

Volume

3

OPCAT SYSTEMS

Vision

Security Add-on

OPCAT SYSTEMS

VISION Security Add-On

© OPCAT Systems (D.H) Ltd
Version 15-2-11

Table of Contents

SECURITY ADD-ON	1
1. DATABASE CONFIGURATION	1
2. UPDATING VISION VERSION	1
3. INSTALLING THE SECURITY ADD-ON.....	2
4. USING THE SECURITY ADD-ON	4
4.1 RUNNING THE SECURITY ADD-ON	4
4.2 CREATING NEW USER	5
4.3 EDITING USER DATA	7
4.4 RESET DATE	8
4.5 RESET PASSWORD AFTER FAILED ATTEMPTS	8
5. ADVANCED CONFIGURATION	8

Security Add-on

The Security Add-on provides improved security and less complicated user creation and editing process. The Security Add-on shall be installed on the server and used by the administrator. This guide assumes that a previous version of Vision is running properly on the server. Please make sure that this is true before starting the installation according to this guide.

1. Database Configuration

In order for the Security Add-on and the Life Cycle Module to work, we first must configure the database. For this purpose open Command Prompt.

- Change the directory to the location of the installation files
- Type **mysql -u root -p -h <Server IP>** {IP of your server – if installing from your server the address is 127.0.0.1}
- Enter your Mysql password
- You will get mysql prompt
- Type **source groups.sql** >Enter
- Type **source users.sql** >Enter
- **quit**

We are now done with the configuration of the Database

2. Updating Vision Version

The changes for the Security Add-on requires you to update Vision. To update Vision do the following:

- Copy the *server.properties* file usually found at *C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\Vision\conf* to your desktop
- Now stop Tomcat service
- Delete *Vision* directory found at *C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps*
- Copy *vision.war* from the installation directory to *...\Apache Software Foundation\Tomcat 6.0\webapps*
- Start Tomcat service
- Copy the *server.properties* file from your desktop to *...\Apache Software Foundation\Tomcat 6.0\webapps\Vision\conf*
- Restart Tomcat service

3. Installing the Security Add-on

The Security Add-on is a java based application and thus can run on any OPCAT server machine. The Security Add-on relies on several new entries in the “server.properties” file of Vision.

To install the Security Add-on follow the next steps:

- Open the *server.properties* file usually found at *C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\Vision\conf* using any text editor.
- Copy the following parameters at the end of the *server.properties* text file

```

system.admin.passworddisabledays=999
system.admin.password.login.tofail=5
system.admin.users.file=C:\\svn_repository\\common\\conf\\users
system.admin.authz.file= C:\\svn_repository\\common\\conf\\auth
system.admin.users.file.type=ssl
system.admin.users.shell.cmd=cmd
system.admin.users.shell.cmd.params=/c start
system.admin.users.shell.pass.command.dir=C:\\Program Files\\CollabNet\\Subversion
Server
system.admin.users.shell.pass.command=saspasswd2.exe -u Local -f
C:\\svn_repository\\Systems\\conf\\sasldb <USER>
system.admin.users.shell.pass.length=10
system.admin.users.shell.pass.alphabet=ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
klmnopqrstuvwxyz1234567890
system.admin.users.shell.pass.alphabet.pre=ABCDEFGHIJKLMNOPQRSTUVWXYZ12345
67890
system.admin.users.shell.pass.alphabet.sup=abcdefghijklmnopqrstuvwxyz1234567890
system.admin.users.shell.pass.alphabet.must1= abcdefghijklmnopqrstuvwxyz
system.admin.users.shell.pass.alphabet.must2= ABCDEFGHIJKLMNOPQRSTUVWXYZ
system.admin.users.shell.pass.maxrep=1
system.db.type = mysql
system.db.port=3306
system.db.databasename=opcat
system.db.urlseparator=/

```

- In case you changed the default installation directories, you may need to edit the paths specified above accordingly
- Restart Tomcat service
- Copy the *OPCAT_Server_User_Manager.jar* and *OPCAT_Server_User_Manager.bat* into any directory on the server.
- *OPCAT_Server_User_Manager.bat* point to the location of your local *server.properties* file. This file usually found at *C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\Vision\conf\server.properties* . If you installed Vision at a different location, you need to edit the path at *OPCAT_Server_User_Manager.bat* accordingly.

