Remote Access Support Solution
User Manual

Version: 1.0
Date: 24-11-2022

Table of contents

1. Introduction

Agrifirm remote accounts are used to perform support on the IT-environment of Royal Agrifirm Group. To perform support the Remote Access Support Solution is used to manage and secure remote access to servers and clients for IT-administrators and vendors.

2. Purpose of document

The purpose of this document is to describe our Remote Access Support Solution in such a way that IT-professionals will get a basic understanding of our remote access environment.

3. Scope

This user manual consists of an description of our Remote Access Support Solution. To achieve a basic understanding of our remote access environment, the following items will be described:

- Logging onto our environment.
- Remote Access Consoles.
- Access to remote objects.
- Important functions.
- Important references.

4. Description of our Remote Access Support Solution

To achieve a basic understanding of our remote access environment read through below paragrafs.

4.1 HOW TO LOGIN ONTO OUR ENVIRONMENT

The tool that makes our Remote Access Support Solution possible is BeyondTrust and can be accessed in two ways from a browser or the client.

Logging in from the browser

1. From a modern browser (Google Chrome, Microsoft Edge or Mozilla Firefox), go to the following URL: https://remoteaccess.agrifirm.com from an inprivate/incognito browser session.
2. Login with your remote support account and use SAML authentication. Approve the login from the MFA-authenticator.
   - If you do not have MFA configured, please see paragraph 4.5 reference for more information about how to configure MFA (our servicedesk can provide assistance if needed).The remote access home page will become visible.

   In the home page the following tabs are mainly important for users:
   - MyAccount: contains your e-mail address. Also contains the Privileged Web Access Console and the download and open link for the Desktop Access console.
   - Vault: gain access to your saved user credentials.
3. Go to the tab “My Account” and open: “PRIVILEGED WEB ACCESS CONSOLE”. The Privileged Web Access Console will open and the remote objects for which you are authorized will become visible.

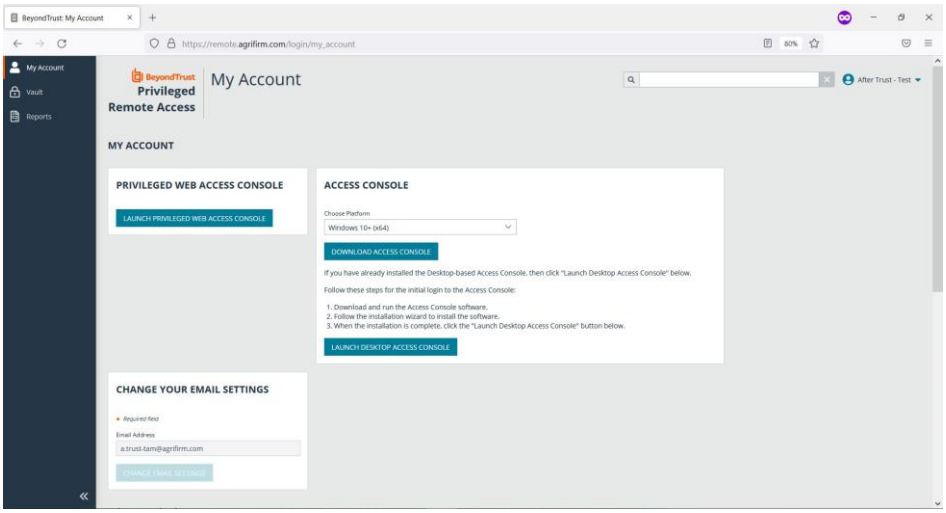


Figure 1: The remote access home page

Note:

- If you get the error “Login failed. Please try again”. Please make sure you are selecting the option: use SAML authentication.

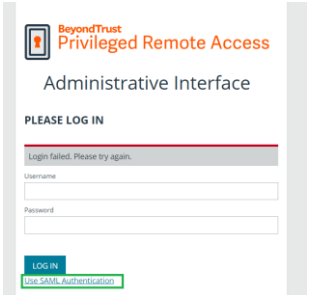


Figure 2: Use SAML authentication when logging in

Logging in from the client

To login from the client, you need to install prerequiste files which can only be accessed by logging in from the browser.

