OSTENDO

One system . **Complete** operations

Ostendo
Continuum Edition

Cloud Server Deployment Guide

(AWS only)

14/01/2026

Revision 1.0.0

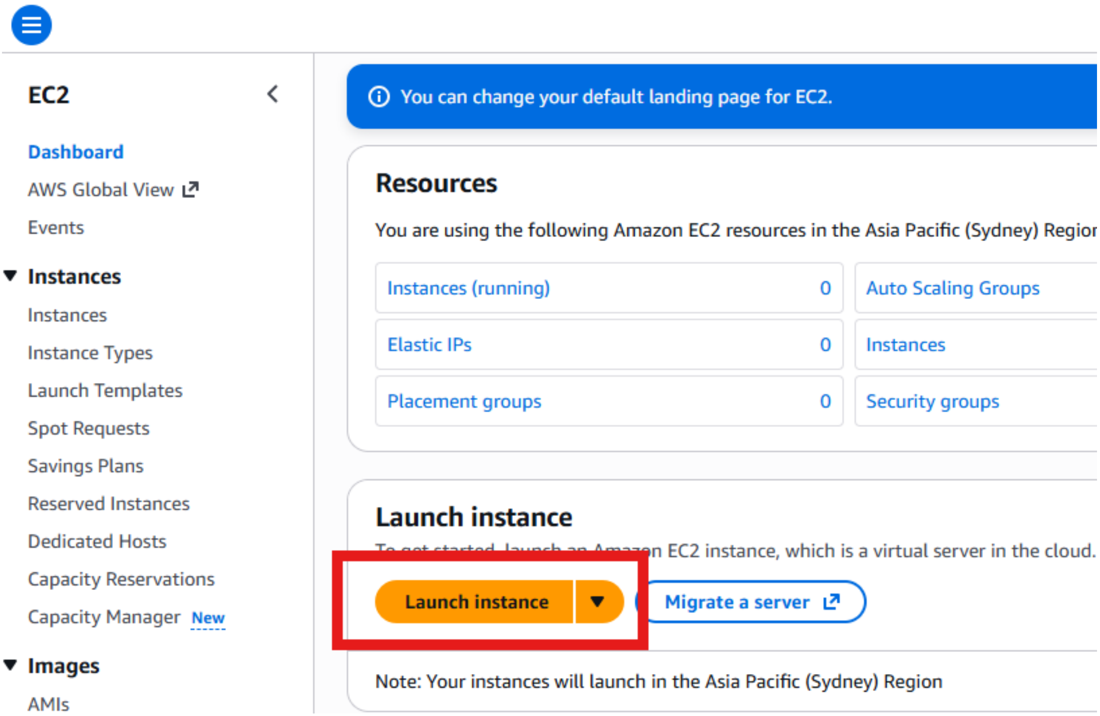
Table Of Contents

Overview

AWS is a popular choice to commission a virtual server in the cloud that can be hosted nationally, spun up easily and charged by the hour. Below is a guide suited for an AWS user to load Ostendo Continuum on an EC2 windows based instance.

Spin up the Server.

Log into AWS, choose your **region**. Search for **EC2** in the search bar and select **Launch instance**



You can change your default landing page for EC2.

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Sydney) Regior

Instances (running)	0	Auto Scaling Groups
Elastic IPs	0	Instances
Placement groups	0	Security groups

Launch instance

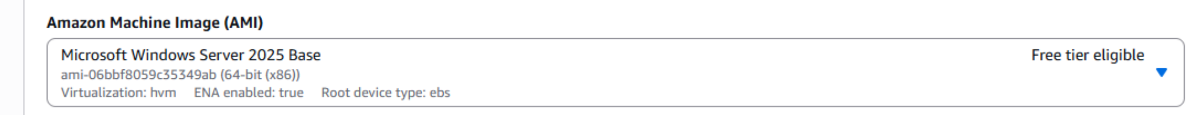
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the Asia Pacific (Sydney) Region

Selections (This is a guide based on an average speed 5 user server. It can easily be upgraded at a later date without affecting data):

a. Name – **'Ostendo cloud'**

b. AMI – **Microsoft Windows Server 2025 Base**

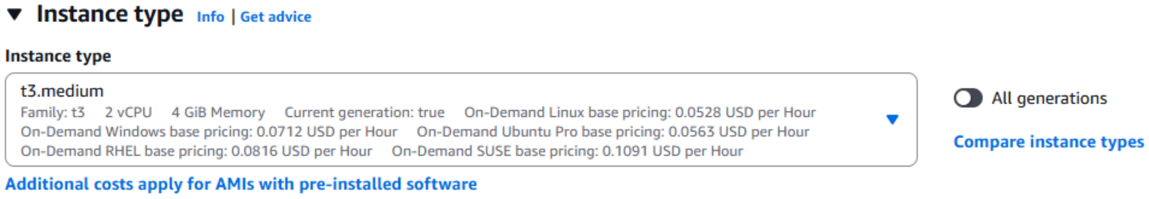


Amazon Machine Image (AMI)