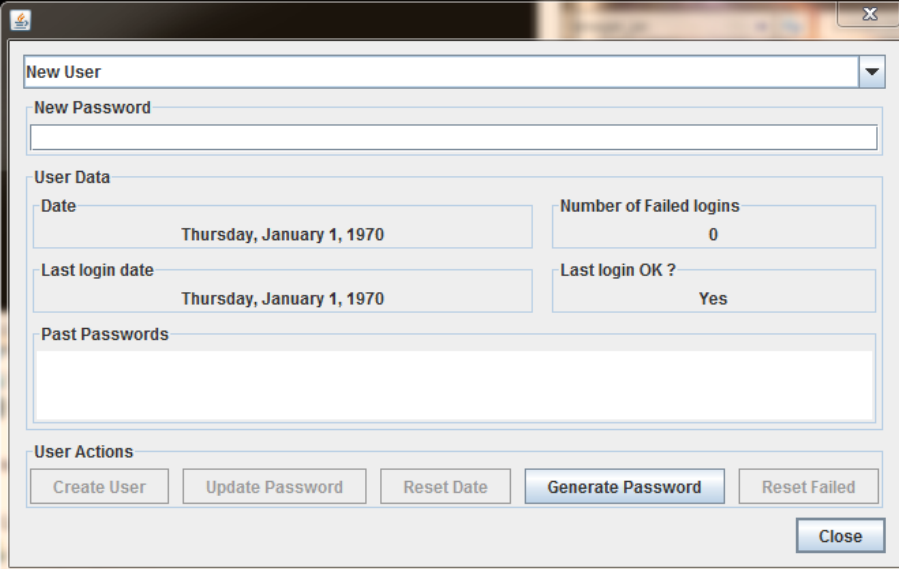
4. Using the Security Add-on

The Security Add-on GUI is used to control the creation of users and passwords for Vision and OPS.

4.1 Running the Security Add-on

To run the Security Add-on double click on the *OPCAT_Server_User_Manager.bat* file.

The following screen will appear:



The screenshot shows a window titled "New User" with a dropdown menu. Below the dropdown is a "New Password" text field. The "User Data" section contains four fields: "Date" (Thursday, January 1, 1970), "Number of Failed logins" (0), "Last login date" (Thursday, January 1, 1970), and "Last login OK ?" (Yes). Below this is a "Past Passwords" text area. The "User Actions" section contains five buttons: "Create User", "Update Password", "Reset Date", "Generate Password", and "Reset Failed". A "Close" button is located at the bottom right.

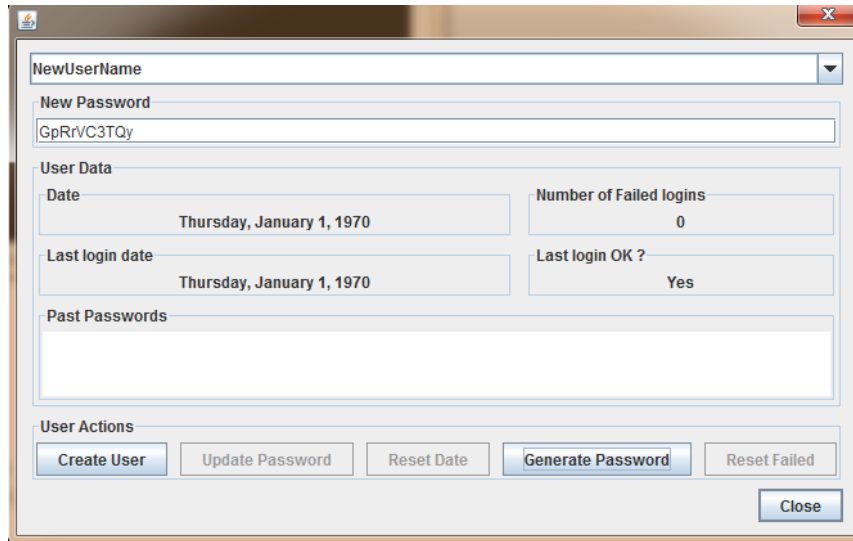
The Security Add-on GUI is divided into 4 main parts:

- **Users drop-down** – a list of the current users and an option to create new users
- **Password field** – this will not contain the current password but only is used to create or change user passwords.
- **User data** – summary of the user data for the user selected at the drop-box.
- **Action buttons** – actions that can be performed by the administrator.

