OSTENDO

One system . **Complete** operations

Ostendo
Continuum Edition

Cloud Sever Deployment Guide

(Generic)

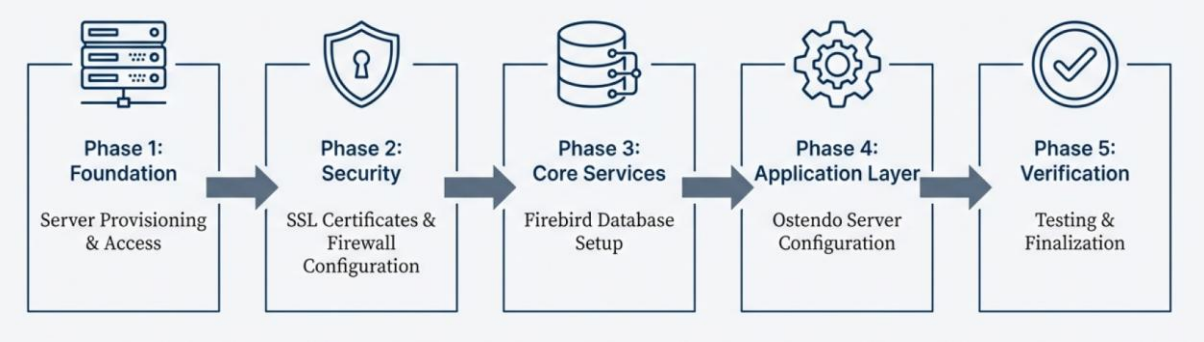
[Publish Date]

[Status]

Table Of Contents

Overview

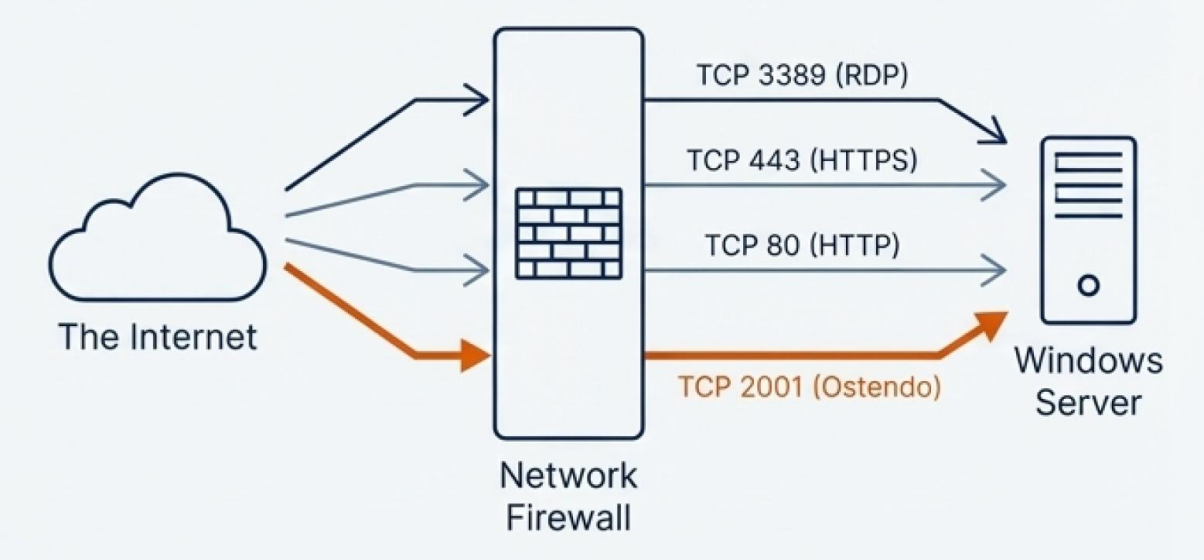
This guide breaks down the installation into five logical phases. Follow this blueprint to ensure a structured, repeatable, and successful setup of your Ostendo server



