# Triofox Installation Guide

## Triofox Server Version 13.5.9497.54016

# Table of contents:


- Introduction
- Overview
- System Components
  - 1. Web Server Component - The Triofox Server
  - 2. Database - Configuration Information and System Log
  - 3. Back-end File Storage - Where Files and Folders are Stored
- Step 1: Prepare the file store
- Step 2: Prepare Active Directory (Optional)
- Step 3: Prepare the Database Server
  - Microsoft SQL Server
  - MySQL Server
  - PostgreSQL
- Step 4: Prepare the Triofox Server
  - EC2 Server Type
  - Azure Virtual Machine Size Recommendation
- Step 5: Start Installation
- Configuration
- Enable SSL
  - Install SSL Certificate
  - External URL
- Setup Worker Node for SSL
- Verify External URL, Internal URL and the Node Name
  - Verify External URL
  - Verify Internal URL
  - Verify Node Name
- Add additional Triofox servers to the cluster

# Introduction

Welcome to the Triofox server installation guide. This guide describes the installation tasks for Triofox, which mobilizes your existing file servers.

Triofox includes Triofox Server, which runs on the Microsoft Windows server platform, and client agent applications for web browsers, Microsoft Windows, macOS, and for mobile platforms such as the Android and Apple iOS operating systems.

# Overview

Triofox is a secure remote and mobile access solution that focuses on faster remote access to on-premises file servers (also known as Cloud-enablement without a VPN). It differentiates itself from other file synchronization and sharing (EFSS) solutions by focusing on security, control, file servers and team collaboration. Triofox stands out because it focuses on improving existing file servers, while competitors try to make file servers obsolete. Impressive features include drive mapping, file locking, folder permissions, single sign-on and Active Directory integration, which are often neglected by the competition. Triofox makes file servers mobile and modern while maintaining traditional file server features. Triofox performs particularly well in the following areas:

1. Integrate existing Active Directory user identity and retain NTFS security permissions.
2. Provide on-demand access while respecting real-time read and write permissions.
3. Mirror local network shares on file servers to enable teams to collaborate on content in the cloud.
4. Provide virtual drive letters for file and folder access.
5. Provide protection against ransomware.
6. Enable offsite backups.
7. Provide file locking, version control, client encryption, and other advanced features to manage all virtual drives.

Triofox Server is a software built on Microsoft Web Platform:

- Windows Server
- IIS (Internet Information Server)
- .NET Framework and ASP.NET
- WCF (Windows Communication Foundation)

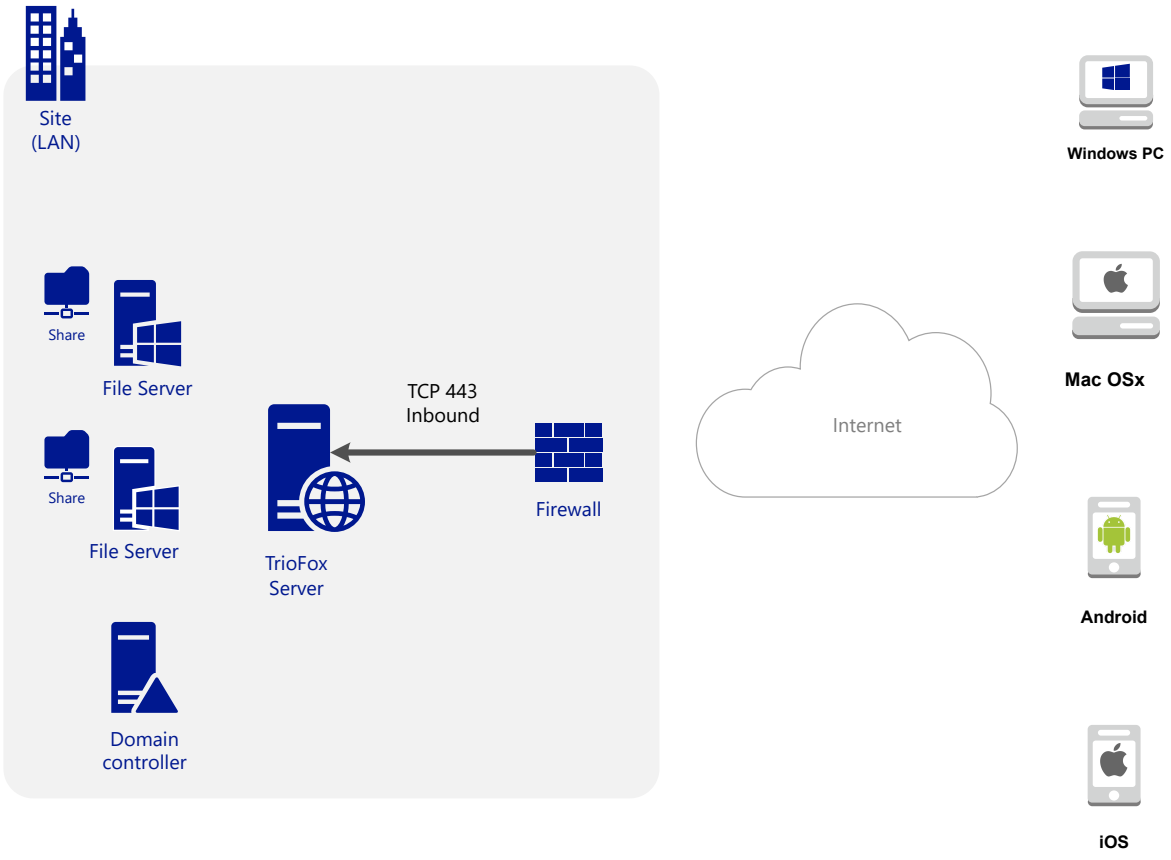
- PostgreSQL, MySQL, or Microsoft SQL Server

Since Triofox Server is built on the Microsoft Web Platform, it integrates very well with other Microsoft components such as NTFS permissions for files and folders, Active Directory users, and File Server network shares.

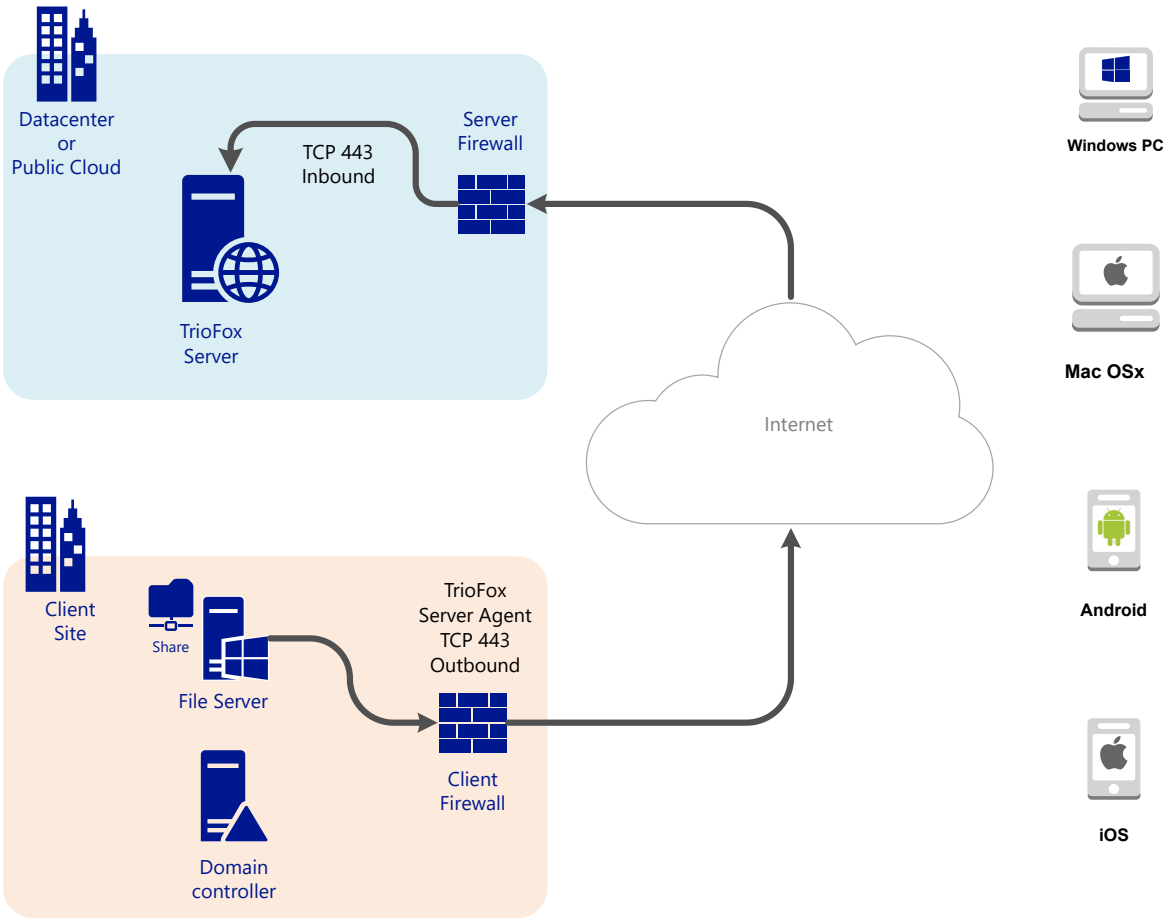
It provides file access and sharing capabilities via client agents for PCs, Macs, file servers, web browsers and mobile devices. The client agent software for Windows and Mac provides true drive mapping and volume mounting support that includes advanced optimization for WAN (Wide Area Network) data transfer.

The services can be used in flexible combinations to meet different requirements. There are two primary ways to deploy Triofox Server:

1. Deploy in the same site as the File Servers and Active Directory domain controllers:




2. Deploy in a site remotely, such as Amazon Web Services EC2, Microsoft Azure, or in a Data Center where the infrastructure is hosted:




## System Components

The Triofox server consists of three different system components (logical components that can coexist on the same server). In the smallest deployment unit, the three different components can coexist on a single machine (all-in-one deployment).

### 1. Web Server Component - The Triofox Server

The web server component is ASP.NET and WFC code hosted by IIS on a Windows server. The web server component actually consists of two separate "sub-components":

- Web Node
- Worker Node

These subcomponents exist for historical reasons and there are still elements in the Cluster Manager user interface that allow you to configure these subcomponents.

### 2. Database - Configuration Information and System Log

The database contains persistent information for the system. This persistent information includes static configuration information such as the user name, file server connection information, and Active Directory connection information. The database also stores dynamic information such as the activity log, file change log, and audit traces.

Triofox supports PostgreSQL, MySQL and Microsoft SQL Server (DMBS) database management systems. In the All-in-One installation, PostgreSQL is installed on the Triofox server. The All-in-One installation is suitable for testing the software, but an external database server is recommended for productive use.

## 3. Back-end File Storage - Where Files and Folders are Stored

The backend file storage component is the permanent storage location for files and folders. There are two different types of storage services. One is managed by Triofox, e.g. the default storage for the server. The other is imported storage, e.g. existing network shares of the file server that were not managed by Triofox but can be imported/connected into Triofox for remote and mobile access.

> If you are installing Triofox Server for the first time, we recommend the All-in-One installation, where you prepare a clean Windows Server 2019/2022/2025 virtual machine and run the installation with all default parameters. The All-in-One installation is the smallest fully functional setup and can be used for a production environment with < 1000 users.

## Step 1: Prepare the file store

The Triofox server connects your local file servers to your remote workers by providing remote and mobile access with synchronization and sharing capabilities. So the first question is: What is your file storage solution?

Your file storage can be a Windows File Server network share or any storage device that supports the CIFS/SMB protocol. It can also be iSCSI devices that you can mount directly as drive letters in the Triofox server. It can also be a container inside a private instance of OpenStack Swift, a bucket in an Amazon S3-compatible storage, or a container from a Windows Azure Blob storage. You need to have the basic access information ready. For example,

### Windows File Server

If it is a Windows File Server, you need the UNC path to the network share and the user credentials to access the folder.

If it is a local C: or D: drive, you need a local user credential that has full access rights to the local folder.

### OpenStack Swift

If it is OpenStack Swift, you will need the authentication URL and credentials. You also need to know the version of your authentication setup, such as KeyStone V2 or KeyStone V3, or just classic authentication.

### Amazon S3

If it is Amazon S3, you will need the access key and secret key and a bucket name. If the access key and secret key are from an IAM user, you must ensure that the IAM user has full permission to the bucket.

### Windows Azure Blob Storage

You need the "Storage Account Name" and the "Primary Key" as well as a container name.

> The initial deployment of Triofox configures the back end storage to use the `C:\Triofox` directory on the Triofox server. This default back end storage location can be changed to another location at a later time by modifying the back end storage of the default server.

## Step 2: Prepare Active Directory (Optional)

If you are including Active Directory, you will need the following information:

- The DNS name (or IP address) of an Active Directory domain controller.
- A service account that can access Active Directory.
- The DNS name of the Active Directory domain.

> If your Active Directory is local, the best practice is to join the Triofox Server machine to the Active Directory Domain first before the installation starts.

> If your Active Directory is located remotely with respect to the Triofox server, you should use the Server Agent software to connect the Active Directory instead of using LDAP to connect to the Active Directory.

## Step 3: Prepare the Database Server

> If you are installing the All-in-One instance, you can skip this step because the All-in-One installer installs a PostgreSQL server and configures the database accordingly. See Step 5: Start Installation below for more about the all-in-one installation. This step is only for installations with a separate database that is not installed by default with a Triofox server in the server farm. All Triofox servers in a server farm share a single central database.

> For Triofox, the default database engine for the "all-in-one" installation is PostgreSQL.

There are two places where persistent information is stored. The first place is the file store mentioned in step 1. The second place is the Triofox database. The database contains configuration information such as username, team folder, shared folder, and login token. The database also contains runtime information such as the audit trace and the file change log.

The default installation of Triofox uses a local PostgreSQL database on the Triofox server. We provide this option to make the POC (Proof of Consent) test installation as easy as possible.

Currently, Triofox supports PostgreSQL, MySQL or Microsoft SQL Server (DBMS) database management systems. Some good reasons for using an external database server are performance, scalability and high availability.

