

---

# **CentreStack Administration Guide Documentation**

***Release 12.2.9413.50838***

**Gladinet, Inc.**

**May 04, 2023**



---

## Contents

---

<b>1</b>	<b>Getting Started</b>	<b>3</b>
1.1	Introduction . . . . .	3
1.2	Overview . . . . .	3
<b>2</b>	<b>Administration Scope</b>	<b>5</b>
2.1	Management . . . . .	5
2.2	Partner Portal . . . . .	6
2.3	Self-Hosted CentreStack . . . . .	6
2.4	Cluster Administrator . . . . .	6
2.5	Tenant Administrator . . . . .	7
<b>3</b>	<b>Cluster Administration</b>	<b>9</b>
3.1	The Basics . . . . .	9
3.2	Tenant Manager . . . . .	12
3.2.1	Create a New Tenant . . . . .	14
3.3	Cluster Branding . . . . .	21
3.3.1	General . . . . .	24
3.3.2	Web Portal . . . . .	27
3.3.3	Client Download . . . . .	28
3.3.4	Windows Client . . . . .	28
3.3.5	Mac Client . . . . .	30
3.3.6	Emails . . . . .	32
3.3.7	Android Client . . . . .	33
3.3.8	iOS Client . . . . .	34
3.3.9	Export/Import . . . . .	34
3.4	Reports . . . . .	34
3.4.1	Upload Report . . . . .	34
3.4.2	Storage Statistics . . . . .	36
3.4.3	Active Users . . . . .	36
3.4.4	Guest Users . . . . .	36
3.4.5	Node Performance . . . . .	36
3.4.6	Bandwidth Usage . . . . .	38
3.4.7	System Diagnostic Report . . . . .	38
3.4.8	Audit Trace . . . . .	38
3.5	Cluster Control Panel . . . . .	38
3.5.1	Cluster Admin . . . . .	38
3.5.2	Email Service . . . . .	40

3.5.3	Application Manager . . . . .	41
3.5.4	Storage Manager . . . . .	43
3.5.5	Client Version Manager . . . . .	49
3.5.6	Settings . . . . .	52
3.5.6.1	Cluster Settings . . . . .	52
3.5.6.2	Performance and Throttling . . . . .	55
3.5.6.3	Timeouts and Limits . . . . .	56
3.5.6.4	Languages . . . . .	56
3.5.6.5	Branding . . . . .	56
3.5.6.6	Change Log . . . . .	58
3.5.6.7	License String . . . . .	59
3.5.7	Anti Virus . . . . .	59
3.5.8	Worker Nodes . . . . .	60
3.5.9	Web Node . . . . .	65
3.5.10	Zones . . . . .	66
3.6	Default Group Policy . . . . .	66
<b>4</b>	<b>Tenant Administration</b> . . . . .	<b>69</b>
4.1	Tenant Dashboard . . . . .	70
4.2	Cloud Backup . . . . .	70
4.3	Active Directory . . . . .	73
4.3.1	Local Active Directory . . . . .	73
4.3.2	Remote Active Directory . . . . .	74
4.4	Backend Storage . . . . .	74
4.4.1	Home Storage . . . . .	74
4.4.2	Attach Storage . . . . .	77
4.4.2.1	File Servers . . . . .	77
4.4.2.2	Local Storage . . . . .	79
4.4.2.3	Cloud Storage . . . . .	80
4.4.3	Migrate to New Storage . . . . .	82
4.5	Tenant Plan . . . . .	82
4.6	Access Control . . . . .	83
4.7	Control Panel . . . . .	85
4.7.1	Administrator Information . . . . .	85
4.7.2	Notifications . . . . .	87
4.7.2.1	Settings . . . . .	87
4.7.2.2	Shared File/Folder . . . . .	89
4.7.2.3	Team Folder . . . . .	89
4.7.3	Active Directory . . . . .	90
4.7.3.1	AD Server . . . . .	90
4.7.3.2	Advanced Settings . . . . .	90
4.7.4	Device Manager . . . . .	93
4.7.5	Application Manager . . . . .	93
4.7.6	Background Tasks . . . . .	94
4.8	User Management . . . . .	94
4.8.1	Regular User . . . . .	94
4.8.2	Guest User . . . . .	99
4.8.3	Group Manager . . . . .	99
4.8.4	Role Manager . . . . .	99
4.9	Team Folders . . . . .	103
4.9.1	Create Team Folder . . . . .	103
4.9.2	Team Folder Information . . . . .	110
4.9.3	Collaborators . . . . .	110
4.9.4	External Sharing . . . . .	110



4.9.5	Access Policy . . . . .	110
4.9.6	Folder Permissions . . . . .	114
4.9.7	Settings . . . . .	114
4.10	Group Policy . . . . .	117
4.10.1	Common Settings . . . . .	117
4.10.1.1	Security . . . . .	117
4.10.1.2	Sharing . . . . .	120
4.10.1.3	File Locking . . . . .	123
4.10.1.4	Client Settings Manager . . . . .	125
4.10.1.4.1	Sync Throttle . . . . .	125
4.10.1.4.2	Scheduled Sync . . . . .	127
4.10.1.4.3	Mapped Drive Control . . . . .	127
4.10.1.4.4	Large File Upload . . . . .	129
4.10.1.4.5	Endpoint Protection . . . . .	130
4.10.1.4.6	Bandwidth Control . . . . .	131
4.10.1.4.7	Outlook Plugin . . . . .	131
4.10.1.4.8	Client Startup Script . . . . .	132
4.10.1.4.9	Client Shutdown Script . . . . .	132
4.10.1.4.10	Mac Client Settings . . . . .	132
4.10.1.5	Retention Policy . . . . .	132
4.10.1.6	Anti Virus . . . . .	134
4.10.2	Account & Login . . . . .	136
4.10.2.1	User Account Settings . . . . .	136
4.10.2.1.1	Guest User . . . . .	136
4.10.2.1.2	Account Info . . . . .	136
4.10.2.1.3	2-Step Verification . . . . .	138
4.10.2.1.4	Login Control . . . . .	139
4.10.2.2	Password Policy . . . . .	140
4.10.2.3	Single Sign-On . . . . .	140
4.10.2.4	Azure AD . . . . .	146
4.10.3	Folder & Storage . . . . .	146
4.10.3.1	Home Directory . . . . .	150
4.10.3.2	Folder and Storage . . . . .	152
4.10.3.3	Attached Folder . . . . .	153
4.10.3.4	Filters . . . . .	155
4.10.4	Client Control . . . . .	156
4.10.4.1	Web Portal . . . . .	156
4.10.4.2	Native Client . . . . .	158
4.10.5	Export/Import . . . . .	160
4.11	Tenant Branding . . . . .	160
4.12	Reports . . . . .	162
4.12.1	Upload Report . . . . .	165
4.12.2	Storage Statistics . . . . .	165
4.12.3	Bandwidth Usage . . . . .	165
4.12.4	Team Folders . . . . .	165
4.12.5	Shared Objects . . . . .	165
4.12.6	Audit Trace . . . . .	165
4.12.7	File Change Log . . . . .	165
4.12.8	Folder Permissions . . . . .	165
4.12.9	Distributed Locks . . . . .	165
4.12.10	Pending Purged Folder . . . . .	165

<b>5</b>	<b>Advanced Topics . . . . .</b>	<b>167</b>
5.1	Connect Your File Server . . . . .	167

5.2	Files and Folder Permission . . . . .	167
5.3	Setting up Active Directory . . . . .	171
5.3.1	AD account auto provision . . . . .	171
5.3.2	AD account auto provision, limiting to Organization Unit . . . . .	172
5.3.3	AD account auto provision, limiting to a specific AD group. . . . .	172
5.4	Setting up Offline Folder . . . . .	174
5.4.1	Team Folder Offline Settings . . . . .	174
5.4.2	User Offline Settings . . . . .	174
5.4.3	User Manual Offline Settings . . . . .	176
5.4.4	Summary . . . . .	176
<b>6</b>	<b>Cloud Backup</b>	<b>179</b>
6.1	Enabling Cloud Backup . . . . .	181
6.2	Cloud Backup for Team Folders . . . . .	183
6.2.1	Enabling Cloud Backup for Team Folders . . . . .	183
6.2.2	Cloud Backup Snapshots . . . . .	183
6.2.3	Disabling Cloud Backup for Team Folders . . . . .	186
6.3	Cloud Backup for Endpoint Devices . . . . .	186
6.3.1	Create a Device Backup Profile . . . . .	187
6.3.2	Configure Devices for Backup . . . . .	187
6.3.3	Restoring from Device Backups . . . . .	187
6.4	Cloud Backup Access . . . . .	191
6.5	Cloud Backup Settings . . . . .	196
6.5.1	Enable Device Backup for All Users . . . . .	196
6.5.2	Change Backup Storage . . . . .	198
6.5.3	Disable Backup to the Remote Backup Server . . . . .	198
6.5.4	Filters for Files and Folders . . . . .	199
6.5.5	Cloud Backup Schedules . . . . .	199
6.5.6	Device Backup Profiles . . . . .	199
6.5.7	Cloud Backup Bandwidth Control . . . . .	202
6.5.8	Cloud Backup Retention Policies . . . . .	203
<b>7</b>	<b>Indices and tables</b>	<b>205</b>

Contents:



### 1.1 Introduction

Welcome to the CentreStack Administration Guide. This guide describes administration tasks for CentreStack, the mobile access and secure file sharing solution that focuses on local file server cloud-enablement.

CentreStack runs on the Windows Server platform and includes client agent software applications for Microsoft Windows, Mac OS X, and Mobile Clients for the Android and Apple iOS operating systems.

