GE
Steam Power
Automation & Controls

February 10th, 2020	PRODUCT LIFE CYCLE BULLETIN	Cybersecurity

Topic: ALSPA Antivirus signature update _ SB20002

Dear Valued Customer,

The purpose of this Service Bulletin is to inform our ALSPA Series 6 customers about the new procedure to be followed to maintain the update of the virus signature database in the ALSPA engineering & HMI stations.

Background

ALSPA Serie 6 control system stations & servers are protected by McAfee antivirus. The signature database of McAfee antivirus must be updated regularly to ensure the protection of the control system and associated data.

McAfee changed the way new signatures can be updated in the anti-virus database by declaring end of support of the FTP previous procedure. Now, to upload the signature files from McAfee Common Updater download sites, the use of HTTP protocol is mandatory and should be selected in replacement of FTP.

Not uploading new signature update increases significantly the Control System exposure to cyber-attacks.

Our Solution

Here is the new procedure to follow to update McAfee signature files.

1. **Updating the virus signature files**
   This operation consists of updating the VirusScan signature files, in order to have an up-to-date database of known viruses. It must be done as often as possible.

   On a PC with an Internet connection, download the directory commonupdater2 from McAfee's Http Virus Scan update site: http://update.nai.com/products

   To upload the commonupdater2 directory on the computer, you can use the command wget (download from https://eternallybored.org/misc/wget/).

Through the command line interface, navigate to the wget.exe folder :
Cd /d <wget.exe folder>

Then
wget.exe -o wget.log -nH --cut-dirs=1 -m -np -P <virus signature destination folder>
http://update.nai.com/products/commonupdater2/

Example with wget.exe file located on "D:\" and virus signature destination folder as "d:\transfert":

D:\> wget.exe -o wget.log -nH --cut-dirs=1 -m -np -P d:\transfert
http://update.nai.com/products/commonupdater2/

This command will upload the commonupdater2 folder in the directory d:\transfert

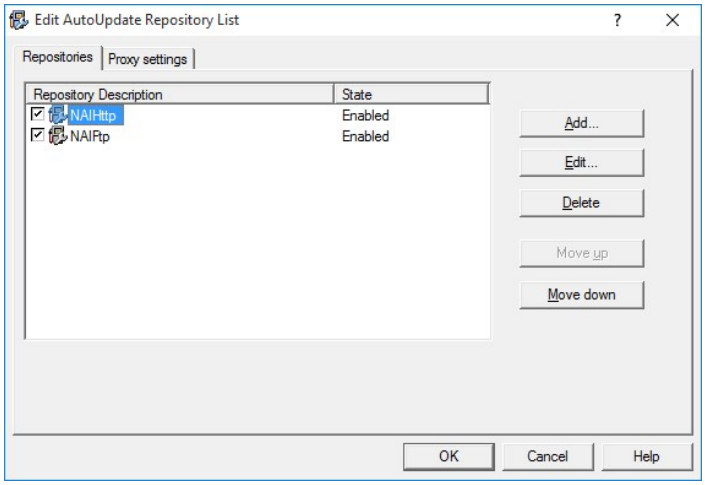
Copy this directory to a removable device (e.g. USB key) and load it on to the Controcad server station at the following location: C:\inetpub\ftproot\.

The ALSPA HMI stations and Controcad client stations are then configured to retrieve the signature files automatically.

