REMOTE EXECUTER

For Remote Desktop Services & Citrix

contact@mqtechnologies.com

Table of Contents

I - INTRODUCTION

Remote Executer for Terminal Server/Citrix is a utility program that permits, through the virtual channel, to execute a command on the client machine from a remote session on the Terminal Server. Using this utility, user can launch any program with parameters on the client side. This program can be also configured to provide URL Host-To-Client redirection.

II - INSTALLATION

Please note that the version for Citrix (ICA) does not work for Terminal Services (RDP) and vice-versa; you have to download the right version for each platform.

1 - SERVER-SIDE: (Server folder)

Execute the installation file RemoteExecuter.msi

For Citrix server, the free version of Remote Executer will not run on Windows 2012/R2 or more recent.

2 - CLIENT-SIDE: (Client folder)

a) For Citrix:
Run the CTXRemoteExec_Client.msi setup file (there is no distinction 32/64-bit for Citrix)

b) For Remote Desktop Services (RDS):
Execute the installation file TSRemoteExecClient_x86.msi on the client (local) machine if it is a 32-bit Windows or TSRemoteExecClient_x64.msi for 64-bit Windows.

TSRemoteExecClient_x64.msi is available only in the commercial version of Remote Executer. The freeware version works only with a 32-bit Windows on the client side.
If you like to try the 64-bit version, please contact: contact@mqtechnologies.com to request a demo version.

When installing/updating Remote Executer on the client side, all remote sessions must be closed. If not the installer will not be able to install or replace the virtual channel driver and it may require a machine restart. It's preferable to close all the remote sessions, uninstall the previous version then re-install the new version. These same steps must be applied on the server side as well.

III - USING

Make a new connection to Terminal Server, open a DOS command prompt at the folder C:\Program Files (x86)\MQTechnologies\RemoteExecuter\ (or at the folder where Remote Executer has been installed), type a command:

RemoteExecuter notepad.exe

Notepad will be launched on the local machine.

You can specify a text file as parameter to open:

RemoteExecuter Notepad.exe C:\My Documents\MyTextFile.txt

If the executable program file has spaces in the name/path, the full path name has to be double quoted:

RemoteExecuter "C:\Program Files\My Program.exe" C:\My Documents\MyTextFile.txt
RemoteExecuter "C:\Program Files\My Program.exe" param1 param2 param3

To open any document file (Word, Excel, Jpg, PDF, etc) with the default associated program on the local machine, just specify the file name as argument:

RemoteExecuter MyWordFile.doc
RemoteExecuter "C:\My Documents\MyPDFFile.pdf" **(with spaces in the path/file name)**

To print a document file with default printer on local machine (new in version 5.8.1):

RemoteExecuter print "C:\My Documents\MyWordFile.docx"

In the PATH/file name, we can use Terminal Server drive mapping schema to specify a document file or a program to open/execute on the local machine. Ex:

RemoteExecuter "\\tsclient\c\my documents\My Text Document.txt"
will be transformed to
RemoteExecuter "c:\my documents\My Text Document.txt"
when executing on the local machine

Environment Variable can be used in the command line, but it must be preceded with ^ escape character. Ex:

RemoteExecuter "^%USERPROFILE^%\My Text Document.txt"

To open a website on the client side browser, just specify the URL as argument

RemoteExecuter *http://www.microsoft.com*

To create a new email on the client side by using mailto protocol:

RemoteExecuter *"mailto:myemail@hotmail.com?subject=Email Subject&body=Email Body"*

Note: the maximum length of the command line is 1500 characters

IV - REDIRECTING HTTP/HTTPS/FTP/FTPS TO CLIENT SIDE

It may be configured on the server to redirect URLs to open on the local machine with the possibility to filter out certain links.

