Hotlist Permit Updater

User Guide
Custom Solutions
Genetec Professional Services Team

Innovative **Solutions**

Genetec

Table of Contents

1 Purpose **3**

2 Document Reviews **3**

3 Overview **3**

4 Installation **3**

4.1 Creation of custom events 3

4.2 Installation of the Raise Custom Event Macro 5

4.3 Creation of the scheduled task 8

5 Configuration **10**

5.1 General Configuration 10

5.2 HTTP or FTP Transfer 10

5.3 SFTP Transfer 11

5.3.1 Configuration 11

5.3.2 Connection mode 12

5.3.3 Username/Password 12

5.3.4 Username/Certificate 12

5.3.5 Username/ Password and Certificate 13

5.4 Backup and Manual download 14

6 Licenses **14**

7 Contacting Professional Services **14**

1 Purpose

The purpose of this document is to explain the numerous features and usage of the Hotlist Permit Updater Plugin.

2 Document Reviews

List of all changes made to this document.

Version	Name	Note	Date
2.0	Carl St-Laurent	Documentation matching V2	2014-10-17
2.0.2	Dumitru Craciunas	Added precisions on the SFTP certificate file	2015-06-09
2.0.3	Shomron Sougang Kamgang	Added Username/ Password and Certificate authentication section	September 1, 2015
2.0.4	Dumitru Craciunas	Added encrypted certificate passphrase	April 6, 2015

3 Overview

This document outline the basic configuration of the plugin.

4 Installation

After installation of the setup package, some preparation steps are needed before the plugin can work properly:

- Creation of custom events
- Installation of the Raise Custom Event Macro
- Creation of the scheduled task

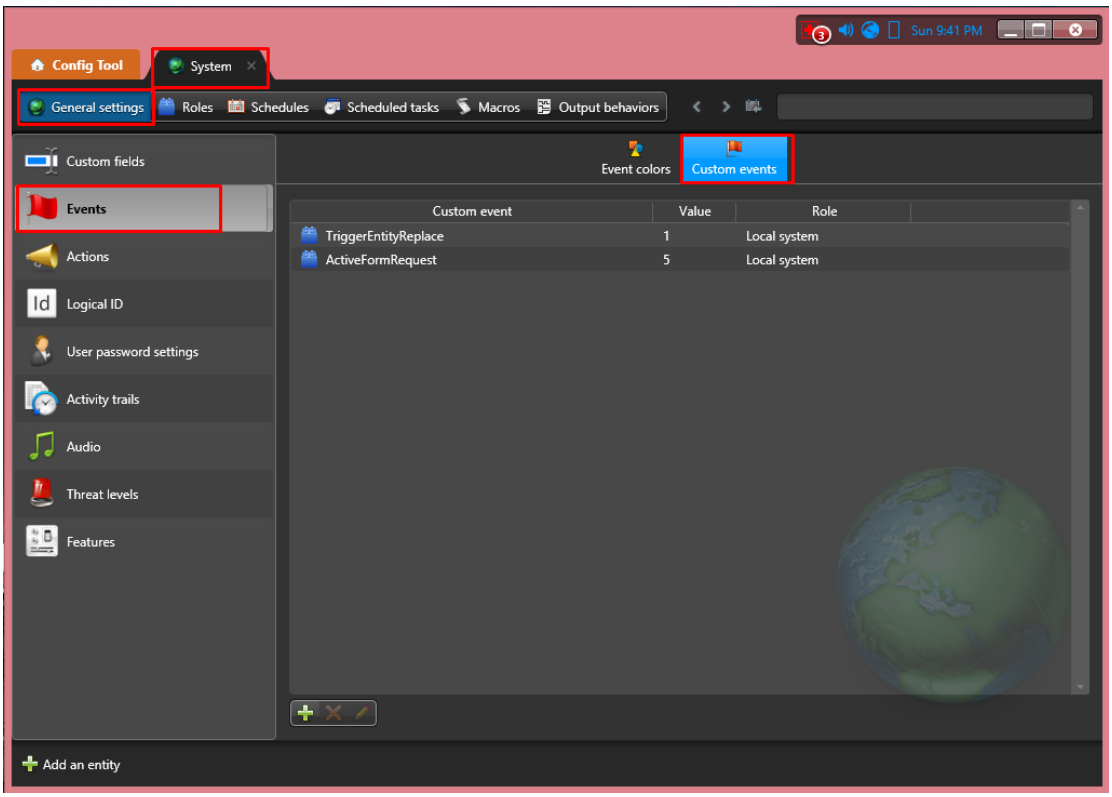
The steps are explained in details in the following sections.

