

Step by step guide – AWS Connector GUI App

The connection to the operating system on EC2 servers in AWS environments can be done using the SSM service. This connection method is considered more secure than other connection methods.

Prerequisites:

To make the connection, you need to download and install the following:

- **Download and install AWS CLI** – You can find download and installation instructions for your operating system here:

<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>

Download for Windows operating system:

<https://awscli.amazonaws.com/AWSCLIV2.msi>

Download for Linux / Mac operating systems – found at the link above.

- **After** downloading and installing AWS CLI – **Requires downloading and installing AWS CLI Session-Manager Plugin** – You can download from here:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-working-with-install-plugin.html>

(In the above link you can find the download links by operating system - for example - for the Windows operating system the download link is:

<https://s3.amazonaws.com/session-manager-downloads/plugin/latest/windows/SessionManagerPluginSetup.exe>)

- Downloading the connector client app that makes the connections – <https://github.com/rahav-r-united/AWS-SSO-SSM-GUI-Connector-App>

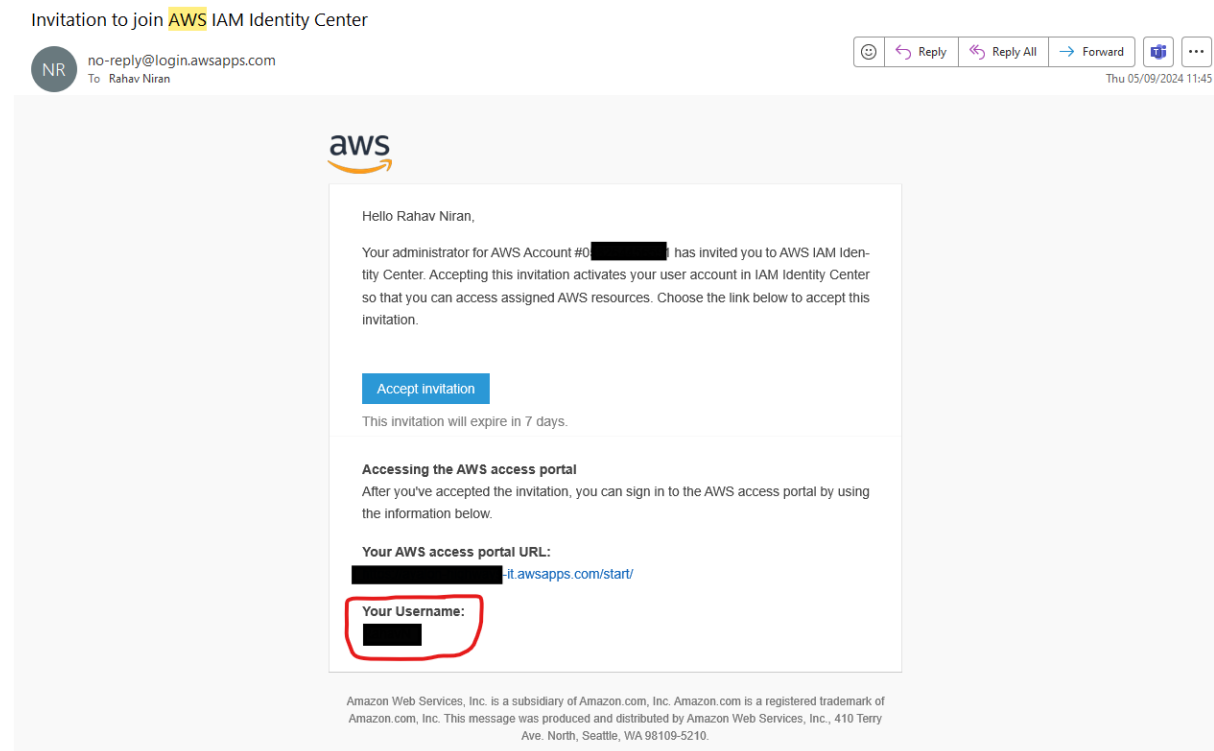
You need download the exe file and the config.json file

The prerequisites only need to be completed once before the first connection. After that, everything remains installed on the computer and no further installations are required.

