



Manual login to the RA environment (macOS)

Remote Access Microdata

Foreword

Welcome to this document designed to guide you through setting up a connection to the Remote Access environment on a macOS system. This particular environment uses a VPN combined with RSA tokens for strong authentication, which ensures secure access to the Remote Access environment.

The following sections detail the steps that must be performed to successfully connect to the Remote Access environment.

Table of contents

Installation preparation and system requirements	3
Set up VPN connection in FortiVPN client.....	4
Configuring the VMware Horizon Client and connecting to the RA environment	7
Useful information	11

Installation preparation and system requirements

Before you begin setting up the Remote Access Microdata session, it is essential to ensure that your workstation meets certain requirements. Following are the installation preparations and system requirements:

1. VPN Client:

- Ensure that the VPN client provided by CBS is installed on your workstation.

2. VMware Horizon Client:

- Install the VMware client on your system. You can obtain the latest version from the official VMware website using the following link for Mac: [click here](#)
- Under “Select Version”, select the latest version available and follow the instructions to download and install the client.

3. System requirements for Remote Access Microdata session:

- Make sure the system meets the minimum system requirements to ensure smooth operation of the Remote Access Microdata session.
- At CBS, we follow a T-1 policy, which means that the Horizon Client and OS must comply with specific criteria. Further information about this can be found on the RA information page.

Required Internet Connectivity

Below traffic to VPN gateway (87.213.43.223)

IPSEC and IKE (UDP on port 500)

FW1_scv_keep_alive (UDP port 18233)

HTTPS (TCP 443)

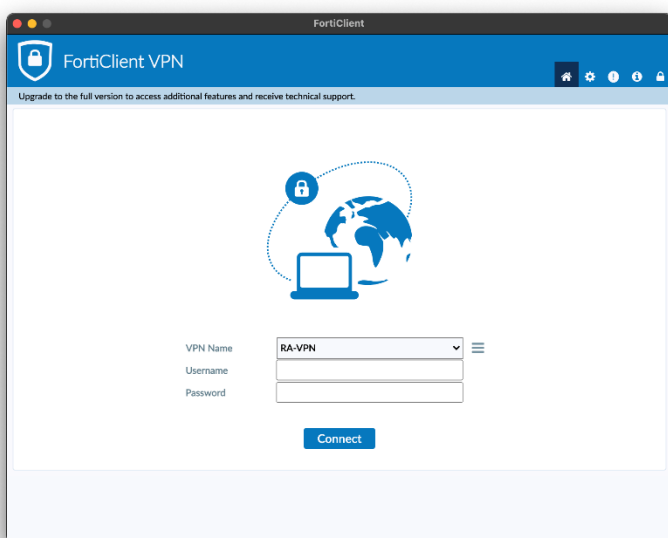
Set up VPN connection in FortiVPN client

Before you can access the Remote Access environment, it is necessary to set up a VPN connection to CBS.

This is done as follows:

1. Open the **FortiVPN client** on your laptop or desktop

The screen below will appear



If you have a (physical) RSA hardware token, enter the following:

- at Username: your 4 letter username (without @remoteaccess.cbs.nl)
- at Password: the PIN code + RSA token code of the hardware token (without the '+' character).

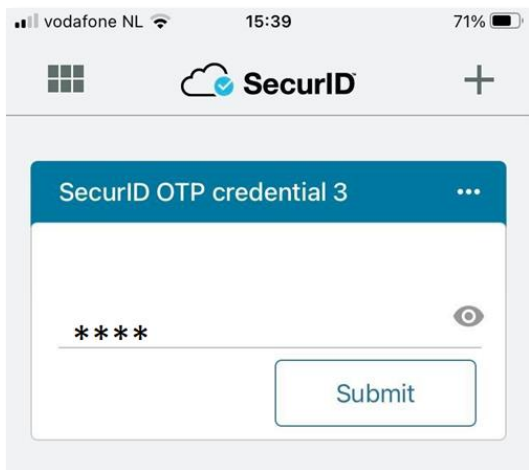
If you own an RSA software token, follow the steps below:

Side note: The RSA application on your phone always shows an 8-digit token code. Even if you leave the field blank OR enter an incorrect PIN. This is because of security reasons.

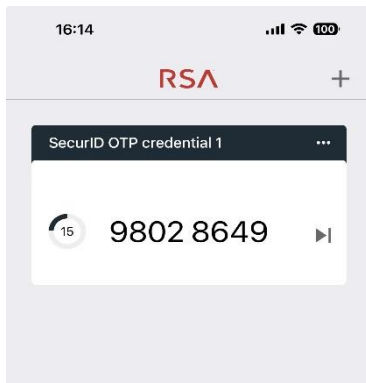
Tip: when in doubt whether you have entered your correct personal PIN, close the RSA application and start again.

