

---

# **CentreStack Installation Guide Documentation**

***Release 12.5.9520.51622***

**Gladinet, Inc.**

**Apr 08, 2023**



---

## Contents

---

<b>1</b>	<b>1 Getting Started</b>	<b>3</b>
1.1	Introduction . . . . .	3
1.2	Overview . . . . .	3
1.3	System Components . . . . .	4
<b>2</b>	<b>Installation</b>	<b>7</b>
2.1	Step 1: Prepare the File Storage . . . . .	7
2.2	Step 2: Prepare Active Directory (Optional) . . . . .	8
2.3	Step 3: Prepare the Database Server . . . . .	8
2.4	Step 4: Prepare the CentreStack Server . . . . .	9
2.5	Step 5: Start Installation . . . . .	10
<b>3</b>	<b>3 Initial Configuration</b>	<b>15</b>
<b>4</b>	<b>Web Portal</b>	<b>17</b>
<b>5</b>	<b>Management Console</b>	<b>19</b>
5.1	Add Tenant . . . . .	20
5.2	Team Folders . . . . .	21
5.3	Storage Manager . . . . .	22
5.4	User Manager . . . . .	23
5.5	Delegate Administration . . . . .	24
5.6	Active Directory Integration (Optional) . . . . .	26
5.7	Group Policy . . . . .	27
5.8	Branding . . . . .	28
<b>6</b>	<b>Enable SSL – Install SSL Certificate</b>	<b>29</b>
<b>7</b>	<b>Setup Worker Node for SSL</b>	<b>35</b>
<b>8</b>	<b>8 Verify External URL, Internal URL and the Node Name</b>	<b>41</b>
8.1	Verify External URL . . . . .	41
8.2	Verify Internal URL . . . . .	41
8.3	Verify Node Name . . . . .	42
<b>9</b>	<b>9 Add additional CentreStack servers to the cluster</b>	<b>43</b>
<b>10</b>	<b>10 Branding</b>	<b>45</b>

10.1 Self-Service Branding . . . . .	45
<b>11 11 Upgrade CentreStack</b>	<b>47</b>
11.1 Using the GUI Installer to Upgrade . . . . .	47
<b>12 Advanced Topics</b>	<b>49</b>
12.1 Split Database . . . . .	49
12.2 Change Authentication Algorithm to Version 2 . . . . .	50
12.3 Change the Synchronized Uploader to Asynchronous Uploader . . . . .	50
12.4 Zone Support . . . . .	51
12.5 Scalability Tuning . . . . .	51
12.6 Need More Information? . . . . .	53
<b>13 Upgrade CentreStack</b>	<b>55</b>
13.1 Using the GUI Installer to Upgrade . . . . .	55
<b>14 Indices and tables</b>	<b>57</b>

Contents:



### 1.1 Introduction

Welcome to the CentreStack Server Installation Guide. This guide describes the installation tasks for CentreStack, the managed file synchronization and sharing solution.

CentreStack includes the CentreStack server, which runs on the Microsoft Windows server platform, and client agent applications for Web browsers, Microsoft Windows, Mac OS X, and for mobile platforms such as the Android and the Apple iOS operating systems.

### 1.2 Overview

CentreStack is a managed file sync and share solution that focuses on local file server cloud-enablement. It differentiates from other file sync and share solutions (EFSS) by focusing on the security, control, file server and team collaboration. CentreStack does really well in the following areas:

1. maintain security by migrating files and folders while keeping the NTFS permissions intact.
2. provide on-demand access that honors read-only and write permission in real-time.
3. mirror local network shares on file servers to allow for team collaboration in the cloud.
4. provide virtual drive letter mapping to the files and folders for access.
5. provide file locking, version control, client encryption, and more advanced features for managing all virtual drives.

CentreStack Server is a software built on top of the Microsoft Web Platform:

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

- PostgreSQL, MySQL or SQL Server

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

It provides file access and sharing functionality through client agents for PCs, Macs, File Servers, Web Browsers, and Mobile Devices. The client agent software on Windows and Mac provides real drive mapping and volume mounting support that contains advanced optimization for WAN(Wide Area Network) data transfer.

The services can be deployed in flexible combinations to meet different needs. There are two primary ways to deploy the CentreStack Server:

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

See also:

[File Server Remote Access](#)

2. Deploy in a site remotely, such as Amazon Web Services EC2, Microsoft Azure, or in a Data Center where the Managed Service Provider (MSP) hosts their infrastructure:

## 1.3 System Components

There are three different system components (logical components that can co-exist in the same server) in the CentreStack server. In the smallest deployment unit, the three different components can co-exist in one single machine (all-in-one deployment).

### 1.3.1 1. Web Server Component - The CentreStack Server

The Web Server component is ASP.NET and WFC code that is hosted by IIS on a Windows Server. The Web Server component is actually comprised of two separate “sub-components”:

- Web Node
- Worker Node

These sub-components exist for historical purposes and there are still elements in the Cluster Manager user interface for configuring these sub-components.

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

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

CentreStack supports the MySQL and Microsoft SQL Server Database Management Systems (DMBS). The all-in-one deployment will deploy MySQL Community Edition on the CentreStack server. The all-in-one deployment is useful for evaluating the software but an external database server is recommended for Production deployments.



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

The back-end file storage component is the persistent storage location for files and folders. There are two different types of storage services. One is managed by CentreStack, such as the default storage for the cluster and the default storage for tenants. The other is imported storage, for example, existing file server network shares that weren't managed by CentreStack but can be imported to CentreStack for remote and mobile access.



**Warning:** If this is the very first time you are installing CentreStack server, it is recommended that you do the all-in-one installation by preparing a clean Windows 2022/2019/2016 virtual machine and installing with all the default parameters. The All-in-one deployment is the smallest fully functional setup and can be used for production environment with < 1000 users.

## 2.1 Step 1: Prepare the File Storage

CentreStack server is about to cloudify your file storage and enable remote and mobile access, with sync and share capability. 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 devices that supports CIFS/SMB protocol. It can also be from iSCSI devices that you can mount storage directly as a drive letter in the CentreStack server. It can also be a container inside a private instance of OpenStack Swift, a bucket in Amazon S3 compatible storage, or a container from Windows Azure blob storage. You will need the basic access information ready. For example,

### Windows File Server

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

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

### OpenStack Swift

If it is OpenStack Swift, you will need the authentication URL and credentials and understand the version of your authentication setup, such as KeyStone V2 or KeyStone V3 or just the 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 is from an IAM user, you will need to make sure the IAM user has full permission to the bucket.

## Windows Azure Blob Storage

You will need the “Storage Account Name” and the “Primary Key” and a container name.

---

**Note:** The initial deployment of CentreStack configures the back end storage to use the `C:\CentreStack` directory on the CentreStack 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 tenant. Each CentreStack tenant can be configured for different back end storage locations.

---

## 2.2 Step 2: Prepare Active Directory (Optional)

If you are integrating 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 the Active Directory.
- The DNS name of the Active Directory Domain.

---

**Note:** If your Active Directory or the client’s Active Directory is remotely located with regard to the CentreStack Server, then you should use Server Agent software to connect the Active Directory instead of using LDAP to connect Active Directory.

---

---

**Note:** If you are using Single Sign-On service such as Azure AD, Active Directory Federation Service, OneLogin or OKTA, you can configure SAML based authentication instead of using Active Directory directly. Normally those identity service providers are connected to the corporate Active Directory anyway.

---

## 2.3 Step 3: Prepare the Database Server

---

**Note:** If you are installing the all-in-one instance, you can skip this step because the all-in-one installer will install a MySQL Community Edition and configure the database accordingly. See [Step 5: Start Installation](#) below for more about the all-in-one installation.

This step is only for installation that has a separate database node which is not installed by default with any worker node.

All CentreStack servers in a cluster will share one single centralized database.

---

**Warning:** With the release of the CentreStack version 9.5.5409.41172, the default database engine for the “all in one” deployment has switched to PostgreSQL or MySQL Community Edition as opposed to Microsoft SQL Server Express Edition. The main reason to make this switch was to avoid the built-in limitations of SQL Server Express Edition (1 GB RAM and 10 GB max database file size).

There are two places that store persistent information. The first place is the File Storage mentioned in Step 1. The second place is the CentreStack database. There is configuration information such as user name, team folder, shared

folder, login token in the database. There is also runtime information such as audit trace and file change log in the database.

The default CentreStack deployment utilizes a MySQL local database on the CentreStack Server. We provide this option to allow the trial installation to be as simple as possible.

Currently CentreStack supports MySQL or Microsoft SQL Server Database Management Systems (DBMS). Some good reasons for deploying an external database server are performance, scalability and/or high availability.

### 2.3.1 Microsoft SQL Server

If you are using an external Microsoft SQL Server as opposed to the default MySQL all-in-one deployment, then you must ensure the **SQL Server Authentication is configured for Mixed Mode Authentication**. The CentreStack Server connection requires the use of a SQL account, not a Windows integrated authentication account.

During the setup of the first worker node, the installer will need to create a database, create tables inside the database and create stored procedures in the database. Therefore, it requires a SQL security account that has enough privileges for the installation.

If the database server is external to the CentreStack server, make sure TCP protocol is enabled and firewall is opened to accept SQL connections. Default TCP port is 1433 and that port needs to be opened on firewall. If you have SQL Server listening on a different port, that port will need to be opened as well.

### 2.3.2 MySQL Server

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

### 2.3.3 PostgreSQL Server

PostgreSQL usually is the default option for the all-in-one installation. The default port is 5679 but most of the time the database is running on the “localhost”, same as the CentreStack server.

## 2.4 Step 4: Prepare the CentreStack Server

The easiest way to prepare the CentreStack server is to have a clean Windows Server 2022/2019/2016 OS with English locale and make sure the worker nodes are all in the same time zone.

We recommend Windows server 2022, 2019 or Windows server 2016 as a preferred server OS running on a virtual machine.

#### Supported Operating Systems

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

#### Supported CPU

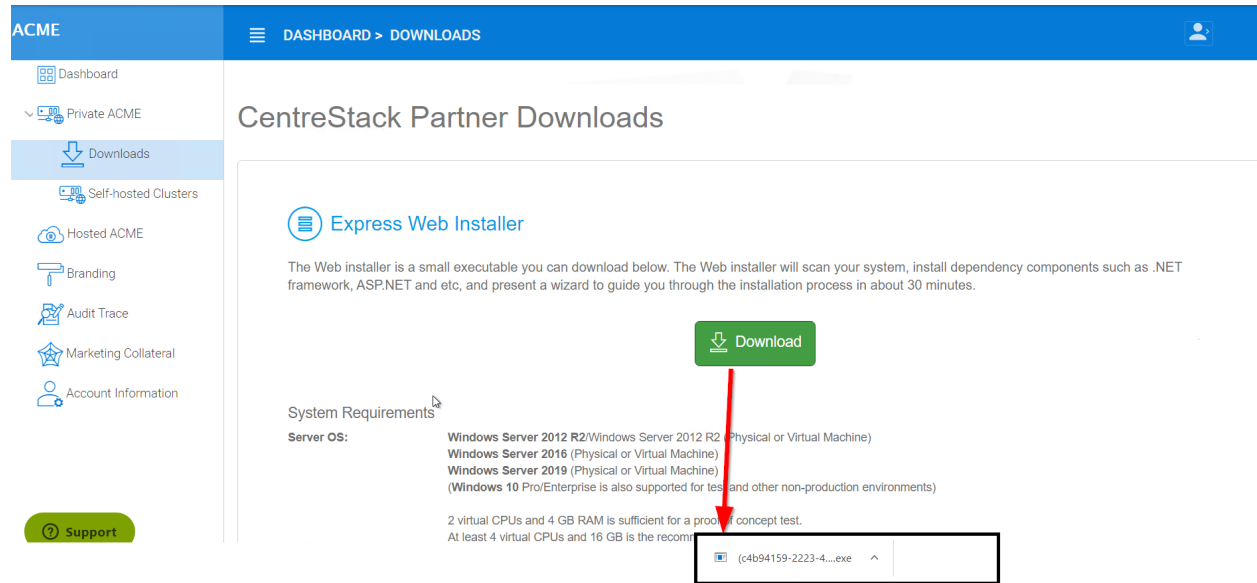
- 64-bit Intel or AMD x64 architecture
- 2 - virtual CPUs minimum (4 - virtual CPUs or more are recommended)

**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 CentreStack server itself.

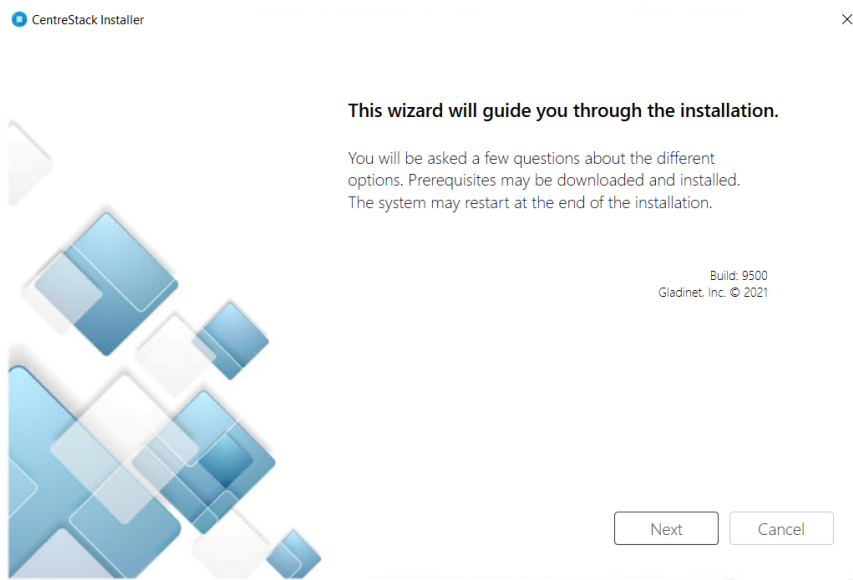
## 2.5 Step 5: Start Installation

You can get the CentreStack installation package from the CentreStack partner portal (by logging in to <http://www.centrestack.com>) and going to the Private CentreStack section.

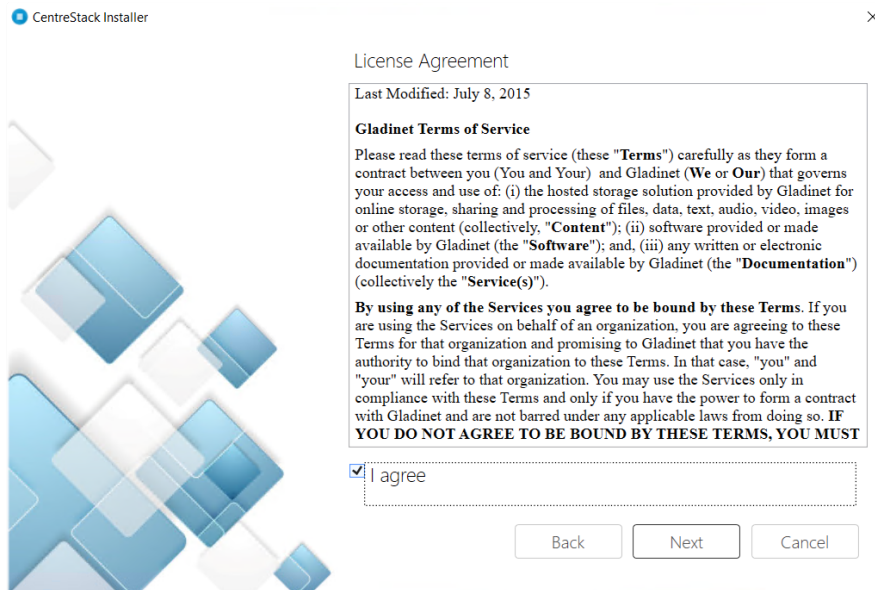


Sign into the CentreStack server console (RDP or physical console are fine) with administrator rights. Once you click the **“Download”** button on the Partner Portal, the installer will appear either in downloads or as a link at the bottom of your browser. Click the executable file to begin the installation.

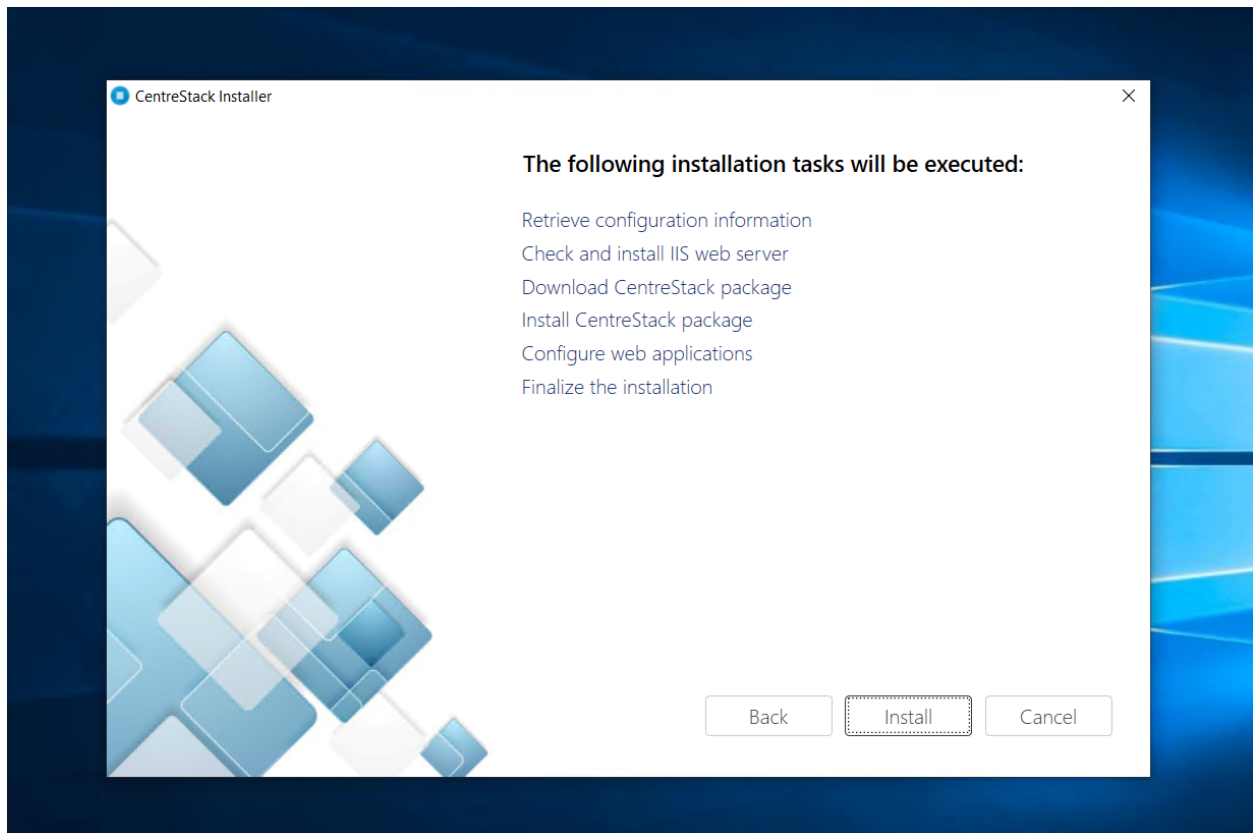
You will see the welcome screen.



