

G/On Management Reference

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

G/On 5.4
Document revision 0.92
2010-05-20

G/OnTM 5

About this document

This document gives an in-depth description of the 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:

- G/On User Guide – Getting started – Fedora
- G/On User Guide – Getting started – Windows XP
- G/On User Guide – Getting started – Windows Vista
- G/On User Guide – Getting started – Windows 7
- G/On User Guide – Getting started – Mac
- G/On User Reference
- Getting started with G/On Setup and Configuration
- Getting started with G/On Management
- Getting started with Field Deployment
- Getting started with Secure Desktop
- G/On Setup and Configuration Reference
- G/On Management Reference
- G/On Customization Reference

© Giritech A/S, 2010
Spotorno Allé 12, 2.
2630 Taastrup
Denmark
Phone +45 70.277.262

Legal Notice

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

Contents

About this document.....	2
Contents.....	3
Basic Concepts.....	4
Menu Actions.....	4
Rules and Elements.....	8
The Management Client.....	12
Preferences.....	12
Introduction to Perspectives.....	13
Introduction to Element Panes.....	15
Introduction to Rule Views.....	17
Element Pane: Users.....	19
Element Pane: User Groups.....	20
Element Pane: G/On User Groups.....	20
Element Pane: Tokens.....	21
Element Pane: Token Groups.....	23
Element Pane: Tags.....	23
Element Pane: Menu Actions.....	25
Element Pane: Authentication Status.....	28
Element Pane: Personal Token Status.....	30
Perspective: G/On User Group.....	31
Perspective: Action Authorization Policy.....	32
Perspective: User Authentication Policy.....	34
Perspective: Personal Token Assignment.....	35
Perspective: Token Software Management.....	36
Perspective: Token Group Management.....	37
Perspective: Menu Structure Management.....	38
Perspective: Reporting.....	39
Best Practices.....	41
Tokens.....	41
Elements.....	41
FAQ.....	42
General.....	42
Rules.....	43
Elements.....	43
Menu Actions.....	44
Tokens.....	44
Users.....	45
Messages.....	45
Menus.....	46
Predefined Menu Action Templates.....	48
FileZilla Templates.....	48
Citrix Web Interface Templates.....	49
Index.....	51

Basic Concepts

The purpose of G/On is to securely connect known 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, and
3. Which groups of users can be authorized to use which applications.

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.

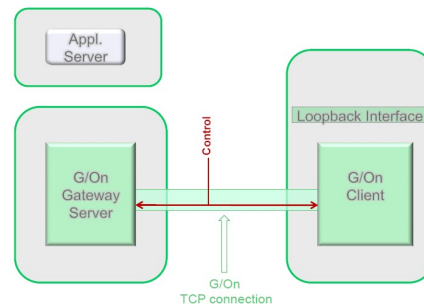
Which authentication factors are sufficient for establishing the identity of a user, and which groups of users can be authorized to use which applications are defined in G/On, in terms of so-called *decision rules*. Decision rules are introduced, below, after the introduction to Menu Actions.

Menu Actions

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

- (0) *Port Forward*. Creates one or more port forwards from the client side to the server side, and may start a client side command.
- (1) *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.
- (2) *G/On Internal*. Starts the build-in G/On actions for installing, updating or removing packages, or doing field enrollment of tokens.
- (3) *Wake-on-LAN*. Sends wake-on-LAN packets from the G/On server to wake up a machine with a given network MAC address.
- (4) *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.
- (5) Currently unused
- (6) *RDP Connection*. Experimental port forward for the RDP protocol. Does single sign-on on the server side, and reacts to re-direction messages from Remote Desktop Connection Broker (Terminal Services Session Broker).

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.



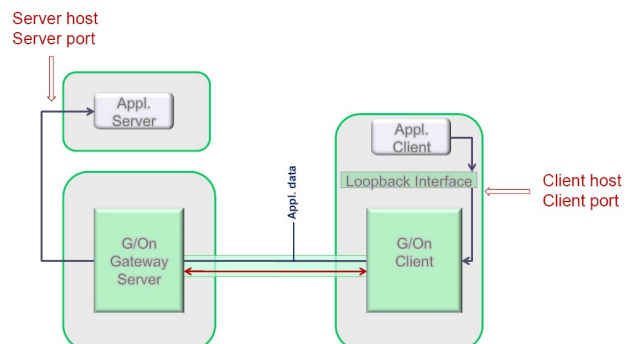
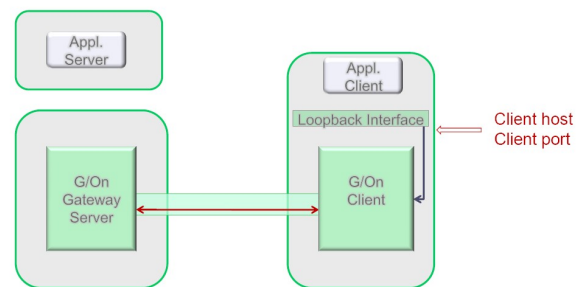
Port Forward Menu Actions

A menu action of type “Port Forward” works as described in the following, when a user activates it.

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.

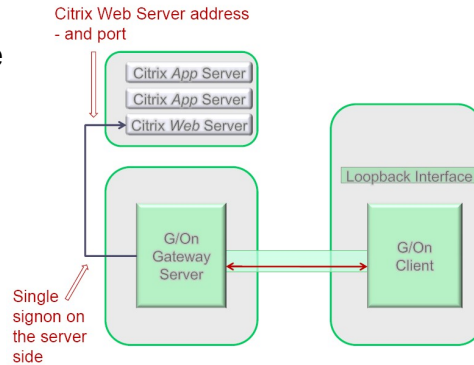
When the application client communicates on the given address and port, the G/On client forwards this communication through its TCP connection to the G/On server, and the G/On server forwards the communication through a connection to the application server at an address and port, that was also defined by the menu action (Server host, Server port).



Citrix Web Interface Menu Actions

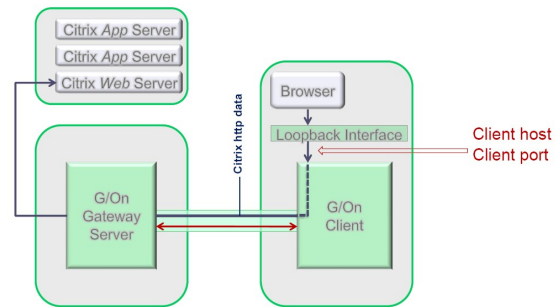
A menu action of type “Citrix Web Interface” works as described in the following, when a user activates it.

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 an user session, and sends a web page with icons for the Citrix enabled applications.

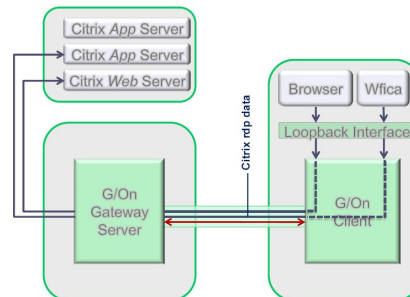
The G/On server forwards this page to the G/On client, which starts a browser. The start URL points to the G/On client itself, and allows the G/On client to serve the web page to the browser, so it can display the page to the user.



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.

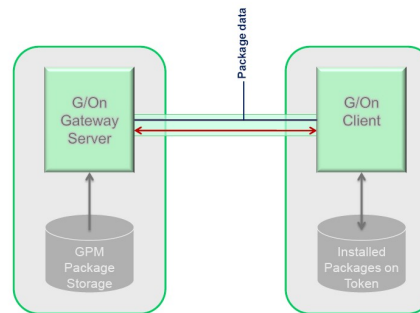
G/Update Menu Actions

A menu action of type “G/Update” works as described in the following, when a user activates it.

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.

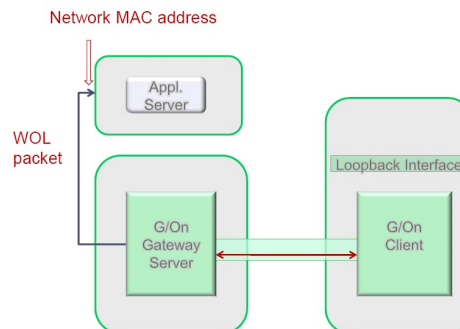


Wake-on-LAN Menu Actions

A menu action of type “Wake-on-LAN” works as described in the following, when a user activates it.

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

A menu action of type “Citrix XML Interface” works as described in the following, when a user activates it.

When a user is authorized for a menu action of this type, the G/On server creates a connection to a web service on a Citrix Web server and logs in as this user. Each of the Citrix applications published for the user is then presented as a G/On menu entry.

When the user chooses one of these menu entries, the menu entry 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 web service on the Citrix Web Server, to get an .ica file which describes how to start the corresponding application through Citrix.

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.

RDP Connection Menu Actions (Experimental)

A menu action of type “RDP Connection” works as described in the following, when a user activates it.