After completing all the prerequisites, you can proceed to the connection stages:

There are 3 main steps-

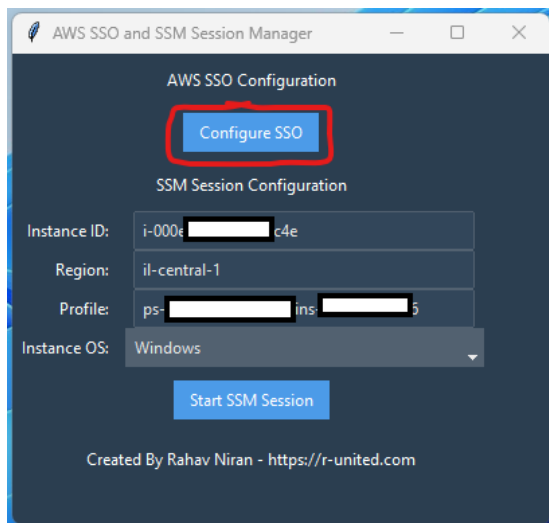
Step 1 - Initial identification with the AWS environment – This identification uses your user in the AWS environment that was created for you, and you received an email from AWS system that asked you to set a password and associating it with MFA (provided via Google Authenticator on mobile) – the email is looks like this:



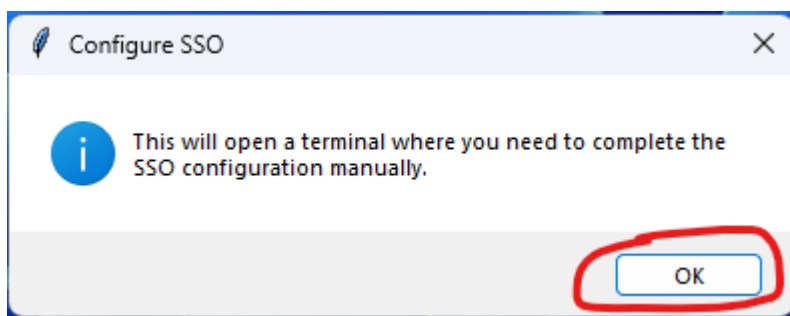
Notice in red – **This is the user that authenticates to the AWS environment itself - the one you enter during the initial authentication with SSO.**

To perform the identification, follow these steps -

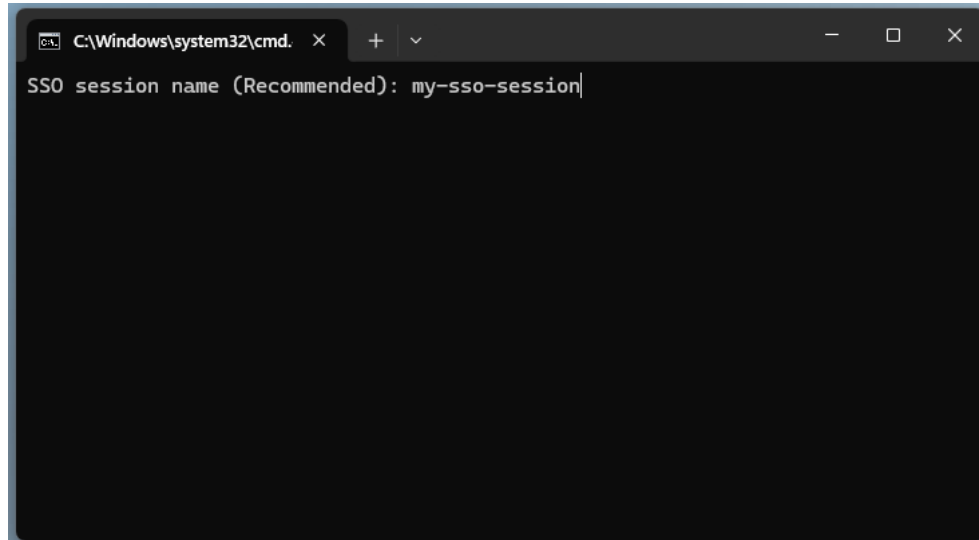
- a. Open the client you downloaded called AWS-SSO-SSM-GUI-Connector-App.exe and click the Configure SSO button.