Click 'Next'  
And accept the EULA

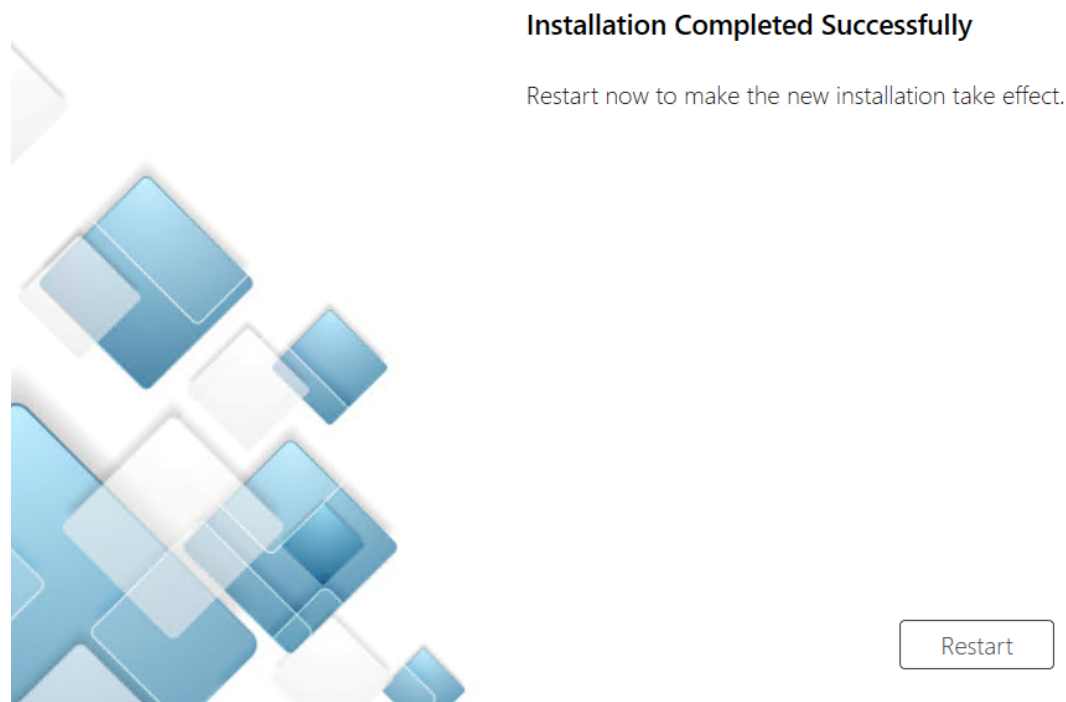


Click 'Next'



And Click Install.





After the installation has been completed successfully, a reboot is required. Click 'Restart'.

---

**Note:** CentreStack will install and then you will need to restart your system to complete the installation.

---

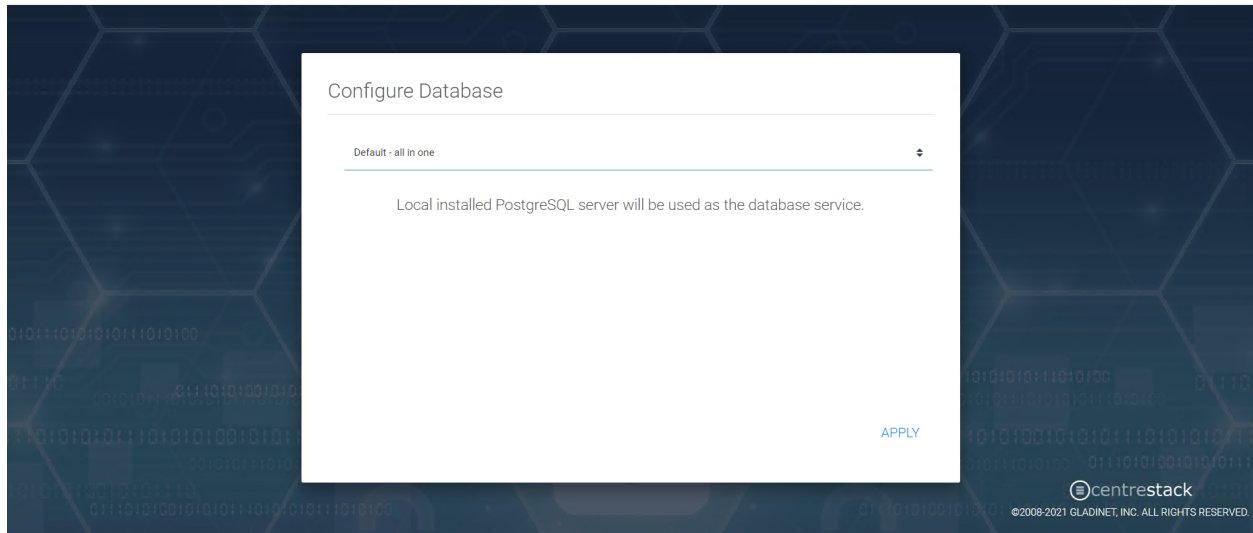
---

**Note:** CentreStack is a multi-tenant solution. The Tenant Manager scope is defined for a tenant administrator. For a multi-tenant Cluster Server system, each tenant has an administrator. For a single-tenant Cluster Server system, the default cluster administrator is also the tenant administrator.

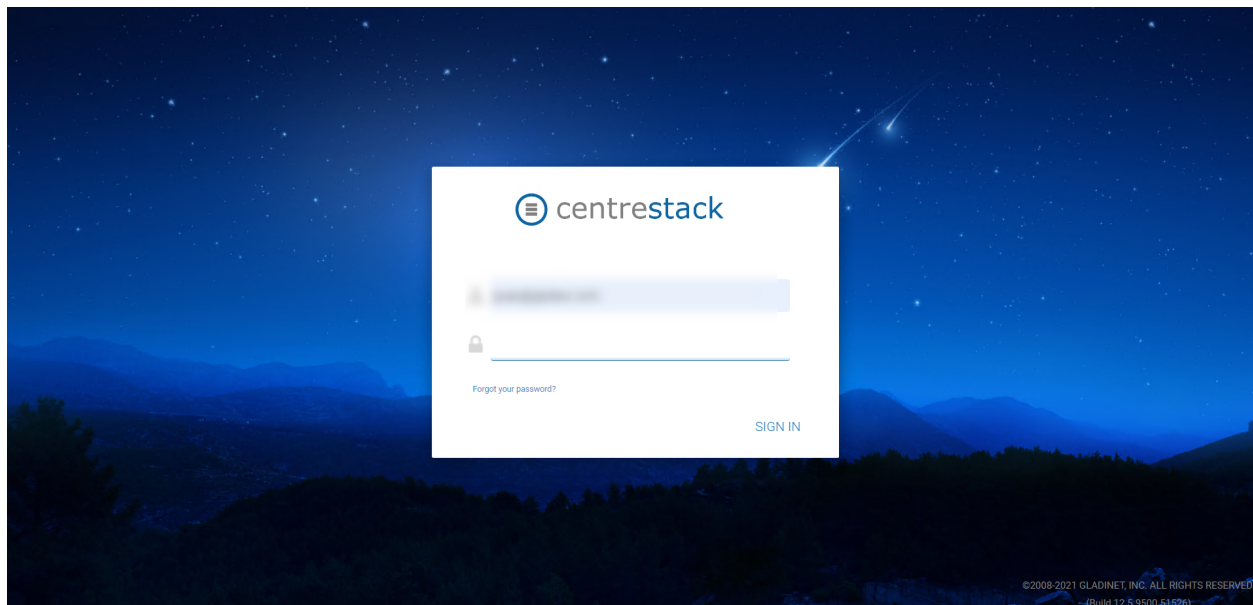
---

**Warning:** After the reboot and login to the Windows session again with the same Windows admin user credential, it may take 3-5 minutes before all the windows services start and a web browser page will pop-up.

For the next screen, if you have an existing database use the pull-down menu to select a different option otherwise use the default which will also install the PostgreSQL Community Edition database.



In the next screen, enter your Partner Account login credentials to complete the installation.

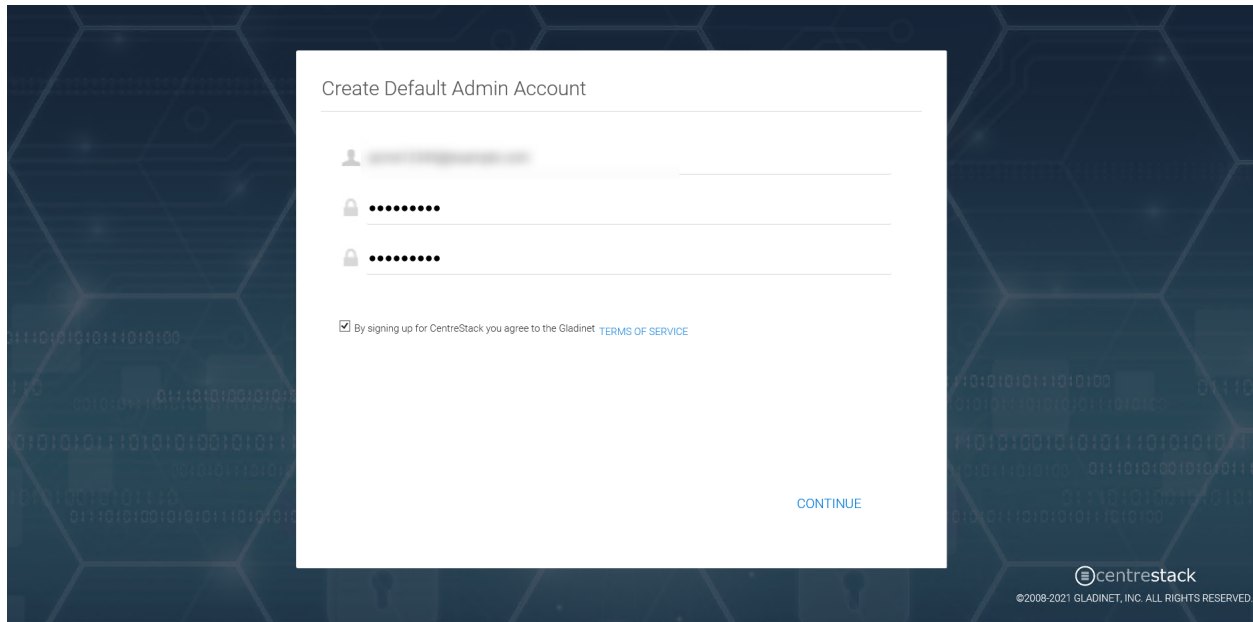


## CHAPTER 3

### 3 Initial Configuration

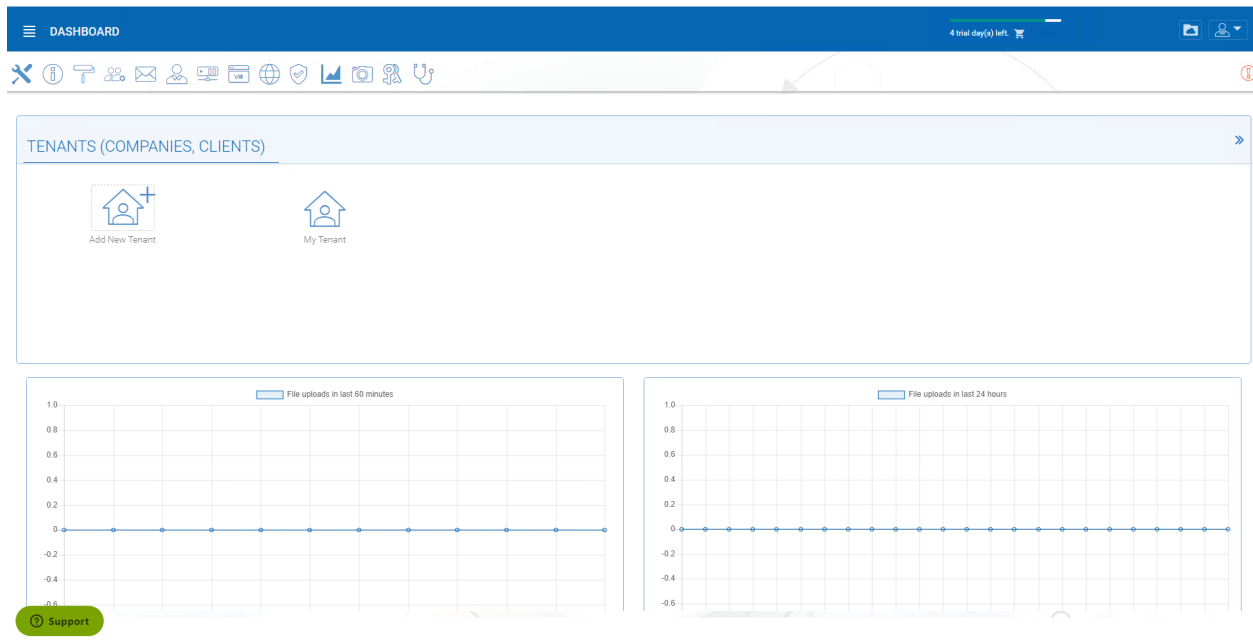
After the machine reboots, the Default administration configuration page will be displayed.

First, setup the cluster administrator account.



The screenshot shows a web interface for creating a default admin account. The form is titled "Create Default Admin Account" and is set against a dark blue background with a hexagonal pattern. It contains three input fields: a username field with a person icon, a password field with a lock icon and a series of dots, and a second password field with a lock icon and a series of dots. Below these fields is a checkbox that is checked, with the text "By signing up for CentreStack you agree to the Gladinet [TERMS OF SERVICE](#)". A "CONTINUE" button is located at the bottom right of the form. In the bottom right corner of the overall image, there is a "centrestack" logo and the text "©2008-2021 GLADINET, INC. ALL RIGHTS RESERVED."

After setting up the cluster administrator account, the cluster administrator's dashboard will appear by default.

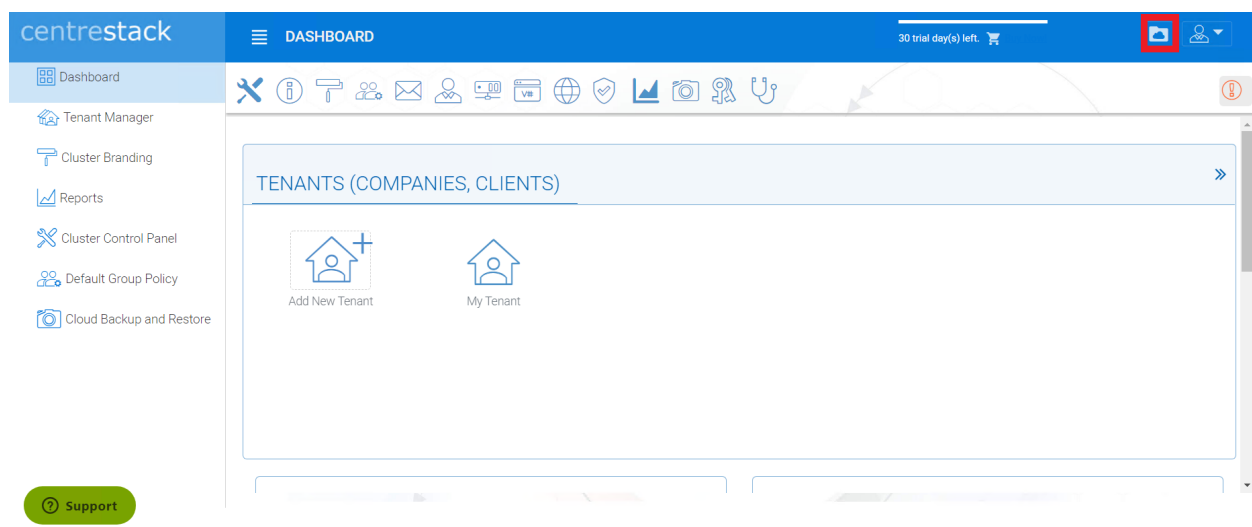


Once you see the dashboard, the CentreStack side of the setup is finished successfully. We will continue to check the storage configuration and make sure all components are fully functional.

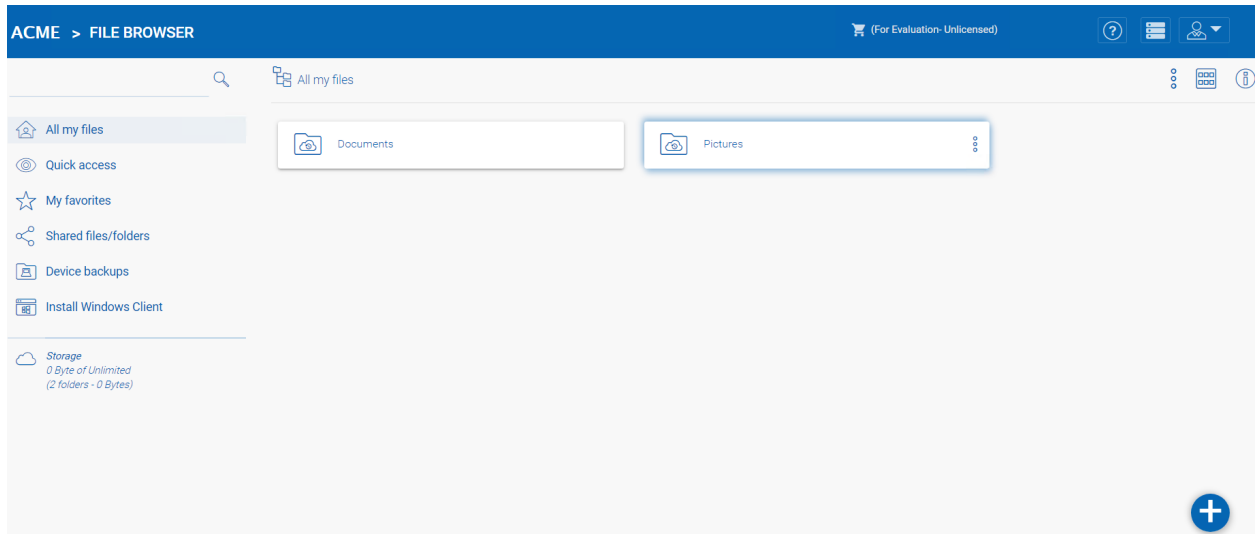
## CHAPTER 4

### Web Portal

Click the Portal – “My Files” Link for the default master admin to view his files/folders over the web portal:



See below image for the files and folder view:

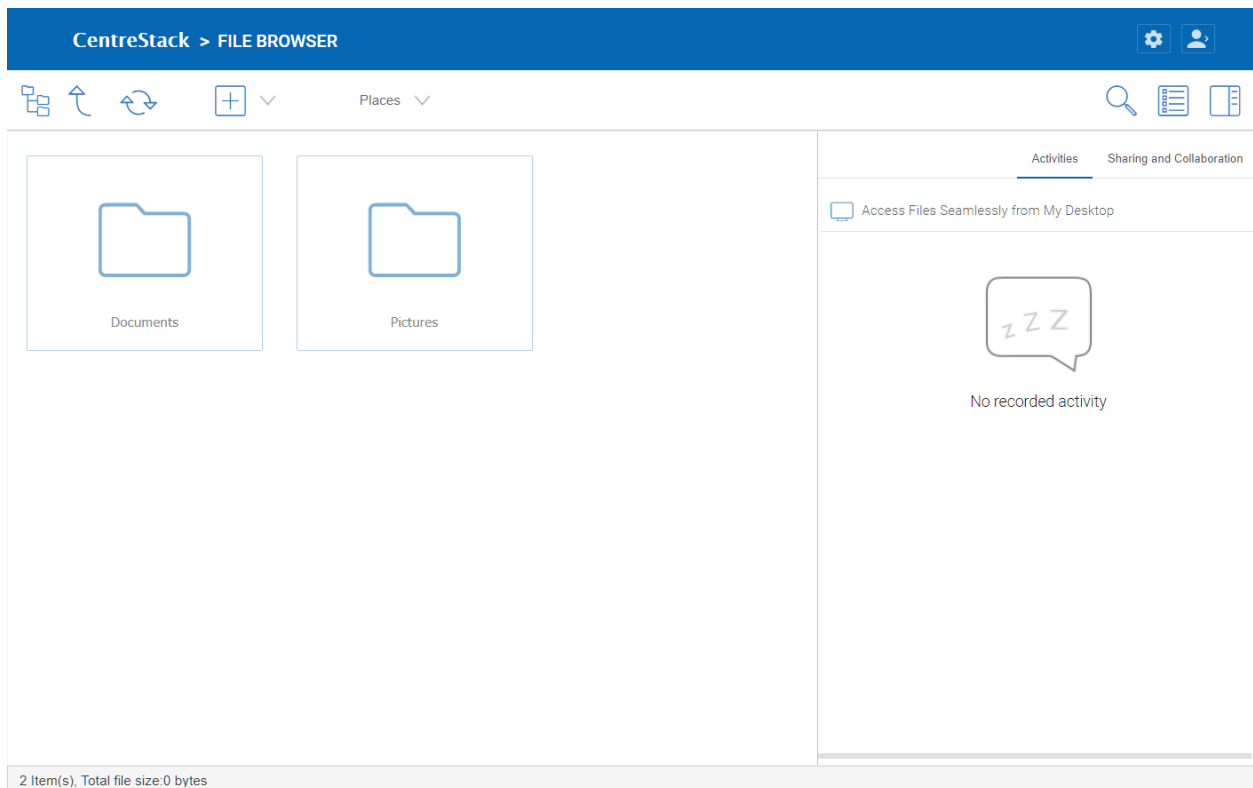


From here you can test the installation by creating files, migrating, editing, sharing and deleting files to verify the storage setup is working as expected.s

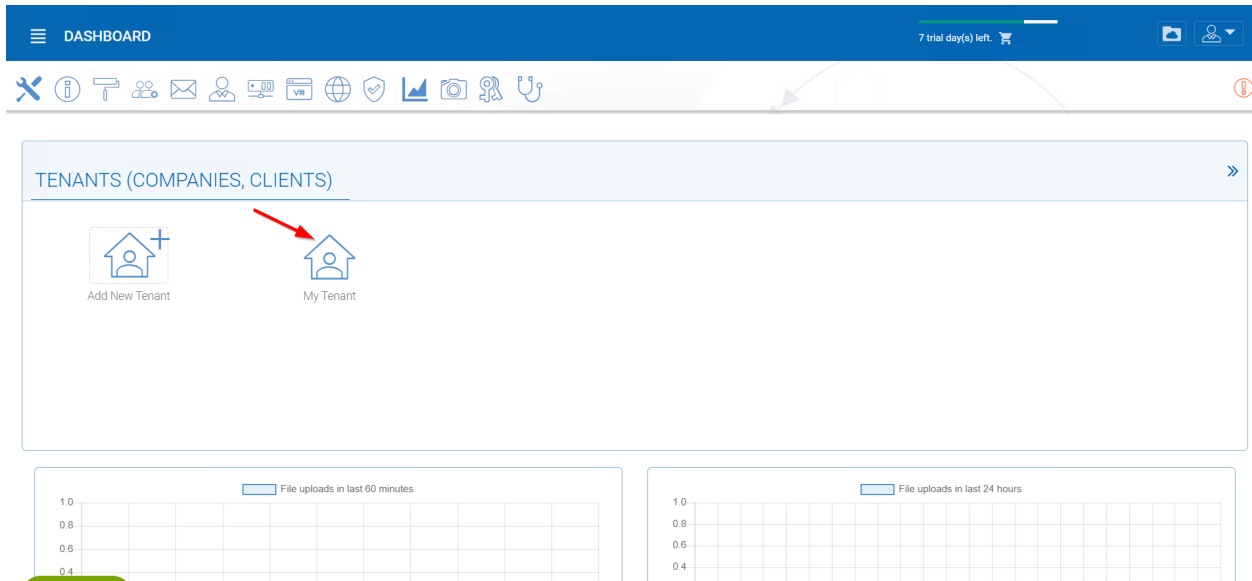
## Management Console

If you are logged in as the Tenant administrator, access the Management Console by clicking the stack icon on the top right of the “**File Browser**” view.

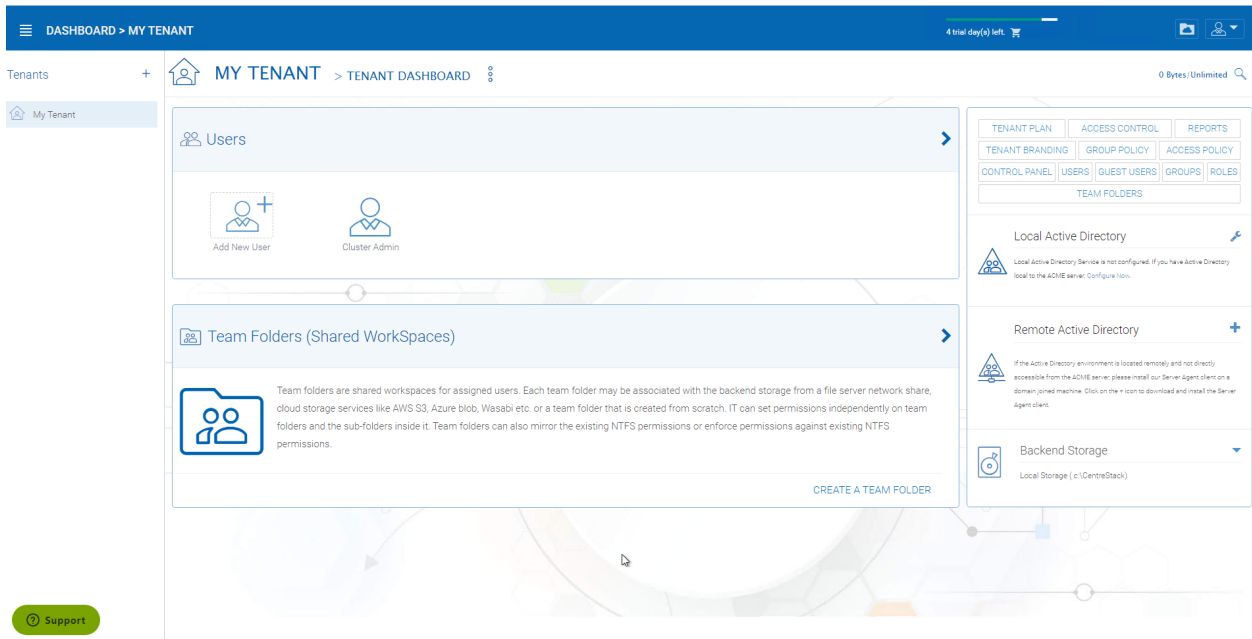
The Tenant Administrator will see the files and folders view by default upon initial login.



**Warning:** If you are the cluster administrator, you may not see the “Management Console” icon. Instead, you can manage the default tenant from the Cluster Manager -> Tenant Manager and click through to manage the default tenant.



Here is the Tenant Management Console.



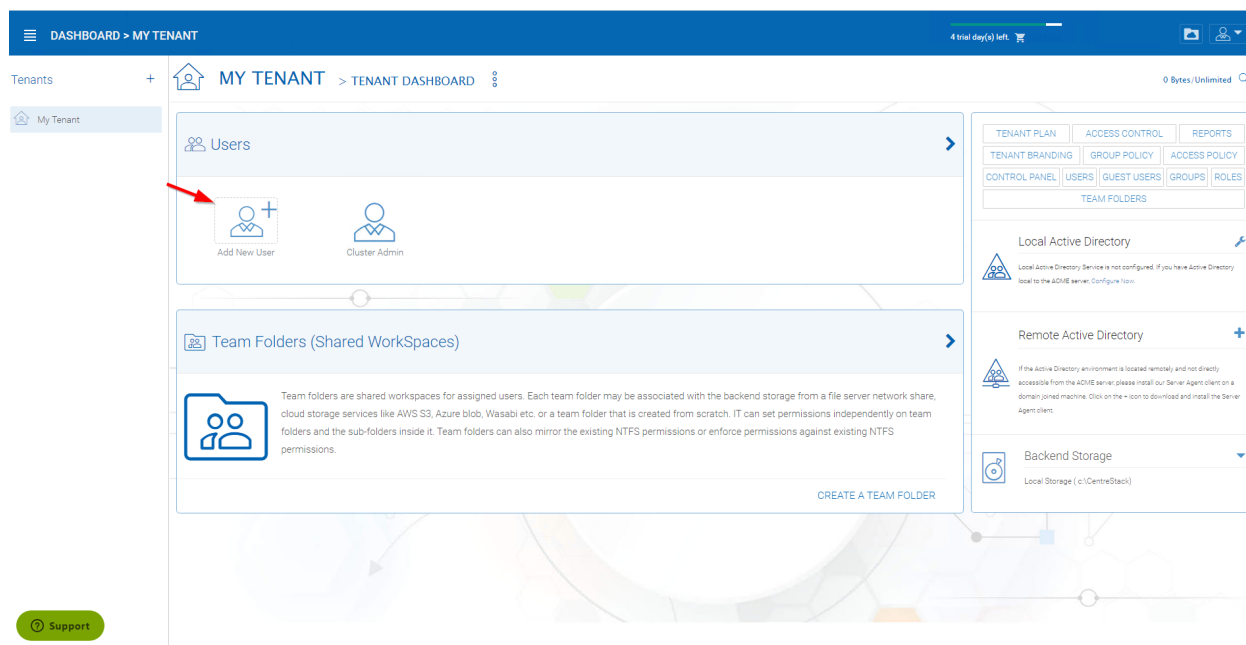
Please reference the [CentreStack Admin Guide](#) for complete details about Tenant administration.

Here are a few points that are more important during the deployment phase.

## 5.1 Add Tenant

You can add a tenant by clicking the ‘Add Tenant’ Button in the Tenant Manager

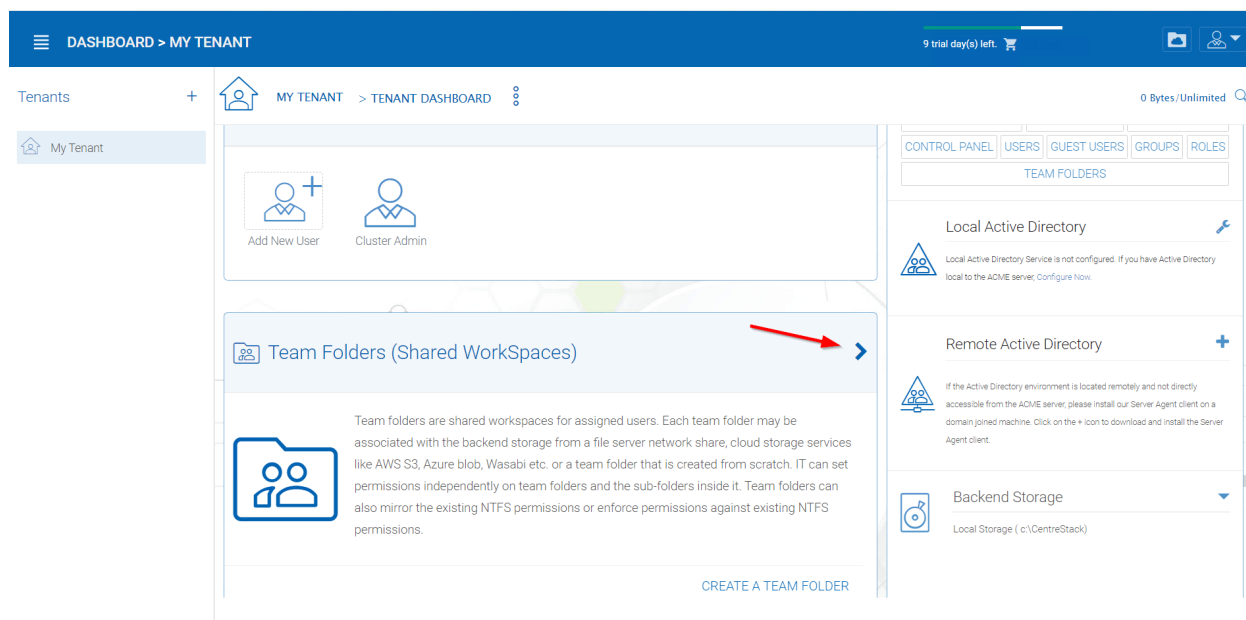




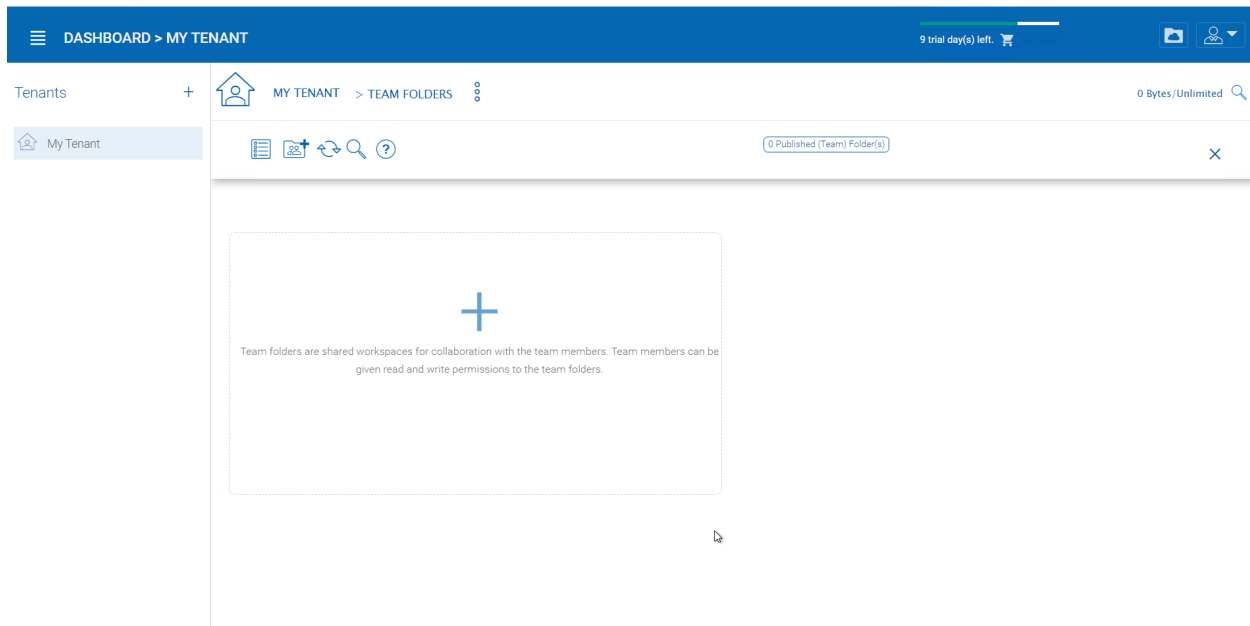
## 5.2 Team Folders

Team Folders are created by the tenant admin. The users that can be assigned to the team folders are the team users within the tenant. Each team user can be assigned read or write permissions to the team folder. For the team users that are not assigned with a specific team folder, the team folder will not show up. Team folders users can also be assigned the “Owner” permission. The owner permission allows the “owner” to maintain and manage the team folder permissions.

You can navigate to the Team Folders by clicking on the arrow in the “Team Folders” tab from the Tenant Manager.



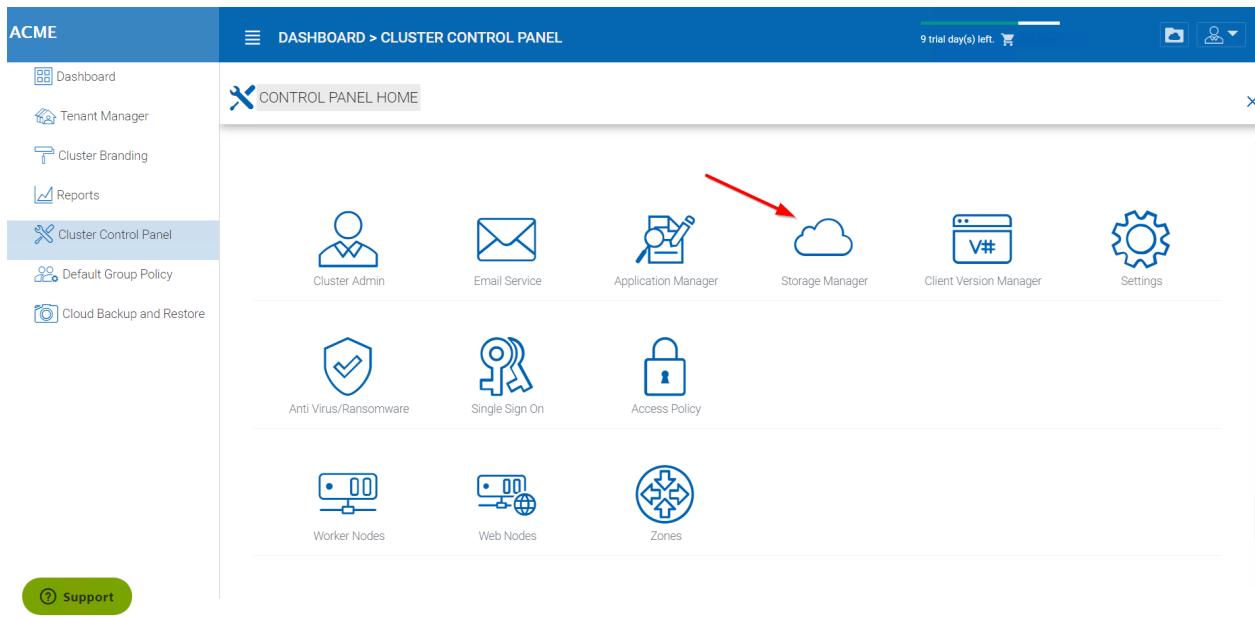
Here is the Team Folders page.



### 5.3 Storage Manager

The tenant admin can update the default (primary) storage configuration information. For example, if the default storage is using Amazon S3, the tenant admin can update the S3 bucket, access key and secret key. However, the tenant admin can not switch the default storage into a different storage service. The cluster admin can help the tenant admin switch the default storage.

First, go to the Cluster Control Panel. Then, click on “Storage Manager”



This will take you to the Storage Manager page.

DASHBOARD > CLUSTER CONTROL PANEL

9 trial day(s) left.

CONTROL PANEL HOME > STORAGE MANAGER

EDIT

Google Drive	<input type="checkbox"/>
Client ID	Not Configured
Client Secret	Not Configured
Redirect URL Make sure the redirect URL configured in Google Drive Console matches	<a href="http://tthcitsv01/portal/storageconfig/googledrivecallback.aspx">http://tthcitsv01/portal/storageconfig/googledrivecallback.aspx</a>
OneDrive	<input type="checkbox"/>
Client ID	Not Configured

The tenant admin can also add auxiliary storage by using the “Attach Storage” options. The default storage is the root folder of the tenant. Attached auxiliary storage is top level folders inside the root folder.