4.1 Creation of custom events

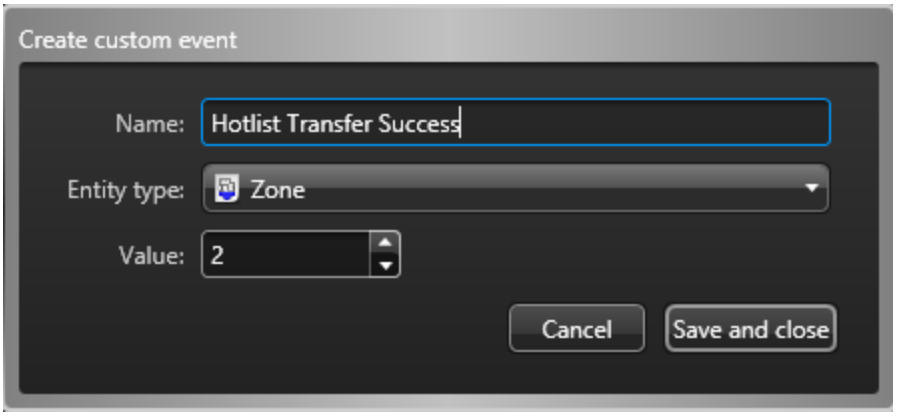
The Hotlist Permit Updater plugin needs 3 different custom to be created for the system to work.

- The transfer success event
- The transfer failure event
- The trigger start transfer event

To create a custom event, open Config Tool and go to the System task in the General Settings section. Click on the Events pane and then, the Custom events tab as shown below:



Click on the + sign and create the 3 events by entering their name. The type and value are not important for the plugin to work but by mean of classification, we will use the Role type:



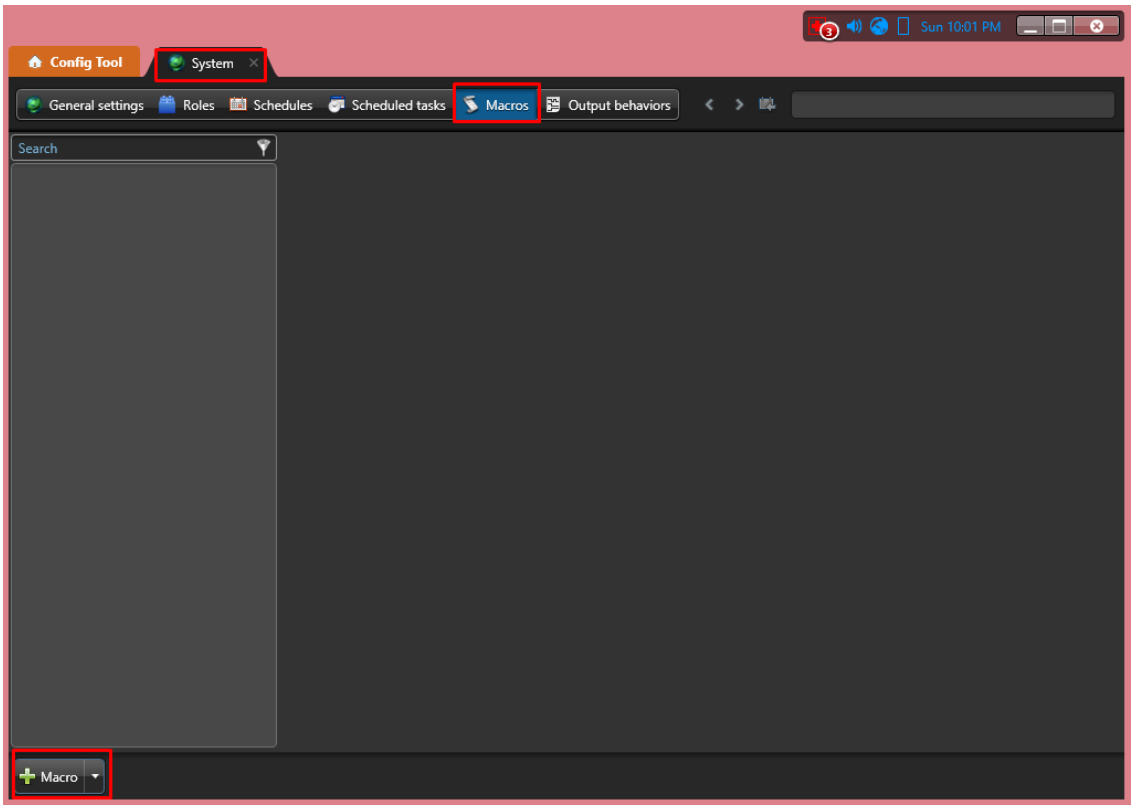
After this step you should have 3 new events to use with the plugin as shown here:

4.2 Installation of the Raise Custom Event Macro

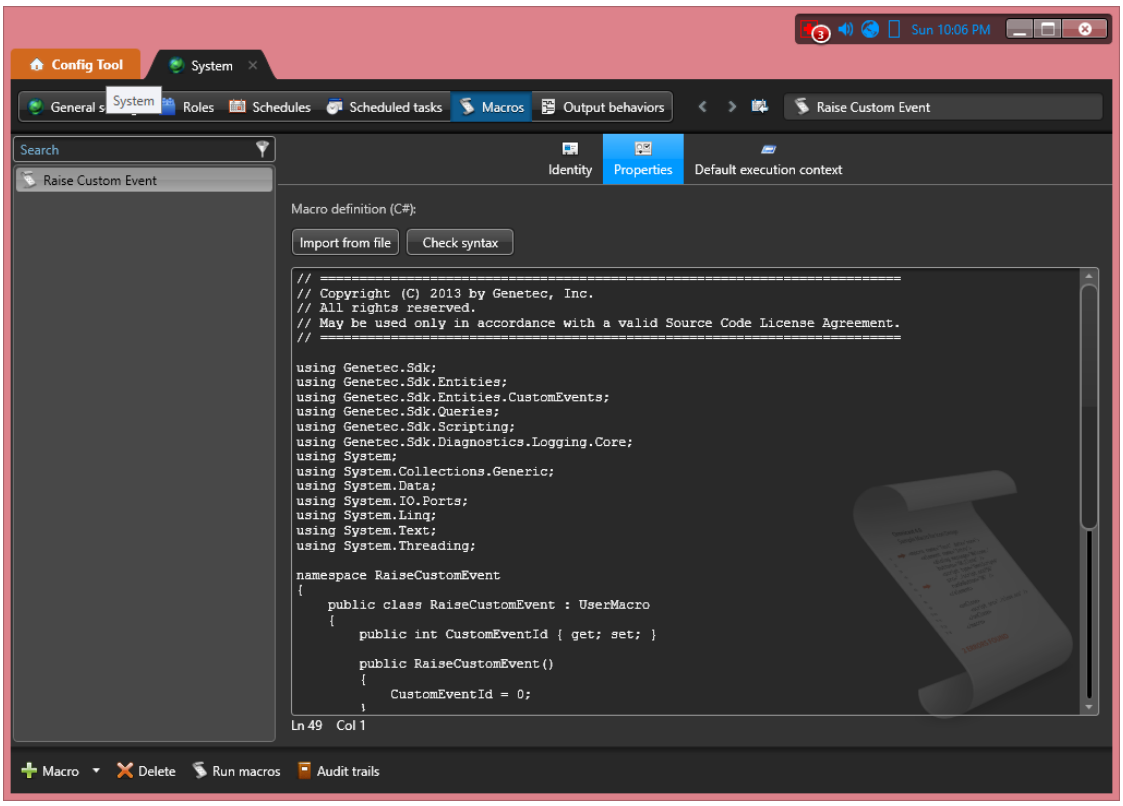
Since Security Center cannot directly trigger a custom event from a schedule task, a small macro need to be installed to link the schedule task to the custom event.

A small text file named RaiseCustomEventMacro.txt is included in the setup package and need to be installed in the system.

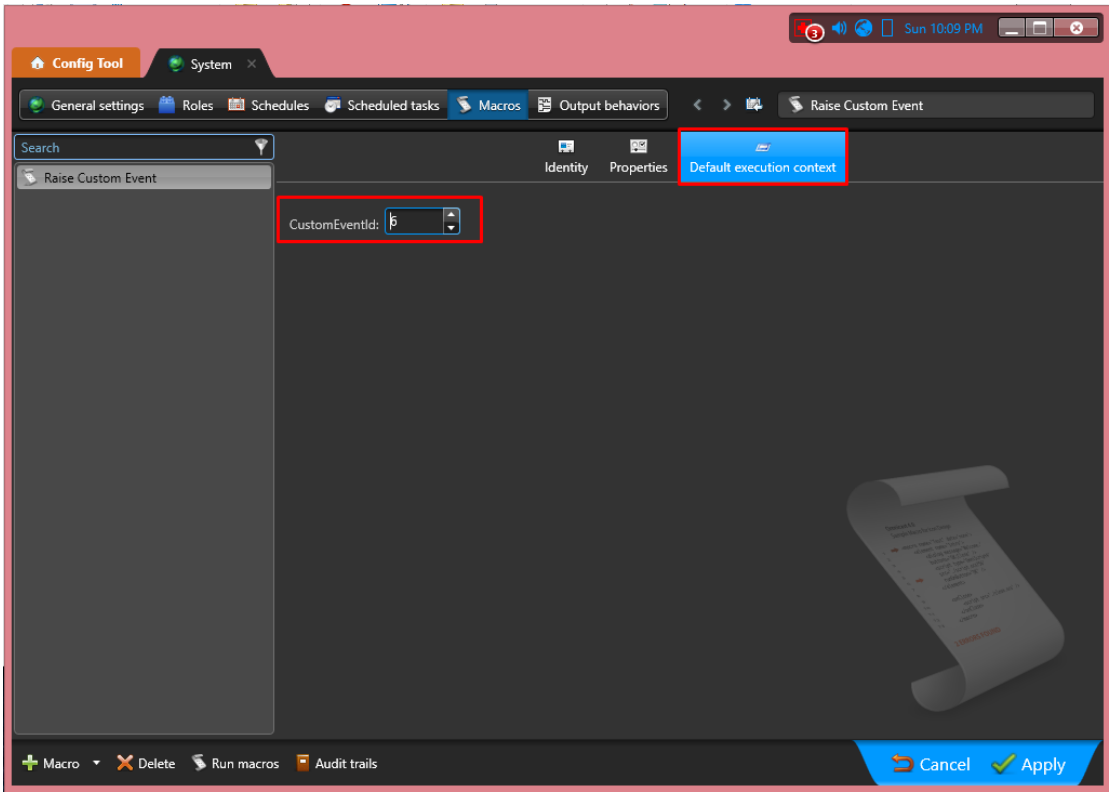
To create a new macro go to the Macro section from the System task and click the + button:



Enter a friendly name such as “Raise Custom Event” to the new macro click next and accept the creation. Go to the Properties tab and replace all the content by the text from the macro file included in the setup package:

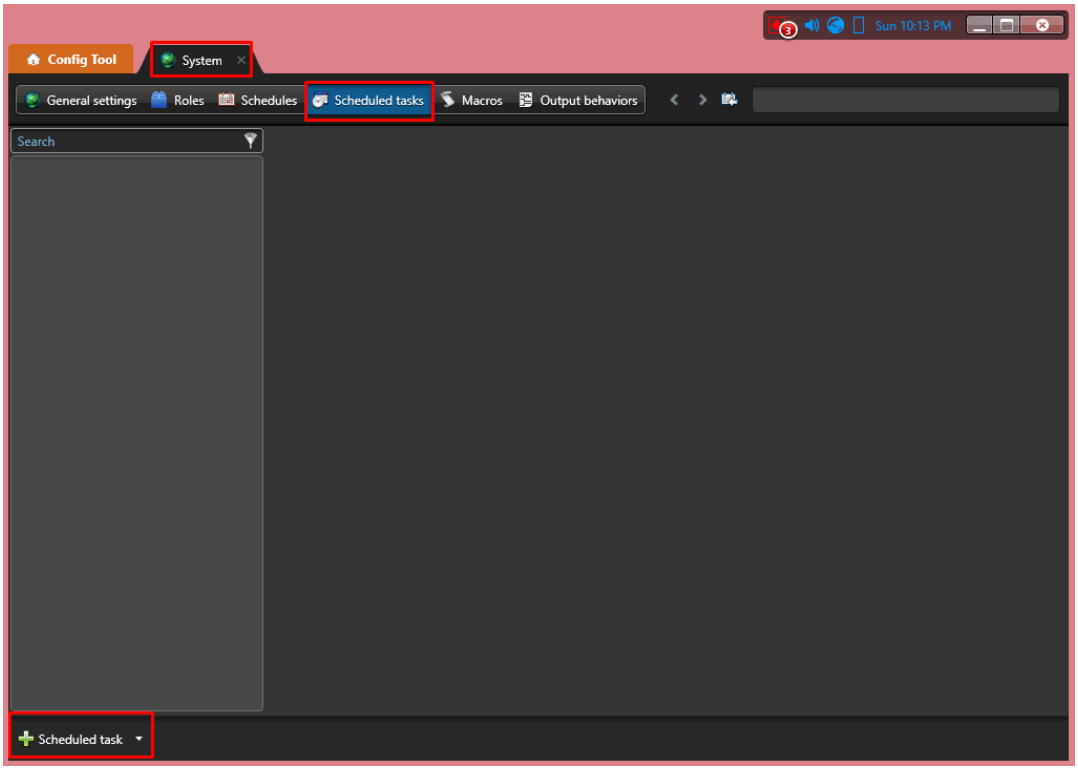


After text has been replaced, go to the Default execution context and modify the CustomEventId for the Hotlist Start Transfer Trigger event Id (Id 6 if we refer to the event previously created):