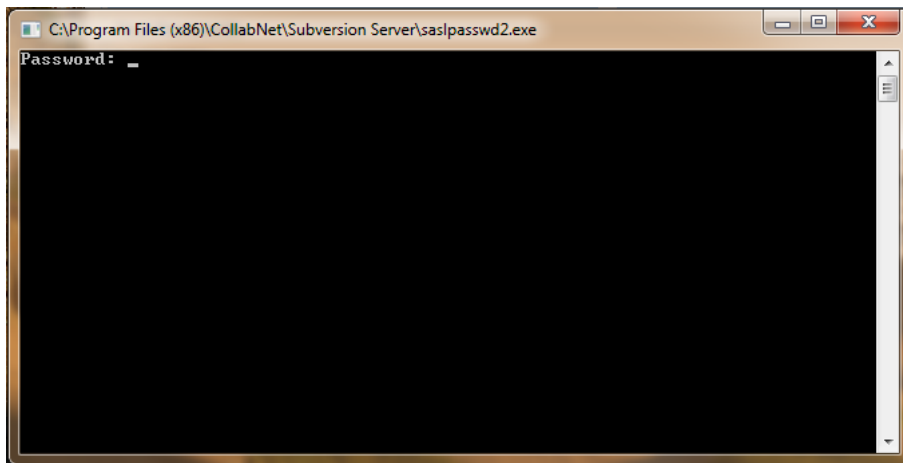
4.2 Creating New User

Each new user needs a user name and a password in order to log into Vision and OPS. In order to create a new user do the following:

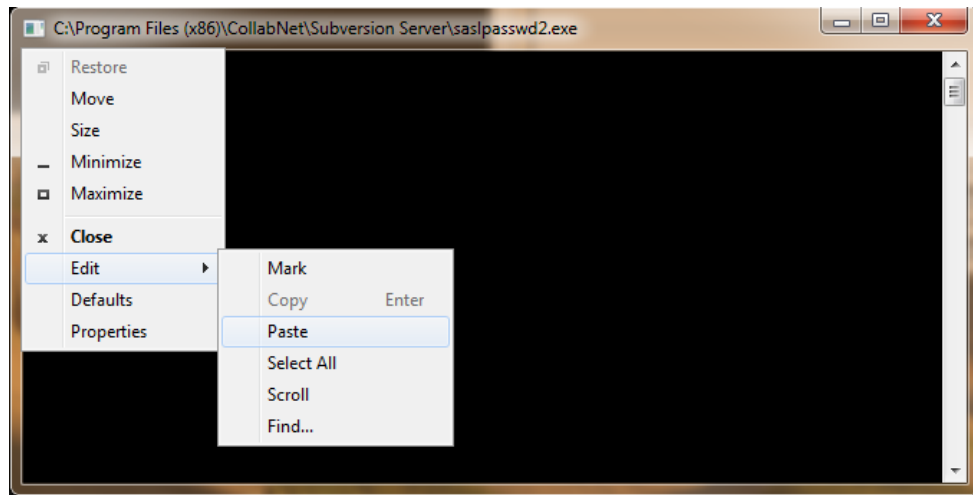
- Type the user name you select at the drop-box.
- Type the required password or press *Generate Password*. If you type a password yourself, it must fulfill the password criteria. Until you meet the criteria the update password will not be lit.



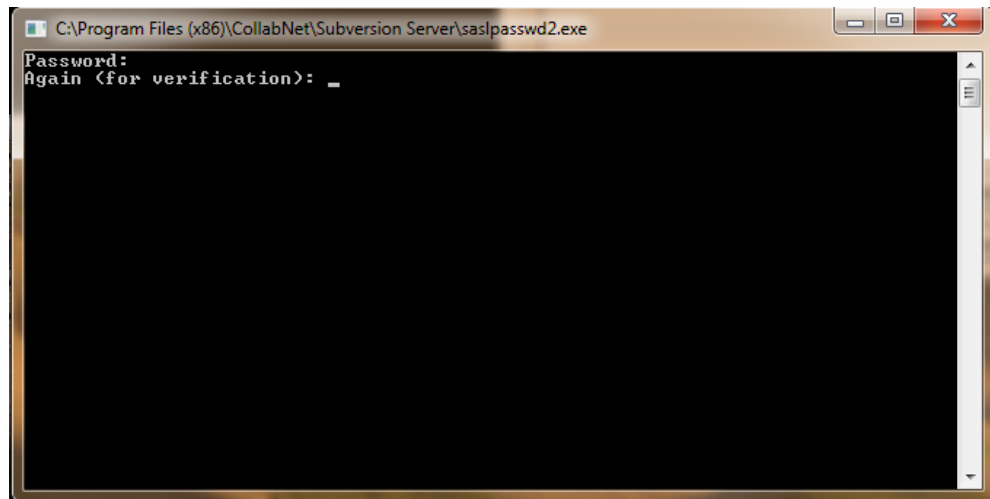
- Type *Create User*. A command prompt will be opened. The password is copied to the clipboard automatically. All you need to do is to paste the password (twice) at the command prompt.



