# Getting started with G/On Management

*A tutorial covering the basics of the G/On Management Client*

G/On Version 5.4
Document revision 0.9
2010-03-23

# 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:

- 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


Spotorno Allé 12, 2.
2630 Taastrup
Denmark
Phone +45 70.277.262

# Contents

# Introduction

This document 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

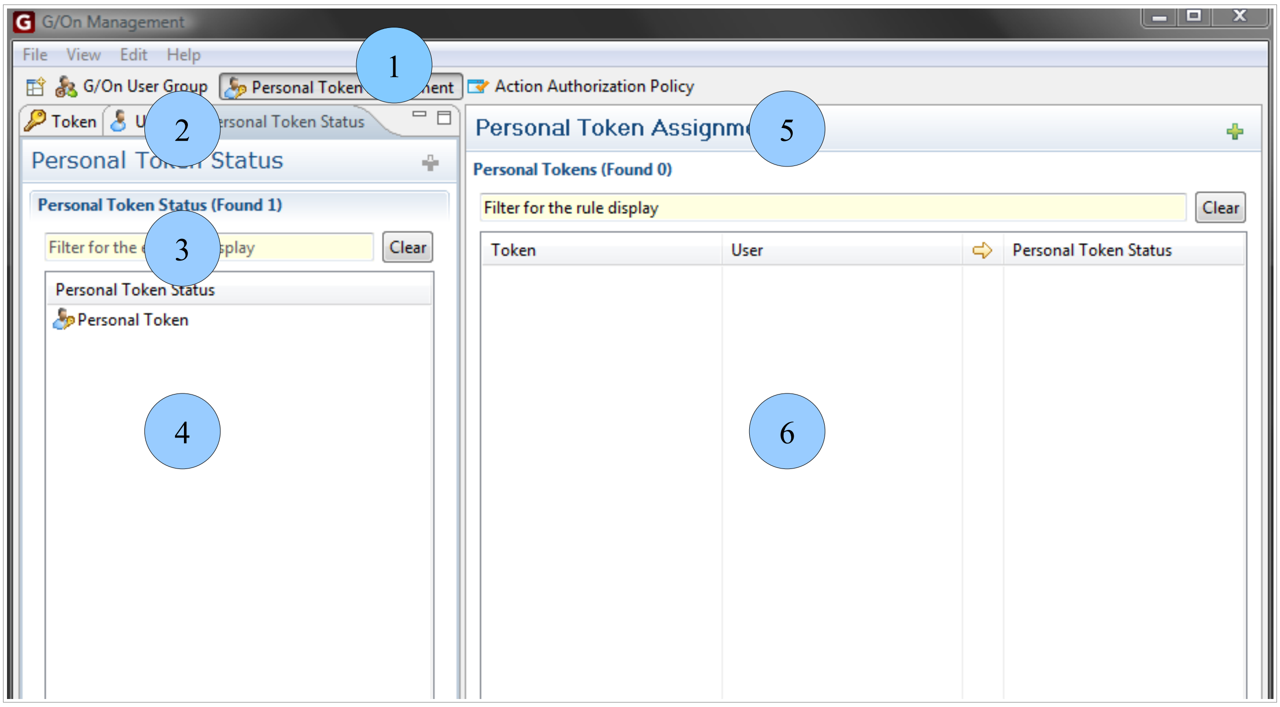
When you first open the G/On management application, you will probably not have any rules in the rule views. This guide will help you set up basic rules for user access to the application of your choice.

**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, 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"*.

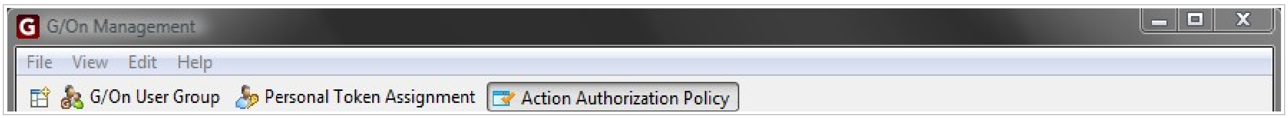
# Overview of the G/On Management Client




**Parts of the Management Client**

1. The **Perspective Selector** is used for selecting between focus areas.
2. The **Element Listing 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 Listing 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 Listing view** lists 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.