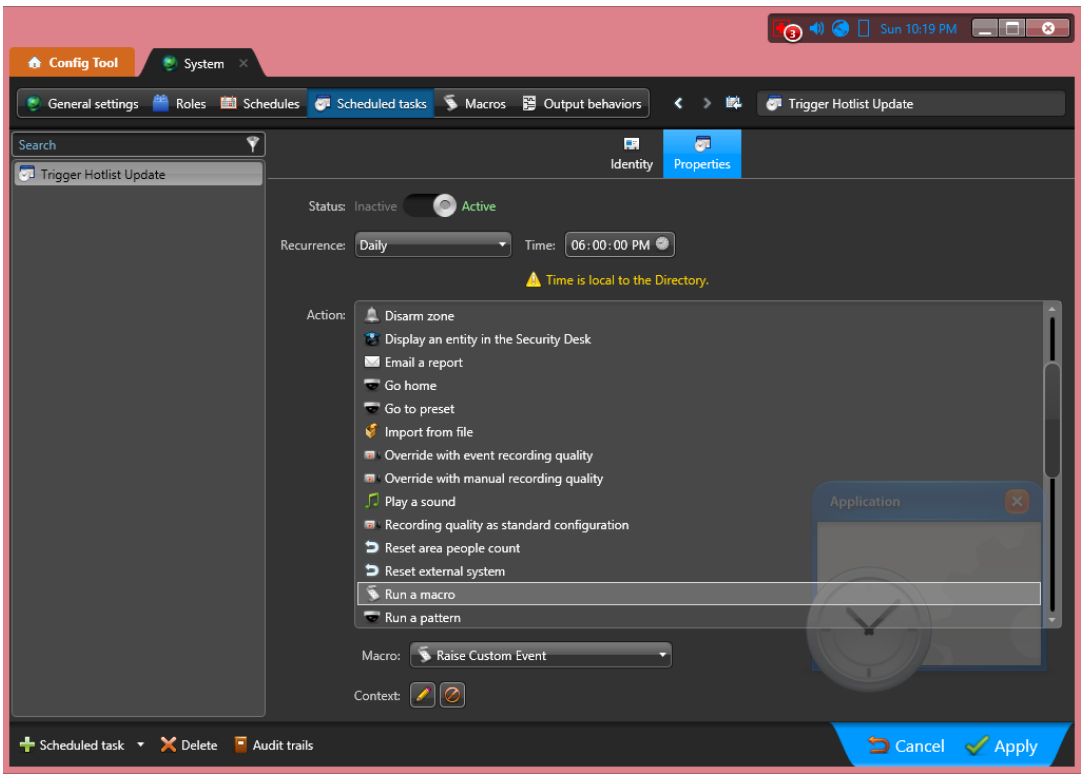


4.3 Creation of the scheduled task

To create a scheduled task, go to the Scheduled tasks section of the system task and click the + sign:



Give the task a friendly name such as Trigger Hotlist Update set its status on active, select the wanted type of Recurrence and select the “Run a macro” Action. Then, select the newly created macro and save the settings:

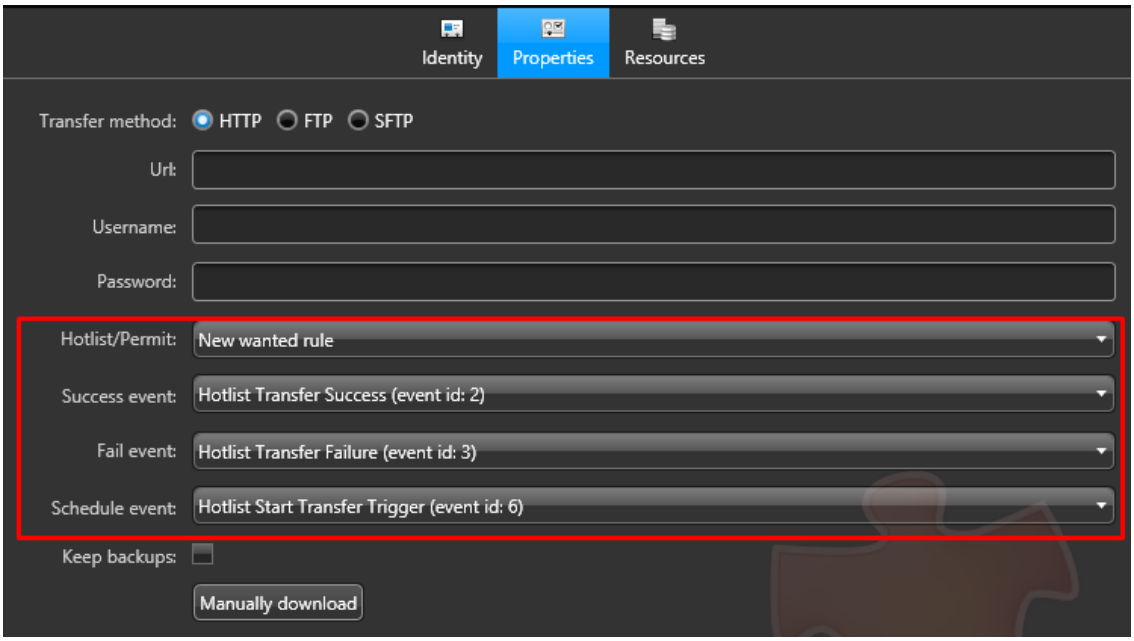


5 Configuration

5.1 General Configuration

To install the plugin, go to the Plugins task in Config Tool and click the + sign. Select HotList Permit File Updater and accept the selection.