- To past the password to the command prompt right click on the top icon then *Edit* and *Paste*. Next you need to press *Enter*



- Repeat this step again

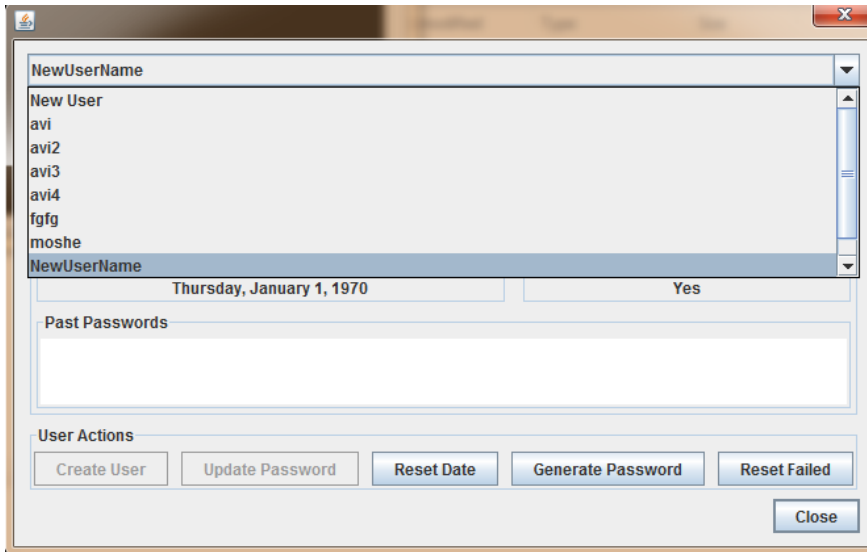


- Now select this user at the Security Add-on drop-box. If the new user is not shown at the drop box then restart the Security Add-on.
- Click on *Reset Date* to reset the date of the password
- Click on *Reset Failed* to reset the number of failures
- Restart *Subversion Service*

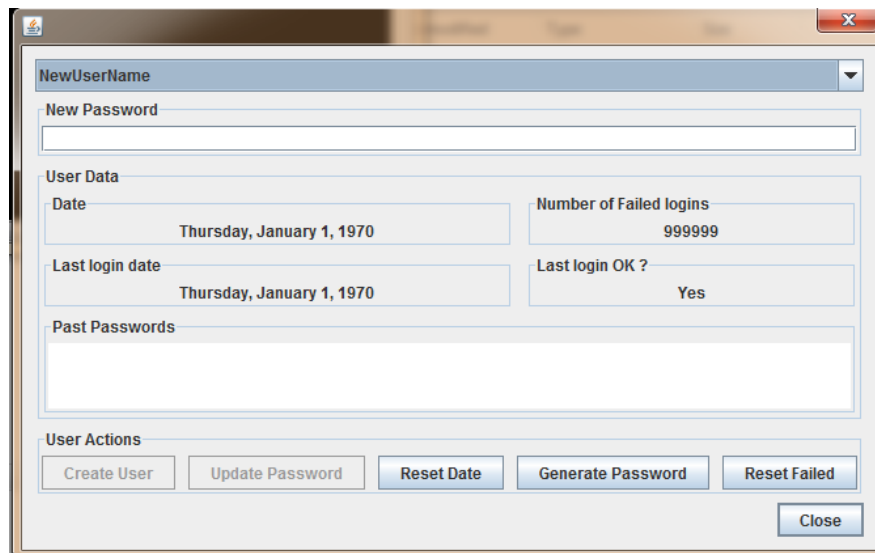
The new user is now ready to start using Vision and OPS. The password is still at the clipboard. You may paste it to an email to be sent to the respected user. The first password you create for a user will not appear at the Past Passwords area until you created another password for the same user.