---

**Important:** CentreStack includes a client application for Windows File Server, which is named “Server Agent”. This document is about CentreStack itself, not about the “Server Agent”.

---

**Attention:** This admin guide is written for CentreStack version 12.2.9413.50838

### 1.2 Overview

CentreStack is a mobile access and secure file sharing solution. It differentiates itself from other File Sync and Share solutions by focusing on data security, permission controls and, file server cloud-enablements including data protection and cloud migration. CentreStack surpasses the competition in the following areas:

1. Maintaining Active Directory, security and NTFS permissions on files and folders.
2. Providing live time sync-and-share with versioning and revision controls.
3. Providing On-Demand access that honors Read-Only, and Write permissions in Real-Time.
4. Mirroring of local network shares for Team Collaboration in the Cloud.
5. Provide drive mapping and file locking functionality for files in the Cloud.

CentreStack is a software solution built on top of the Microsoft Web Platform. It provides file access and sharing functionality from PCs, Macs, File Servers, Web Browsers, and Mobile Devices. In addition, it also brings data protection and cloud migration features.

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

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

See also: [File Server Remote Access](#)

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

Please reference the “[Installation Checklist](#)” as well as the “[Installation Guide](#)” for information on how to setup and deploy CentreStack. This guide is focused on the administration of CentreStack.

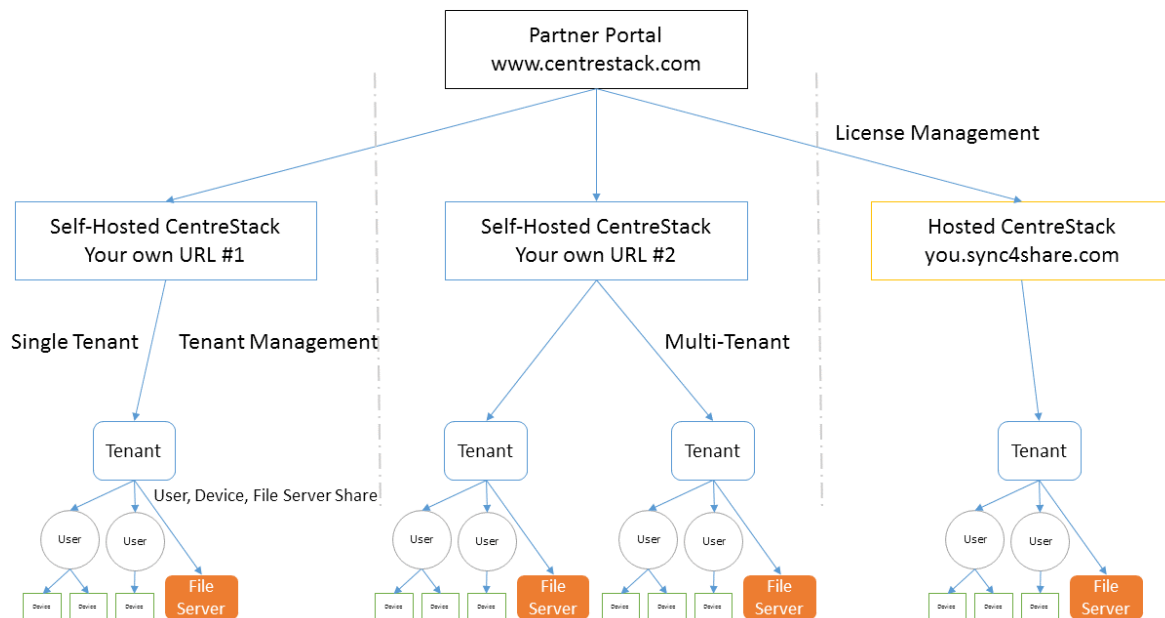
---

**Note:** This Administration Guide is for the Self-Hosted CentreStack. For Hosted-CentreStack, please reference the Hosted CentreStack Admin Guide.

---

### 2.1 Management

In CentreStack, objects that can be managed are defined in the following picture. You can manage objects at different levels from one single management portal.



## 2.2 Partner Portal

The Partner Portal is used primarily for managing licenses and licenses distribution amongst all of your CentreStack Servers.

The partner portal is located at <https://www.centrestack.com>, and you can login through here: <https://www.centrestack.com/management/partnerloginpage.aspx>. From the Partner Portal you can download the CentreStack software as well as manage the licensing of your Servers.

---

**Tip:** Commonly, you will download the CentreStack software, set it up and leverage the built-in 30 day trial time to finish the setup. Towards the end of the trial, you assign licenses from the partner portal to your Server and activate it into a production environment.

---

Both Self-Hosted Servers and Hosted CentreStack Tenants (sync4share) can be managed via the Partner Portal.

## 2.3 Self-Hosted CentreStack

In the User Interface, the Self-Hosted CentreStack instance is referred to as a Cluster or a Server Farm. A Cluster can be as small as a single Server or scaled out to include multiple Servers in a Server farm.

### Hosted CentreStack

In the Partner Portal, you can also manage tenants which are hosted by CentreStack (sync4share). This document doesn't cover Hosted CentreStack. Please refer to the Hosted CentreStack Administration Guide (<https://www.centrestack.com/Library/HostedCentreStackGuide/index.html>) for more information on hosted options.

### Tenants

In a CentreStack management interface, most of the time you are managing tenants. It can be a single tenant when deployed for a single company, or it can be multiple tenants. A tenant is a management and billing scope that includes a number of users and a specific amount of storage. It normally maps to a company or a client of yours.

### Users, Devices, File Server Shares

In each tenant, the objects you manage include Users and Devices as well as File Server Network Shares for Team Folder collaboration (Team Shares).

This document is focused on the management scope for a Self-Hosted CentreStack. In the server management interface, there are two administration scopes: Cluster Administrator and Tenant Administrator.

## 2.4 Cluster Administrator

The Cluster Administrator can manage cluster-wide functionalities, such as email SMTP server setup and worker node properties etc.

In the Deployment Guide, the Cluster Administrator is often referred to as the Master Admin, Root Admin, or just Server Administrator. Even though the Cluster Server Farm can have multiple Servers, most of the time, a server-farm with one single server is sufficient for your use case and your user base.



## 2.5 Tenant Administrator

Tenant Administrator can manage Tenant-Wide functionalities, such as Group Policies. The Cluster Admin is also a Tenant Admin for the very first Tenant (Default Tenant) so the Cluster Administrator manages both Cluster Administration and Tenant Administration (for the default tenant). In the multiple-tenant case, each Tenant Administrator will be responsible for the Tenant's administration scope.

The Cluster Administrator by default can help each Tenant Administrator manage at the tenant level.

In real-world scenarios, the tenant is often mapped to an organization; a client of an MSP or a customer that has many employees.

There are two icons related to cluster administration and tenant administration:

- Cluster Manager icon



- Tenant Manager icon



---

**Hint:** Tenant(s) usually map to your organization(s) or client(s).

If you are logged in as the Default Cluster Admin, you will manage the tenant-level scope from the “Tenant Manager” instead of using the “Tenant Manager icon”.

---

---

**Note:** 1: All the administration work is performed via the web portal inside a web browser. Recommended browsers include Google Chrome first, followed by Firefox, Internet Explorer, Safari, and Opera. (Internet Explorer requires version 9 and above and includes Microsoft Edge Browser)

2: The very first user who installed the Cluster Server is also the Cluster Admin and Tenant Admin for the Default Tenant. In order for the Cluster Admin to be familiar with the tenant functionality, the Cluster Admin is provided a small 3-user default account (Tenant Account).

3: You can start the administration work at any time by pointing your web browser to the Cluster Server's IP Address or DNS name. If you are on the Cluster Server console, you can even use <http://localhost> to get started.

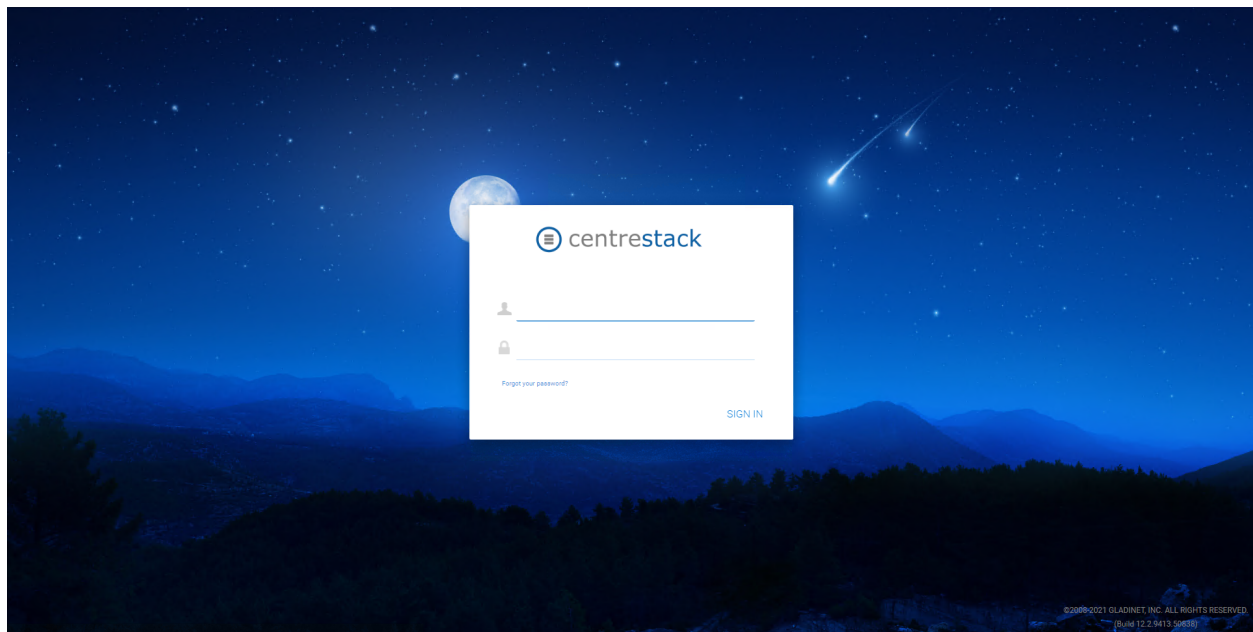
---



### 3.1 The Basics

To access your Cluster Administration features, log in to the Web Portal on the server. **The description in this guide presumes that you are signed in as the Master Administrator** (aka., Cluster Administrator, Server Administrator). Some of the options listed may not be available if you are logged in with different permissions (e.g. Delegated Administrator). In this document the CentreStack will also be referred to as simply, Cluster Server.