Installing the prequisite files:

1. From a modern browser (Google Chrome, Microsoft Edge or Mozilla Firefox), go to the following URL: https://remoteaccess.agrifirm.com from an inprivate/incognito browser session.
2. Login with your remote support account and use SAML authentication. Approve the login from the MFA-authenticator.
   - If you do not have MFA configured, please see paragraph 4.5 reference for more information about how to configure MFA (our servicedesk can provide assistance if needed).
3. The remote access home page will become visible. Go to the tab “My Account”.
4. Under Access Console, select your OS (for example: Windows 10+ (x64). Download the Access Console software. Follow the installation wizard to install the software and uncheck: application autostart.
   - Note: this setup can also be used to upgrade your existing client. Instead of “install”, the button “upgrade” will appear.

Opening the client from startmenu:

1. Click on start, go to all programs and under the folder Bomgar select Access console.
2. Select SAML credentials, the preferred language and press login. The Privileged Remote Access Console will open as an application and the remote objects for which you are authorized will become visible.
   - Note: If you get the login error: “SSO - Sorry, but we’re having trouble signing you in”. Please see the below login method. This means that the wrong account is automatically selected from local cached credentials.

Opening the client from the home page:

1. From a modern browser (Google Chrome, Microsoft Edge or Mozilla Firefox), go to the following URL: https://remoteaccess.agrifirm.com from an inprivate/incognito browser session.
2. Select SAML and Login with your remote support account. Approve the login from the MFA-authenticator.
3. The home page of BeyondTrust will become visible. Go to the tab “My Account”.
4. Click on the "Launch Desktop Access Console" button.
5. The file “rep-script.brcs-agrifirm” will be downloaded. Open this file, you will automatically be logged in. The Privileged Remote Access Console will open as an application and the remote objects for which you are authorized will become visible.

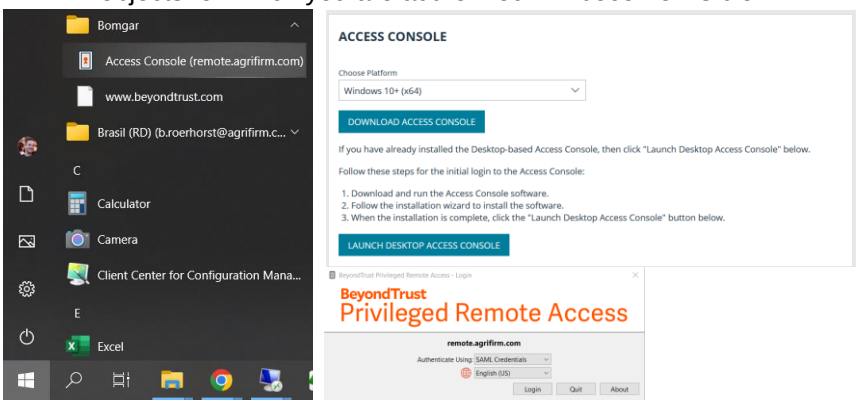


Figure 3: The cliënt and login screen

4.2 DIFFERENT REMOTE ACCESS CONSOLES EXPLAINED

As mentioned in the before paragraf. Access to remote objects can be given from:

1. Privileged Web Access Console.
2. Privileged Remote Access Console.

Within each access console the following will be found:

WHAT	Explanation
Jump group names	Catagories for one ore more remote objects. Example: BE-Grobbendonk-OT-Servers which contains all Grobbendonk OT-servers.
Hostnames/IP	Contains the IP\hostname from one remote server\client object. Example: BEOPVMWAP001 which is an application server remote object.
Jump methods	This is the protocol which will be used to connect to the machine. Agrifirm Group IT supports the following jump methods: 1. Jump client: Connection runs via an local installed BeyondTrust agent. Used to view an existing session from a screen sharing connection. ✓ This connection method supports the most functionalities (FileTransfer Commander, CMD, Registry, Systeminformation). ✓ This connection method supports single sign on (SSO). ✗ This connection is limited to one session at the same time. ✗ This connection opens slower then for example RDP. 2. Remote RDP: Connection via the MSTSC Remote desktop protocol. Used to login or take over an existing session. ✓ This connection method supports two parallell sessions. ✗ This connection method support less functionalities than the agent method. Also manual login information is needed for access. 3. Remote Shell: SSH connection via console\CMDlet. 4. Tunnel Jump: client-to-client connection via a tunnel.