A window will open explaining that you are now entering an identification process that you need to complete manually - click OK

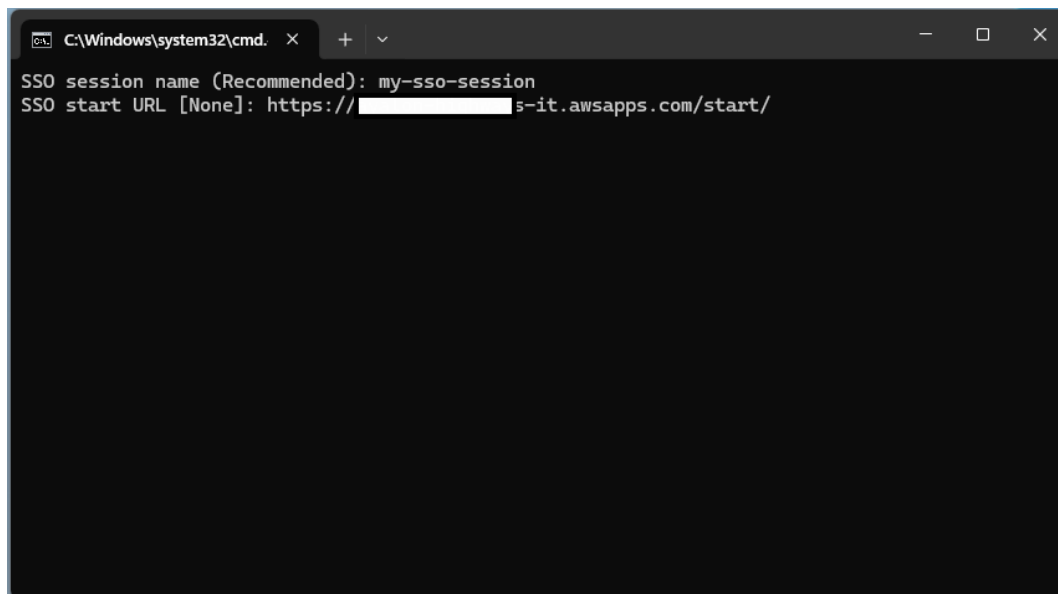


- b. Now a CMD window will open, and we will begin the identification process – first it will ask us to choose an SSO session name (if you have performed such identification before, you can choose the name you have already entered before and it will automatically insert what is needed) – we will choose a name that will be convenient for us:



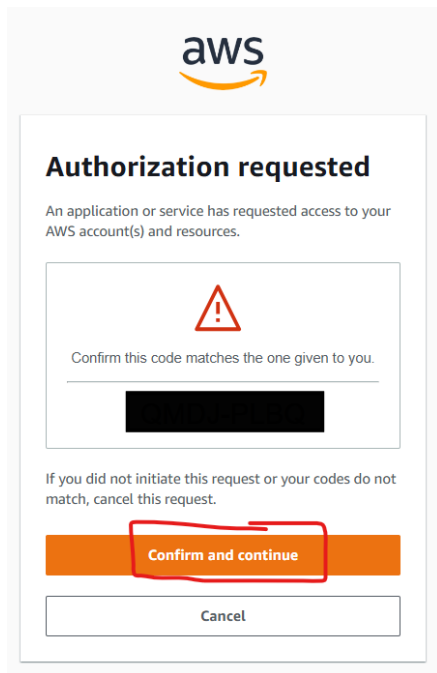
```
C:\Windows\system32\cmd. x + v
SSO session name (Recommended): my-sso-session|
```