Phase 1: Laying the Foundation

1. **Provision a Windows Server**
   - **Recommended OS**: Microsoft Windows Server 2022 Base or newer.
   - **Minimum Specifications**: 2+ CPU Cores, 4GB+ RAM (e.g. Azure B-Series B2ls_v2)
   - **Storage Allocation**: Drive space needed is *Database Size + Document Storage Space + Room to grow*. As a guideline allow minimum 50GB more than the OS for an SME with 5 users.
2. **Assign a Static IP Address**
   - **Rationale**: A static public IP is critical for production servers. It ensures DNS records remain valid and remote connections are reliable, even after the server is rebooted or restarted.
3. **Establish Remote Desktop (RDP) Access**
   - **Action**: Securely connect to your new server instance.
4. **Download and Unpack the Ostendo Setup Files**
   - **Action:** Download the `Ostendo_Server_Install.zip` package from the official Ostendo download site https://ostendo.info/downloads/ostendo/Ostendo_Server_Install.zip.
   - **Action:** Create a dedicated folder (e.g. `C:\Ostendo`) on your server and unzip the content of the package into it.

Phase 2: Securing the Perimeter (Part 1 – Network)



Before any traffic can reach the server's operating system, it must pass through the network firewall. This could be a cloud providers security group (e.g. Azure Network Security Group inbound and outbound rules), a corporate hardware firewall, or a virtual appliance.

Required Firewall Rules (Inbound Traffic):

- **RDP (Port 3389)**: Allow traffic from trusted IP addresses for administration.
- **HTTPS (Port 443) and HTTP (Port 80)**: Allow traffic from the internet. This is temporarily required for SSL certificate validation.
- **Ostendo Service (Custom TCP Port)**: Create a new rule to allow traffic for your chosen Ostendo Port. The example port used throughout this guide is **2001**.

Phase 2: Securing the Perimeter (Part 2 – SSL)

1. **Point a Domain Name to your Server**
   - **Action**: In your registrar's DNS settings, create an 'A' record that points your desired hostname (e.g. `ostendo.yourcompany.com`) to a static IP address assigned in Phase 1.
2. **Generate & Install an SSL Certificate**
   - **Goal**: Obtain a valid SSL certificate that is bound to your domain name.
   - **Options**:
     - You can use free tools like Let's Encrypt (which can be automated via scripts) or
     - purchase a commercial SSL certificate for assured security (e.g. ssl2buy.com, thesslstore.com) or
     - run the provided script (`Setup_SSL.ps1`) in Powershell which utilises Let's Encrypt, OpenSSL and Chocolatey to automate a free Let's Encrypt certificate.

- **Process**: This typically involves running an installer or script on the server which communicates with the certificate authority to validate your domain ownership.

> ***Pro-Tip:*** *DNS changes can take time to propagate globally. If you encounter errors during certificate validation, wait a while to try again.*

Phase 3: Installing Core Services

Set Up the Firebird 5.0 Database Engine

1. **Download**: Search for and download the latest Windows installer for Firebird 5.0. At the last edit of this document the Latest version is 5.0.3 which can be downloaded from https://www.firebirdsql.org/en/firebird-5-0/
2. **Install Location**: Run the installer as an administrator. It is best practice to install it to a dedicated folder (e.g. `C:\Firebird\Firebird_5_0`).
3. **Installation Options**: Accept the default components. Use the recommended SuperServer model, which efficiently manages resources in a multi-user Ostendo environment.
4. **Finalise**: Complete the installation and ensure the "Start Firebird service now" option is checked.

> **Critical Security Warning**
>
> During Installation, you will be prompted to set a SYSDBA password.
> **Do not use 'masterkey'.** Choose a unique password and store securely in your password manager. This password is the master key to your database

Phase 4: Application Layer (Part 1 – Database)

Choose the option that matches your scenario to set up the Database:

Option A: Restore a Firebird 2.5 Database Backup

- **Action**: Place your Firebird 2.5 Ostendo (v243) backup database file (e.g. `243_Ostendo.fbk`) into a sub-folder (e.g. `C:\Ostendo\Database`).
- **Action**: Navigate to your Firebird directory (e.g. `C:\Firebird\firebird_5_0`). Open a command prompt and restore the backup using the gbak utility:

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

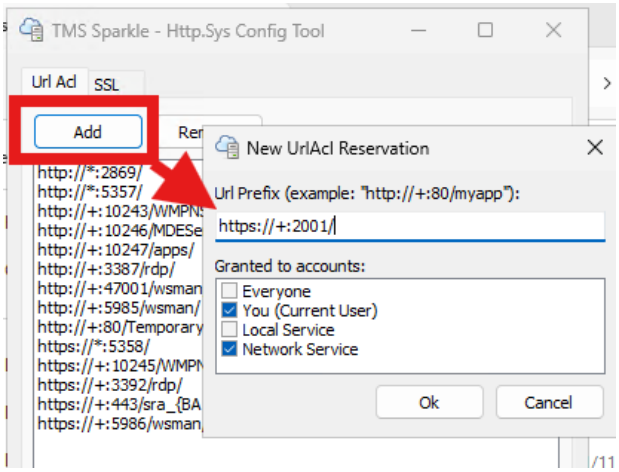
Option B: Use an existing Firebird 5.0 Database

- **Action**: If you already have a compatible Firebird 5.0 database file (.fdb), simply copy it to your chosen database directory (e.g. `C:\Ostendo\Database`). The Database must be an Ostendo Version 243 database.

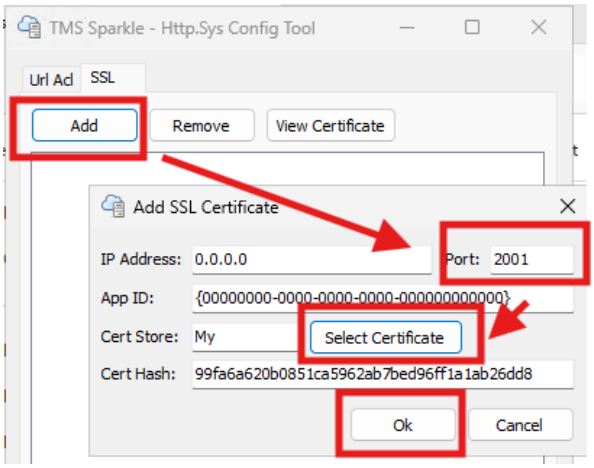
Phase 4: Application Layer (Part 2 - HTTPS Binding)

Configure the Ostendo HTTP Service

Tool: Run TMSHttpConfig.exe from your Ostendo installation folder (e.g. `C:\Ostendo`).



1. Add Service Port: On the main tab, click **Add**. Enter the custom TCP port you opened in your network firewall for Ostendo (e.g. **2001**) and click ok. The entry should look like this: `https://+:2001/`



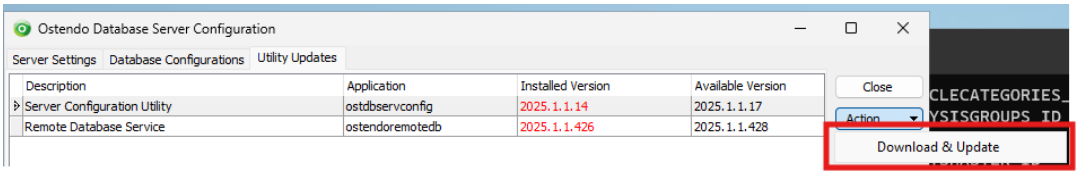
2. Navigate to the **SSL** tab. Click **Add**. Change the port to match your service port (e.g. **2001**). Select the SSL certificate you generated in Phase 2 from the dropdown list. Click **OK** to save the binding.

Phase 4: Application Layer (Part 3 – Server Settings)

