



OSTENDO

One system ▪ Complete operations

Ostendo Continuum Edition

Remote Server Ostendo API Setup for Freeway and Third Party Connections

2026 © Development-X Ltd

20/07/2026

Revision 1.0.1

Table Of Contents

Overview	1
Prerequisites.....	1
Choose a Port and Open Environment Security Settings	1
AWS Security Permissions	2
Azure Security Group Settings.....	3
Open Port in Windows Firewall.....	5
Windows Firewall Outbound Rule.....	5
Windows Firewall Inbound Rule	7
Bind SSL Certificate to the Port.....	7
Configure and Install API Service.....	8
Step 1. Upload installation file.....	8
Step 2. Create configuration and installation scripts	9
Create files	9
Configure files.....	9
ostendoapi.ini example:.....	9
ostendoapi.ini Settings Reference:.....	10
InstallAPI.bat.....	10
InstallAPI.bat Settings Reference:	10
UninstallAPI.bat.....	10
UninstallAPI.bat Settings Reference:.....	10
Step 3 – Start the service	11
Test the API	12
Check the Service is Running.....	12
Check Internet Access to the API Port.....	12
Install Freeway and Connect a Solution	12

Overview

This guide covers the setup, configuration and installation of the Ostendo API Service that allows external applications (e.g. Freeway, PowerBI, Excel) to access an Ostendo Continuum database.

The instructions below use AWS and Azure as examples which can be easily applied to other server platforms, whether on a local or remote server.

Note – The method of configuring an API service in the previous Ostendo 242 version within the Ostendo Client using **File->API Service->Api Configuration** will **not work** in Ostendo Continuum if the Server is separate from the client machine.

Note – For multiple API connections to different databases it is recommended to follow this guide separately for each connection, using a different port and API installation folder for each.

Prerequisites

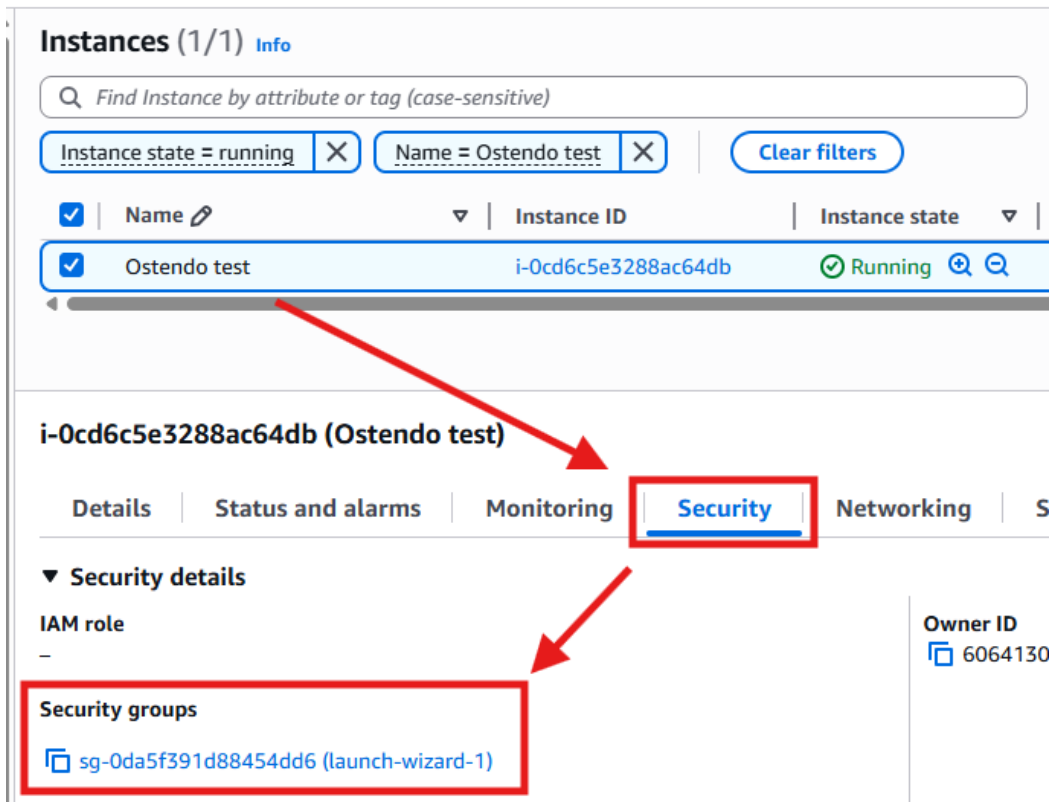
1. Server administrator access to the server or Ostendo root folder installation.
2. The Ostendo API Service installation file. In the absence of a Continuum download being available it is OK to copy your existing Ostendo Ver 242 API executable, `ostendoapi.exe`. For sites configured for an HTTPS environment all necessary Ostendo API files can be found in the OstendoAPI folder within the Ostendo Server Install bundle.
- 3.
4. A registered domain name with a valid SSL certificate installed.
5. The path to your Ostendo database file (.FDB).
6. Windows and virtual server firewall access to the required port.

