Secure Automation Stick (SAS)

Sicherer, installationsfreier Zugriff auf Automationsanlagen

Diese Dokumentation beschreibt die Handhabung des Secure Automation Sticks (SAS) und erläutert im Kapitel 4 die Besonderheiten beim Zugriff auf Steuerungen diverser Hersteller.

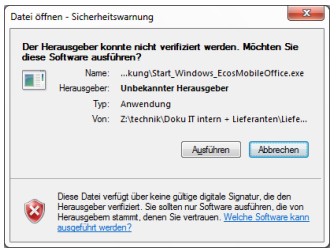
Inhaltsverzeichnis

1. Start des Secure Automation Stick

Stecken Sie den Secure Automation Stick an eine freie USB-Schnittstelle Ihres Windows PCs/Notebooks, der über einen Internetzugang verfügen muss.

Starten Sie je nach Version des SAS die exe-Datei *Start_SecureAutomationStick.exe* bzw. *Start_Windows_Isona.exe* o.ä. im obersten Verzeichnis (Root) des Secure Automation Sticks.

Falls ein auf dem System befindlicher Virenscanner die exe-Datei als „unsicher“ anzeigt, müssen Sie die Datei in die Whitelist des Virenscanners eintragen.
Bei manchen Windows-Versionen bzw. -Einstellungen erscheint beim Aufruf des Programms ein Warnhinweis, den Sie mit dem Button „Ausführen“ bestätigen müssen:



Jetzt öffnet sich das folgende Windowsfenster (Abb. ähnlich):

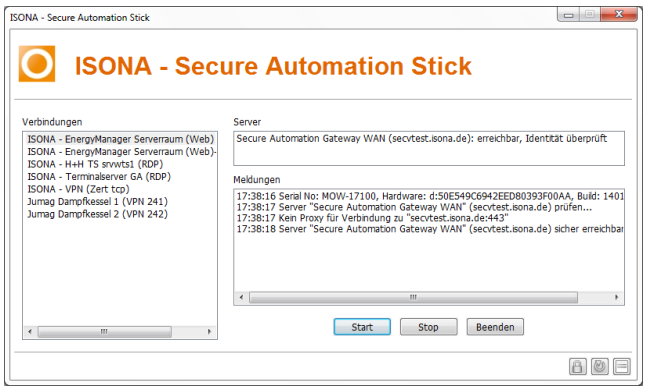


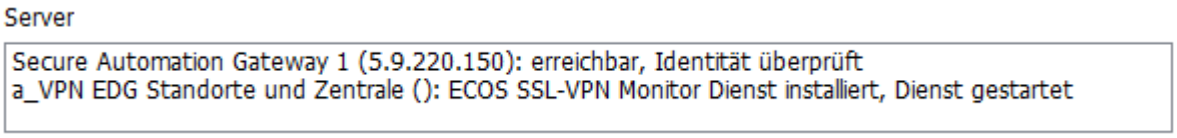
Abb.1: Windows-Fenster des Secure Automation Sticks mit Verbindungsprofilen

Im linken Feld „Verbindungen“ sieht man die für den jeweiligen Benutzer freigegebenen Verbindungsprofile.

Ab Version 5 des SAS sind neue Funktionen verfügbar. Wenn z.B. sehr viele Verbindungsprofile im Feld „Verbindungen“ vorhanden sind, erscheint automatisch eine Suchfunktion:

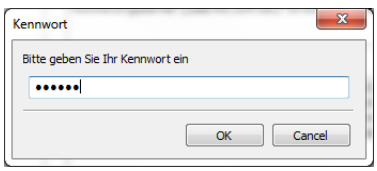
Damit kann man in allen Profilen nach einem Wort oder Wortteil suchen. Gibt man in dieses Suchfeld ein Wort oder einen Wortteil ein, dann werden alle Profile angezeigt die dem eingegebenen Wert entsprechen. Wenn man den Suchbegriff löscht, werden wieder alle verfügbaren Profile angezeigt.

Bevor Sie ein Profil starten stellen Sie bitte sicher, dass der PC über eine aktive Internetverbindung verfügt und den zentralen Server erreicht, dies wird im SAS Feld „Server“ folgendermaßen in der ersten Zeile angezeigt (Beispiel):



Falls auf dem SAS ein SSL VPN-Zugriffsprofil vorhanden ist, wird in der zweiten Zeile (siehe Bild oben) angezeigt, ob der entsprechende Dienst „ECOS SSL-VPN ‚Monitor Dienst“ auf dem PC/Notebook gestartet ist. Nur wenn dieser gestartet ist, kann ein SSL VPN Zugriffsprofil erfolgreich aufgerufen werden!

Erst wenn das Secure Automation Gateway erreichbar ist (Zeile 1 im Bild oben), darf ein Verbindungsprofil mit einem Doppelklick auf den Namen im Feld „Verbindungen“ aufgerufen werden. Alternativ kann man auch einen Eintrag im Feld „Verbindungen“ mit der Maus markieren und anschließend auf den Button „Start“ klicken.
Jetzt erscheint beim Aufruf des ersten Verbindungsprofils ein Fenster, in dem man das zugeteilte Kennwort zur Authentifizierung eingeben muss:



Nach der erfolgreichen Anmeldung wird dann die gewählte Verbindung geöffnet und in dem entsprechenden Programm (Browser, RDP, VNC usw.) angezeigt.

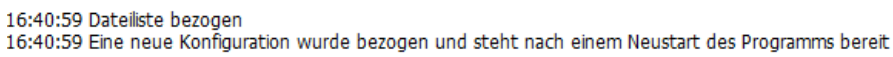
In dem rechten Fenster „Meldungen“ sieht man die Logeinträge und kann im Fehlerfall eine Diagnose durchführen.
Mögliche Fehlerursachen sind (siehe hierzu auch Kapitel 4 „Hilfe im Fehlerfall“):

- Der Windows PC hat keine Verbindung zum Internet
- Eine lokale Firewall blockiert die Zugriffe des SAS
- Der SSL VPN Dienst ist auf dem PC nicht installiert / automatisch als Dienst gestartet worden

Die Konfiguration der SAS erfolgt zentral in dem Secure Automation Gateway (SAG), einem VPN-Gateway auf das sich alle SAS über einen verschlüsselten Tunnel verbinden.
Wenn auf dem SAG seit dem letzten Start weitere Zugriffsprofile freigeschaltet wurden, dann aktualisiert sich der Secure Automation Stick automatisch bei der nächsten Einwahl, im Fenster „Meldungen“ wird dann der Text „Konfiguration aktualisieren“ angezeigt, dieser Prozess kann je nach Umfang mehrere Minuten dauern.
Während dieser Phase sollte kein Verbindungsprofil aufgerufen werden, da dies zu Fehlfunktionen führen kann!
Wenn der Aktualisierungsprozess beendet ist, wird der Text „Konfiguration aktualisiert“ angezeigt.

Sie können bei Bedarf direkt nach dem Start die Aktualisierung der Konfiguration über den Button  rechts unten im SAS-Fenster anstoßen. Dabei wird die Eingabe des Kennworts gefordert.

Ab **Version 5** des SAS wurde der Aktualisierungsprozess verändert und auch beschleunigt. Im Feld „Meldungen“ erscheint nach der Aktualisierung der Profile folgender Eintrag:



Jetzt muss der Stick beendet werden, beim Neustart sind die Änderungen dann aktiv und werden entsprechend angezeigt.