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.

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:

(1) **Token:** *micro_smart_0002*, **User:** *Bob@giritech.com* \Rightarrow **Personal Token Status:** *Personal Token*

(2) **User Group:** *Employees*, **Personal Token Status:** *Personal Token*
 \Rightarrow **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, are defined in G/On (not in the user directory)

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 \Rightarrow Personal Token Status

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

<i>Personal Token Status</i>	\Rightarrow	<i>Authentication Status</i>
<i>User Group, Personal Token Status</i>	\Rightarrow	<i>Authentication Status</i>
<i>G/On User Group, Personal Token Status</i>	\Rightarrow	<i>Authentication Status</i>
<i>Token Group</i>	\Rightarrow	<i>Authentication Status</i>
<i>User Group, Token Group</i>	\Rightarrow	<i>Authentication Status</i>
<i>G/On User Group, Token Group</i>	\Rightarrow	<i>Authentication Status</i>
<i>User Group</i>	\Rightarrow	<i>Authentication Status</i>
<i>G/On User Group</i>	\Rightarrow	<i>Authentication Status</i>

Action Authorization Policy rules register policies for giving access to menu actions. The rules have one of the types:

<i>Authentication Status, User Group</i>	\Rightarrow	<i>Menu Action</i>
<i>Authentication Status, G/On User Group</i>	\Rightarrow	<i>Menu Action</i>
<i>User Group</i>	\Rightarrow	<i>Menu Action</i>
<i>G/On User Group</i>	\Rightarrow	<i>Menu Action</i>
<i>Authentication Status, User Group</i>	<i>Token Group</i>	\Rightarrow <i>Menu Action</i>
<i>Authentication Status, G/On User Group</i>	<i>Token Group</i>	\Rightarrow <i>Menu Action</i>
<i>User Group</i>	<i>Token Group</i>	\Rightarrow <i>Menu Action</i>
<i>G/On User Group</i>	<i>Token Group</i>	\Rightarrow <i>Menu Action</i>
	<i>Token Group</i>	\Rightarrow <i>Menu Action</i>

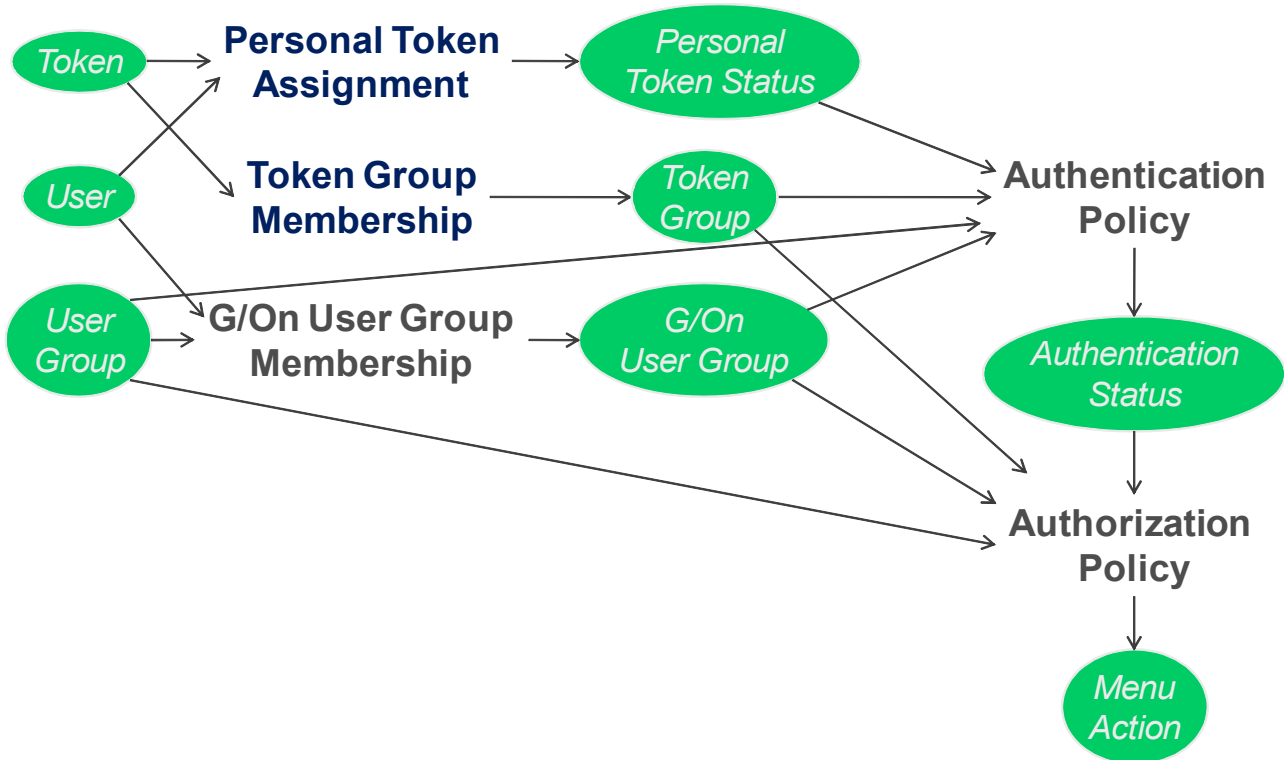
Token Group Membership rules register the fact, that a given token is a member of a token group. The rules have the type:

Token \Rightarrow *Token Group*

G/On User Group Membership rules register the fact, that a user or all the users of a group from the user directory are members of a G/On user group. The rules have one of the types :

<i>User</i>	\Rightarrow	<i>G/On User Group</i>
<i>User Group</i>	\Rightarrow	<i>G/On User Group</i>

Overview of the way rules fit together in G/On



The Rule Engine

The G/On rule engine 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.

The Management Client

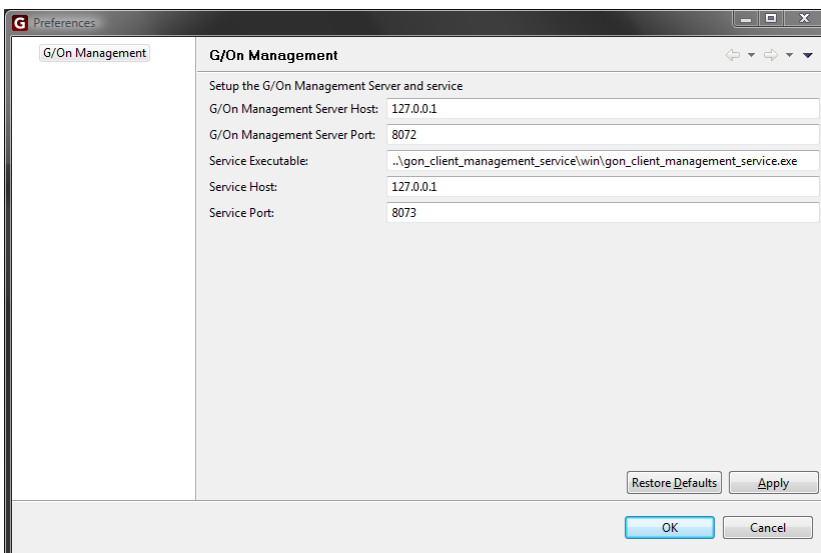
The management client is a tool that, among other things, lets an administrator add rules to the rule engine and create tokens for users. After installation there should be a sub-menu in the windows start menu called 'G-On'. Navigate to the menu item labelled G-On Management and use this menu item to launch the management client.

NOTE: On Windows Server 2008, you must run the G/On Management program, as Administrator: Find the program in the Windows Start Menu, right-click 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 can be used for setting host name and port for communication with the G/On management Server. The two top most fields are used for that. The service executable is used for enrolling tokens and should normally be running on the local host so the administrator can insert tokens into the physical machine.



Introduction to Perspectives

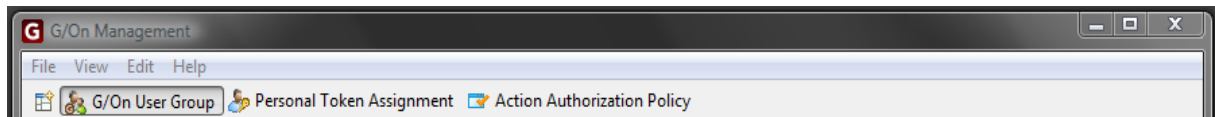
Perspectives are defined as a full window with a specific purpose. Most perspectives are used for defining rules for the rule engine. Additional perspectives are used for adding software to tokens or display reports on system usage.

The perspectives included in the management client are:

- **G/On User Group Perspective** adds user or groups to local G/On 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.