## Microsoft SQL Server

If you are using an external Microsoft SQL Server instead of the default PostgreSQL All-in-One deployment, you must ensure that **SQL Server authentication** is configured for **Mixed Mode** Authentication. The Triofox Server connection requires the use of a SQL account, not a Windows built-in authentication account.

During the setup of the first Triofox Server in the server farm (the server farm can be so small that it contains only one Triofox Server), the installer needs to create a database, create tables in the database, and create stored procedures in the database. Therefore, a SQL security account with sufficient rights is required for the installation.

If the database server is located outside the Triofox server, make sure that the TCP protocol is enabled and the firewall is open for SQL connections. The default TCP port is 1433 and this port must be open in the firewall. If your SQL server listens for incoming connections through another port, this port must also be open instead of the default TCP port.

## MySQL Server

MySQL typically listens on TCP port 3306. Make sure this port is opened on the firewall.

### PostgreSQL

The default TCP port for PostgreSQL is usually 5432, however this can easily be changed in the postgresql.

## Step 4: Prepare the Triofox Server

The easiest way to prepare the Triofox server is to use a clean Windows Server 2019/2022/2025 OS with English locale. If you want to use multiple Triofox servers to form a server farm, please make sure that the servers in the server farm are all in the same time zone.

> The Triofox server provides localization support for multiple languages, regardless of the fact that the base Windows OS works with the English locale.

We recommend Windows Server 2025, 2022, or 2019 as the preferred server OS, running on a virtual machine.

- **Supported Operating Systems**
  - Windows Server 2025
  - Windows Server 2022
  - Windows Server 2019
- **Supported CPU**
  - 64-bit Intel or AMD x64 architecture
  - 4+ cores
- **Memory**

  8GB RAM minimum (16 GB or more is preferred)
- **Hard Disk Space**

  100 GB minimum, preferably SSD. This assumes back end file storage is not located on the Triofox server itself.

### EC2 Server Type

> If you are installing Triofox in Amazon Web Service (AWS), here is the minimum AWS EC2 instance types we recommend for production use.

- t2.xlarge (general purpose, 4 vCPU, 16 GB)
- t3.xlarge (general purpose, 4 vCPU, 16 GB)

Please check the AWS EC2 Instance Types for more information.

### Azure Virtual Machine Size Recommendation

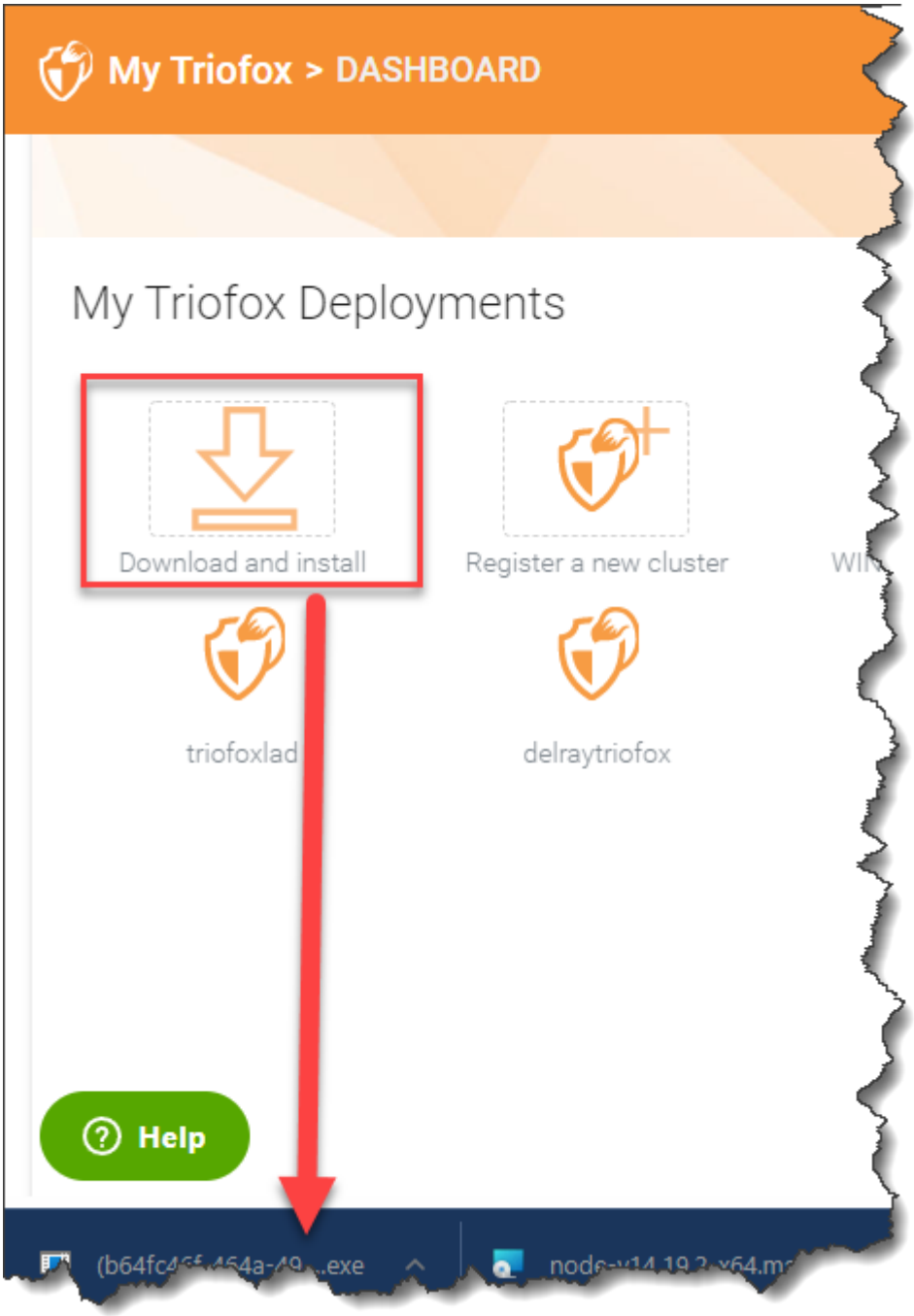
> If you are installing Triofox in Microsoft Windows Azure, here is the minimum Azure Virtual Machine size we recommend for production use.

- D4a V4 (4 vCPU 16GB)
- D4as V4 (4 vCPU 16GB)
- D4d V4 (4 vCPU 16GB)
- D4ds V4 (4 vCPU 16GB)
- D4 v4 (4 vCPU 16GB)

## Step 5: Start Installation

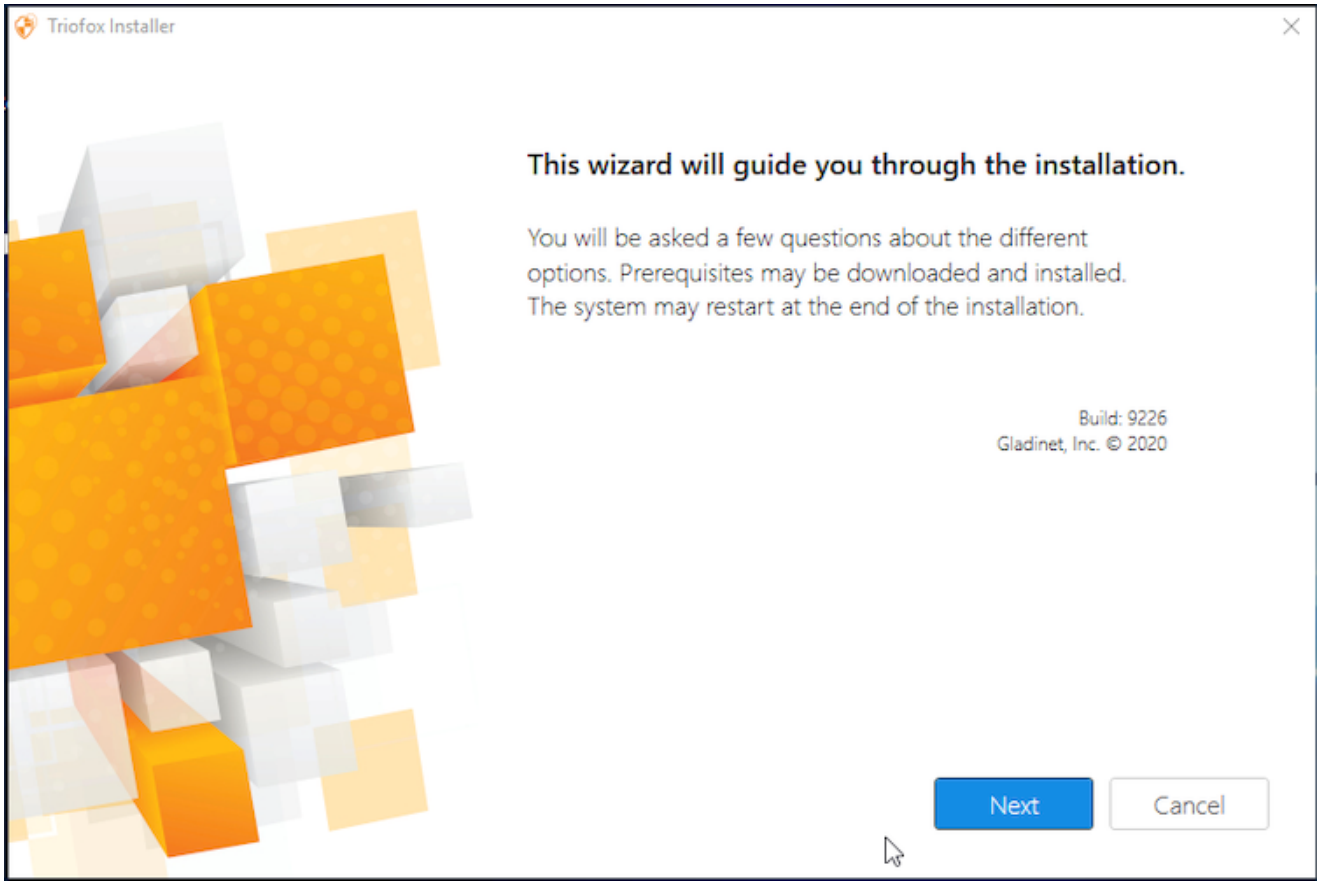
> We recommend download and install either the Google Chrome browser or the Microsoft Edge Browser (Chromium-based) and set the browser as the default browser before installation. We do NOT recommend using Microsoft Internet Explorer as the default browser for management tasks inside a web browser interface.

You can get the Triofox installation package from the Triofox customer portal (by login to https://www.triofox.com) and get to the Private Triofox section.



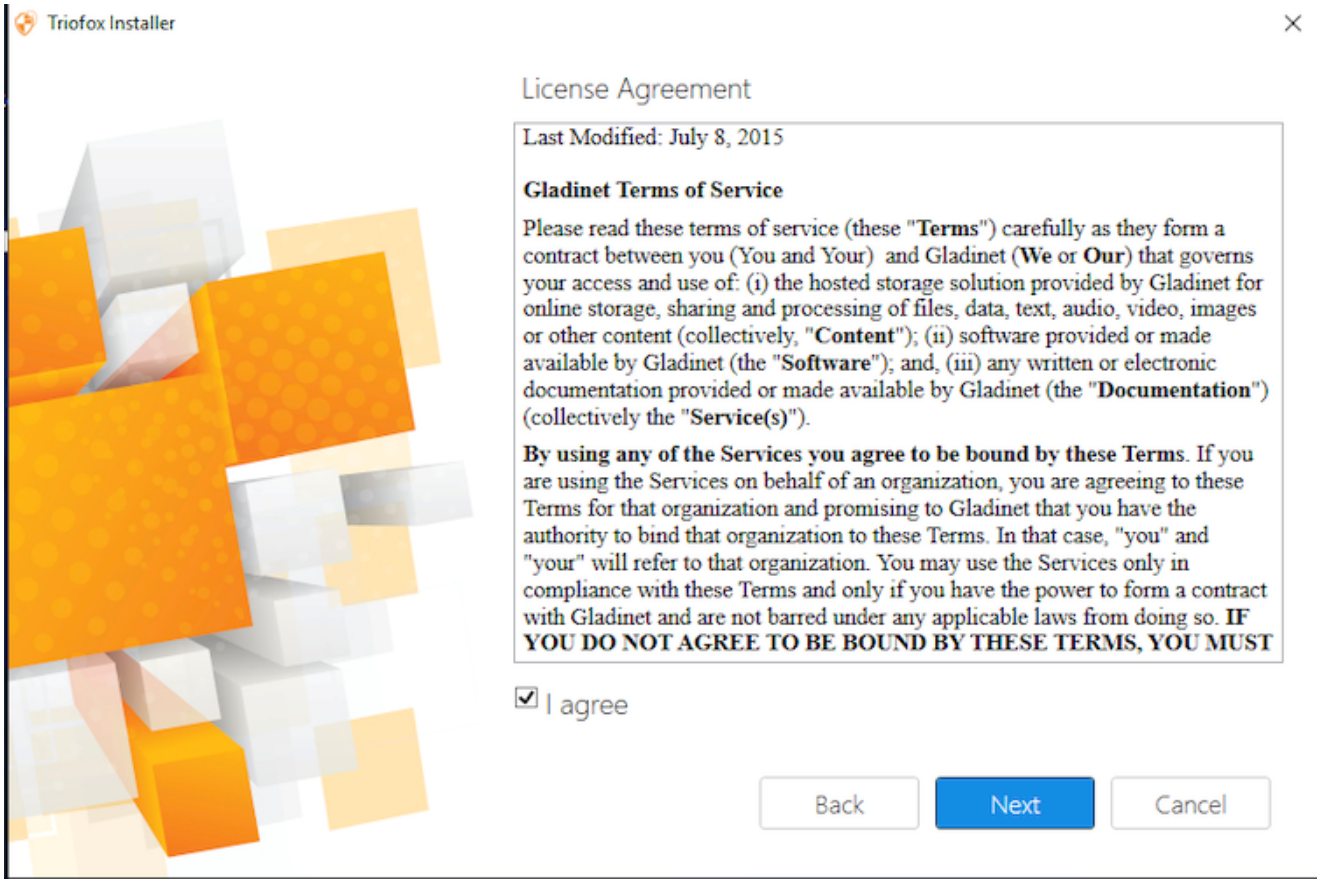

Log in to the Triofox server console (RDP or physical console are fine) with administrator privileges. Once you click on the "Download" button in the customer portal, the installer will appear either in the Downloads section or as a link at the bottom of your browser. Click the executable file to start the installation.

