RiskMatch

Partner Broker Data Connectivity Overview

Table of Contents

1 Overview

This document provides an overview and the requirements for loading data onto RiskMatch® platform.

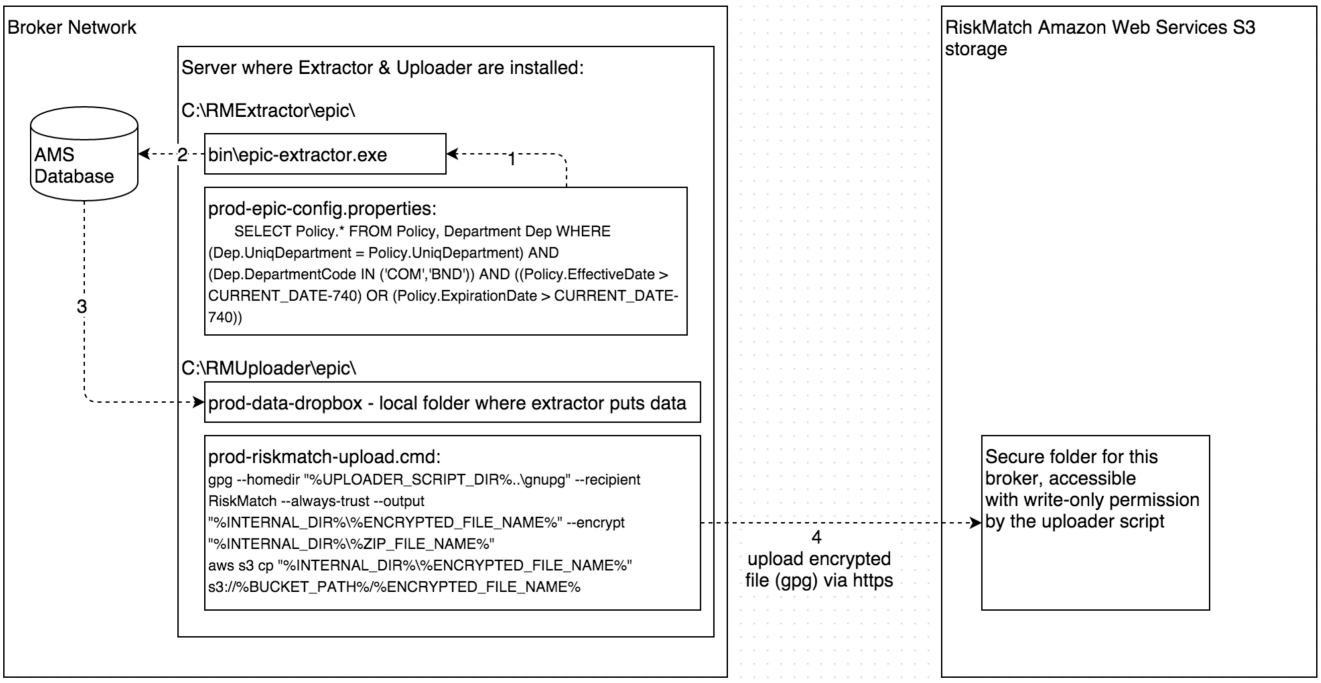
2 In a Nutshell

RiskMatch provides Broker IT with a **turn-key** solution consisting of two components: 'Extractor' and 'Uploader'.

Extractor is installed by Broker IT on one of the Broker's servers having connectivity to the Agency Management System's database. Extractor is pre-configured to run a set of SQL queries to extract required information. The extracted information is stored locally on the Broker's server.

When information is extracted, the Extractor will invoke **Uploader** (typically installed on the same server) to encrypt the extracted information and to upload it to RiskMatch servers. This is a 'push' solution from Broker infrastructure point of view.

There is no need for Broker IT to engage in any custom feed development. ***All SQL queries performed by the Extractor are visible to Broker IT, as well as the encryption steps taken by Uploader***.