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:

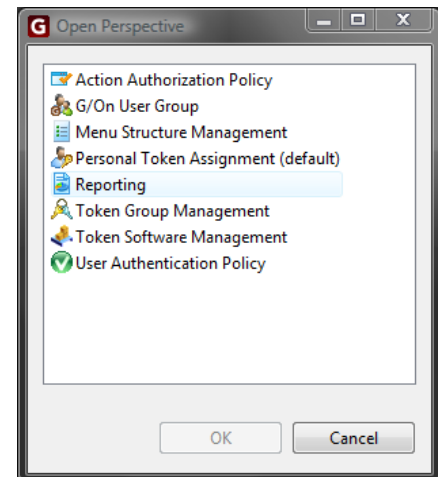
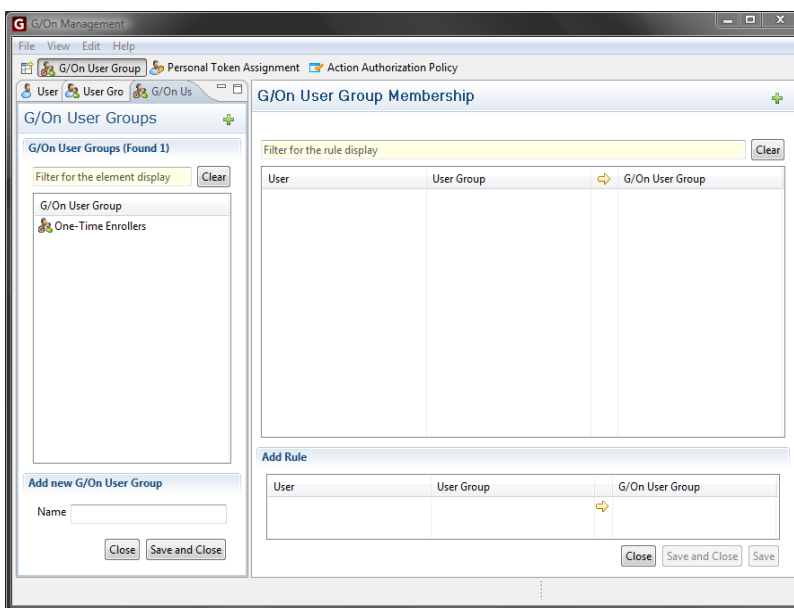
- G/On User Group – for defining the group of users who are allowed to enroll a personal token “in the field”
- Personal Token Management – for activating personal token assignments and thereby approving field enrollment requests
- Action Authorization Policy - for defining which menu actions are authorized for use by which user groups, under which which circumstances

Selecting other perspectives

To the far left of the perspective buttons is a smaller button that can be used for opening additional perspectives. Clicking this button will lead to opening a window listing all the available perspectives.

Using the perspective selector it is possible to select which perspective buttons should be in the perspective bar. Buttons in the perspective bar can be removed using the context menu that appears when right clicking the button.

Perspective layout



Underneath the perspective bar on the left hand side is number of element panes. The element panes holds a listing 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 editor area appears at the bottom.

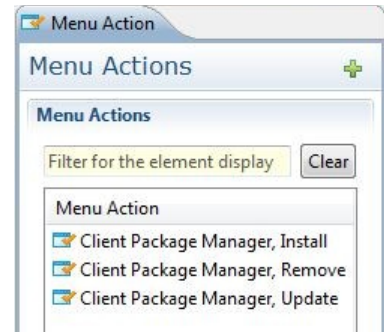
At the right hand side is a listing of rules related to the selected perspective. When adding or editing a rule the rule editor will appear at the bottom.

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 main menu and choose view > reset window.

Introduction to Element Panes

The elements in the element panes are used for creating rules that are located in the rules listing. For each type of element there is an element listing. The element panes available in any perspective reflects the elements that can be used in rule creation in that specific perspective.



Listing elements

The listing should show all the available elements of the selected type. It is possible to refresh the element listing, thereby ensuring that all elements are displayed:

- Click anywhere in the listing area. Then choose view > refresh in the menu.
- Click anywhere in the listing 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 select 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 element panes for details.

Creating new elements

There are several ways of adding new elements:

- Click the plus (+) sign in the upper right corner of the personal token status element listing.
- Right-click anywhere in the listing 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 listing area. Then choose Edit > New in the main menu.
- Click anywhere in the listing 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 in the main menu.
- 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 listing adjusts to display the relevant elements. Use the clear button to clear the filter and display all available elements.

Introduction to Rule Views

The rule listing shows all the rules that correspond to a specific perspective.

Personal Token Assignment +

Clear

Token	User	Personal Token Status

Add Rule

Token	User	Personal Token Status
micro_smart-0001		Personal Token

Close
Save and Close
Save

Listing rules

The rule listing should show the rules related to the selected perspective. It is possible to refresh the rule listing, thereby ensuring that all rules are displayed:

- Click anywhere in the rules listing. Then press the keyboard short cut F5.
- Click anywhere in the rules listing. Then choose view > refresh from the main menu.

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 of the rule view.
- Click anywhere in the rules listing. Then press the keyboard short cut Ctrl-N.
- Click anywhere in the rules listing. Then choose edit > new in the main menu.
- Right-click anywhere in the rules listing. Then select new in the context menu.

Any of these should result in the rule editor 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 select edit in the context menu.
- Select the rule. Then press the keyboard short cut Ctrl-E
- Select the rule. Then select edit > edit in the main menu.

At this point it is not possible to remove single elements from an existing rule. Elements can only be added. If a rule has too many elements, remove the rule and create a new one.

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 from the main menu.
- Right-click the rule. The select 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 listing adjusts to display the relevant rules. Use the clear button to clear the filter and display all available elements. The filter considers all elements in a rule to see if something matches.

Adding elements to a rule

Elements are selected from the element panes. There are several ways of adding an element to a rule:

- Select the element and drag it onto the rule editor.
- Select the element and drag it into the rule listing.
- Select the element. Then press the keyboard short cut Ctrl-A
- Right-click the element and select add to rule editor from the context menu.
- Select the element. Then choose edit > add to rule editor from the main menu.

Adding an element to a rule should result in that element appearing in the rule editor 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.

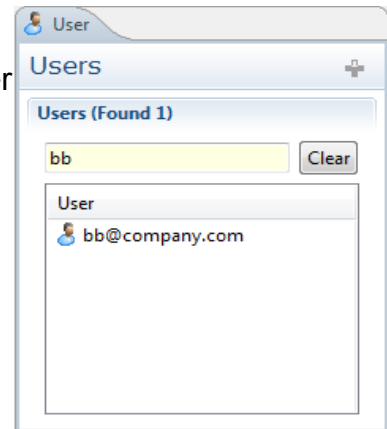
Element Pane: Users

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.

New

It is not possible to add new users. Users should be created in one of the external User Directories.



Edit

The user elements can be edited. See page 15 for information on how to start editing.

The settings that can be changed for a user are the user's personal workstation settings. This 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

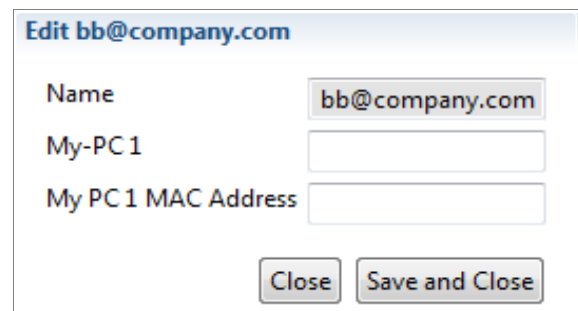
enter the data for the first one, save it and then edit the user again. It is now possible to add information on workstation 2 and save it. After that you can add workstation 3 and so on.

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 actions listing tab. See page 25 for more information on the menu actions listing tab.

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

Delete

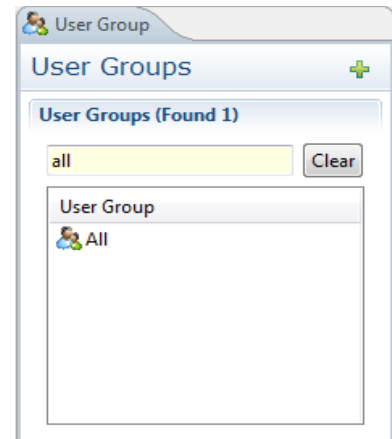
It is not possible to delete users.



Element Pane: User Groups

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.

OBS: In the perspectives: User Authentication Policy and Action Authorization Policy, the user group listing is actually a *mix* of groups from both 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 15 for information on how to create new elements.

Edit

It is not possible to edit any settings for User Directory groups. In the G/On User Group Management Perspective it is possible to edit the title of G/On User Groups.

Delete

It is not possible to delete User Directory user groups from within the G/On management client. It is possible to delete G/On user groups when in the G/On user group management perspective. But only if they are not used in any rule.

Element Pane: G/On User Groups

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 an action in the end-user G/On client.



New

It is possible to create new G/On user group elements. See page 15 for information on how to create new elements.