Microsoft Windows Server 2025 Base
ami-06bbf8059c35349ab (64-bit (x86))
Virtualization: hvm   ENA enabled: true   Root device type: ebs

Free tier eligible

c. Instance Type – **t3.medium**



Instance type Info | Get advice

Instance type

t3.medium
Family: t3   2 vCPU   4 GiB Memory   Current generation: true   On-Demand Linux base pricing: 0.0528 USD per Hour
On-Demand Windows base pricing: 0.0712 USD per Hour   On-Demand Ubuntu Pro base pricing: 0.0563 USD per Hour
On-Demand RHEL base pricing: 0.0816 USD per Hour   On-Demand SUSE base pricing: 0.1091 USD per Hour

Additional costs apply for AMIs with pre-installed software

d. **Key Pair** – Select a key pair if you have one to use, or else create one (RSA, .pem) and save the .pem file somewhere safe.

e. Network settings (firewall):
   i. Check **Create security group**
   ii. Allow RDP Traffic
   iii. Allow HTTPS traffic from the internet
   iv. Allow HTTP traffic from the internet

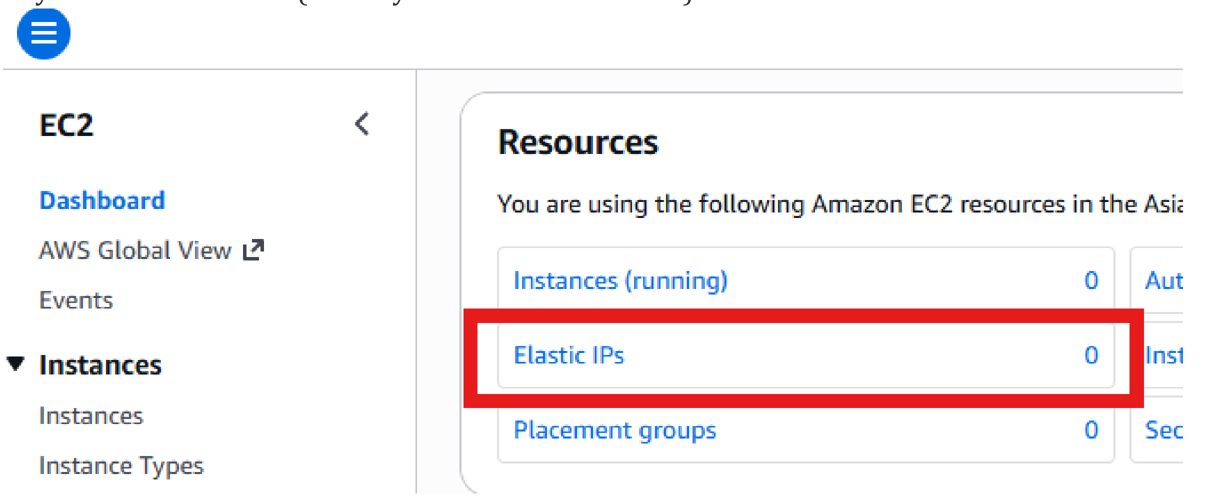
f. **Configure storage** – Allow 20GB for the operating system plus your database size plus any documents you want to store, for example Job Documents, Customer Documents.
   20GB + DB + Documents

g. Select **Launch instance**

Assign an elastic IP.

If you are intending on using this as a production server then it is good practice to assign an IP address to the EC2 instance (VPC) so that you can stop the server, upgrade and restart the server without having to reset any DNS settings. AWS provide use of elastic IP addresses for this reason free to use. If you are just testing and don't plan to use this server for long, then you can skip this step.

a. In your EC2 dashboard (where you started in 1a above) select Elastic IPs:



You are using the following Amazon EC2 resources in the Asia

Instances (running)	0
Elastic IPs	0
Placement groups	0

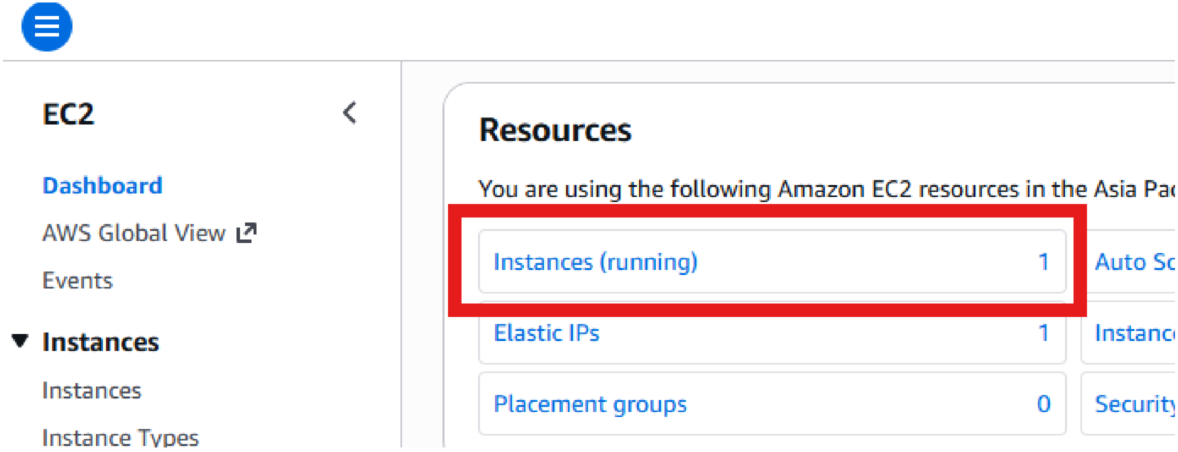
b. Select Allocate Elastic IP address and click Allocate