To redirect http link (or https, ftp, ftps protocols) from server to client we have to modify Windows Registry on the server:

Please backup your registry before making the modification, if you are not sure about this, DON'T DO IT

Use Regedit.exe to change the setting of HTTP protocol. Follow these steps to make the change to registry:

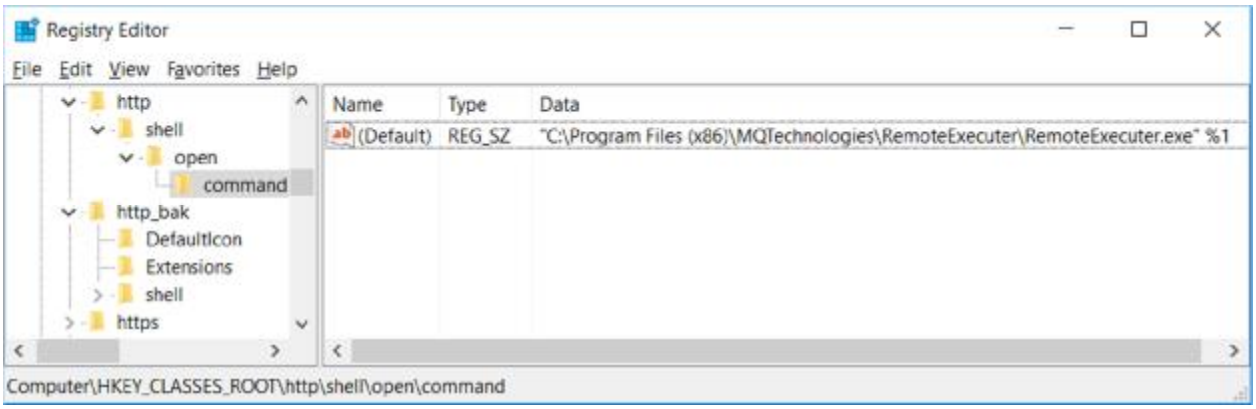
Step 1 : Backup registry keys

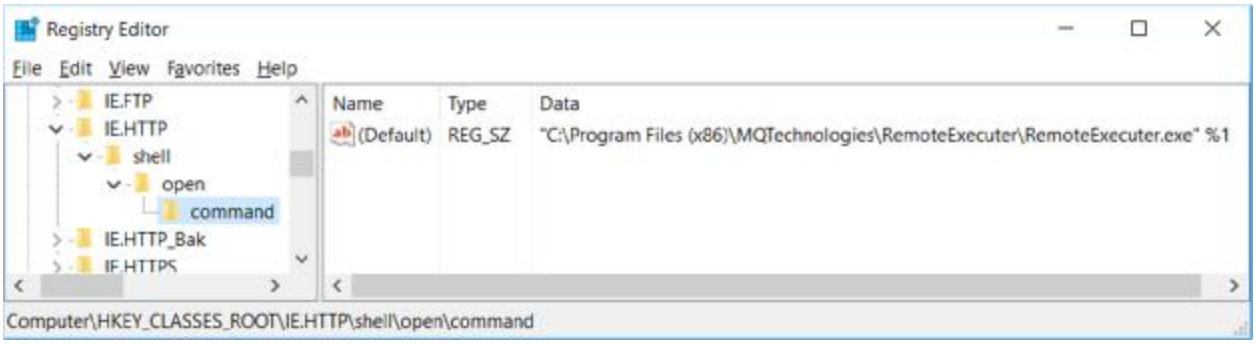
- **Find the HKEY_CLASSES_ROOT\HTTP and rename it to HTTP_bak (don't edit it)**
- **Find the HKEY_CLASSES_ROOT\IE.HTTP and rename it to IE.HTTP_bak**

Step 2 : Configure http protocol for using with Remote Executer

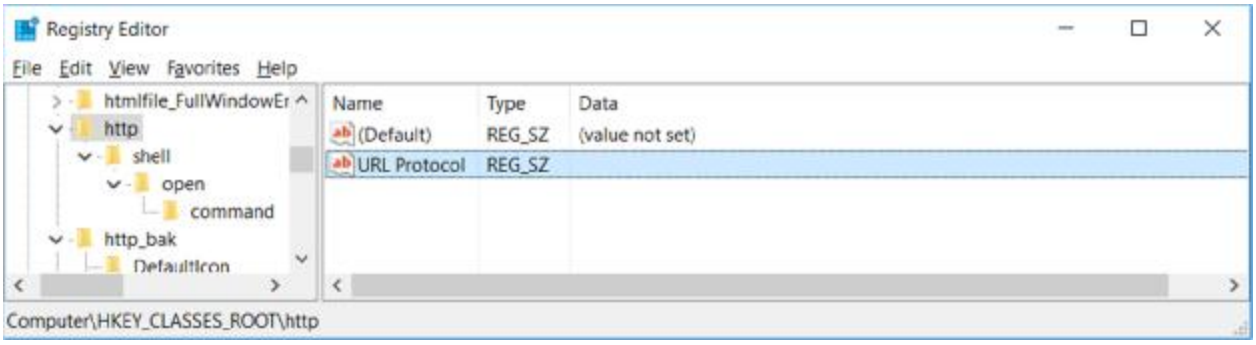
- **Recreate the same registry keys HTTP and IE.HTTP with the shell\open\command**
- **Edit and change the Default value to RemoteExecuter.exe:**