Edit

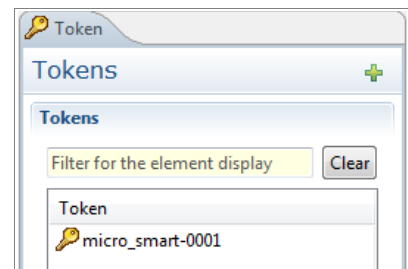
You can edit the name of any G/On user group that is not built-in. See page 15 for information on how to start editing elements.

Delete

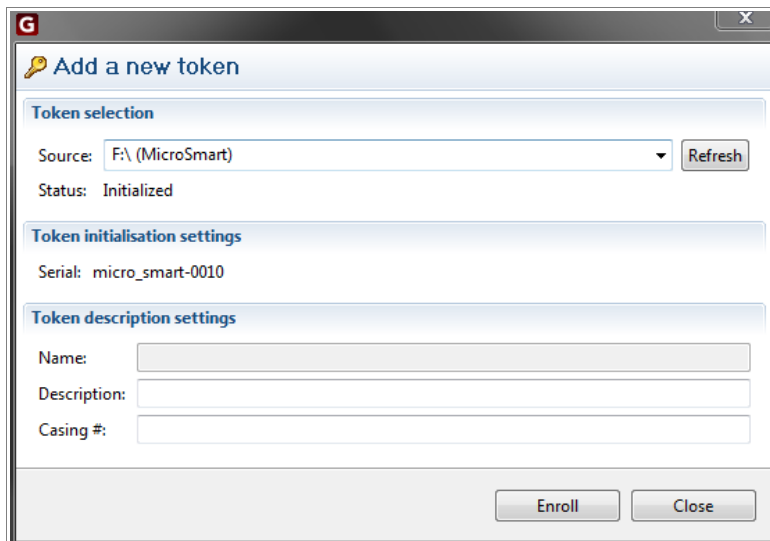
It is possible to delete G/On user groups that are not built-in or in use in any rules. See page 16 for general information on how to delete elements..

Element Pane: Tokens

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 given 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 15 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:** Tokens must be initialized in order to be valid. 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 the 'refresh' button. For any token you can add a description and a casing number. Click the 'Enroll' button to add the selected token to the G/On Server. The new tokens serial number should now appear in the token listing.

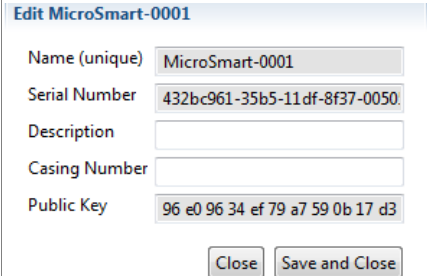
Click the 'Close' button to close the editor without saving. Click the 'Save and close' button to save the changes and close the editor.

Edit

The Tokens that are enrolled into the server can be edited. See page 15 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 the 'Close' button to close the editor without saving. Click the 'Save and close' button to save the changes and close the editor.



Edit MicroSmart-0001	
Name (unique)	MicroSmart-0001
Serial Number	432bc961-35b5-11df-8f37-0050
Description	
Casing Number	
Public Key	96 e0 96 34 ef 79 a7 59 0b 17 d3
<input type="button" value="Close"/> <input type="button" value="Save and Close"/>	

Delete

It is possible to delete token elements. But only if the token is not used in any rules. See page 16 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.

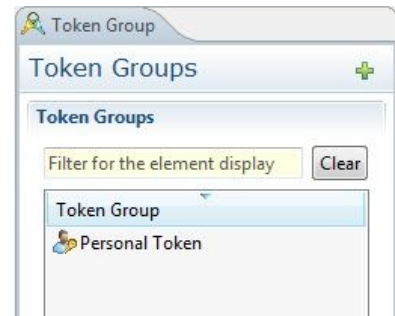
Computer User Token is a computer (PC or other computing device) where a (possibly non-admin) user has "installed" a private key and the G/On software in the users home directory/registry on a computer. The key file is typically locked to a specific computer by a screening check of the MAC addresses.

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. The G/On software must be installed on the PC, but this can be done without requiring admin rights.

Element Pane: Token Groups

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 perspective: Token Group Management.

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 perspective: Personal Token Assignment.



New

It is possible to add new token group elements. See page 15 for general information on how to create new elements.

Edit

It is possible to change the name of token groups – but only in the perspective: Token Group Management. See page 15 for more information on how to start editing elements.

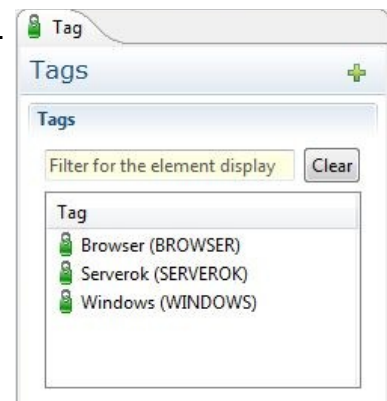
Delete

Any token group elements that is not built in can be deleted when they are not used in any rules - but only in the perspective: Token Group Management. See page 16 for general information on how to delete elements.

Element Pane: Tags

The tag elements can be used to categorize your menu actions. Any 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 27.



New

It is possible to add new tags. See page 15 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 27.

Edit

It is possible to edit tags. See page 15 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 alphanumerical 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 catching 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.
- **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.

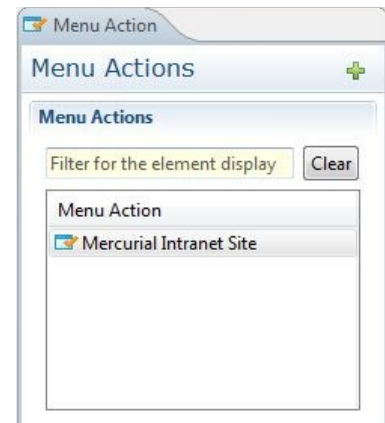
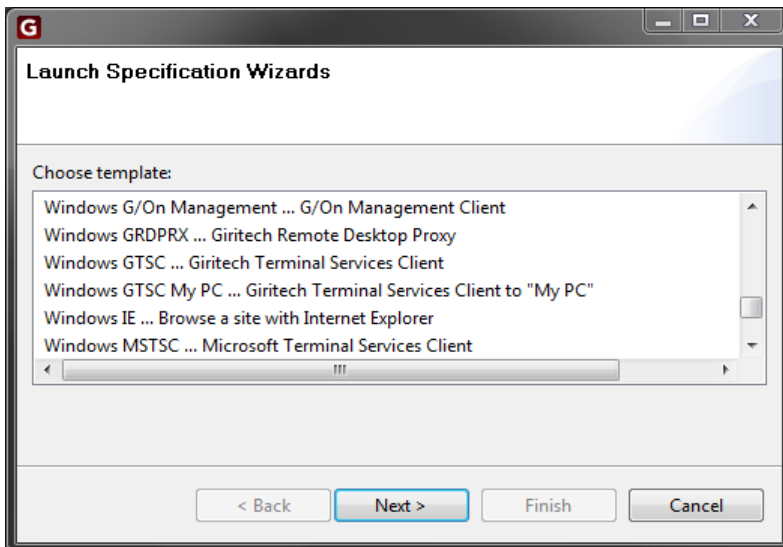
Delete

It is possible to delete tag elements. See page 16 for general information on how to delete elements.

Element Pane: Menu Actions

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.

New



It is possible to add new menu action elements. See page 15 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 action: choose the context menu item: 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 listing.

Some menu actions require information about specific user's workstation settings. These settings are added in the user's information editor. See page 19 for more information on editing user settings.

Some menu actions require a special setup of an application server. These are documented on page 48.

Edit

It is possible to edit a menu action element. The editor resembles the wizard pages for the specific menu actions. See page 15 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 16 for general information on how to delete elements.

General Features of Menu Action Elements

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 meaning can be summarized as follows.

Field for identifying the menu action

Each menu action has a unique name and a title, that is used in the menu entry, when the action appears in the menu of an end-user :

- *Name*
- *Menu Title*

Fields for defining the port forward(s)

A menu action can define 1 or more port forwards. Each port forward is defined by the address and port on the client side and the address and port on the server side:

- *Client Host*
- *Client Port*
- *Server Host*
- *Server Port*

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

1. An application on the remote client machine 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 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 means until the program exits, -1 means no limit on the lifetime)
- *Parameter file template*

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)
- *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 that 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 23 and 38. 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 users' 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 users' 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.

There are currently two types of tag generators:

`client_ok::IfPlatformIs("os")` where *os* is win, mac or linux.

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 Pane: Authentication Status

The authentication status listing 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 15 for general information on how to create new elements.

Edit

It is possible to edit the name of the authentication status elements. See page 15 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 16 for general information on how to delete elements.

Element Pane: 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 element listing 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 element listing also contains “Personal Token” as a special token group.

New

It is *not* possible to add new personal token status elements.