Choose a Port and Open Environment Security Settings

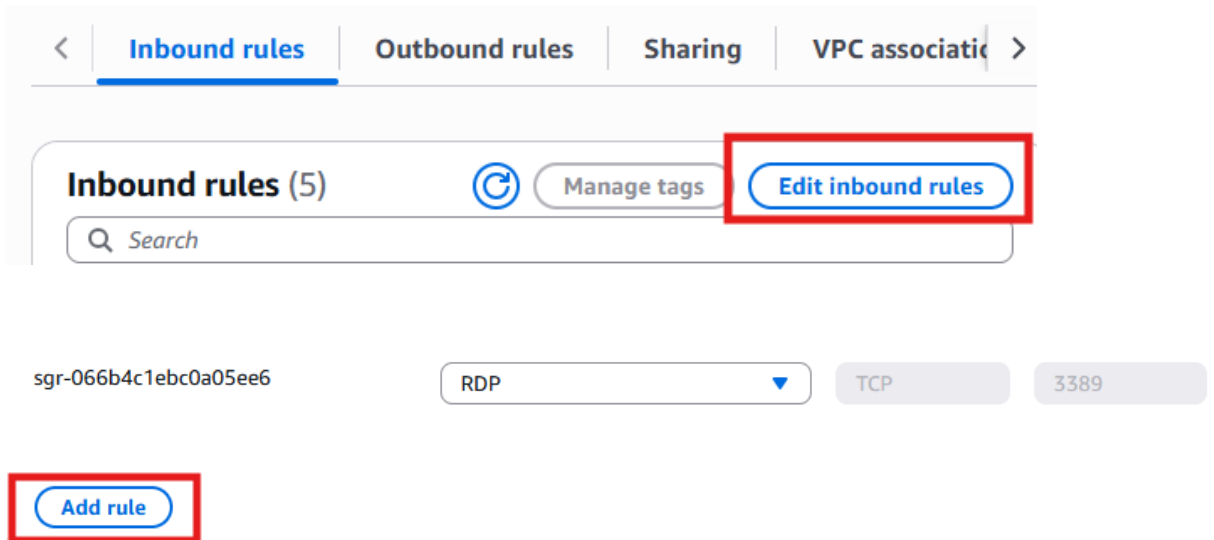
Choose an unused port for the API to handle connections through. This guide uses **Port 8441** as an example. The chosen port must be open to allow all incoming and outgoing TCP traffic from your desired IP range and/or location. Here are examples of how to do this in AWS and Azure.

AWS Security Permissions

1. Open your Ostendo EC2 server instance within the AWS console online.
2. Click on **Security** and go to the security group that is linked to this instance



3. Select **Edit Inbound Rules** -> **Add Rule**



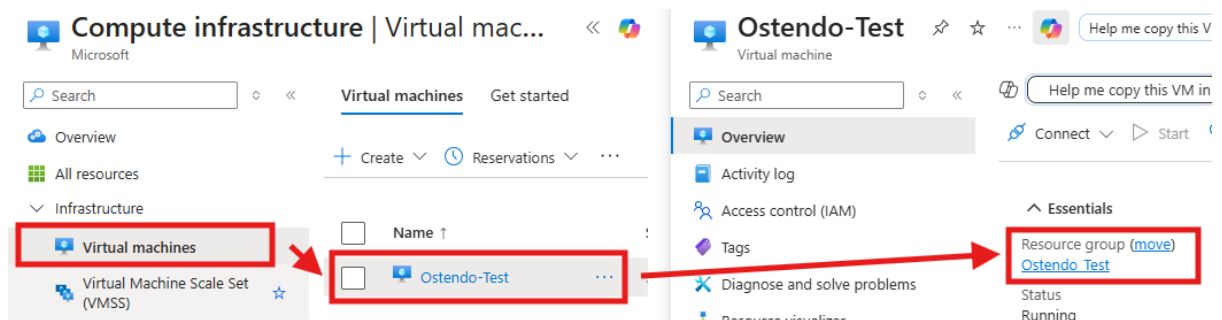
4. Add the following information:
 - a. **Type** – Custom TCP
 - b. **Port Range** – 8441
 - c. **Mask** – 0.0.0.0/0 (from anywhere)
5. click **Save Rules**

Remote Server Ostendo API Setup for Freeway and Third Party Connections

6. You can add an outbound rule if necessary. However, as a default AWS EC2 instances already allow all outbound traffic so usually there is no need to.

Azure Security Group Settings

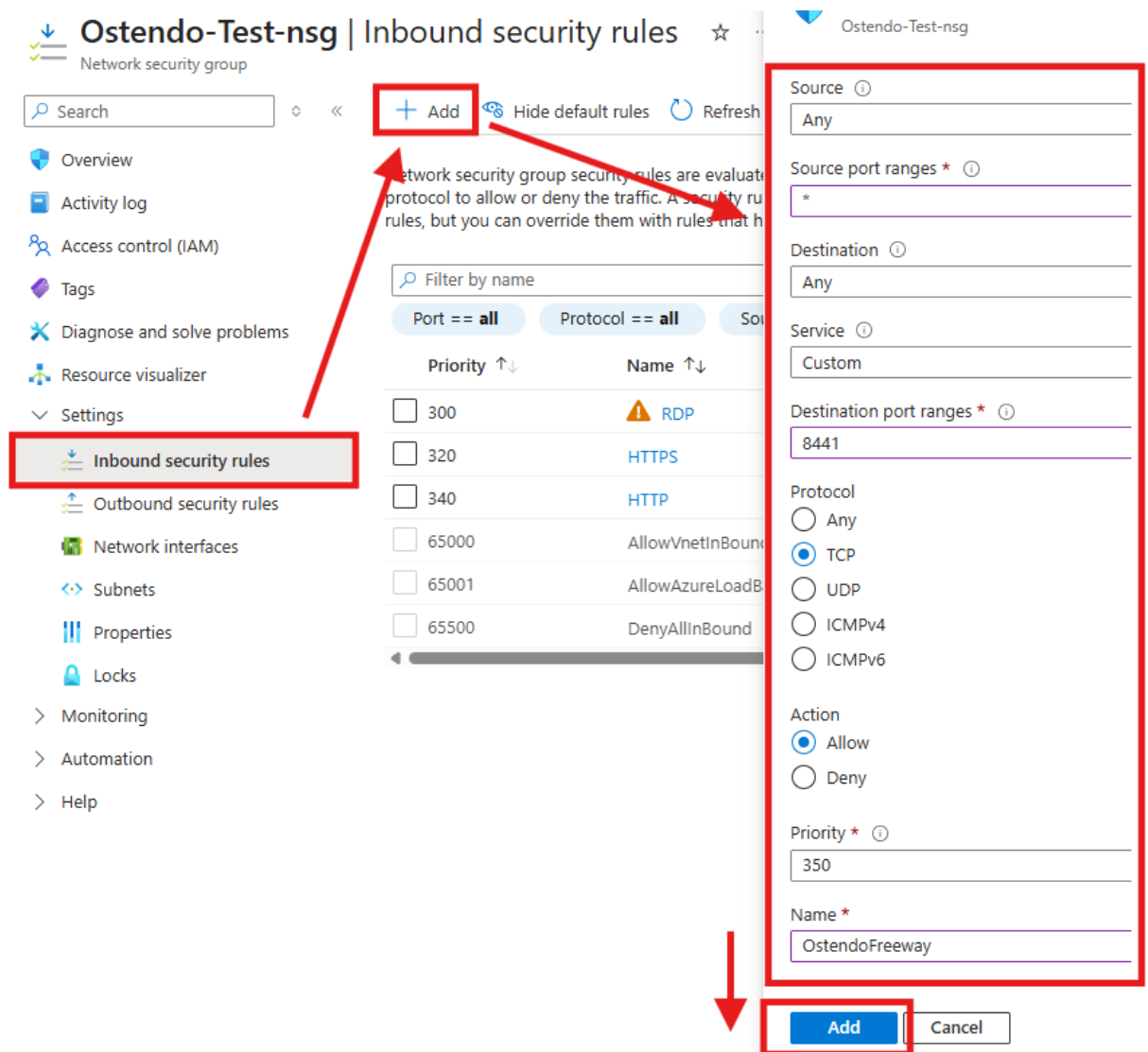
1. Navigate to the **Virtual Machine** that hosts the Ostendo Server, then select the **Resource Group**