  With full path **(64-bit Windows Server)**:
  "***C:\Program Files (x86)\MQTechnologies\RemoteExecuter\RemoteExecuter.exe*" *%1***





Add a URL Protocol string value to both http and IE.HTTP key. This is mandatory on Windows 2016.



Or create a registry file (e.g: RemoteExecuter.reg) with these lines and import it on the server

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\http]
@="URL:HyperText Transfer Protocol"
"URL Protocol"=""
"EditFlags"=dword:00200002

[HKEY_CLASSES_ROOT\http\shell\open\command]
@="\"C:\\Program Files (x86)\\MQTechnologies\\RemoteExecuter\\RemoteExecuter.exe\" %1"

[HKEY_CLASSES_ROOT\IE.HTTP]
@="URL:HyperText Transfer Protocol"
"URL Protocol"=""
"EditFlags"=dword:00200002

[HKEY_CLASSES_ROOT\IE.HTTP\shell\open\command]
@="\"C:\\Program Files (x86)\\MQTechnologies\\RemoteExecuter\\RemoteExecuter.exe\" %1"
```

Step 3 : Specify Default Browser program on the server

- **Find the registry key, on 32-bit Windows Server:**
  [HKEY_LOCAL_MACHINE\SOFTWARE\MQTechnologies\RemoteExecuter\UrlRedirection\Protocol\http

  On a 64-bit Windows Server, the registry key will be at:
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MQTechnologies\RemoteExecuter\UrlRedirection\Protocol\http

- **Modify the DefaultBrowser key with the value to point to the default browser:**
  "C:\Program Files (x86)\Internet Explorer\iexplore.exe"

  Important: On a 64-bit Windows Server (2008R2, 2012/R2), always use the 32-bit folder: "C:\Program Files (x86)\Internet Explorer\iexplore.exe"

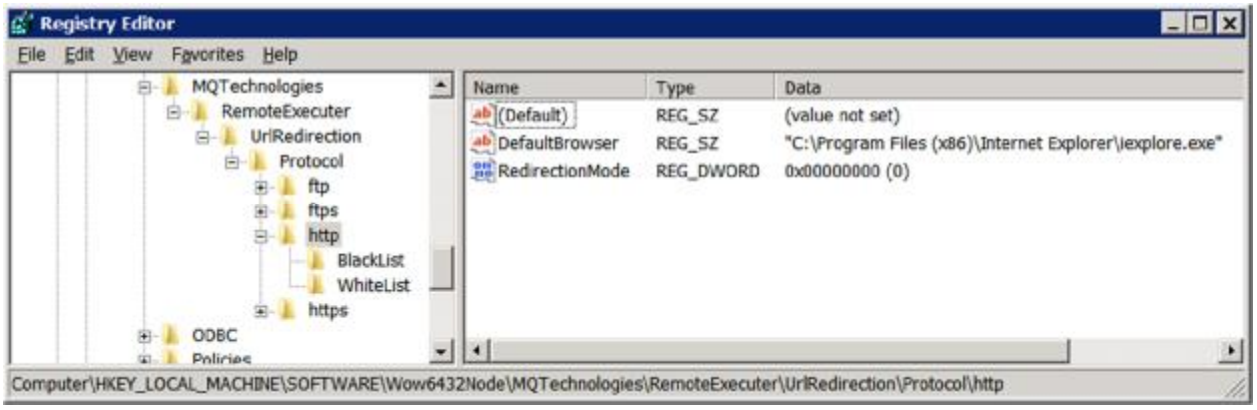
  If the default browser is not IE, (ex: FireFox), the command line will be:
  "C:\Program Files (x86)\Mozilla Firefox\Firefox.exe"

Step 4 : Configure redirection mode with option using Black List or White List

- **Find the registry key (32-bit Windows Server):**
  [HKEY_LOCAL_MACHINE\SOFTWARE\MQTechnologies\RemoteExecuter\UrlRedirection\Protocol\http

  On a 64-bit Windows Server, the registry key will be at:
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MQTechnologies\RemoteExecuter\UrlRedirection\Protocol\http

- **Modify the value of RedirectionMode to 0 or 1 or 2:**
  - **0 : redirect All http links without any restriction;**
  - **1: redirect http link only when the link IS-NOT-IN the BlackList;**
  - **2: redirect http link only when the link IS-IN the WhiteList.**



Step 5 : adding links into Black List or White List

- **Depending on the setting of RedirectionMode, you need to fill in the BlackList or WhiteList.**

  On a 32-bit Windows Server the BlackList (and WhiteList) are located in registry at:

  [HKEY_LOCAL_MACHINE\SOFTWARE\MQTechnologies\RemoteExecuter\UrlRedirection\Protocol\http\BlackList]
  "url1"="http://www.microsoft.com/"
  "url2"="http://www.yahoo.com/"
  "url3"="http://www.google.com/"