Go to the Properties tab and enter the wanted Hotlist of Permit, select the different corresponding events and save the configuration. The page should now look like this:

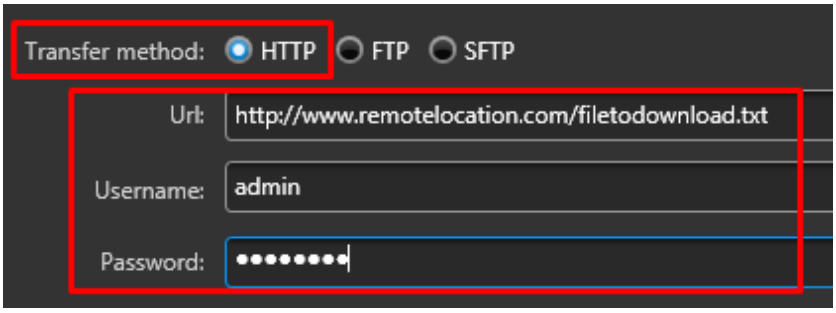


The preferred transfer method and its configuration will be done in the following sections.

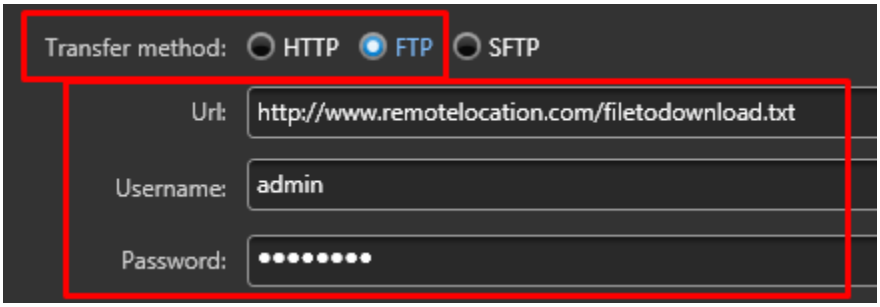
5.2 HTTP or FTP Transfer

Since HTTP and FTP uses similar logic both of them can be configured in the same way.

To use HTTP select with the transfer methods selector and enter the remote URL where the file to download is located:



And for FTP:



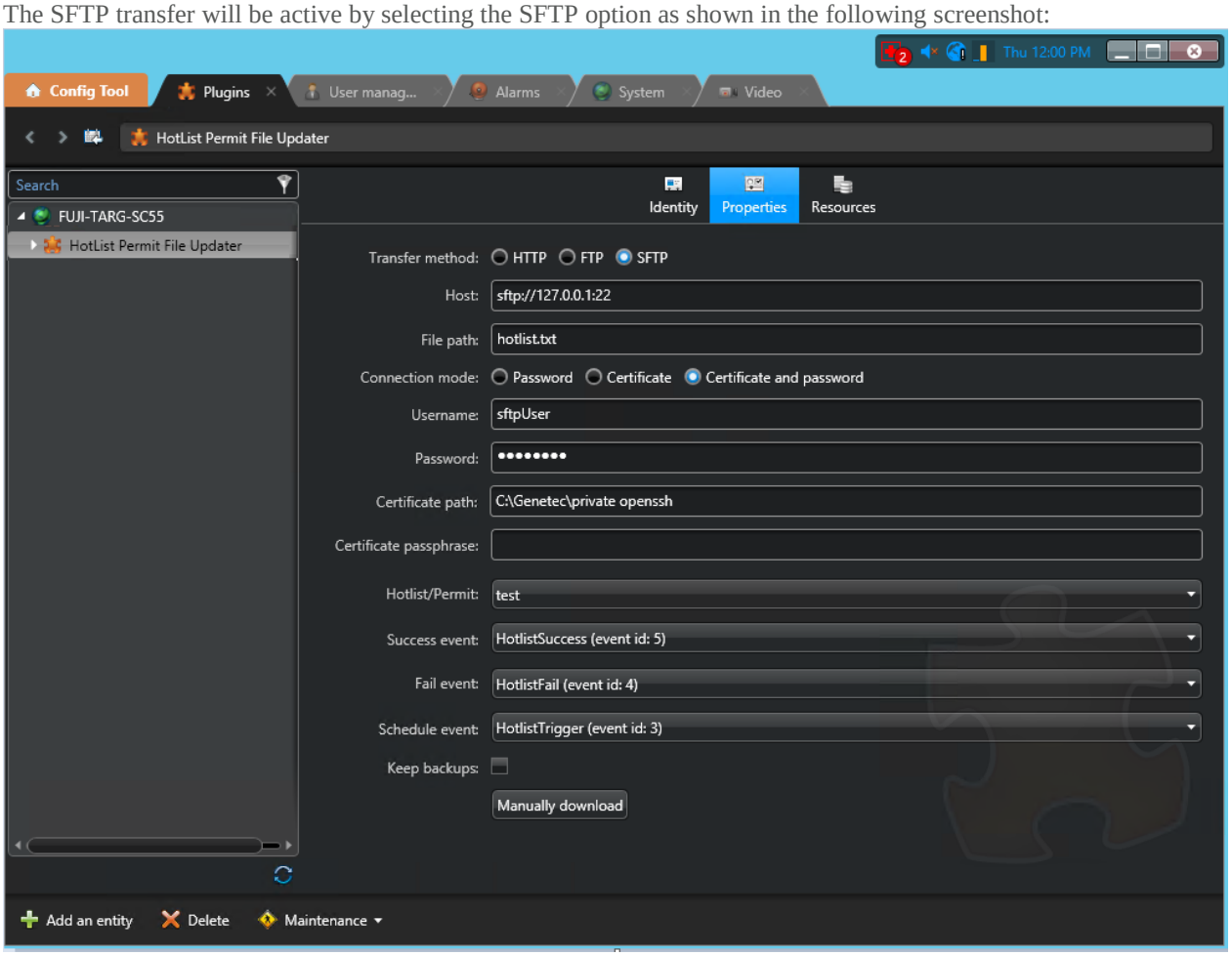
Please make sure to specify the protocol extension in the URL. Use http:// for the HTTP protocol and ftp:// with the FTP protocol