4.3 Editing User Data

To change the password for existing user do the following:



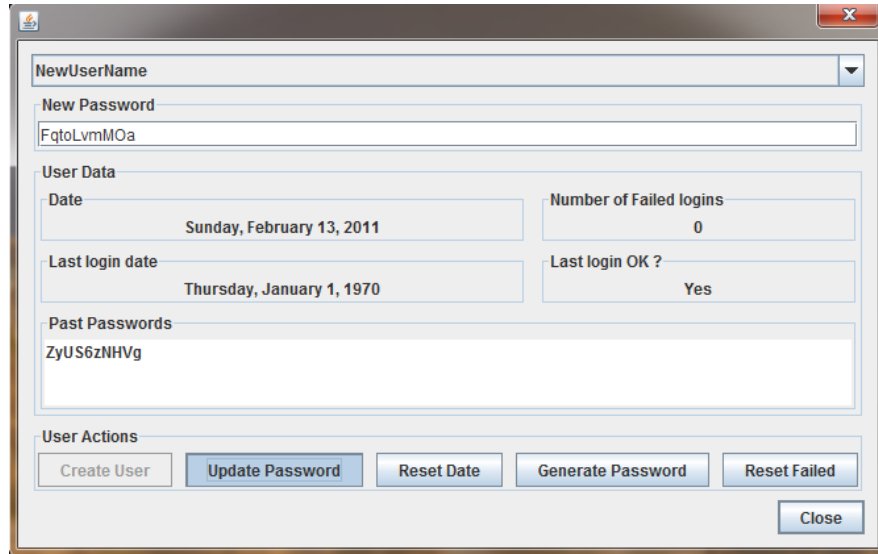
- Type new password or press *Generate Password*



- Press *Update Password*
- Copy the password to the command prompt as explained above.
- Restart *Subversion Service*

4.4 Reset Date

The administrator can re-establish a password that exceeded the expiration date. To do so press the *Reset Date* button.



The screenshot shows a window titled "User Management" with a close button (X) in the top right corner. The window contains several sections:

- NewUserName:** A dropdown menu.
- New Password:** A text input field containing "FqtoLvmMOa".
- User Data:** A section with four fields:
 - Date:** "Sunday, February 13, 2011"
 - Number of Failed logins:** "0"
 - Last login date:** "Thursday, January 1, 1970"
 - Last login OK ?** "Yes"
- Past Passwords:** A text input field containing "ZyUS6zNHVg".
- User Actions:** A row of five buttons: "Create User", "Update Password", "Reset Date", "Generate Password", and "Reset Failed".
- Close:** A button in the bottom right corner.

4.5 Reset Password after failed attempts

If the user attempted to enter Vision or OPS using a wrong password for more than the limited tries set at the *server.properties* file, then he or she will not be able to use this password, unless the administrator reset the number of failures by pressing *Reset Failed* button.

5. Advanced Configuration

At the beginning of this guide, we copied some parameters to the *server.properties* file. Below is an explanation of the different parameters. The administrator may select to change the default settings set above.

- **system.admin.passworddisabledays** – the number of days before a user password expires from the password date which is set in the Security Add-on
- **system.admin.password.login.tofail** – number of attempts before a user is disabled. The failed attempts are counted on the server thus ignoring the machine used. Number of failed attempts for a user is zeroed when the user successfully logs in.
- **system.admin.users.file** – location of the OPCAT Server MC users file
- **system.admin.authz.file** – location of the OPCAT Server MC authorities file
- **system.admin.users.file.type** – type of users file which is decided in the initial installation of Vision. The options are : “text” or “ssl”, usually “ssl” is used.
- **system.admin.users.shell.cmd** – the command in order to execute a shell on the local server.

- **system.admin.users.shell.cmd.params** – parameters to the shell command to execute a command on the server.
- **system.admin.users.shell.pass.command.dir** – location of the MC Server installation directory
- **system.admin.users.shell.pass.command** – command line in order to add the new password to the ssl database if “ssl” option is used in 5.
- **system.admin.users.shell.pass.length** – minimum length of the password
- **system.admin.users.shell.pass.alphabet** – the characters allowed in a password
- **system.admin.users.shell.pass.alphabet.pre** – the characters allowed in the beginning of a password
- **system.admin.users.shell.pass.alphabet.su** – the characters allowed in the end of the password.
- **system.admin.users.shell.pass.maxrep** – maximum repetition of any character in a password.
- **system.admin.users.shell.pass.alphabet.must1**= one of the characters must appear in the password
- **system.admin.users.shell.pass.alphabet.must2**= one of the characters must appear in the password