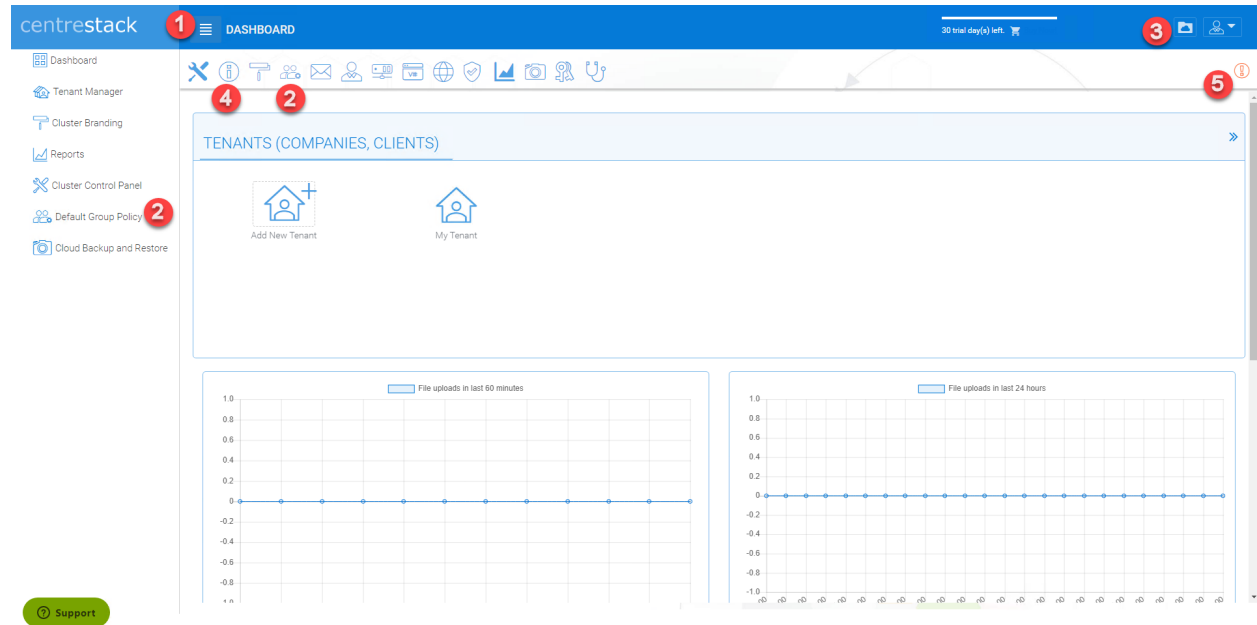
**Tip:** The Web Portal URL is the server's DNS name, the IP Address or local host if you are on the server console.



## LOGIN SCREEN

**Note:** At the bottom of the Login screen, there is version information, which will be useful to see which version you have installed.

The following graphic describes the various icons and components of the Administrator Dashboard and its sub-sections. Please refer to it as you read this guide to determine how to access various features.



## CLUSTER MANAGER DASHBOARD

After logging in, you will see the Cluster Manager Dashboard. The small “hamburger” menu icon (1) in the top left corner of this portal page will toggle the reveal of the left-side menu.

Some of the features can be accessed in several ways; for instance, you can see the **Default Group Policy** icon (2) in both the left-side menu and the Cluster Control Panel on the right side (or top side) of the Dashboard.

By clicking the folder icon (3) In the top right of the interface you can toggle between the File Browser and Cluster Manager views. The **File Browser** (My Files) view of the interface gives you access to your shared and unshared folders. This is also where you can create folders and upload files and folders for access. When the cluster administrator clicks the folder icon to get into the files and folder’s view, the files and folders belong to the default tenant.

**Note:** the cluster administrator will not be able to access files and folders that are not in the scope of the default tenant. To access files and folders that belong to a specific tenant, the web portal login has to be that of the tenant. So basically the cluster administrator can do administration work for a tenant that is under management. However, it is not easy for the cluster administrator to see the files and folders for that specific tenant until he/she gets the permission and the login credentials.

The Cluster Manager (aka., Dashboard) allows you to manage Tenants, Cluster Branding, Reports, Cluster Control Panel, and Group Policies. If you need to know the version and cluster ID information for your Cluster Manager installation, this can be accessed by clicking the “i” (4). The following image represents the Cluster Info pop-up window.

## CLUSTER INFO

Cluster Id: [00/20T9tNjmh8WKR7ICba2JzL78N4CVOH39wEz4TU58bPmuJVy5sPn+NsitMo2bk](#)

Version: [12.2.9413.50838](#)



CLOSE

In the center of the Dashboard screen, you can access your Tenants (Companies, Clients) and system reports.

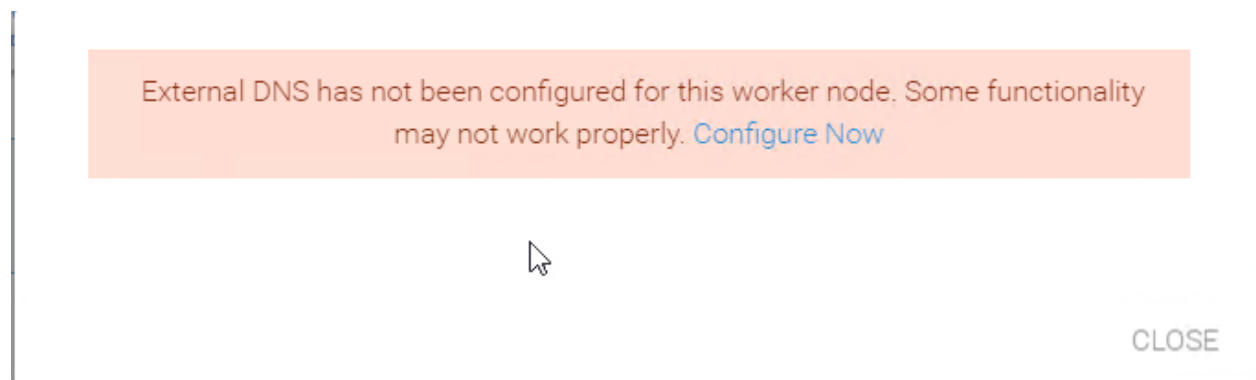
---

**Note:** At a high level, the CentreStack web browser management interface allows you to manage clients (Tenants) and the overall system performance and statistics reports.

---

### EXTERNAL DNS WARNING

At the top left corner of the cluster dashboard (5), if you see a warning icon, it is the external dns warning indicating the external dns name is not setup yet.



External DNS (External URL) is a very important property. It is used in directing how outside remote clients connect to the Cluster Server. It is also used in various email templates. If this property is not properly configured, the email template may be using IP address or NETBIOS name as the URL link.

To configure this setting, you must have a DNS name and SSL certificate setup; therefore, you can postpone the configuration of your DNS until you are ready.

#### Related tasks

- Configure the DNS registration to point a DNS name to the public static IP address of the Cluster Server.
- Configure the IIS “Default Web Site” to bind to an SSL certificate.

## 3.2 Tenant Manager

Cluster Manager > Tenant Manager

---

**Note:** A tenant is usually mapped to a client of yours, a company, or a division of a company.

---

The Cluster Server is multi-tenant capable, but can also be used for a single Tenant. To add or manage your tenants, choose Tenant Manager (1) in your Dashboard.

You can also access other important settings from this context menu (2) (Each tenant block has a tenant specific context menu):

- Manage Tenant
- Force full scan for storage quota usage,
- Change Tenant Admin Password,
- Edit Existing Default Storage