  On a 64-bit Windows Server the BlackList (and WhiteList) are located in registry at:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MQTechnologies\RemoteExecuter\UrlRedirection\Protocol\http\BlackList]
  "url1"="http://www.microsoft.com/"
  "url2"="http://www.yahoo.com/"
  "url3"="http://www.google.com/"

  You can add link to the black list as many as you want, each with a new key following the format:
  url1=
  url2=
  url3=

When the RediectionMode=0 (Redirect all links), with this setup, when user clicks on an Internet http link in an Outlook email, the execution will be forwarded to Remote Executer, the program itself will verify:

1. **If it isn't under a Remote Session, the link will be opened by the browser on the server, with the Default Browser specified at Step 3.**

2. **If it is under a Remote Session, the link will be opened in the browser on the client machine.**

When the RediectionMode=1 (Use BlackList), with this setup, when user clicks on an Internet http link in an Outlook email, the execution will be forwarded to Remote Executer, the program itself will verify:

1. **If it isn't under a Remote Session, the link will be opened by the browser on the server, with the Default Browser specified at Step 3.**

2. **If it is under a Remote Session, Remote Executer will verify if the link IS-NOT-IN the Black List the link will be then opened in the browser on the client machine.**
   If the link IS-IN the Black List, the link will be opened on the server with the DefaultBrowser specified at Step 3.

   To block all pages of a web site, add the asterisk * character at the end.
   Ex: url1=http://www.google.com/* will block all pages and folders of http://www.google.com
   Note that http://www.google.com/* is different with http://google.com/*

   To block all sub-domains and pages of a website, use the * for the sub-domains. Ex: http://*.google.com* will block everything of google.com.

When the RediectionMode=2 (Use WhiteList), with this setup, when user clicks on an Internet http link in an Outlook email, the execution will be forwarded to Remote Executer, the program itself will verify:

1. **If it isn't under a Remote Session, the link will be opened by the browser on the server, with the DefaultBrowser specified at Step 3.**

2. **If it is under a Remote Session, Remote Executer will verify if the link IS-IN the White List, the link will be then opened in the browser on the client machine.**
   If the link IS-NOT-IN the White List, the link will be opened on the server with the DefaultBrowser specified at Step 3.

Repeat all the same settings for other protocols like: https, ftp, ftps protocols if you want.

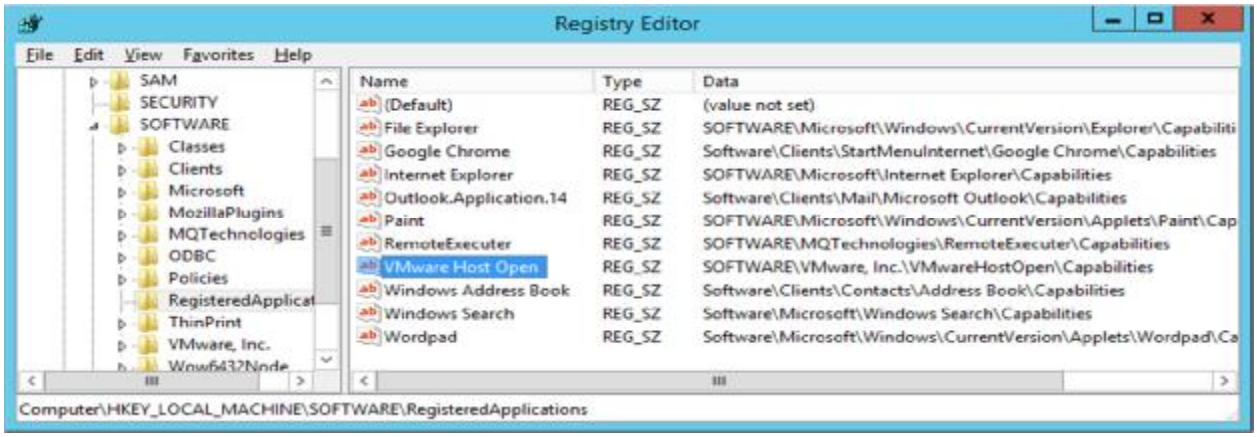
VMWARE TOOLS & OTHER BROWSER