## 5.4 User Manager

In the user manager, you can create users, import users from Active Directory over LDAP or import users from Active Directory via Server Agent. Click on the arrow in the “Users” tab.

DASHBOARD > MY TENANT

7 trial day(s) left.

Tenants + MY TENANT > TENANT DASHBOARD

0 Bytes/Unlimited

My Tenant

Users

Add New User Cluster Admin

Team Folders (Shared WorkSpaces)

Team folders are shared workspaces for assigned users. Each team folder may be associated with the backend storage from a file server network share, cloud storage services like AWS S3, Azure blob, Wasabi etc. or a team folder that is created from scratch. IT can set permissions independently on team folders and the sub-folders inside it. Team folders can also mirror the existing NTFS permissions or enforce permissions against existing NTFS

TENANT PLAN ACCESS CONTROL REPORTS

TENANT BRANDING GROUP POLICY ACCESS POLICY

CONTROL PANEL USERS GUEST USERS GROUPS ROLES

TEAM FOLDERS

Local Active Directory

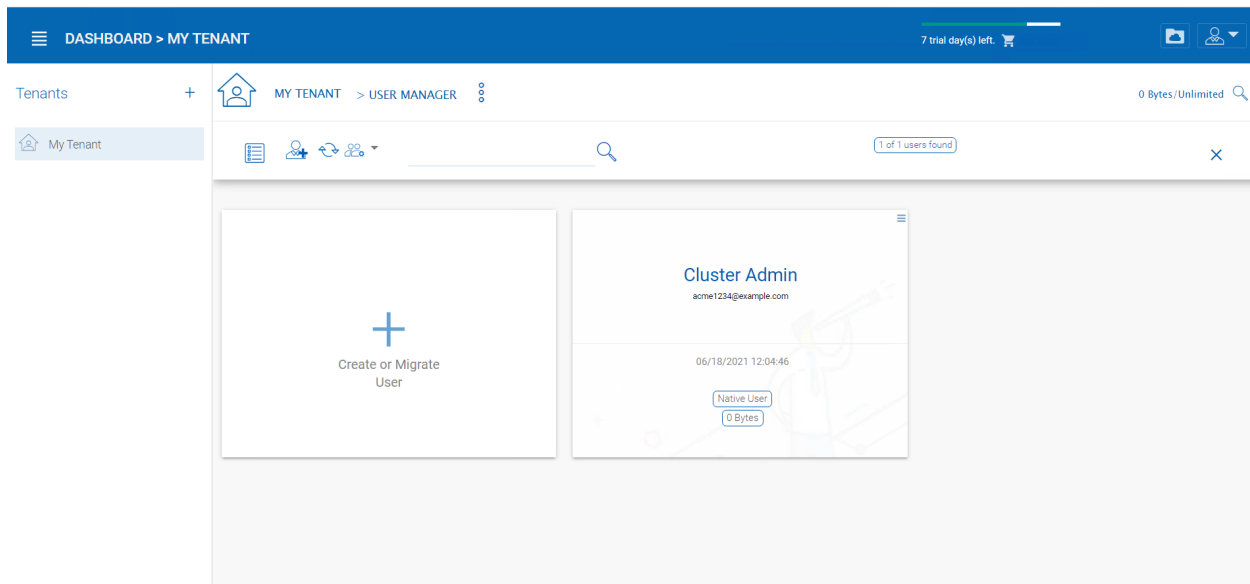
Local Active Directory Service is not configured. If you have Active Directory local to the ACME server, Configure now.

Remote Active Directory

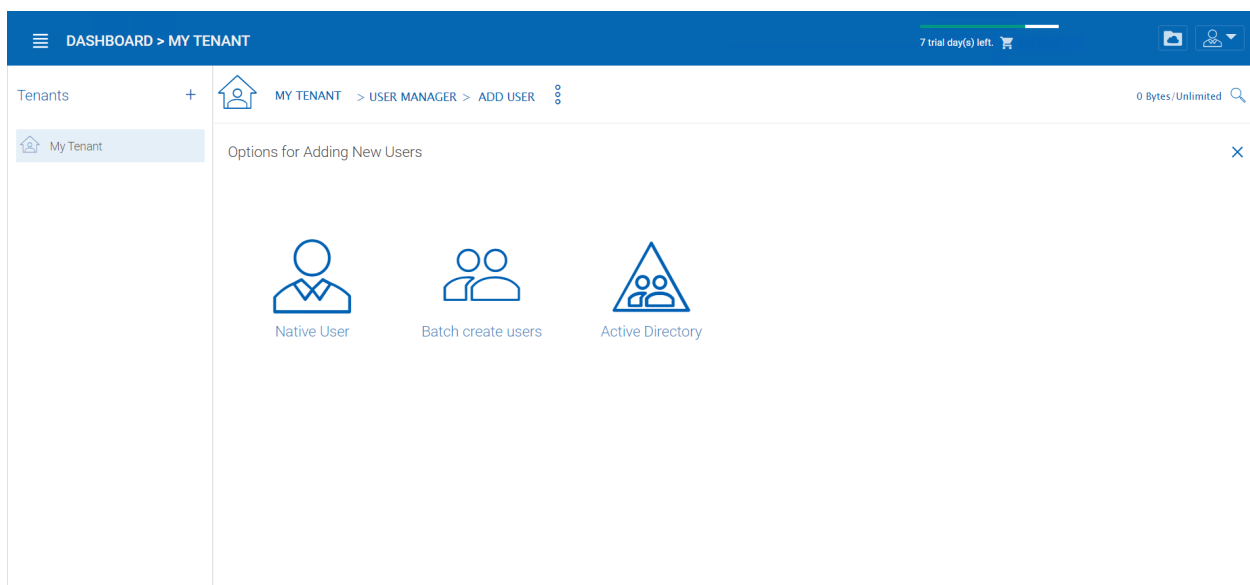
If the Active Directory environment is located remotely and not directly accessible from the ACME server, please install our Server Agent client on a domain joined machine. Click on the + icon to download and install the Server Agent client.

Backend Storage

Then click on “Create or Manage Users”.

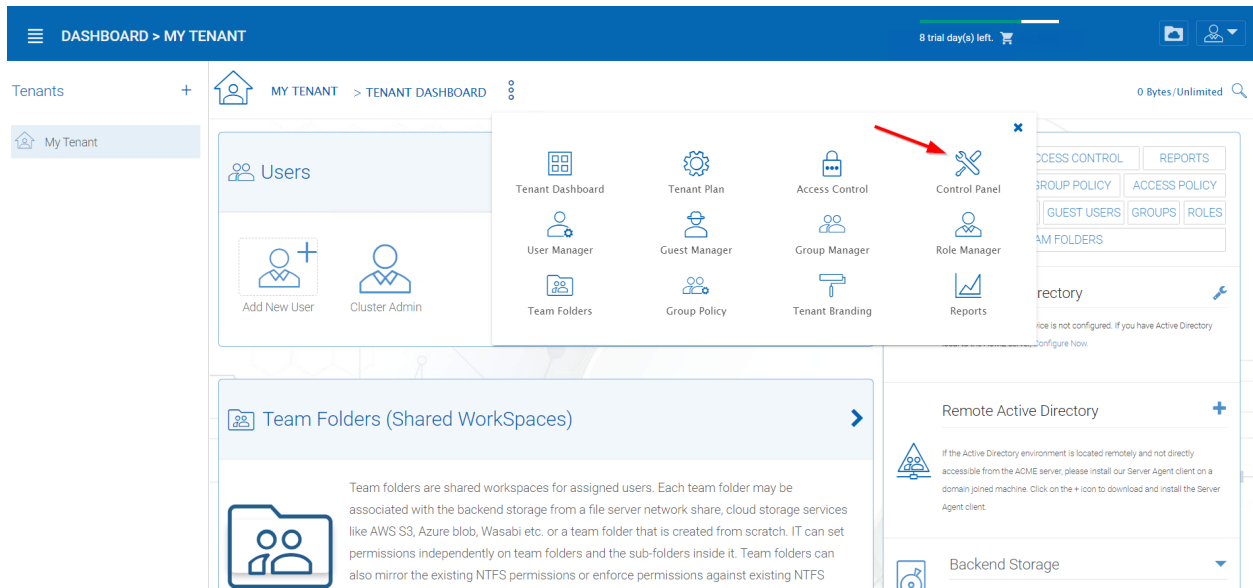


This should take you to a menu of options to add a new user to the tenant.

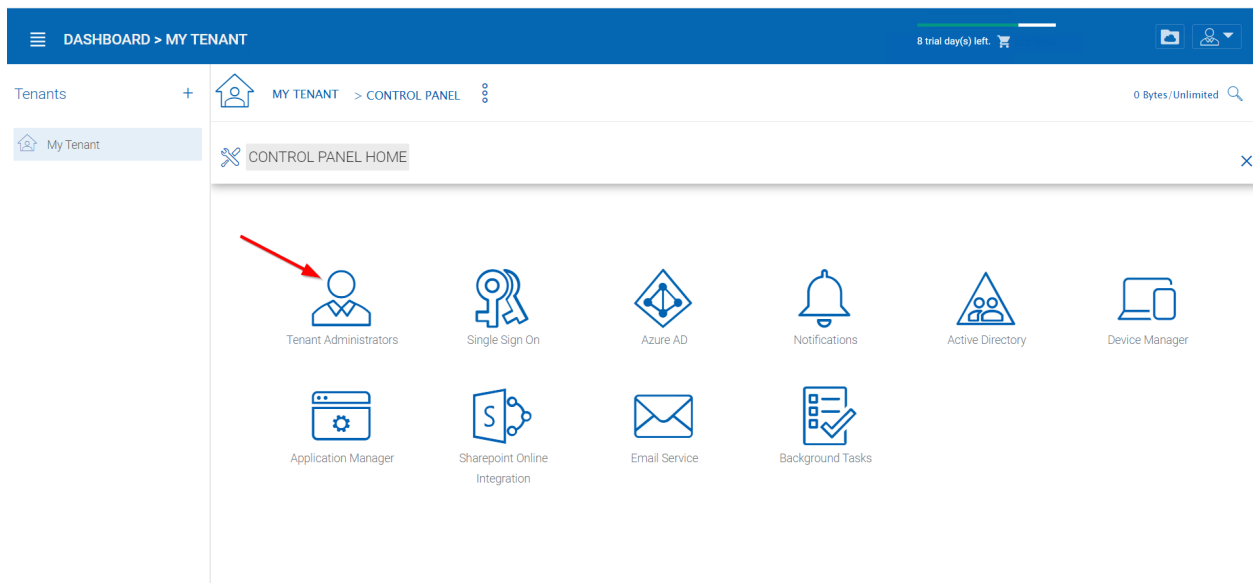


## 5.5 Delegate Administration

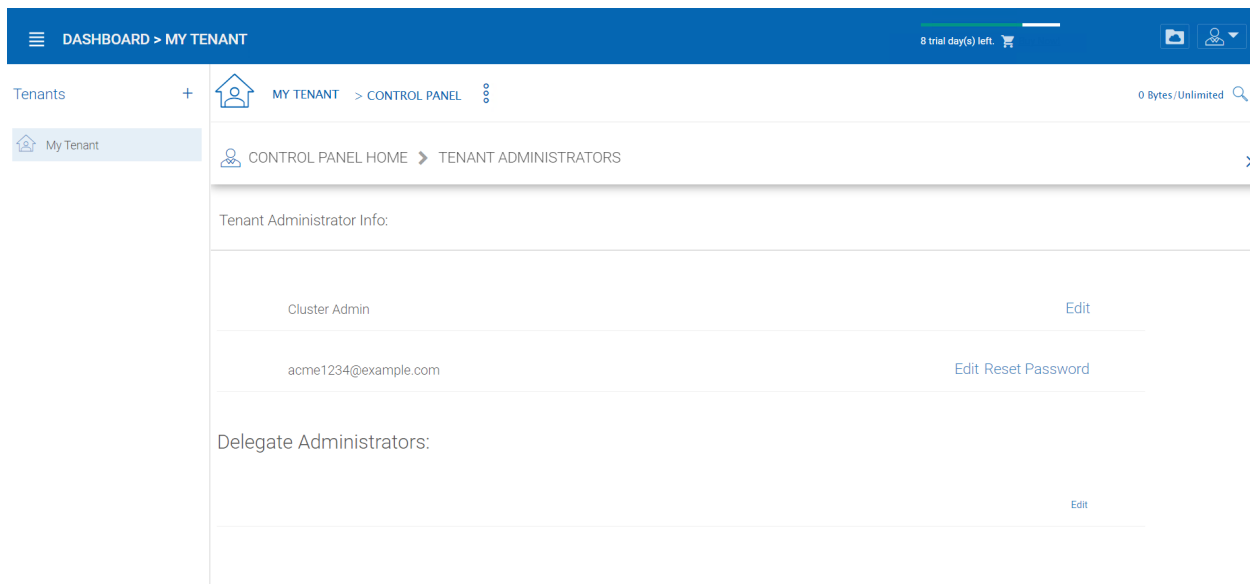
You can add full delegated admin to the list of “Cloud Administrators”. Once you reach the tenant page, click the drop down menu, and then go to the “Control Panel”.



In Control Panel, Click on “Tenant Administrators”.



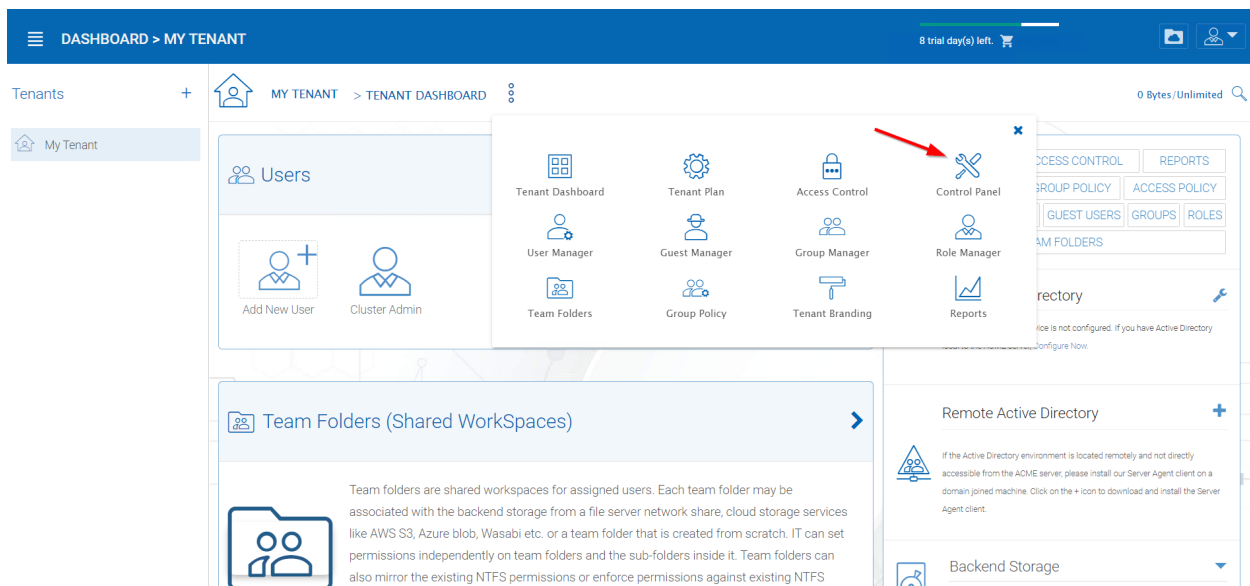
At the bottom of the Tenant Administrators page, you can designate the delegated admin.



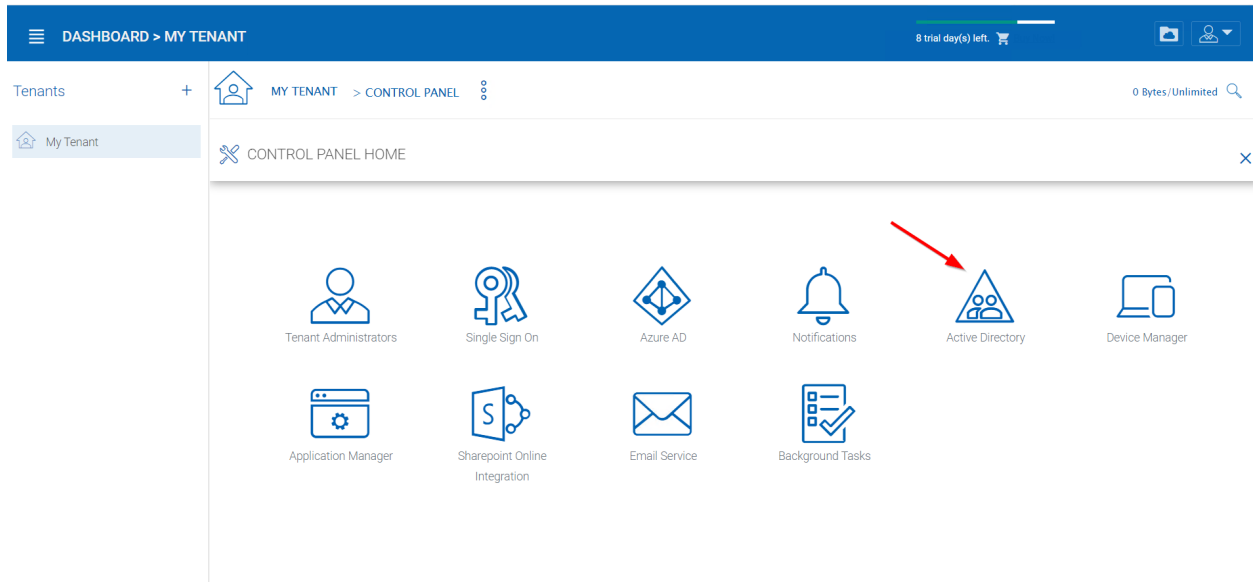
## 5.6 Active Directory Integration (Optional)

It is optional to setup the Active Directory Integration. You can get to the integration page from the Management Console -> Advanced -> Active Directory Settings. The active directory setting here refers to local Active Directory with LDAP integration. For remote Active Directory, server agent can be used to connect remote file server folders and remote Active Directory.

