Secure Automation Webclient (SAW)

Sicherer, installationsloser Zugriff auf Automationsanlagen

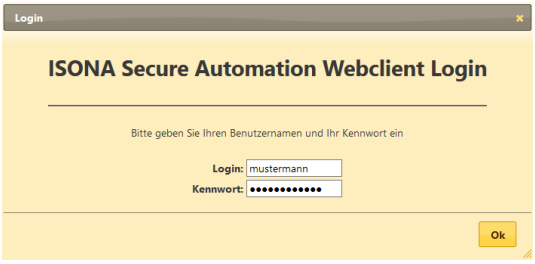
Diese Dokumentation beschreibt die Handhabung des Secure Automation Webclients (SAW).

Wichtiger Hinweis: Die Screenshots in diesem Handbuch sind lediglich Beispiele. Je nach Betriebssystem- und Browserversion können diese beim Benutzer anders aussehen!

Einrichten des Secure Automation Webclients auf einem PC

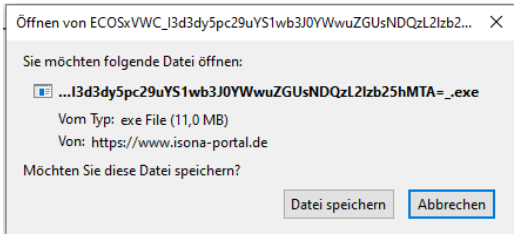
Soll der Secure Automation Webclient zum ersten Mal auf einem PC/Notebook gestartet werden, dann muss man eine spezielle Internetadresse in einem Browser starten. Diese Internetadresse ist auf dem Einlegeblatt der DVD-Box vermerkt oder wurde Ihnen vom Administrator mitgeteilt.

Nach dem Aufruf (Beispiel für eine Internetadresse: https://www.isona-portal.de/vwc) in einem Browser, erscheint das folgende Anmeldefenster (Abb. ähnlich):



Hier geben Sie den ihnen mitgeteilten Benutzernamen sowie das statische Kennwort ein.
Wenn die eingegebenen Daten richtig sind, wird im Browser ein Downloadlink angezeigt:

Speichern Sie die heruntergeladene Datei auf dem PC ab, am besten in den Ordner „Desktop“. Sie dürfen den Dateinamen dabei nicht verändern, sonst funktioniert der Virtual Web Client nicht mehr! Denn in dem Dateinamen ist der Zielserver enthalten (verschlüsselt), auf den sich der Virtual Web Client verbindet.



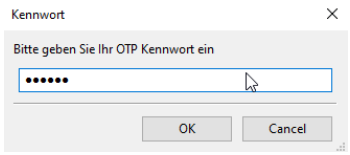
Tipp: Diese .exe-Datei kann man auf mehrere Windows PCs, Notebooks oder Windows Tablets kopieren, um auch von dort aus den Virtual Web Client aufzurufen zu können.
Jetzt kann man das Browserfenster schließen.

Benutzung des Secure Automation Webclients

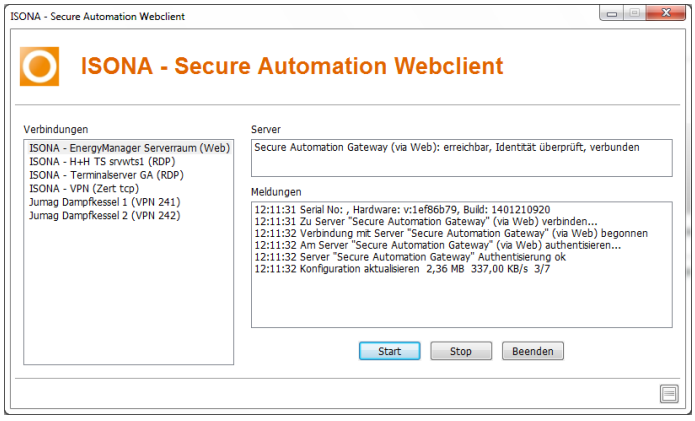
Diese heruntergeladene Datei muss man mit einem Doppelklick starten, wenn man den Secure Automation Webclient aufrufen möchte.

Es erscheint dann das folgende Anmeldefenster, in dem man den Benutzernamen und das statische Kennwort eingibt:

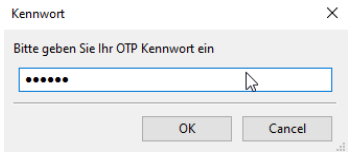
Hat man die richtigen Anmeldedaten eingegeben, erscheint das folgende Fenster für die Eingabe des Einmalkennworts, das man per OTP-Token, per SMS, per E-Mail oder per Authenticator-App (auf dem Smartphone oder Tablet) erzeugt hat:



Danach öffnet sich das Windows-Fenster des Secure Automation Webclients (Abb. ähnlich):