c. Tick the check box beside the elastic IP just created and in the **Actions** menu above select '**Associate IP Address**'

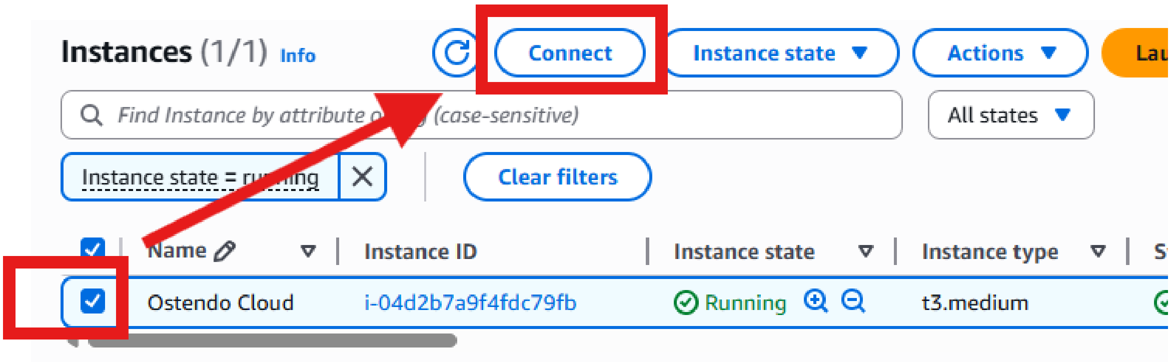
d. In the Associate Elastic IP Address page tick '**Instance**' and select the instance name in the Instance field, then click '**Associate**'

Set up RDP

a. From the EC2 dashboard page select **Instances (running):**

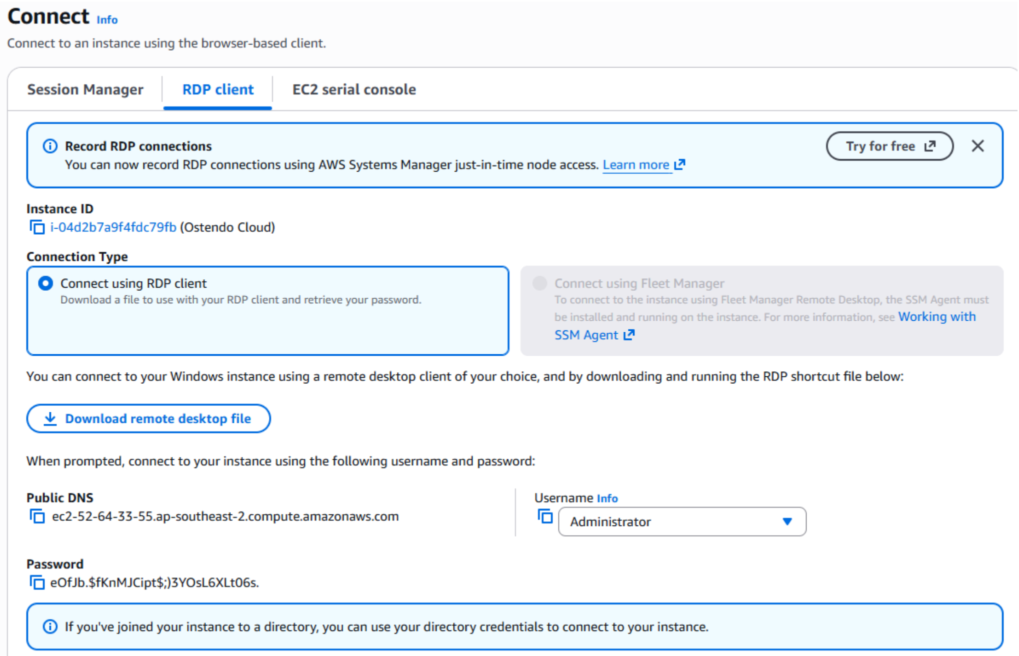


b. In the Instances screen check the ‘Ostendo Cloud’ instance and click Connect:



c. In the Connect page select ‘Connect using RDP client’ and click ‘Get password’.

d. In the resulting Get Windows Password screen click ‘Upload private key file’ then upload the `.pem` file you saved in step 1.d. Then click 'Decrypt password’ and save the password in a safe place. The resulting screen should look something like this:



Connect Info

Connect to an instance using the browser-based client.