2. Click on the Network Security Group in the list of Resources.

☐	Ostendo-Test	...	Virtual machine
☐	Ostendo-Test-ip	...	Public IP address
☐	Ostendo-Test-nsg	...	Network security group
☐	ostendo-test925_z1	...	Network Interface
☐	Ostendo-Test_OsDisk_1_c08476bb92274763accc618a7a1a3fde	...	Disk
☐	vnet-newzealandnorth	...	Virtual network

3. In the Network Security Group screen click **Settings->Inbound security rules->Add**



4. Enter the following information and click **Add**.
 - a. Source: Any (Allows traffic from any IP address)
 - b. Source Port Ranges: *
 - c. Destination: Any
 - d. Service: Custom
 - e. Destination port ranges: 8441
 - f. Protocol: TCP
 - g. Action: Allow
 - h. Name: OstendoFreeway (or a user friendly name for this port)

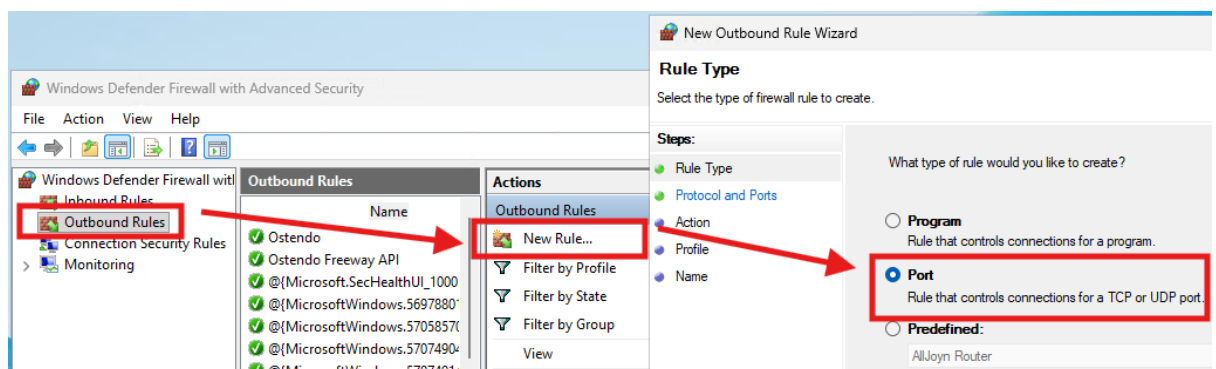
Open Port in Windows Firewall

The Windows Server will have it's own firewall with only necessary ports open. You must allow inbound and outbound traffic through the firewall by manually creating 2 rules for each port that you want to open. In this example only 1 port is required so we create 2 rules, one for **Inbound Traffic** and one for **Outbound Traffic**.

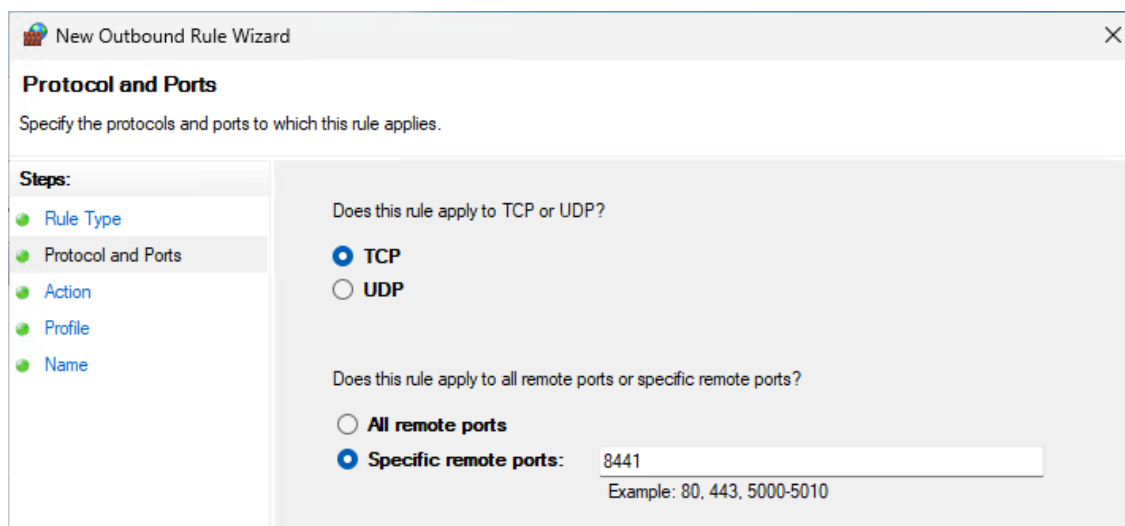
Open **Windows Defender Firewall with Advanced Security** by searching for 'Defender' in the windows home search bar.