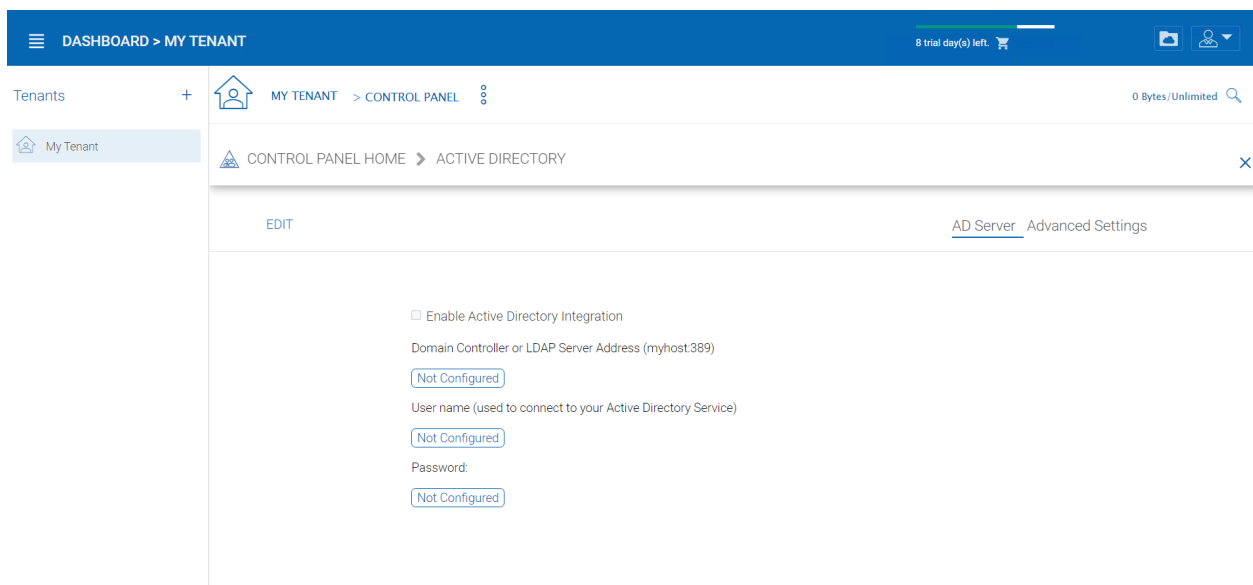
Once you reach the tenant page, click the drop down menu, and then go to the “Control Panel”.



On the menu that pops up, go to the “Active Directory” option.



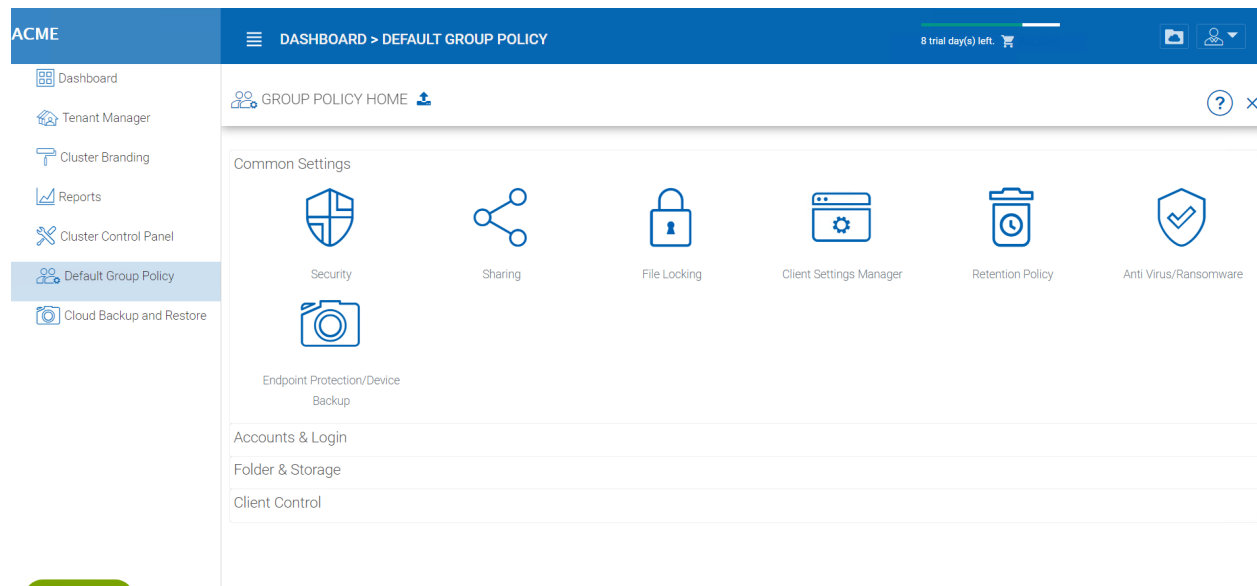
This will take you to the Active Directory Page.



**Note:** If this specific tenant's Active Directory is at a remote location, please use the CentreStack Server Agent to connect the Active Directory (No need to use LDAP over Internet WAN connection).

## 5.7 Group Policy

Granular group policies can be configured for the entire tenant users from Management Console -> Group Policy.

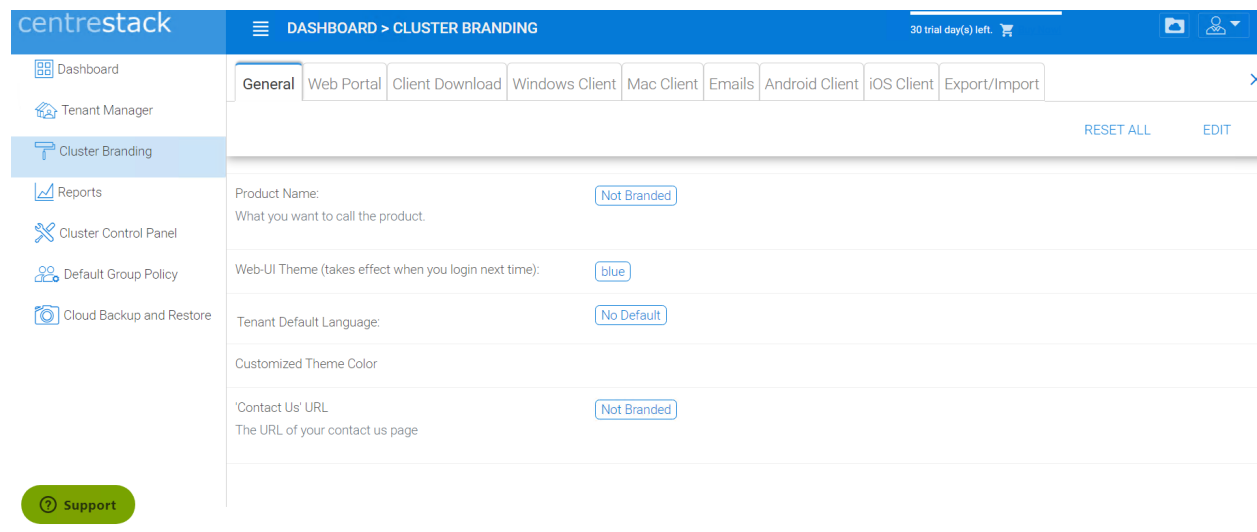


## 5.8 Branding

You can brand the web portal, Windows and Mac clients, iOS and Android Applications.

The self-service branding starts with the “Cluster Manager”. In order to start the branding, you will login to the web portal as the Master Administrator.

After you login to the web portal, click to the “Cluster Branding” Pages.



Please reference the “Cluster Branding” section in the [Admin Guide](#) for the self-hosted CentreStack server.



---

### Enable SSL – Install SSL Certificate

---

---

**Note:** Assuming that you have already setup your DNS to point to a DNS name connected to the CentreStack server and an SSL certificate already purchased for the DNS name. If not, you can acquire an SSL certificate from your SSL vendor.

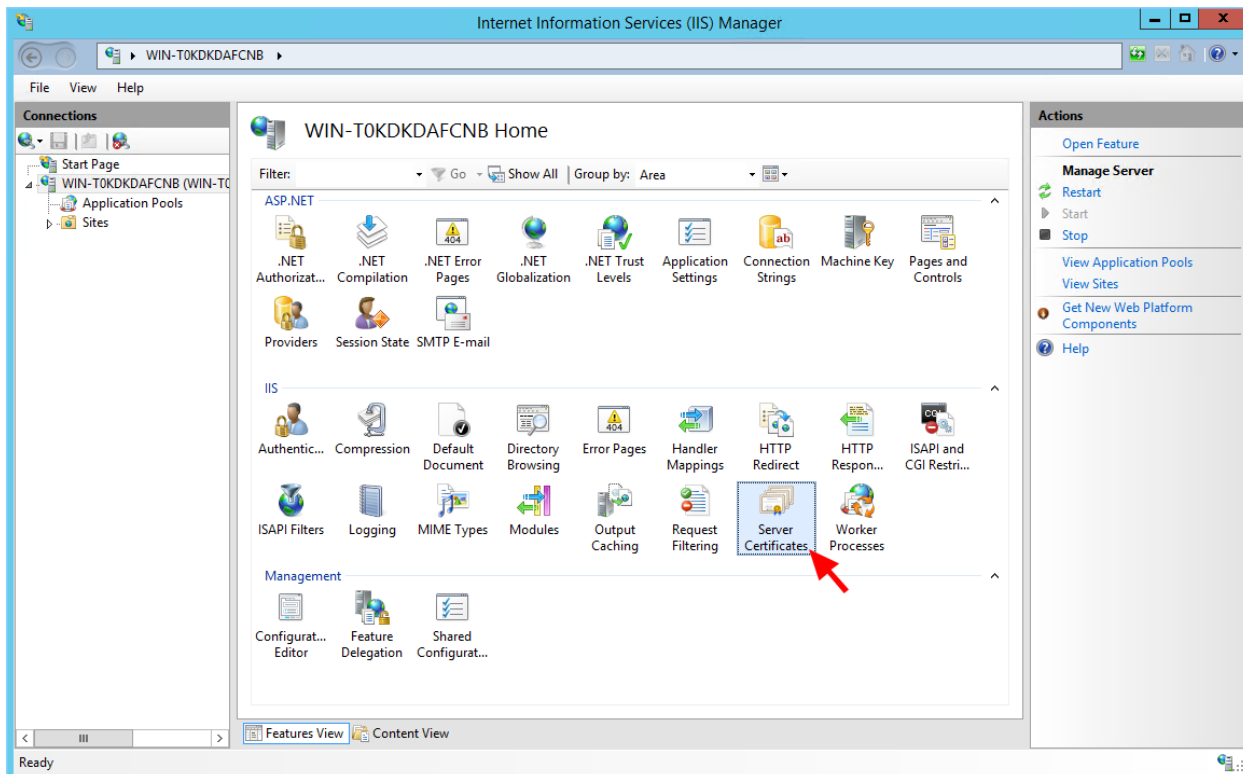
We recommend using <https://www.ssllabs.com/> to test your SSL setup because the SSL Labs site will produce a report on whether the SSL is compatible with all devices such as iOS devices.

You can also use openssl to check the SSL certificates and whether or not the whole certificate trust chain is completely installed on the server side.

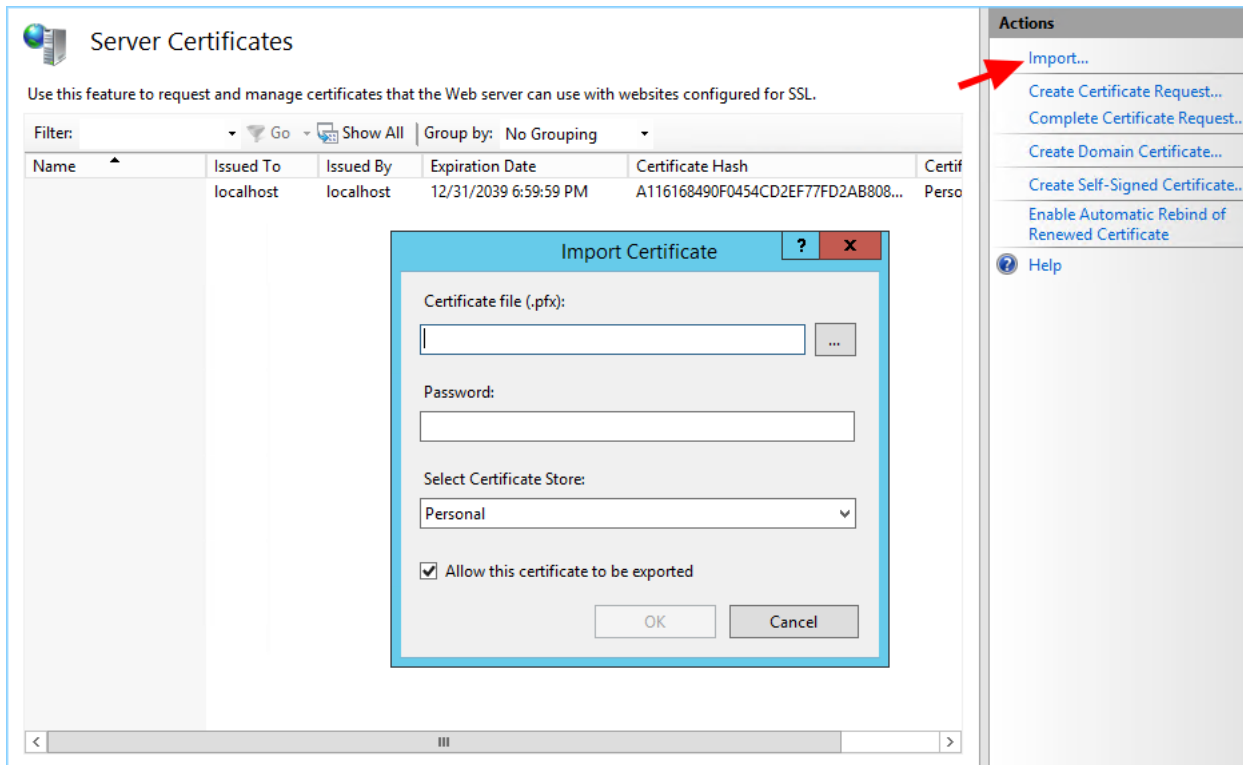
```
openssl s_client -connect server.yourwebhoster.com:443
```

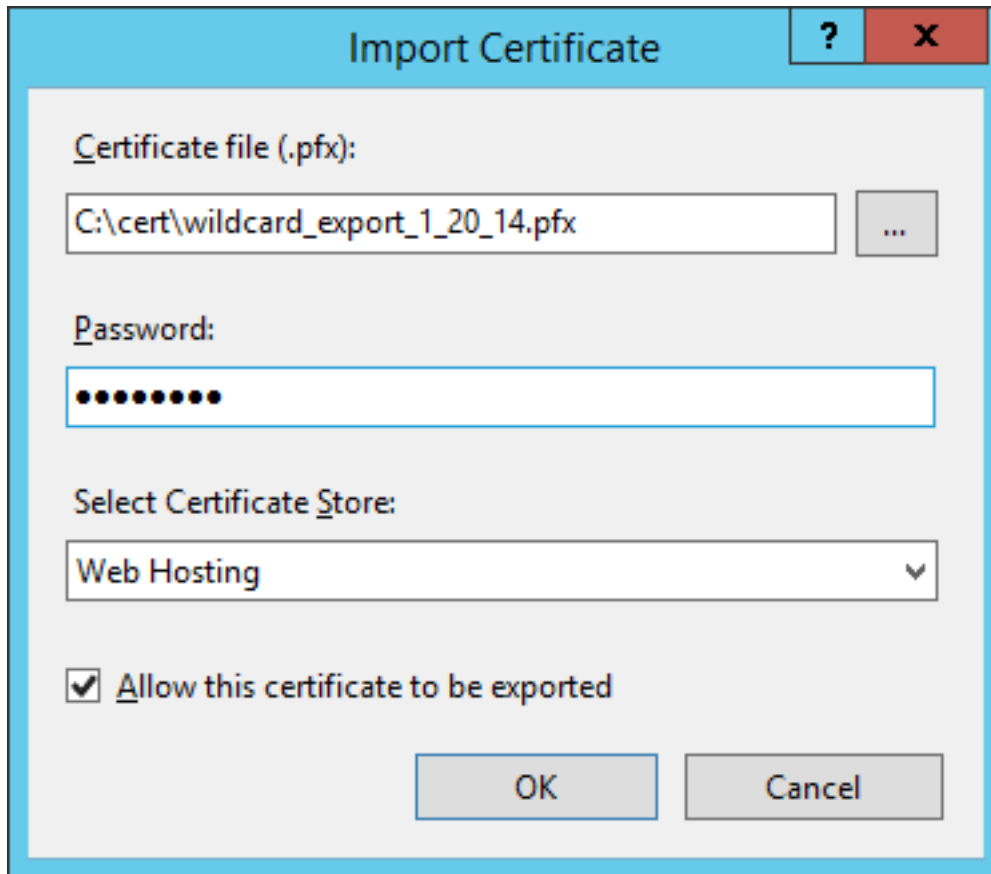
---

You will install the SSL certificate by using the IIS Manager. Look for “Server Certificates” and double click on it.

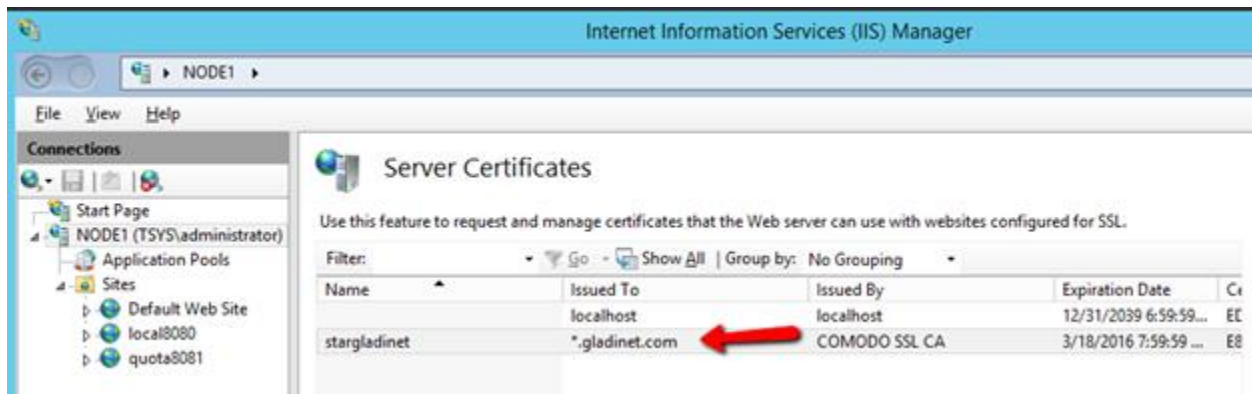


Click on “Import” to import an existing SSL Certificate. Leave the Certificate Store as “Personal” or “Web Hosting”, either way is fine.