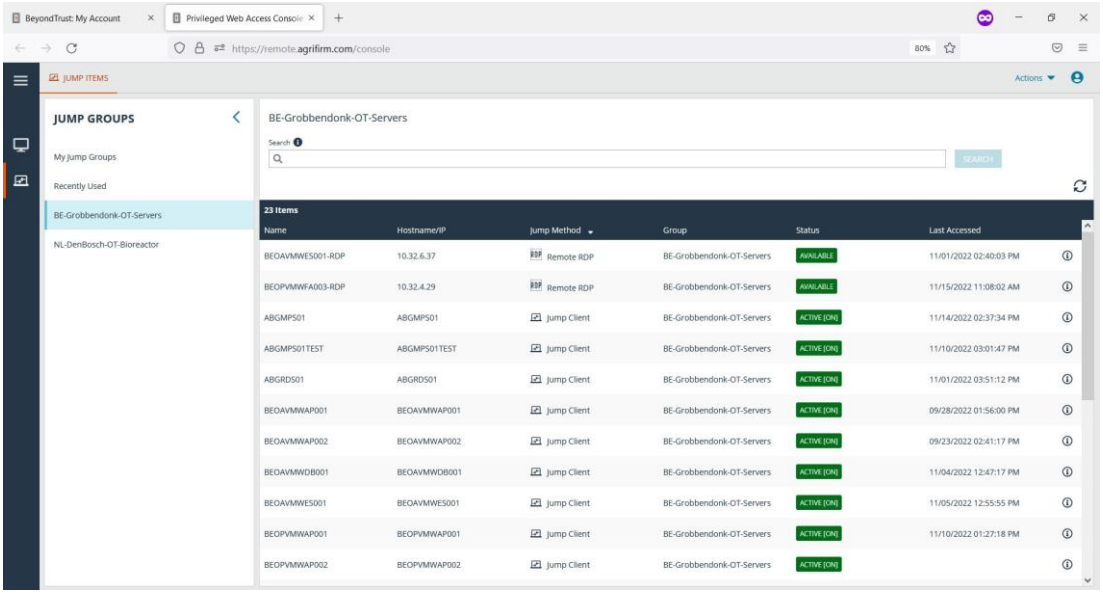


Figure 4: Example of the Privileged Web Access Console

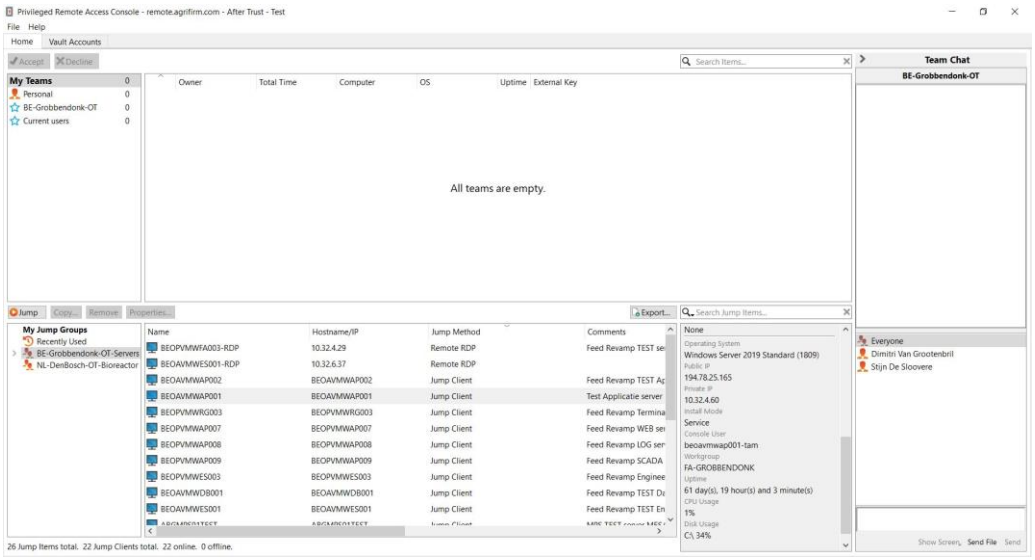


Figure 5: Example of the Priviliged Remote Access Console

The main difference between the two consoles is that the remote console has more features then the webconsole. The Remote Access console:

- Generally shows remote object information more clear:
  - Remote object information is immediately available.
  - Vault accounts are reachable from a tab in the top left corner.
  - Additional columns: comments and tags are automatically added.
- The Remote Access console has a easy to access search function in the middle rightside of the screen, next to the Export button.
  - It is possible to do search query's based on IP, Countrycode like BE or tags.
  - Supervisor roles (which are given to Agrifirm Functional/Technical administrators) are the only ones that may change the remote object comments and tags. These changes are then centrally applied for everybody.
- Supports team chat.
- Supports one additional connection method: Tunnel jump which the Web Access console doesn't support (see paragraph 4.4 for more information).

Our advice is therefore to mainly use the remote access console.

4.3 GAIN ACCESS TO REMOTE OBJECTS

To access an remote object. Click on the Jump group and select the remote object and click on jump or twice click on an remote object to open the machine

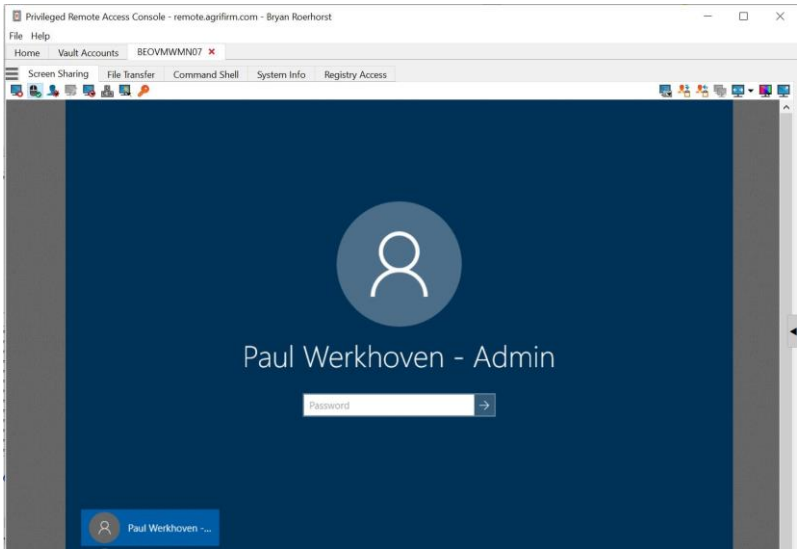


Figure 6: Remote object: beovmwmn07 opened

When loggin in you may get an additional screen, which asks to specify the reasoning to access the machine. See our remote access policy for more information (reference is in paragraph 4.5).

To disconnected an remote object session click on close and then on end session.