Windows Firewall Outbound Rule

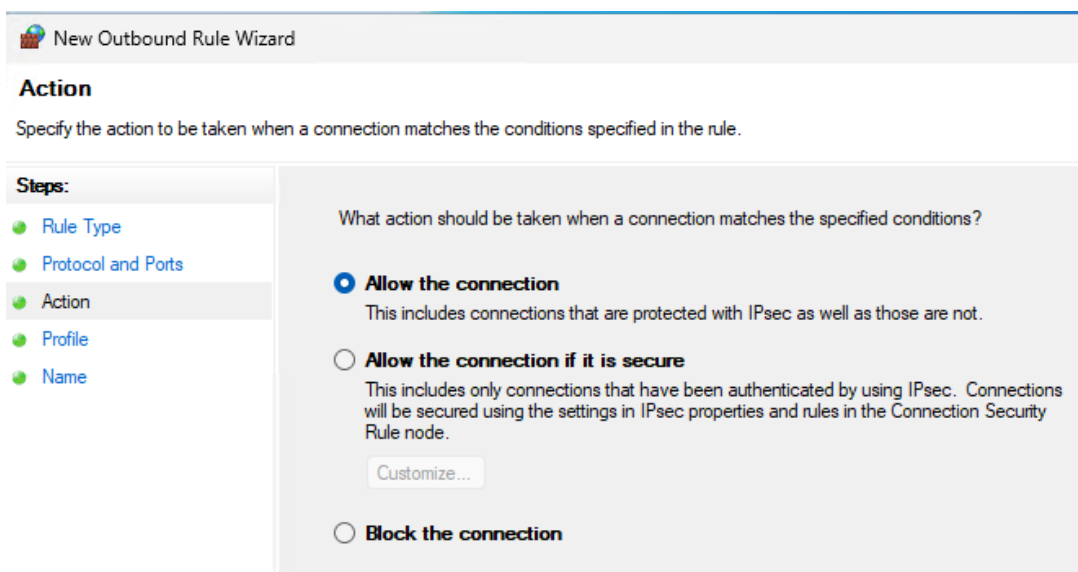
1. Click on **Outbound Rules->New Rule->Port**



2. Use the following screenshots to set the Outbound Rules and click **Next** in each stage.



3. Allow the connection



New Outbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

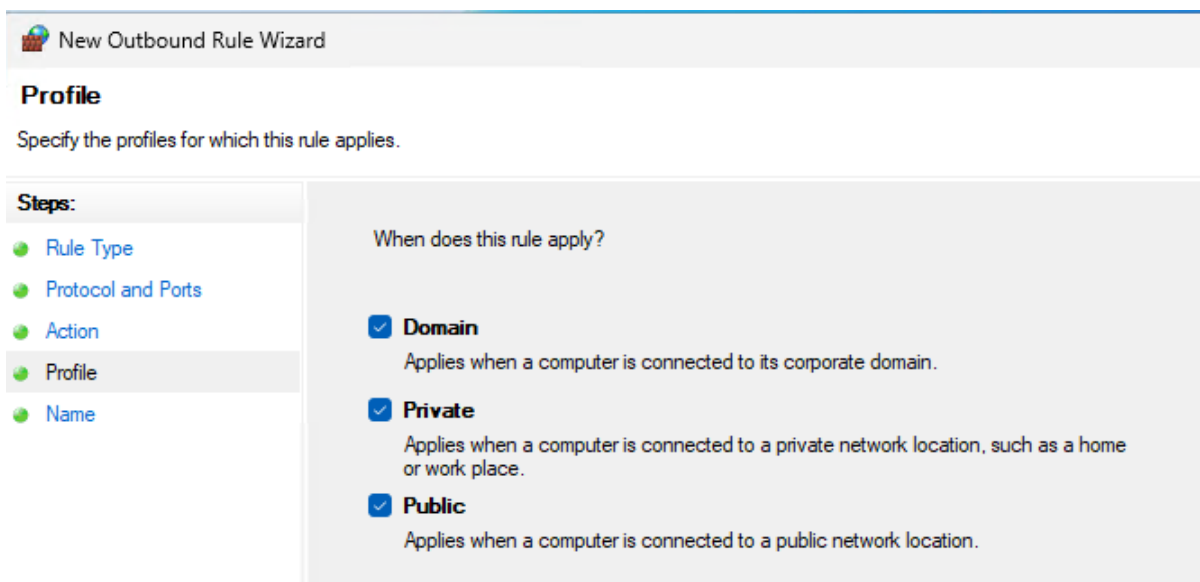
☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

[Customize...](#)

☐ **Block the connection**

4. Tick Domain, Private and Public



New Outbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile**
- Name

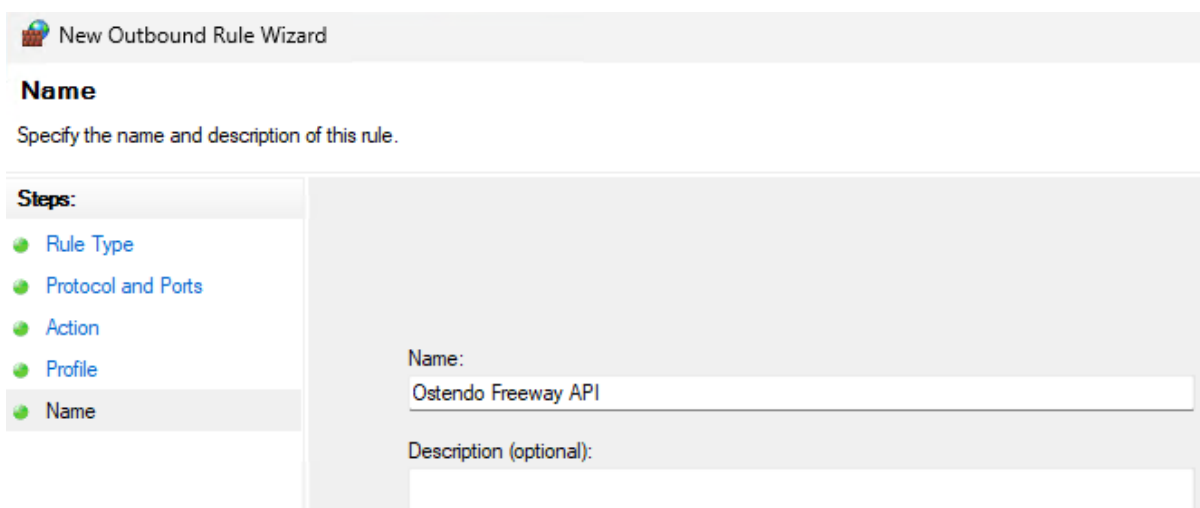
When does this rule apply?

☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**
Applies when a computer is connected to a public network location.