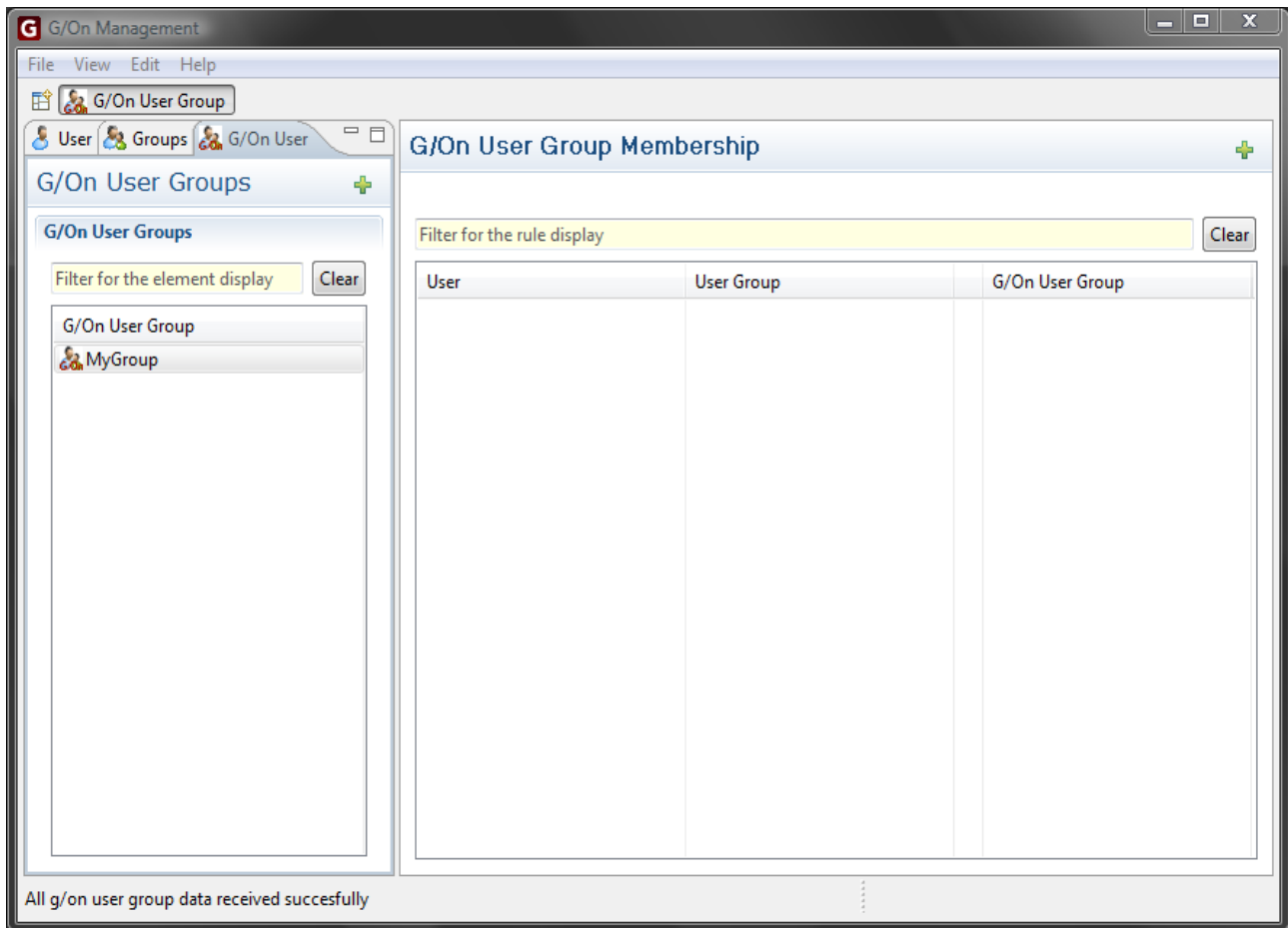
Edit

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.

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. In the element pane: Groups, there is a context menu command: Add members to One-Time Enrollers. This can be used for adding all members of a 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 group on the left hand side means they are placed in the G/On group at the right hand side.

Usage

Rules can be added, edited and deleted. See page 17 and onwards for general information on how to do this rule. For general information on how to add elements to a new rule or an existing rule, see page 18.

Perspective: Action Authorization Policy

Authentication Status	User Group	Token Group	Menu Action
Authenticated			Client Package M...
Authenticated			Client Package M...
Authenticated			Client Package M...

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 may need access to different applications than guest users.

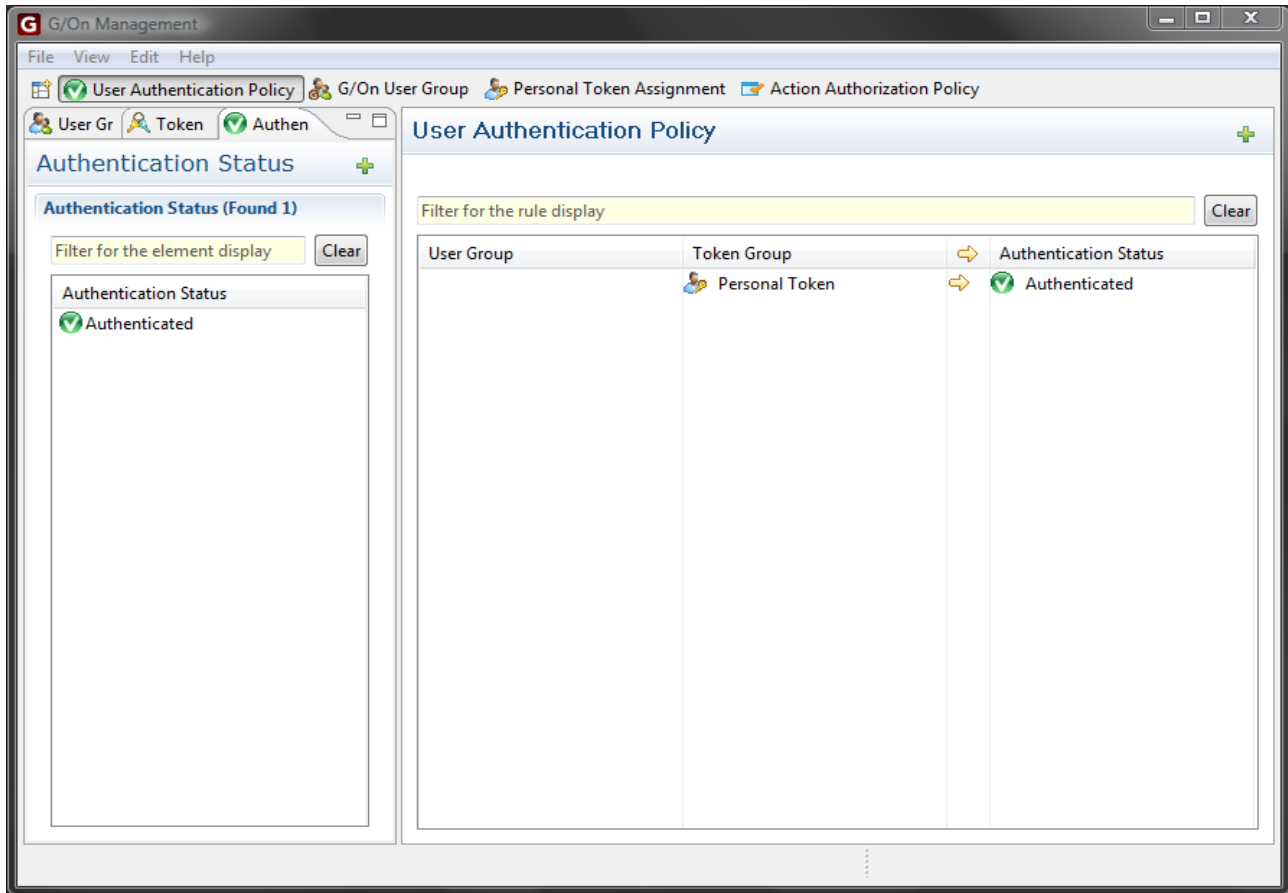
The token group elements are defined in the Token Group Management perspective. In authorization rules, token groups can be useful as a way of identifying groups of PCs which must be used, in order for certain actions to be authorized. For instance, the PCs could each have a MicroSmart Token or a smart 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 action elements 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 17 and onwards for general information on how to do this rule. For general information on how to add elements to a new rule or an existing rule, see page 18.

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.