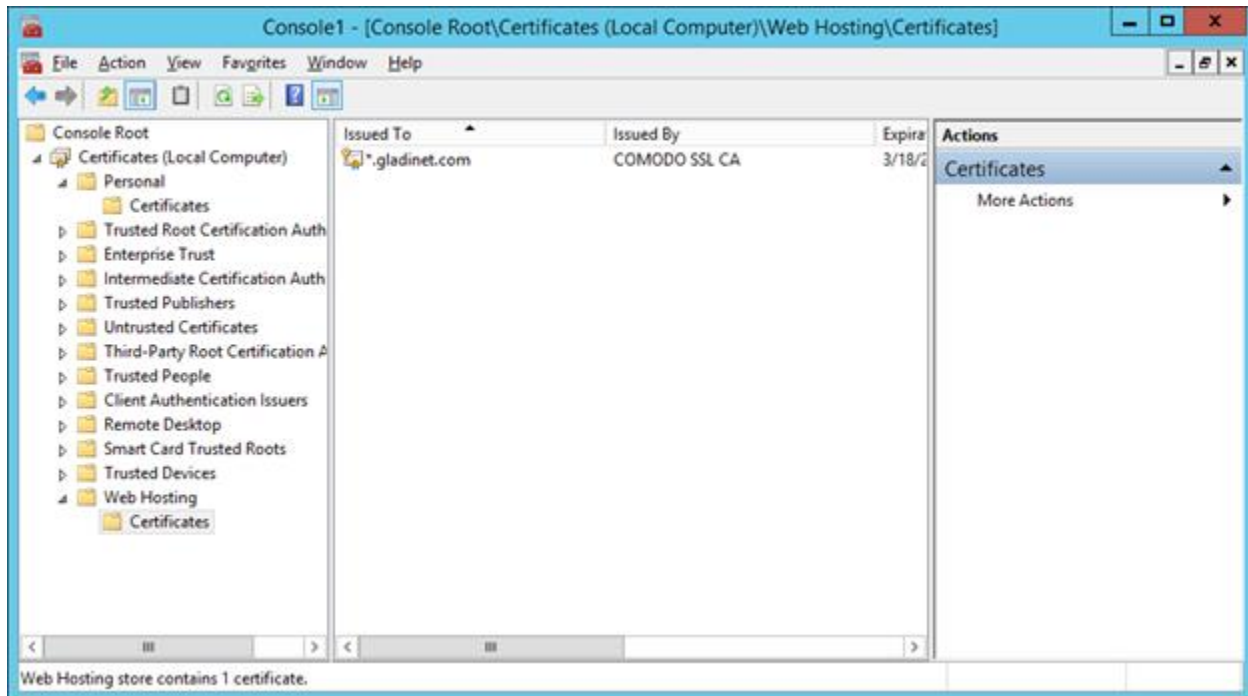




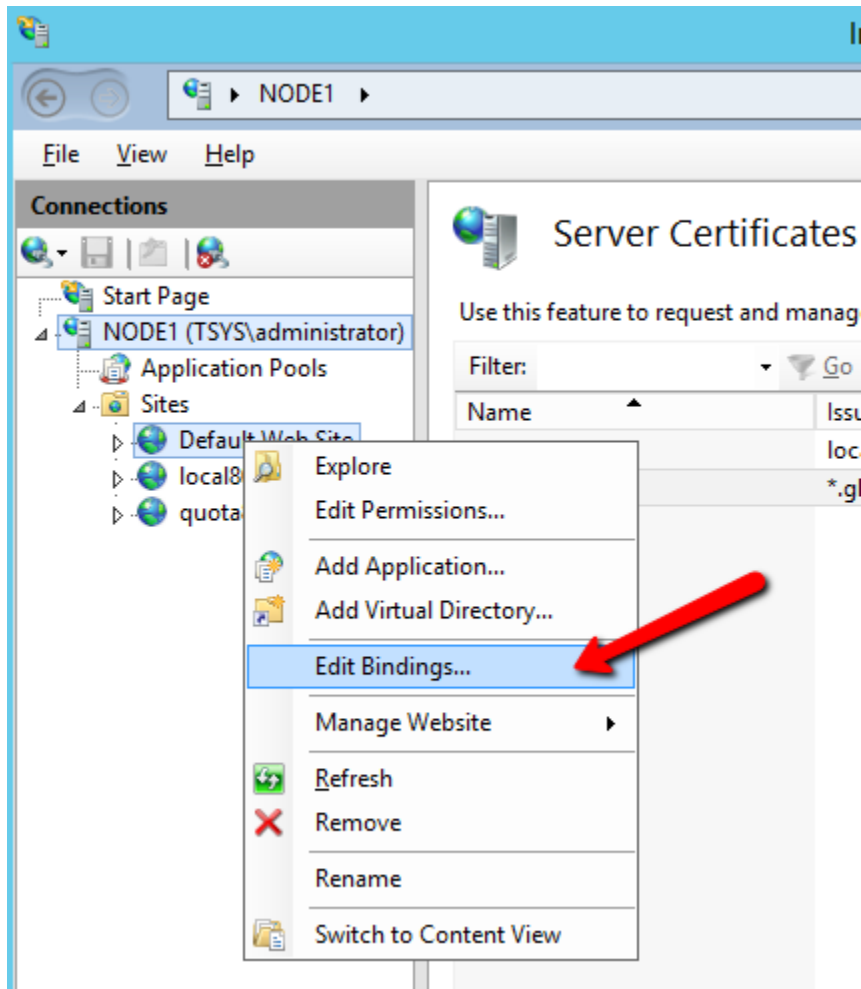
Verify that the certificate is available:



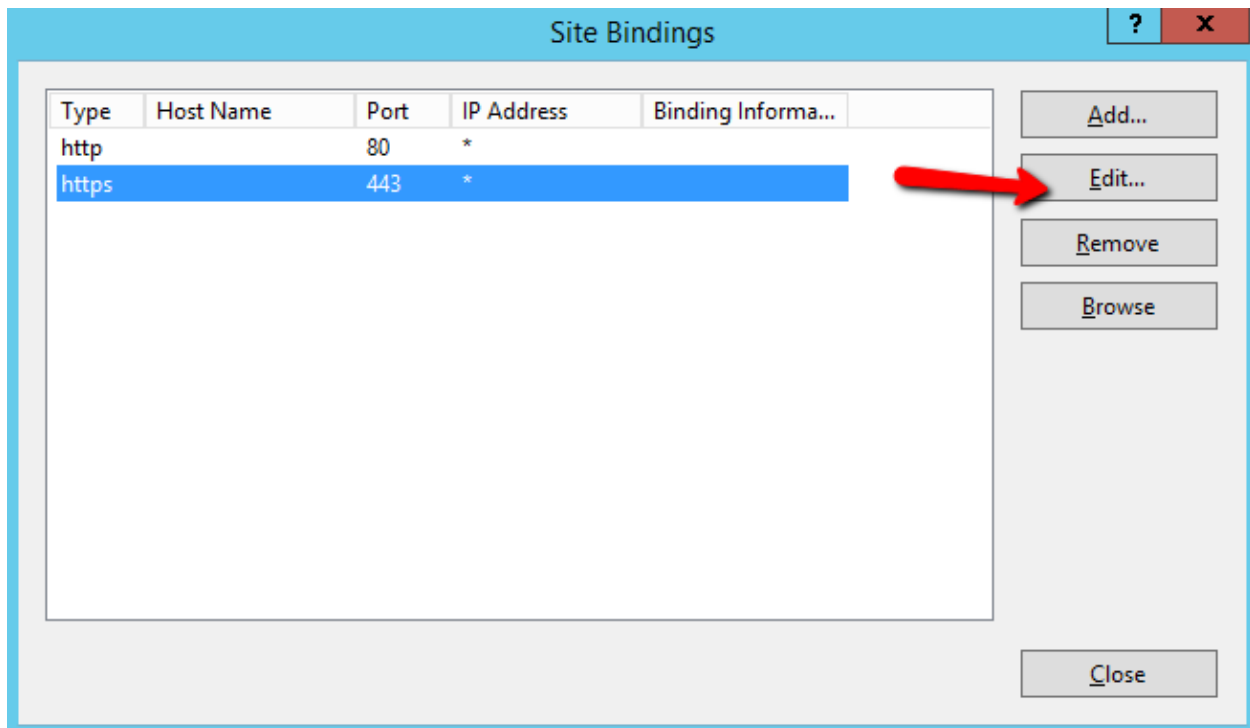
You can also verify the SSL certificate from the MMC/Certificates snap-in (Local Computer).



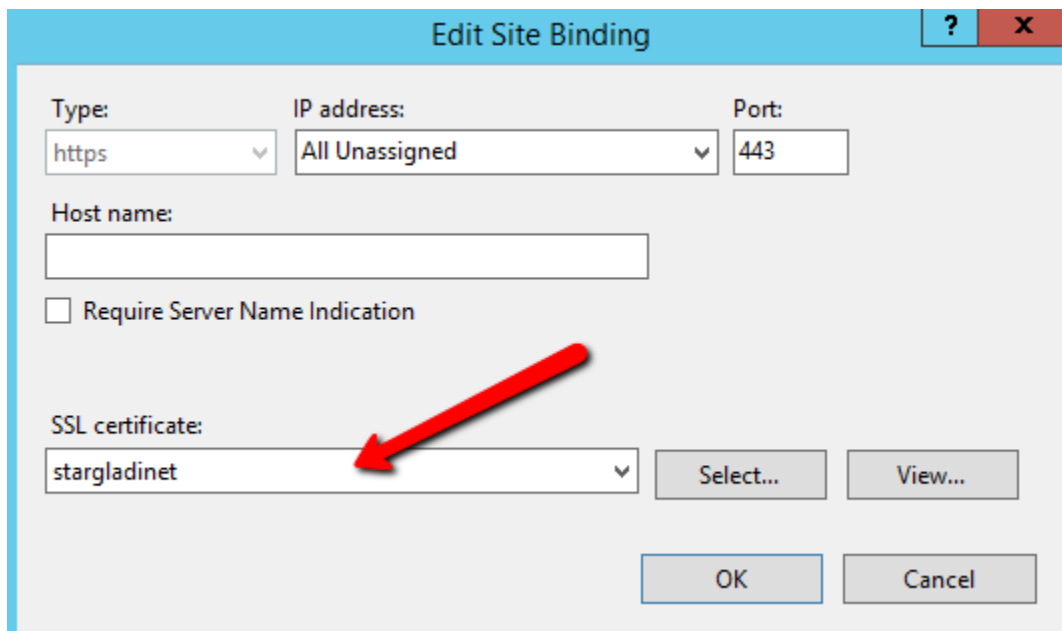
Now you can bind the “Default Web Site” to the SSL certificate for HTTPS. Right click on the “Default Web Site” and select “Edit Binding”.



At the binding dialog, edit the HTTPS binding.



Now, change the SSL Certificate binding drop-down to the imported SSL certificate.



---

### Setup Worker Node for SSL

---

Login to the Web Portal as the master administrator, then, under the menu next to dashboard, go to “Cluster Control Panel”.



\_static/image\_s7\_1\_1\_v2.png

After this, go to “Worker Nodes”.

ACME

DASHBOARD > CLUSTER CONTROL PANEL

29 trial day(s) left.

CONTROL PANEL HOME > WORKER NODES

1 Worker Node(s)

Database: All-In-One: PostgreSQL (10.13) - Log Database: All-In-One: PostgreSQL (10.13)

	Node Name	Version	Status	Management UI
1	tthcitsv01	12.5.9500.51526	Idle	Yes

Support

There is an “Advanced Setting” icon on the page.

DASHBOARD > CLUSTER CONTROL PANEL

18 trial day(s) left.

CONTROL PANEL HOME > WORKER NODES

Advanced Settings

- ☒ Always force SSL on Login
- ☒ Always force SSL for Native Clients
- ☐ Do not follow incoming request DNS
- ☐ Disable worker-node load balancing.

You may have already taken care of the load balancing at a different level (such as the DNS level), so you don't need worker-node load balancing anymore. All the user interactions will stay at the same incoming worker-node.

☒ Per-tenant load balance:  
Always load balance all users belonging to the same tenant to the same node. This works best if you have many tenants.

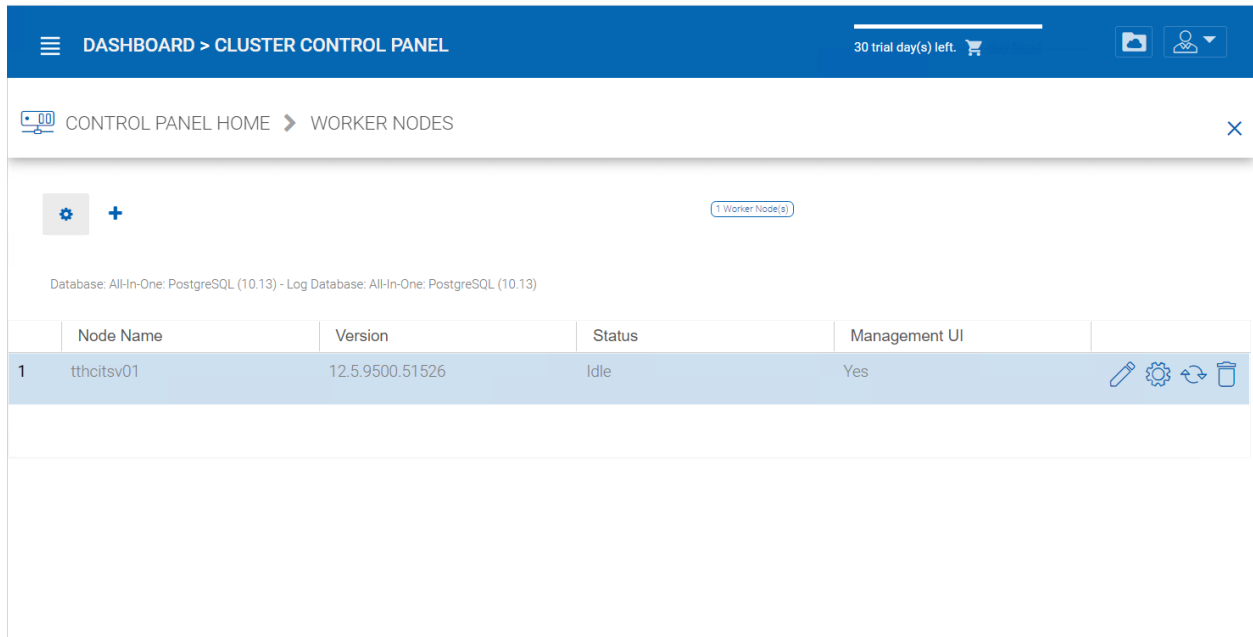
☐ Per-user load balance:  
Load balance users to different nodes regardless whether they belong to the same tenant or not. This works best if you few large tenants.

CLOSE

Now, check “Always force SSL on Login” and “Always force SSL for Native Clients” boxes.

**Warning:** If you use the self-signed SSL certificate, the web portal is the only client that allows you to login after some SSL certificate warning. All other native clients such as Windows, mobile, and Mac clients will reject the connection.





DASHBOARD > CLUSTER CONTROL PANEL

30 trial day(s) left.

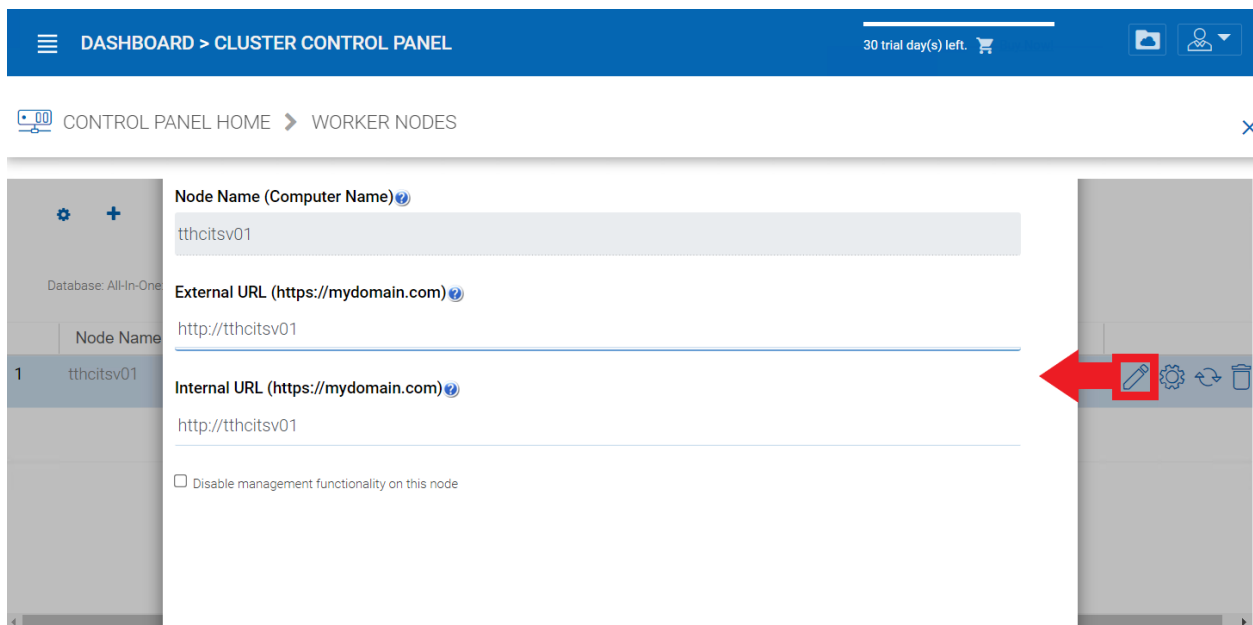
CONTROL PANEL HOME > WORKER NODES

1 Worker Node(s)

Database: All-In-One: PostgreSQL (10.13) - Log Database: All-In-One: PostgreSQL (10.13)

	Node Name	Version	Status	Management UI
1	tthcitsv01	12.5.9500.51526	Idle	Yes

You can also modify the node property for the node.



DASHBOARD > CLUSTER CONTROL PANEL

30 trial day(s) left.