Record RDP connections
You can now record RDP connections using AWS Systems Manager just-in-time node access. Learn more

Instance ID
i-04d2b7a9f4fdc79fb (Ostendo Cloud)

Connection Type

● Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

○ Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see Working with SSM Agent

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

When prompted, connect to your instance using the following username and password:

Public DNS
ec2-52-64-33-55.ap-southeast-2.compute.amazonaws.com

Username Info
Administrator

Password
eOfJb.$fKnMJCipt$;)3YOsL6XLt06s.

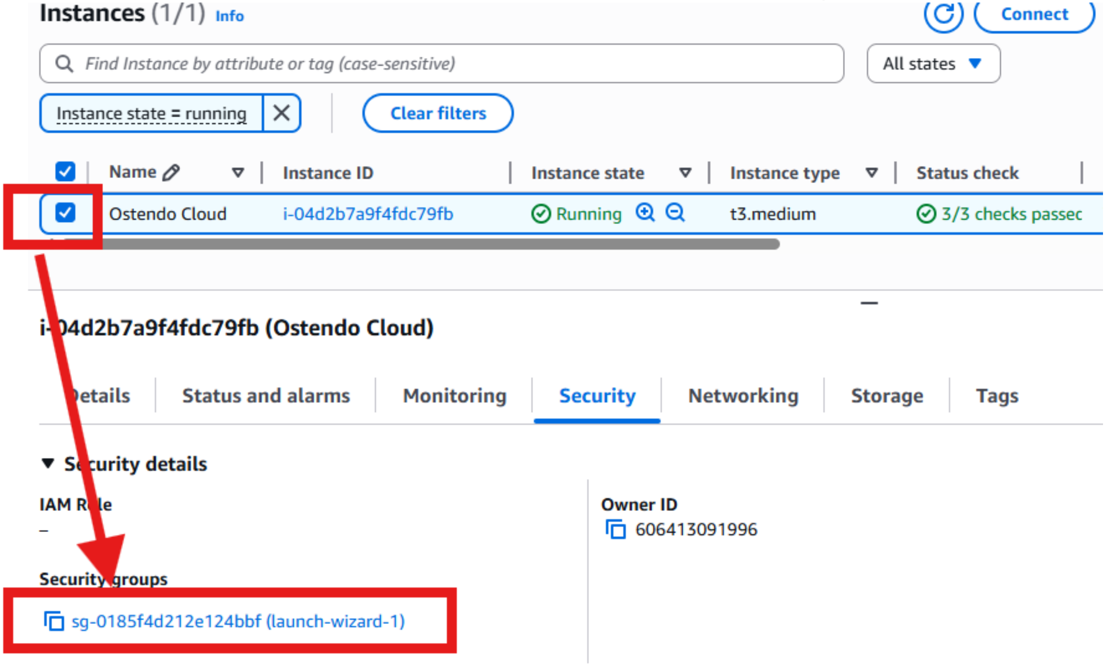
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

e. Click **Download remote desktop file**, and save the .rdp file in your computer for remote access.

Open TCP port in security group.

This allows traffic on a port for Ostendo HTTPS connection.

a. In the EC2 dashboard page select Instances (running), select 'Ostendo Cloud' instance and click into the Security tab. Click the associated Security group:



Instances (1/1) Info

☑	Name	Instance ID	Instance state	Instance type	Status check
☑	Ostendo Cloud	i-04d2b7a9f4fdc79fb	Running	t3.medium	3/3 checks passec

i-04d2b7a9f4fdc79fb (Ostendo Cloud)

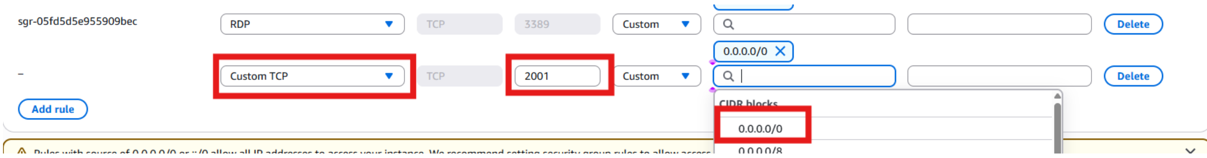
▼ Security details

IAM Role
–

Owner ID
606413091996

Security groups
sg-0185f4d212e124bbf (launch-wizard-1)

b. Click **Edit inbound rules**, then **Add rule**, then enter '**Custom TCP**'. Choose a port you want Ostendo HTTPS connection to run on, e.g. **2001,** and the port range as **0.0.0.0/0**.



sgr-05fd5d5e955909bec	RDP	TCP	3389	Custom	0.0.0.0/0		Delete
–	Custom TCP	TCP	2001	Custom			Delete

CIDR blocks
0.0.0.0/0
0.0.0.0/8

Add rule

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access

c. Click **Save rules**.