- c. Then it will ask us for the SSO start URL – this is the URL you received in the email with the user created for you in the AWS environment – be sure to enter the entire URL in its entirety, including https at the beginning and including the slashes to the end -



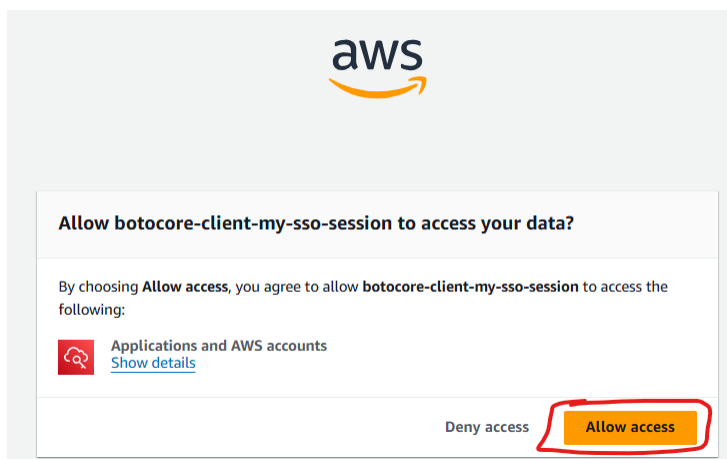
```
C:\Windows\system32\cmd. x + v
SSO session name (Recommended): my-sso-session
SSO start URL [None]: https://[redacted]s-it.awsapps.com/start/
```

- d. It will ask us for the SSO Region – we will enter our Region
e. It will ask us for SSO registration scopes – do not enter anything here and press Enter
f. The browser will then automatically open and ask you to confirm the identification request - click Confirm and continue



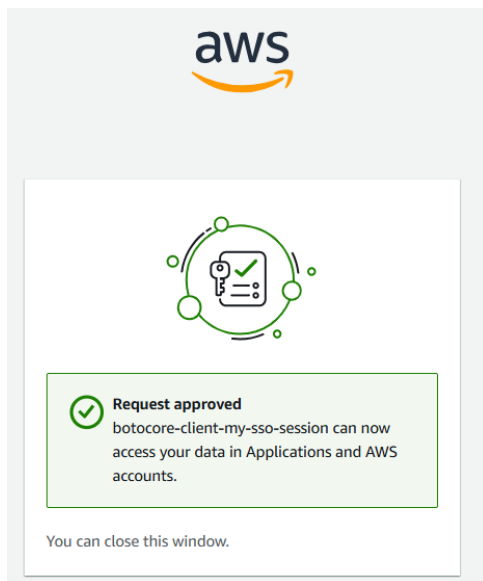
The screenshot shows the AWS 'Authorization requested' screen. At the top is the AWS logo. Below it, the title 'Authorization requested' is followed by a message: 'An application or service has requested access to your AWS account(s) and resources.' A red warning triangle icon is displayed above a text prompt: 'Confirm this code matches the one given to you.' Below this prompt is a black rectangular box representing the MFA code. Further down, a note states: 'If you did not initiate this request or your codes do not match, cancel this request.' At the bottom, there are two buttons: an orange 'Confirm and continue' button, which is highlighted with a red hand-drawn rectangle, and a white 'Cancel' button.

- g. You will then be taken to entering user information – please note – **Here you enter the username you received in the email in step 1 to identify yourself to the AWS environment itself.**
- h. After you successfully enter your username, password, and MFA code, it will ask you to approve access – click Allow access.