5. Give it a name



New Outbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

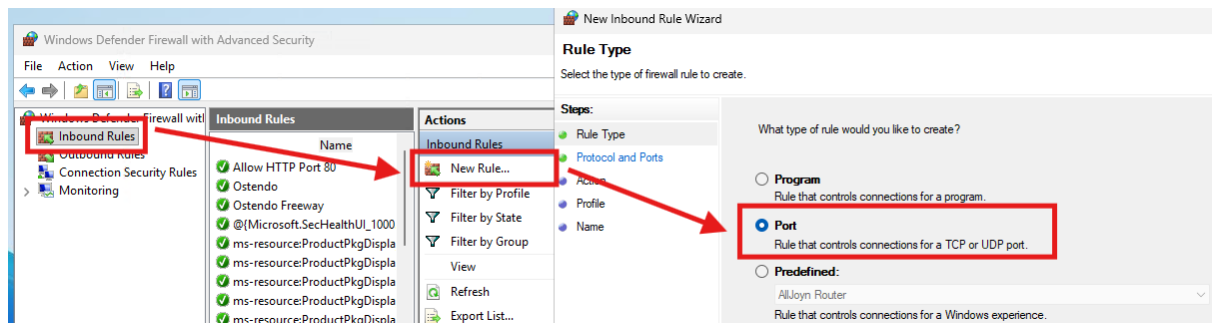
Name:

Description (optional):

- Click **Finish** in the last stage.

Windows Firewall Inbound Rule

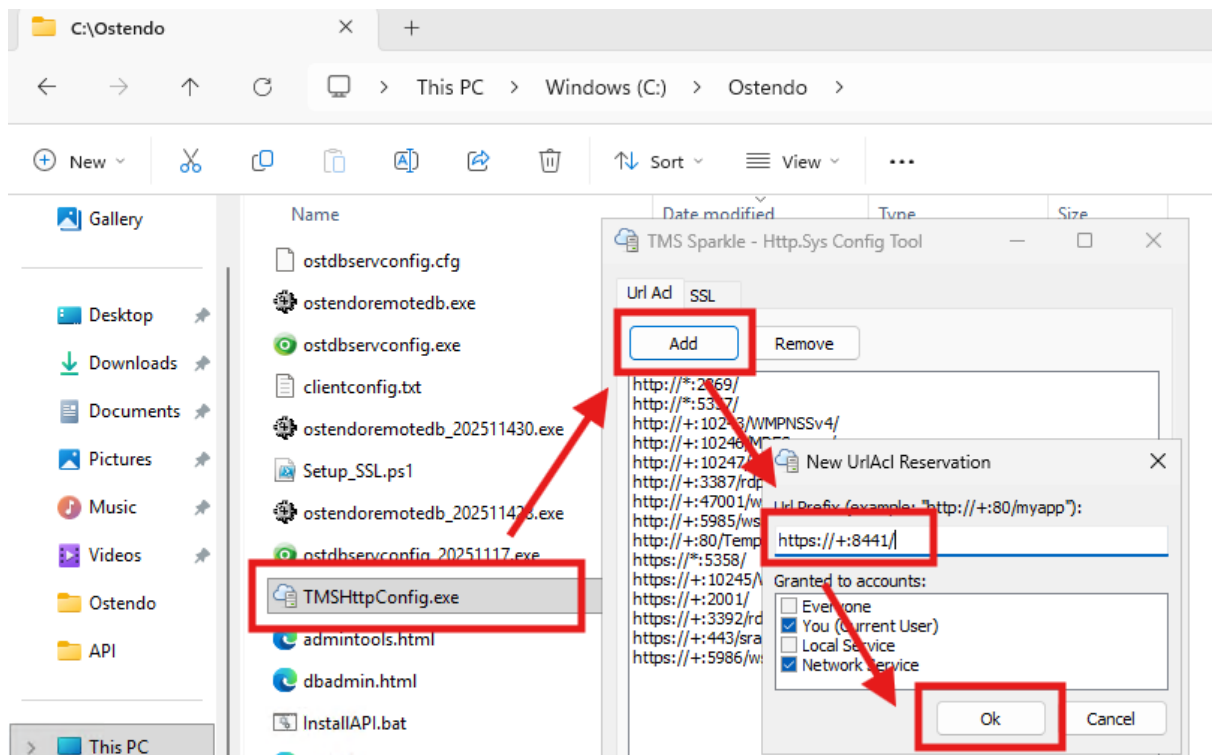
- Click on **Inbound Rules->New Rule->Port**



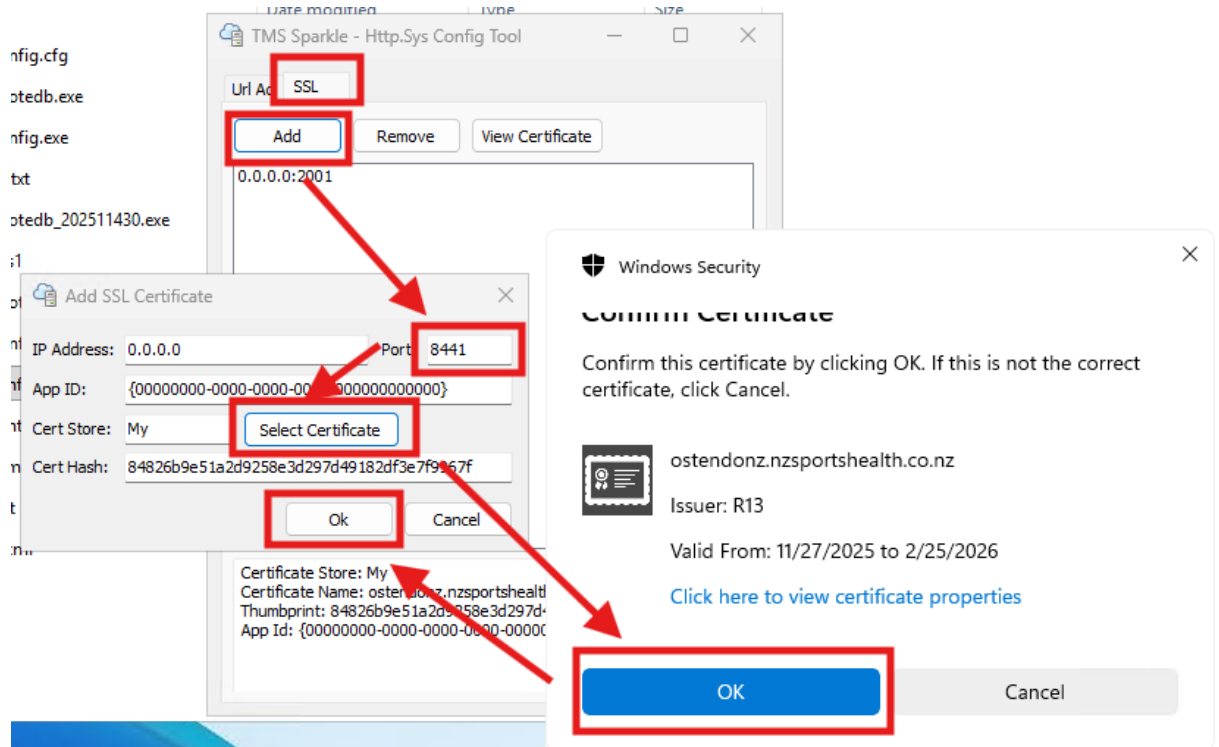
- Follow steps 2 to 6 above. The inbound and outbound rules use the same settings.