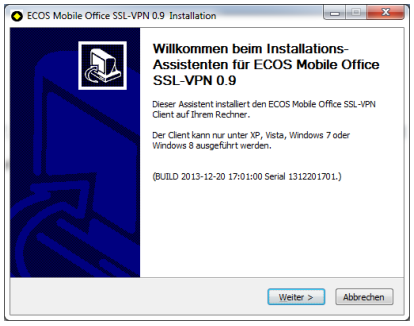
Zum Beenden des Secure Automation Stick klicken Sie bitte auf den Button „Beenden“. Jetzt können Sie den Stick, nach dem „Auswerfen“ mit der entspr. Windows-Funktion, abziehen bzw. die SD-Karte entfernen. Der Button „Stop“ hat nur eingeschränkte Funktionen und wird üblicherweise nicht benötigt.

Wichtig: nach dem Arbeiten aus Sicherheitsgründen die Applikation immer zeitnah beenden. Dann den USB-Stick abziehen, vor allem auf Systemen bei denen nicht sichergestellt ist ob auf dem Rechner ein Virenscanner läuft und eine Personal Firewall!

Ein Teil des USB-Sticks ist mit den integrierten Programmen belegt, die nicht gelöscht werden dürfen! Speziell an dem Ordner „rws“ dürfen **keine** Veränderungen vorgenommen werden, sonst funktioniert der SAS nicht mehr!
Der Stick kann **nicht** auf einen anderen Stick kopiert (geklont) werden, dort funktioniert der SAS ebenfalls nicht mehr!
Der restliche Speicherbereich kann für die Speicherung von beliebigen Dateien verwendet werden. Bitte achten Sie aber darauf, dass der USB-Stick dabei nicht durch Sicherheitstools o.ä. verschlüsselt wird!
Außerdem ist darauf zu achten, dass nicht der gesamte Speicherbereich des Sticks belegt wird, da das SAS-Programm noch temporären Speicher benötigt.

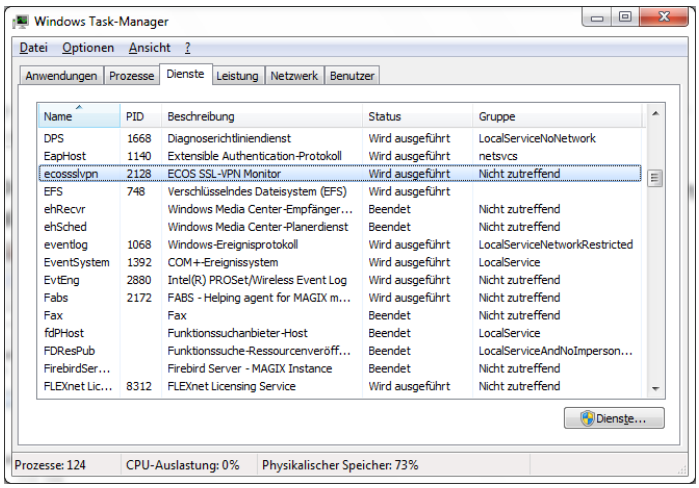
2. Besonderheiten bei SSL VPN Profilen

Der Secure Automation Stick kann nicht nur getunnelte Applikationen starten, sondern auch einen transparenten SSL VPN Tunnel aufbauen. Dies wird in den Profil-Einstellungen auf dem Secure Automation Gateways (SAG) konfiguriert.
Startet man ein SSL-VPN Verbindungsprofil, dann wird beim erstmaligen Start auf dem Windows PC ein VPN-Hintergrunddienst installiert, für den man Admin-Rechte benötigt.
Es erscheint das folgende Installationsfenster (ähnlich):



Klickt man auf „Weiter“, wird ein kleines Softwaremodul (Dienst) installiert, je nach Windows-Konfiguration kann noch die Eingabe des Admin-Kennworts notwendig sein.

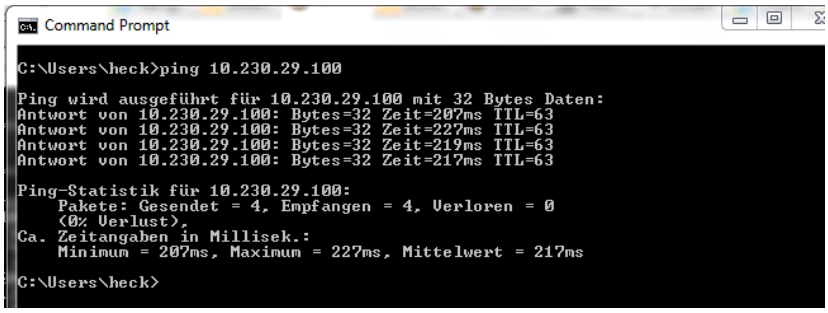
Dieser Dienst wird beim Neustart des PCs immer automatisch gestartet. Man kann dies im Taskmanager überprüfen, es zeigt sich dann der folgende Eintrag:



Alternativ sieht man einen gestarteten VPN-Hintergrunddienst auch an dem folgenden Eintrag oben rechts im SAS-Fenster „Server“ (ähnlich):

ECOS SSL-VPN Monitor Dienst installiert, Dienst gestartet, verbunden

Um zu überprüfen, ob der SSL VPN-Tunnel erfolgreich aufgebaut ist und die Steuerungen darüber auch erreichbar sind, kann man einen Ping-Test ausführen auf die ext. IP-Adresse (soweit die Steuerungen auf einen Ping antworten):



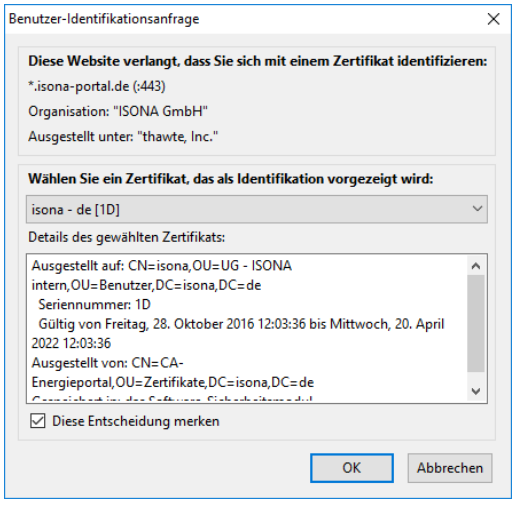
Jetzt kann man mit beliebigen Programmen und Ports auf die Steuerung zugreifen (z.B. mit einem Programmiertool oder per FTP usw).

Im Fenster „Meldungen“ des SAS kann man den erfolgreichen Aufbau eines SSL VPN-Tunnels an dem Eintrag „SSL-VPN Verbindung zu „xxxxxxxx gestartet“ sehen.
Erst wenn diese Meldung angezeigt wird, kann man mit den entsprechenden Tools und Programmen transparent via VPN auf die Steuerungen usw. zugreifen!

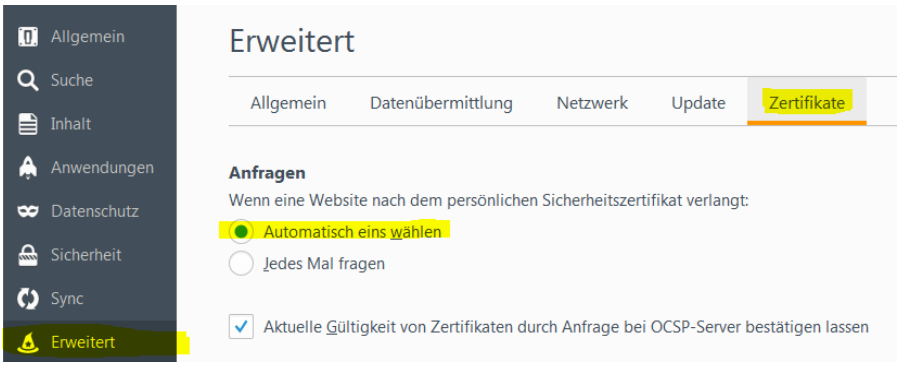
3. Besonderheiten beim Zugriffsprofil auf das Automation WebCenter oder andere Webserver

Auf dem SAS können direkte Zugriffsprofile auf ein ISONA Automation WebCenter (Kundenwebportal) oder auch andere Webserver angelegt werden. Dabei wird z.B. das ISONA Automation WebCenter mit dem SAS-internen Firefox-Browser geöffnet und man ist automatisch über das Benutzerzertifikat des SAS mit dem richtigen Benutzernamen am Webportal angemeldet, die Anmeldung mit einer Zwei-Faktor-Authentisierung am Webportal erübrigt sich dadurch.