The screenshot shows the AWS 'Allow botocore-client-my-sso-session to access your data?' screen. At the top is the AWS logo. The main heading is 'Allow botocore-client-my-sso-session to access your data?'. Below this, a message reads: 'By choosing **Allow access**, you agree to allow **botocore-client-my-sso-session** to access the following:'. A red icon is shown next to the text 'Applications and AWS accounts', with a blue link 'Show details' underneath. At the bottom, there are two buttons: a white 'Deny access' button and an orange 'Allow access' button, which is highlighted with a red hand-drawn rectangle.

- i. You can now close the browser window –



- j. Now return to the CMD window you started with and if you have permission for multiple accounts, it will ask you to choose which account you want to connect to - select the desired account and press Enter -

```
C:\Windows\system32\cmd. x + v
SSO session name (Recommended): my-sso-session
SSO start URL [None]: https://[redacted].awsapps.com/start/
SSO region [None]: il-central-1
SSO registration scopes [sso:account:access]:
Attempting to automatically open the SSO authorization page in your default browser.
If the browser does not open or you wish to use a different device to authorize this request, open the following URL:
https://device.sso.il-central-1.amazonaws.com/
Then enter the code:
[redacted]
There are 21 AWS accounts available to you.
> [redacted]
```

- k. After you have selected the account you want to connect to, if you have multiple types of permissions, it will also allow you to select the permission you want to connect with. You can then leave everything blank and press Enter on all other questions until the end.

- I. Once you have completed the identification, it will give you your profile name – the profile name consists of the permission name (the name of the Permission set) and the account number – as marked in red -

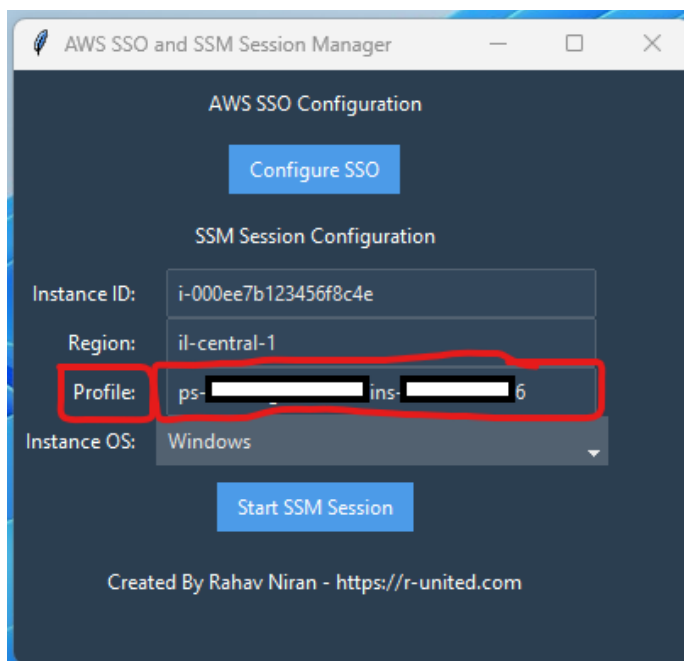
```
C:\Windows\system32\cmd. x + v
SSO session name (Recommended): my-sso-session
SSO start URL [None]: https://[redacted]t.awsapps.com/start/
SSO region [None]: il-central-1
SSO registration scopes [sso:account:access]:
Attempting to automatically open the SSO authorization page in your default browser.
If the browser does not open or you wish to use a different device to authorize this request, open the following URL:
https://device.sso.il-central-1.amazonaws.com/

Then enter the code:
[redacted]

There are 21 AWS accounts available to you.
Using the account ID 1[redacted]96
The only role available to you is: ps-[redacted]ins
Using the role name "ps-[redacted]ins"
CLI default client Region [None]:
CLI default output format [None]:
CLI profile name [ps-[redacted]ins-1[redacted]6]:

To use this profile, specify the profile name using --profile, as shown:
aws s3 ls --profile ps-[redacted]ins-1[redacted]6
```

