Secure a Montitoring Station to Windows Agent communication with TLS 1.2

Use the following information to secure an Uptime Infrastructure Monitor Monitoring Station to Windows Agent communication with TLS v1.2. Users must have administrator access to the machines on which you want to install and configure Agents and to the Monitoring Station.

Stunnel configuration

Begin by setting up the stunnel configuration file to allow only TLS 1.2.

Next, modify the stunnel config file located at:

```
C:\Program Files\uptime software\Uptime agent\stunnel\config\stunnel.conf
```

using the following information:

```
[up.time agent]
accept = 9997
connect = 9998
cert = stunnel.pem
options = NO_SSLv2
options = NO_SSLv3
options = NO_TLSv1
options = NO_TLSv1.1
```

Firewall modification

Create a firewall rule that blocks port 9998 incoming on the Agent machine so that no insecure connections can be made to the Agent. It is a good idea to set the firewall to notify you when applications are blocked as it aids in configuring it with stunnel.

Run stunnel as a service on the Agent machine

Run stunnel as a service that starts when Windows starts so that the connection is re-established once the Agent server is rebooted. Open a command prompt as an administrator, and then change the directory path to the stunnel config file that we edited in the previous Stunnel configuration section, for example:

```
C:\users\robert>cd\Program Files\uptime software\Uptime agent\stunnel\config
```

Execute from stunnel's bin folder:

```
stunnel –install
```

For example:

```
C:\Program Files\uptime software\Uptime agent\stunnel\config>..\bin\stunnel.exe –install
```

Now, open the Services control panel (**Start** > **Run** > **services.msc**), and find the stunnel service. Although the service is set to automatically start, it is not yet running so you must manually start the service. If your windows firewall asks for confirmation, click **Yes**.

Monitoring station configuration

In this step, you must modify the Uptime Infrastructure Monitor configuration to restrict secure agent communications to use the version and ciphers of SSL /TLS that you want to use. It is important that you run Notepad as an administrator or use Notepad++ to make these changes. The file is located in the Uptime Infrastructure Monitor installation directory. If you used the default installation, it is located at: `C:\Program Files\uptime software\uptime`.

At the end of the file, add a section similar to the following lines:

```
#Agent connection security stuff
clientSocketTlsVersion= TLSv1.2
```

Note that this step is opposite from the Agent setup where you specify what certificate versions NOT to use. For this example, we only allow TLS 1.2, the strongest encryption currently offered by IDERA.

After making the changes, be sure to save the file. Restart the Uptime Data Collector Service on the Monitoring Station to pick up the changes. Open the Services control panel. Right-click **Uptime Data Collector**, and then select **Restart**. The restart may take several seconds to complete. If several minutes pass, open Task Manager and stop the process, and then attempt to manually start the service.

Adding secured machines to Uptime Infrastructure Monitor or reconfiguring existing monitored servers

> If you make the following changes in the Uptime Agent Global Configuration window and there are already configured agent machines that are NOT using these new settings, those machines will stop working correctly. If you have other agent machines that are NOT using global settings, these will continue to work without issue.

The final step in this process is to add the agent-based machine or reconfigure it if it already exists in Uptime Infrastructure Monitor. If you want to have TLS 1.2 (or another version) on all agents, it is easy to set that up in the Uptime Agent Global Configuration located under the Config tab. The **Agent Port Number** field and **Use SSL (HTTPS)** checkbox allow you to make these changes. Change the port number from **9998** to **9997**, and then check the SSL box. You can use these same steps to add a secured agent to Uptime Infrastructure Monitor followed by clicking **Infrastructure > Add system/network device**, and then choosing the aforementioned options.

To modify an *existing* agent machine you already have in Uptime Infrastructure Monitor but now includes secure communications, find the agent in Uptime Infrastructure Monitor by typing the hostname in the search field available in the menu bar. In the Info tab for that element, click **Edit system profile and collection**. Verify the correct settings in the displayed window. If you updated the Global Configuration Settings mentioned earlier, verify that it is set to use the global settings. If it is set to anything other than port **9997** and **Use SSL** checked, change it to reflect these settings, and then click **Save**.

The final step in this process is to test that the settings are working as expected. While on the Info window, click the poll agent option in the left-hand menu, and then wait for the results. If all of your settings are correct, the output should be clear. If the settings are incorrect, it is likely that you may have not specified corresponding ciphers on the monitoring station and agent, the TLS or SSL versions do not match, or you specified the wrong ports. Review your settings. Contact support if you continue to have an issue.

This information is available online at:
http://docs.uptimesoftware.com/display/KB/Securing+the+Windows+Agent+with+SSL

If you would like to use a preshared key (PSK), refer to the following topic:
http://docs.uptimesoftware.com/display/KB/Configuring+PSK+for+Agents

For more information about configuring agents for specific levels and ciphers, please see:
http://docs.uptimesoftware.com/display/KB/Configuring+Allowed+TLS+Versions+and+Ciphers+for+the+Monitoring+Station+and+Agents

Check out the Idera community forums at http://community.idera.com