Process flow:

1. Extractor executable reads plain-text configuration file with the SQL queries
2. Extractor runs the queries against AMS database server
3. Extractor stores the extracted information locally
4. Uploader (plain-text windows .cmd script) zips the folder, encrypts it, and uploads to secure location on Amazon Web Services

3 Extractor

3.1 Installing RiskMatch Extractor

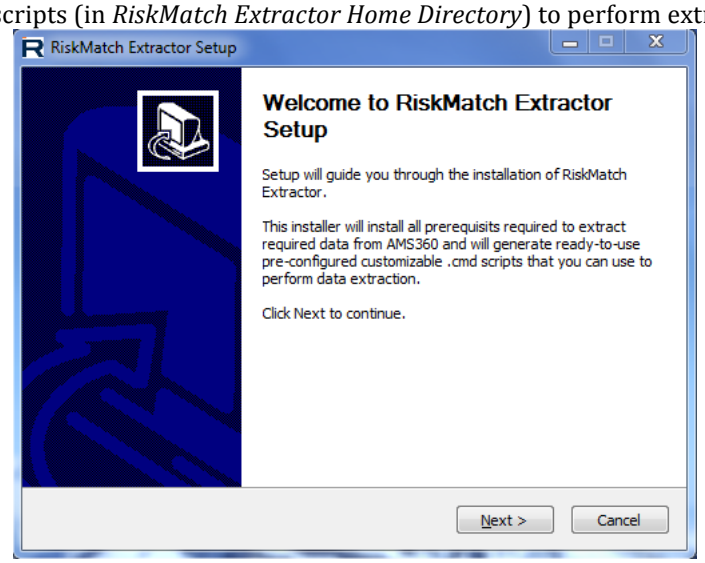
RiskMatch Extractor installer creates **ready-to-use** windows .cmd scripts that will perform all the steps required to extract the data from Agency Management System(s).

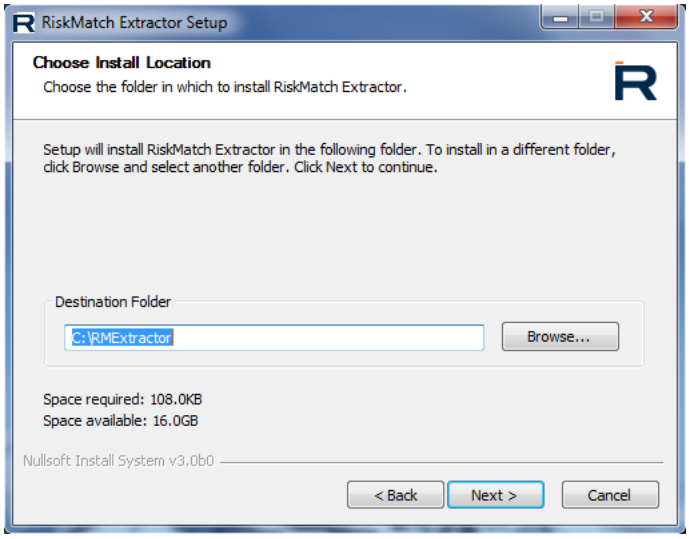
Privileged & Confidential Information: Not for distribution. US pat. 9,165,324 and pat. 8,666,788

Your IT team will receive an executable installer from RiskMatch IT team, generated specifically for your broker company and for the specific type(s) of your Agency Management System(s) (AMS360/EPIC/Sagitta/Vision/TAM).

One launched, the installer will perform the following actions:

1. Create a directory we will refer to as '*RiskMatch Extractor Home Directory*' in this section (we recommend using the default location of 'C:\RMExtractor')
2. Generate .cmd scripts (in *RiskMatch Extractor Home Directory*) to perform extraction of the data.





3.2 Using RiskMatch Extractor

Under *RiskMatch Extractor Home Directory* there is an individual directory for each instance of the Agency Management System to extract the data from. The types and quantities of each Agency Management System would have to be provided to RiskMatch IT in advance and the custom-built extractor will have everything pre-configured.

For each Agency Management System the folder will contain the following:

- **bin** (directory) – contains the executable
- **prod-configuration.properties** – contains all the parameters for the extractor, including SQL queries to be executed and the directory where to store extracted data
- **prod-credentials.properties** – contains the SQL Server connectivity information: name of the server, name of the database in SQL Server, and login/password for SQL Server authentication (in case Integrated

Privileged & Confidential Information: Not for distribution. US pat. 9,165,324 and pat. 8,666,788

Security is used login/password section can be blank). This file is populated by the Broker IT, RiskMatch does not need to know any of the connectivity details or credentials.

- **prod-extract.cmd** – will run the extractor and will store the extracted files in the directory specified in prod-configuration.properties file. This script does not upload anything to RiskMatch.
- **prod-extract-upload.cmd** – will run prod-extract.cmd and then will invoke the Uploader to encrypt the data and upload it to RiskMatch servers. This is the file that will be scheduled by Broker IT to run on a daily basis (typically during the night).