CONTROL PANEL HOME > WORKER NODES

Node Name (Computer Name)

tthcitsv01

External URL (https://mydomain.com)

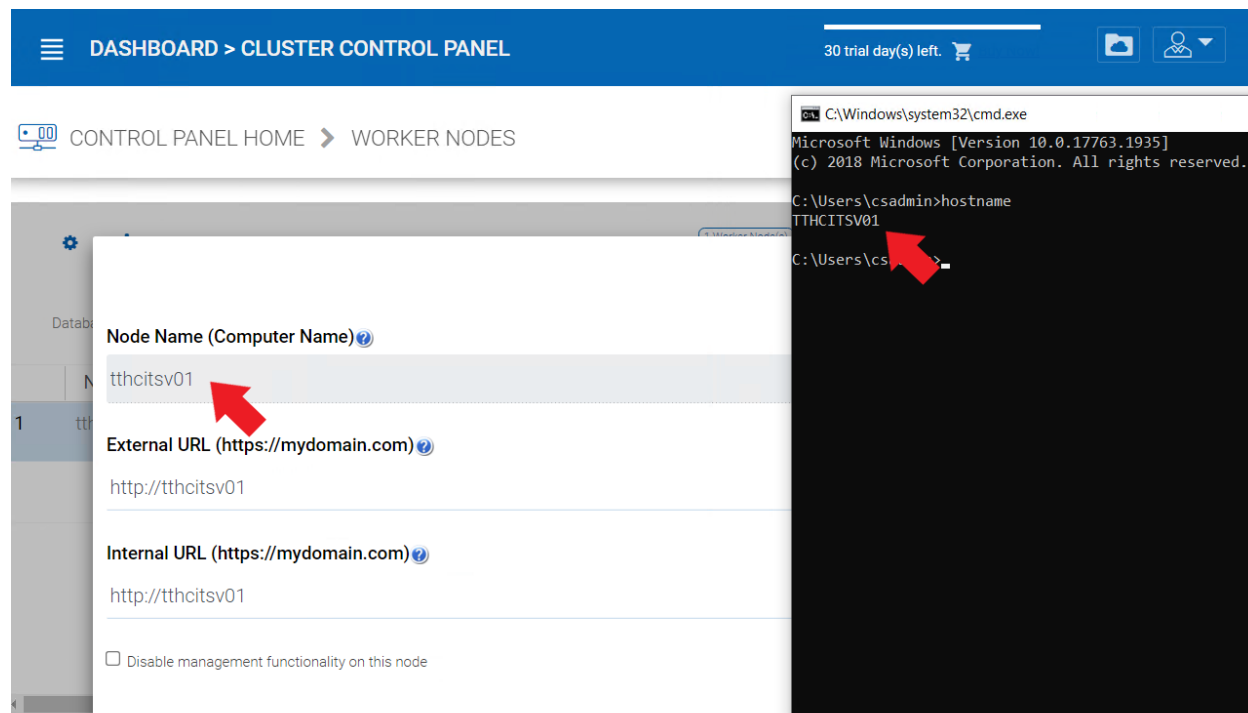
http://tthcitsv01

Internal URL (https://mydomain.com)

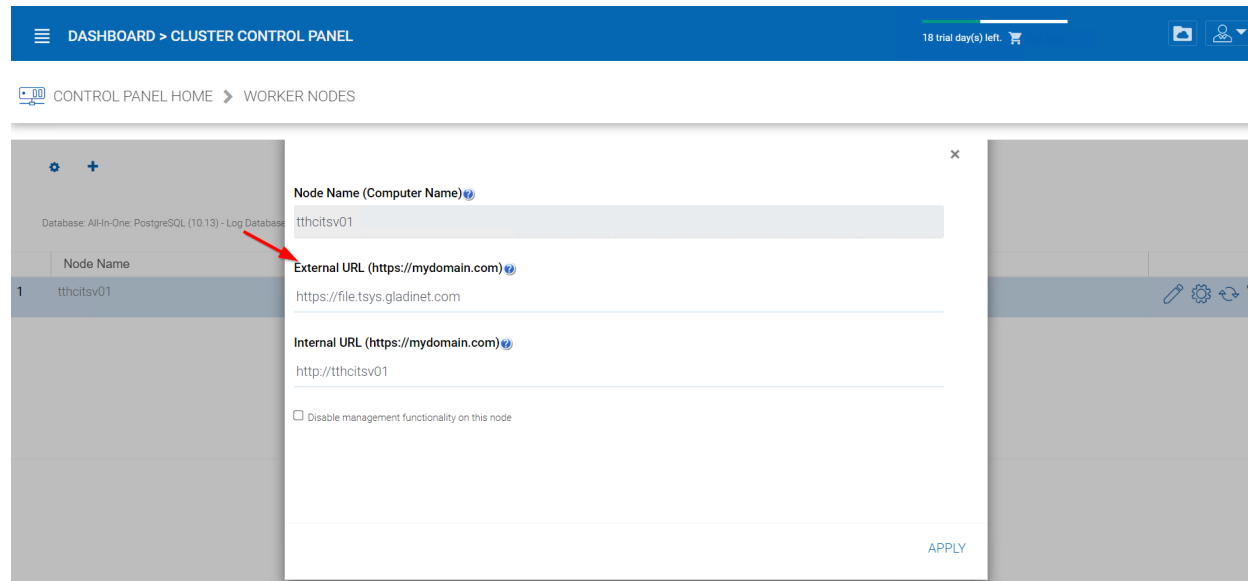
http://tthcitsv01

☐ Disable management functionality on this node

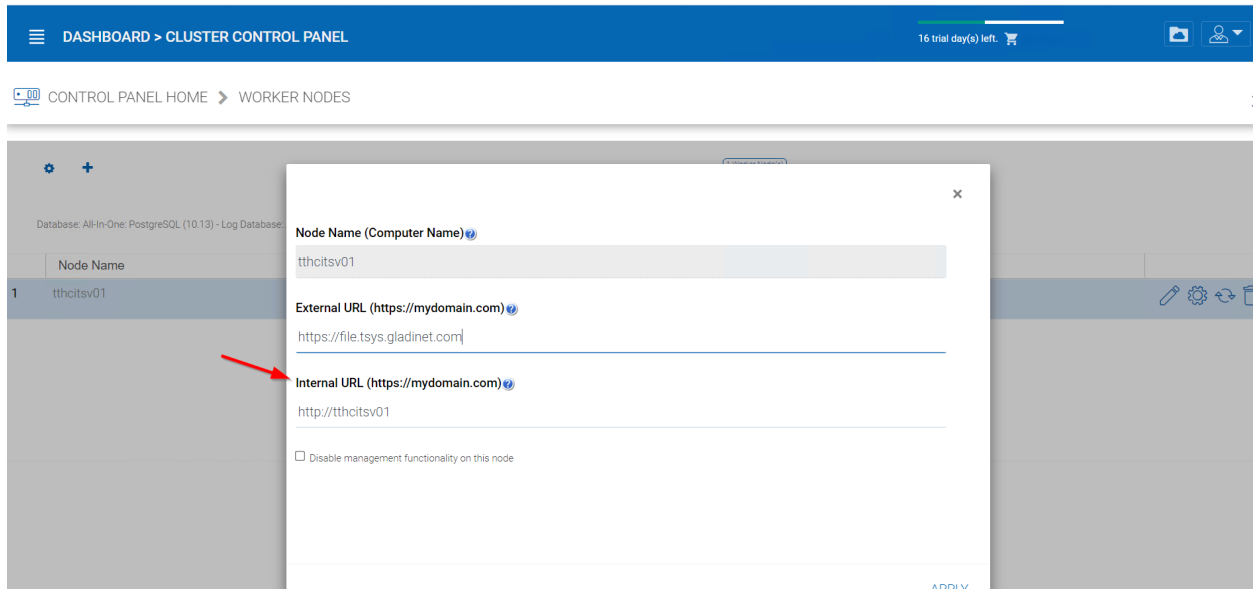
The Node Name needs to match the hostname of the node. You can get the hostname of the node by going into Command Prompt(Press Windows+R and then type in cmd) and typing in hostname.



The External URL should match the external URL for HTTPS. (If you do not have a 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.





---

# 8 Verify External URL, Internal URL and the Node Name

---

## 8.1 Verify External URL

It is very straight forward to verify whether or not your external URL is set correctly. You just need to point your web browser to the external URL and verify that the Login Page shows up and there is no SSL warnings.

You can also verify the External URL by doing a file share to your own email address outside of the CentreStack system. A file sharing invitation will be sent to that Email address. After you receive the Email, click on the link included in the Email and make sure the link points to the External URL.

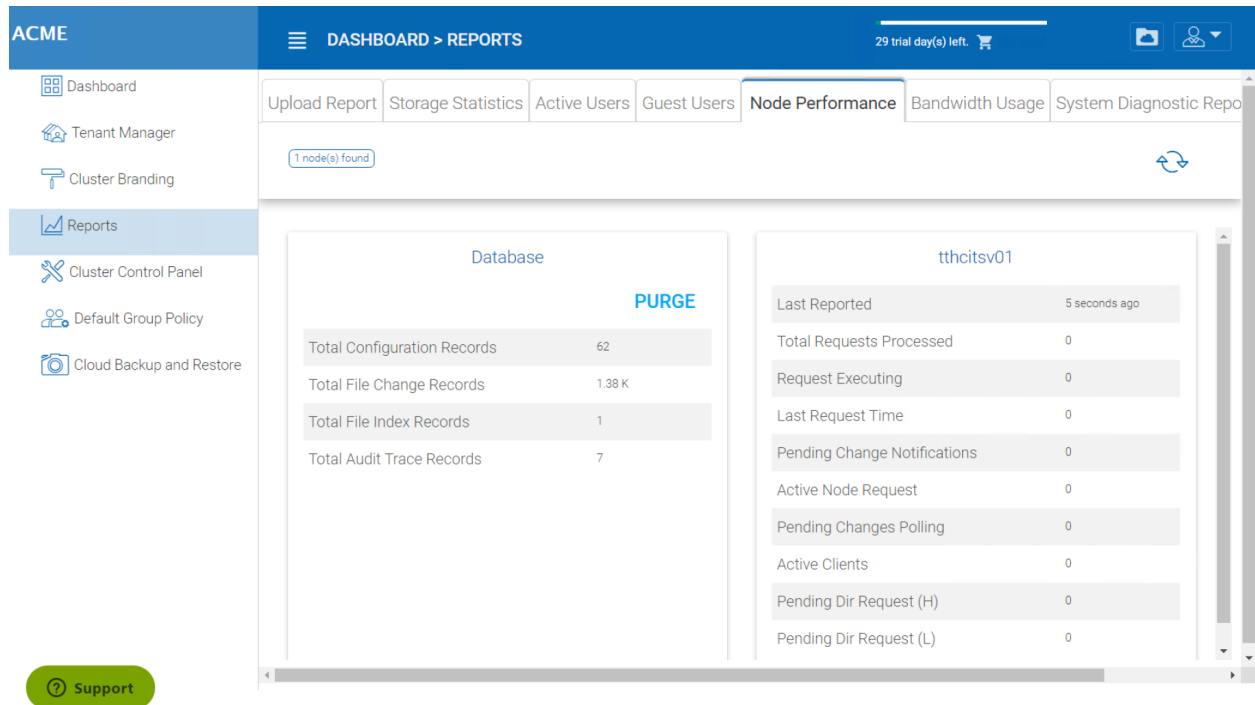
---

**Note:** The external URL is used in the email sharing template. So a simple file sharing test will verify whether the External URL is setup correctly.

---

## 8.2 Verify Internal URL

For the verification of Internal URL, you can use the Node Performance page to make sure the node performance information shows up. (Reports -> Node Performance).



**ACME** DASHBOARD > REPORTS 29 trial day(s) left.

Upload Report Storage Statistics Active Users Guest Users **Node Performance** Bandwidth Usage System Diagnostic Report

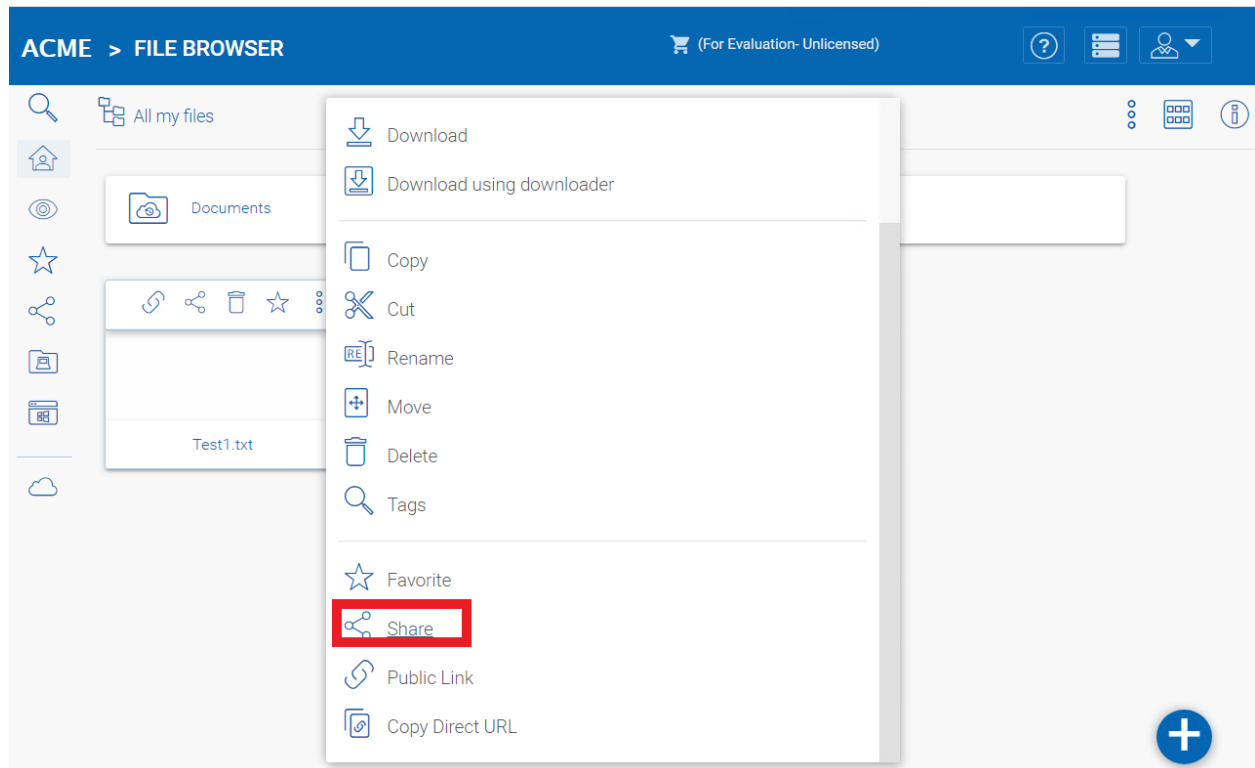
1 node(s) found

Database		tthcitsv01	
PURGE		Last Reported	5 seconds ago
Total Configuration Records	62	Total Requests Processed	0
Total File Change Records	1.38 K	Request Executing	0
Total File Index Records	1	Last Request Time	0
Total Audit Trace Records	7	Pending Change Notifications	0
		Active Node Request	0
		Pending Changes Polling	0
		Active Clients	0
		Pending Dir Request (H)	0
		Pending Dir Request (L)	0

Support

## 8.3 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 has been received and is correctly pointing to an external URL.



**ACME > FILE BROWSER** (For Evaluation- Unlicensed)

All my files

Documents

Test1.txt

- Download
- Download using downloader
- Copy
- Cut
- Rename
- Move
- Delete
- Tags
- Favorite
- Share**
- Public Link
- Copy Direct URL

---

### 9 Add additional CentreStack servers to the cluster

---

Adding an additional CentreStack server is as simple as installing the first CentreStack server. Run the CentreStack server installation program on another server, specifying the same database as the first server in the cluster.

**Warning:** Adding additional CentreStack servers to an existing cluster is optional.

If you only have a few hundred users, you don't need to have a second node from a scalability perspective. The scalability point of adding a second CentreStack Server is at 1000 users. For best practices, you will always scale vertically first such as making a 2-CPU machine into a 4-CPU machine and add RAM to the CentreStack Server before scaling horizontally by adding more CentreStack Servers.

However, from a high availability(HA) perspective, you may want to have a second CentreStack Server.

**Warning:** An external database server should be deployed if you are scaling out the cluster to more than one CentreStack server. The “all-in-one” deployment with a local MySQL database is not intended to be used for scaling out or high availability.

**Warning:** A hardware or software load balancer will be required if more than one CentreStack server is deployed in a cluster.

**Warning:** All CentreStack servers in the same cluster must use the same time zone.



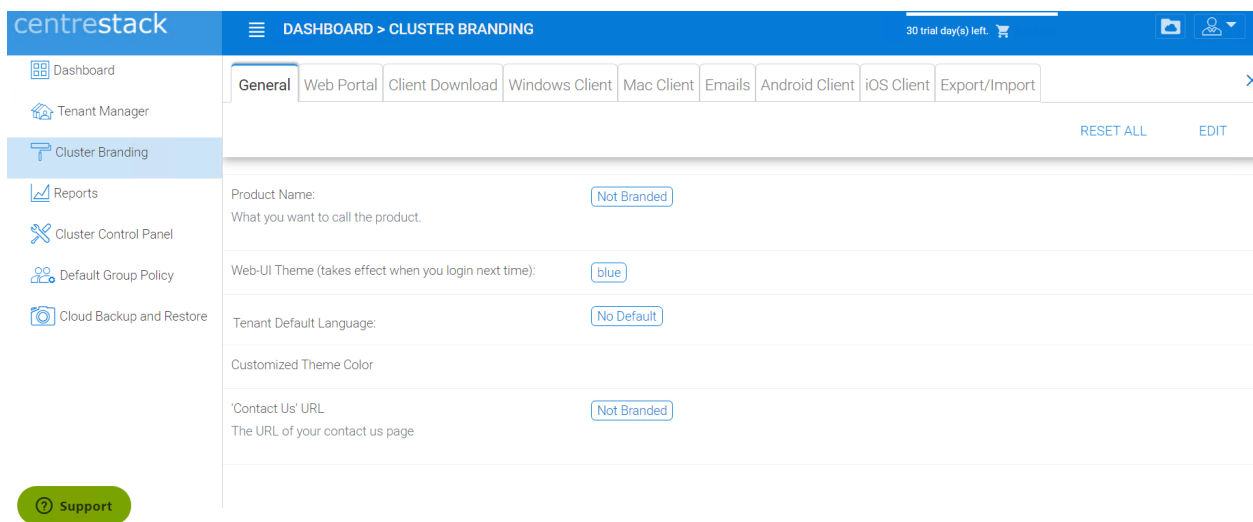


You can brand the web portal, Windows and Mac clients, iOS and Android Applications.

### 10.1 Self-Service Branding

The self-service branding starts with the “Cluster Manager”. In order to start the branding, you will login to the web portal as the Master Administrator.

After you login to the web portal, click to the “Cluster Branding” Pages.



The screenshot shows the CentreStack web portal interface. The top navigation bar is blue with the 'centrestack' logo on the left and a user profile icon on the right. Below the navigation bar is a sidebar menu with icons for Dashboard, Tenant Manager, Cluster Branding (highlighted), Reports, Cluster Control Panel, Default Group Policy, and Cloud Backup and Restore. The main content area is titled 'DASHBOARD > CLUSTER BRANDING' and features a tabbed interface with tabs for General, Web Portal, Client Download, Windows Client, Mac Client, Emails, Android Client, iOS Client, and Export/Import. The 'General' tab is active, displaying a form with the following fields: Product Name (Not Branded), Web-UI Theme (blue), Tenant Default Language (No Default), Customized Theme Color, and 'Contact Us' URL (Not Branded). A 'Support' button is visible in the bottom left corner.

Please reference the “Branding” section in the [Admin Guide](#) for the self-hosted CentreStack server.



# CHAPTER 11

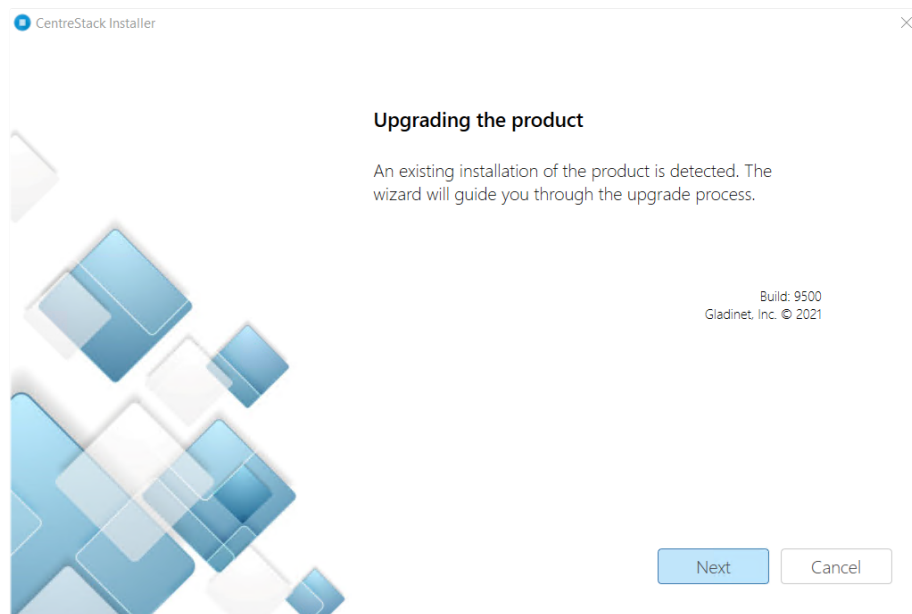
---

## 11 Upgrade CentreStack

---

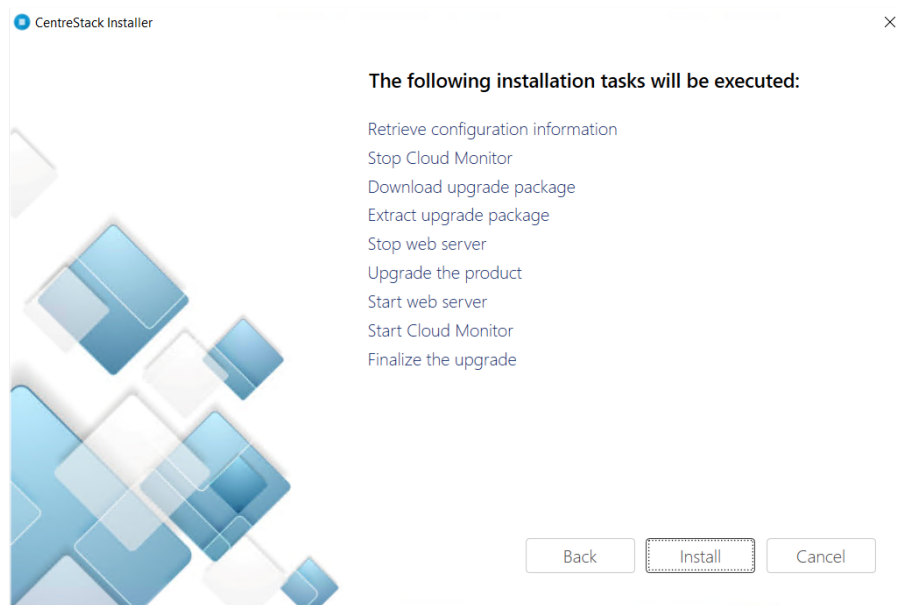
We publish updated notes to our public blog forum called [lprodname Blog](#). It is recommended that you perform an update if your self-hosted CentreStack and clients are three months or older.