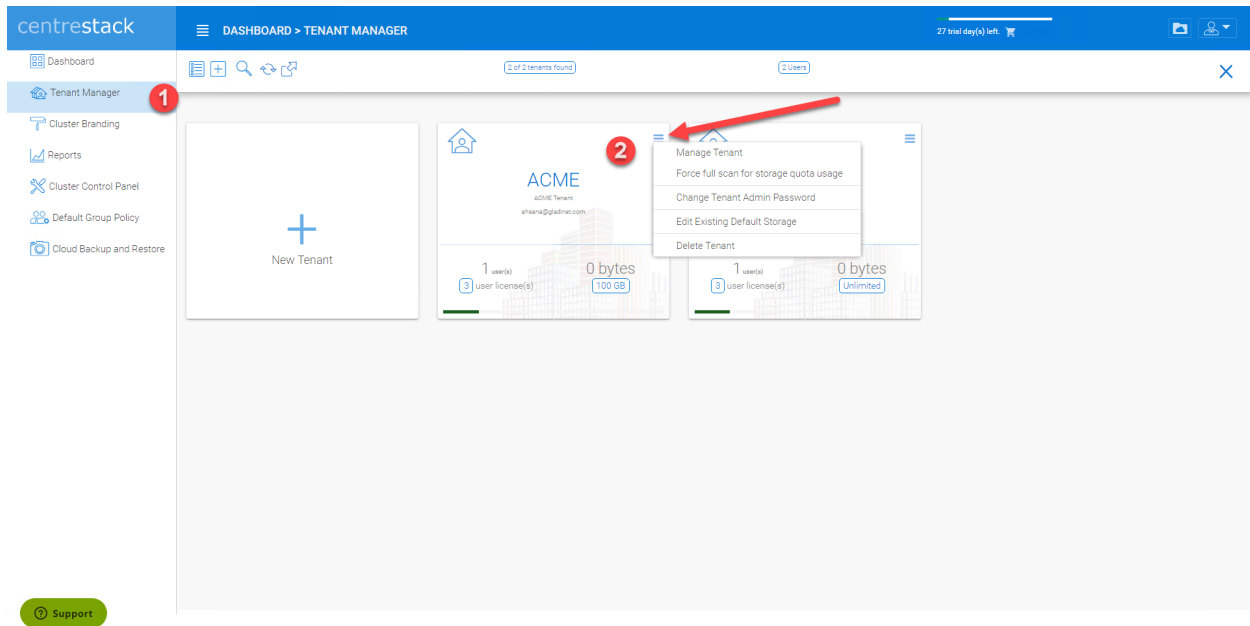


Fig. 1: TENANT MANAGER

- Delete Tenant

### Manage Tenant

This will drill deeper into the per-tenant management page view. By clicking the “Manage Tenant” (2) option (see above image), the Cluster Admin sees the Tenant Dashboard as well as additional options to configure the Tenant settings.

### Force full scan for storage quota usage

This will start a full scan of storage usage for the Tenant. As files are uploaded, modified or deleted during daily operation, the Tenant Quota is calculated. To ensure that the quota value shown for the tenant is accurate, it is important that you occasionally force a full scan of the tenant’s quota usage.

### Change Tenant Admin Password

Provides a method for the Cluster Administrator to assist the Tenant Administrator with resetting passwords.

### Edit Existing default storage

When a Tenant outgrows their allocation of storage space or needs to move to a different storage location, this setting allows the Cluster Administrator to change the storage location.

**Tip:** When changing a storage location for a Tenant; you typically manually copy the folder to the new location then re-configure the default storage location.

**Warning:** If you want to change the tenant’s default storage location, make sure you copy tenant’s file AS-IS from the source folder to its destination folder before you change the storage location here.

### Delete Tenant

Deletes the tenant.

---

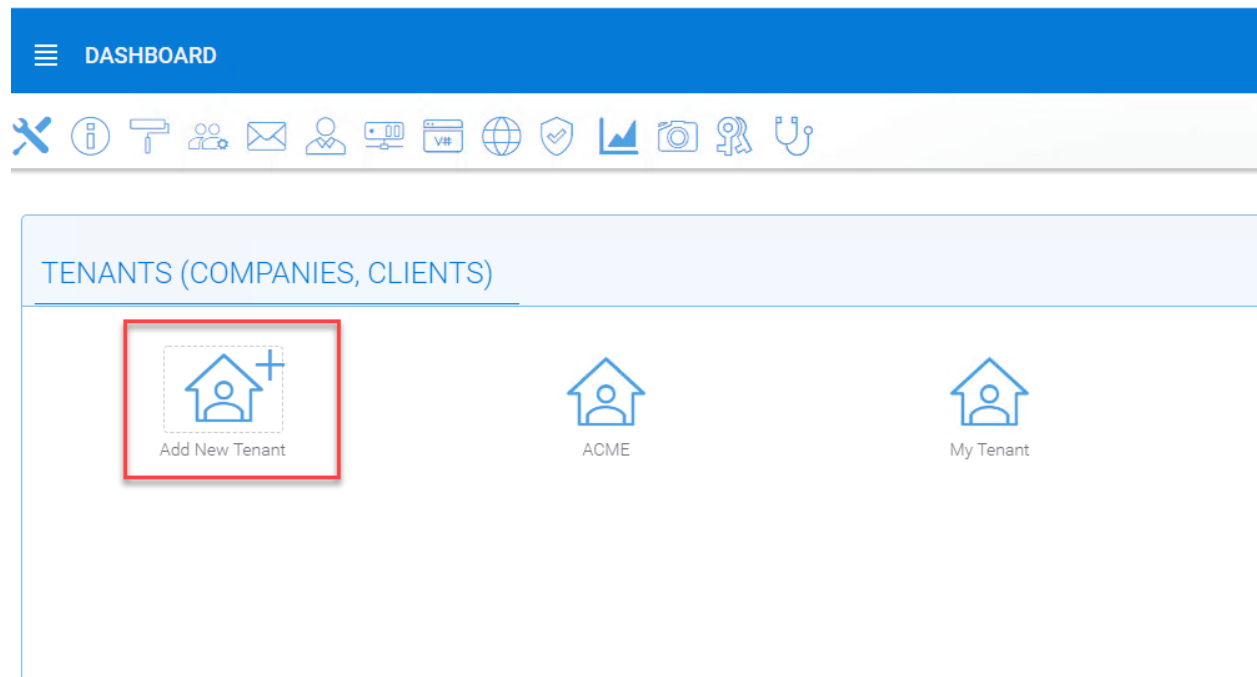
**Note:** For more details about the Tenant Management and all the configuration check ...

---

### 3.2.1 Create a New Tenant

Cluster Manager > Tenant Manager

Click on the “Plus” sign in the New Tenant to start the creation of a new tenant.



The first screen under “New Tenant” is asking for “Start from Scratch” or “Import and migrate data from Anchor”.

When you select “Add New Tenant from Scratch”, The next screen is asking for a few parameters related to who the tenant is.

“**Create with Default Settings**” will get it done and the tenant will be granted all default settings, including the storage location allocation.

“**Continue**” allows you to customize the settings and storage location.

If you pick “**Continue**”,

The second screen under “Add Tenant from Scratch” is asking for the division of work between the cluster administrator and the tenant administrator.

The third screen under “Add Tenant” is asking where the root storage for the tenant will be at.

#### Automatically assign a sub-folder from cluster default tenant

When selected, the tenant’s default storage will be a sub-folder inside the cluster default tenant’s storage folder. It is easier to manage when you don’t need per-tenant storage access credentials. This is the easiest option because if every tenant is allocated a sub-folder from the default tenant, then the default tenant storage location is a single place to take care of all of your storage needs. The storage location is sandboxed away from the default tenant so even though from a physical location’s perspective, it is a sub folder of the default tenant, but the default tenant will not be able to see the folder from CentreStack.



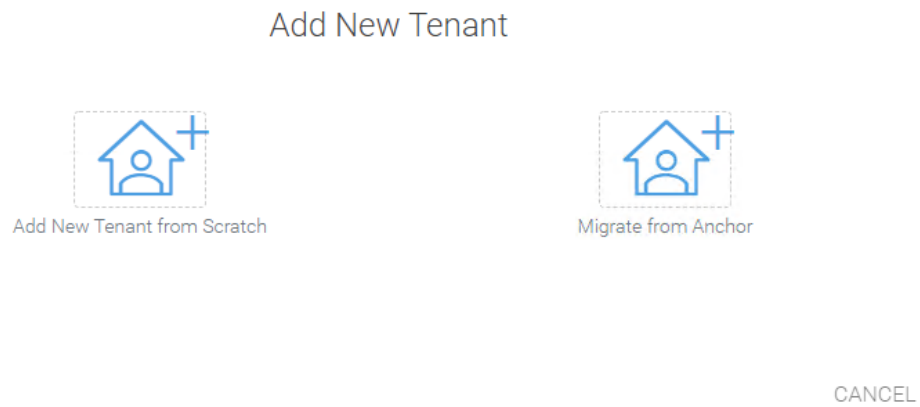


Fig. 2: CREATING A NEW TENANT

DASHBOARD > NEW TENANT > ADD NEW TENANT FROM SCRATCH

### Tenant Admin Information

First Name	Last Name
<input type="text"/>	<input type="text"/>
Email	Organization Name
<input type="text"/>	<input type="text"/>
<input checked="" type="checkbox"/> Let system generate password (password will be sent via email)	
User Plan:	Storage Plan (0-Unlimited):
3	100 <span>GB</span>

CREATE WITH DEFAULT SETTINGS
CONTINUE
CANCEL

Fig. 3: TENANT MANAGER SETTINGS 1

DASHBOARD > NEW TENANT > ADD NEW TENANT FROM SCRATCH
23 trial day(s) left.

### Advanced

Custom Domain (i.e. yourcompany.com) (leave this field blank unless you want to support per-tenant branding)

---

#### Tenant Administrative Control:

There are certain features you can expose to tenant administrators, such as setup LDAP for Active Directory or mount extra external storage services. Check the following features that you would like to expose to tenant administrator.

☒ Tenant Never Expires

☒ Allow tenant to attach external cloud storage

☒ Allow tenant to edit branding setting

☒ Allow creation of guest users

☐ Show Data-At-Rest Encryption configuration page (Requires empty storage container)

☒ Allow tenant edit LDAP setting

☒ View and edit group policy

☐ Allow tenant to increase user plan automatically

BACK CONTINUE CANCEL

Fig. 4: TENANT MANAGER SETTINGS 2

## Add New Tenant - Default Storage

- ☒ Automatically assign a sub-folder from cluster default tenant

When selected, the tenant's default storage will be a sub-folder inside the cluster default tenant's storage folder. It is easier to manage when you don't need per-tenant storage access credentials.