Note: in the same directory you will see similar files whose names start with 'test' instead of 'prod'. These files will be used in case further customization is required (for example SQL queries are added/changed) but the changes must be tested prior to applying them to what is currently is the 'live' configuration of the extractor (in 'prod' files)

3.3 What Is Extracted By The Extractor

The full list of extracted data tables is specific to the Agency Management System and to the Broker, and can be found in prod-configuration.properties configuration file of the Extractor. On a high level, the following entities are extracted:

Policy

Only the Commercial Property & Casualty policies:

- All bound policies that are:
  (a) Currently inforce, or
  (b) Started or expired after 1/1/2014

Endorsements/Transactions

Changes or amendments to the policies.

Client

Client and name insured referenced by the extracted policies.

Party

This consists of information about entities that the broker does business with, or has a relationship with. It can be the insurer, issuing paper, pay-to, wholesaler, MGA, MGA-wholesaler, captive, syndicate etc.

Person

Personnel working for, or on behalf of the broker organization, like the account executive, specialist etc.

Various Reference Data

Various metadata such listing of Lines of Business, Offices, Departments, Agencies, types of Transaction Codes etc.

3.4 Requirements

Extractor can be run on the following operating systems:

- Windows 7 (32 and 64 bit)
- Windows 8 (32 and 64 bit)
- Windows Server 2003 SP2 (32 and 64 bit)
- Windows Server 2008 (32 and 64 bit)
- Windows Server 2008 R2 (64 bit)
- Windows Server 2012 (64 bit)
- Windows Server 2012 R2 (64 bit)
- Windows Server 2016 (64 bit)

Minimum Hardware requirements:

- 2GB of RAM
- 1.2 GHz CPU

Privileged & Confidential Information: Not for distribution. US pat. 9,165,324 and pat. 8,666,788

- 2GB of free space on HDD

Network Connectivity requirements:

- **Epic/AMS360/Vision**: Since extractor will be extracting the data from the Agency Management System(s), it needs to be able to execute SQL queries against the SQL Server storing the Agency Management System's data:
    - The server on which Extractor will be installed **must have network connectivity to the SQL Server** in order to execute SQL queries
        - For AMS360 deployed in the Vertafore cloud, the broker needs to work with Vertafore to purchase and configure necessary VPN equipment to establish VPN connectivity to the SQL server in the Vertafore cloud
        - For EPIC deployed in the Applied Systems cloud, the broker needs to work with Applied Systems to purchase and configure necessary VPN equipment as well as broker-hosted MS SQL Server instance into which Applied will be pushing the replicated data from their cloud SQL Server (Applied Systems refers to this process as BDE – Bulk Data Extract)
    - SQL Server authentication: either via Integrated Security (via OS user – this is the recommended option unless SQL Server is hosted/managed by Vertafore or Applied Systems) or via explicit SQL Server user credentials (since Extractor is installed and configured on Broker's server by Broker's IT personnel, RiskMatch does not need to ever know these credentials)
        - SQL Server permissions: regardless of the sql server authentication, the sql user only needs read-only access to the Epic/AMS360/Vision schema
- **Sagitta**: Extractor uses ODBC connection of UniVerse database
- **TAM**: since TAM is VisualFoxPro-based, the windows user account running the extractor executable must have access to two network directories where TAM stores its data files (names of the directories are: *TAM, APPS*).
    - When configuring extractor, it is recommended instead of mapped drive names to use server share paths (i.e. instead of G:\TAM;G\APPS to specify \\share\applied\TAM;\\share\applied\APPS)