To log in with the RSA software token in the FortiVPN client, proceed as follows:

1. Launch the **RSA application** on the mobile device and open the **FortiVPN client** on the laptop or desktop.
2. In **FortiVPN client**, under Username, enter your **4-letter username**.
3. In the **RSA application**, enter your **personal PIN** and press **Submit**



4. Next, the 8-digit token code is generated



5. Enter these 8 digits in FortiVPN-client at **Password** and press **Connect**

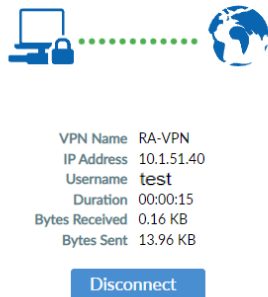
VPN Name	RA-VPN	⌵	☰
Username	test		
Password	••••••••		
<div>Connect</div>			

NOTE

When FortiVPN client asks for an **'SMS'** and/or **'Answer'** after entering a correct token code, wait for the 8 digit token code in the RSA application to jump to a new token code and then enter the new token code.

After **5x incorrect login**, your token is locked and you will need to contact Microdata Services.

6. The following screen will appear if a VPN connection has been successfully established to CBS.



This connection blocks all Internet and network connections and only allows connection to the CBS Remote Access environment.

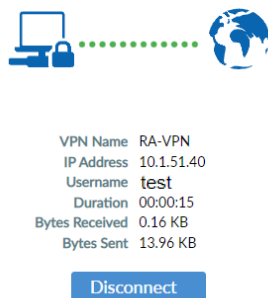
If a VPN is successfully set up, it is only possible to connect to the CBS Remote Access environments. Other Internet and network addresses are blocked.

To exit the VPN, click on the FortiVPN client icon at the top of the macOS screen and choose **Disconnect RA-VPN**. After this, all Internet and network addresses are accessible again.

Configuring the VMware Horizon Client and connecting to the RA environment

Initial configuration of the VMware client is an essential step when using it for the first time. Follow the steps below to complete it:

1. Set up **VPN connection** in the **FortiVPN client**

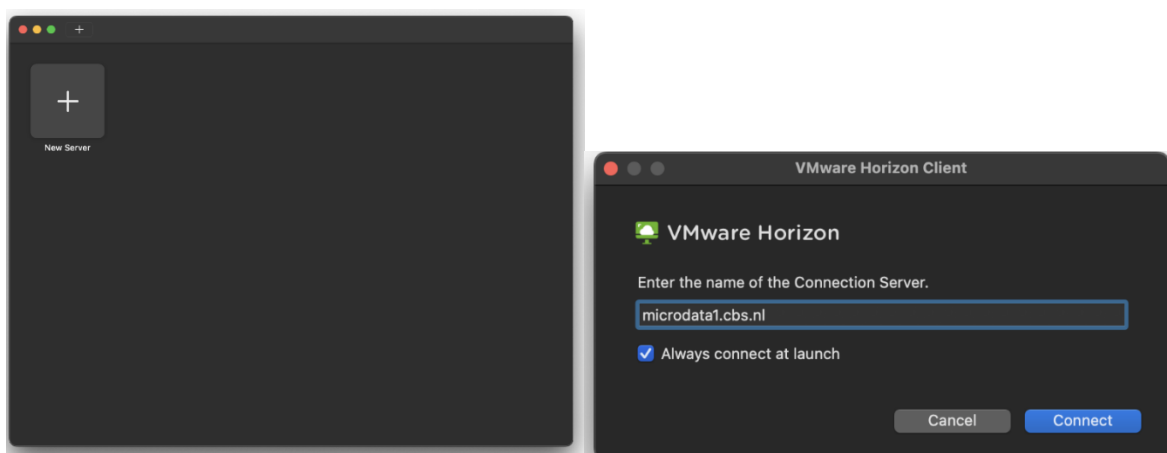


2. Open **VMware Horizon Client**

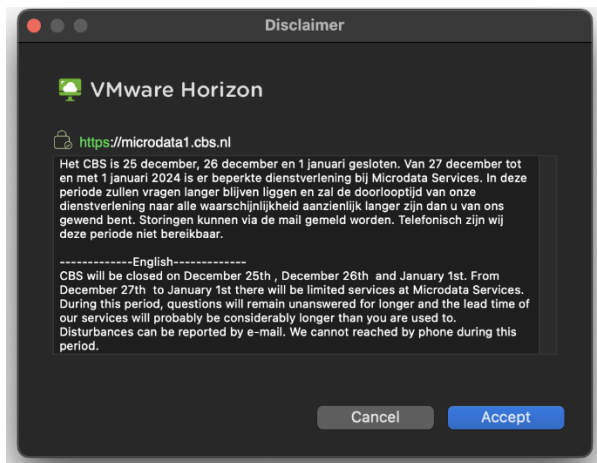
If you do not already have the VMware client installed, follow the installation instructions as mentioned earlier.