It is possible to enter credentials if needed. If the source is not secured using a username and password leave fields blank.

5.3 SFTP Transfer

5.3.1 Configuration

The SFTP transfer will be active by selecting the SFTP option as shown in the following screenshot:



It is now possible to enter the Host and the Remote File path for the download.

The host can be entered using the following formatting:

- sftp://(hostname or IP):(port)
- sftp://(hostname or IP) → Not specifying the port will use the default port 22
- (hostname or IP) → Not specifying the protocol in the host name will still use SFTP

If the hostname do not resolve an IP address by a DNS query, the plugin will be in an error state.

The file path is relative to the home directory of the connected user on the SFTP server.

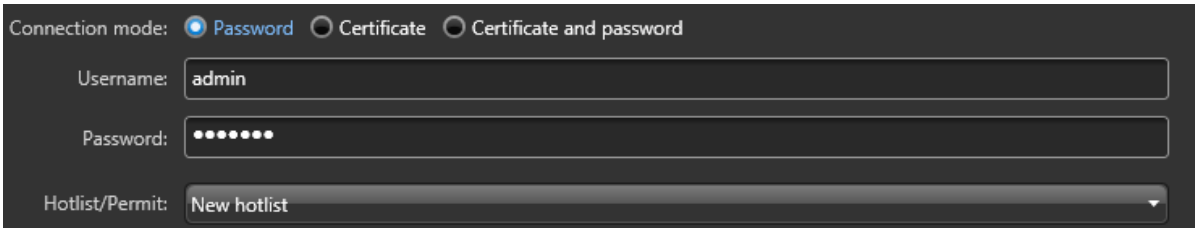
The Hotlist/Permit selection and all events is using the same configuration as the HTTP or FTP transfer

5.3.2 Connection mode

To support the full SFTP feature set, two connection mode are offered: Password or Certificate.

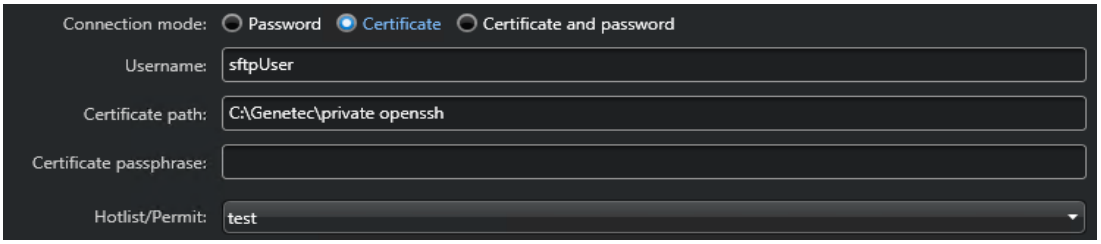
5.3.3 Username/Password

The Username/Password mode is similar the FTP connection mode but provide the secure transfer of SFTP. To use this connection mode, select the Password connection mode on the screen and provide a valid Username and associated password to connect to the server.



Please note that some SFTP server do not allow or support Username/Password authentication. If that is the case, use the following method.