4 Uploader

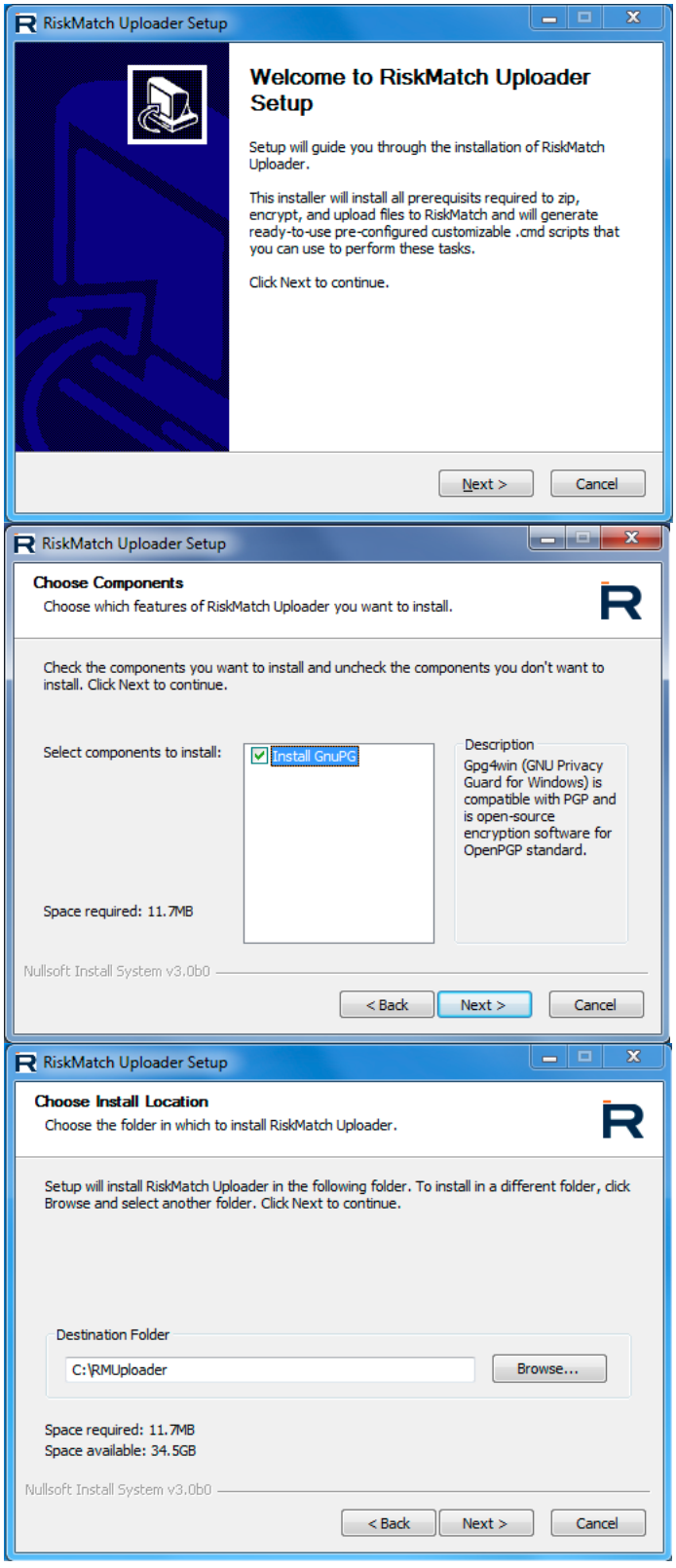
4.1 Installing RiskMatch Uploader

RiskMatch Uploader installer creates **ready-to-use** windows .cmd scripts that will perform all the steps required to zip, encrypt, and upload the file(s) from specific directory to RiskMatch, without you having to configure anything.

Your IT team will receive an executable installer from RiskMatch IT team, generated specifically for your broker company and pre-configured with your security credentials. One launched, the installer will perform the following actions:

1. Install AWS Command Line support
2. Install GnuPG and add RiskMatch public key to its keyring (this step is optional step in case you prefer to use PGP)
3. Create a directory we will refer to as '*RiskMatch Uploader Home Directory*' in this section (we recommend using the default location of 'C:\RMUploader')
4. Put a 7-zip command line executable in *RiskMatch Uploader Home Directory* (this is used to zip files for upload. If you have winzip installed you can change the .cmd script to use winzip if you prefer).
5. Generate .cmd scripts (in *RiskMatch Uploader Home Directory*) with correct security credentials and AWS upload destination so that you can use these scripts right away to upload test files.

Privileged & Confidential Information: Not for distribution. US pat. 9,165,324 and pat. 8,666,788



4.2 Using RiskMatch Uploader

Under *RiskMatch Uploader Home Directory* there is an individual directory for each instance of the Agency Management System to upload the data from. The types and quantities of each Agency Management System would have to be provided to RiskMatch IT in advance and the custom-built Uploader will have everything pre-configured.