Wenn sich das Fenster mit dem Firefox-Browser öffnet, kommt immer die folgende Zertifikatsmeldung, diese mit „OK“ bestätigen:

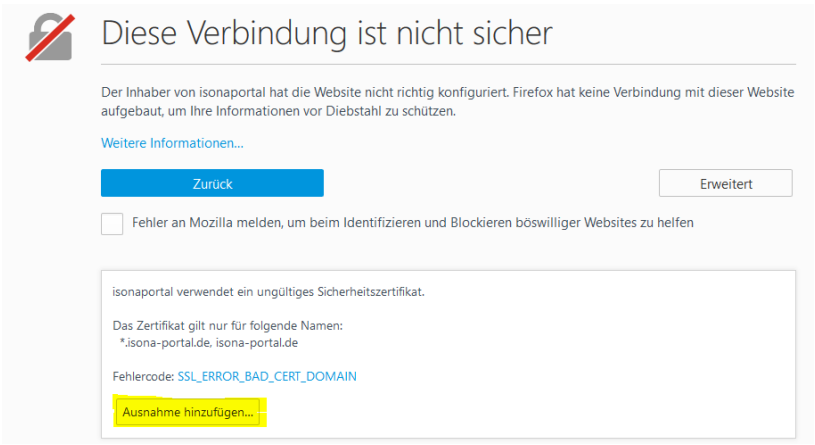


Man kann die o.g. Meldung bei jedem Neustart des SAS -Profilaufrufs vermeiden, wenn das Häkchen bei „Diese Entscheidung merken“ (siehe Bild oben) gesetzt ist und man einmalig in den Einstellungen des Firefox-Browsers folgendes auswählt:

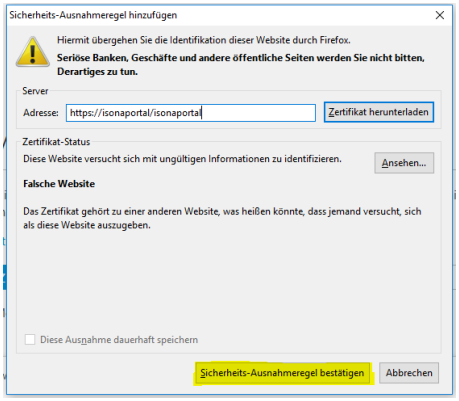


Wenn sich der Firefox per https auf das Webportal verbindet, kommt technisch bedingt immer die folgende Browserwarnung, da meist auf dem Webserver kein gültiges Webserverzertifikat installiert ist:

Hier auf „Erweitert“ klicken und im folgenden Fenster auf „Ausnahme hinzufügen“ klicken:



Jetzt erscheint die Meldung:



Hier auf „Sicherheits-Ausnahmeregel bestätigen“ klicken.

Jetzt öffnet sich das Webportal und man ist mit dem entspr. Benutzernamen und den im Webportal konfigurierten Zugriffsrechten angemeldet (angemeldeter Benutzer wird in der Fußzeile des Webportals angezeigt: „Angemeldet als Benutzer: xxxxx“).

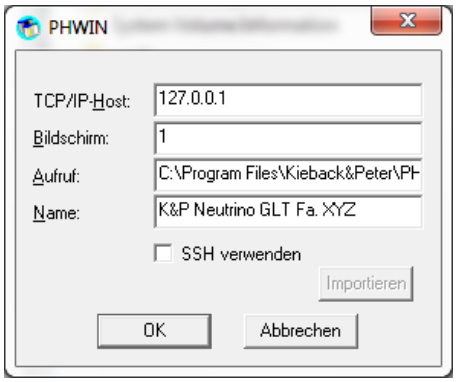
Zum Abmelden aus dem Webportal einfach das Firefox-Fenster schließen.
Der Abmelde-Button wird deshalb beim Zugriff auf das Webportal über den SAS nicht in der Menüleiste angezeigt.

4. Besonderheiten bei Verbindungen auf spezielle Steuerungen und GLT-Server

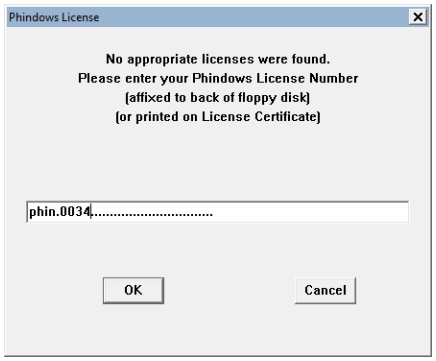
Bei Steuerungen, GLT-Servern usw., auf deren Anlagenvisualisierungen man nicht mit einem normalen Browser zugreifen kann, erfolgt der Zugriff meist mit herstellerspezifischen Windows-Clients (Viewern). Diese Windows-Clients sind dann im SAS integriert, beim Aufruf sind die in diesem Kapitel erläuterten Besonderheiten zu beachten.

4.1 Zugriffsprofil via PHWIN-Client auf eine Neutrino-GLT (Kieback&Peter)

Beim ersten Aufruf des PHWIN muss im folgenden Fenster als IP-Adresse die **127.0.0.1** eingegeben werden, das Feld „Aufruf“ und „Bildschirm“ darf nicht verändert werden. Das Feld „Name“ kann freibleiben, dieses Feld hat keine Bedeutung:



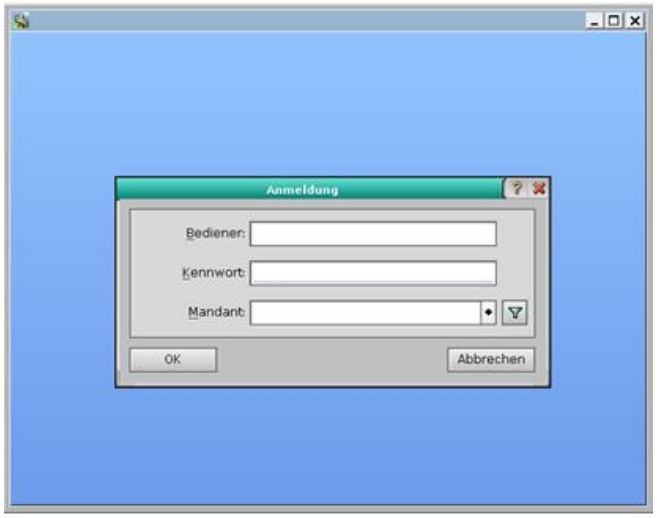
Im nächsten Fenster muss einmalig der Lizenzschlüssel für das PHWIN (aufgedruckt auf Kieback&Peter CD) eingegeben werden:



Diese Informationen werden direkt auf dem SAS abgespeichert und müssen bei der nächsten Verwendung nicht mehr eingegeben werden.