- ☐ Use existing file server or local disk as default storage

- ☐ Use Cloud Storage as default storage

BACK CONTINUE CANCEL

Fig. 5: ADD TENANT STORAGE OPTIONS 1

### Use existing file server or local disk as default storage

Using this option, you can connect the tenant’s root folder to a file server network share. If you want the tenant users to continue to share file server network share outside of CentreStack, it is recommended you use the “Import Network Share” feature in “Team Folder” instead of pointing the default storage to the file server share, because the Cluster Server will assume it has 100% of the control of the storage location.

## Add New Tenant - Default Storage

☐ Automatically assign a sub-folder from cluster default tenant

☒ Use existing file server or local disk as default storage

Local Storage Location (C:\myfolder or \myfileserver\share): ☐ Create if doesn't exist

---

User Name (for local storage access):

---

Password (for local storage access):

---

☐ The share is from a Linux/Unix/ZFS Server

☐ The share is a DFS share

☐ Always access the storage using the logon user identity

The specified user will be used to verify the storage and will also be used to access the storage for the admin account. If the above checkbox is checked, the storage will always be accessed using the team-user’s Active Directory identity when the storage is published as a team folder. Non-Active Directory users will access the storage using the specified user account.

☐ Publish Tenant Home Storage As a Team Folder

The tenant’s home storage will be published to the Active Directory users in the same tenant so they can see files and folders contents from the home storage. Some specialized folders, such as folders from remote file servers or remote cloud storage services are not included in this scope.

Fig. 6: ADD TENANT STORAGE OPTIONS 2

### Use Cloud Storage as default storage

when using this option, you can connect the tenant’s root folder to Amazon S3, Windows Azure Blob, OpenStack storage as well as others.

#### Using Amazon S3 bucket for tenant storage

Tenant Manager > {Create New Tenant} > Use Cloud Storage as Default Storage > Amazon S3

You can pick Amazon S3 as the target storage for the tenant if you want to.

After you pick the Amazon S3, the first screen will be asking for Access Key and Secret Key.

You will need to log into your AWS console to get the access key and secret key. You can use master access key and secret key, by default the master key has default access to all buckets. You can also create an IAM user and use the key from a specific IAM user. However, by default, the IAM user is locked out of access to any bucket until bucket access policy is created and attached to the IAM user.

## Add New Tenant - Default Storage

☐ Automatically assign a sub-folder from cluster default tenant

☐ Use existing file server or local disk as default storage

☒ Use Cloud Storage as default storage

Amazon S3



BACK

CONTINUE

CANCEL

Fig. 7: CLOUD STORAGE SETTINGS

DASHBOARD > NEW TENANT > ADD NEW TENANT FROM SCRATCH
25 total day(s) left

Amazon S3 Account Configuration

☒ Enable Inplace Versioning

BACK
CONTINUE

Fig. 8: AMAZON S3

If you use IAM user, here is a sample S3 Bucket access policy to grant an IAM user to a specific bucket. As shown below, the policy gives an IAM user the ability to use bucket “user3onlybucket”

