

1. Initially, you need to enroll *at least one* Token and install the G/On Windows client on it, using the server machine. If you cannot access a USB port on the server machine, you can create a “soft Token” on the hard disk and then copy it to a location where you can put it on an ordinary USB flash drive. See the section Initialization of Soft Tokens on HD in the Advanced Setup Topics section of the G/On Setup and Configuration Reference. Alternatively, make a field installation of a Computer User Token, as described in the separate document: G/On Field Deployment.
2. On the Management server machine use G/On Management and create a menu item for starting the Management Client and authorize it for the Users who are going to use it remotely.
3. Start the G/On client on the Token that you created in step 1. In the G/On menu, select G/Update – Install, and install the G/On Management and Management service packages.
4. In the G/On menu, choose the menu item that you created in step 2.

Will the end-user client automatically reconnect?

It is not currently possible to have the client reconnect if the network temporarily fails. Security concerns makes this a non trivial task. So for now the User will have to restart the client to reconnect.

Rules

Why can't I make Rules for individual Users in the policy perspectives?

The policy perspectives are meant as general policies that should not be changed often. The day to day management of the G/On server should be about assigning new Tokens to Users and handing them out. The Users should in most cases fall into a User Group from the central User Directory that already has the proper authentications.

Elements

I see a tab called Rule Elements?

Click the tab to refresh the tabs header.

Menu Actions

How to specify multiple port forwards

Use the template called (default), when creating the Menu Action: First enter information in the Server Host field, then save, and open again, and enter information in the Server Host 1 field, etc.

Tokens

How to enroll Tokens without having to plug them into the server machine?

The G/On Management client can be run remotely through a G/On connection. See the FAQ entry above, on How to run the G/On Management Client remotely. So you can run it on a PC of your choice with a USB port where you can plug in the Tokens to be enrolled.

There are no Tokens listed in the Source drop down list?

Tokens should be listed in the source drop down. Make certain that you have inserted a proper Token into the local machine. Click Refresh to refresh the drop down list.

Note: however, that Tokens from which a G/On client has been started (and is still running) will not be listed in the drop down list.

The Enroll button is inactive (grey)?

If a Token is selected in the drop down list, and the Enroll button is inactive (grey), this indicates that the Token is already enrolled in the system. It must be deleted from the Token Element list, before it can be re-enrolled.

Can a Token be used by a group of Users?

Yes it can but it is not the best practice. Best practice is to have each Token identifying a specific user. However it is possible to create a Token Group and add a token to that group. In the User Authentication Policy, link the created Token Group and a User Group to say that those Users can use the Tokens from the newly created Token Group and then be properly authenticated.

Users

Can I create G/On Users?

It is not currently possible to create local individual Users in the G/On management. It is possible to

create local G/On User Groups. This means that it is possible to collect groups and individuals from the User Directory into one User Group and use that to simplify the policies and other Rules. This should also be a help if it is not possible or viable for the G/On administrator to create new groups in the central User Directory.

Can I force an update of the user menu?

Yes, it is possible to update a user menu from G/On Management. See page 84 for further details.

When will a login window appear to the Users?

If there is a Rule where the system needs to know who the user is then the login window will appear. For example if a Rule says that a User is properly authenticated if he is using a Personal Token. Then the system needs to know who the User is and which Token he is using.

Messages

I get the error: 'Unable to connect to server'?

If you get a message saying: "Unable to connect to server", when starting the G/On Management client, try adjusting the preferences (by choosing View > Preferences).

I get the error: 'This element cannot be deleted'?

Certain Element lists have predefined and built in Elements intended for use in best practice based set-up. These Elements can not be deleted.

I get the error: 'Unknown element type [type]'?

This can happen if the perspective has Element lists that hold types that should not be added to the current Add/Edit Rule area. The perspective has probably not been properly refreshed. Choose View > Reset Window. This should reset all the perspectives views and lists.

I get the error: 'Token has already been used in another rule'?

Tokens should identify one User only. If you want a Token to identify a different User, first delete the Rule where the Token is currently used.

An end-user gets a notification: 'Insufficient authorization' in the G/On client?

If it turns out that the User is not authorized to do any Menu Action, this notification will be displayed, and the G/On client will terminate. This may happen for different reasons, depending on how the authentication and authorization policies have been set up. These are two scenarios, often seen:

1. The User has not presented the right User Name/Password/Token, so he is not properly authenticated, and all Authorization Policies require proper authentication.
2. The administrator has forgotten to set up some Action Authorization Policies. So this User is not authorized to do any Menu Action, even when he is properly authenticated.