Falls bei der o.g. IP-Eingabe aus Versehen eine falsche IP eingegeben wurde, muss man den SAS beenden und dann auf dem Stick im Ordner „rws“ den ganzen Unterordner „sandbox“ löschen. Wenn man jetzt den SAS neu startet und ein PHWIN-Profil aufruft, wird die IP und der Lizenzkey wieder abgefragt.

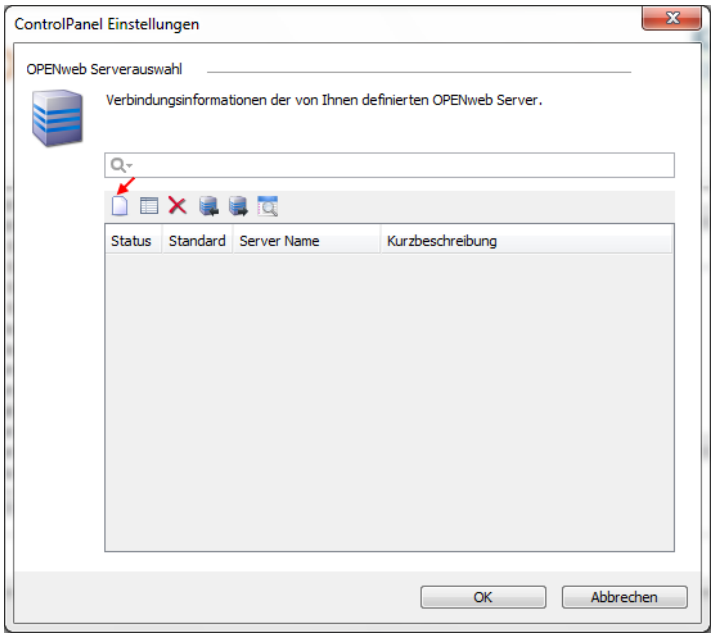
Beim Aufruf des PHWIN-Profils zeigt sich das folgende PHWIN-Fenster mit der Anmeldemaske der Neutrino-GLT (Abb. ähnlich):



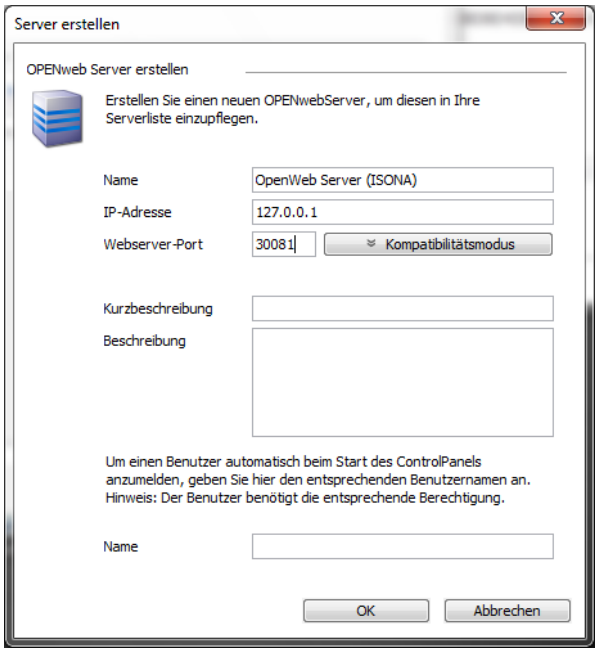
Zum Beenden des Zugriffs schließt man das PHWIN-Fenster über den „Fenster-schließen-Icon“ rechts oben in der Ecke, nicht auf „Abmelden“ klicken!
Wichtig: hat man auf dem SAS mehrere PHWIN-Zugriffsprofile auf unterschiedliche Neutrino GLTs eingerichtet, dann muss man nach Beenden des PHWIN-Fensters den SAS beenden und danach neu starten. Jetzt kann man sich auf andere Neutrino GLTs verbinden. Befolgt man diese Vorgabe nicht, verbindet sich das PHWIN immer wieder auf die gleiche Neutrino GLT, egal welches PHWIN-Profil man wählt!

4.2 Zugriffsprofil via ControlPanel auf einen OpenWeb-Server (DEOS AG)

Wenn das ControlPanel zum ersten Mal auf einem PC aufgerufen wird, müssen einige Server-Parameter voreingestellt werden und es zeigt sich folgendes Fenster, in dem man auf den Icon „Neu“ (roter Pfeil) klickt:



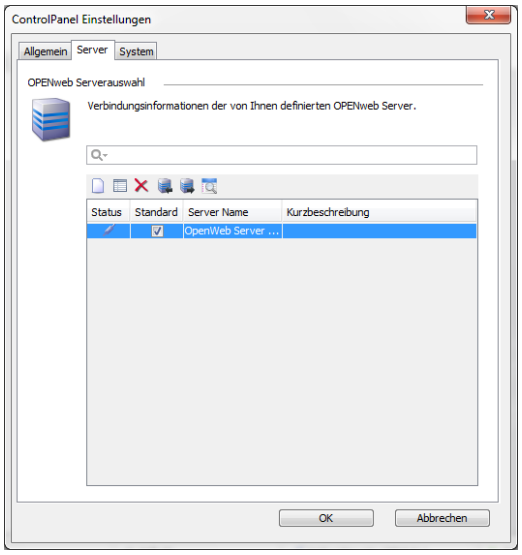
Im sich öffnenden Fenster (s.u.) trägt man die folgenden Daten ein:
IP-Adresse 127.0.0.1 (ist bei allen Anlagen identisch, entspricht localhost)
Webserver-Port 30081 (Beispiel, der Port differiert von Anlage zu Anlage je nach Konfiguration im SAG)



und klickt dann auf „OK“.

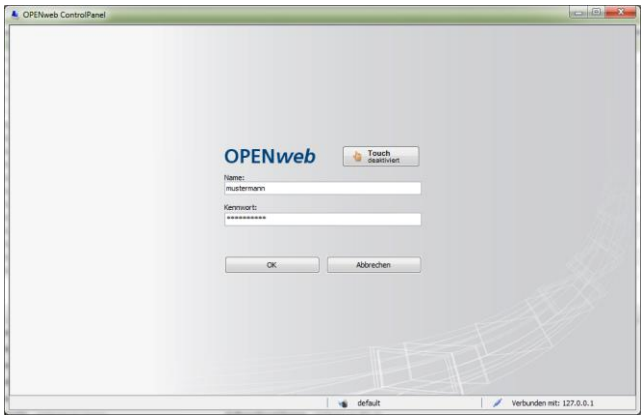
Falls das obige Fenster nicht mehr sichtbar ist (weil man z.B. die Parameter aus dieser Doku über die Zwischenablage kopieren möchte), kann man rechts unten in der Taskleiste auf das Symbol klicken.

Jetzt erscheint das folgende Fenster:

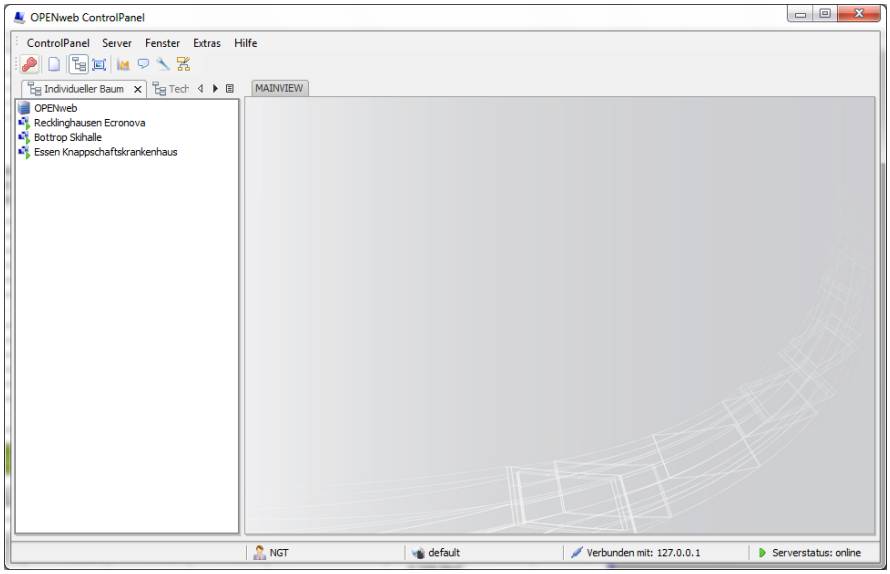


Kickt man auf OK wird eine größere Menge an Daten vom OpenWeb-Server geladen, was einige Minuten dauern kann (eine entspr. Ladeanzeige signalisiert den Fortschritt des Downloads).