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectTorrent",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionTorrent",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectTagging",
        "s3:PutObjectVersionAcl",
        "s3:PutObjectVersionTagging",
        "s3:ReplicateDelete",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource": [
        "arn:aws:s3:::user3onlybucket/*"
      ]
    }
  ]
}
```

After it is all setup properly, you can use the IAM user’s access key id and secret access key to connect to the Amazon S3 bucket.

When the correct access credentials are given, the next screen is to select a bucket from Amazon S3.

You can pre-create a bucket in Amazon S3 and then pick the bucket in the current page. After that, it will take a short

DASHBOARD > NEW TENANT

### Amazon S3 Account Configuration

Access Key ID

AKIAJFOQV6BK5PTISSKQ

Secret Access Key

.....

BACK CONTINUE

Fig. 9: AMAZON S3 USER'S ACCESS KEY

DASHBOARD > NEW TENANT

### Amazon S3 Account Configuration

Select a Bucket :

user3onlybucket

BACK FINISH

Fig. 10: AMAZON S3 SLECTING A BUCKET

while for the system to be ready for the new tenant created.

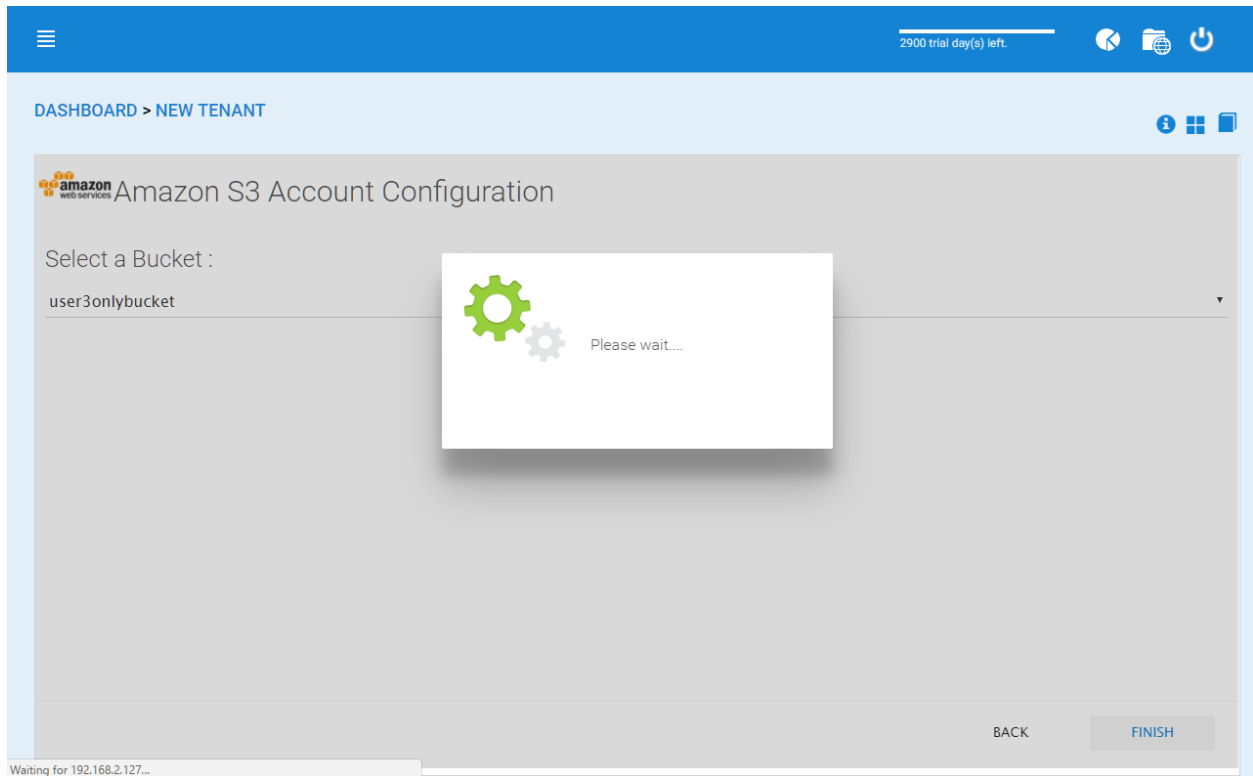


Fig. 11: FINISHING AMAZON S3 CONFIGURATION

After the tenant is created, you will be looking at the dashboard of the tenant.

### Using Windows Azure Blob Storage for tenant storage

In addition to Amazon S3 bucket, you can also use Windows Azure Blob Storage as the tenant's back end storage.

Similar to the above Amazon S3 setup process, you can pick "Windows Azure Blob" as the option during the tenant creation process.

The next screen will be asking for Blob URL and the Primary key.

You can get this information from the Azure Portal.

Here is a simple mapping between azure portal and the parameters it ask for.

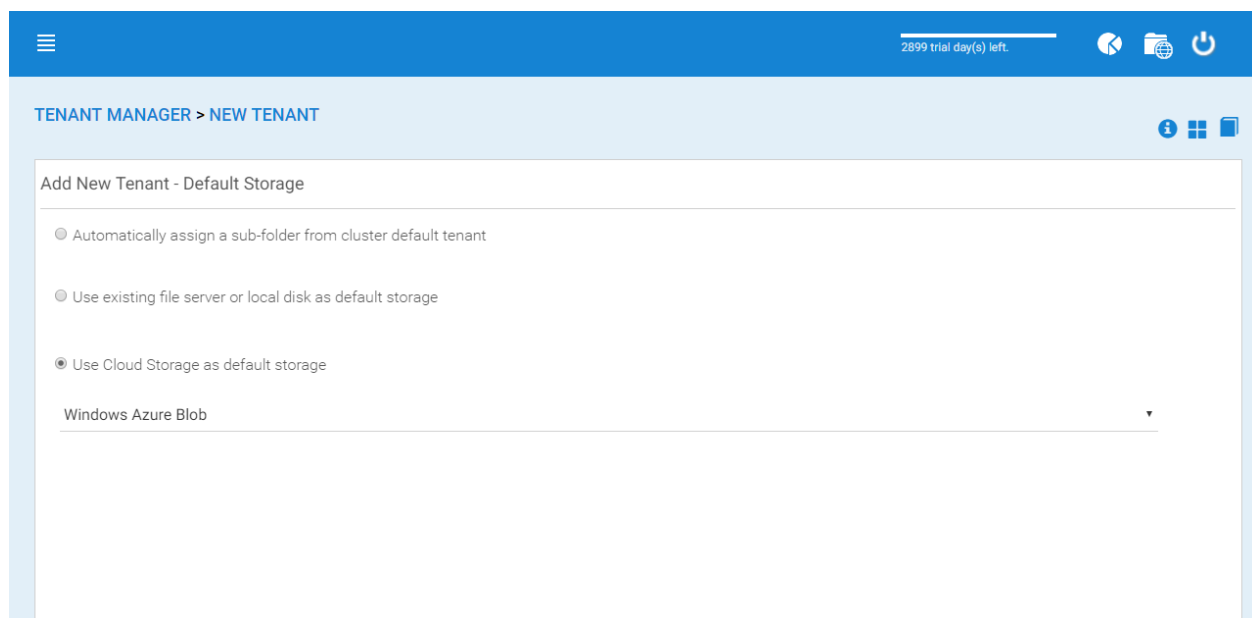
After you put in the account information, the next screen asks to pick a container to use.

After the container information is all set, the tenant account will be created.

## 3.3 Cluster Branding

Cluster Manager > Cluster Branding

Cluster Branding is for changing the logo, bitmaps and other branding related information. There are two branding supports. One is self-service built-in branding, which is completely controlled by the "Cluster Branding" settings on the "Cluster Manager". The other is full-branding service. Both rely on the "Cluster Branding" to change the look-and-feel of the web portal.



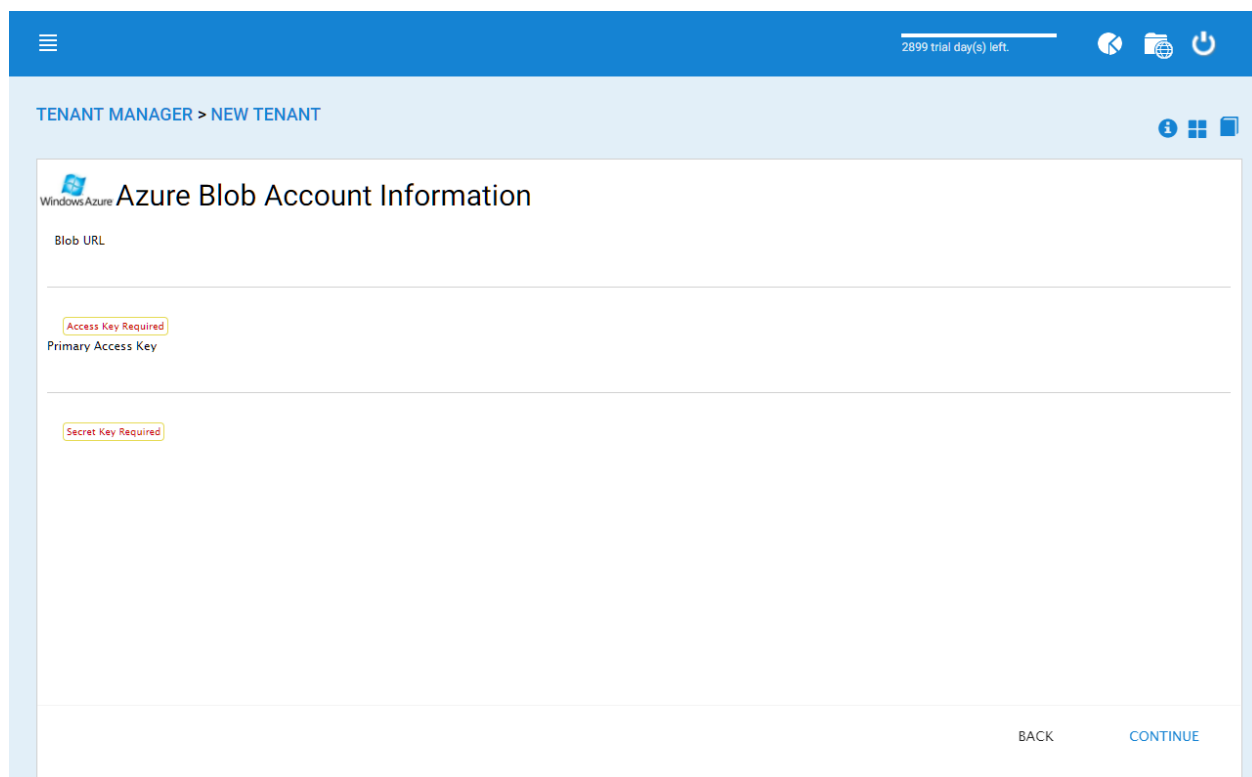
TENANT MANAGER > NEW TENANT

### Add New Tenant - Default Storage

☐ Automatically assign a sub-folder from cluster default tenant  
☐ Use existing file server or local disk as default storage  
☒ Use Cloud Storage as default storage

Windows Azure Blob

Fig. 12: WINDOWS AZURE BLOB SETUP