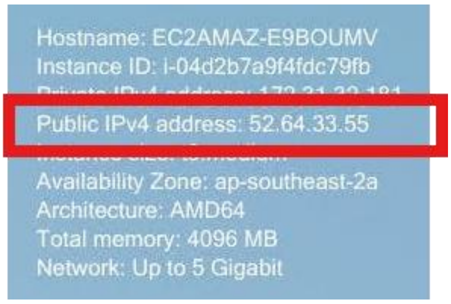
The following step creates a free SSL certificate using Lets Encrypt, OpenSSL and Chocolatey, ready for binding to the HTTPS port for Ostendo cloud use. This is necessary for HTTPS connection. You will need access to a web domains DNS settings to add an 'A' type DNS record. You can skip this if you already have an SSL certificate you can use, or if you want to set up an insecure connection using http (not recommended).

Download your installation files.

Go to http://ostendo.info/downloads/ostendo/20251119_Ostendo_Server_Install.zip and download the server installation files needed for the following steps.

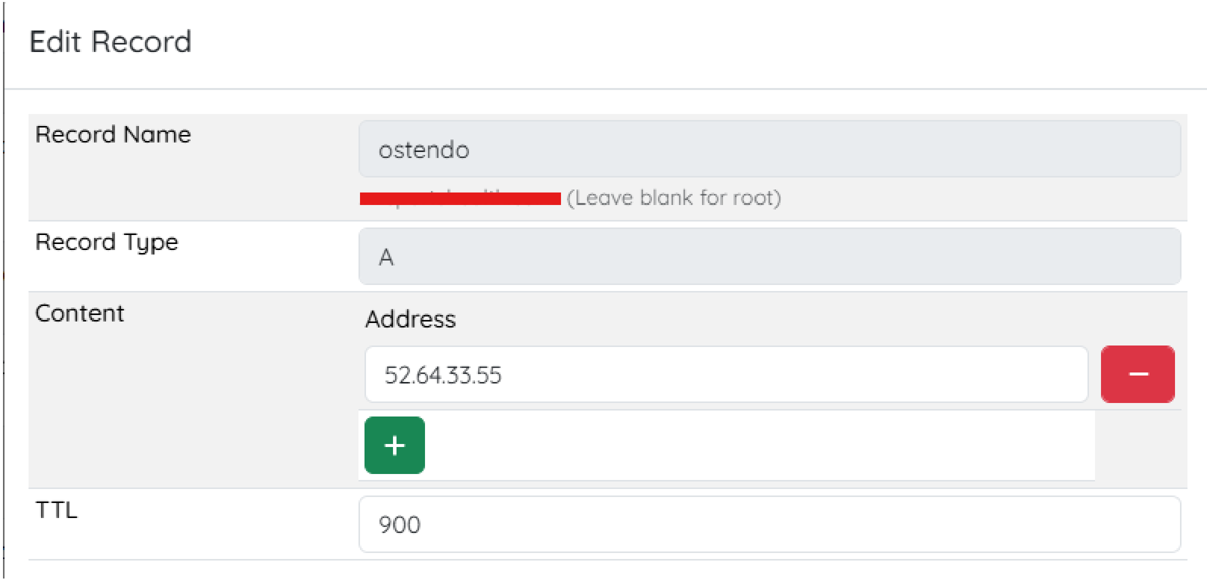
Log into RDP and create SSL certificate.

a. Using the `.rdp` file you downloaded in step 3.e and the password you saved in 3.d log into remote desktop. Your public IP address should be displayed in the top right hand corner of the desktop:



```
Hostname: EC2AMAZ-E9BOUMV
Instance ID: i-04d2b7a9f4fdc79fb
Private IPv4 address: 172.31.30.181
Public IPv4 address: 52.64.33.55
[illegible]
Availability Zone: ap-southeast-2a
Architecture: AMD64
Total memory: 4096 MB
Network: Up to 5 Gigabit
```

b. Add an 'A' type entry to your DNS settings for a domain record using the above IP address. This example is set in webcentral.au. The DNS record may take some time to propagate, if you have problems with the next steps it pays to wait a while before continuing.



Edit Record

Record Name	ostendo [redacted] (Leave blank for root)
Record Type	A
Content	Address 52.64.33.55
TTL	900

c. Unzip the Ostendo installation files sent to you, upload and run the script in powershell. Follow the prompts and answer all questions. This may take 3 to 5 minutes to complete.