Configure Core Ostendo Server Parameters

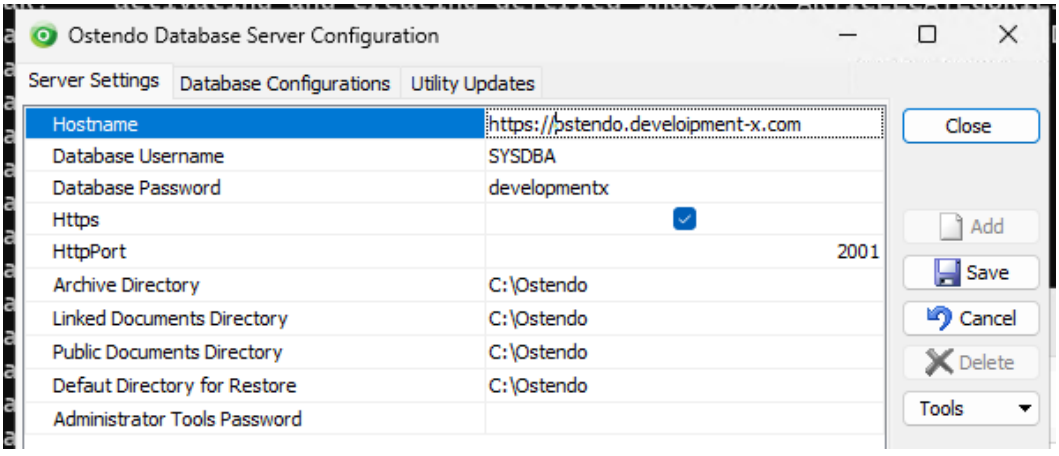
Tool: Run ostdbservconfig.exe as Administrator from your Ostendo folder.

1. **Update Utilities**:
   - First navigate to the **Utilities Tab**.
   - For each item in the list, select **Action -> Download & Update** to ensure you are running the latest versions.



   - You may need to restart the tool after an update.

2. **Configure Server Settings**:
   - Navigate to the **Server Settings** tab
   - Enter the following:
     - **Hostname** – Your domain name that is bound with the SSL certificate (e.g. https://ostendo.yourcompany.com)
     - **Database Password** – Enter the secure SYSDBA password you created during the Firebird installation.
     - **HttpPort**: Enter the custom port you configured (e.g. 2001)
   - Click **Save**.

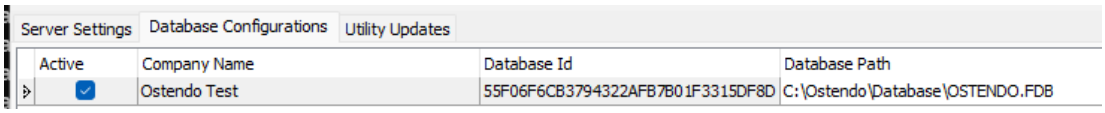


Phase 4: Application Layer (Part 4 – Company Config)

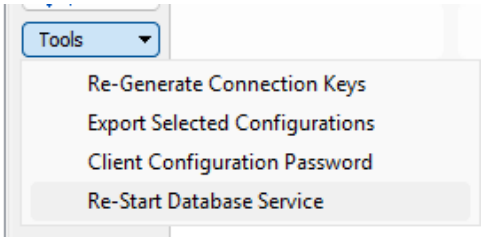
Finalise Company Database and Services

Tool: Continue using `ostdbservconfig.exe`

1. **Link the Company Database:**
   - Go to the **Database Configurations** tab.
   - Click **Add** to create a new configuration
     - **Company Name**: Assign a descriptive name. This name will become the Ostendo instance name for the client (e.g. My Company Live).
     - **Database Path**: Browse to and select your .fdb database file.
   - Click **Save**.



2. **Activate and Export:**
   - Restart service by selecting the menu **Tools->Re-Start Database Service**.
   - Select **Tools->Export Select Configurations**. **Save** the resulting `clientconfig.txt` file to your Ostendo folder. This file is all you need for client setup.