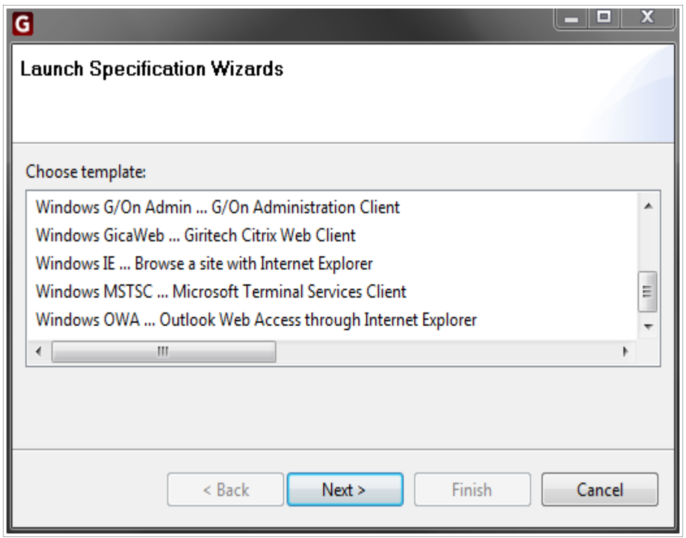
# Setting up Authorization Policies




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 Selector to see the perspective. The perspective contains a number of Element Tabs on the left, and a Rule Listing on the right.

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

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



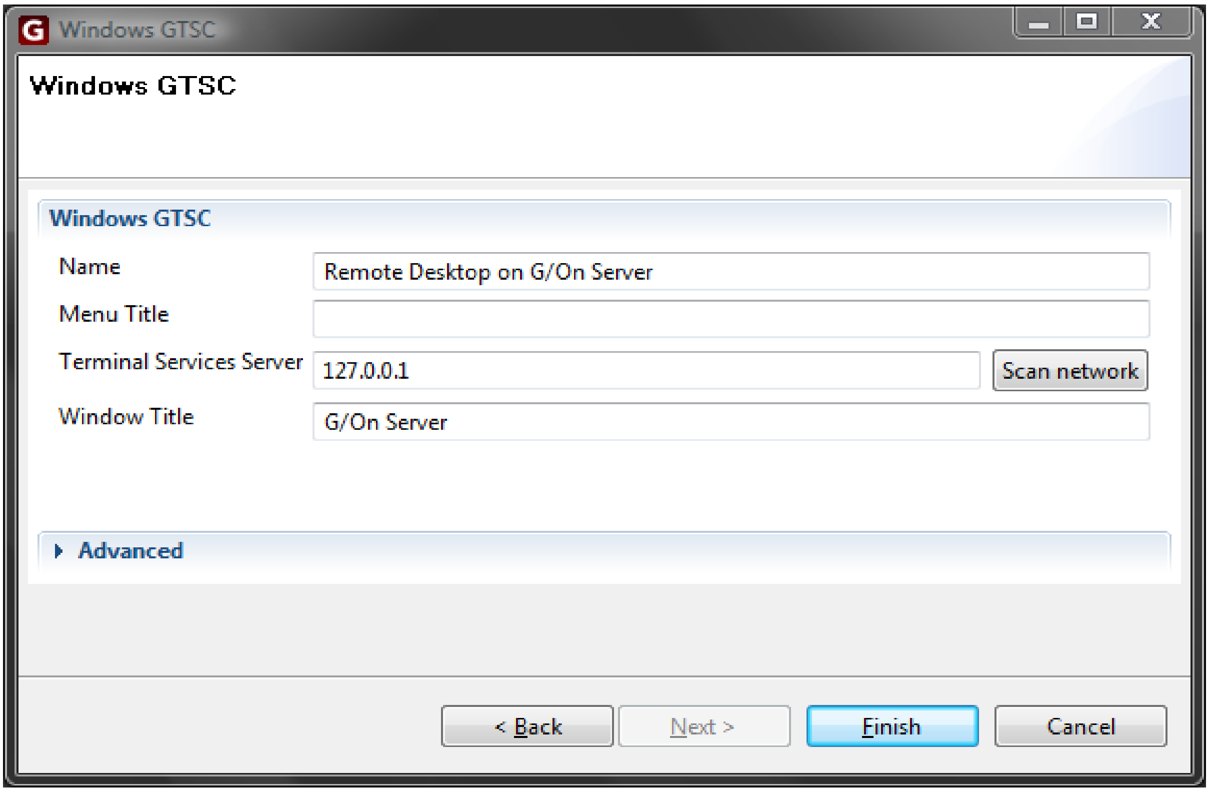

### Create an Authorization Policy

1. Select the **Authorization Policy button** from the perspective selector.
2. From the **Authentication Status listing** select the **'Authenticated'** element and **drag** it into the rule listing.
3. Select a **group of users** you want to allow this authorization from the **User Groups listing** and **drag** the element representing them into the rule editor.
4. Select a **menu action** from the **Menu Actions listing** and add it to the rule. The menu action will be added to the users menu if policies and rules permit it.
5. Click the **'Save and Close'** button to save the new rule.