Wenn alle Daten geladen wurden, verbindet sich das ControlPanel mit dem OpenWeb-Server und zeigt die folgende Login-Seite an (ähnlich):

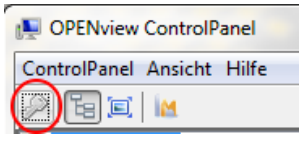


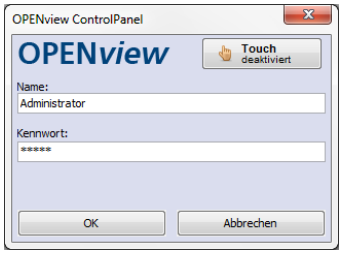
Nach der erfolgreichen Anmeldung wird folgendes Bild mit den konfigurierten Anlageorten angezeigt (Beispiel):



4.3 Zugriffsprofil via OPENview-Client auf eine OpenEMS-Steuerung (DEOS AG)

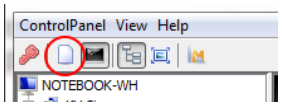
Wenn sich das Fenster des OPENview-Clients öffnet, muss man sich über den folgenden Menüpunkt einloggen:



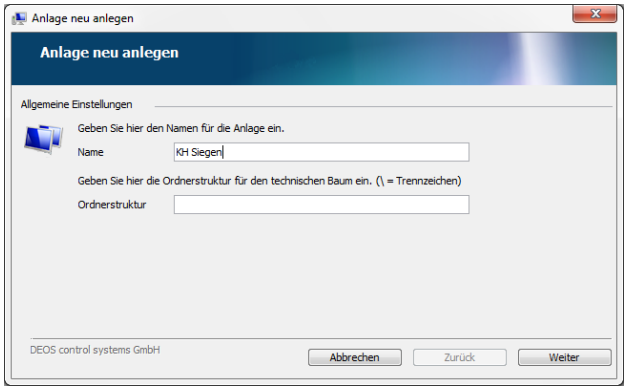


Hier gibt man die entsprechenden Zugangsdaten ein:
Benutzer: ist bei Ihrem zuständigen DEOS-Partner zu erfragen
Kennwort: ist bei Ihrem zuständigen DEOS-Partner zu erfragen

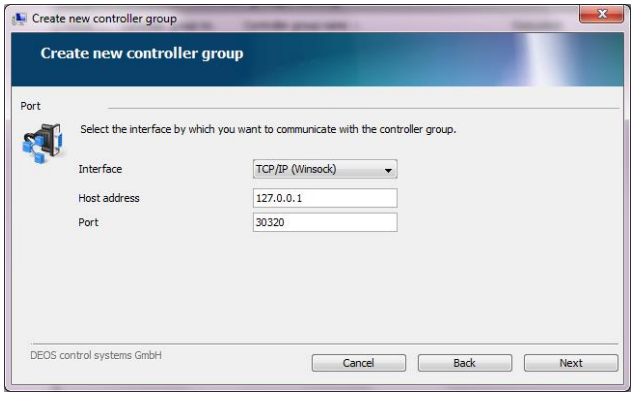
Will man einen neuen Anlageort (OPEN-Steuerung) anlegen, klickt man auf den Menüpunkt:



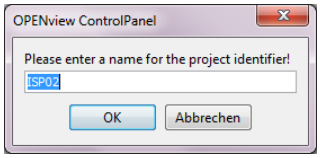
In dem folgenden Fenster zuerst den Namen des Anlageortes eingeben (Beispiel):



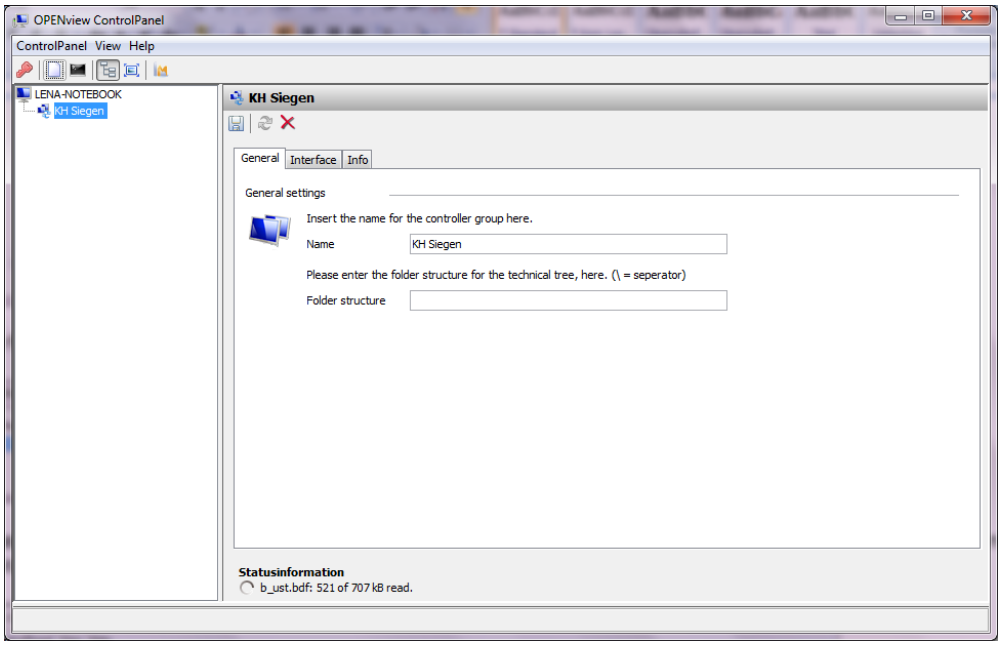
Dann auf „Weiter“ klicken und die Localhost IP-Adresse 127.0.0.1 der OPEN-Steuerung eintragen sowie der Port, der abhängig von der Steuerung variiert. Die benötigte Portnummer kann im Secure Automation Gateway (SAG) nachgesehen werden, Beispiel:



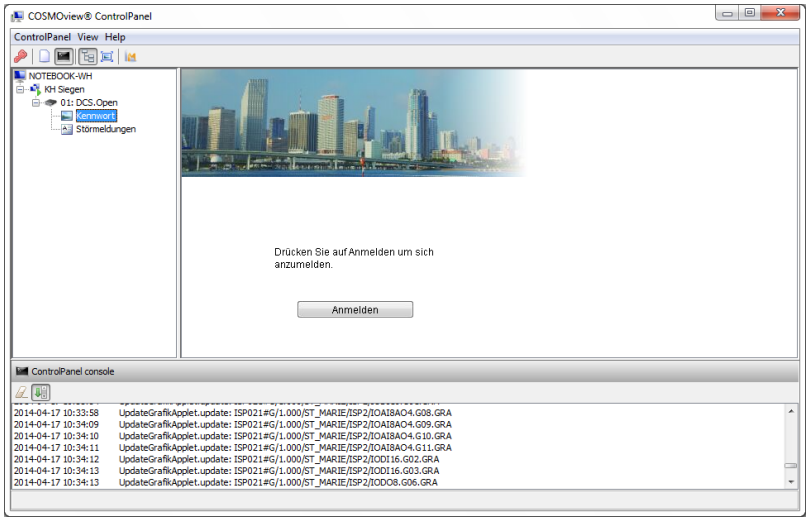
Im folgenden Fenster **keine Änderungen vornehmen** und auf OK klicken:



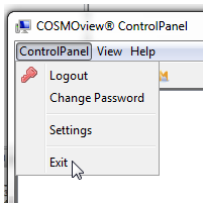
Das Profil wird jetzt angelegt, der Viewer verbindet sich mit der Steuerung und lädt die benötigten Dateien (Grafikdateien usw.) herunter, der Fortschritt wird in der Statuszeile unten angezeigt. Dieser Vorgang kann mehrere Minuten dauern:



Wenn alle benötigten Dateien von der Steuerung heruntergeladen wurden, wird das folgende Fenster angezeigt mit dem Anmeldebutton:



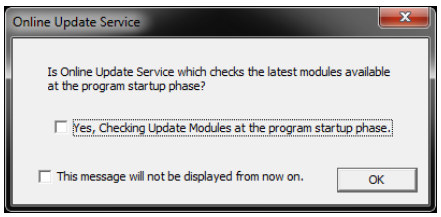
Um den Viewer zu beenden, niemals nur das Fenster schließen, sondern **immer** im Menü „Exit“ wählen:



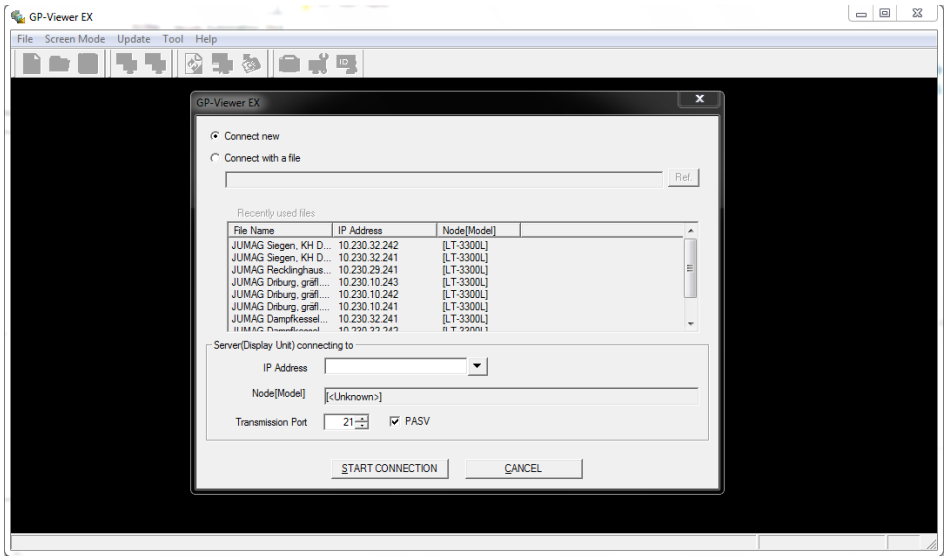
4.4 Zugriffsprofil via GP-Viewer auf Pro-Face Steuerung (Jumag Dampfkessel)

Bei diesem speziellen Zugriffsprofil wird parallel zum Aufruf des GP-Viewers ein SSL-VPN Tunnel (siehe Hinweise zum SSL-VPN-Tunnel weiter oben) aufgebaut, da der GP-Viewer mit mehreren Ports mit der Pro-Face Steuerung kommuniziert.

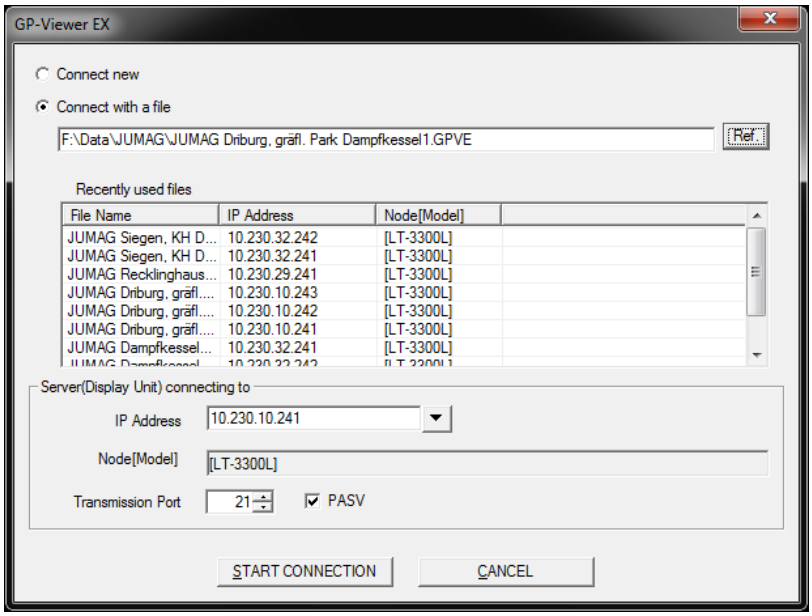
Nach dem erstmaligen Aufruf des GP-Viewer auf einem PC erscheint u.U. eine Kontrollfrage. Hier das Häkchen aus der oberen Checkbox „Yes, Checking Update …“ entfernen, da der installationslose GP-Viewer nicht auf diese Art upgedatet werden kann. Bei der unteren Checkbox “This message will not be displayed from now on“ muss man das Häkchen setzen:



Klickt man auf „ok“, erscheint das folgende Fenster:

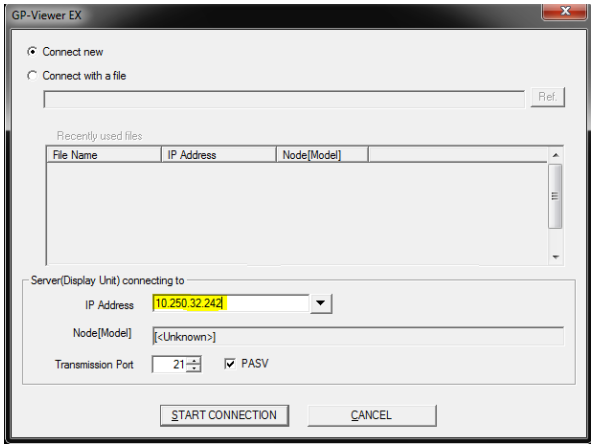


1. Handelt es sich um eine Pro-Face Steuerung, auf die man mit dem SAS schon einmal zugegriffen und die zugehörigen Dateien bereits auf dem SAS abgespeichert hat, wählt man hier „Connect with a file“ aus:

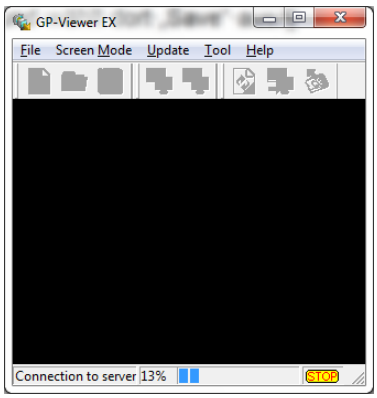


Über den Button „Ref.“ wählt man die gewünschte Profildatei auf dem SAS aus und klickt dann auf den Button „START CONNECTION“. Weiter zu Punkt 3.

