Tech Tip 1- HTTPS on Windows GDMA

Tech Tip 1 (01/2016) - Installing HTTPS on Windows GDMA clients

The Windows GDMA client can support encrypted communications over https. This tip explains how to make this work.

Since Windows can be particular about certificates and formats, we do not recommend copying the certificate files from the GroundWork Monitor server to the GDMA client. Instead, follow the steps below. Note you must use an account with Administrator access to the Windows server. These instructions assume that the Target server in the GDMA configuration has been set appropriately to use https:// instead of the standard http://

1. On the Windows server, launch an IE browser session.
2. To test that you can make a connection to the GroundWork Monitor server on port 443 and also allow you to work through any certificate issues (if found), enter the following in the address bar:

```
https://<insert GW monitor server name>/gdma/
```

3. Once the certificate path is validated, begin to export each of the certificates in the chain as follows:
    a. Right click anywhere within the page window and select **Properties**, then click **Certificates**.
    b. Click the **Certificate Path** tab to see how many certs are in the path. Each one will have to be saved to a file.
    c. Starting with the last cert in the list, click the **Details** tab.
    d. Click **Copy to File**.
    e. At the **Welcome to the Certificate Export Wizard**, click **Next**.
    f. Select **Base-64 encoded X.509 (.CER)** for the format, **Next**.
    g. Give the file a name (generally best to use the same name as the certificate) and a place to save the file. The file will be saved with a **.cer** extension.
    h. Proceed through steps a-g above for each certificate in the chain.
4. Once all certificates have been saved, verify them by opening with **wordpad.exe**:
    a. Open WordPad by clicking **Start** and then typing **wordpad.exe** in the search prompt.
    b. Open each of the files and ensure that the first line says **-–- BEGIN CERTIFICATE** ---. You will need to change the **File Extensions** box to **All Documents** to show the **.cer** files.
5. Once the certificate files have been verified, rename the file extension to **.pem**. This is important because **c_rehash** only looks for **.pem** files.
6. Copy the files to one of the directories listed here:

```
C:\Program Files\groundwork\gdma\certs
```

```
C:\Program Files (x86)\groundwork\gdma\certs
```

7. Open a command window and change to one of the directories listed here:

```
C:\Program Files\groundwork\gdma\certs
```

```
C:\Program Files (x86)\groundwork\gdma\certs
```

8. Run **c_rehash** for the certificates for one of the directories listed below. If successful proceed, if not fix the issues found.

```
C:\Program Files\groundwork\common\bin\c_rehash
```

```
C:\Program Files (x86)\groundwork\common\bin\c_rehash
```

9. Stop the gdma service and restart from command window:

```
net stop gdma
```

```
net start gdma
```

10. Verify the GDMA is now reporting into the GroundWork Monitor server. If so, create a zip file with the certificates and then distribute them to all other Windows servers running GDMA.
    a. For each Windows server, delete any existing certificate files in **gdma\certs**.
    b. Copy the zip and extract the **.pem** certificate files to the **gdma\certs** directory.
    c. Run the following command:

```
groundwork\common\bin\c_rehash run
```

    d. Issue the following commands:

```
net stop gdma
```

```
net start gdma
```