Comprehensive Guide for Connecting IoT Devices to AWS IoT Core and Establishing Secure Tunnels

Version: Ver 1.0

Date: 21 May 2024

Author: saeed hamad

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

Documentions for connecting iot device to AWS and create a secure tunnel ..... **Error! Bookmark not defined.**

1. Abstract 4
2. General 4
3. Manual connection of the RP to iot core: 5
4. Connect the RP with provisioning template and claim certificate 6
5. create aws client on the RP: 12
6. Open secure tunnel into the RP: 13
7. Conclusion 14

Figure 1 iot core 5
Figure 2 create policy 6
Figure 3 create certificate 7
Figure 4 creation instrucutions 7
Figure 5 policy attachment to the certificate 8
Figure 6 templates dashboard 9
Figure 7 Iam role creation 9
Figure 8 certificate registration 10
Figure 9 tunnel creation 13

Table 1 - document version control 3

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

Version	Editor	modifications	notes
V1.0	Saeed Hamad	Preliminary HLD	

Table 1 - document version control

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

1. Abstract

This documentation provides detailed steps for connecting a Raspberry Pi to AWS IoT Core using both manual connection methods and provisioning templates. It also covers creating secure tunnels for remote device management.

2. General

Connecting a Raspberry Pi to AWS IoT Core involves configuring the device to securely communicate with AWS services. This can be achieved through manual configuration or by using provisioning templates, which streamline the process and enhance security. This document outlines the necessary steps to establish a secure and reliable connection, manage device permissions, and create secure tunnels for remote access and management.

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

3. Manual connection of the RP to iot core:

- Connect to the RP and run : pip install awsiotsdk
- Open [aws iot core]

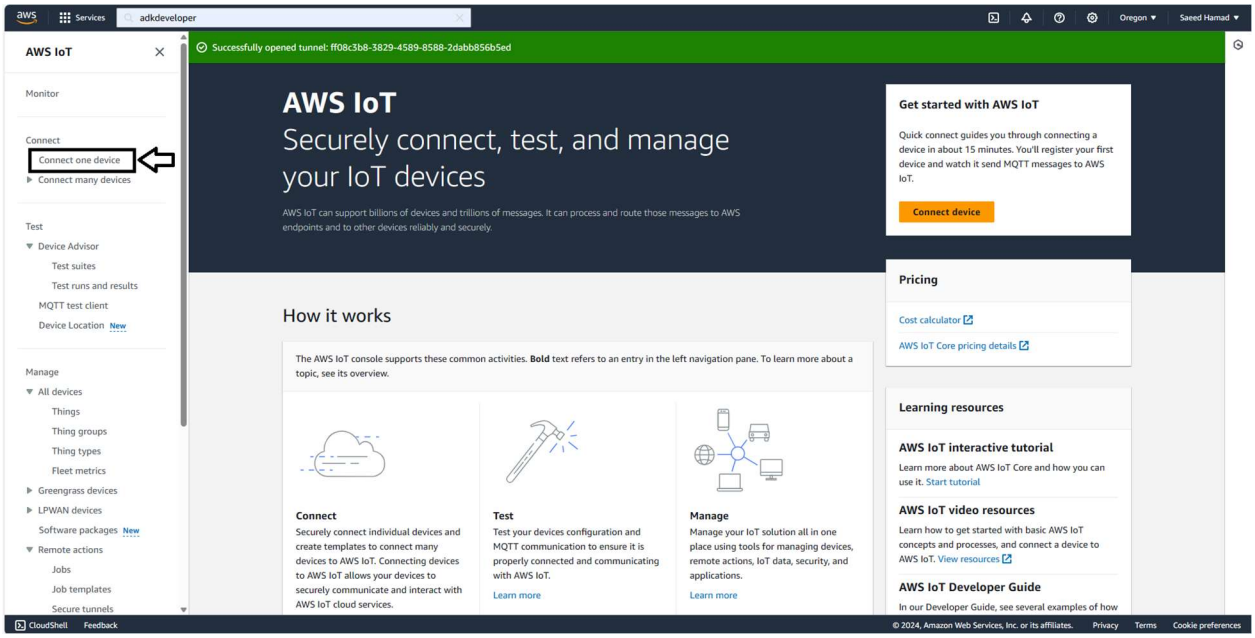

Figure 1 iot core

- connect one device > follow the instructions
- Create policy with the needed access and attach to the certificate of the created thing