Set up Firebird

a. Create a Firebird Folder in remote desktop. In this example **C:/Firebird**.
b. Search for the latest version of Firebird 5.0. At the time of this writing the latest is at: https://www.firebirdsql.org/en/firebird-5-0/
c. Download the latest 64 bit Windows executable file into the above Folder, and **run as administrator**.
d. Install Firebird in your own folder, e.g. C:/Firebird/Firebird_5_0.
e. Select all defaults and choose your own SYSDBA password. Make the password **different to 'masterkey'** for security reasons and store this password somewhere safe. In firebird 5.0 the most common setup is superserver. This efficiently allocates CPU cores and RAM across multiple users in an Ostendo environment.
f. Click **Install** then **Start firebird service**.

Upload Ostendo installation files

Upload Ostendo Installation files to Remote desktop, e.g. C:/Ostendo. If you already have a firebird 5.0 database then upload this also, e.g. to C:/Ostendo/Database.

Set up Ostendo – Database

Skip this step if you already have a firebird 5.0 Ostendo version 243 database

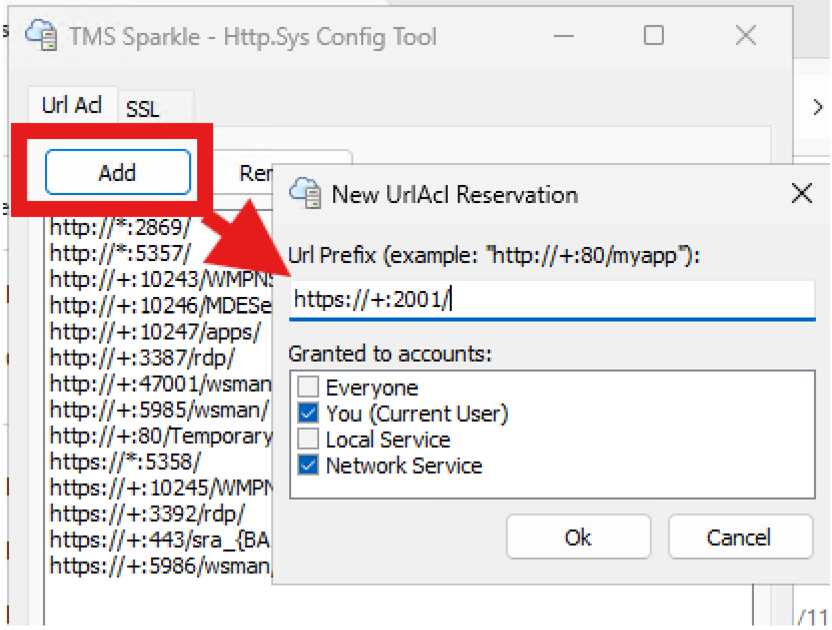
a. Create a database folder, e.g. C:/Ostendo/Database. Upload a backed up version of a Firebird 2.5 Ostendo 243 database, e.g. C:/Ostendo/Database/243_Ostendo.FBK.
b. Navigate to your Firebird 5.0 Folder (e.g. Firebird/Firebird_5_0/) and open a command window (Type **cmd** in **navigator bar**)
c. Restore the backup using gbak command (replace database locations if necessary and substitute your_sysdba_password):

```
gbak -create -verbose -user SYSDBA -password your_sysdba_password
c:/Ostendo/Database/243_Ostendo.fbk c:/Ostendo/Database/Ostendo.fdb
```

Set up Ostendo – Config.

a. Run **TMSHttpConfig.exe** in your Ostendo folder where you uploaded the setup files.

b. **Add** an entry using the port number you set up in security settings step 4.b (in this example port 2001) and click **OK**:



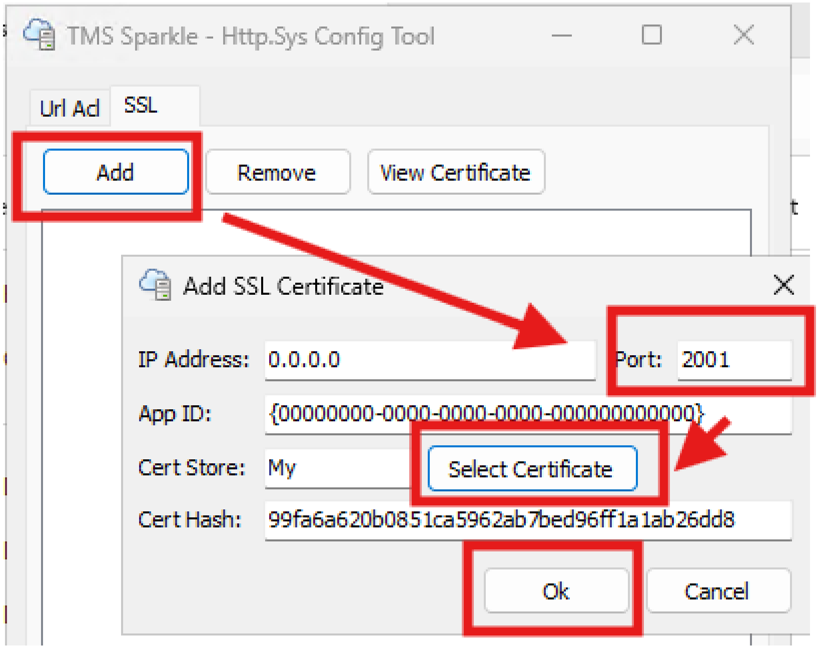
http://*:2869/
http://*:5357/
http://+:10243/WMPN:
http://+:10246/MDESe
http://+:10247/apps/
http://+:3387/rdp/
http://+:47001/wsman
http://+:5985/wsman/
http://+:80/Temporary
https://*:5358/
https://+:10245/WMPN
https://+:3392/rdp/
https://+:443/sra_{BA
https://+:5986/wsman