You will see the welcome screen.

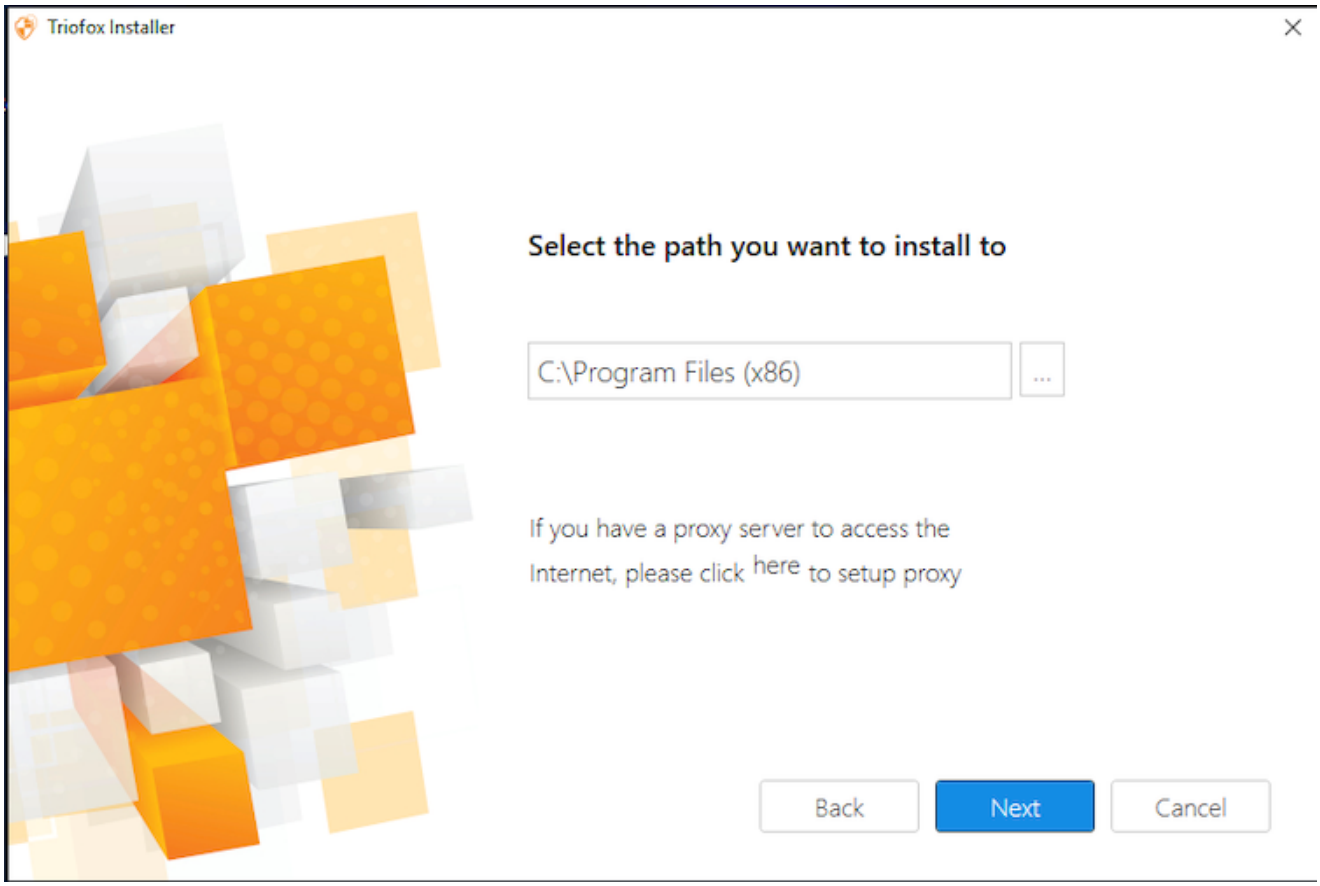



Click 'Next'

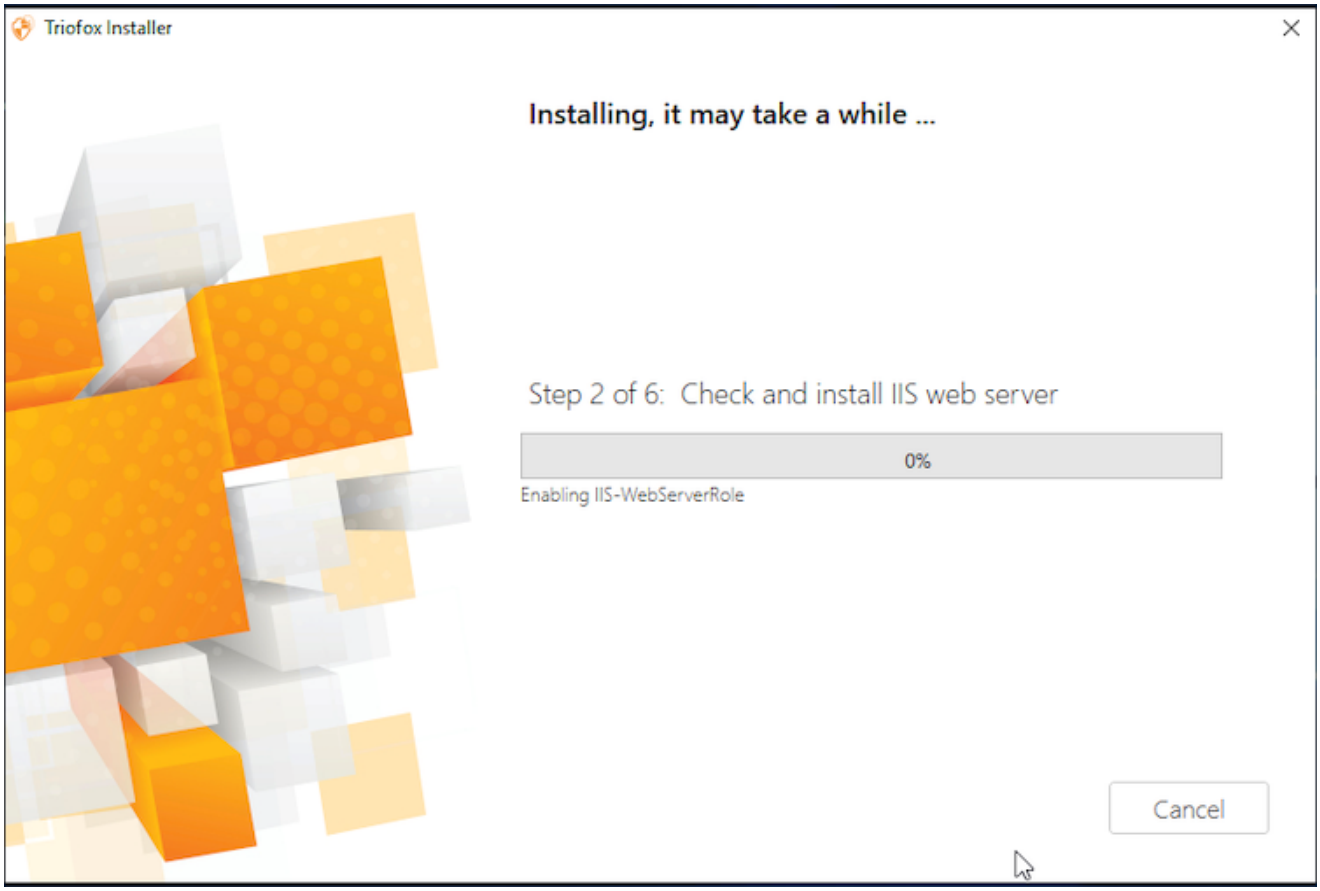
And accept the EULA and click Next.



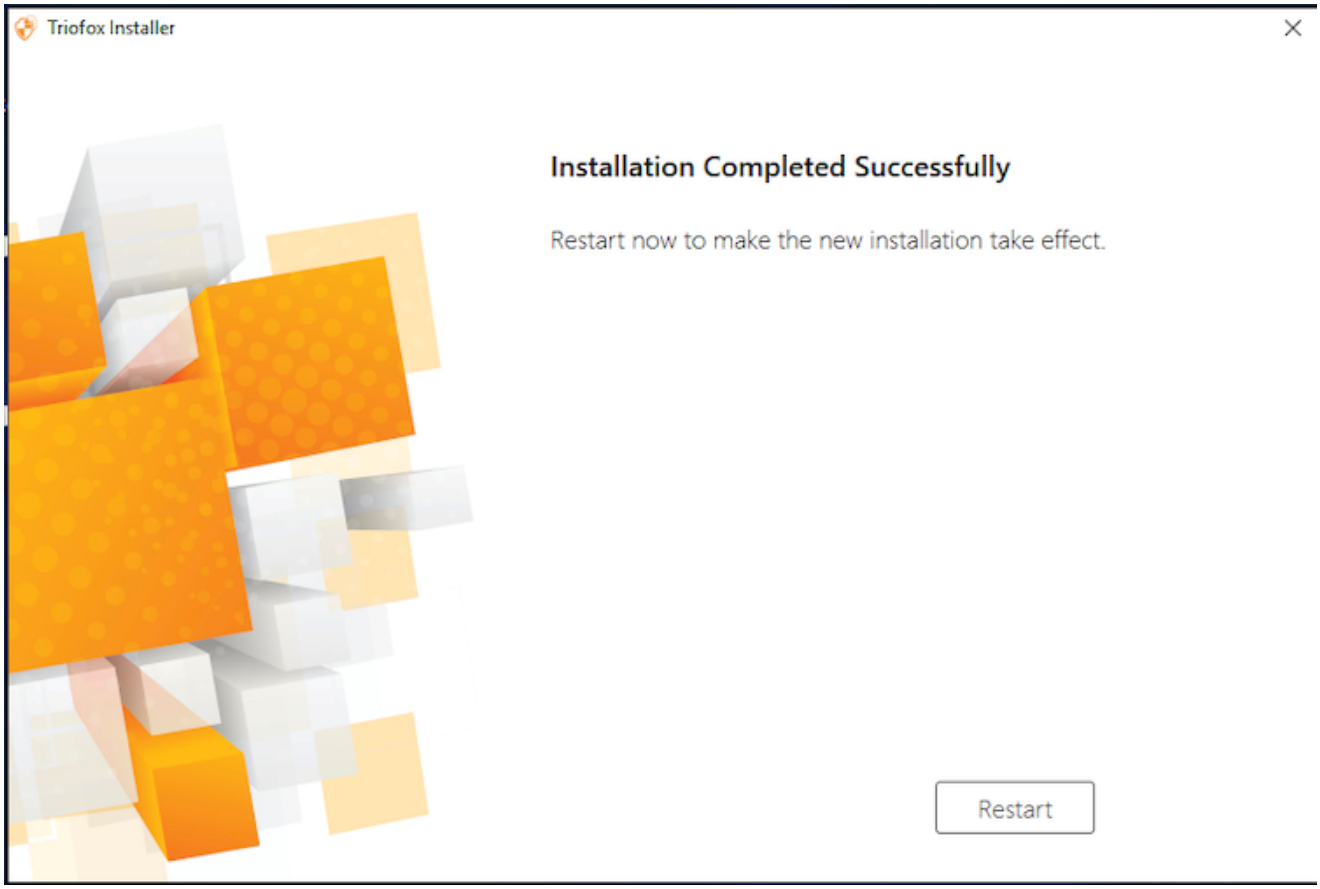
Select the path you wish to install Triofox to.




Then click Install.



Triofox will install and then you will need to restart your system to complete the installation.

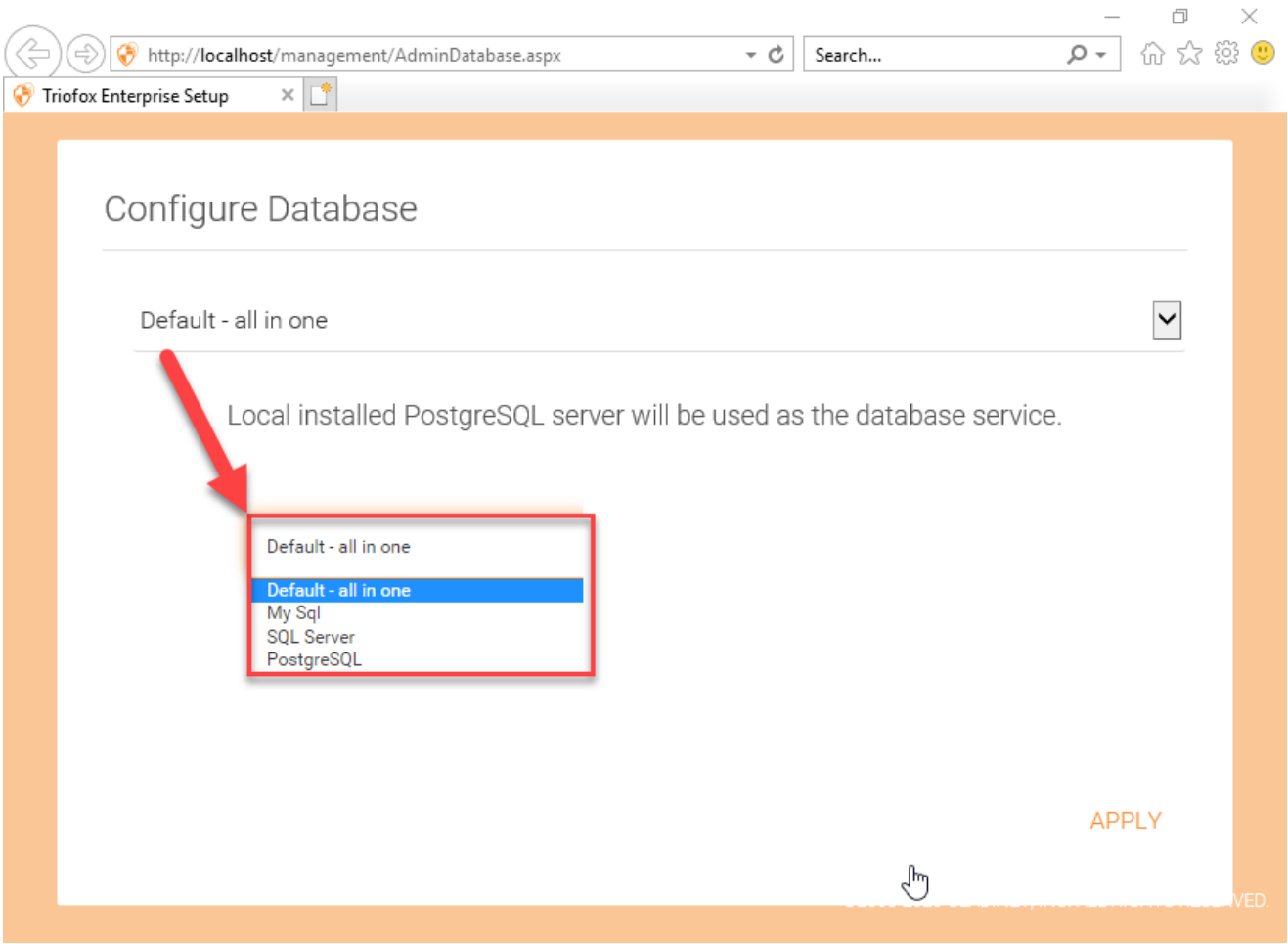



> After the installation, the server will need a reboot, a web browser will pop up for the **initial configuration**.