Menus

What are menus in G/On 5?

The menu which is shown when you log into G/On is created from the *Tags*, which are attached to the Menu Actions you have access to. In other words, when you log into G/On, the system first calculates which Menu Actions you have access to, then it builds the menu based on the Tags attached to these Menu Actions. The Tags are both used for sorting out or disabling irrelevant actions (e.g. a Linux based application when running Windows) and as building blocks for the menu tree. On each Tag you can choose whether it should be shown as a menu or not. If the Tag is set to be shown as a menu and you have access to one or more Menu Actions with this Tag attached, then it will be shown in the menu tree containing the Menu Actions in question. The Tag can also have parent Tags, in which case it will be shown as a sub menu in all the menu folders created from these parent Tags.

What does the Menu Structure Management view show?

The Menu Structure Management view shows the menu tree derived from all the Menu Actions which have been created in the system. In other words it shows you how the menu would look for a User who has access to, and is able to run all Menu Actions in the system. So for most Users the menu will not look like the one you see in Menu Structure Management. But it would however always be a *subset* of the menu tree shown, in that the User's menu would consist of the Menu Actions available to the User at the same position(s) in the menu tree.

Why can I not create a new Menu Action?

You can create Menu Actions and specify who are allowed to use them in the Action Authorization

Policy perspective. This automatically puts the Menu Actions into the menus. So you do not need to go into Menu Structure Management perspective. You only need to open the Menu Structure Management perspective, if you have some special requirements regarding the structure of the menu (new sub-menus, or sub-sub menus etc.). So the Menu Structure Management perspective, is only for the final “polishing” of how the menu will appear. The main part of the work: deciding who get access to which Menu Actions, you do in the Action Authorization Policy perspective. In order to promote this new work flow, the creation of Menu Actions has been disabled in the Menu Structure Management perspective.

How do I create a personal menu?

The short answer: You don't! Or more precisely: You don't have to – the menu is already personal.

In G/On 5, the personal menu is created in two steps. First, access to an application is given in the Authorization Policy view, in which you can give access to a certain application for a specific group of authenticated Users. As a special case a User Group could consist of just one person, but we recommend not to name the group after the person, because we find that almost all authorization is given to people because of their *role* rather than because of who they are. As an example, most G/On administrators like to have a personal menu, in which they can add administrative applications. In G/On 5 this would be solved by creating a G/On Administrator group either in the User Directory (e.g. AD) or in G/On Management. Then access to the applications can be given to this User Group (along with the “Authenticated” condition). But if you really want a personal User Group, it is possible to create it in the G/On User Group view.

How should I manage menus in G/On 5

One of the objectives of using tags for creating menus is to diminish the amount of work regarding menu management. Consider the task of adding a new application to G/On: In G/On 3 you would create the application string, and then you would manually enter the new application into the menus of the users or groups who should be able to access it. In G/On 5 you will normally create the application (Menu Action) using a template. Then you have to decide who should have access to it (and under what circumstances) and create corresponding rules. And in most cases that's it - you don't have to explicitly add the application to the menu, it will already be there underneath the menu folders derived from its tags. You can of course change this, either by changing the tags directly on the Menu Action element or by using Menu Structure Management.

Predefined Menu Action Templates

The G/On system comes with a number of predefined Menu Action templates. Most of these are self explanatory, but a few need a specific setup of the server, or have other prerequisites. These are documented in the following.

FileZilla Templates

FileZilla is an FTP client, which connects to an FTP server using the FTP protocol. It can operate in two modes: Active or Passive.

The FileZilla client starts by "telling" the FTP server whether to use active or passive mode.

In active mode the server will try to initiate connections back to the client, based on information that the client has supplied about its address and a port. Opening connections from the server to the client is not supported by G/On, so this mode cannot be used with G/On.

In passive mode, the server will dynamically select a new port for data traffic, and send information to the client that it should connect to this port. However, this is not possible if the G/On connection is simply one port forward from the FTP client to the FTP server: G/On does not "know" that it has to open a new port forward, for the data traffic. The solution is to configure FileZilla so it uses the SOCKS protocol, and then set up a SOCKS server on the server side.

Setting up the Server Side

Install the GSOCKS service, e.g. on the same server as the one running the G/On Servers, and set up the gsocks.ini file, so it allows access to the desired FTP server.