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

4. Connect the RP with provisioning template and claim certificate

Create policy:

1. Go to the aws iot dashboard :

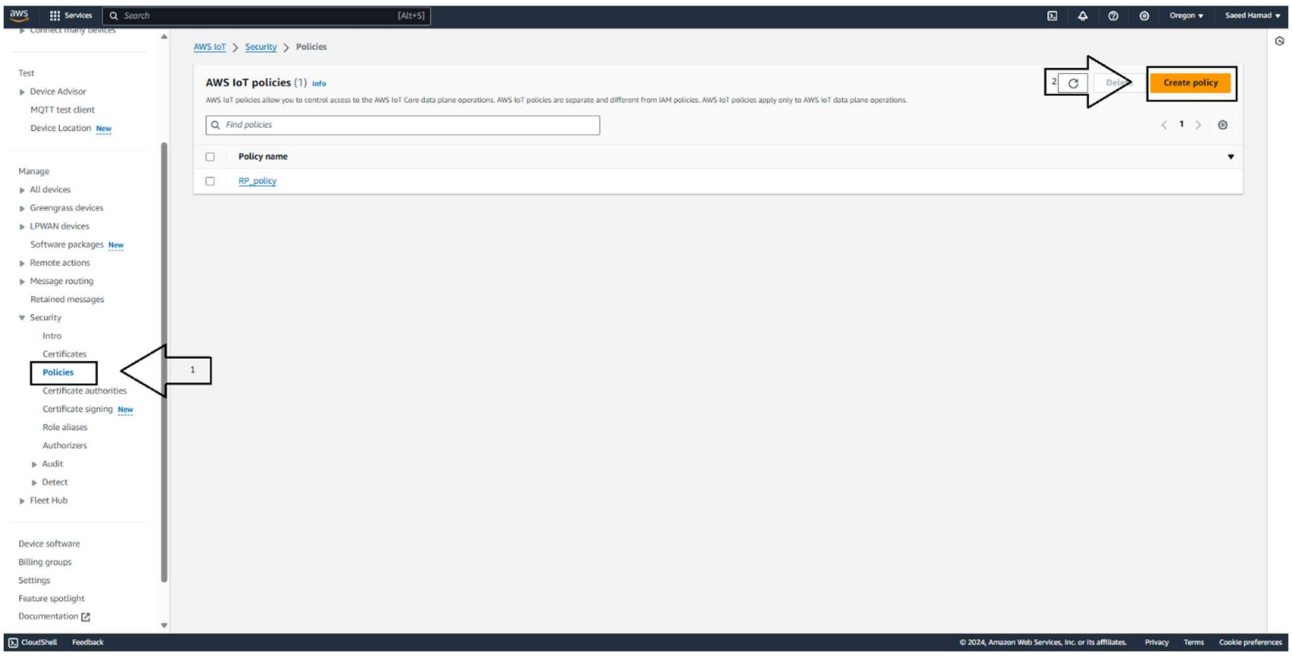

Figure 2 create policy

2. Give the policy a name and the required permissions
3. Create the policy

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

Create certificate:

1. Go to certificates:

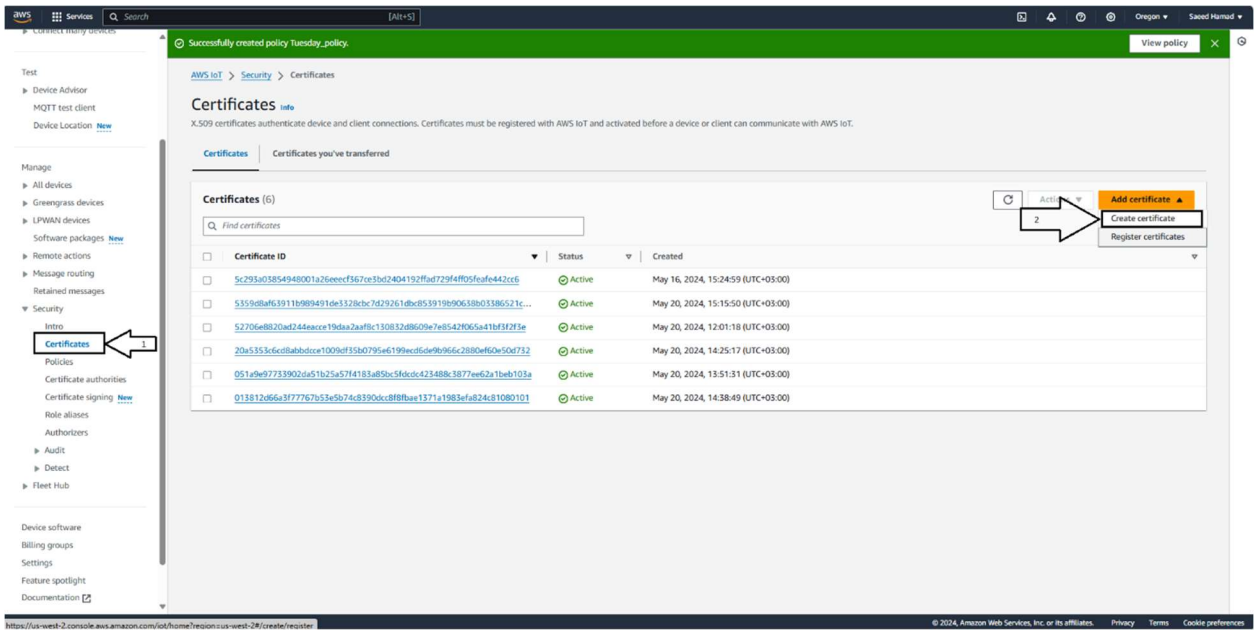

Figure 3 create certificate

2. Create new certificate and download the keys and certificates:

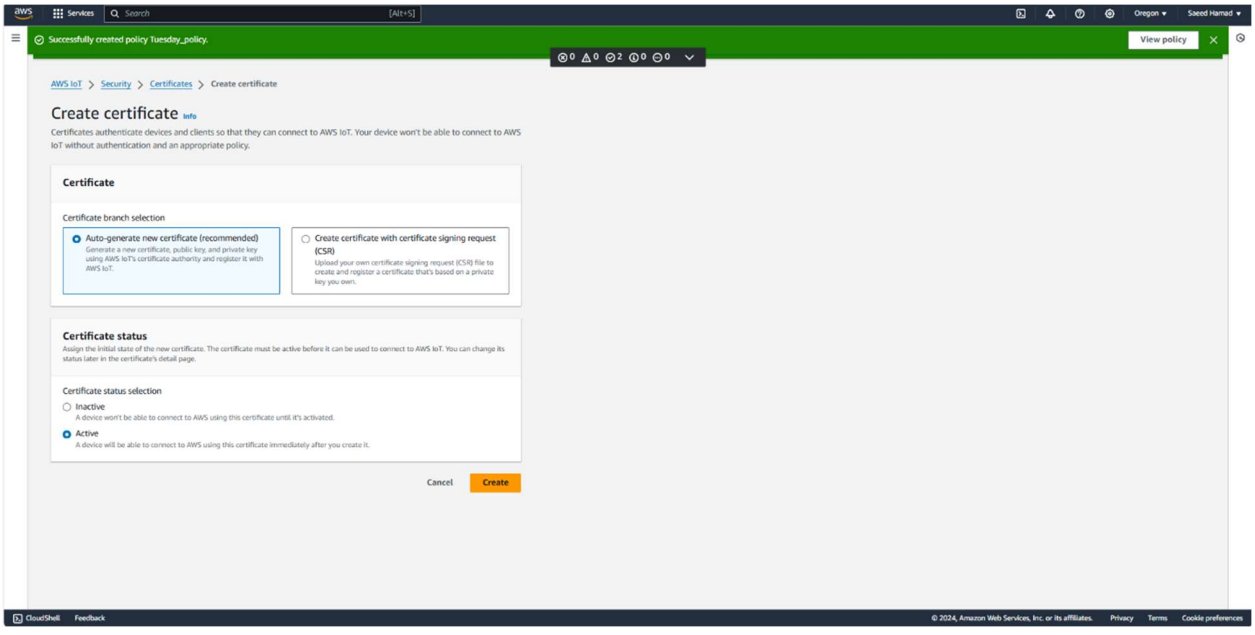

Figure 4 creation instrucutions