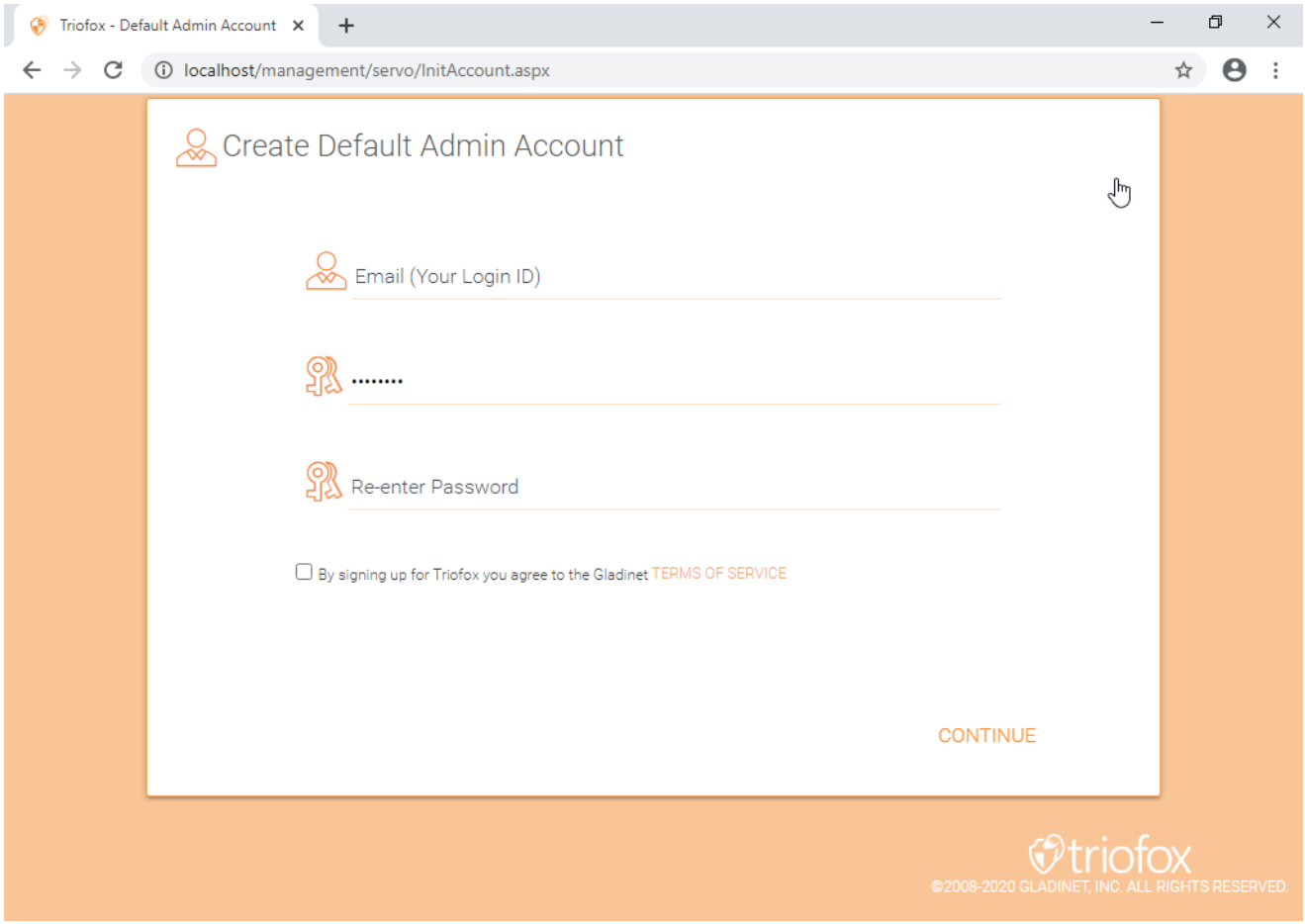
# Configuration

When your server restarts, it will configure Triofox in the background and launch a web browser with the next steps to set up your Triofox instance.

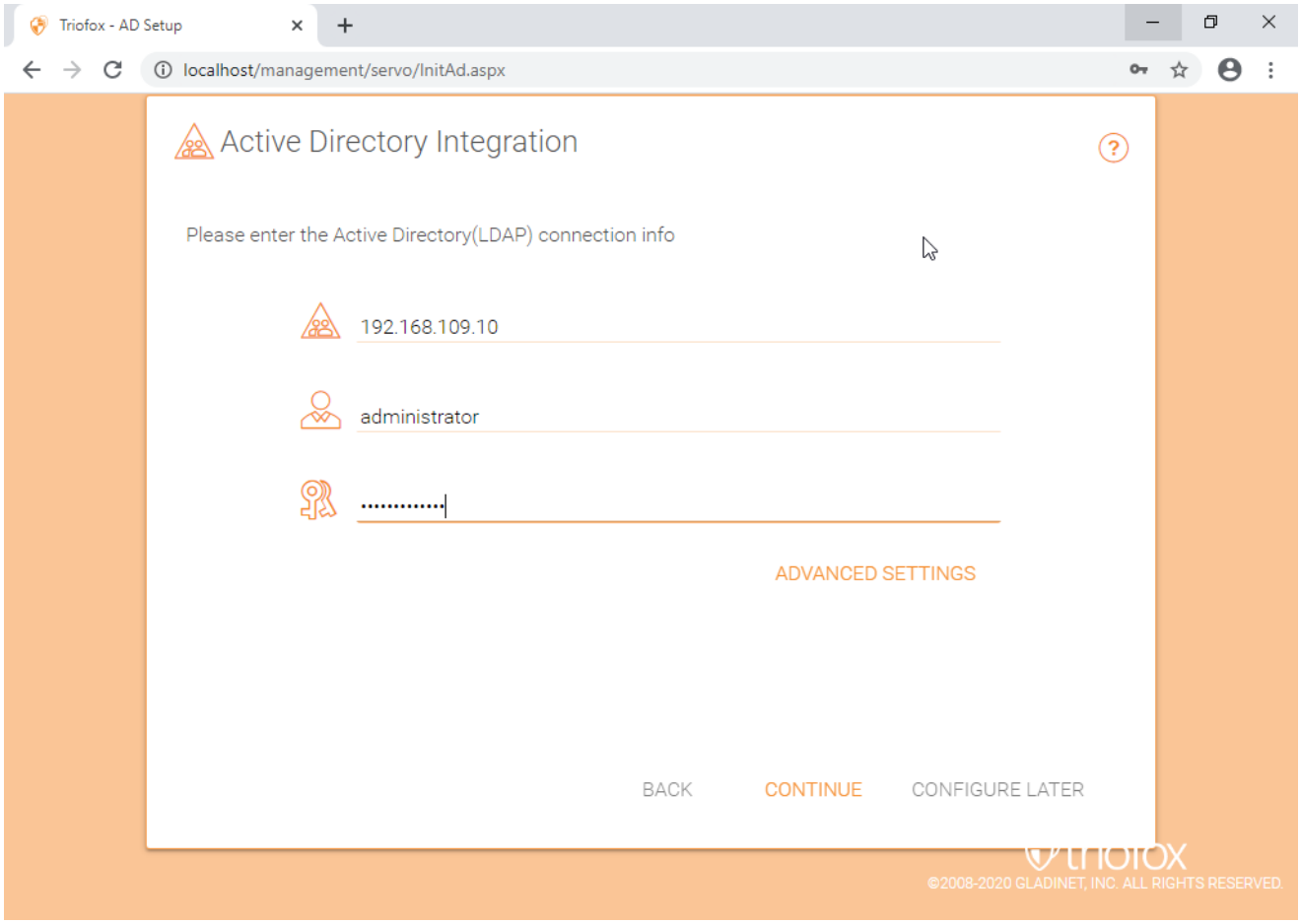
If you have an existing database, use the pull-down menu on the next screen to select a different option, otherwise use the default setting, which will also install the PostgreSQL database.



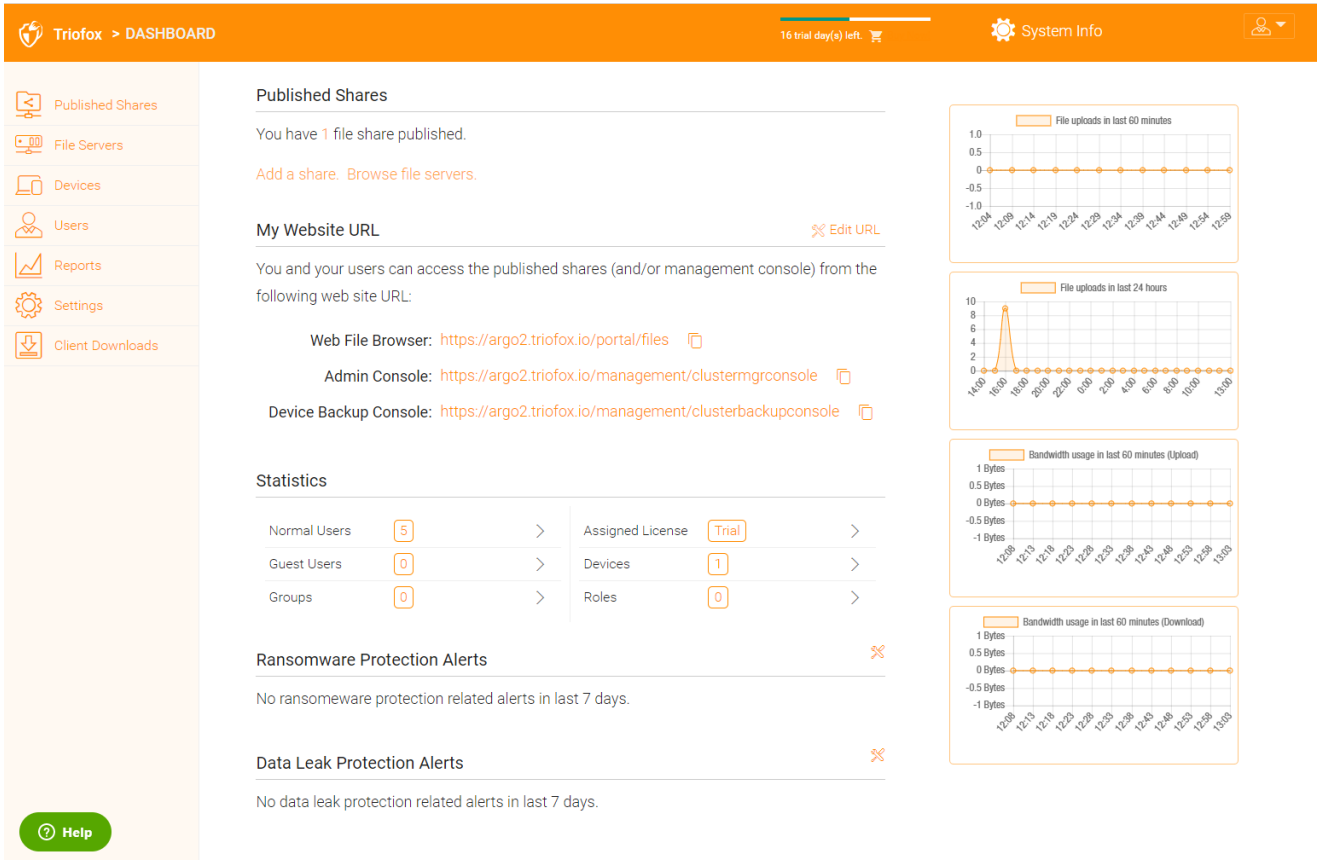

In the next screen, create the default administrator's credentials and click **CONTINUE**.