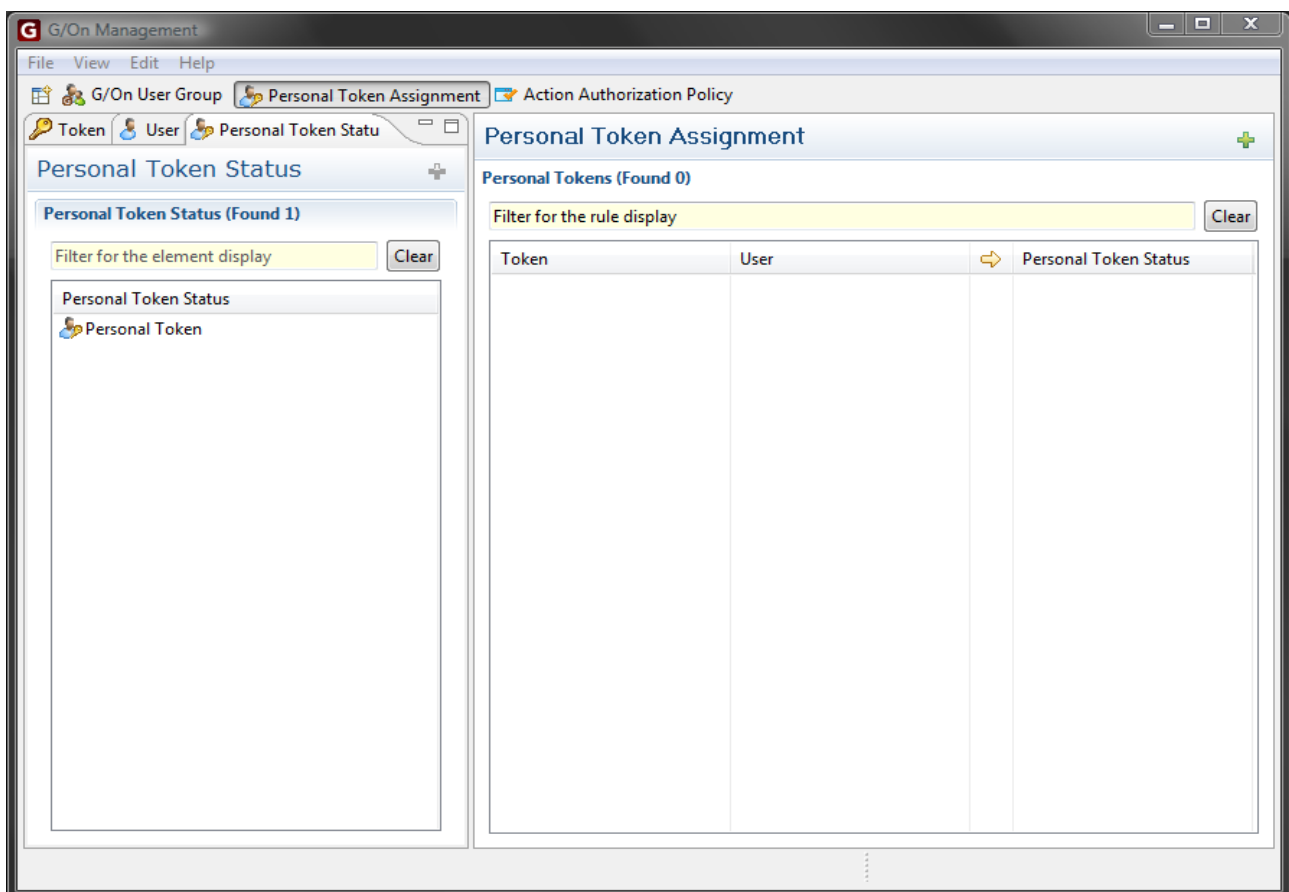
Authentication status elements are the result elements in the rules in this perspective. If all

the specified elements on the left hand side of the rules are true, then the selected 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 17 and onwards for general information on how to do this rule. For general information on how to add elements to a new rule or an existing rule, see page 18.

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.

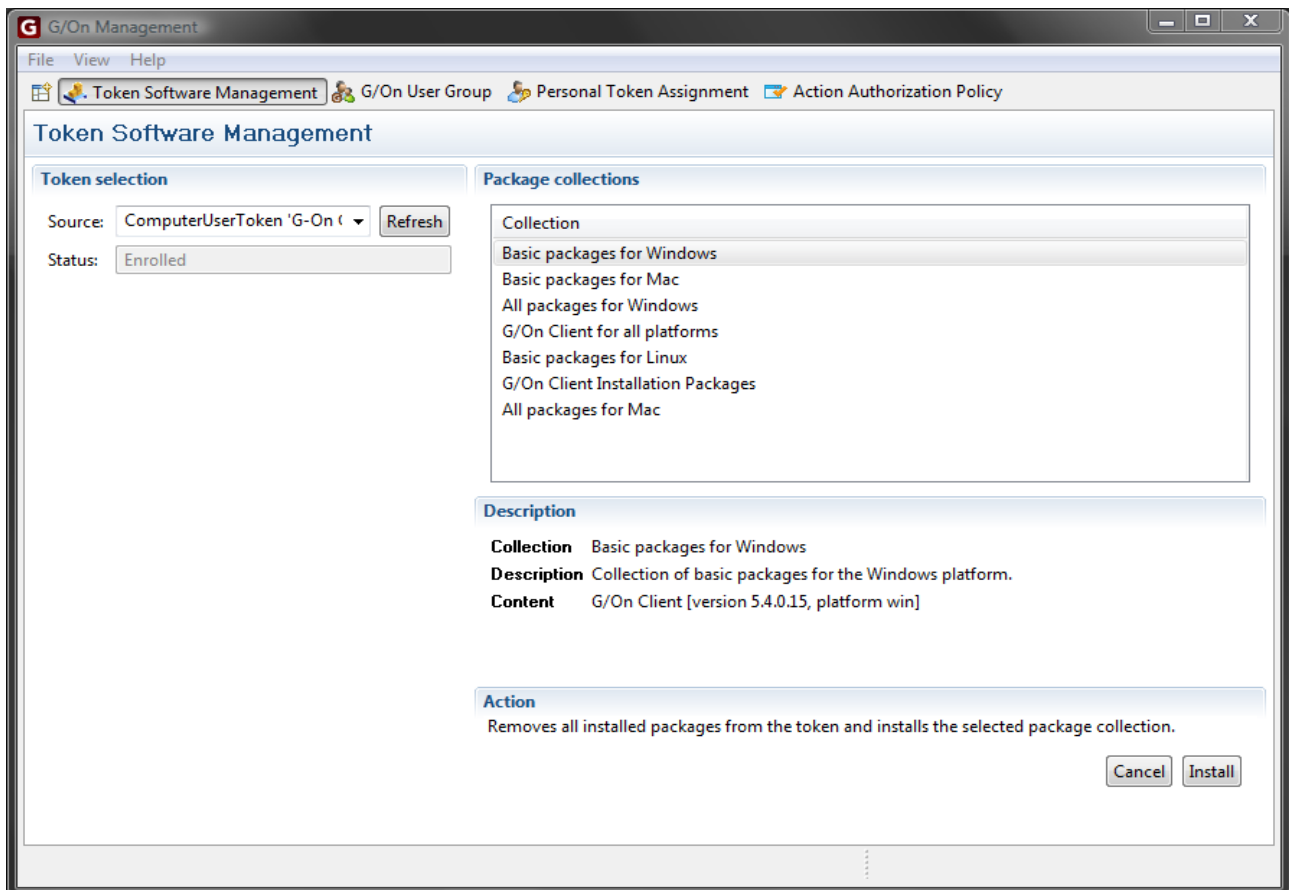
Personal token status elements are the result element of the rules in this perspective. It is *not* possible to create other personal token status elements.

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

Usage

Rules can be added, edited and deleted. See page 17 and onwards for general information on how to do this rule. For general information on how to add elements to a new rule or an existing rule, see page 18.