Url Prefix (example: "http://+:80/myapp"): https://+:2001/

Granted to accounts:

- ☐ Everyone
- ☑ You (Current User)
- ☐ Local Service
- ☑ Network Service

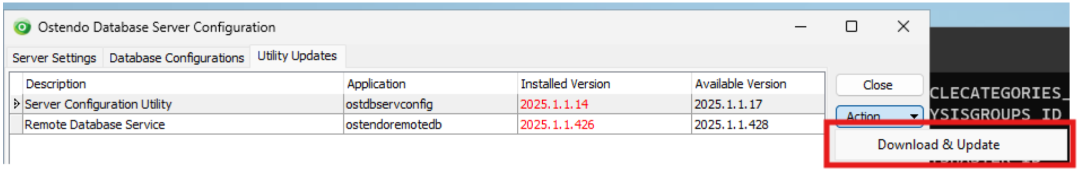
c. Navigate to the **SSL** tab and bind the SSL certificate you created in step 6.c. Click **Add**, then change the port to your Ostendo port (e.g. 2001), select the certificate and click **OK**.



IP Address: 0.0.0.0
Port: 2001
App ID: {00000000-0000-0000-0000-000000000000}
Cert Store: My
Cert Hash: 99fa6a620b0851ca5962ab7bed96ff1a1ab26dd8

d. Run **ostdbservconfig.exe** as **Administrator**

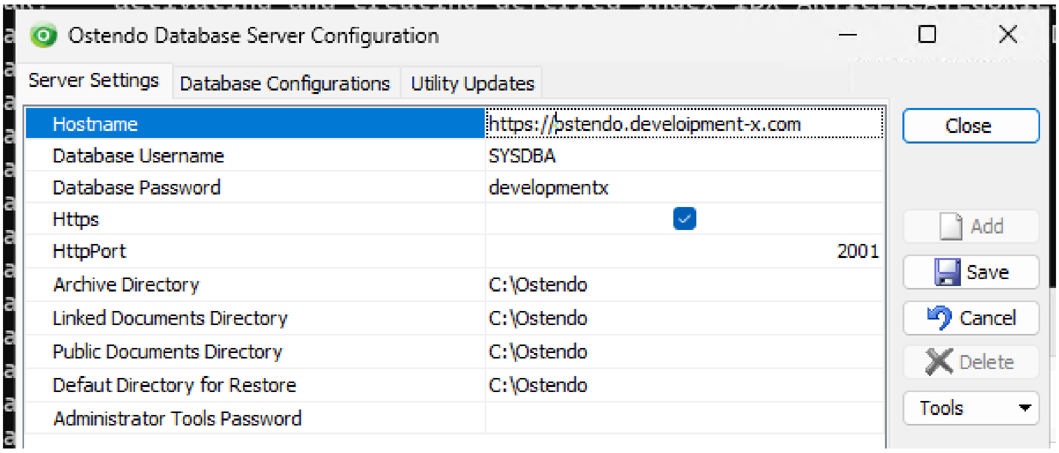
i. Go to the **Utility Updates** tab and ensure the utility versions are up to date by selecting **Action->Download & Update** for each line. You may be required to restart ostdbservconfig.exe each time:



Description	Application	Installed Version	Available Version
Server Configuration Utility	ostdbservconfig	2025.1.1.14	2025.1.1.17
Remote Database Service	ostendoremotedb	2025.1.1.426	2025.1.1.428

ii. In the **Server Settings** tab enter the Database and default folder settings and click **Save**:

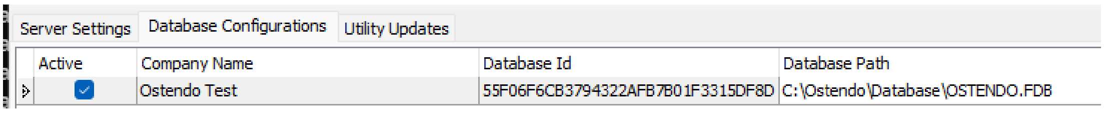
- **Hostname** – Your domain name that is bound with the SSL certificate (e.g. https://ostendo.development-x.com)
- **Database Password** – Your Firebird SYSDBA password set in step 7.e
- **HttpPort** – The Ostendo port that you have bound your SSL certificate to in step 10.c (e.g. 2001)
- **Default directories** – you to change the default directories that Ostendo works in.
- **Administrator Tools Password** – To be used at a later date for remote administration. Not needed for now.