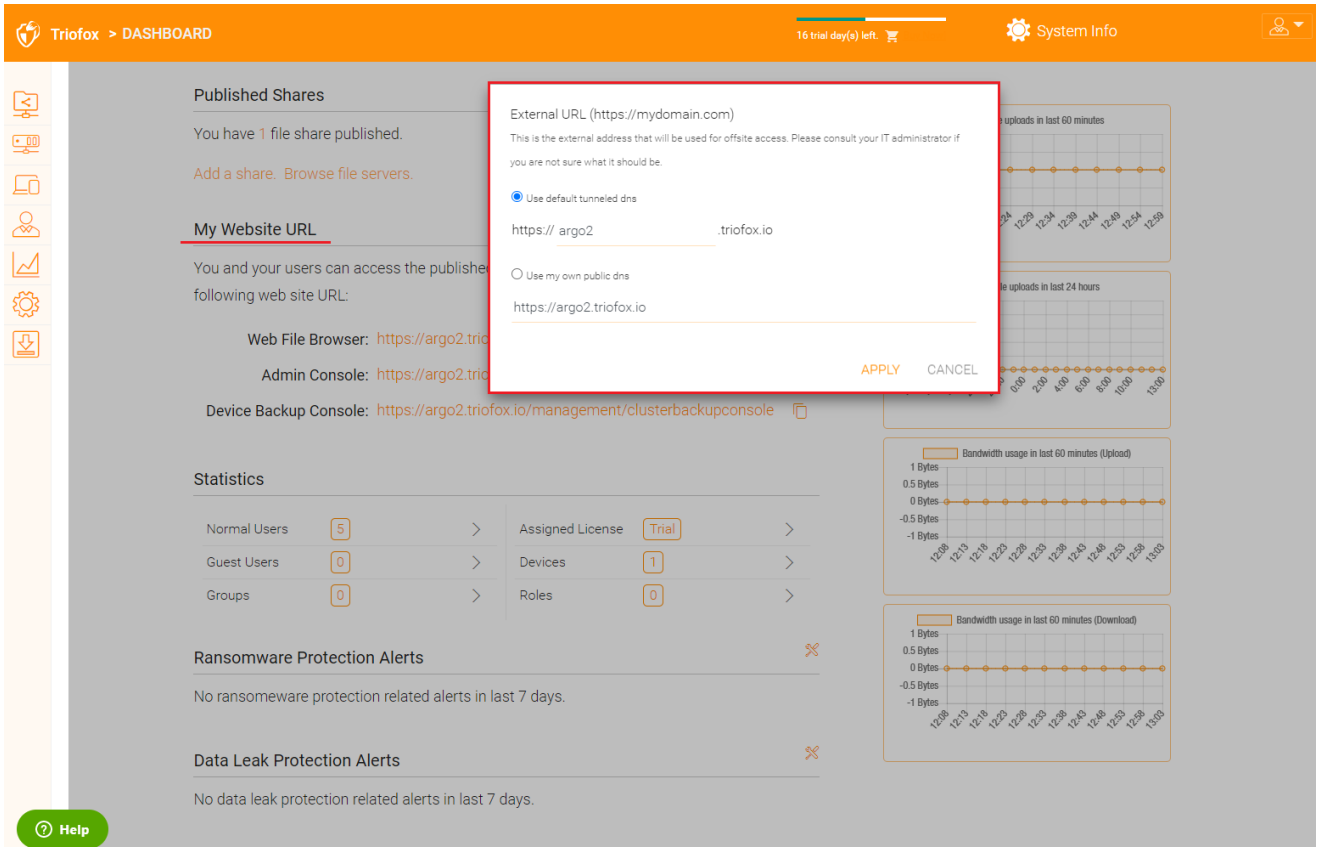

Then you will be able to enter your Active Directory information or opt to Configure Later.



You will then be taken to the Triofox Dashboard.




Once you see the dashboard, the Triofox side of the setup is finished successfully. We will continue to connect file server network shares and add users to the Triofox solution, and make sure all components are fully functional.



**External DNS is not configured for this Triofox server**. By default, an external DNS (secure https URL) is provided for you to use immediately to test functionality from the public Internet. This way, you do not need to install an SSL certificate on the Triofox server or open any ports in the firewall. This is good for testing or if you have no way to secure your own SSL certificate or open ports on your firewall. We recommend that you purchase your own SSL certificate and public DNS name if you want to have a branded URL showing your own corporate domain. If you already have a wildcard SSL certificate, you can also use it for the Triofox server.

# Enable SSL

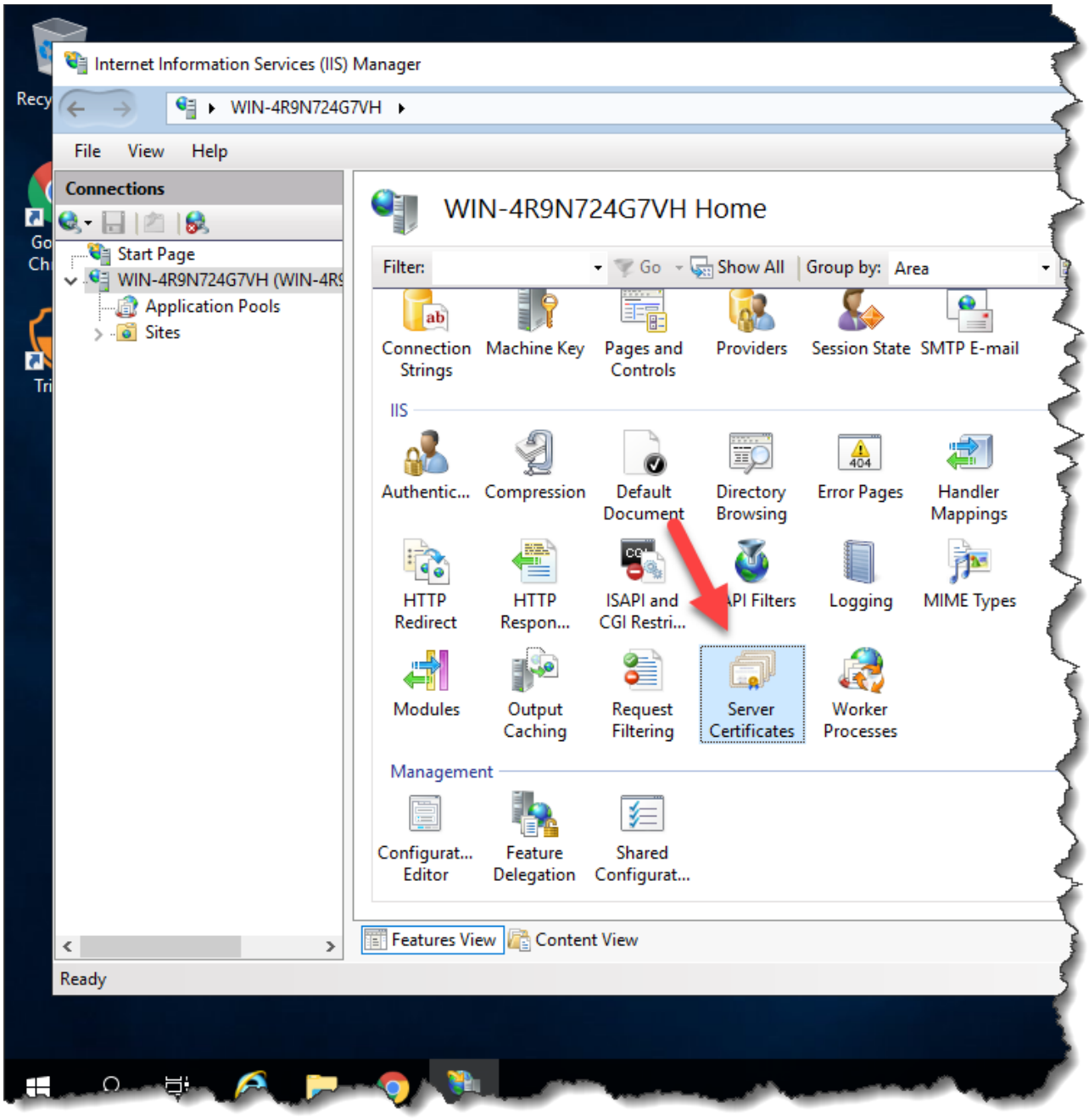
## Install SSL Certificate

> We assume that you have already set up your external Domain Name Service (DNS) to point to a DNS name of the Triofox server and that you have already purchased the SSL certificate with this DNS name. If not, you can acquire an SSL certificate from your SSL provider.

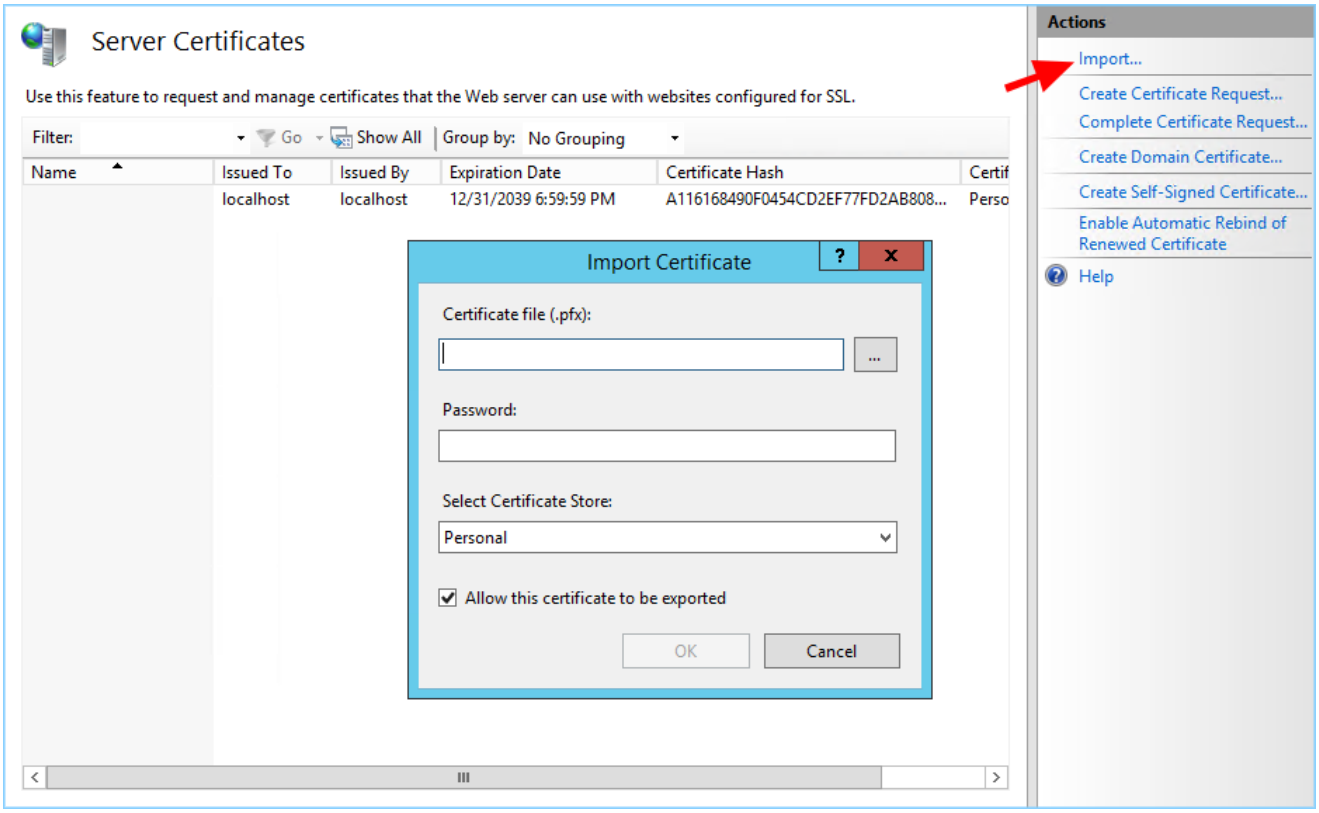
> We also recommend that you use https://www.ssllabs.com/ to test your SSL setup. The SSL Labs website generates a report on whether the SSL certificate you installed on the Triofox server is compatible with all devices, including mobile devices such as iOS or Android.

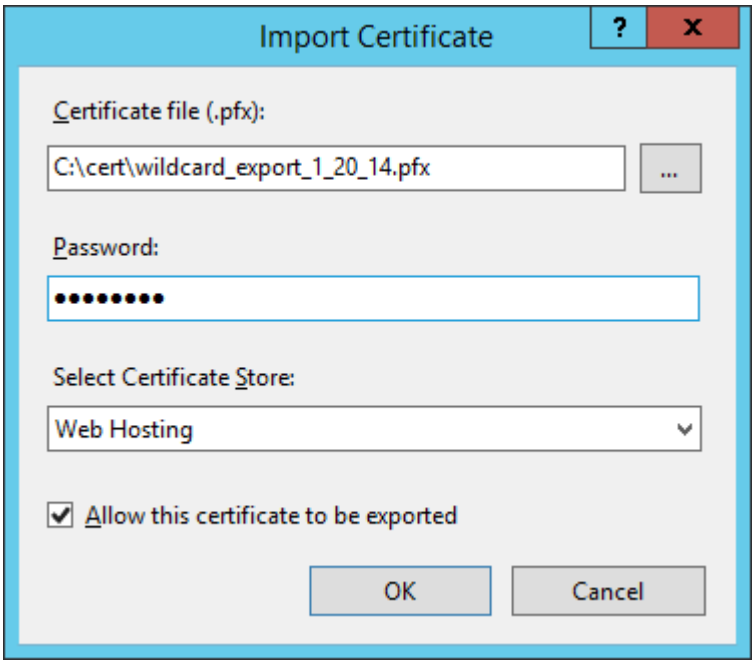
> You can also use openssl to check the SSL certificates and see if the entire certificate trust chain is fully installed on the server side. `openssl s_client -connect server.yourwebhoster.com:443`

You install the SSL certificate via the IIS Manager. Search for "Server Certificates" and double-click it.



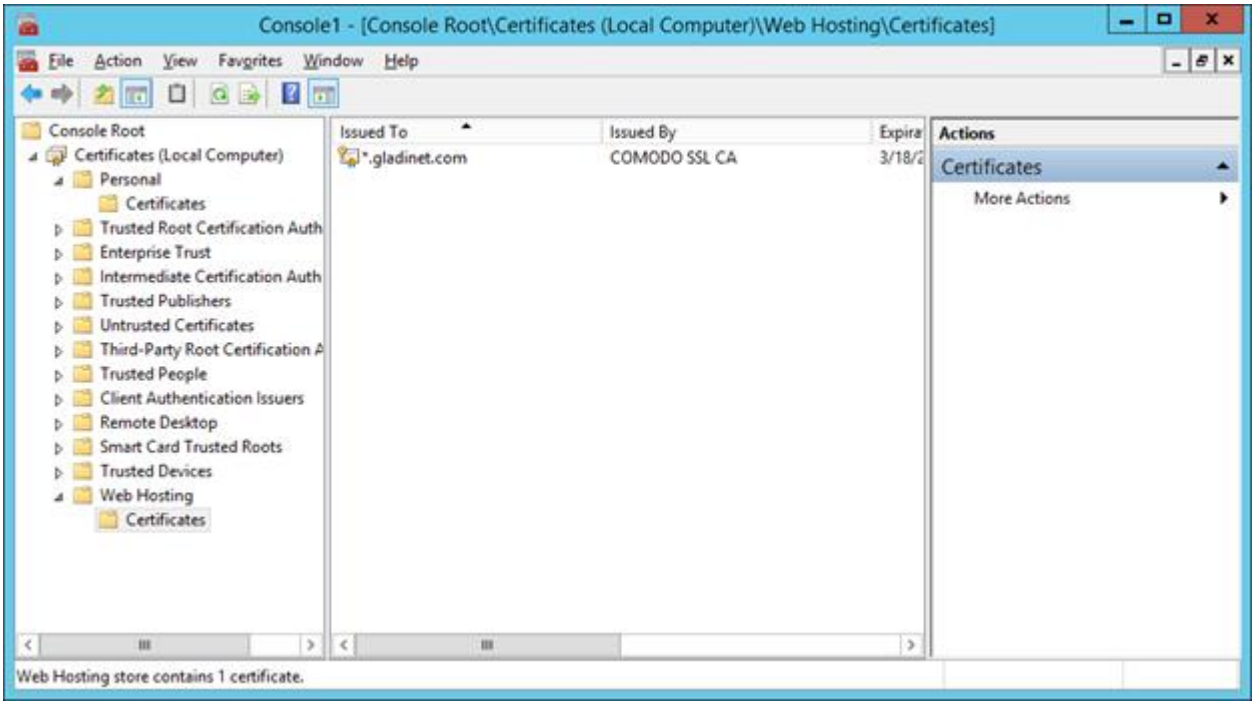

Click "Import" to import an existing SSL certificate. Leave the "Certificate Store" set to "Personal" or "Web Hosting", either is fine.