Using the template to define menu actions

Notes regarding selected fields in the template:

Server Folder The folder on the FTP server, which is shown in the FileZilla client, when connected. Unfortunately, Filezilla uses a very special syntax for specifying the path to this folder. Assuming that the server is a windows or linux/unix server, the syntax is as follows:

```
1 0 /1 name1 /2 name2 ....
```

where /1 is the number of characters in name1

and name1 is the name of the top level folder

Likewise for /2 and name2, etc.

For example the Windows path: \Documents and Settings\abc should be written as follows:

```
1 0 22 Documents and Settings 3 abc
```

Notes regarding usage of menu actions generated from the template

Due to the fixed port being used for the SOCKS connection on the client side, it is not possible to have two instances of FileZilla running at the same time through G/On. When trying to launch the second instance is you get an error: "Unable to create port forward - address is in use".

Citrix Web Interface Templates

G/On supports a special type of menu actions for creating a http proxy connection between a browser on the client side and a Citrix Web server on the server side. The http proxy implements single sign-on the server side and launch of the Citrix client on the client side, without having to install anything on the client PC or browser.

Setting up the Server Side

We assume that Citrix Web Interface has been configured with:

- "Authentication Point" "At Web Interface"
- "Authentication Method" "Explicit"
- No "secure client access" (just "Direct" Access Method)
- No special "client-side proxy" (just "User's browser setting")
- "Access Method" Allow Users to access published resources using
- browser bookmarks

When configuring or debugging G/On Citrix and Web Interface integration then first try to log on to the web interface directly from a browser, preferably running on the Gateway server.

Verify that you get a login.aspx html page and verify that the User Name and Password you are using for testing G/On works. Note whether a domain must be specified or not.

Verify that the Web Interface application menu contains the expected applications. Check the URL and verify that the Citrix Web Server Address and Citrix Metaframe Path is configured correctly in G/On.

Internet Explorer sometimes hides important debug information, so if it shows an error page instead of the Web Interface through G/On then try to open the same URL in Firefox.

Using the template to define menu actions

There are two different classes of Citrix templates:

Arch Citrix Web Templates for making Citrix menu actions for launching the Citrix web interface in a browser. *Arch* is either Mac, Win or Linux

Arch Citrix Templates for making Citrix menu actions for launching a single application. *Arch* is either Mac, Win or Linux

Notes regarding selected fields in the *Arch* Citrix templates:

Citrix Application Path This is the part of the URL in the Citrix Web Interface, that comes after “?Nfuse_Application=” and is used for identifying an application. Note that Special characters must be url-encoded. For example: space must be replaced with “+” or “%20”. Be aware that browsers often encode and decode the url format differently for different uses. Example value in this field:

```
Citrix.MPS.App.G-MPS40.Word+2003+on+CTX01
```

Index

Index

1. Permitted Server Address.....	53	Delete.....	37
1. Permitted Server Port.....	53	editing.....	36
Action Authorization Policy perspective.....	33	filter.....	37
Action Authorization Policy Rules.....	26	list.....	36
Active Menu Action.....	30	new.....	36
Active Zones.....	30	Element type.....	23
Authenticated.....	24	Element:43-45, 47, 48, 50, 56, 58	
Authentication Policy Perspective.....		Element: Authentication Status.....	56
elements.....	72	Element: G/On User Group.....	44
Authentication Status.....	24	Element: IP Range.....	62
Authentication Status Element.....		Element: Login Interval.....	67
delete.....	57, 61	Element: Management Role.....	59
edit.....	57	Element: Operating System State.....	64
new.....	57, 61	Element: Personal Token Status.....	58
Authorization Policy Perspective.....		Element: Tag.....	48
elements.....	71	Element: Token.....	45
usage.....	71	Element: Token Group.....	47
Authorized Menu Actions	30	Element: User.....	41
AUTOLAUNCH.....	56	Element: User Group.....	43
AUTOLAUNCH_FIRST_START.....	56	Element: Zone.....	61
Citrix Web Interface.....	17	ENABLED	55
Citrix Web Interface Menu Actions.....	20	Field Enrollment.....	69
Citrix XML Interface.....	17	Field enrollment.....	44
Citrix XML Interface Menu Actions.....	21	G/O.....	18
Client Host.....	52, 53	G/On Decision Rule.....	23
Client Port.....	52, 53	G/On Internal.....	18
client_ok::IfPlatformIs.....	56	G/On User group.....	24
CLIENTOK.....	55	G/On User Group Elements.....	
Close Command.....	54	delete.....	44
Close with process.....	54	edit.....	44
Command.....	54	new.....	44
Computer User Token.....	46	G/On User Group Membership Rules.....	27
Conclusion.....	23	G/On User Group Perspective.....	
Dialog Tag generators.....	55	elements.....	70
Dialog Tags.....	55	usage.....	70
Element.....	23	G/On User Group perspective.....	33
add.....	36	G/Update Menu Actions.....	21
best practice.....	87	Gateway Servers perspective.....	33