*The download link can be found above under **Installation Preparation and System Requirements***

3. Click **Add Server**, then enter "**microdata1.cbs.nl**" as the server address.



4. Click **Accept**

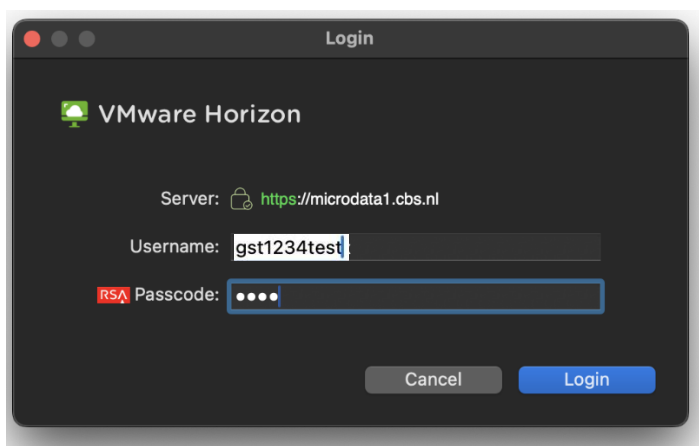


5. Under **Username**, enter your **Microdata account name (gst-projectnr username)**

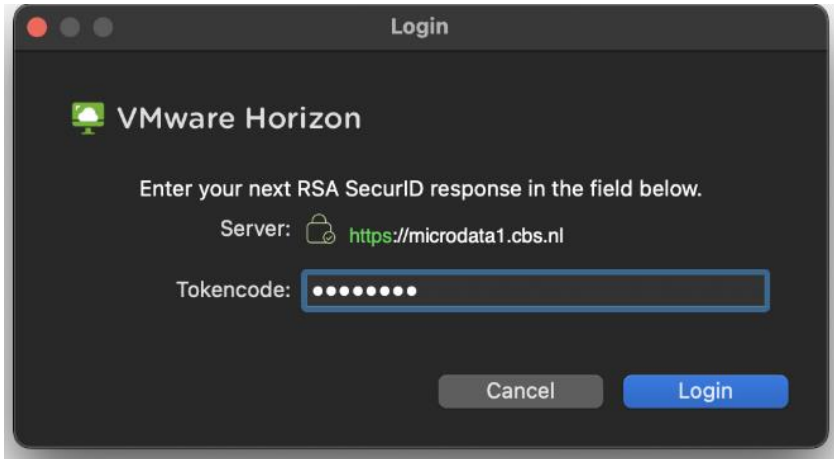
6. Under **RSA Passcode**, enter **project number**

For example if your Microdata account name is: gst1234test, then the RSA Passcode is: 1234.

7. Then click **Login**

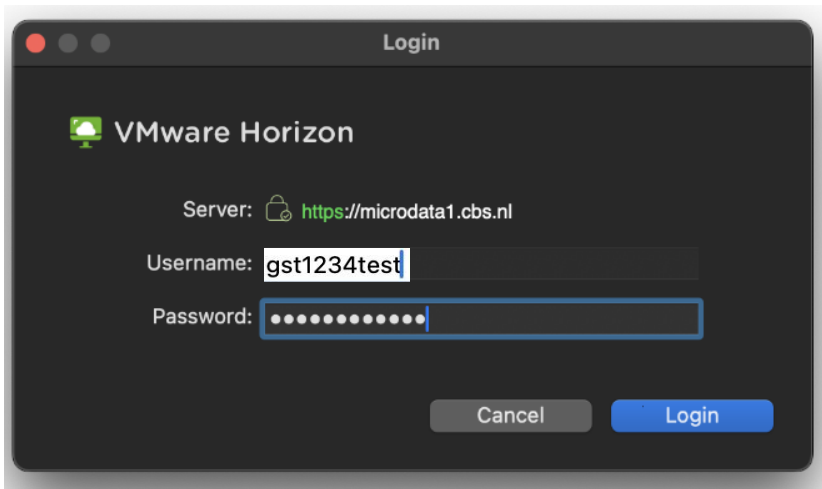


8. An **8-digit access code** has been sent to your **cell phone** for verification. Enter the received code in the next screen to log in.
9. Click **Login**