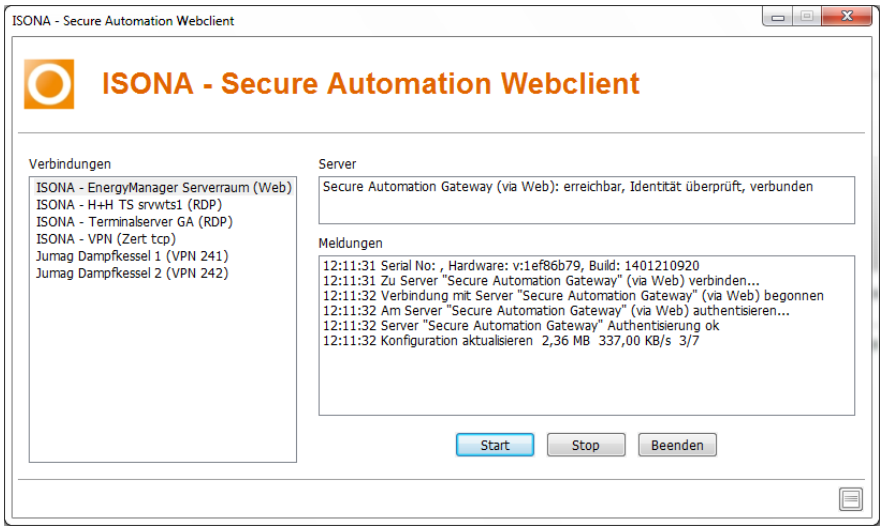


Wenn man jetzt ein Verbindungsprofil startet, erscheint beim allerersten Mal ein Eingabefeld zur sicheren Authentifizierung des Benutzers:



Hier tragen Sie die Zahl ein, die Sie mit Ihrem OTP-Token erzeugt haben (dazu die Taste am OTP-Token kurz drücken).

In dem Fenster des Secure Automation Webclients sieht man jetzt alle für den angemeldeten Benutzer freigegebenen Verbindungsprofile (Anlagen):



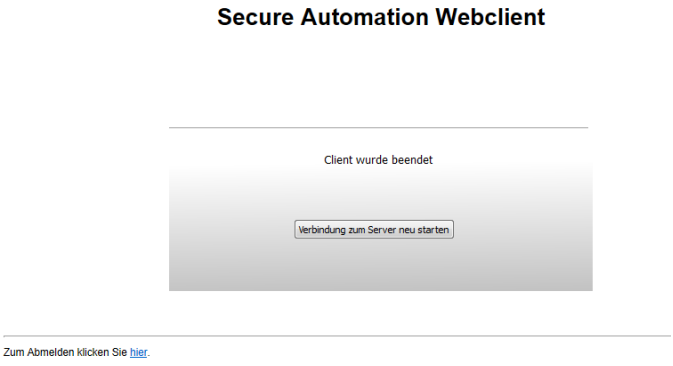
Um auf eine Anlage zuzugreifen, wird diese mit einem Doppelklick auf den Verbindungsnamen aufgerufen. Oder man markiert den Eintrag mit der Maus (wird dann blau hinterlegt) und klickt danach auf den Button „Start“.
Je nachdem, welche Applikation dem Verbindungsprofil hinterlegt ist, wird ein Browser, ein VNC-Client oder ein RDP-Client o.ä. geladen und man wird mit der Anlage verbunden.

Wichtig: Dies funktioniert auch dann, wenn RDP oder VNC im Firmennetzwerk gesperrt sein sollte, da die Clients in einer isolierten Sandbox ablaufen.

Um eine Verbindung zu einer Anlage zu beenden kann man entweder das zugehörige Browser- bzw. Client-Fenster schließen oder man klickt auf den Button „Stop“.

Mit dem Button „Beenden“ wird der Secure Automation Webclient ganz geschlossen.

Danach muss man sich am folgenden Browserfenster über den Link „Zum Abmelden klicken Sie hier“ abmelden, das Browserfenster wird dann geschlossen:



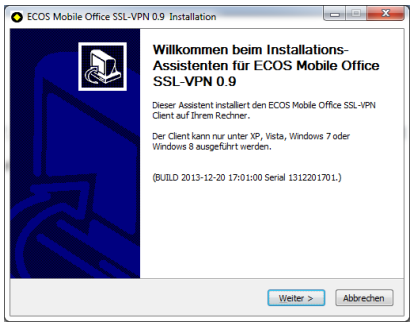
Oder man kann über den Button „Verbindung zum Server neu starten“ den Secure Automation Webclient bei Bedarf erneut starten.

Besonderheiten bei SSL VPN Profilen

Der Secure Automation Webclient kann nicht nur getunnelte Applikationen starten, sondern auch einen transparenten SSL VPN Tunnel aufbauen. Dies wird in den Profil-Einstellungen des ISONA Secure Automation Gateways (SAG) konfiguriert.