Privileged & Confidential Information: Not for distribution. US pat. 9,165,324 and pat. 8,666,788

For each Agency Management System the folder will contain the following:

- **prod-data-dropbox** (directory) – this is a directory where the Extractor will be putting the data file(s) to upload to RiskMatch. There is no need to clean this directory, the Extractor scripts will do that automatically. For you convenience there is a simple prod-clean.cmd script that you can use to clean this directory.
- **prod-internal** (directory) – internal directory used by prod-riskmatch-upload.cmd to prepare the zip file and encrypt it. You don't have to clean this directory, it is done automatically by the script. Basically, just ignore this directory.
- **prod-riskmatch-upload.cmd** – the script to zip, encrypt, and upload the files from prod-data-dropbox directory. This is the script to upload your data to RiskMatch.
- **prod-clean.cmd** – simple script to clean prod-data-dropbox directory

Note: in the same directory you will see similar files whose names start with 'test' instead of 'prod'. These files will be used in case further customization is required (for example, Extractor's SQL queries are added/changed) but the changes must be tested prior to applying them to what is currently is the 'live' configuration known to RiskMatch™ Platform.

4.3 Requirements

The OS/hardware requirements for Uploader are the same as for the Extractor.

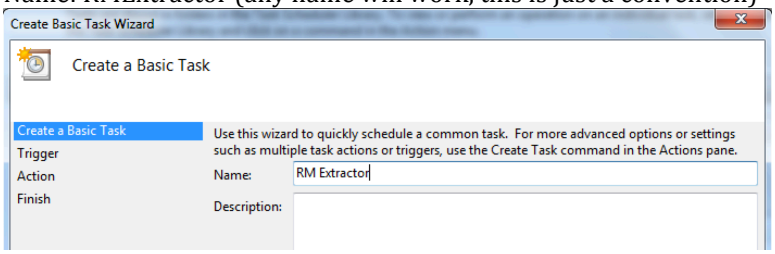
Network Connectivity requirements:

- Outbound connections on TCP port 443 must be enabled for s3.amazonaws.com

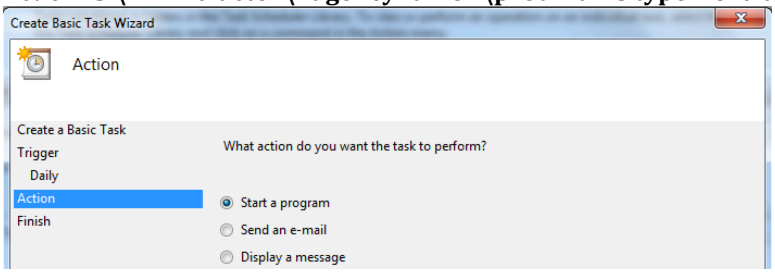
5 Setting Up Automatic Nightly Upload

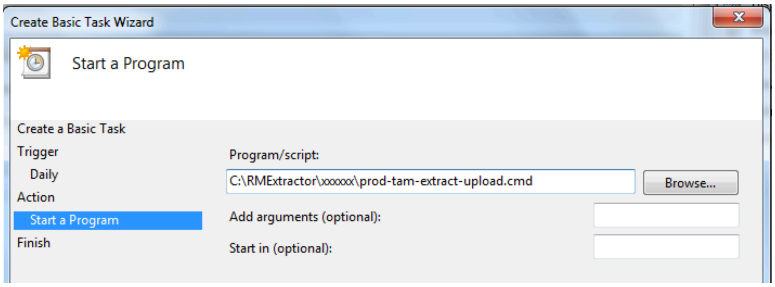
To configure automatic nightly upload to RiskMatch:

1. Using windows task scheduler, set up a daily task (if some UI parameter is not specified below it means use the default value):
    a. Name: RMExtractor (any name will work, this is just a convention)