TENANT MANAGER > NEW TENANT

### Azure Blob Account Information

Blob URL

Access Key Required

Primary Access Key

Secret Key Required

BACK CONTINUE

Fig. 13: AZURE BLOB URL AND PRIMARY KEY



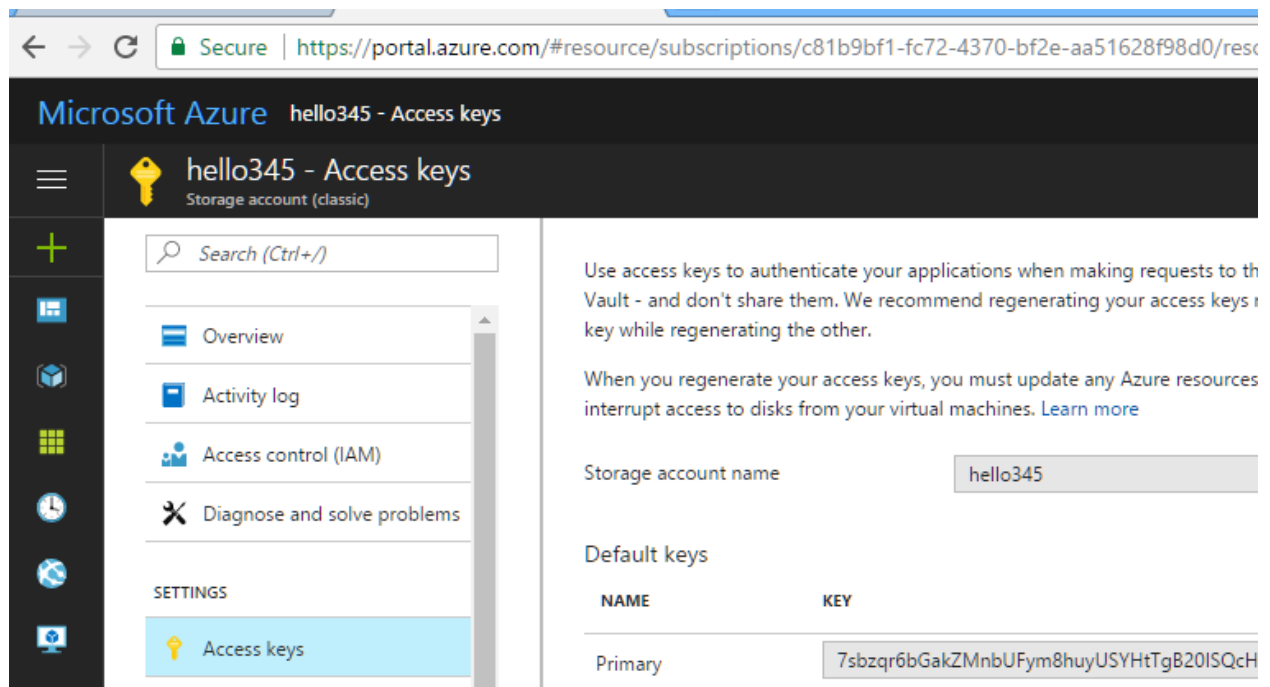


Fig. 14: AZURE BLOB ACCESS KEYS

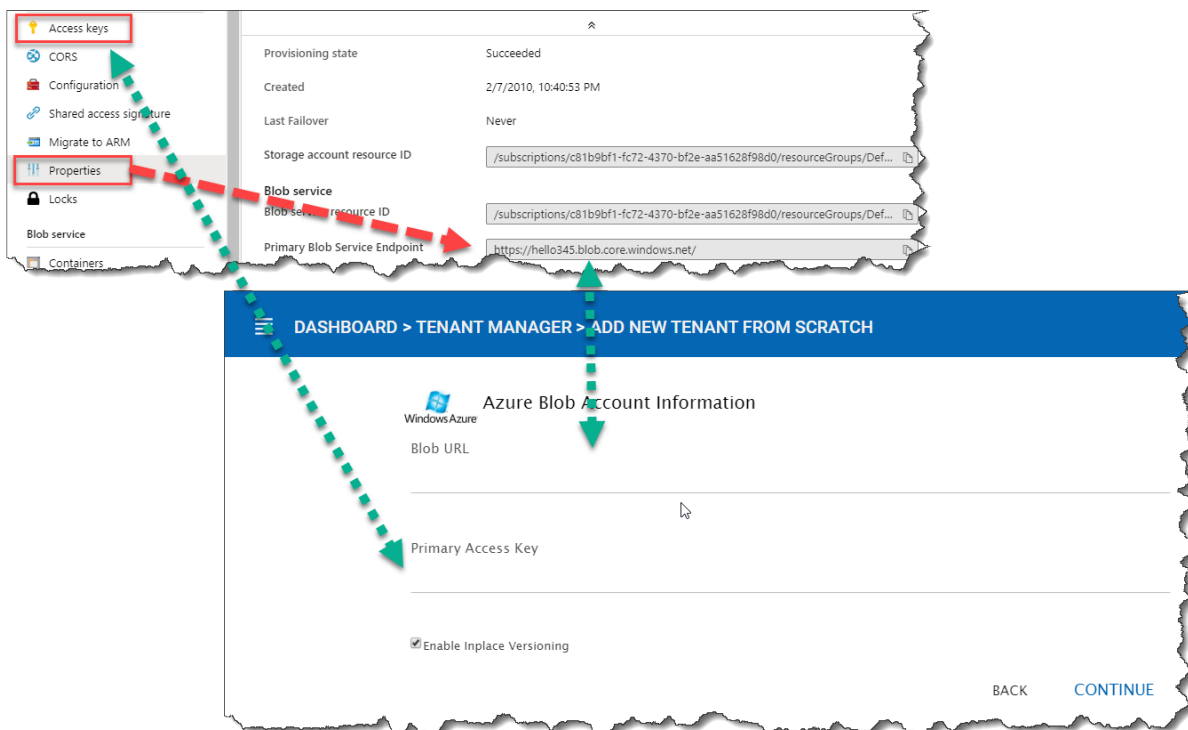


Fig. 15: AZURE BLOB ACCOUNT SETTINGS

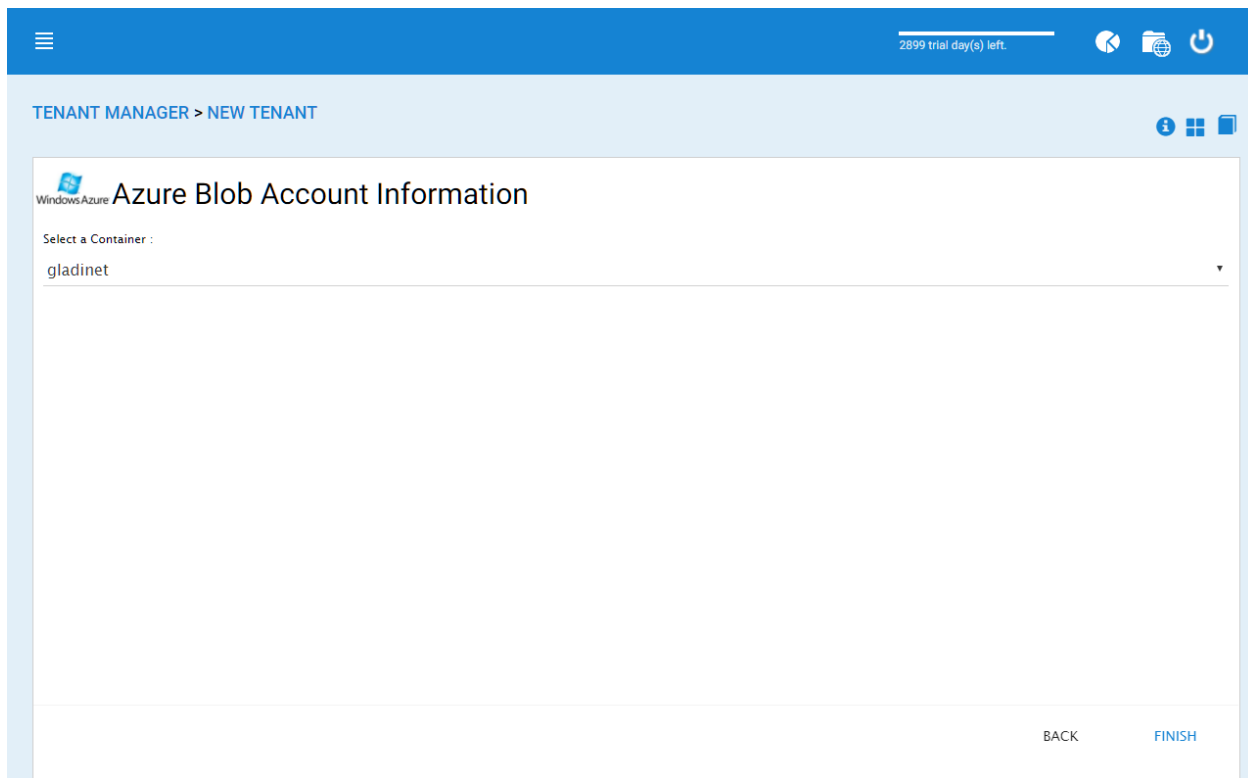


Fig. 16: AZURE BLOB ACCOUNT INFORMATION

Built-in branding will work with white-label clients, which upon the first connection to the cluster, will download the branding related information and use the branding related information. As compared to full-branding service, the full branding clients will have artworks, logo bitmaps and related information burned into the client binaries.

### 3.3.1 General

Cluster Manager > Cluster Branding > General

Under the general tab you can specify the name and other settings as specified below.

#### Product Name

This is where you will specify what you would like to call the product. This is the name that users will see when they login either in web portal or the client applications. To access branding settings click the branding icon (1) then “EDIT” (2) and then change the setting you want (3). Don’t forget to save your settings. You can also choose a color theme which you would like your users to see when they login to the portal. You can choose a color theme that is close to your company colors.

#### Feedback Email

Users’ feedback will be delivered to this email address.

#### Home Page URL

This is the URL of your ‘Home Page’ page (1).

#### ‘Copyright’ Statement

This is the contents of your ‘Copyright’ statement (2).

- Cluster Branding**
- Reports
- Cluster Control Panel
- Default Group Policy
- Cloud Backup and Restore

Product Name: What you want to call the product.	ACME
Web-UI Theme (takes effect when you login next time):	blue
Tenant Default Language:	No Default
Customized Theme Color	
'Contact Us' URL The URL of your contact us page	Not Branded

Fig. 17: CLUSTER BRANDING

ACME

- Dashboard
- Tenant Manager
- Cluster Branding**
- Reports
- Cluster Control Panel
- Default Group Policy
- Cloud Backup and Restore

DASHBOARD > CLUSTER BRANDING

23 trial day(s) left.

General Web Portal Client Download Windows Client Mac Client Emails Android Client iOS Client Export/Import

RESET ALL EDIT

Product Name: What you want to call the product.	ACME
Web-UI Theme (takes effect when you login next time):	blue
Tenant Default Language:	No Default

Fig. 18: CLUSTER BRANDING

ACME

- Dashboard
- Tenant Manager**
- Cluster Branding
- Reports
- Cluster Control Panel
- Default Group Policy

Support

DASHBOARD > TENANT MANAGER

26 trial day(s) left. Buy Now

2 of 2 tenants found 5 Users

New Tenant

Default Tenant

1 user(s)  
3 user license(s)

0 bytes  