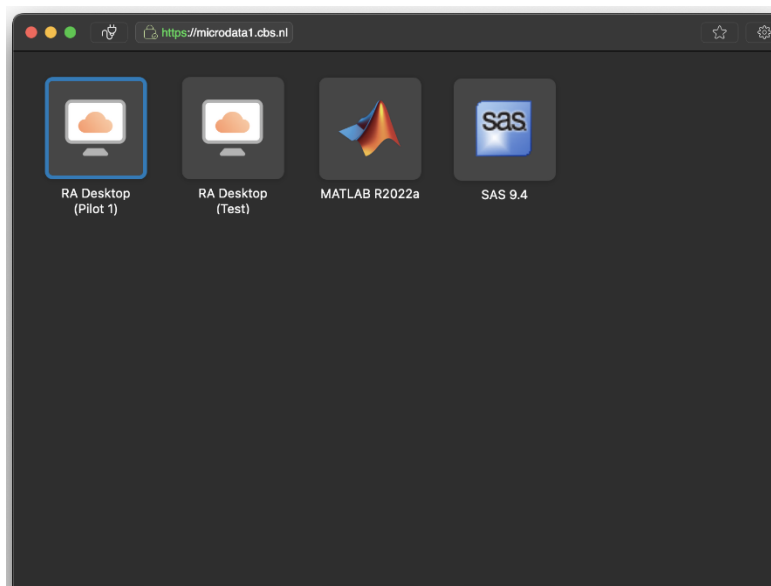
The screenshot shows a macOS-style window titled "Login" with the VMware Horizon logo. The text "Enter your next RSA SecurID response in the field below." is displayed. Below this, the "Server:" field shows a lock icon and the URL "https://microdata1.cbs.nl". The "Tokencode:" field is a text box containing eight dots, indicating an 8-digit code. At the bottom right are "Cancel" and "Login" buttons.

10. In the next screen, enter the Microdata account password.
11. Click **Login**



The screenshot shows the same "Login" window. The "Server:" field remains "https://microdata1.cbs.nl". The "Username:" field now contains the text "gst1234test". The "Password:" field is a text box filled with dots, with a blue selection box around it. The "Cancel" and "Login" buttons are at the bottom right.

You are now logged in to the VMware Microdata environment and a desktop session can be started.



By double clicking on an environment you can start a session. MATLAB and SAS are still required to be started via an application session.

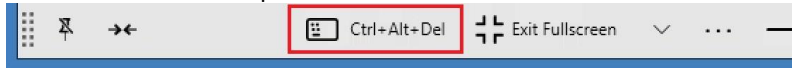


After connecting to your desktop session above window will show up and count down. When the countdown is finished your applications are ready for use.

Useful information

CTRL + ALT + DEL

When the session is locked, the screen says to press CTRL + ALT + DEL. To unlock the session when you are working on a Windows computer, instead of using the keyboard keys, use the CTRL + ALT + DEL button in the gray toolbar to unlock the session(see below). Are you working on macOS? Click Connection > Send Ctrl-Alt-Del in the toolbar on the top of the screen.

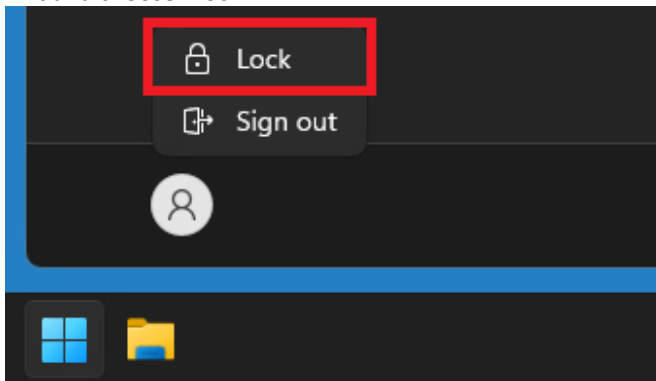


Creating shortcuts

You can create shortcuts on the desktop as an alternative to the favorites list in the tile interface. To create a shortcut, you can first open the start menu via the Start button in the lower left corner of the screen. Then click on "All apps." Now a list appears with all the applications you have access to. Drag your favorite applications from this list to the desktop to create a shortcut.

Disconnect, lock or sign out

- Locking the screen: When you walk away from your computer, the best option is to lock the screen. You can find this option in the Start menu. Open the Start menu, click on the gray circle with the figure in it and choose "Lock":



- Disconnect: Do you have any scripts or processes running that need to continue? Then disconnect the session using the toolbar at the top of the screen. In the toolbar, click the X to disconnect:



- Signing out: Have you finished your work and has everything been saved and closed? Then sign out the session. It is recommended to use this option as much as possible. This keeps the environment working in the most stable way. You can also find this option in the Start menu. Open the Start menu, click on the gray circle with the figure in it and choose "Sign out":