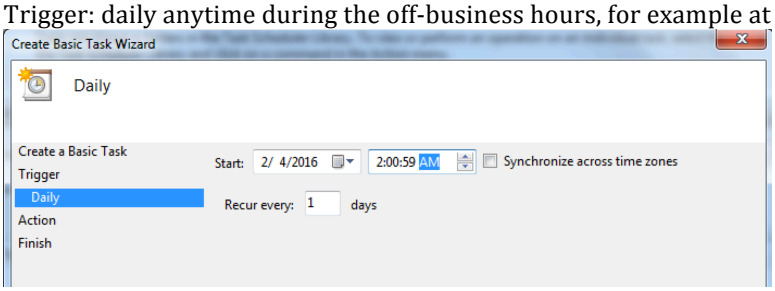


    b. Action: **C:\RMExtractor\<agencyname>\prod-<ams type>-extract-upload.cmd**

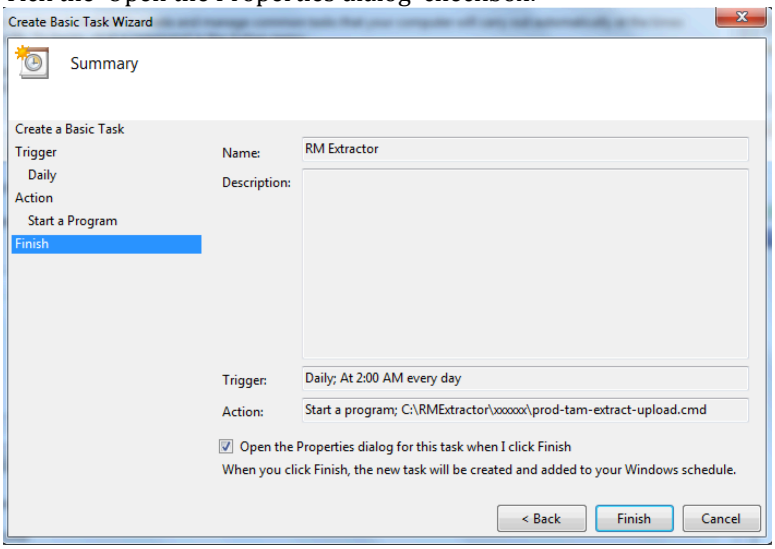




c. Trigger: daily anytime during the off-business hours, for example at 2:00 am

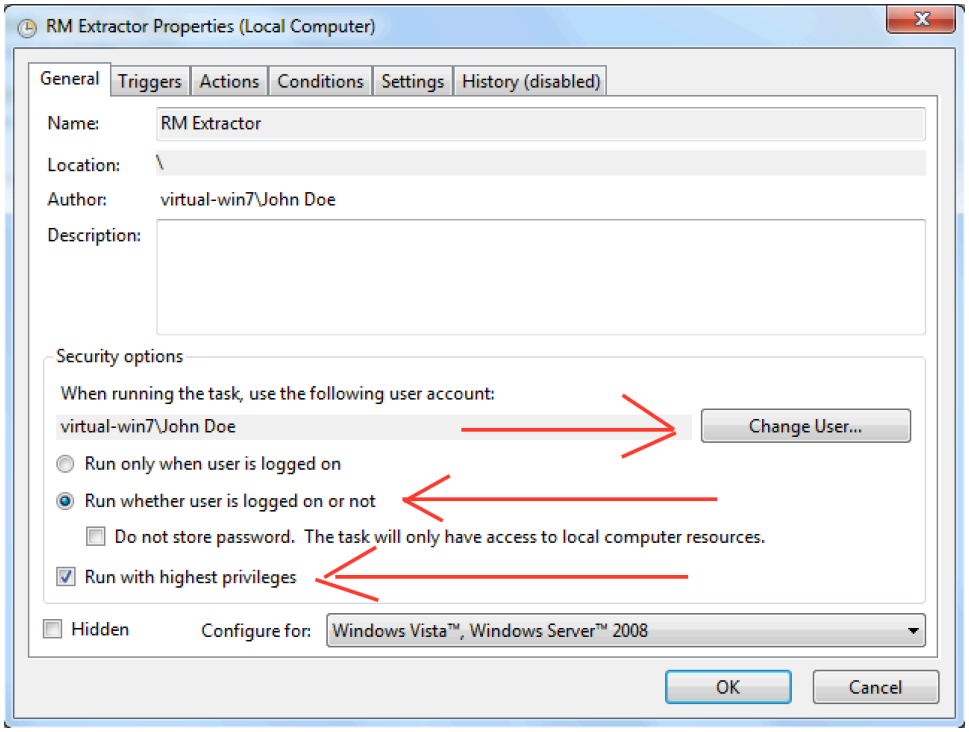


d. Tick the 'Open the Properties dialog' checkbox:



2. On the General properties you have to specify 3 things:

Privileged & Confidential Information: Not for distribution. US pat. 9,165,324 and pat. 8,666,788



a. Specify the administrative user who has access to the C:\RMExtractor and C:\RMUploader folders (and in case of TAM – to network share of TAM and APPS directories as discussed in 'Extractor Requirements' section)
b. Select 'Run whether user is logged on or not'
c. Select 'Run with highest privileges'

Privileged & Confidential Information: Not for distribution. US pat. 9,165,324 and pat. 8,666,788