Bind SSL Certificate to the Port

- Open the TMSHttpConfig.exe executable in your Ostendo Installation folder.
- Click Add
- Enter the https record for the port like `https://+:8441/`
- Click ok:



5. Navigate to the **SSL** tab and bind your SSL Certificate to this port:
 - a. Click **Add**
 - b. Enter the port number
 - c. Click **Select Certificate**
 - d. In the windows security screen click **OK**
 - e. When you are taken back to the **Add SSL Certificate** screen click **Ok**.



You may close all windows. The background windows setup is complete. The next section uses Ostendo scripts and configuration files to run the API application as a service for connecting to the Database.

Configure and Install API Service

Step 1. Upload installation file

Upload the `ostendoapi.exe` file to your server. As a guide, save the file in your Ostendo Application directory in a newly created folder 'API'. For sites configured for an HTTPS environment all necessary Ostendo API files can be found in the OstendoAPI folder within the Ostendo Server Install bundle.

Note: In the absence of an Ostendo Continuum API executable it is ok to copy your existing Ostendo 242 `ostendoapi.exe`

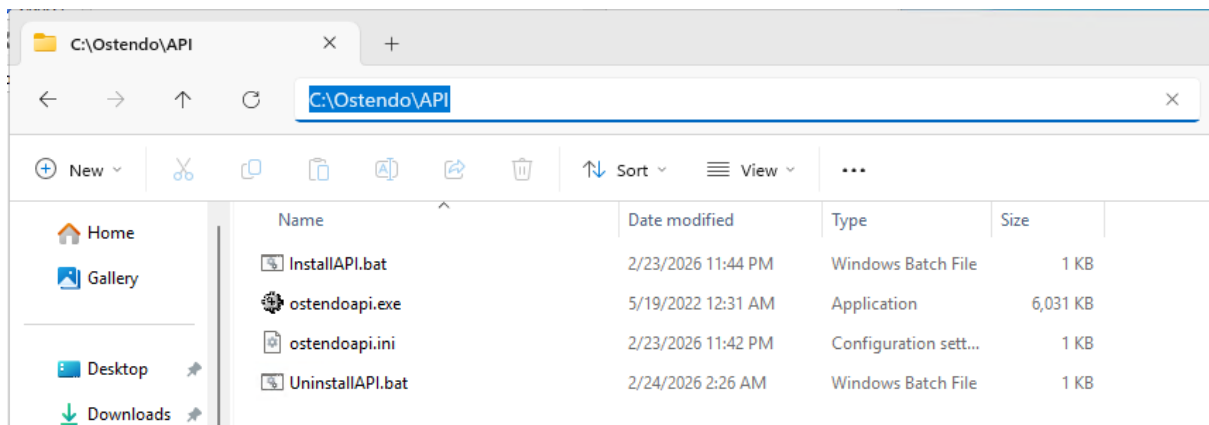
Step 2. Create configuration and installation scripts

Create files

Create 3 files in your newly created API folder:

- InstallAPI.bat
- UninstallAPI.bat
- ostendoapi.ini

Your file structure should look something like this:



Configure files

Edit the files created in the last step and add your version of the content below.

ostendoapi.ini example:

```
[Settings]
DBUsername=SYSDBA
DBPassword=yourdbpassword
UseHttps=1
HttpsPort=8441
SSLCert=
SSLKey=
StaticFileDirectory=C:\Path\To\Documents\Ostendo
OverrideIP=yoursubdomain.yourdomain.com.au
OverrideIPRemote=yoursubdomain.yourdomain.com.au

[Configuration_0]
Active=1
Freeway=1
Database=C:\PathToDatabase\OSTENDO.FDB
```

ostendoapi.ini Settings Reference:

- **DBUsername:** Your database username, almost always SYSDBA
- **DBPassword:** Your database password as was set up in the Firebird Installation process
- **UseHttps:** Set to 1 to enable HTTPS (strongly recommended)
- **HttpsPort:** Set the HTTPS port number created in the steps above
- **StaticFileDirectory:** Path for API file storage and access
- **OverrideIP:** Your domain that the SSL certificate is bound to
- **OverrideIPRemote:** Same as OverrideIP
- **Database:** Full path to your .FDB file

InstallAPI.bat

```
cd\  
cd %~dp0  
ostendoapi.exe /install /name "ostapisvc1" /display "Ostendo API  
Live"  
net start "ostapisvc1"  
PAUSE
```

InstallAPI.bat Settings Reference:

- **/name:** use a different service name for each port or API instance
- **/display:** A user friendly name

UninstallAPI.bat

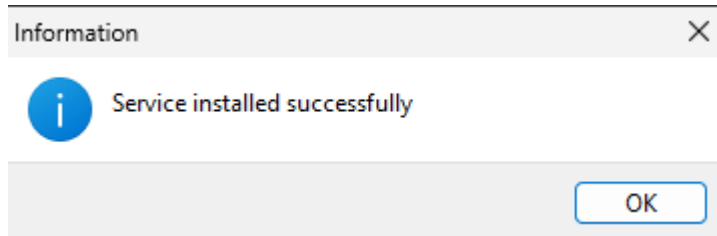
```
NET STOP "ostapisvc1"  
cd\  
cd %~dp0  
OstendoApi.exe /uninstall /name "ostapisvc1" /display "Ostendo API  
Live"
```