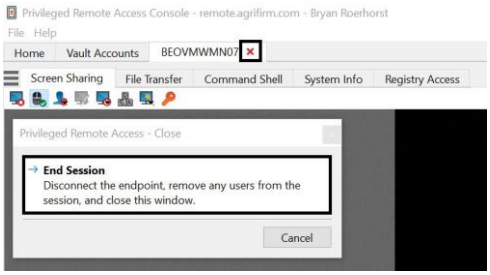


Figure 7: example of a disconnect

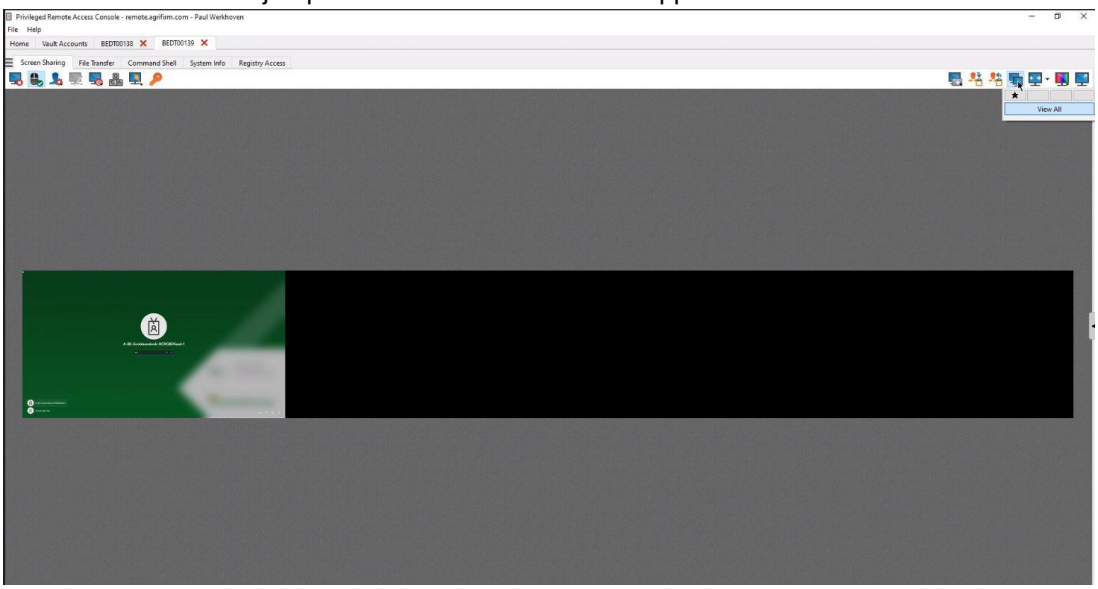
4.4 IMPORTANT FUNCTIONS

This paragraph describes important remote access functions.
Note: the functions may differ with each of the connection method used.

Screen Sharing function

When using the Jump client connection method it is possible to view multiple or selected screens via the screensharing function. The RDP method also support screen features. The function can be accessed via tab: Screen Sharing and via top rightside screen icons.

- Note: the jump client connection method supports the most screen features.



File Transfer functions

When using the Jump client connection method to open a remote object, it is possible to copy files from an commander interface to an remote object via the function File Transfer. This function is only available within this connection method.

With the RDP connection method it is only possible to copy/paste files via the default clipboard.

For our rules regarding File Transfer see our remote access policy (reference is in paragraph 4.5).

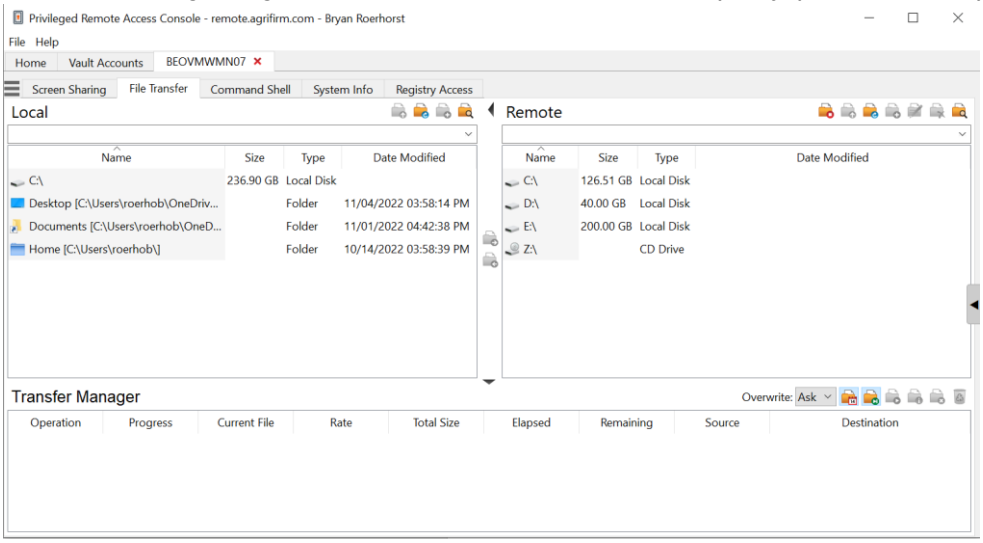


Figure 8: Jump cliënt filetransfer screen

Tunnel Jump Loopbackadapter function

As mentioned in paragraph 4.2 the method Tunnel Jump can only be used in the Priviliged Remote Access Console and is a tunnel connection solution.