Perspective: Token Software Management



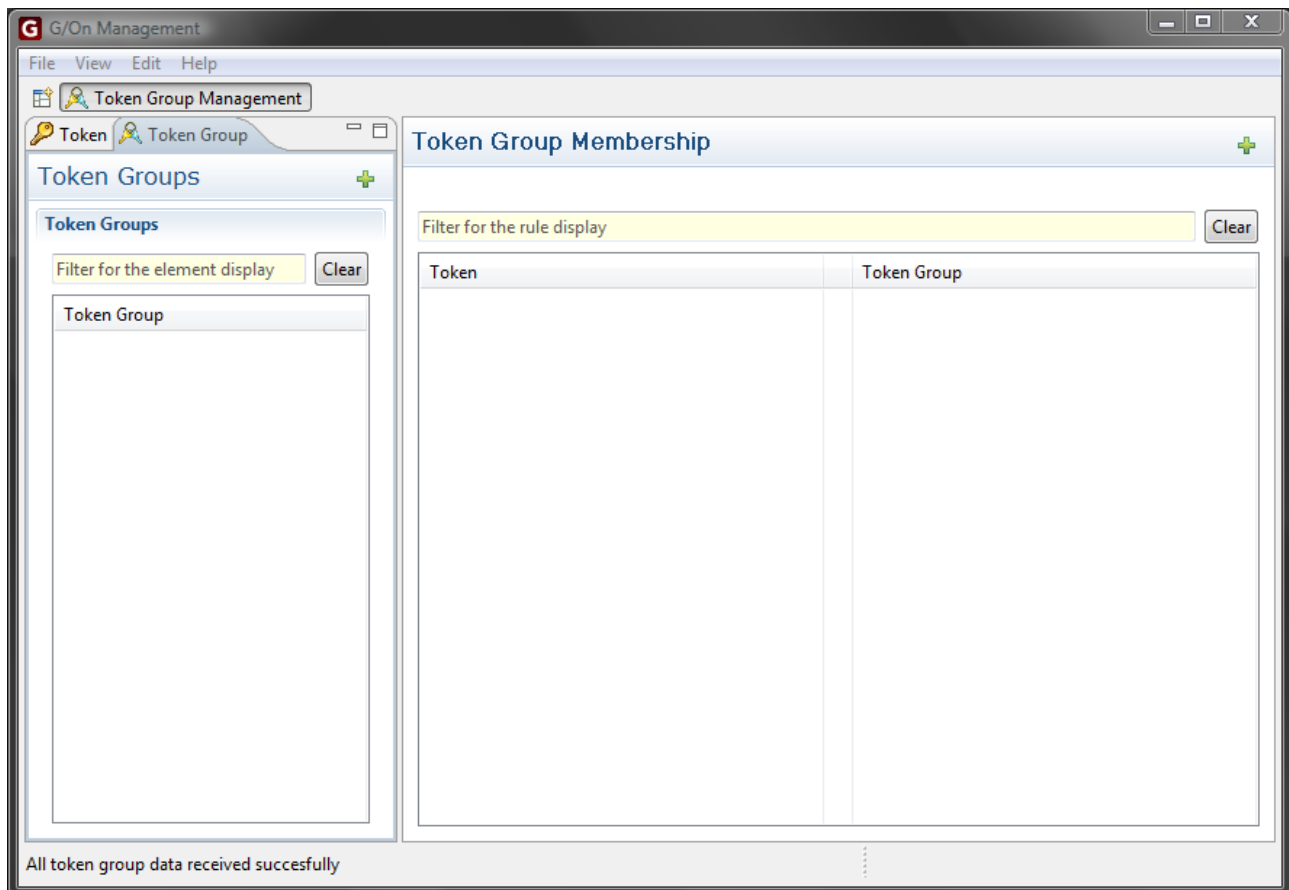
The token software management perspective is used for installing software package collections to tokens before handing them to the users. The tokens in the source list are the tokens inserted in the USB ports of the local workstation.

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 group is by creating a rule for each token saying that it is a part of a particular 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.

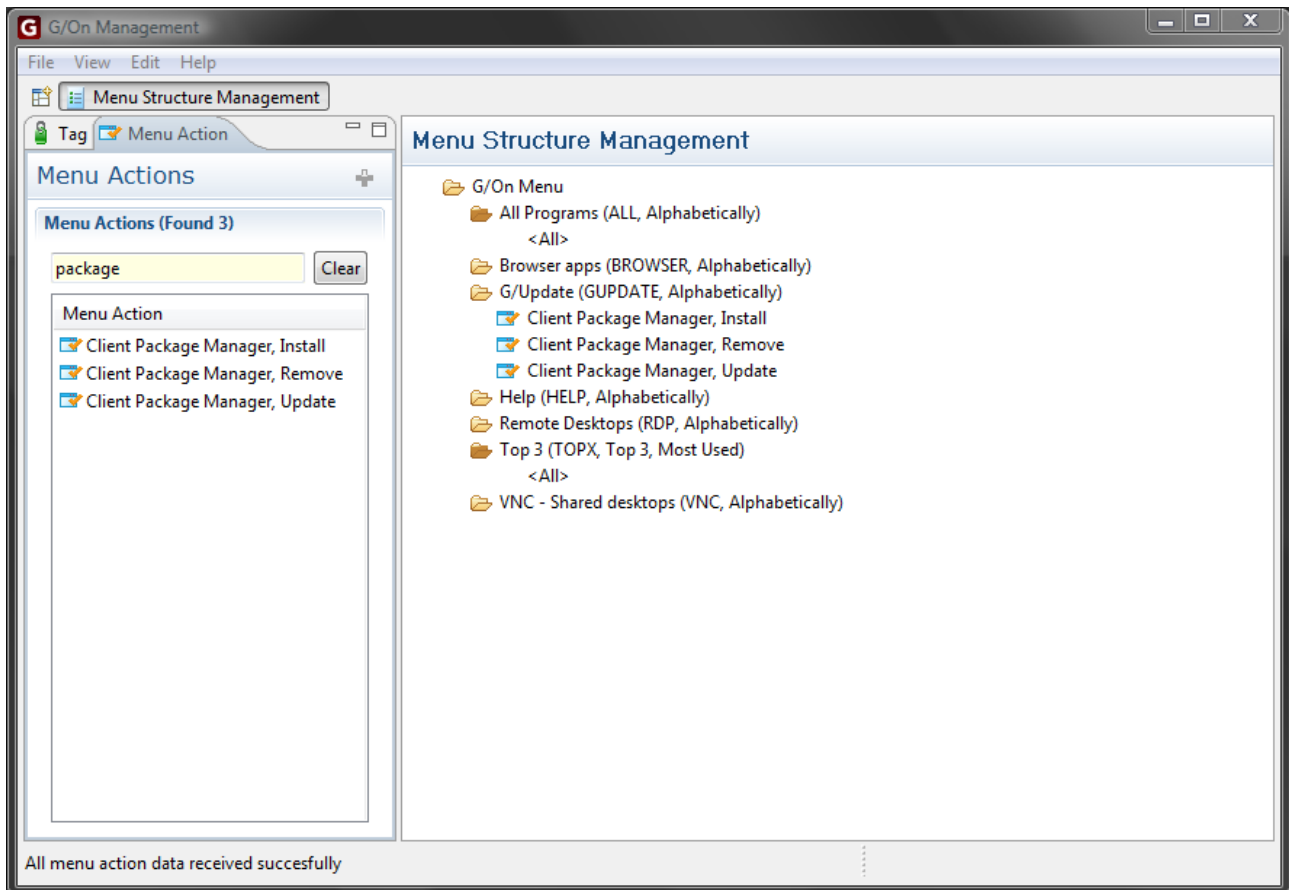
Rule Elements

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 group.

Usage

Rules can be added, edited and deleted. See page 17 and onwards for general information on how to do this rule. For general information on how to add elements to a new rule or an existing rule, see page 18.

Perspective: Menu Structure Management



The Menu Structure Management perspective is used for structuring the content of end users' 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 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 element pane. 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. Tags

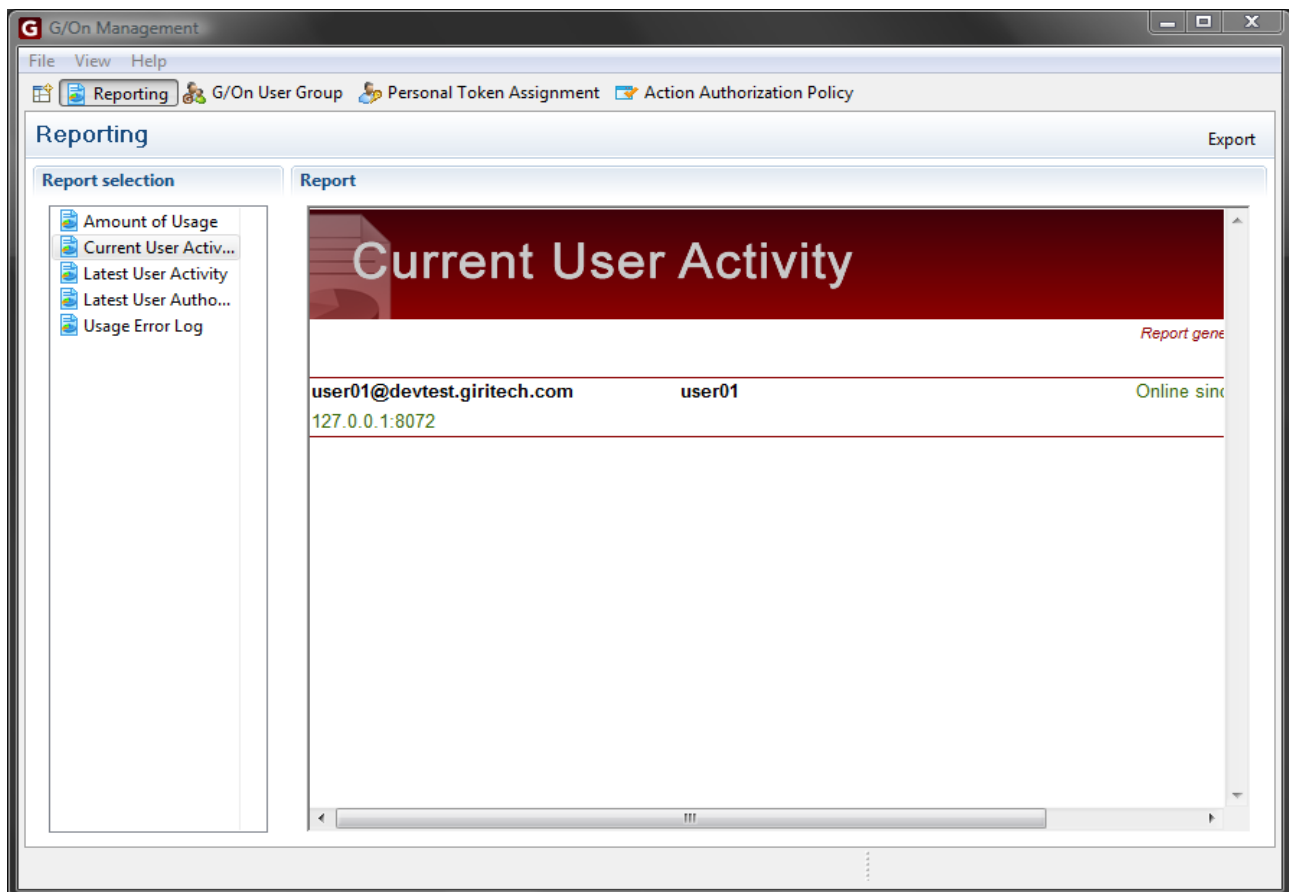
are added to the folder structure by dragging and dropping. Tags can be dragged onto other tags in the menu structure in order to create sub-menus.