### 11.1 Using the GUI Installer to Upgrade



To install an update go to your Partner Portal at <https://www.centrestack.com/management/partnerloginpage.aspx> and

download the GUI installer. When you run the GUI installer, it will detect the existing installation and perform an upgrade.



These advanced topics require changes to the web.config file which is critical for the smooth operation of CentreStack, therefore, it is not recommended that you change the web.config file without first consulting Gladinet support.

### 12.1 Split Database

The database contains two types of information.

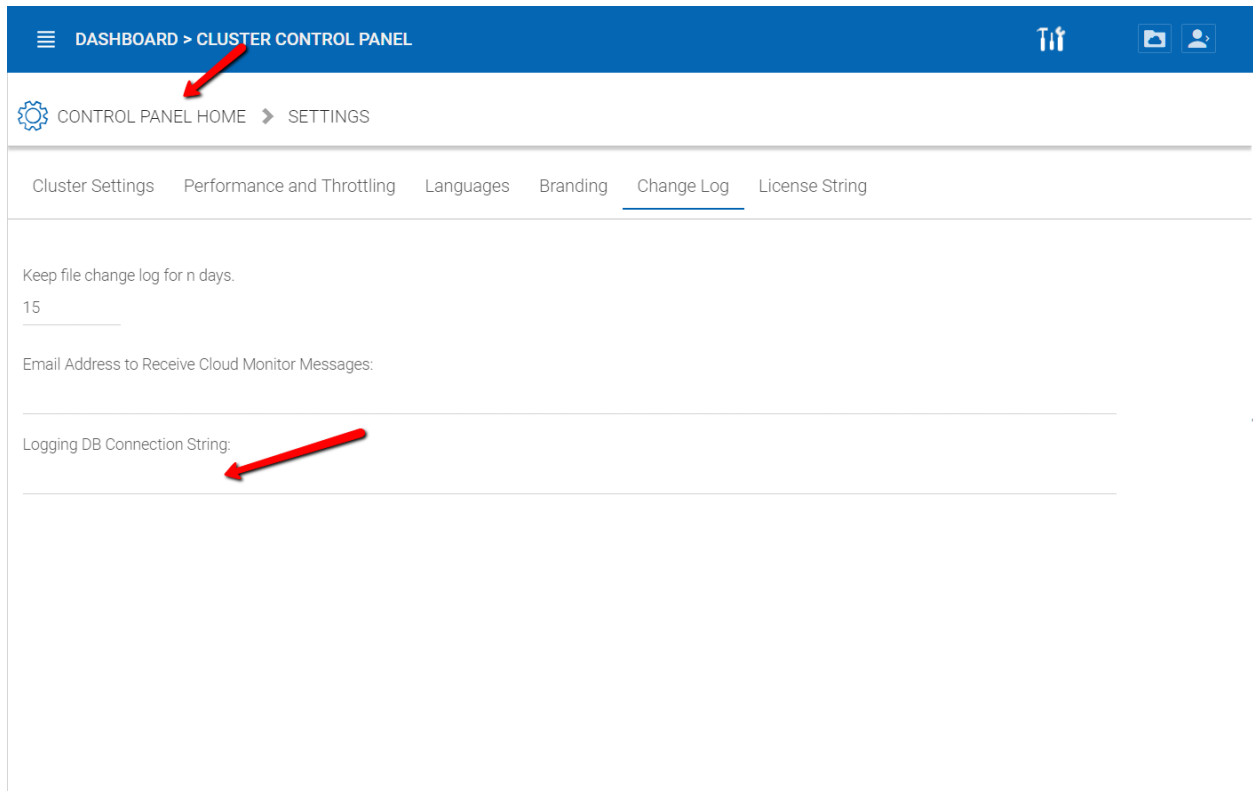
The first type of information is the configuration data that is relatively static. For example, user name, user email, user's published shared files and folder etc. This type of information is relatively small. It can be estimated at 5000 bytes per user. So if you have 2000 users, it can be estimated at 10 MB.

The second type of information is relatively more volatile. For example, the file change log, the audit trace and the file list for index. It can be estimated at 100 file changes per user per day and each file change can be estimated at 1000 bytes for database storage. So for a 15 day (Default change log history), it can be estimated at  $100 * 1000 * 15 = 1.5\text{MB}$  per user for 15 day period. If you need HIPPA compliance, the default change log history can be significantly longer so this part of the database will be much bigger.

For performance and regulatory reasons, it is recommended to split the database into two separate databases, one that contains static information and one that contains relatively more volatile information.

The secondary database (for more volatile data) can be either MySQL Database or Microsoft SQL Database.

To split the database, first create a new database that will be used to store the volatile information. Create a database user and allow this user full access to the database (equivalent to db\_owner). Once the database and user are created, sign into the CentreStack management console as the cluster admin and navigate to Cluster Control Panel > Settings > Change Log. Update the "Logging DB Connection String" setting using an appropriate connection string:



DASHBOARD > CLUSTER CONTROL PANEL

CONTROL PANEL HOME > SETTINGS

Cluster Settings Performance and Throttling Languages Branding Change Log License String

Keep file change log for n days.  
15

Email Address to Receive Cloud Monitor Messages:

Logging DB Connection String:

#### Connection String Example for MySQL Database

```
Server=localhost;Port=3306;Database=gladinet;Uid=root;Pwd=password;
```

#### Connection String Example for Microsoft SQL Database

```
Data Source=server_name;Initial Catalog=logging_db_name;User Id=user_id;Password=user_
password;
```

## 12.2 Change Authentication Algorithm to Version 2

If you have a new installation of CentreStack without any legacy user, we recommend you hard code the authentication algorithm to version 2.

You can locate the web.config file in the root folder of the installation directory (same web.config file as referenced in the previous section) and add a line inside the <appSettings file="branding.config"> section.

```
<add key="sys_access_ver" value="2" />
```

## 12.3 Change the Synchronized Uploader to Asynchronized Uploader

Under the C:\Program Files (x86)\CentreStack(or the installation directory), look into the UploadDownloadProxy and identify the web.config file. Find the line with the SyncedStorageProxiedPutUploadHandler and change it to StorageProxiedPutUploadHandler.

This optimization might not work on all systems, therefore, it is recommend you test web portal Drag and Drop upload after you make the change. If it does not work for your IIS, you can revert the change back or consult Gladinet support.

```
<add name="storageuploadex" path="proxiedupload.up" verb="PUT"
type="GladinetStorage.SyncedStorageProxiedPutUploadHandler"
resourceType="Unspecified" precondition="integratedMode" />
```

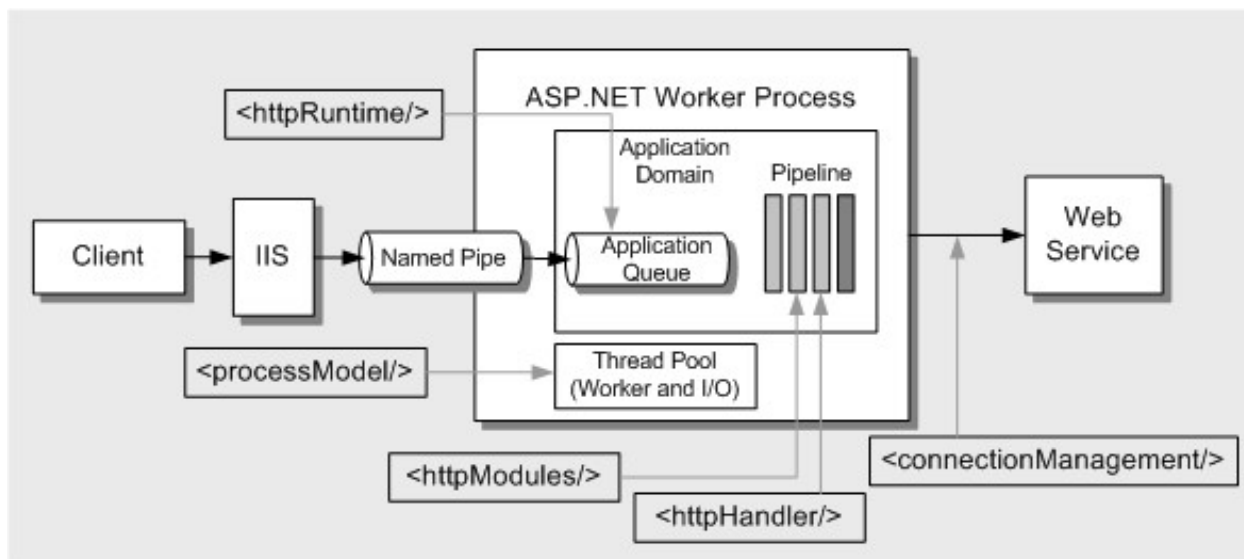
## 12.4 Zone Support

If you have two independent CentreStack clusters, for example, one cluster in US and one cluster in UK, you can use the zone support to connect the two clusters together. The advantage of using zones is the end user login request will automatically be redirected to the zone the user belongs to.

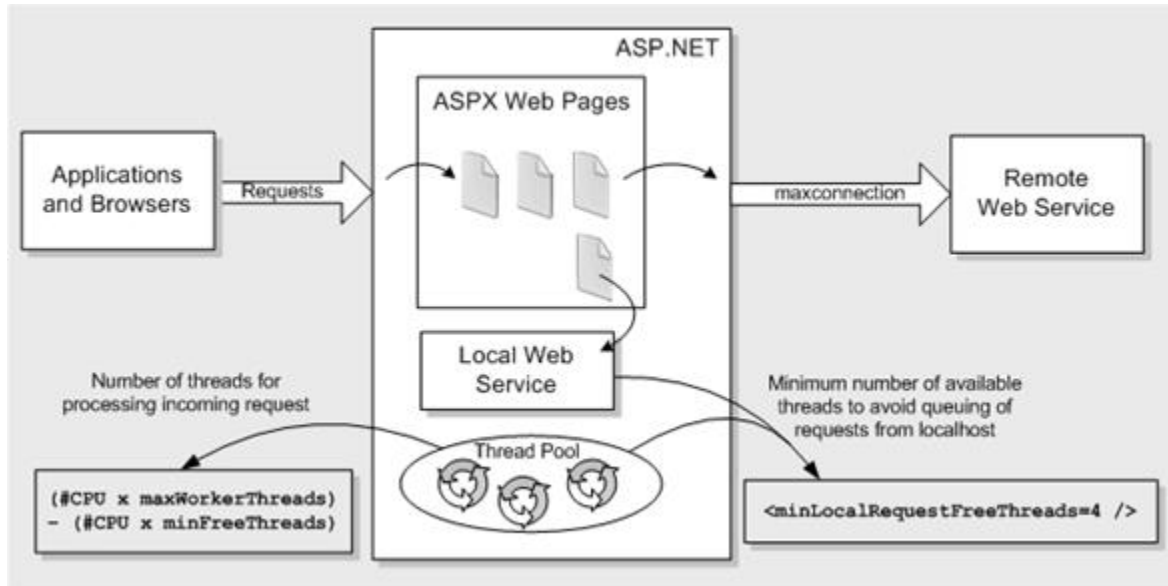
## 12.5 Scalability Tuning

CentreStack is built on top of ASP.NET and WCF. By default, both ASP.NET and WCF has throttle control parameters that we can tune and remove. Please reference this MSDN article for performance tuning:

<http://msdn.microsoft.com/en-us/library/ff647813.aspx>



(image source: <http://msdn.microsoft.com/en-us/library/ff647813.aspx>)



(image source: <http://msdn.microsoft.com/en-us/library/ff647813.aspx>)

### 12.5.1 Tuning #1 – namespace/web.config

There are three parameters about max concurrent calls, concurrent sessions and concurrent instances.

```
<serviceThrottling
  maxConcurrentCalls="100"
  maxConcurrentSessions="100"
  maxConcurrentInstances="1000" />
```

This is set in the `<CENTRESTACKInstallDir>\namespace\web.config` file

There may be existing blocks of `serviceBehaviors` and `behavior` blocks there. You can simply add the `serviceThrottling` block.

```
<serviceBehaviors>
  <behavior name="WcfWebService.Service1Behavior">
    <serviceThrottling
      maxConcurrentCalls="100"
      maxConcurrentSessions="100"
      maxConcurrentInstances="1000" />
    </behavior>
  </serviceBehaviors>
```

### 12.5.2 Tuning #2 – aspnet.config

The `aspnet.config` is under `c:\windows\Microsoft.NET\Framework64\v4.0.30319`

`system.web` is an element of `<configuration>` so you can add it inside the `<configuration>` block.

```
<system.web>
  <applicationPool
    maxConcurrentRequestsPerCPU="5000"
```

(continues on next page)



(continued from previous page)

```
requestQueueLimit="20000"/>
</system.web>
```

### 12.5.3 Tuning #3 – machine.config

Machine.config is at %windir%\Microsoft.NET\Framework64\[version]\config\machine.config

(%windir% typically is c:\windows. [version] is 4.0.30319 for .NET framework 4)

#### processModel

processModel is under <system.web> and <system.web> is under <configuration>. Most likely the processModel block is there already but with autoConfig set to true. We can change it to set to false and with the attributes set below.

```
<processModel
  autoConfig="false"
  maxWorkerThreads="500"
  maxIoThreads="500"
  minWorkerThreads="2"/>
```

#### connectionManagement

<system.net> is a block below <configuration>. Typically if <system.net> doesn't already exist, the block can be added to the bottom of the config file, right before the closing tag of <configuration>.

```
<system.net>
  <connectionManagement>
    <add address="*" maxconnection="20000"/>
  </connectionManagement>
</system.net>
```

### 12.5.4 Tuning #4 – appConcurrentRequestLimit

```
appcmd.exe set config /section:serverRuntime /appConcurrentRequestLimit:50000
```

## 12.6 Need More Information?

Contact Gladinet Support ([support@gladinet.com](mailto:support@gladinet.com)) for more information.



## CHAPTER 13

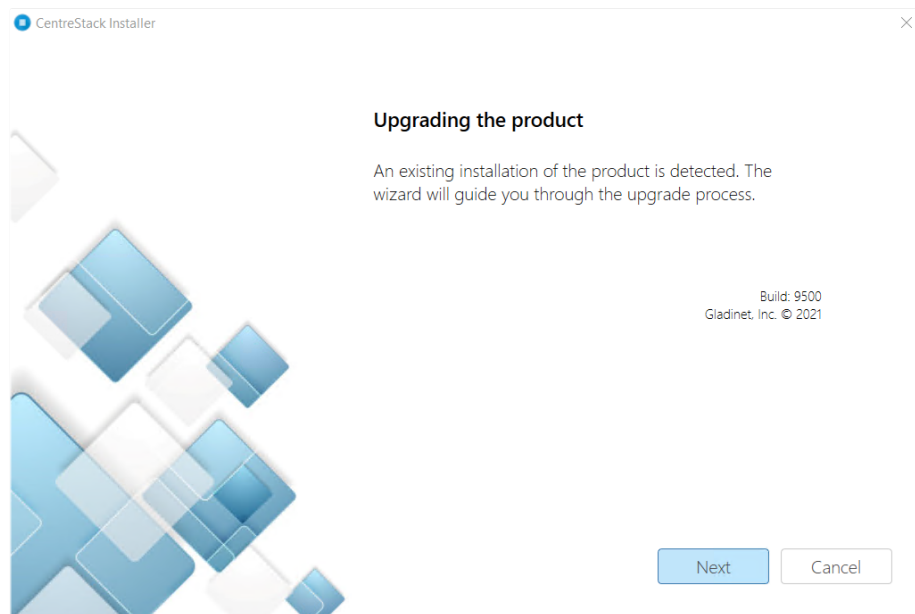
---

### Upgrade CentreStack

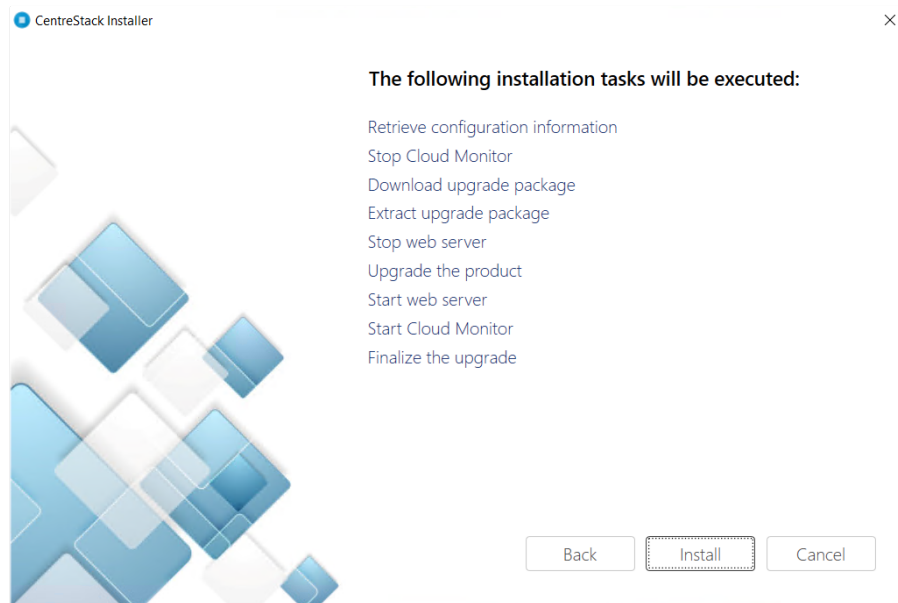
---

We publish updated notes to our public blog forum called [CentreStack Blog](#). It is recommended that you perform an update if your self-hosted CentreStack and clients are three months or older.

#### 13.1 Using the GUI Installer to Upgrade



To install an update go to your [Partner Portal](#) and download the GUI installer. When you run the GUI installer, it will detect the existing installation and perform an upgrade.



## CHAPTER 14

---

### Indices and tables

---

- `genindex`
- `modindex`
- `search`