This connection in an tunneling method and is meant for remote support users that only want to connect directly from an local management application to our environment.

- For example: this is useful in the context of taking over PLC's.

The Tunnel Jump working can be summarized in one sentence:
"By using the local loopback adapter (127.0.0.1), a one-to-one tunnel connection is set up to a remote object via a in our Remote Access Support Solution defined jump point machine which listens on specific ports and is preconfigured to redirects specified incoming port connections."

To use a Tunnel Jump following steps are needed:

1. To use a Protocol Tunnel Jump double click on a tunnel jump remote object. A session appears in your access console.
2. Click the Protocol Tunneling button to establish the connection. Connection information and port indicated will be displayed.
    - Note: If screen recording is enabled a prompt appears. Click OK to continue. If enabled also an indicator will appears at the top of your session screen.
3. Start the local management application. To perform tasks on the remote system. Configure the local management application to connect via 127.0.0.1 and use the ports indicated to connect from the application through the Jumpoint.
    - In the following printscreens examples we use VNC. Other local application can be for example: WinCC or Siemens S7 class software.

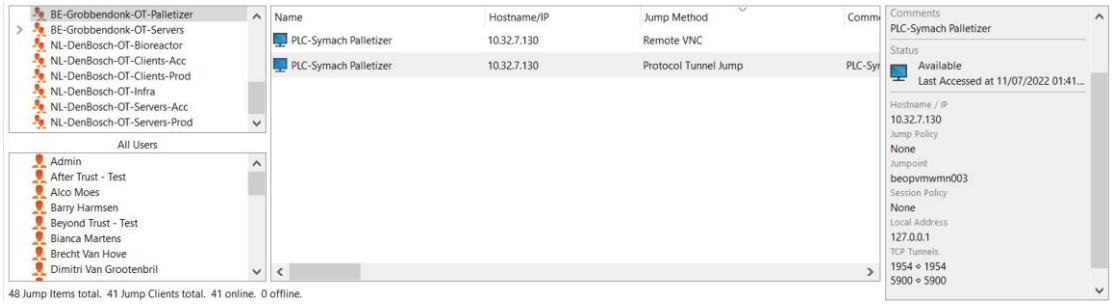


Figure 9: Example of the Tunnel Jump remote object (step 1)

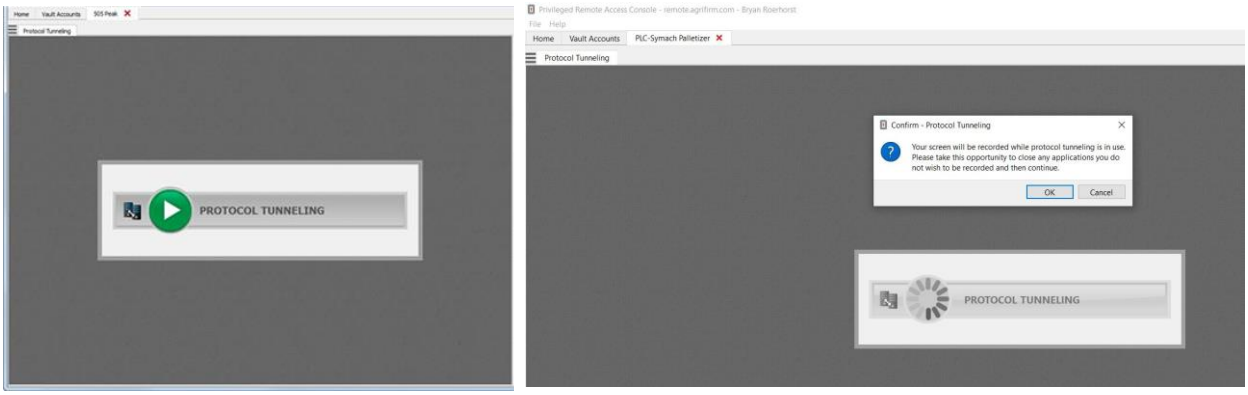


Figure 10: Example of connecting via Tunnel Jump (step 2)

Figure 11: Example of an established connection (step 2)