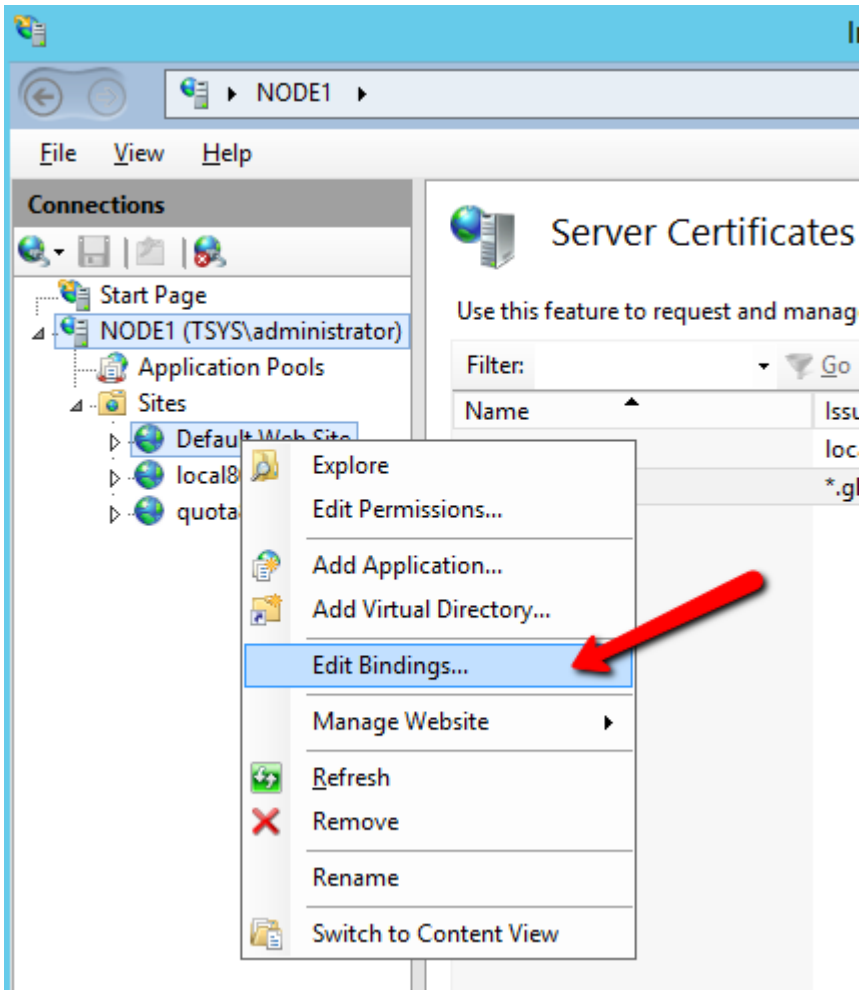




Verify that the certificate is available:

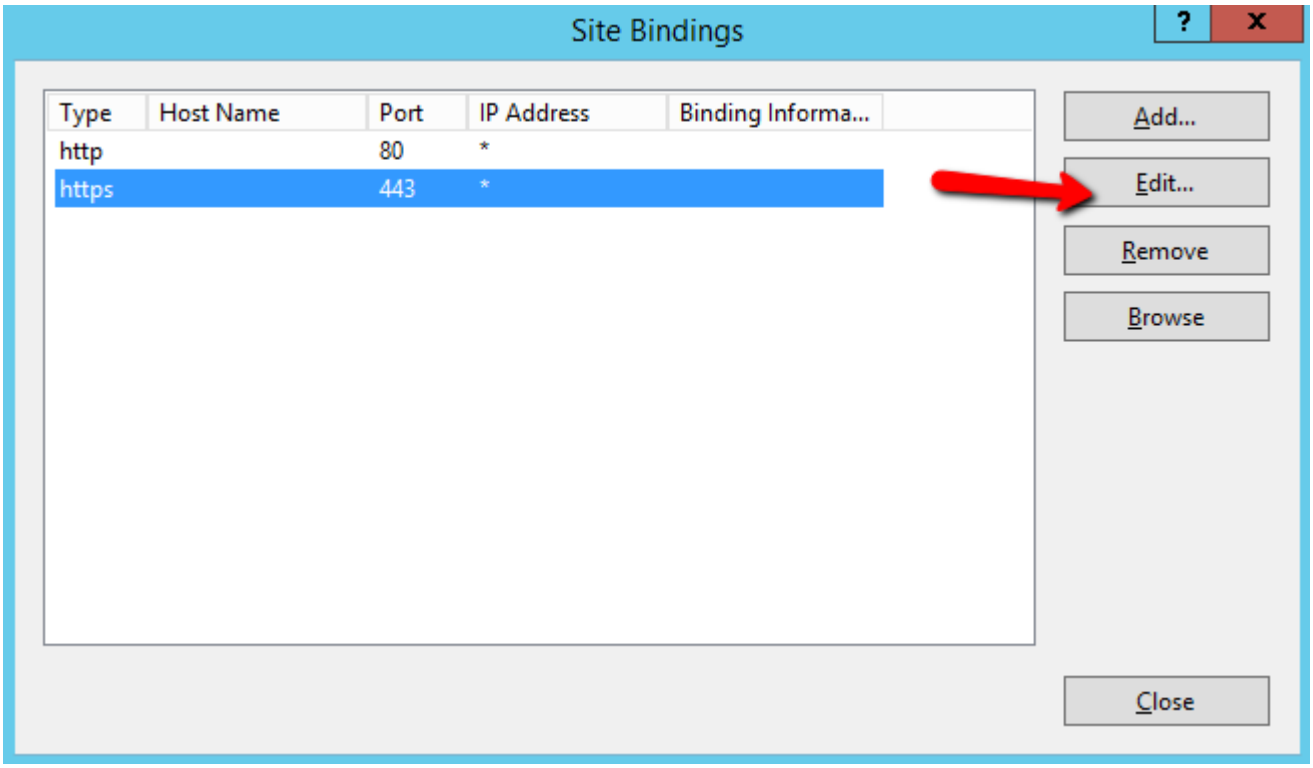
You can also verify the SSL certificate from the MMC/Certificates snap-in (Local Computer).



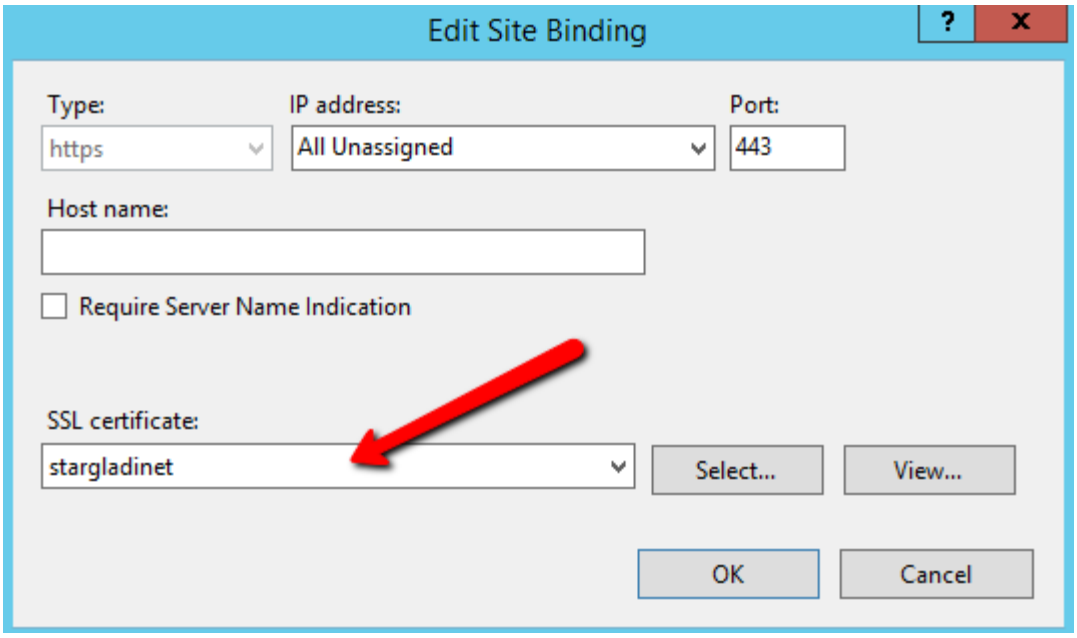

Now you can bind the "Default Web Site" to the SSL certificate for HTTPS. Right click on the "Default Web Site" and select "Edit Bindings".



In the Site Bindings dialog, edit the HTTPS binding.

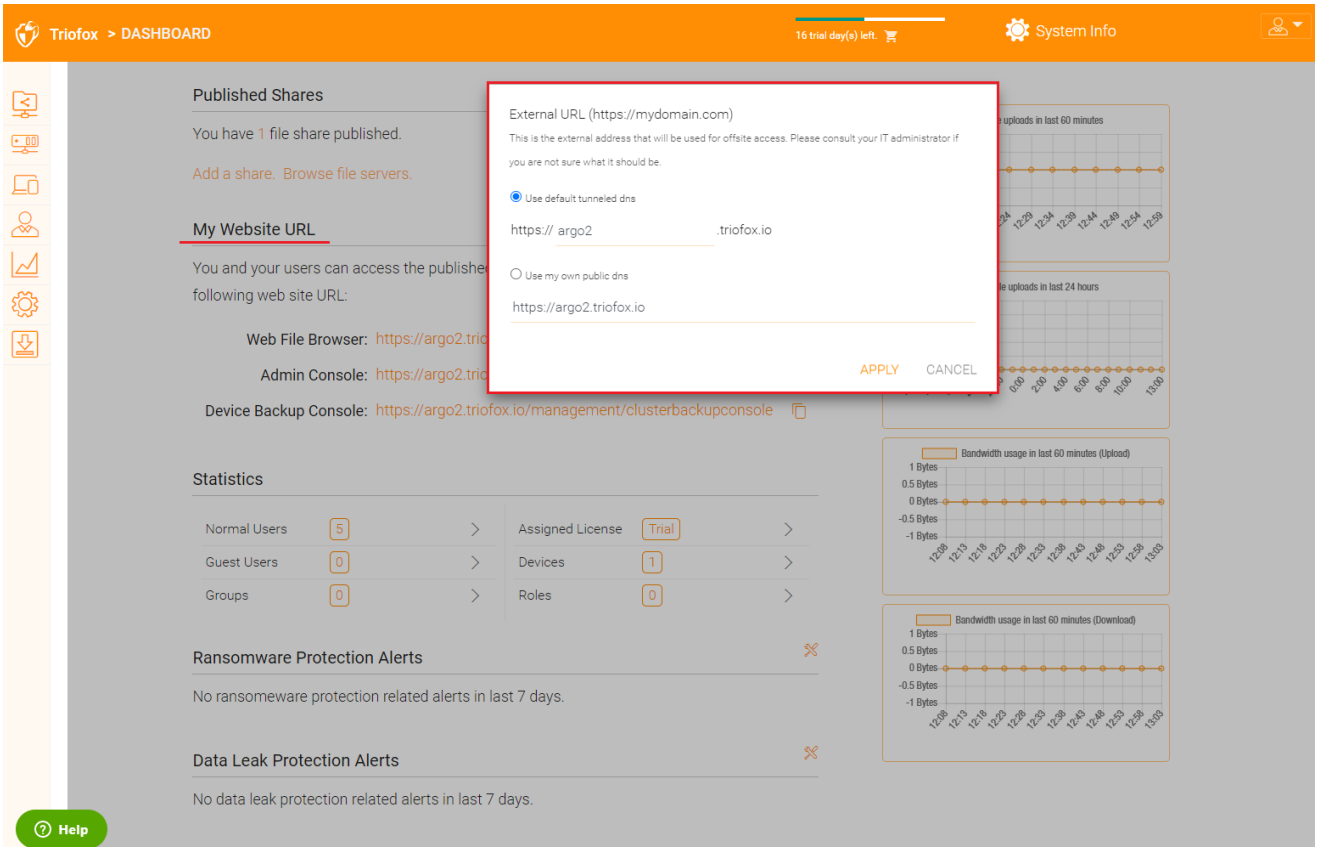



Now change the "SSL certificate" binding drop-down list to the imported SSL certificate.