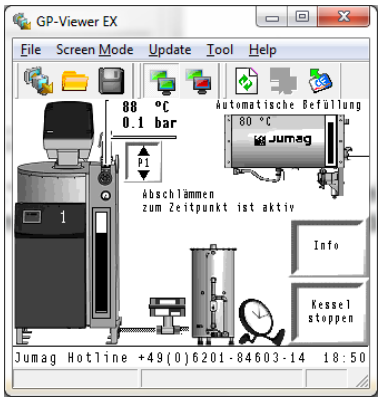
2. Handelt es sich um eine Pro-Face Steuerung, auf die man mit dem SAS bisher noch nicht zugegriffen hat, wählt man hier „Connect new“, trägt die gewünschte IP (aus dem VPN-Netzwerk) ein und klickt dann auf den Button „START CONNECTION“.



3. Die Verbindung zur Steuerung wird jetzt aufgebaut und die benötigten Daten werden heruntergeladen. Der Ladefortgang der Daten wird unten in der Statuszeile angezeigt:

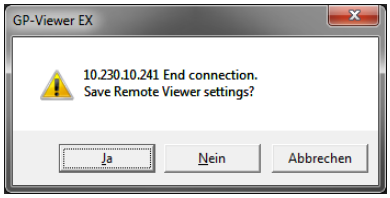


Danach wird das Anlagenbild angezeigt (Beispiel eines JUMAG Dampfkessels):

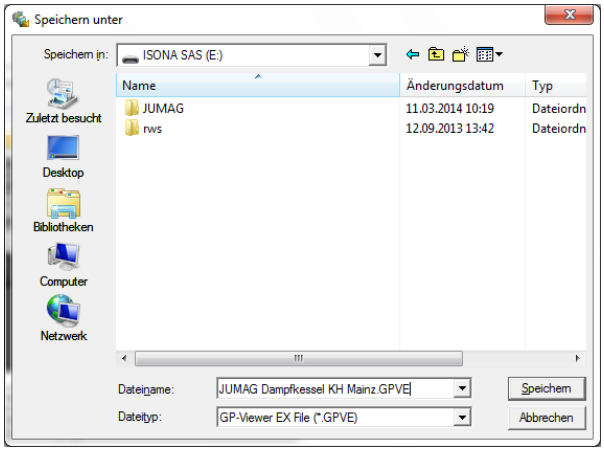


Beenden des GP-Viewers

Wenn man den GP-Viewer beendet, erscheint die Kontrollfrage:



Hier klickt man im Normalfall auf „Nein“, wenn man die temporären Dateien schon auf dem SAS abgespeichert hat. Damit wird der GP-Viewer geschlossen und das zugehörige Verbindungsprofil (SSL VPN-Tunnel) im Secure Automation Stick wird beendet.
War es aber der erstmalige Aufruf einer Steuerung mit dem SAS, klickt man in dem obigen Fenster auf „Ja“. Dann legt man fest, unter welchem Namen diese Dateien abgespeichert werden sollen, der Dateiname sollte aussagekräftig sein wenn man viele Pro-Face Steuerungen im Zugriff hat (Beispiel für JUMAG Dampfkessel):



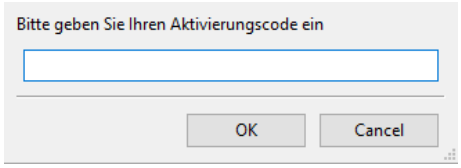
Klickt man auf den Button „Speichern“, wird eine .GPVE-Datei (Konfigurationsdatei) auf dem Secure Automation Stick angelegt sowie ein Unterordner mit den weiteren vom GP-Viewer aus der Steuerung heruntergeladenen Dateien.

5. Stick neu aktivieren und Hilfe im Fehlerfall

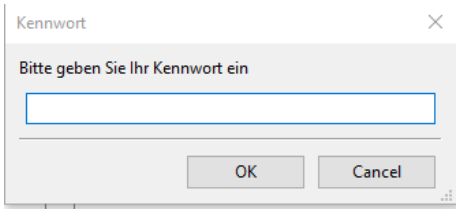
Wenn beim Start des SAS eine Fehlermeldung erscheint, sollte man die genaue Ursache klären.

Auf Rücksprache mit ISONA kann der Stick im Extremfall neu aktiviert werden, indem man rechts unten im SAS-Fenster auf den Button klickt und dann den Button „Neu Aktivieren“ wählt.

Die dann angezeigte Warnmeldung mit „ja“ quittieren, jetzt wird die Eingabe eines Aktivierungscodes verlangt:

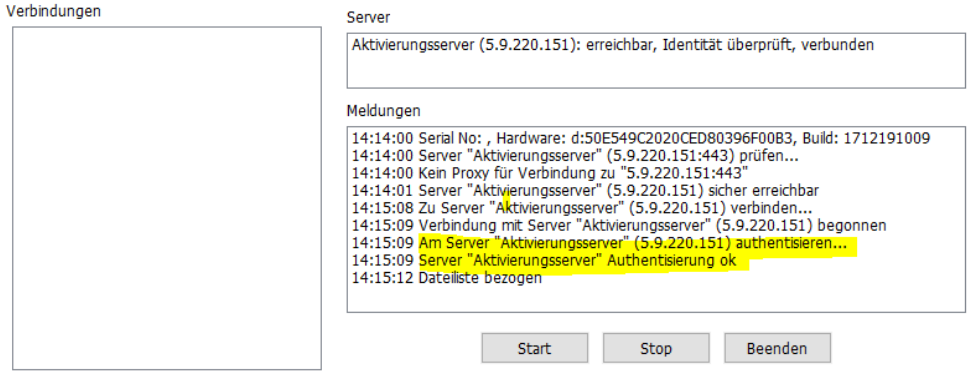


und danach eines Aktivierungskennworts (dies ist NICHT das Kennwort, das man normalerweise beim SAS verwendet!) verlangt:

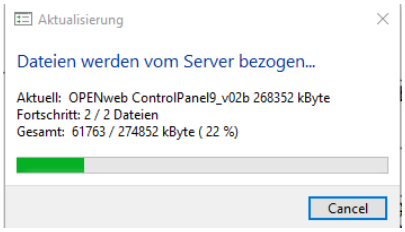


Den Aktivierungscode und das Aktivierungskennwort vorher bei ISONA per Mail an support@isona.de anfordern, dazu unbedingt die Seriennummer des SAS mit angeben!

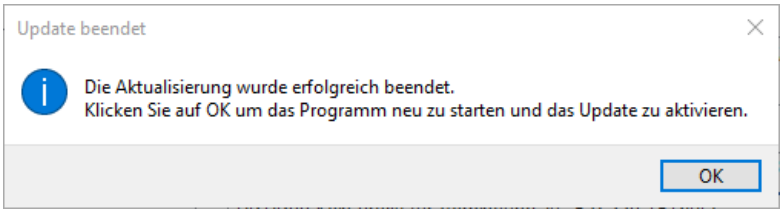
Nach Eingabe des Aktivierungskennworts zeigt sich folgendes Bild:



Jetzt werden die benötigten Dateien vom Secure Automation Gateway geladen:



Nach erfolgreicher Aktivierung des SAS erfolgt diese Meldung:



Nach einem Neustart des SAS

Erweitertes Logging
Wenn im laufenden Betrieb irgendwelche Probleme beim Aufruf eines Profils auftreten, dass findet man im Feld „Meldungen“ immer einen entsprechenden Hinweis auf die Ursache des Fehlers.
Will man diese Meldungen exportieren um sie z.B. dem Support zur Verfügung zu stellen, dann klickt man mit der rechten Maustaste in das Feld „Meldungen“, es erscheint dann das folgende Auswahlmenü:

Mit „Copy to Clipboard“ werden alle Meldungen in diesem Feld in die Zwischenablage kopiert.
Mit „Save as….“ kann man alle Meldungen in diesem Feld in einer Datei abspeichern.
Diese Logs kann man z.B. zu Diagnosezwecke an den Support o.ä. senden.