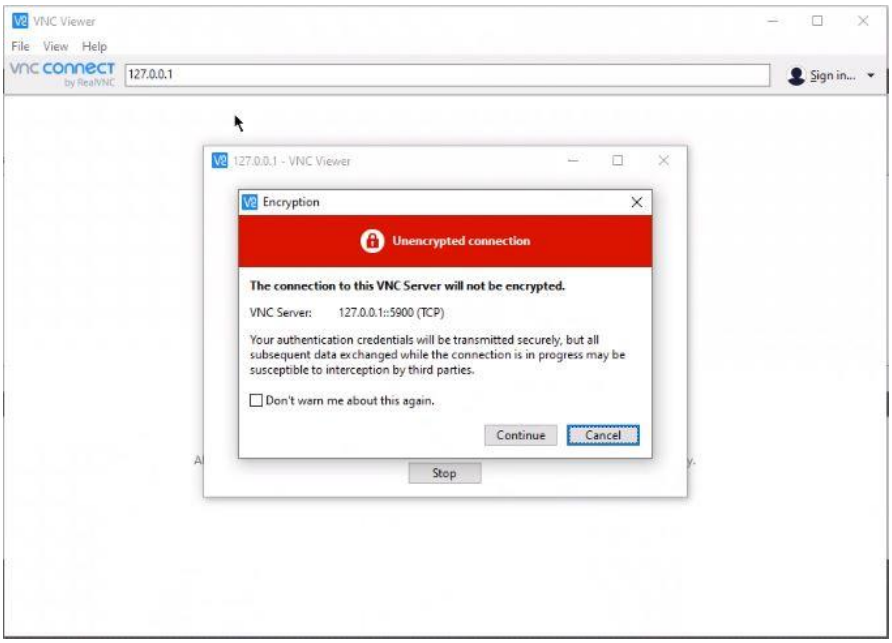


Figure 12: Example of connecting to 127.0.0.1 from a management application (step 3)

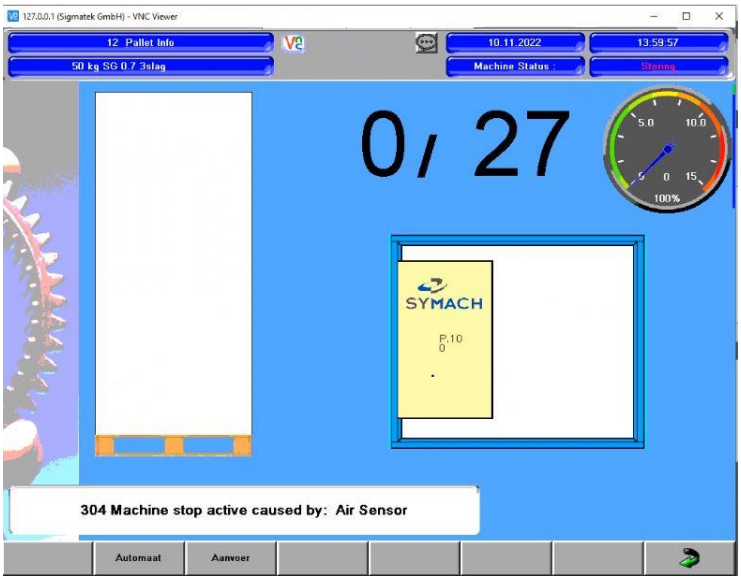


Figure 13: Result of connecting via Jump Tunnel method (step 3)

4.5 IMPORTANT REFERENCES

For more information about the policy and regulations regarding the usage of our Remote Access Support Solution see: Remote Access Support Policy v1.0.pdf. Note the policy's in this document are mandatory for external IT-administrators that want to provide support on our environment.

For our Remote Access Support Solution MFA is mandatory. For more information about the configuration of MFA see:: "Agrifirm EN Configure MFA User Account V1.2.pdf".

For more information about the policy and best practices regarding setting up virtual machines, see "Agrifirm Group IT VM template.pdf".

Agrifirm Group BV

Landgoedlaan 20, 7325 AW Apeldoorn, The Netherlands
PO Box 20000, 7302 HA Apeldoorn, The Netherlands

T +31 88 488 10 00
F +31 88 488 18 00

info@agrifirm.com
www.agrifirm.com