Hagiwara.....	46	Personal Token Assignment Perspective.....	
Hagiwara H2/H3 USB Token.....	46	elements.....	74
HTTP and SOCKS Proxy.....	17	usage.....	74
HTTP and SOCKS Proxy Menu Actions.....	22	Personal Token Assignment perspective.....	33
Inactive Menu Action.....	30	Personal Token Assignment Rules.....	26
Introduction to perspectives.....	33	Personal Token Status.....	24
IP Range.....	24	Personal Token Status Elements.....	
Kill process on close.....	54	delete.....	58, 60
known User.....	24	edit.....	58
License information.....	32	new.....	58, 60
Lock to process name.....	54	Perspective.....	
Lock to process PID.....	54	included.....	33
Login dialogue.....	30	layout.....	34
Login Interval.....	25	most used.....	33
Management Role.....	25	reset.....	34
Management Role Assignment perspective.....	33	Perspective:	69, 70, 72, 73, 75, 76, 80, 85
Management Role Assignments Rules.....	27	Perspective: Action Authorization Policy.....	70
Management session.....	30	Perspective: G/On User Group.....	69
Menu Action.....	17, 24	Perspective: Gateway Servers.....	81
Menu Action Elements.....		Perspective: Management Role Assignment.....	78
delete.....	51	Perspective: Menu Structure Management.....	80
new.....	50	Perspective: Personal Token Assignment.....	73
Menu Actions.....	17	Perspective: Reporting.....	85
Menu Image ID.....	51	Perspective: Token Group Management.....	76
Menu Structure Management Perspective.....		Perspective: Token Software Management.....	75
elements.....	80	Perspective: User Authentication Policy.....	72
Menu Structure Management perspective.....	33	Perspective: Zone.....	77
Menu Title.....	51	Perspective: Zone Management.....	77
MicroSmart.....	46	Port Forward.....	17
MicroSmart Token.....	46	Port Forward Menu Actions.....	18
MicroSmart USB Token.....	46	Preferences.....	31
Mobile Token.....	46	Premise.....	23
Name.....	51	RDP Connection.....	17
One-Time Enrollers.....	44, 69	RDP Connection Menu Actions.....	22
Operating System State.....	25	Reporting perspective.....	33
package::CheckPackage.....	56	export.....	86
Parameter file template.....	54	reports.....	85
Parameter file lifetime.....	54	Rule.....	
Parameter file name.....	54	add elements to a.....	39
Personal Token.....	24	Delete.....	39

Edit.....	39	new.....	47
filter.....	39	Token Group Management Perspective.....	
list.....	38	elements.....	76, 78, 79
new.....	38	usage.....	77-79, 81
Rule Engine.....	30	Token Group Management perspective.....	33
Server Host.....	52, 53	Token Group Membership Rules.....	27
Server Port.....	52, 53	Token Software Management perspective.....	33
SERVEROK.....	55	Token types.....	46
SHOW.....	55	two factors.....	23
Smart Card Token.....	46	types of Elements.....	24
SoftToken.....	46	types of Rules.....	26
sub processes.....	54	User.....	24
Tag Elements.....		User Authentication Policy perspective.....	33
automatically add to all items.....	49	User Authentication Policy Rules.....	26
caption.....	48	User Elements.....	
delete.....	49, 63, 66, 68	delete.....	42
edit.....	48	edit.....	41
max items to show.....	49	new.....	41
name.....	48, 62, 64, 67	User Group.....	24
new.....	48, 62, 64	User Group Elements.....	
override item show.....	49	delete.....	43
parent tags.....	48	edit.....	43
show in menu.....	48	new.....	43
sort option.....	49	User session.....	30
Tag generators.....	56	Wake-on-LAN.....	18
Token.....	24, 45	Wake-on-LAN Menu Actions.....	21
Token Elements.....		Working directory.....	54
best practice.....	87	Zone.....	25
delete.....	46	Zone Detection Rules.....	27
New.....	45	Zone Management perspective.....	33
Token Group.....	24	_MENU_ROOT.....	55
Token Group Elements.....		#failover.....	52
delete.....	47	#random.....	52
edit.....	47	#timeout.....	53