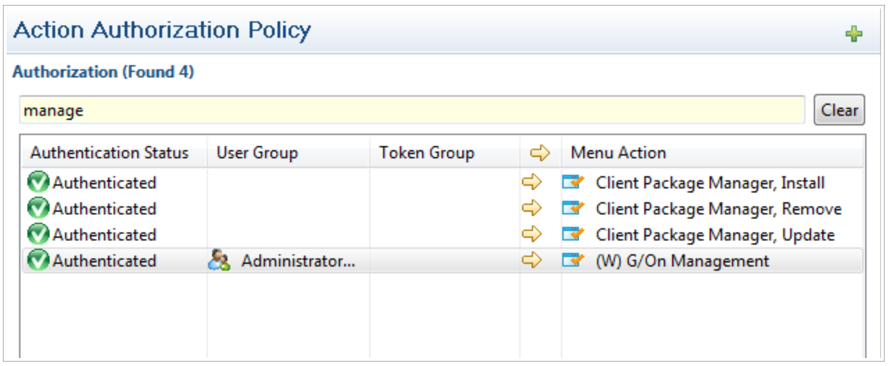
The last listing view contains the menu actions. These are the actions that will be listed in the users menu if they are allowed to use them and if the computer they are using can handle it.

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 listing view. 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 GTSC", and fill in the fields in the basic section:



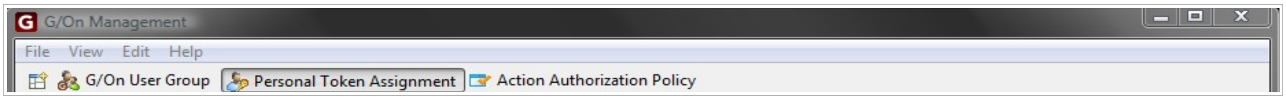

In this example (in the first three rules) a menu action provides access to the end-user package manager for installing, updating and removing packages, to any users that are Authenticated.




The fourth rule states that Authenticated Administrators are allowed access to the G/On Management Client.

You can create as many authorization rules as you like, to give access to various applications.

# Register a Personal Token for a User

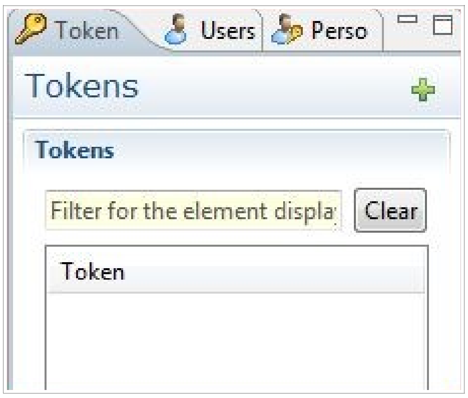



Two different perspectives are used for making the tokens ready to hand over to users: the Personal Token Assignment perspective and the Token Software Management perspective (the latter will be described in the next part "Adding Software to the Token").

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 listing of Users, a listing of Tokens and a listing of a Personal Token Status indication.

Select the Tokens listing by clicking the Token tab. You will notice that there are no tokens to choose yet. That's because you have to register tokens before they can be used. Click the green plus sign (+) to add and register a new token into the system.

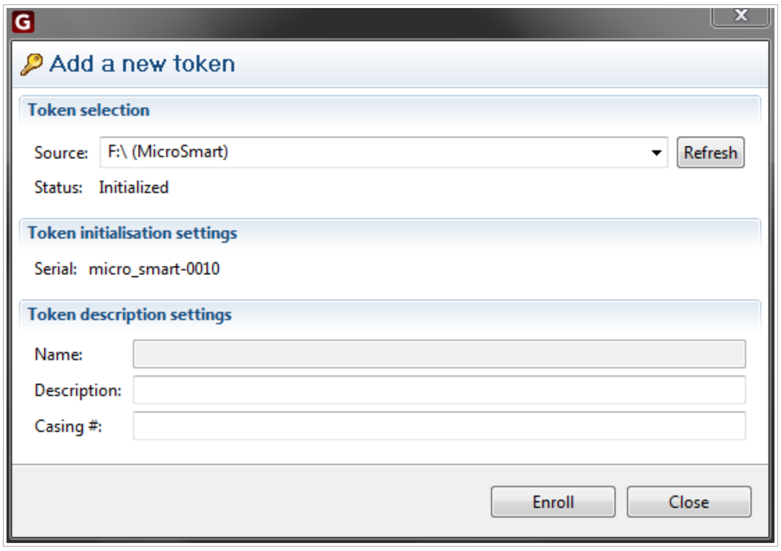



### Register a Personal Token

1. Select the **Personal Token Assignment** button from the perspective selector.
2. In the Token listing click the plus sign (+) to **enroll a new token**.

   A: **Insert the token** into your local workstation and click the **refresh** button.

   B: Click the **enroll** button to register the token into the system.
3. **Drag the new token** into the rule listing from the token listing.
4. From the **User Listing** drag a user into the rule view to register that the token should **identify** that user.
5. From the **Personal Token Status listing** select the element called **'Personal Token'** and add it to the rule.
6. Click the **'Save and Close'** button to save the new rule.