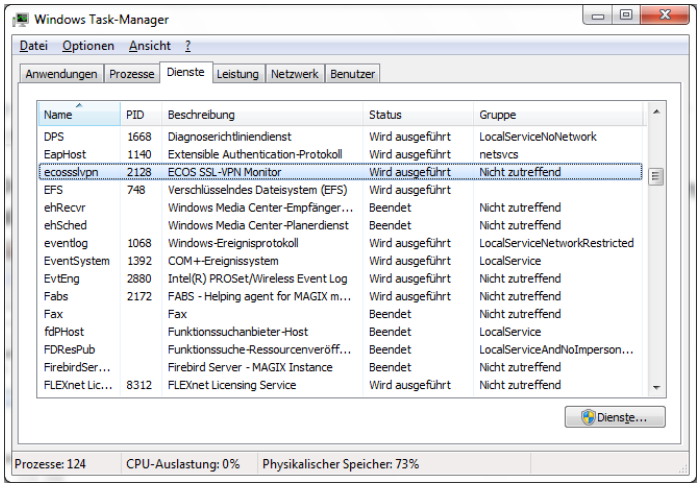
Wichtig: falls es bei gewissen Anwendungsfällen zu Problemen mit dem transparenten VPN-Tunnel kommt, sollte alternativ das Produkt ISONA Secure Automation OpenVPN Zugriff (SAO) verwendet werden!

Startet man ein Verbindungsprofil mit hinterlegtem SSL-VPN, dann wird beim allerersten Start auf dem Windows PC ein VPN-Hintergrunddienst installiert, für den man Admin-Rechte benötigt.
Es erscheint das folgende Installationsfenster:

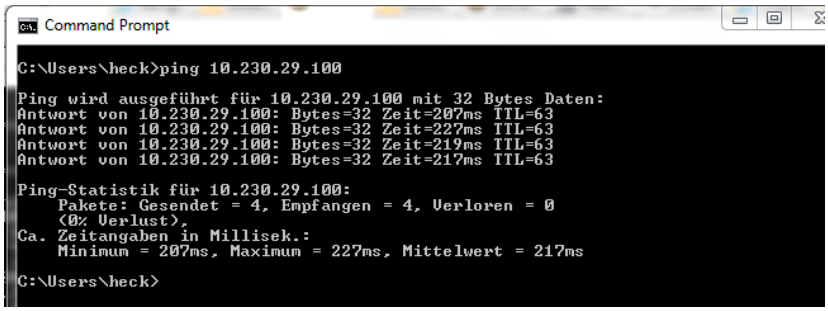


Klickt man auf „Weiter“, wird ein kleines Softwaremodul (Dienst) installiert, je nach Windows-Konfiguration kann noch die Eingabe des Admin-Kennworts notwendig sein.

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



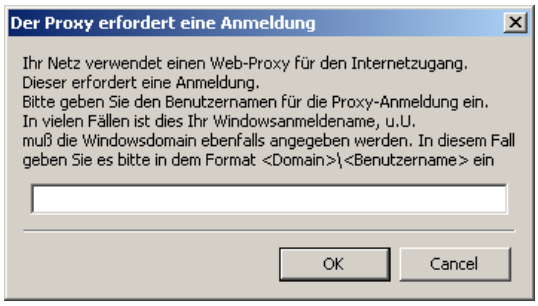
Um zu überprüfen, ob der SSL VPN-Tunnel erfolgreich aufgebaut ist und die Steuerungen darüber auch erreichbar sind, kann man einen Ping-Test ausführen (soweit die Geräte/Steuerungen auf einen Ping antworten) auf die ext. IP-Adresse (Beispiel):



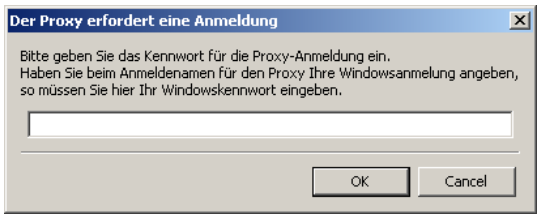
Jetzt kann man mit beliebigen Programmen und Ports auf die Steuerung zugreifen (z.B. mit einem Programmiertool oder per FTP usw.).

Besonderheiten, wenn in einem Firmennetzwerk ein Proxy verwendet wird

Wenn man sich in einem Firmennetzwerk befindet bei dem ein Proxy vorgeschaltet ist, erscheint nach dem Login am Secure Automation Webclient ein Fenster zur Webproxy-Anmeldung, in das man zuerst den Windows-Anmeldenamen (bei manchen Firmennetzwerken muss dabei der Domainnamen vorangestellt werden) eingibt:



Wenn man auf OK klickt erscheint ein weiteres Proxyfenster, in das Sie normalerweise ihr Windows-Anmeldekennwort eingeben müssen:



Bei Problemen wenden Sie sich an Ihren Administrator.