These modifications are not required if URL redirection works after the modification of HTTP and IE.HTTP registry keys in previous steps.

If there is VMware Tools and/or other browser as FireFox, Chrome installed on the server; the WMware Host Open feature will take over control of http opening action. In that case, there are more registry modifications need to be done. The idea is to configure Remote Executer as a Default Program to handle http protocol, every time an http link is clicked, the link will be passed to Remote Executer program.

1. **Run Regedit.exe. Find the registry key:**
   HKEY_LOCAL_MACHINE\Software\RegistreredApplications
   If you see VMware Host Open on the right panel, delete it (make a backup of your registry key by exporting it or take note of that line)

   If there is FireFox or Chrome (Google Chrome line in the picture) installed on the server, delete their entries as well



Since now when an http link is clicked the link will be forwarded to Remote Executer and it will be redirected to local machine browser.

IMPORTANT NOTES:

1. **When adding url into the Black or White List, add the prefix protocol (i.e: http://, https://, ftp://, etc) because they are different and from Outlook a link without protocol, ex: www.microsoft.com will be converted by Outlook to http://www.microsoft.com/ before sending to the Shell command .**

2. **On the server side, with Windows 2008 R2 (and Windows 2012/R2), if user has made a choice for the Default Browser (FireFox or IExplorer), a registry key: "HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\UserChoice" will be created.**

   In that case, the HKEY_CLASSES_ROOT\HTTP\Shell\Open\command key will be then ignored and HKEY_CLASSES_ROOT\IE.HTTP\Shell\Open\command will be used by Windows prior to the standard HTTP key.

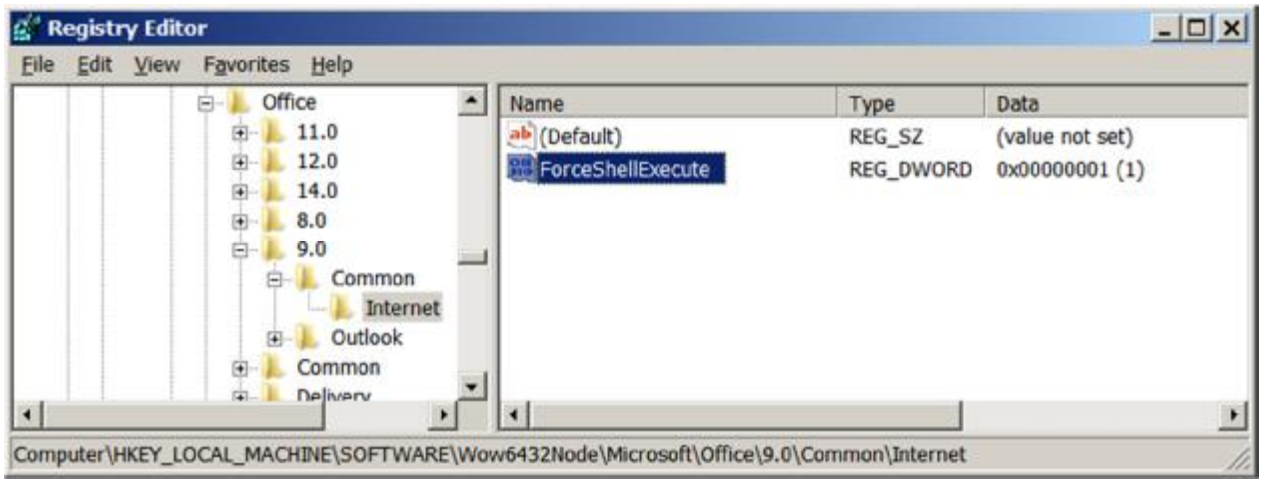
VI - REDIRECTING URL FROM MS OFFICE DOCUMENTS (WORD, EXCEL) TO CLIENT SIDE

TO MAKE URL REDIRECTION WITH MS WORD, EXCEL
(REF: Follow this KB http://support.microsoft.com/kb/218153)

Add the registry key:

ForceShellExecute=1

If you are running 32-bit Office on 64-bit Windows:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\9.0\Common\Internet



If you are running 64-bit Office on 64-bit Windows, the registry key will be:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\9.0\Common\Internet

Remember it's always under \9.0\ either with Office 2007 or 2010

If User Choice has been made, and IE.HTTP is used. MS Word (and other MS Office programs) might ignore this setting, it always uses value setting in IE.HTTP

VII - SCRIPTING/PROGRAMMING WITH REMOTE EXECUTER

Remote Executer can be used from a command line or it can be used with any programming language that can use COM as VBScript, Visual Basic, C++, C#.
For example, with a VBS file, it can be used to run a program on local machine:

```
'Create Remote Executer COM object:
Set oRemExec = CreateObject("RemExecuter.RemExec")

' Run Notepad on client machine
oRemExec.Exec "Notepad.exe"

'Open C:\My Documents\MyTextFile.txt with notepad on the client machine
oRemExec.Exec "Notepad.exe", "C:\My Documents\MyTextFile.txt"

'Open C:\My Documents\MyTextFile.txt with notepad on the client machine, and with
'Maximized (3) mode (1: Normal Window; 2: Minimized, 3: Maximized window)
oRemExec.Exec "Notepad.exe", "C:\My Documents\MyTextFile.txt", 3
```

RemExecuter.RemExec COM object has 4 methods:

1. **CheckConnection: return True if the connection (communication) can be established from Terminal Server to local (client) machine. Usually, this method is used to detect if Remote Executer has been installed on the client machine or not.**

2. **IsRemoteSession: return True if it's running under a Remote Session (Terminal Server or Citrix)**

3. **Exec(*szCommand*, [optional]*szParameters*, [optional]n*ShowCmd*)**
   This method is used to run/open on the local machine, a command line, a document file with default associated program or open an http link in the local browser. The second and third arguments are optional. The total string length of these parameters must be less than 1600 characters.

   The third parameter n*ShowCmd* can be 1(open window in normal mode), 2 (open window in minimized mode) or 3 (open window in maximized mode).
   This method does not return value and is recommended to avoid unnecessary traffic between the server and client side.

4. **ExecScalar(*szCommand*, [optional]*szParameters*, [optional]n*ShowCmd*)**
   This method is similar as Exec, but it does return an integer value. A value greater than 32 means the function call is successful. Otherwise, the returned value is the error code of ShellExecute function. If not really need, use method Exec instead.

Important notes:

1. **When using in programming mode, especially with Windows 2012/R2, you must keep only an instance of RemoteExecuter. Don't create and destroy the RemExecuter.RemExec COM object multiple times.**

2. **If there are several programs that use RemExecuter.RemExec at the same time in a same remote session, you must use a Mutex object when calling its methods to control the access to RemExecuter.RemExec COM object.**

3. **Remote Executer may or may not work properly in some specific use cases and depending on Remote Desktop Connection version and the combination of Windows version on both client and server machines.**

4. **This program cannot work if using as command line under a published DOS window because there are some security restrictions on the server. Only a DOS prompt window from a published full desktop can run Remote Executer. However, any published Remote App program can call (execute) Remote Executer.**

TROUBLESHOOTING

Please contact contact@mqtechnologies.com for any question

When contacting us for troubleshooting, please provide all the details as many as possible such as Windows version on the Server and Local machine; full desktop mode or with a published RemoteApp and how you are using the program (command line or function call from another program or via registry modification, etc).

Release notes:

- **2016-01-17: v5.8.2 Add print command**
- **2016-03-10: v5.8.6 New version to reduce traffic when calling by command line**
- **2017-11-09: v5.8.8 Change protocol detection on Windows 2016/Windows 10**

Updated on January 31st, 2018