UninstallAPI.bat Settings Reference:

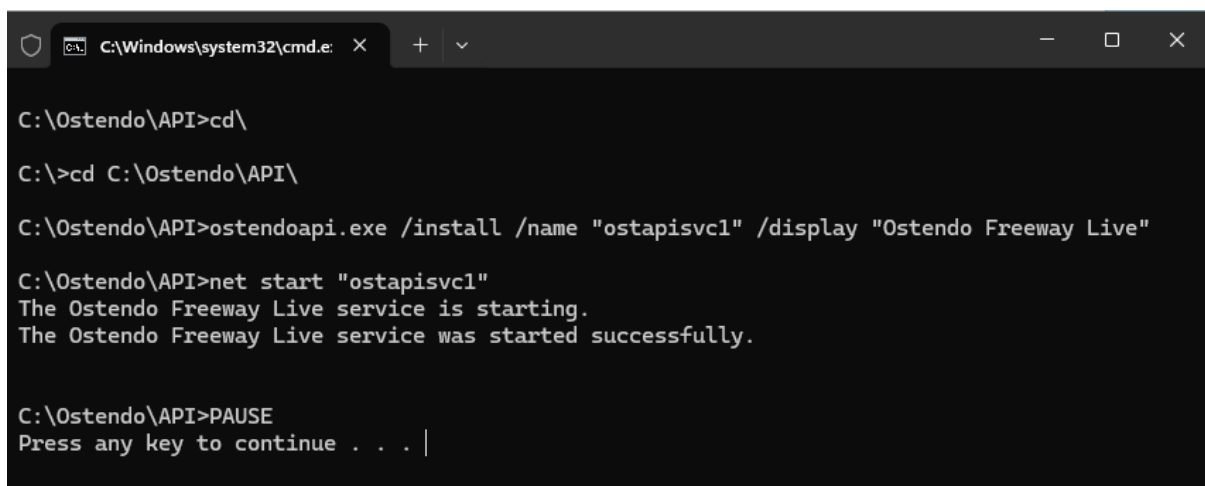
- Use the same **/name** and **/display** settings as above

Step 3 – Start the service

Double click **InstallAPI.bat**. You should, after a moment, see a **Service installed successfully** window pop up.



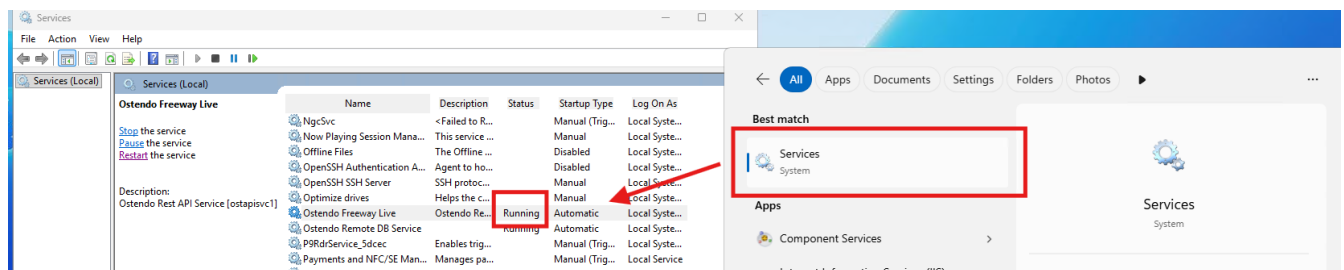
Click **OK** and a Windows Command window should eventually look like this:

A screenshot of a Windows Command Prompt window. The title bar shows 'C:\Windows\system32\cmd.e' and standard window controls. The command history is as follows:
C:\Ostendo\API>cd\
C:\>cd C:\Ostendo\API\
C:\Ostendo\API>ostendoapi.exe /install /name "ostapisvc1" /display "Ostendo Freeway Live"
C:\Ostendo\API>net start "ostapisvc1"
The Ostendo Freeway Live service is starting.
The Ostendo Freeway Live service was started successfully.
C:\Ostendo\API>PAUSE
Press any key to continue . . . |

Test the API

Check the Service is Running

1. Type 'Services' in the Windows home search bar and click on **Services** to bring up the Services Window.
2. Search for your API service, e.g. "Ostendo Freeway API"
3. Make sure the service has a status of **Running**

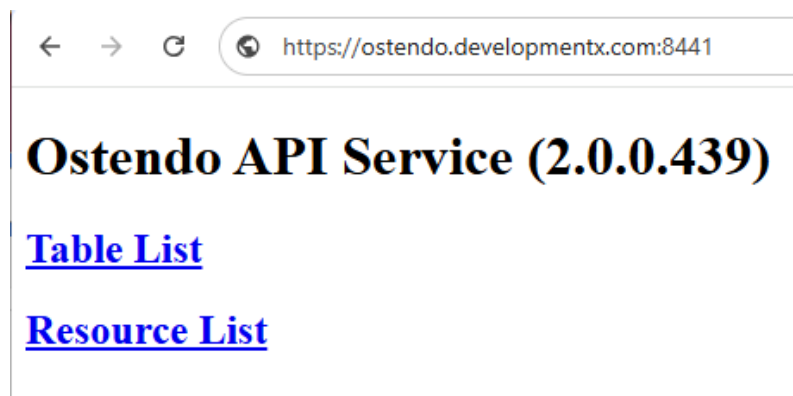


Check Internet Access to the API Port

In a browser on your client machine type in your HTTPS URL with port number in the address bar like:

<https://ostendo.yourdomain.com:8441>

The result should look something like this:

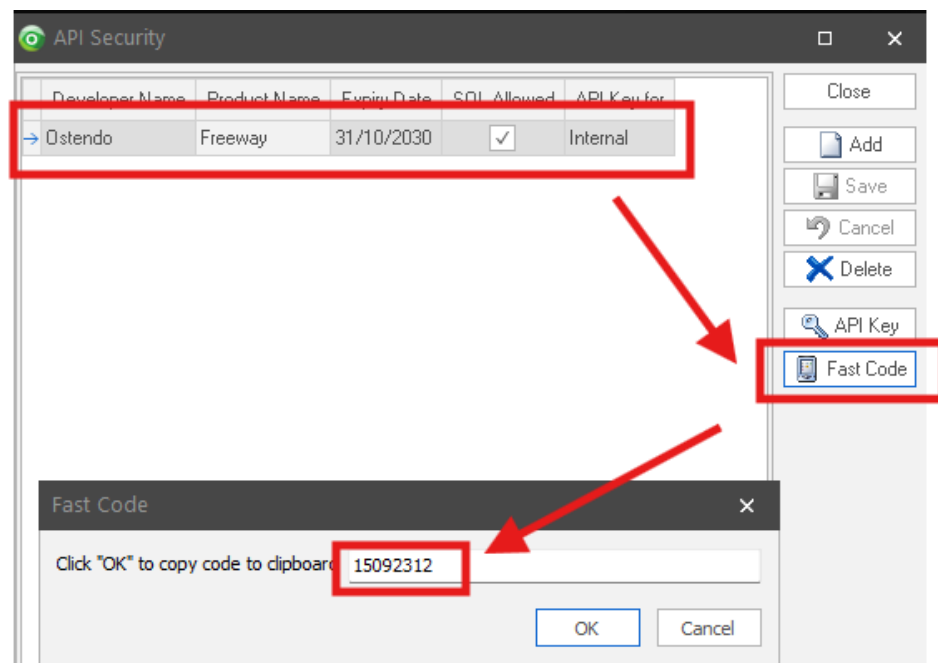


Install Freeway and Connect a Solution

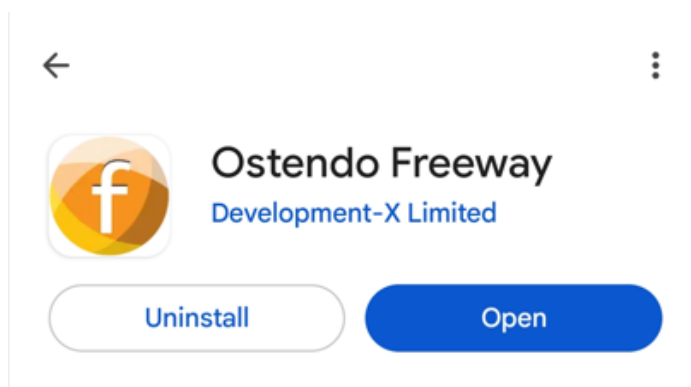
1. Obtain a **Fast Code** from **Ostendo**.
 - a. Log into **Ostendo** on your Client machine using an account with Administrator Privileges.

Remote Server Ostendo API Setup for Freeway and Third Party Connections

- b. Navigate to **File->API Service->API Security**
- c. By default **Ostendo** will have an API connection security record called **Ostendo | Freeway**. If it is not visible, click **Add** and create one with:
 - i. **SQL Allowed** – Tick,
 - ii. **API Key for** – Internal
- d. Highlight this security record and click the **Fast Code** button in the right-hand menu.
- e. Record the resulting **Fast Code** number. This will be used in the steps below to connect to **Ostendo** through your newly created port.

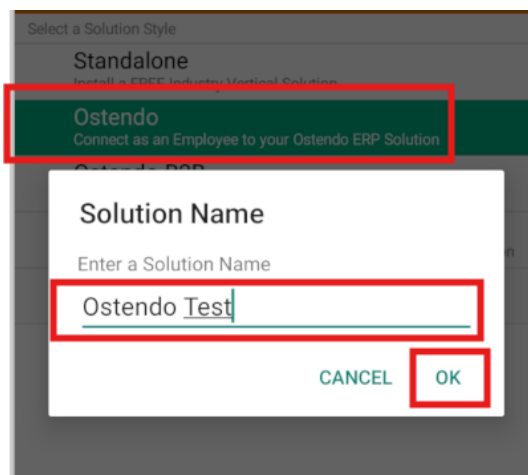


2. Install **Ostendo Freeway** in your Android or IOS phone through the Play or App Store. Make sure the originator is **Development-X Limited**:

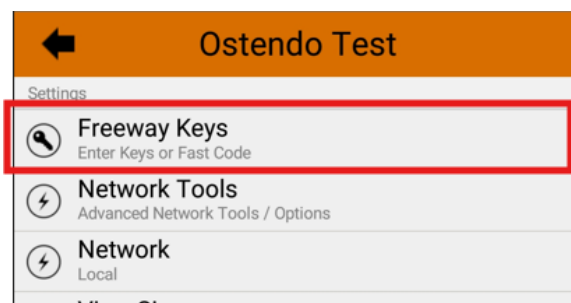


3. Open the application and select **Ostendo – Connect as an Employee to your Ostendo ERP Solution**.

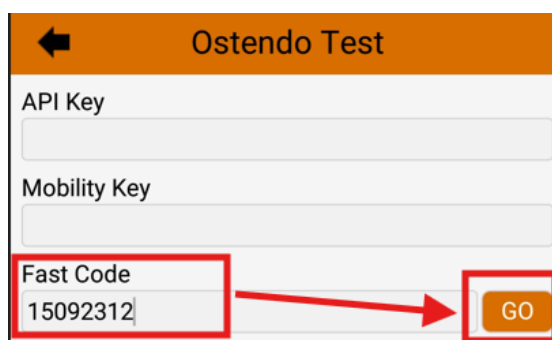
4. Enter a user friendly **Solution Name** (anything will do) and tap **OK**.



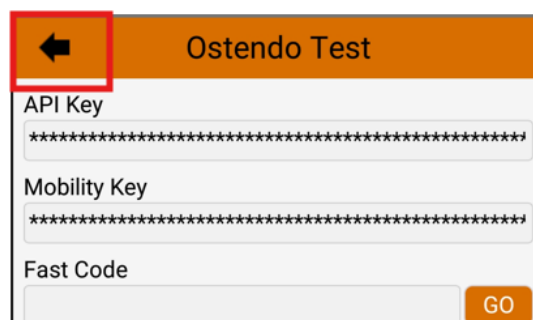
5. Tap **Freeway Keys** from the resulting menu.



6. Enter the **Fast Code** from the above **Step 1** and tap **OK**. The result, after a moment, should be a line of asterisks in the **API Key** and **Mobility Key** fields. This means the App has connected with the Ostendo Cloud store and has retrieved the correct keys.



7. Tap the back button



8. Then tap **Network Tools->Diagnostics**. If all has gone well, you will see 4 green ticks saying the connection to your database API has been successful.