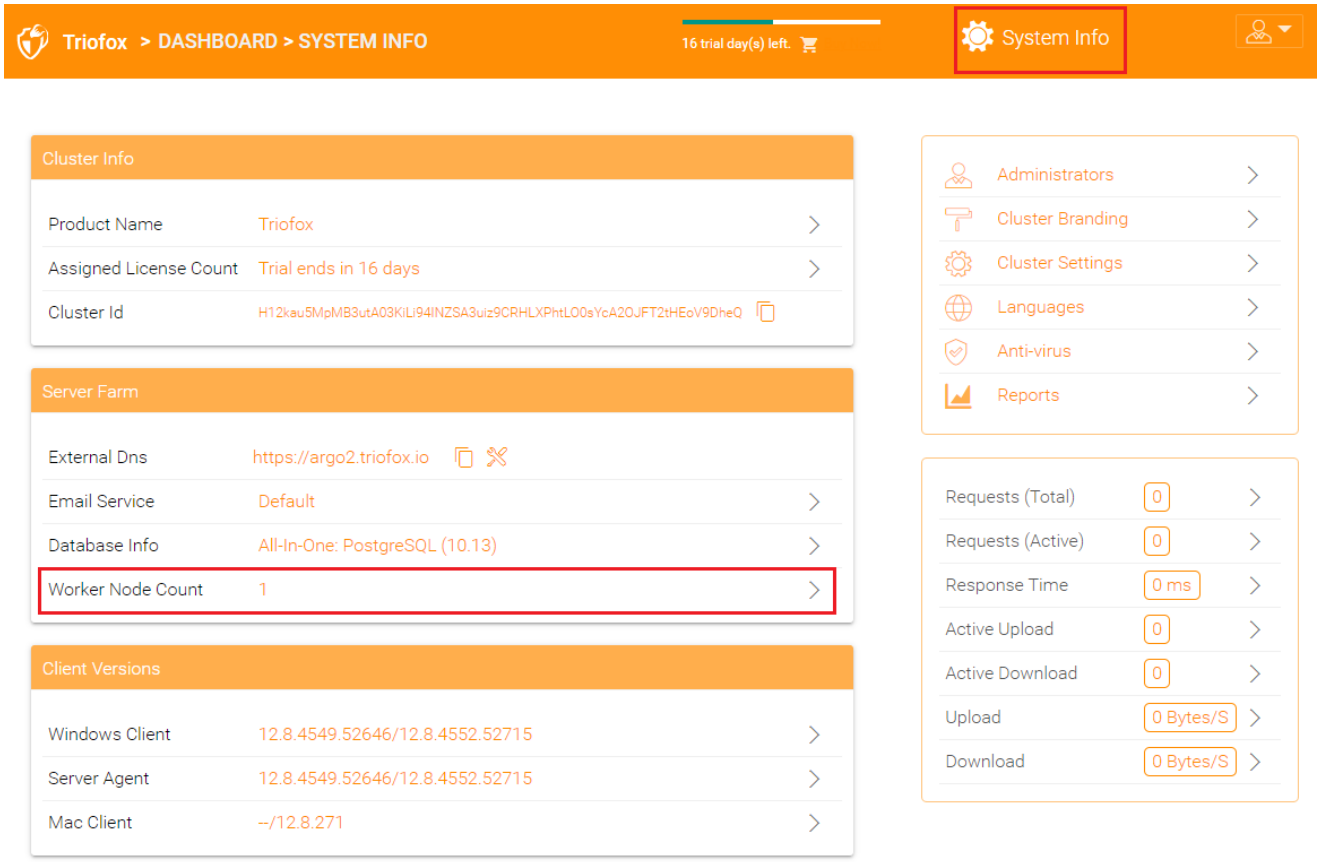


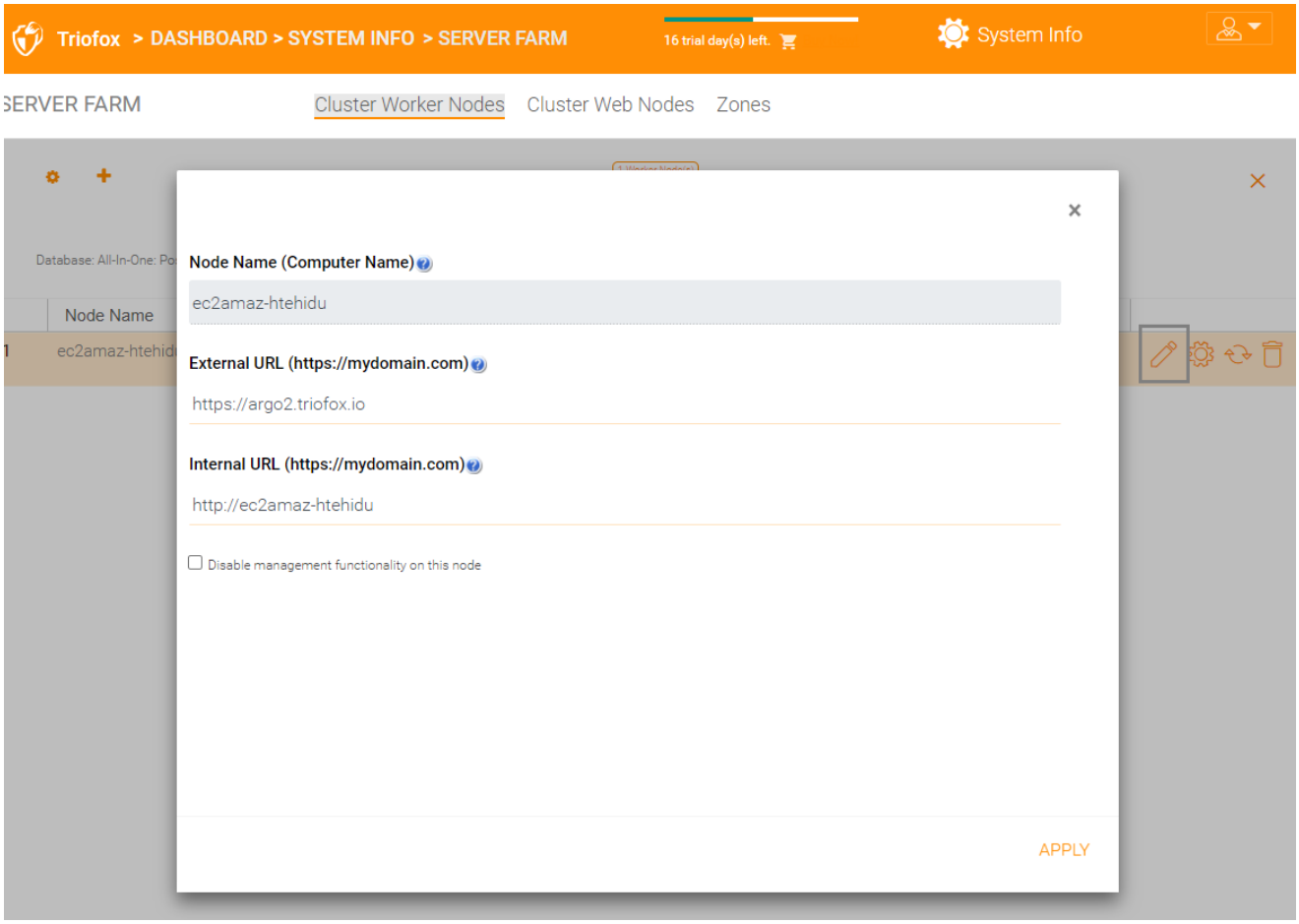

## External URL

Now we can go back to the **Dashboard** and **Edit URL** to configure the external URL for the Triofox server.




For specific settings regarding the Worker Nodes, go to **System Info** at the top and then access the **Worker Node Count**.






- **Node Name**

This corresponds to the host name of the triofox server. This doesn't need to be changed.

- **External URL**

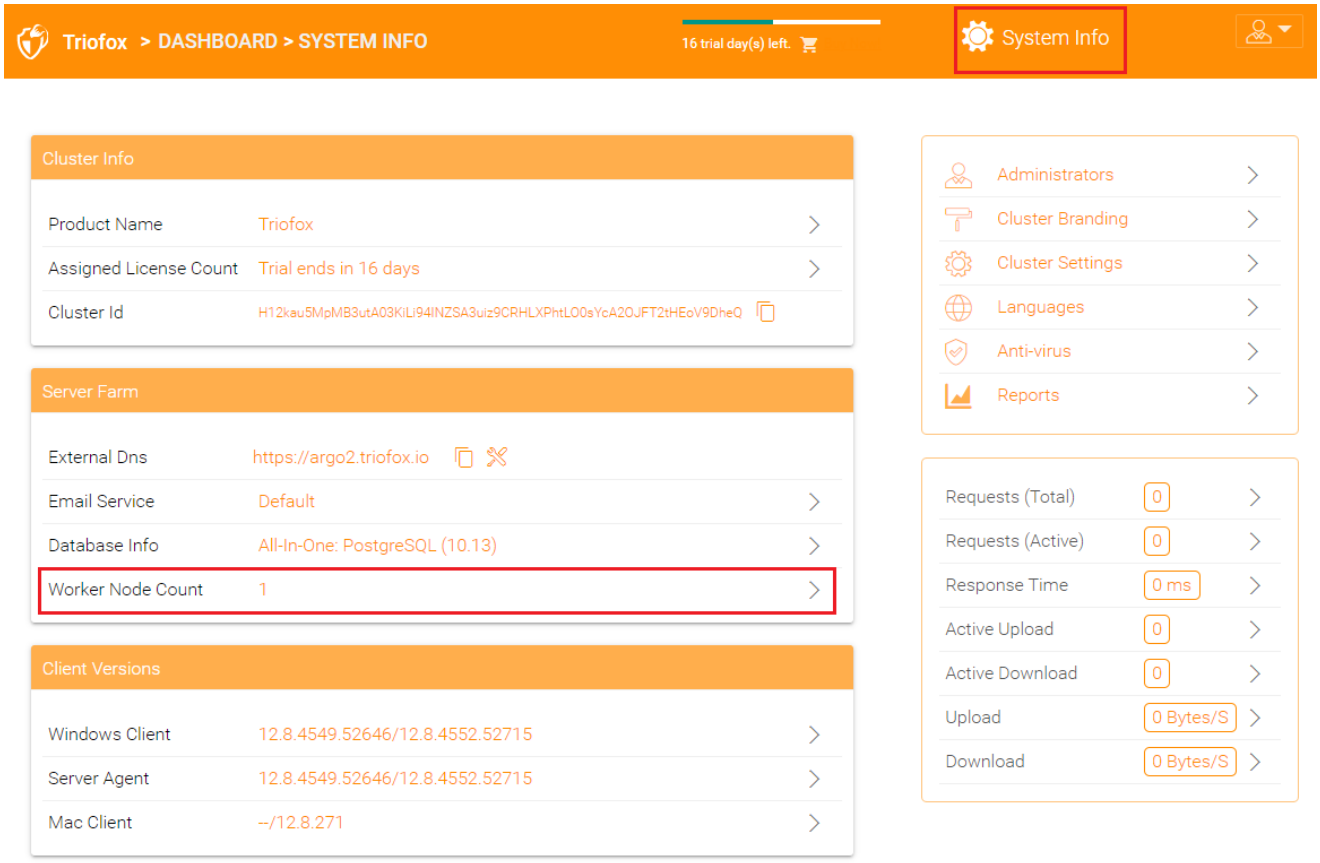
This is the external URL/DNS name that needs to be configured.

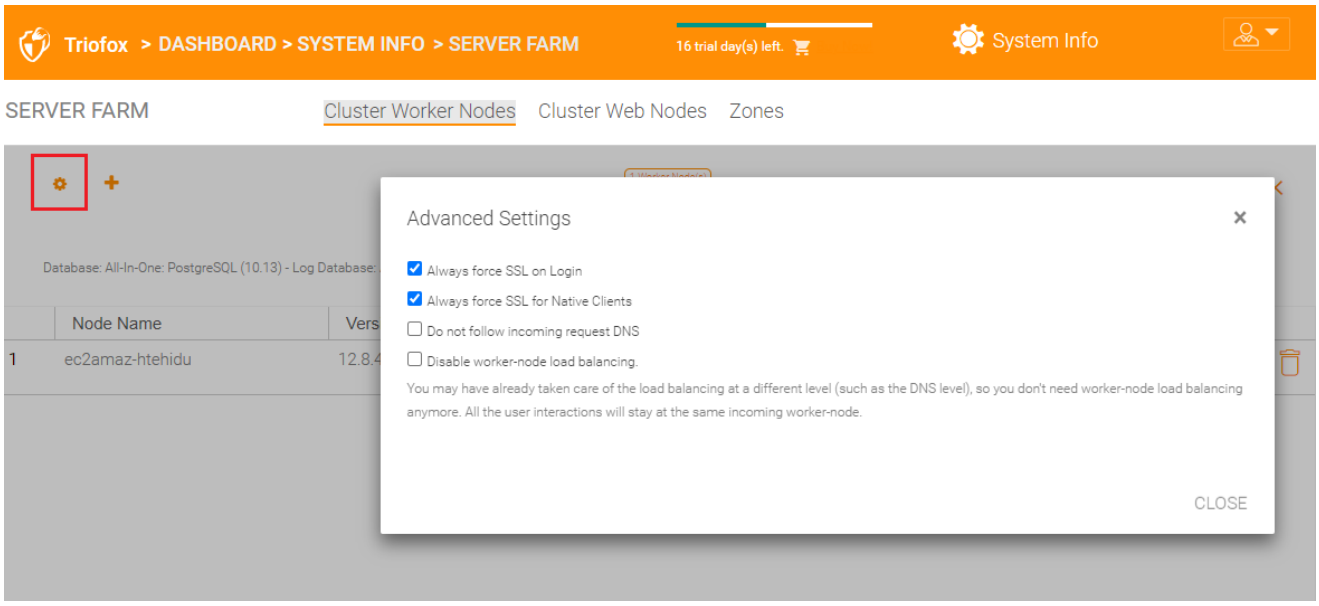
- **Internal URL**

This doesn't need to be changed.

# Setup Worker Node for SSL

Log in to the Web Portal as an administrator and select **System Info** at the top. You can then click **Worker Node Count** to view **Advanced Settings** for the Cluster.