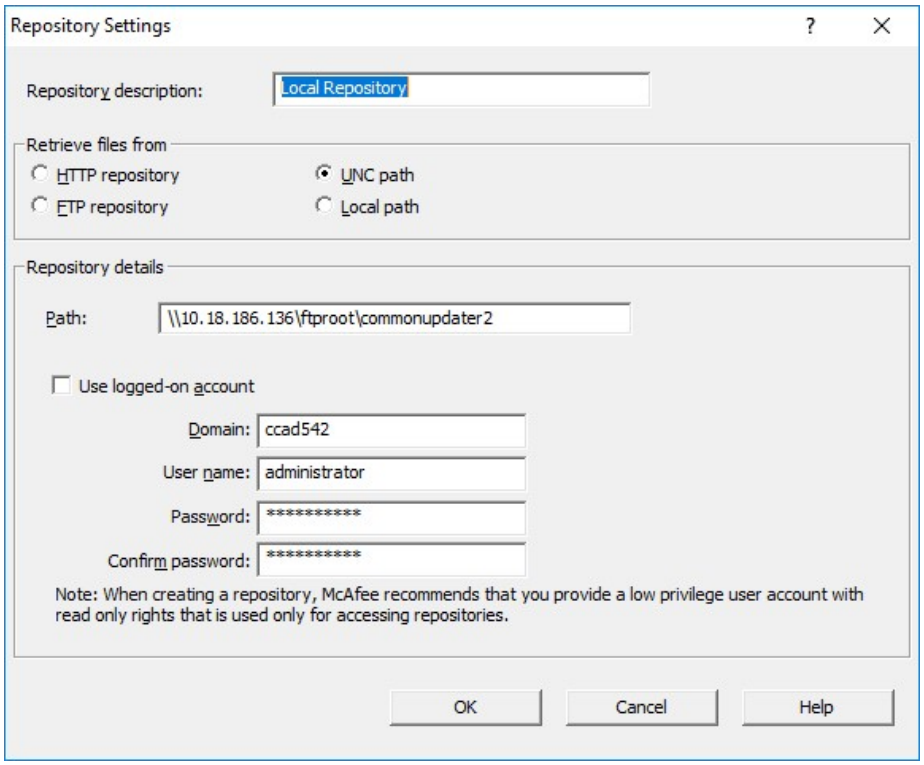
2. Configuring AutoUpdate

In complement to the end of support of FTP by McAfee, we recommend using shared directory instead of FTP for the Auto update of the workstations. Given that the station does not have Internet connection, virus signature updates must be done from the Controcad station server. VirusScan must therefore be configured, so that it regularly gets update files from the Controcad station.

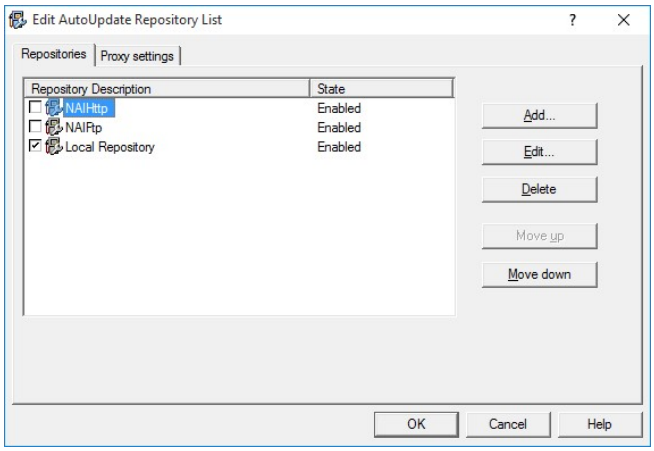
- In the **VirusScan Console** window, click on the menu **Tools > Edit AutoUpdate Repository List**.



- Unselect the first two lines and click on the **Add** button.



- Proceed as follows to configure the repository:
  - Rename the repository to: **Local Repository**;
  - Tick **UNC path**;
  - Enter, in the **Path** field, the UNC path (\\IP address of the Controcad server\ftproot) and add **\commonupdater2**;
  - Enter **the name of the computer** in the **Domain** field;
  - Enter **User name**.
  - Enter the **Password** and **Confirm Password**
- Click on the **OK** button to continue.



- In the window which lists the repositories, check that the **Local Repository** line has been added and click on the **OK** button to continue.

Your Benefits

Implementing the above procedure will allow you:

- To integrate McAfee regular update on virus signature, in order to enable the antivirus tool to operate as efficiently as possible
- By reducing the cyber attack surface, to improve the availability and reliability of your ALSPA Series 6 system

The procedure can be performed at site by a control system maintenance engineer with ALSPA background

Next Step

The optimal cyber security solution is based on defense in depth strategy. The anti-virus update procedure can be completed with a **station hardening offer**, both for operator stations and engineer stations. Station hardening offer will include the configuration of a **whitelisting** tool to improve the endurance against most of malware/virus. This will be done thank to a permanent comparison of computer processes running on the system stations, versus a registered baseline. Any newly activated and non-registered task (including. malware) will be detected and automatically disabled.

Please contact us to learn more about these improvements. Our team will be pleased to help you design the optimal upgrade to your system to continue to operate safely and with the highest availability your power station.

We appreciate your business and you, our valued customer. **Please contact your GE Power Automation & Controls sales person or our Help Desk at +33 1 60 13 43 91 / helpdesk.control-systems@ge.com** for help on ordering and upgrades.

Hugues Moreau
Product Manager Power Automation & Controls, GE Steam Power
Hugues.moreau@ge.com