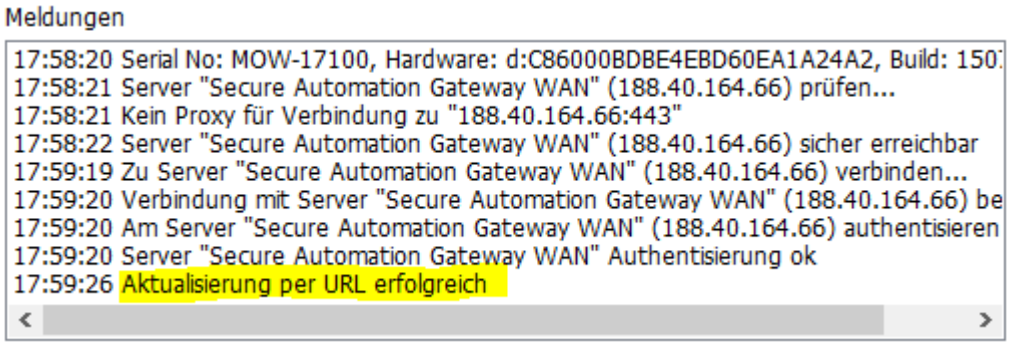
Teilweise sind die Meldungen für Diagnosezwecke nicht detailliert genug. Dann kann man rechts unten im SAS-Fenster auf den Button  klicken. In dem sich öffnenden Fenster aktiviert man dann das Häkchen bei „Debugausgabe“ und schließt das Fenster wieder:

Ab dann werden detailliertere Logeinträge in das Feld „Meldungen“ eingetragen, die man dann per Mail an support@isona.de sendet.

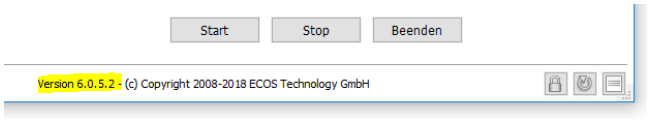
6. Hinweise zum Update des SAS von Version 4.x auf Version 5.x/6.x

Bei einem Update des zentralen Secure Automation Gateways (SAG) von Version 4.x auf Version 5.x oder 6.x wird der Secure Automation Stick (SAS) ebenfalls upgedated.
Je nach Vorversion des SAS kann der Update-Prozess variieren.

Bei neueren SAS 4.x Versionen erfolgt der Update automatisch, wenn man den Stick startet, dies wird entsprechend im Fenster „Meldungen“ angezeigt;

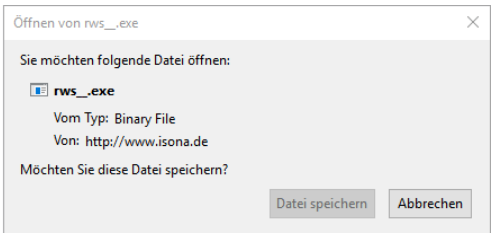


Jetzt muss der SAS beendet und danach neu gestartet werden, um das Update zu aktivieren.
Einen erfolgreichen Update des SAS erkennt man an der Versionsnummer „5.xx“ oder „6.xx“ im Fuß des SAS-Fensters (Beispiel):

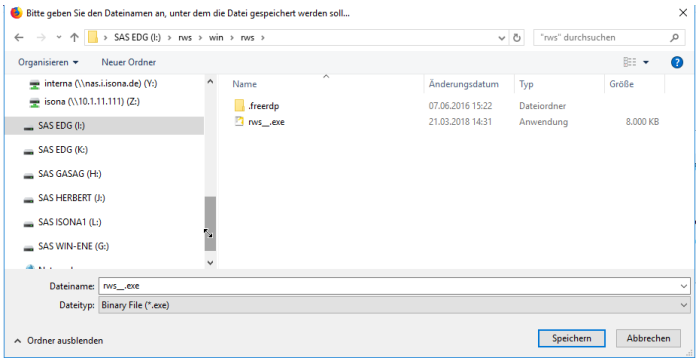


Sollte nach dem Start des SAS das SAS-Fenster NICHT erscheinen, dann müssen Sie folgendermaßen vorgehen, um den SAS upzudaten:

1. Bei ISONA einen Aktivierungscode und ein Aktivierungskennwort anfordern unter support@isona.de, dabei unbedingt die Seriennummer des SAS in der E-Mail mitteilen!
2. Auf dem SAS im Ordner \rws\win\rws alle .exe-Dateien löschen
3. Von der Internetadresse www.isona.de/download/SAS/rws__.exe diese Datei herunterladen:



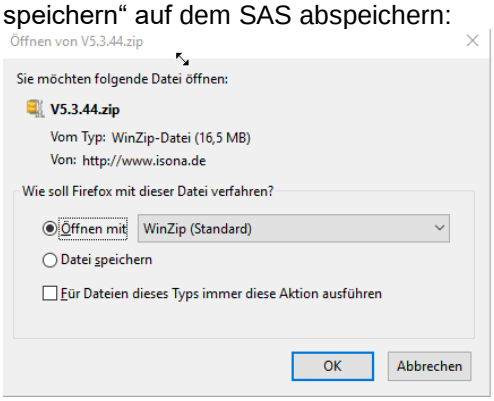
und auf dem Stick in den Ordner \rws\win\rws abspeichern:



Danach Stick neu starten.

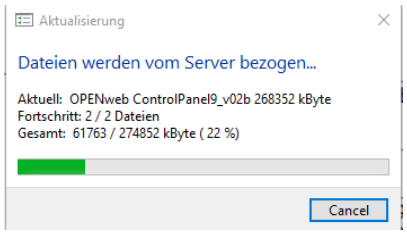
In seltenen Fällen führt die oben beschriebene Prozedur nicht zum Erfolg, in diesem Fall müssen Sie folgendermaßen vorgehen:

1. Bei ISONA einen Aktivierungscode und ein Aktivierungskennwort anfordern unter support@isona.de, dabei unbedingt die Seriennummer des SAS in der E-Mail mitteilen!
2. Auf dem SAS alle Dateien löschen
3. Über den Link http://www.isona.de/download/SAS/sas.zip die zip-Datei herunterladen und mit „Datei speichern“ auf dem SAS abspeichern:

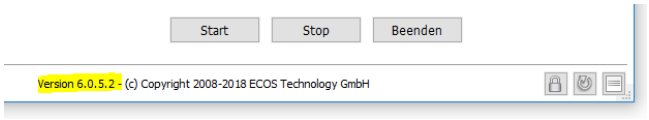


4. Die o.g. zip-Datei (z.B. mit WinZIP) entpacken und den Inhalt auf dem SAS abspeichern
5. Die zip-Datei auf dem SAS löschen
6. Jetzt die .exe-Datei auf dem SAS starten und wie oben beschrieben den Aktivierungscode und das Aktivierungskennwort eingeben

Es werden jetzt eine Reihe von Dateien vom SAG-Server auf den Stick geladen, was einige Minuten dauern kann:



Danach den SAS neu starten, die neue Version wird dann im Fuß des SAS-Fensters angezeigt:



7. Kontakt

ISONA GmbH
Tulpenstraße 5
D-55276 Dienheim

E-Mail support@isona.de
Internet www.isona.de