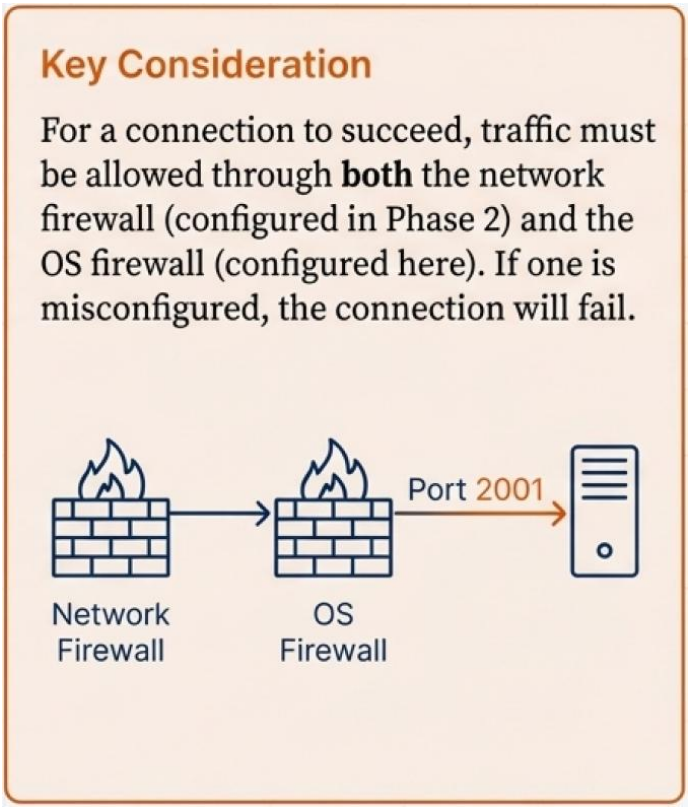
3. **Install Ostendo Service:**
   - From your Ostendo folder installation files, find and run `InstallAPI.bat` as an Administrator. This uses everything set up so far and installs the service required for remote database connections over HTTPS.

Phase 5: Verification (Part 1 – OS Firewall)

Configure the Windows Defender Firewall

Tool: Open **Window Defender Firewall with Advanced Security** from the Windows start menu.

1. **Create Inbound Rule**
   - Select **Inbound Rules->New Rule…**
   - **Rule Type**: Port
   - **Protocols and Ports**: TCP, Specific local ports: 2001 (or your chosen port).
   - **Action**: Allow the connection
   - **Profile**: Leave all profiles ticked
   - **Name**: Give it a descriptive name (e.g. Ostendo Server)
   - Click **Finish** to save
2. **Create Outbound Rule:**
   - Select **Outbound Rules->New Rule…** and repeat the process above. Be sure to change the default Action **Block the Connection** to **Allow the Connection**.



Phase 5: Verification (Part 2 – Testing)

Testing and Troubleshooting

Test 1: Web Service Connection (External)

- Action: From any web browser, navigate to your servers address (e.g. https://ostendo.yourcompany.com:2001)
- Expected result: There should be minimal delay before you get a `standard service unavailable (HTTP error 503)` message within your browser.

Test 2: Database Connection (Internal)

- Action: On the server itself, run the ISQL tool from the Start Menu.
- Don't forget the semi-colon at the end

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

- Command: Enter the following to test the direct database link:
- Expected Result: The prompt should change to SQL>, and state that it is connected to your Database. This indicates a successful connection from the Firebird service to your Database.

Troubleshooting Common Issues

Connection failed? Check these first.

- **DNS Propagation**: Has your 'A' record fully propagated? Use a command line tool like `nslookup your-domain.com` to verify the IP address is correct.
- **Firewalls** (Plural): Double check that both your network firewall and the Windows OS firewall have rules allowing TCP traffic on your specific Ostendo port.
- **Running Services:** Open `services.msc`. Confirm that both the Firebird Server service and the Ostendo Connection services are in a Running state.
- **SSL Certificate Binding**: Is the certificate valid and correctly bound in `TMSHttpConfig.exe`? If you used the PowerShell script provided in the installation files to load a free SSL certificate then check the detailed error logs in the `C:\Certs\ folder` on the server.
- **The Universal Restart**: When in doubt reboot the server.

Phase 5: Verification (Part 3 - Finalising & Deployment)

1. **Security Hardening (Best Practice):** Once you have confirmed your HTTPS connection (e.g. on port 2001) is fully working, you should close the temporary ports on your network firewall.
    - **Action**: Remove the **Allow** rules for Port 80 (HTTP) and Port 443 (HTTPS) if they are not required for other applications on this server.
2. **Client Deployment**: The `clientconfig.txt` file you generated in *Phase 4* contains all the connection information your client workstation needs.
3. **Next Steps**: Securely distribute the `clientconfig.txt` file and the Ostendo Client installer to your end-users for setup on their machines.