Menu action elements 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. 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 listing 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 that menu actions cannot be created in the element listing in this perspective. Use the Action authorization perspective when you want to create menu actions.

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
- Current user activity
- Latest user activity
- Latest user authorization
- Usage error log

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 that 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 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 labelling 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 action to the server.
6. Based on the action name, the server looks up the definition of the 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 afterwards 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”.
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 directory that already has the proper authentications.

Can I delete elements from a rule?

It is not currently possible to delete individual elements from an already existing rule. To remove an element from a rule the G/On administrator will have to create a new rule without the element that should be removed and then delete the old rule.

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 fill-in the field “Server Host”, then save, and open again, and fill-in “Server Host 1”, 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. Hit the 'Refresh' button to refresh the listing in the drop down. 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.

The “Enroll” button is inactive (grey)?

If a token is selected in the drop-down, 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 pane, before it can be re-enrolled.

What can be used as a token?

Tokens are meant to be an authentication factor. Therefore the tokens should be entities that the user will and can protect, so nobody else gets hold of them.

Currently supported token types are:

- MicroSmart (with and without USB adapter)
- SoftToken
- Computer User Token
- Hagiwara H2 and H3

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 user 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/groups directory into one 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/groups directory.

Can I force an update of the user menu?

It is not currently possible to force a users menu to be updated. Creating new rules in the G/On management client will impact the users menu on the next login.

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 management client, try adjusting the preferences (menu: View -> Preferences).

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

Certain element panes have predefined and built in elements that we think should be used for the 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 panes that hold types that should not be added to the current rule editor. The perspective has probably not been properly refreshed. Choose the menu action: View > Reset Window. This should reset all the perspectives views and panes.

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 username/password/token, so he is not properly authenticated, and all authorization rules require proper authentication.
2. The administrator has forgotten to set up some authorization rules. 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 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 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 applications 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 "Authorization Policy". This automatically puts the menu actions into the menus. So you do not need to

go into “Menu Structure Management“. You only need to go into “Menu Structure Management“, if you have some special requirements regarding the structure of the menu (new sub-menus, or sub-sub menus etc.). So “Menu Structure Management“, 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 “Authorization Policy“. In order to promote this new work flow, the creation of Menu Actions has been disabled in the Menu Structure Management view.

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 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. Then access to the applications can be given to this group (along with the “Authenticated” condition). But if you really want a personal 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

Introduction

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

Introduction

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 username 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 (not including the quotes):

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

Index

Action Authorization Policy Perspective.....	13	Element Pane: Authentication Status.....	28
Action Authorization Policy rules.....	10	Element Pane: G/On User Groups.....	20
Add members to One-Time Enrollers.....	31	Element Pane: Personal Token Status.....	30
Authenticated.....	9	Element Pane: Tags.....	23
authentication factors.....	4	Element Pane: Token Groups.....	23
Authentication Policy Perspective.....		Element Pane: Tokens.....	21
elements.....	34	Element Pane: User Groups.....	20
Authentication Status.....	9	Element Pane: Users.....	19
Authentication Status Element.....		Element type.....	8
authenticated (built in).....	41	ENABLED	27
delete.....	28	Field Enrollment.....	31
edit.....	28	Field enrollment.....	20
new.....	28	G/O.....	4
Authorization Policy Perspective.....		G/On decision rule.....	8
elements.....	33	G/On Internal.....	4
usage.....	33	G/On User group.....	9
authorized applications.....	4	G/On User Group Elements.....	
authorized menu actions	11	delete.....	21
AUTOLAUNCH.....	28	edit.....	21
AUTOLAUNCH_FIRST_START.....	28	new.....	21
Citrix Web Interface.....	4	G/On User Group Membership rules.....	10
Citrix Web Interface Menu Actions.....	6	G/On User Group Perspective.....	13
Citrix XML Interface.....	4	elements.....	32
Citrix XML Interface Menu Actions.....	7	usage.....	32
Client Host.....	26	G/Update Menu Actions.....	7
Client Port.....	26	Hagiwara.....	22
client_ok::IfPlatformIs.....	28	Hagiwara H2/H3 USB Token.....	22
CLIENTOK.....	27	Introduction to Perspectives.....	13
Close with process.....	27	Kill process on close.....	27
Command.....	26	known user.....	9
Computer User Token.....	22	Lock to process name.....	27
Conclusion.....	8	Lock to process PID.....	27
decision rules.....	4	login dialogue.....	11
Dialog tag generators.....	27	menu action.....	4
Dialog tags.....	27	Menu Action Elements.....	
Element.....	8	delete.....	25
add.....	15	edit.....	25
best practice.....	41	new.....	25
Delete.....	16	Menu Actions.....	4
editing.....	15	Menu Structure Management Perspective.....	13
filter.....	16	elements.....	38
listing.....	15	Menu Title.....	26
new.....	15	MicroSmart.....	22
Element Pane:	20, 21, 23, 25, 28, 30	MicroSmart token.....	22

MicroSmart USB token.....	22	listing.....	17
One-Time Enrollers.....	20, 31	new.....	17
package::CheckPackage.....	28	view.....	17
Parameter file template.....	26	Rule Engine.....	11
Parameter file lifetime.....	26	Server Host.....	26
Parameter file name.....	26	Server Port.....	26
Personal Token.....	9	SERVEROK.....	27
Personal Token Assignment Perspective.....	13	SHOW.....	27
elements.....	35	Smart Card Token.....	22
usage.....	36	SoftToken.....	22
Personal Token Assignment rules.....	9	sub processes.....	27
Personal Token Status.....	9	Tag Elements.....	
Personal Token Status Elements.....		automatically add to all items.....	24
delete.....	30	caption.....	24
edit.....	30	delete.....	24
new.....	30	edit.....	24
Perspective.....		max items to show.....	24
bar.....	13	name.....	24
included.....	13	new.....	23
layout.....	14	override item show.....	24
listing.....	14	parent tags.....	24
most used.....	13	show in menu.....	24
remove.....	14	sort option.....	24
reset.....	14	Token.....	9, 21
Perspective:	31, 32, 34-39	Token Elements.....	
Perspective: Action Authorization Policy.....	32	best practice.....	41
Perspective: G/On User Group.....	31	delete.....	22
Perspective: Menu Structure Management.....	38	New.....	21
Perspective: Personal Token Assignment.....	35	Token Group.....	9
Perspective: Reporting.....	39	Token Group Elements.....	
Perspective: Token Group Management.....	37	delete.....	23
Perspective: Token Software Management.....	36	edit.....	23
Perspective: User Authentication Policy.....	34	new.....	23
Port Forward.....	4	Token Group Management Perspective.....	13
Port Forward Menu Actions.....	5	elements.....	37
Preferences.....	12	usage.....	38
Premise.....	8	Token Group Membership rules.....	10
RDP Connection.....	4	Token Software Management Perspective.....	13
RDP Connection Menu Actions.....	8	Token types.....	22
Reporting perspective.....	13	two factors.....	9
export.....	40	types of elements.....	9
reports.....	40	types of rules.....	9
Rule.....		User.....	9
add elements to a.....	18	User Authentication Policy Perspective.....	13
delete.....	18	User Authentication Policy rules.....	10
edit.....	18	User Elements.....	
filter.....	18	delete.....	19

edit.....	19	new.....	20
new.....	19	user session.....	11
User Group.....	9	Wake-on-LAN.....	4
User Group Elements.....		Wake-on-LAN Menu Actions.....	7
delete.....	20	Working directory.....	26
edit.....	20	23