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 the Enroll button to register the token. Repeat this step with as many tokens as you like.

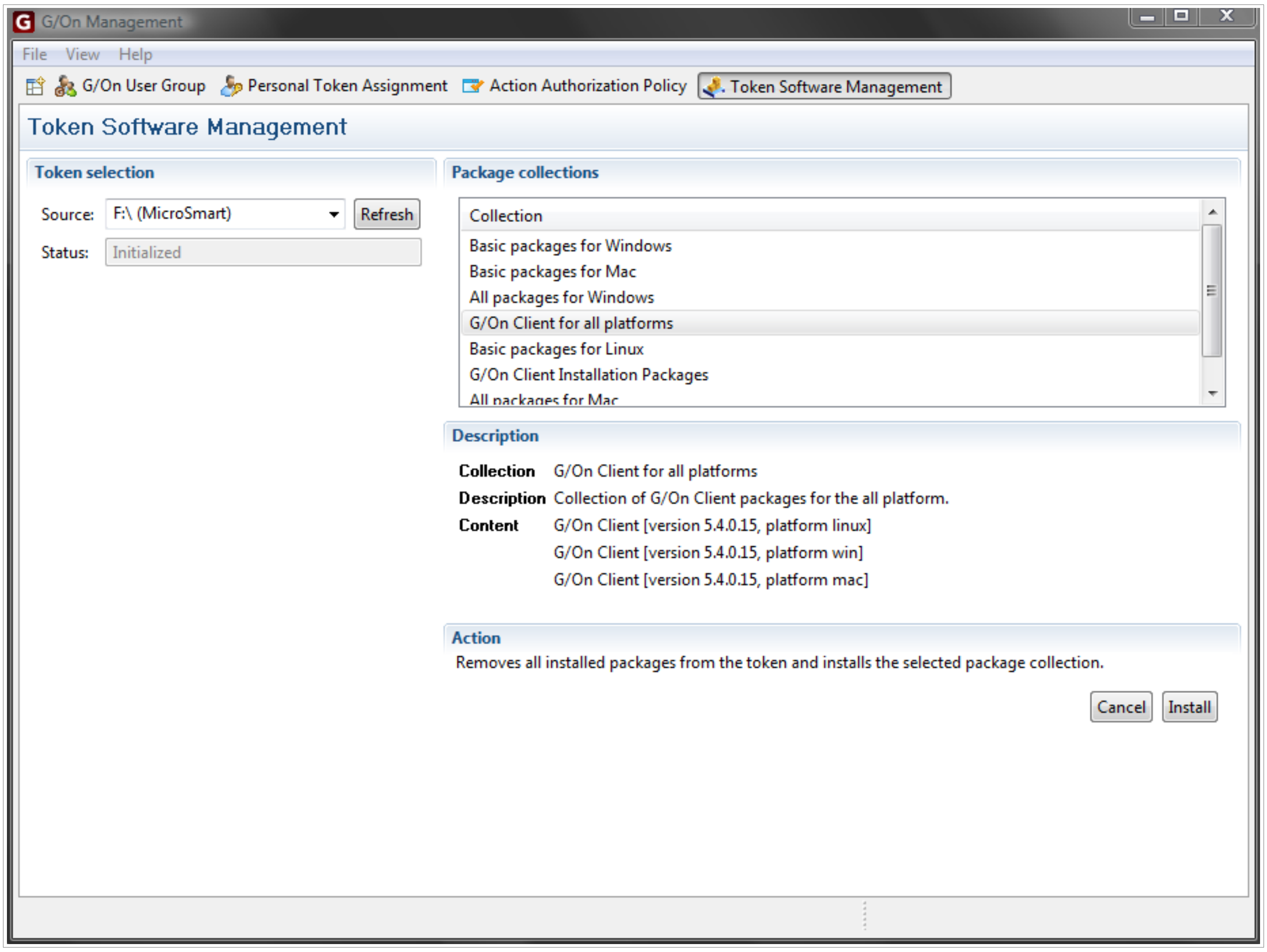
The Personal Token Status tab contains an element called 'Personal Token'. This is a special token group that holds tokens that are assigned to a specific user and only that specific user.

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 Listing area on your right to start creating a new rule. A Rule Editor appears at the bottom right. From the Users Listing on the left you can then drag a user into the rule view. Finally add the 'Personal Token' into the rule editor and click the save and close button. The rule now appears in the rule listing.

**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.

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

**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.

**Adding Token Software**

1. Select the **Personal Software Management** button from the perspective selector.
2. **Select a token** from the source listing. Click refresh if it does not show.
3. **Select a package collection** to add to the token depending on user needs.
4. **Click the install button** to add the collection to the token.

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 the Install button to start installation.

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

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