Now you enter this profile name in the Profile field in the connector app -



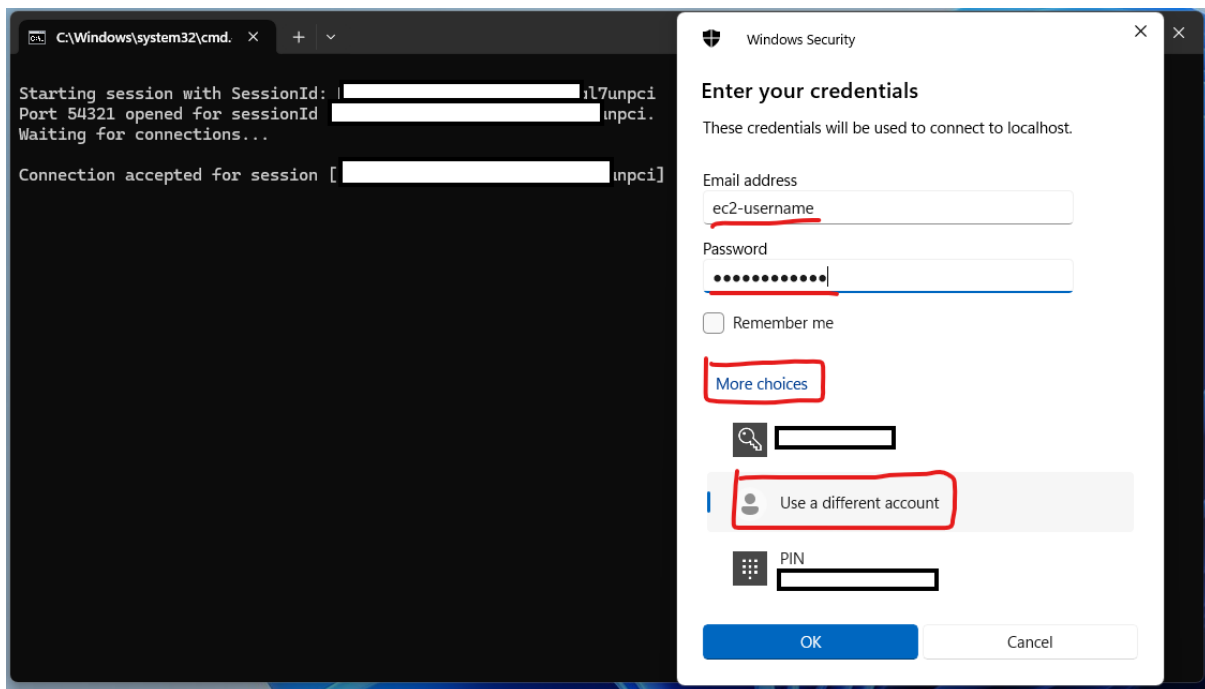
Step 2 – Connecting to the EC2 server using SSM -

- a. Enter all the required data in the application as you received it – Instance ID, Region, Profile, Instance OS (note that you can enter this data in the config.json file you downloaded so that it is saved for future use) and then click Start SSM Session.
- b. If it's Linux, it will open a CMD window with a Linux shell into the server, ready to work. If it's Windows, it will automatically connect and pop up an RDP window (note

- in the case of Windows, if it fails to connect or gets a Timeout, try closing the error window and clicking Start SSM Session again).

Step 3 – Authentication with the EC2 OS – *Relevant to Windows servers only*

- a. If you selected Windows and the connection is made with RDP – you are required to authenticate in front of the server as soon as the RDP window opens - **The username and password you are entering belong to a server local user or a domain user that different from your AWS environment user.** This user has nothing to do with the credentials you entered in the previous steps! This is a user on the server itself!



After entering the username and password given to you to connect to the server, click OK and this will connect you via RDP directly into the server.

If the RDP authentication window displays an error – try closing it (just the error window) and clicking Start SSM Session again.

Good luck!

Regards,

Rahav Niran,

IT Services

Mobile: 0524280495

Mail: rahav@r-united.com

<https://r-united.com>