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

3. Attach the created policy to the certificate:

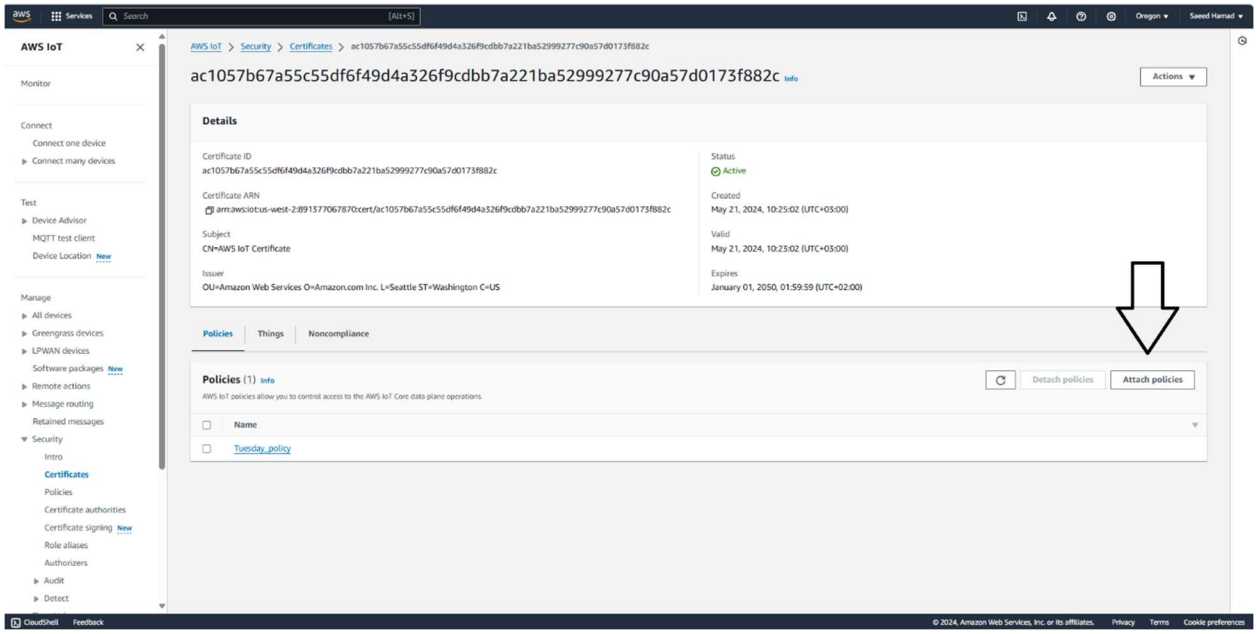

Figure 5 policy attachment to the certificate

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

Create provisioning template:

1. Choses the “Provisioning devices with claim certificates” option

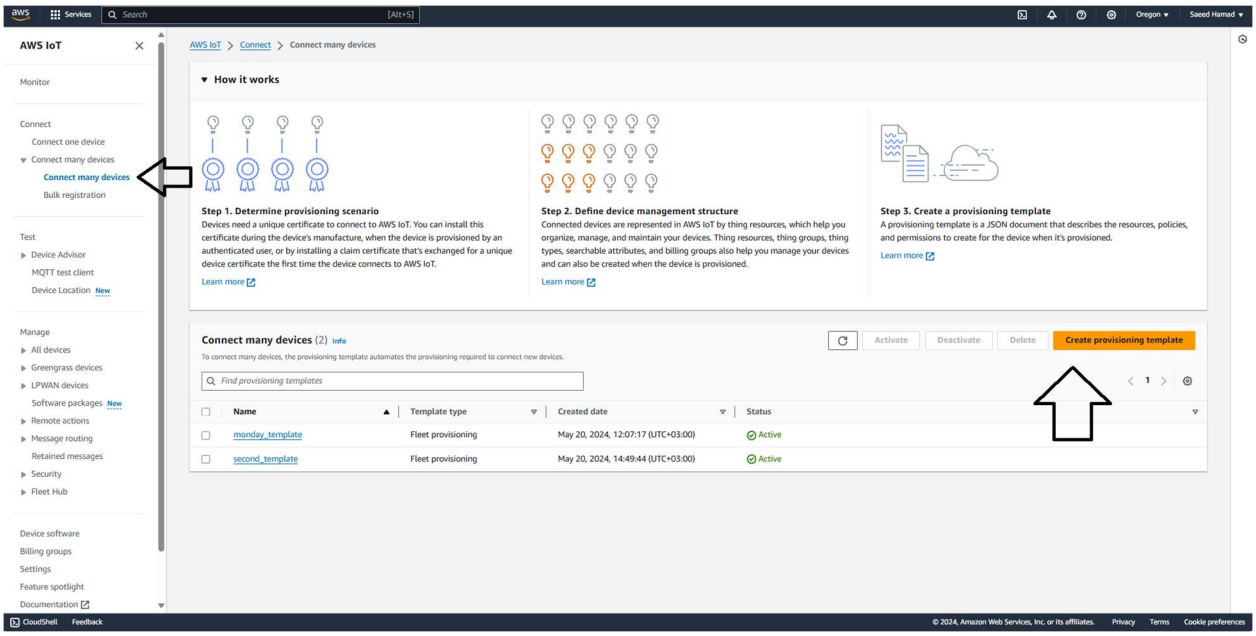

Figure 6 templates dashboard

2. Create Iam role and attach to it the required policies especially “AWSIoTThingsRegistration policy” :

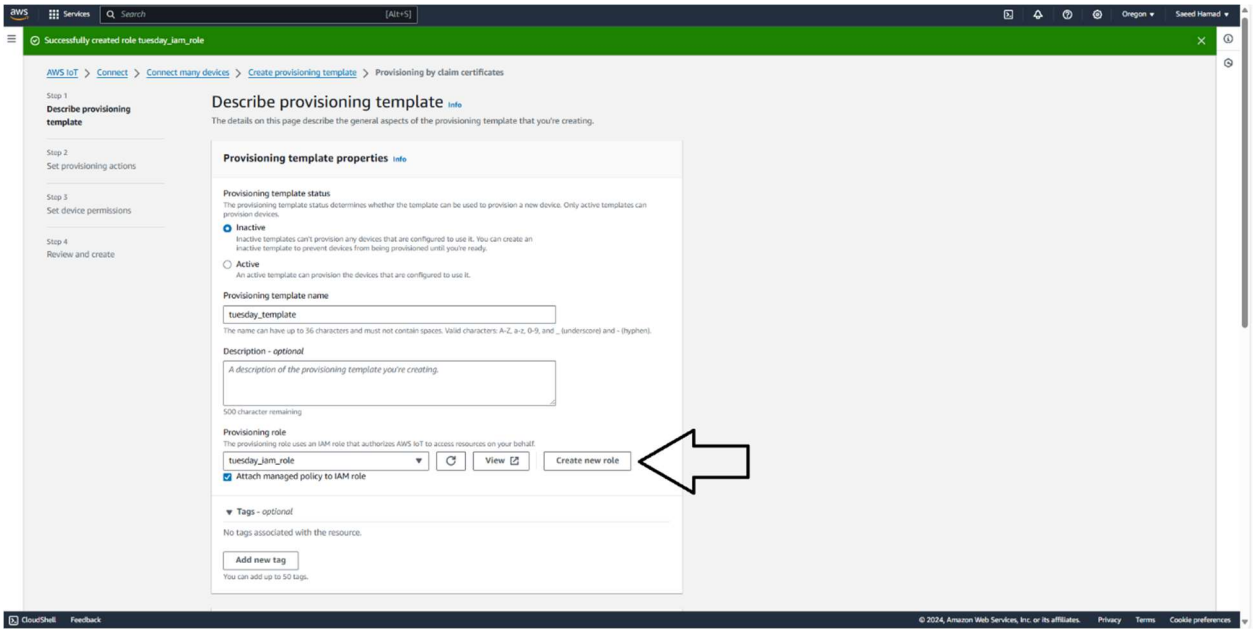

Figure 7 Iam role creation

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

3. Register your downloaded ca certificate to claim certificate:

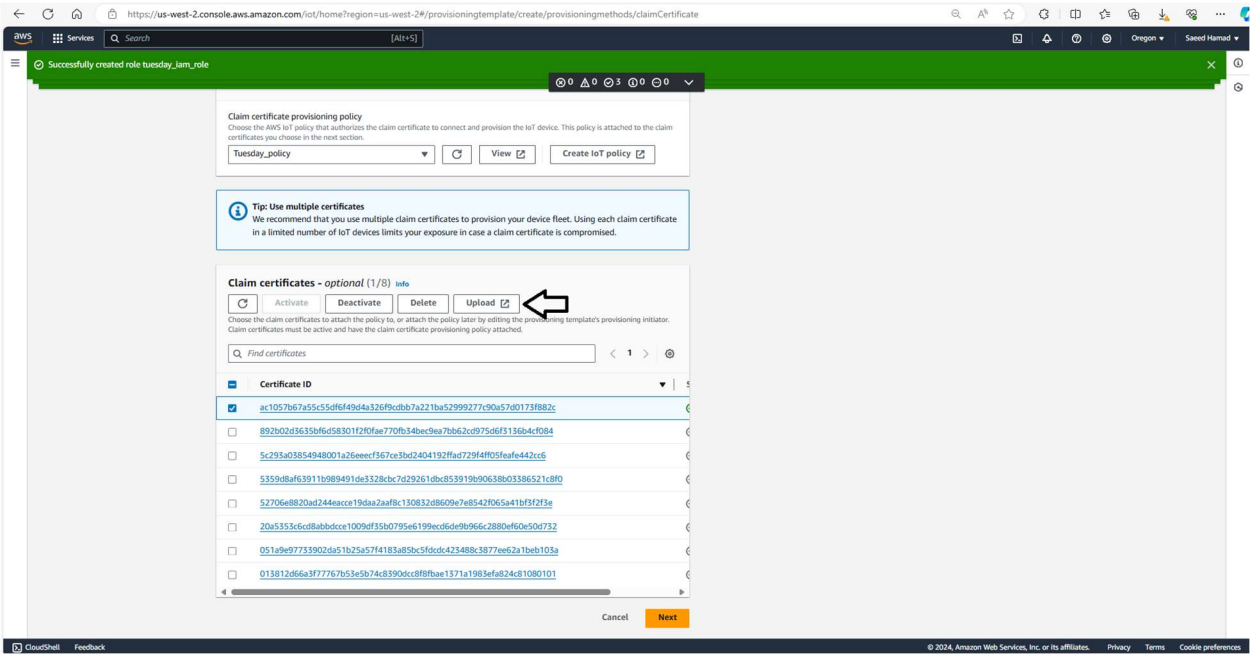

Figure 8 certificate registration

4. Choses the created policy and certificate to be used with this template
5. Add prefix to be added to the device name if needed
6. Select the required policy to give permissions to the device

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

Add device the iot core:

- Copy the certificates and keys to the raspberry pi with scp command
- Create a bash script with the following commands
- Create python script named connection.py with the code from the github
- Then :

bash Copy code

```
# Make the bash script executable
chmod +x bash_script.sh

# Execute the bash script
./bash_script.sh
```


32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

5. create aws client on the RP:

Connect to the RP from the local machine then follow the instructions:

- Create client.sh script with the following commands
- Then do the following:

```bash
# Set permissions for the directory "keys_directory" to allow only the owner to rea
chmod 700 keys_directory

# Set permissions for the file "private_key" to allow only the owner to read and wr
chmod 600 private_key

# Set permissions for the file "root_ca" to allow the owner to read and write, and
chmod 644 root_ca

# Set permissions for the file "certificate" to allow the owner to read and write,
chmod 644 certificate

# Add execute permission to the script "client.sh" for the owner, group, and others
chmod +x client.sh

# Execute the script "client.sh" with elevated privileges using sudo.
sudo ./client.sh
```


32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

6. Open secure tunnel into the RP:

Navigate to the Thing you created in AWS IoT Core, create a secure tunnel, and follow the on-screen instructions to establish the tunnel connection. This enables secure remote access to the Raspberry Pi for management and monitoring.

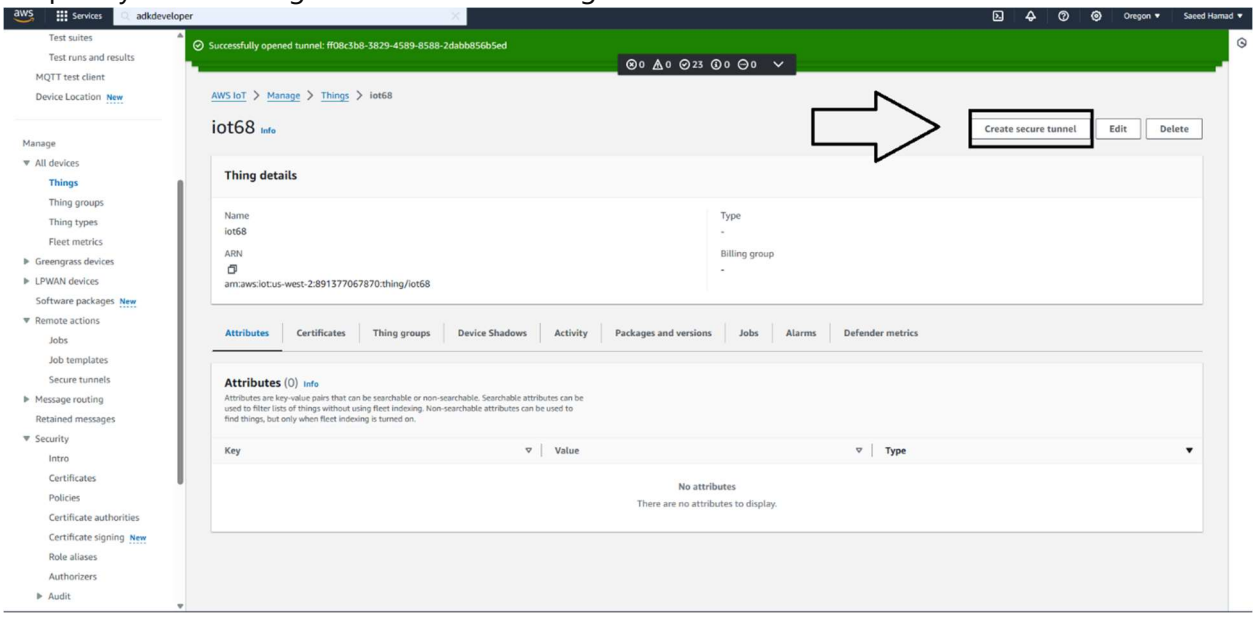

Figure 9 tunnel creation

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com

7. Conclusion

In conclusion, establishing a connection between a Raspberry Pi and AWS IoT Core is fundamental for deploying IoT applications securely. By adhering to the documented procedures for manual connection and provisioning templates, users can navigate through the setup process efficiently. Additionally, the ability to create policies, certificates, and provisioning templates enables fine-grained control over device access and management within the AWS ecosystem. With the provided documentation, users can confidently integrate Raspberry Pi devices into their IoT solutions, leveraging the scalability and flexibility of AWS services.

32 Dov Hoz, Herzliya, 4658132, Israel
+972(9)9559525 info@ad-knight.com