Hostname	https://ostendo.develoipment-x.com
Database Username	SYSDBA
Database Password	developmentx
Https	☑
HttpPort	2001
Archive Directory	C:\Ostendo
Linked Documents Directory	C:\Ostendo
Public Documents Directory	C:\Ostendo
Defaut Directory for Restore	C:\Ostendo
Administrator Tools Password	

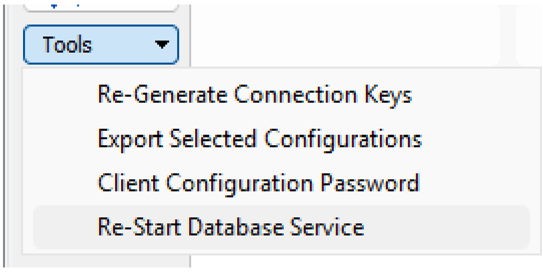
iii. Navigate to the **Database Configurations** tab and set up a company config for the Database you uploaded earlier with the following and click **Save**:

- **Company Name** – Choose a name that will be displayed in the client connection for the connected database
- **Database Path** – Browse and select the Database you restored/uploaded in steps 8 and/or 9.
- **Client Password** – Optional. Used to set a password the client needs so they can configure their client machine to access this Database



Active	Company Name	Database Id	Database Path
☑	Ostendo Test	55F06F6CB3794322AFB7B01F3315DF8D	C:\Ostendo\Database\OSTENDO.FDB

iv. Restart the database – **Tools->Re-Start Database Service**


Tools
Re-Generate Connection Keys
Export Selected Configurations
Client Configuration Password
Re-Start Database Service

v. Create the config file for client install – **Tools->Export Selected Configurations** and save **clientconfig.txt** to your Ostendo Folder.

e. Run **InstallAPI.bat** as **Administrator** from the install files. This installs the Ostendo remote database service required for HTTPS protocol. This is not the Ostendo API.

f. You may now close the config window, Ostendo server has been set up. Copy the **clientconfig.txt** file to your local computer to set up the 243 client install as you would have done previously.

Open the Firewall to the Ostendo port

Create a firewall incoming and outgoing rule to allow traffic on the server to the Ostendo Port.

a. Open **Windows Defender Firewall with Advanced Security** from the windows toolbar search.

b. Navigate to **Inbound Rules** and select **New Rule**. Cycle through and set the following settings:

- Rule Type – **Port**
- Protocol and Ports – **TCP**, **Specific local ports** add port name (e.g. 2001)
- Action – **Allow the connection**
- Profile – Leave default ticked for all
- Name – 'Ostendo Server 1'

Click **Finish** to save.

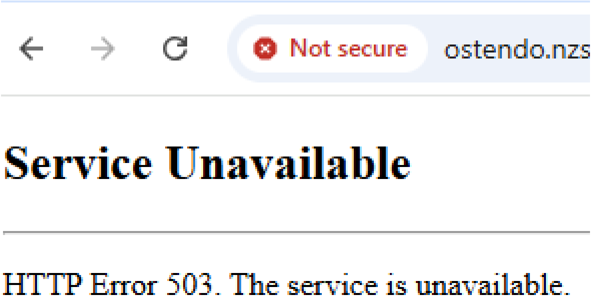
c. Navigate to Outbound Rules and select New Rule. Cycle through and set the following settings:

- Rule Type – Port
- Protocol and Ports – **TCP**, **Specific remote ports** add port name (e.g. 2001)
- Action – **Allow the connection**
- Profile – Leave default ticked for all
- Name – 'Ostendo Server 1'

Trouble Shooting

If you experience an issue with the install here are some steps to follow that could help:

a. In a browser navigate to https://your-domain.com:your_port. You should see something like the following if all is running correctly:



Service Unavailable

HTTP Error 503. The service is unavailable.

b. Check the certificate log on the server in C:/Certs/

c. Check the Windows event log on the server for errors

d. From the window start menu run ISQL. Make sure you can connect to the database with the command:

```
connect "localhost:C:/Ostendo/Database/Ostendo.fdb" user 'SYSDBA'
password 'your_sysdba_password';
```

e. Restart the OstendoDB service. Run **ostdbservconfig.exe** as administrator, and in the Server Settings tab select **tools->Stop Database Server**, then **Tools->Start Database Server**.

f. Reboot the server and try again

Tidy up

a. If you no longer need port 80 or port 443 to be open it would be good practice to delete the entry in the AWS Security Group that relates to this instance. Follow step 4.a and then delete the port 80 and/or port 443 lines.