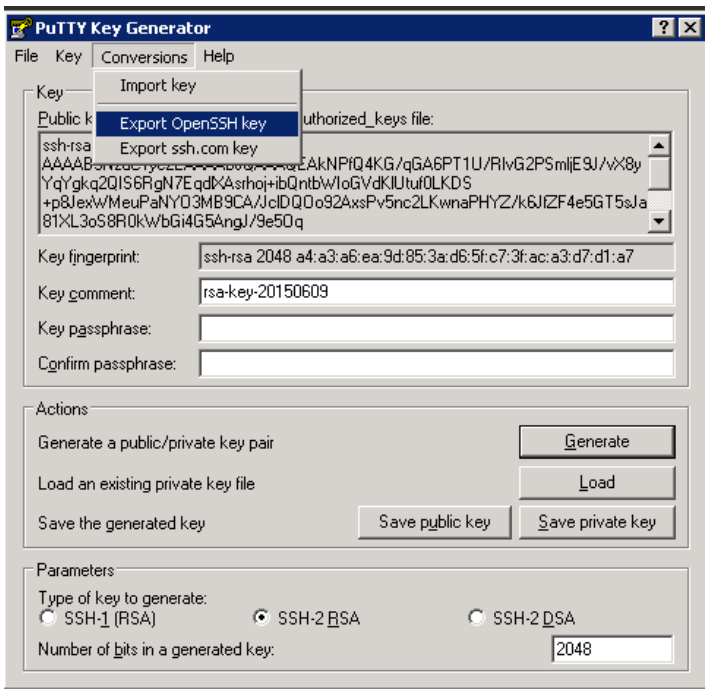
5.3.4 Username/Certificate



The certificate authentication method is more secure than the password as a way to authenticate to a SFTP server. To use this method, select the Certificate connection mode and enter the username you wish to use. The certificate path is where the certificate file associated with the user is located. Please note that the certificate must be located on the server the plugin is running on and not the computer from which Config Tool is used – The path must also reflect the location of the file on the server.

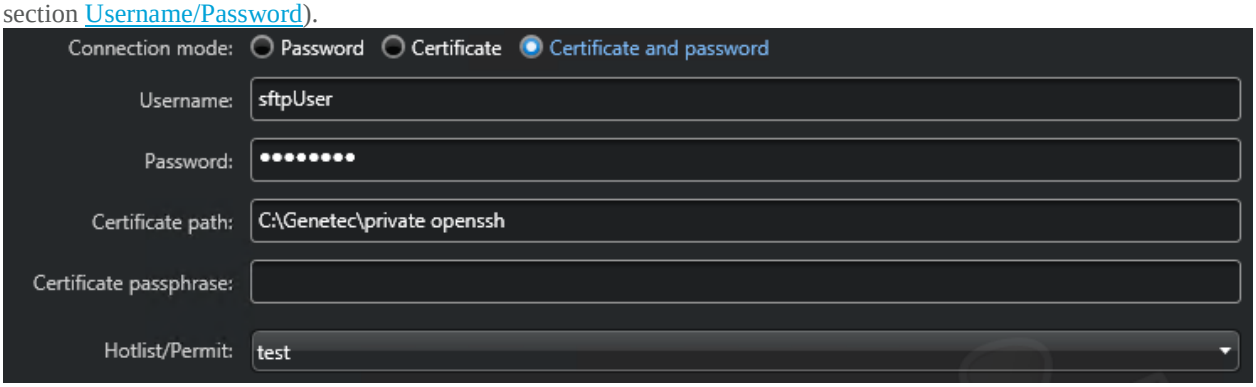
The certificate file should contain a private key in an OpenSSH format. SSH-2 keys are supported. Note that SSH-1 keys are unsafe and unsupported by the OpesSSh format. The certificate passphrase should be entered if the private certificate key is encrypted.

A SSH-2 private key in a *.ppk format can be converted to an OpenSSH key format using, for example, *PuTTY Key Generator*. Load the *.pkk key into *PuTTY Key Generator* then exported it to OpenSSh using the *Conversions* menu.



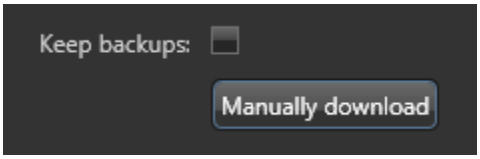
5.3.5 Username/ Password and Certificate

The password and certificate authentication method is most secure way to authenticate to a SFTP server. It involves setting up a certificate (refers to section Username/Certificate) and at the same time providing a password (refers to section Username/Password).



5.4 Backup and Manual download

This section is about the backup options and the manual download button:



If the Keep backups is selected, it will create a backup of the currently existent hotlist file before downloading the new one. It will use the original name + the current date and time + the .bak extension as a format (Ex.: “hotlist2.tbl” → “hotlist2.tbl 04-12-2012 11h10m55.bak”).

The manual download button can be used to trigger the download right away. This can be used for testing purposes or when is it not possible to wait to the next scheduled download.

6 Licenses

The Hotlist Permit File Updater requires a valid license for GSC-CUSTOM-HOTLISTPERMITFILEUPDATER.

7 Contacting Professional Services

Please contact:

Ilya Naduev
Custom Solutions Project Manager
inaduev@genetec.com