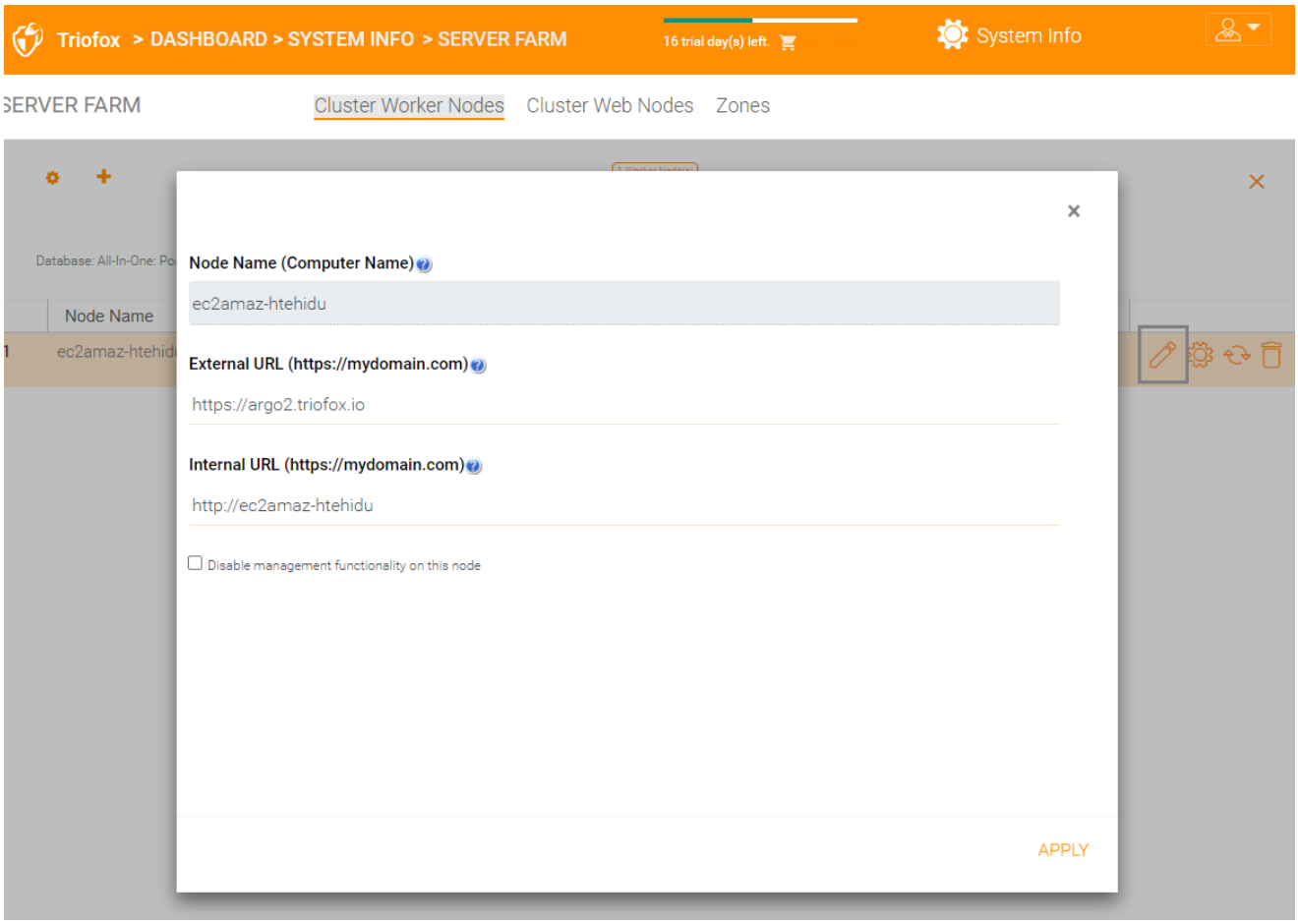




Now select **"Always force SSL on Login"** and **"Always force SSL for Native Clients"** checkboxes.

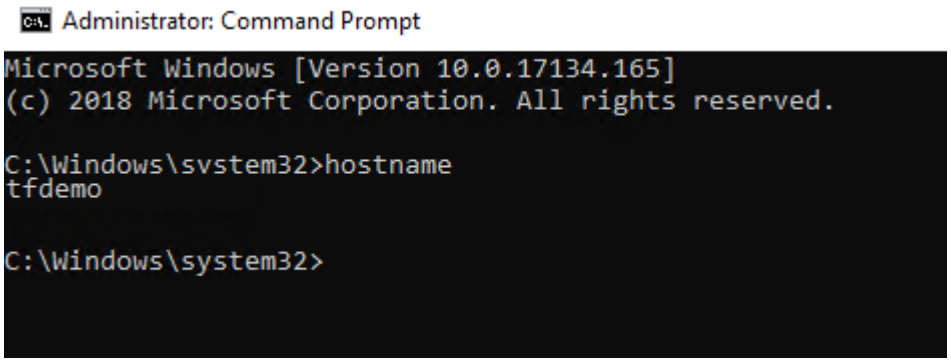
> If you are using the self-signed SSL certificate, the web portal is the only client that allows you to log in after some SSL certificate warning. All other native clients, such as Windows, mobile, and Mac clients, reject the connection.

> If you have a load balancer in the front of the triofox server and offload SSL to the load balancer. You will not need to check the 'Always force SSL' checkbox. Otherwise, the connection may fail because SSL is already offloaded to the load balancer.

You can also change the properties of the node.




The Node Name needs to match the hostname of the node.




The External URL shall match the external URL for HTTPS. (If you do not have SSL certificate installed yet, this can be HTTP for now).

The Internal URL will need to match the internal IP address or node's private DNS name and the HTTP or HTTPS protocol.

# Verify External URL, Internal URL and the Node Name

## Verify External URL

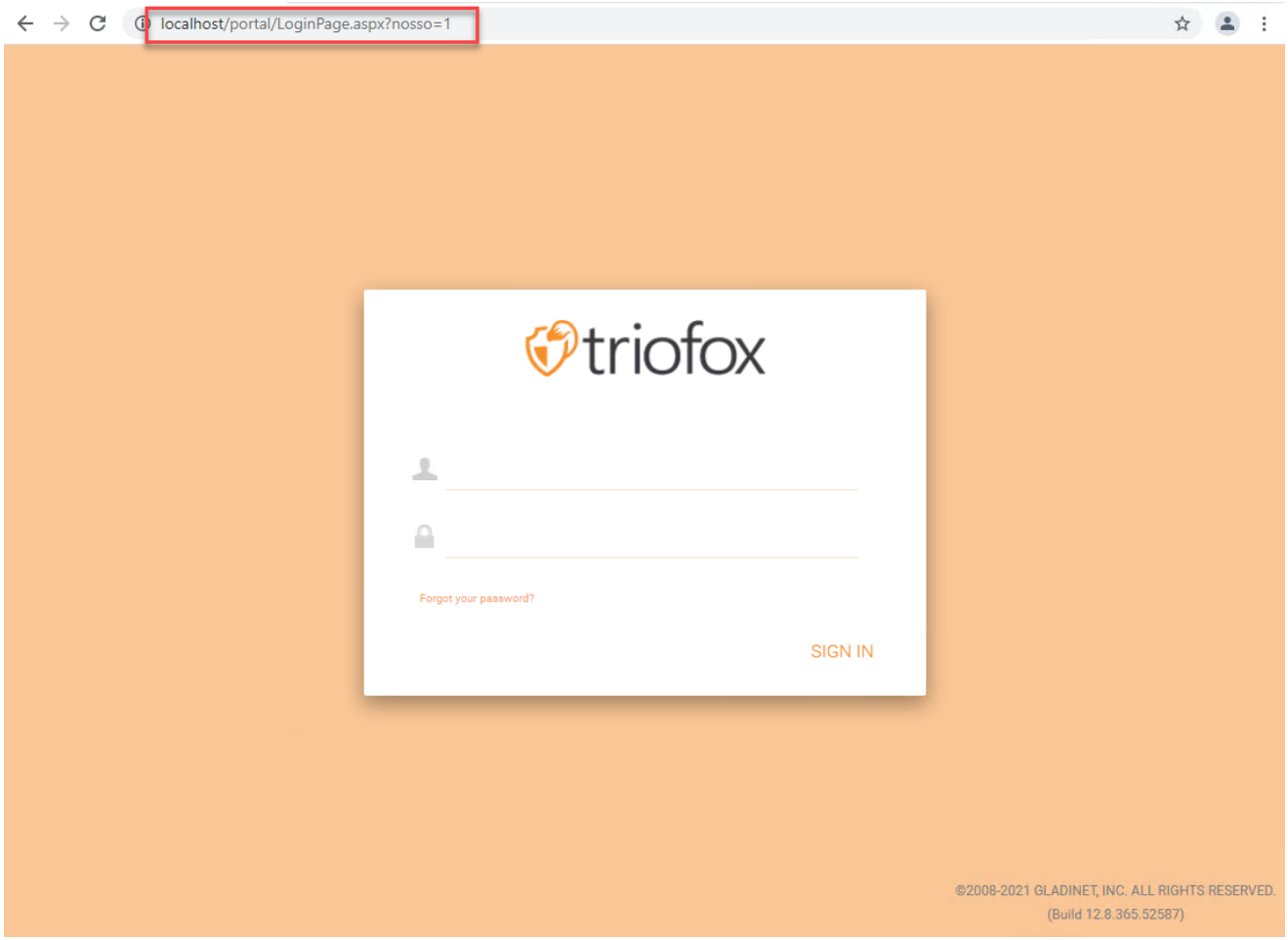
It is very easy to check if your external URL is set correctly. You just need to point your web browser to the external URL and check that the Login Page is displayed, and no SSL warnings appear.

You can also verify the external URL by performing a file share to your own email address outside of the Triofox system. A file sharing invitation will be sent to that email address. After you receive the email, click the link in the email and verify that the link points to the external URL.

> The external URL is used in the email sharing template. So with a simple file sharing test, you can verify that the external URL is set up correctly.

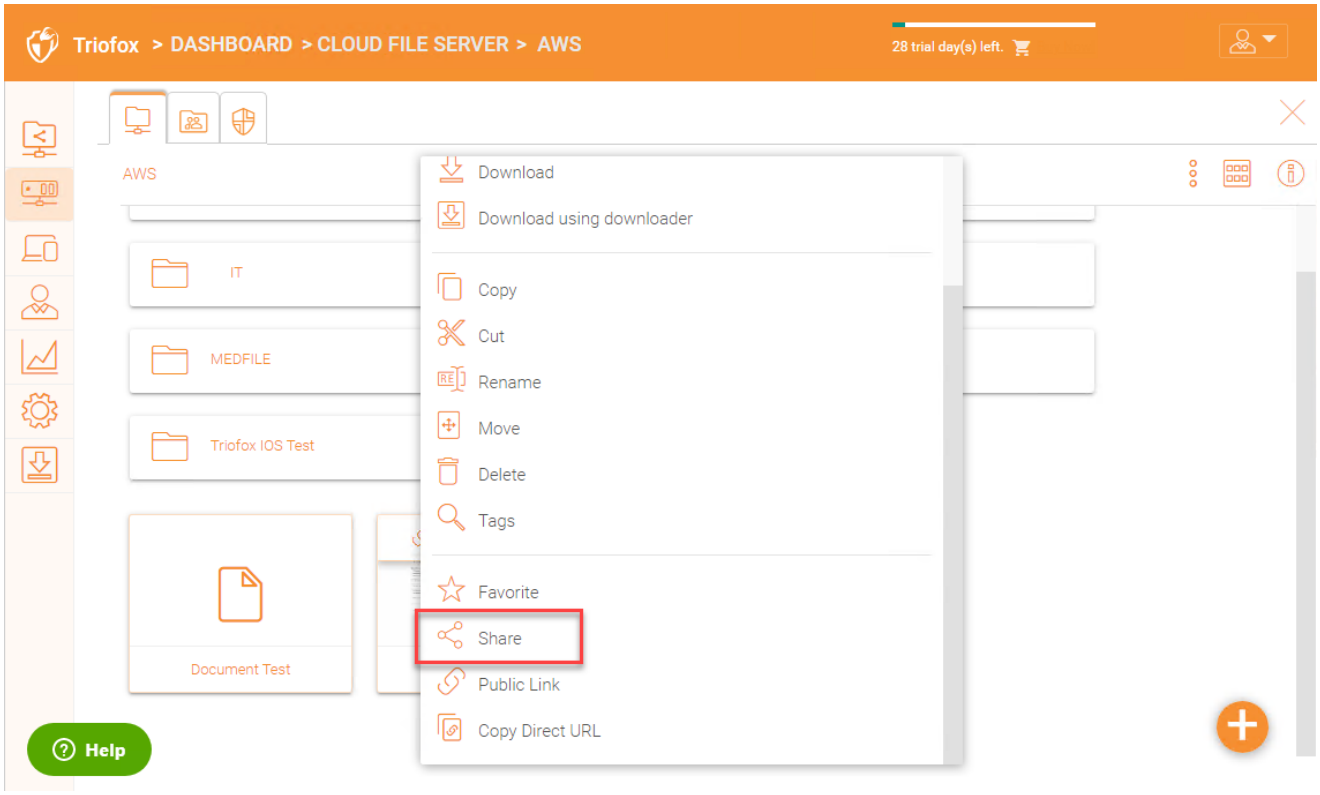
## Verify Internal URL

To check the internal URL, you can access the address on a computer connected to the same network using your web browser.




## Verify Node Name

To verify that the node name is correct, you can right-click on a folder and use the **"Share"** option to verify that the email was received and correctly points to an external URL.


Triofox > DASHBOARD > CLOUD FILE SERVER > AWS
28 trial day(s) left.
AWS
IT
MEDFILE
Triofox IOS Test
Document Test
Download
Download using downloader
Copy
Cut
Rename
Move
Delete
Tags
Favorite
Share
Public Link
Copy Direct URL
Help

# Add additional Triofox servers to the cluster

Adding an additional Triofox server is as easy as installing the first Triofox server. Run the Triofox server installer on another server, specifying the same database as the first server in the server farm.

> Adding more Triofox servers to an existing server farm is optional.

> If you only have a few hundred users, you do not need a second node from a scalability perspective. The scaling point for adding a second Triofox server is 1000 users. It is always best to scale vertically first, e.g. by turning a 2 CPU machine into a 4 CPU machine and adding RAM to the Triofox server, before scaling horizontally by adding more Triofox servers.

> However, from a high availability point of view (HA), it may make sense to use a second Triofox Server.

> In the user interface, if you see cluster, it means the server farm

If you want to scale the cluster to more than one Triofox Server, you should use an external database server. The "all-in-one" deployment with a local PostgreSQL database is not intended for scaling or high availability.

A hardware or software load balancer is required if more than one Triofox Server is deployed in a cluster.

All Triofox servers in the same cluster must use the same time zone.