Unlimited

4 user(s)  
4 user license(s)

43.1 MB  
100 GB

Manage Tenant

- Force full scan for storage quota usage
- Change Tenant Admin Password
- Edit Existing Default Storage
- Delete Tenant

Fig. 19: FEEDBACK EMAIL

Tenant Default Language:	<a href="#">Not Branded</a>
Customized Theme Color	
'Contact Us' URL The URL of your contact us page	<a href="#">Not Branded</a>
'Feedback' Email The Email account that will receive user's feedback	<a href="#">Not Branded</a>
'Home Page' URL The URL of your 'Home' page	<a href="#">https://acme.site/hos.html</a>
'Term of Use' URL The URL of your 'Term of Use' page	<a href="#">Not Branded</a>
'Privacy Policy' URL The URL of your 'Privacy Policy' page	<a href="#">Not Branded</a>
'Copyright' Statement	<a href="#">2021 ACME SYSTEMS</a>

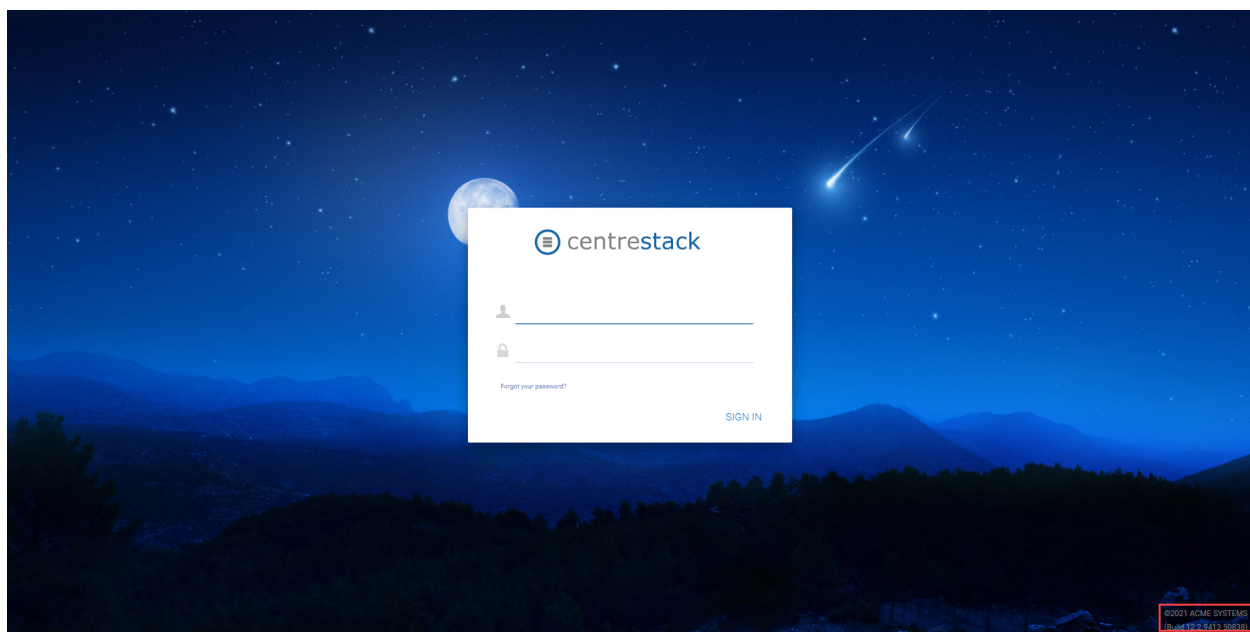


Fig. 20: HOME PAGE URL AND COPYRIGHT STATEMENT

### 3.3.2 Web Portal

Cluster Manager > Cluster Branding > Web Portal

**Note:** In previous builds, the best way to get icons to work is by putting the icon files on the same server and reference the icons via a relative link.

For example, you can create a sub folder under the Install Folder of the Cluster Server, such as under root/imagetest folder. The dimensions for all icons for each setting under web portal should match what is displayed for each setting. The branding of the icons and images require the icons and images with the same width/height as specified or same aspect ratio if the resolution is higher.

In later builds, the icons used are what-you-see-is-what-you-get and you can upload those icon sets.

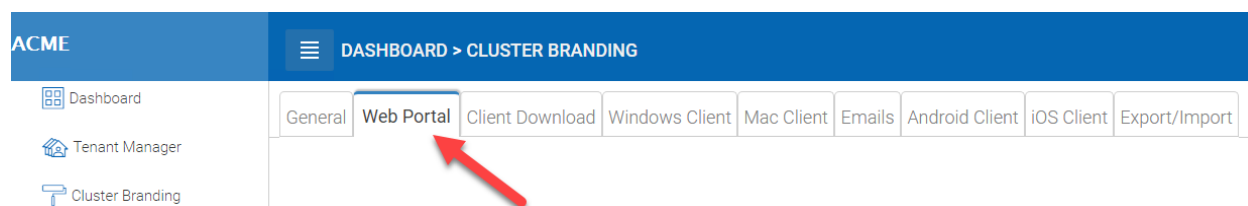


Fig. 21: WEB PORTAL SETTINGS

#### Application Icon

From the Web portal (1) section of cluster branding, you can change the application icon (2). This is the image that is displayed next to the product name in the web portal.

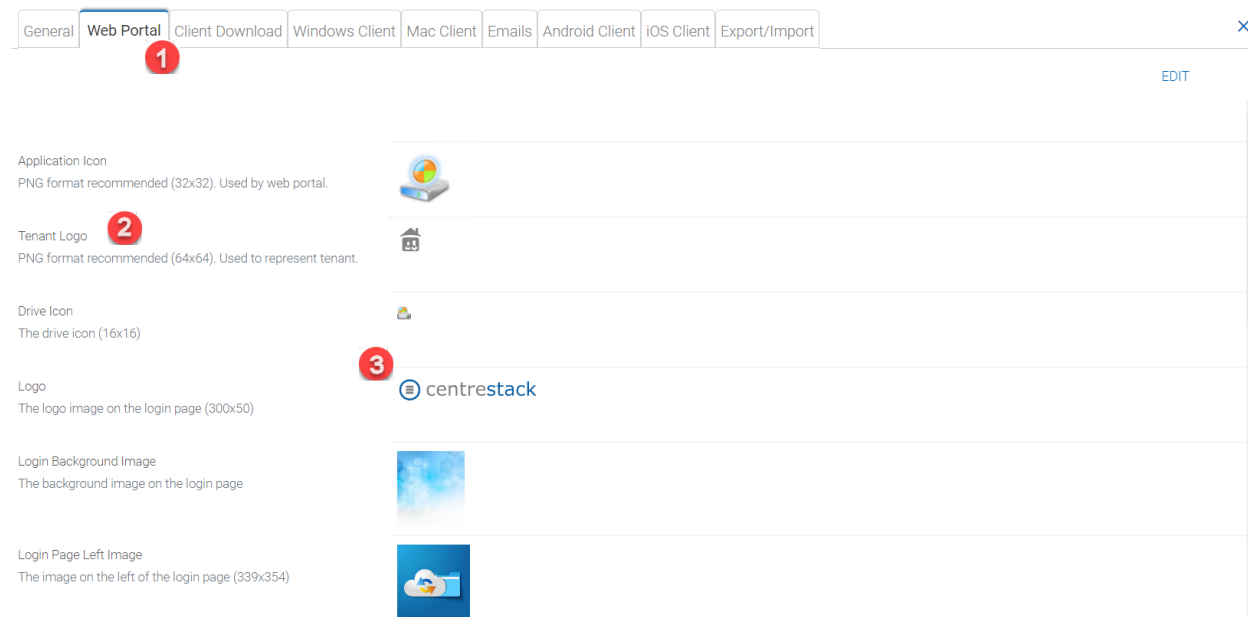


Fig. 22: WEB PORTAL BRANDING

#### Tenant Logo (3)

This is where the logo that represents each tenant should be uploaded.

#### Drive Icon (4)

This is the icon that will be used for the cloud drive. For example in the web portal tree view.

#### Logo Url & Login Page Left Image (5)

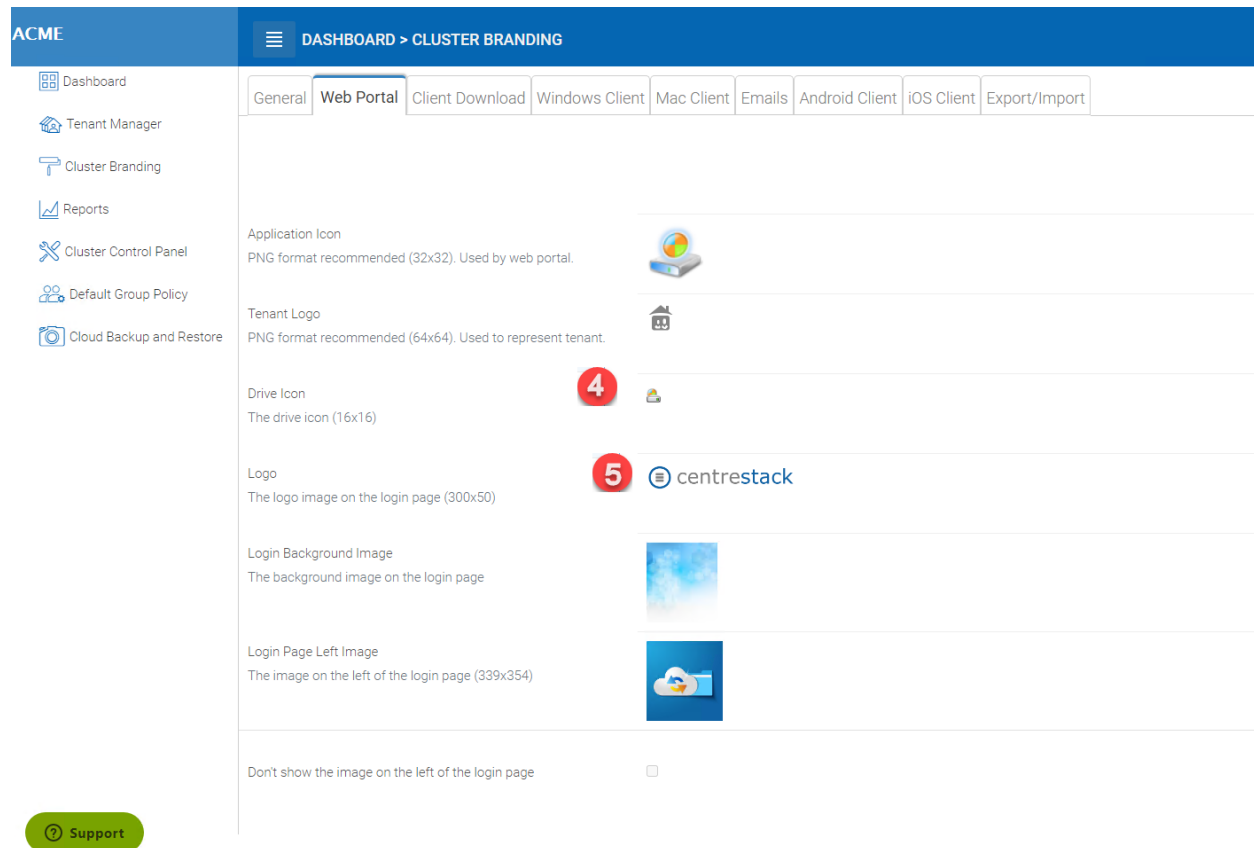


Fig. 23: LOGIN PAGE ICON

Please follow the same steps for branding settings for 'Login Background Image', 'File Share Stamp Icon', 'IOS Client App ID', 'Login Page Note', 'Change Password URL', 'Tutorial Page URL'.

### 3.3.3 Client Download

Cluster Manager > Cluster Branding > Client Download

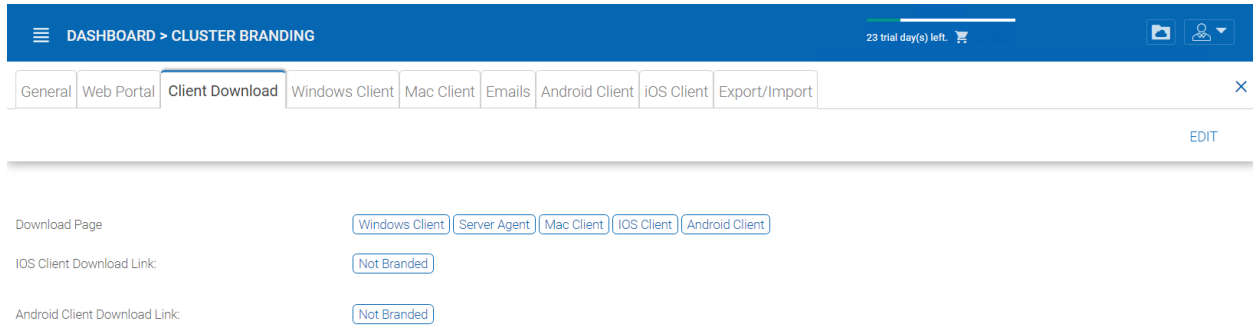
You can choose not to show the download link for some clients here.

#### Mobile Clients Download Links

Once you brand your own iOS client and/or Android Client you can point the download link to your own AppStore and Google Play locations.

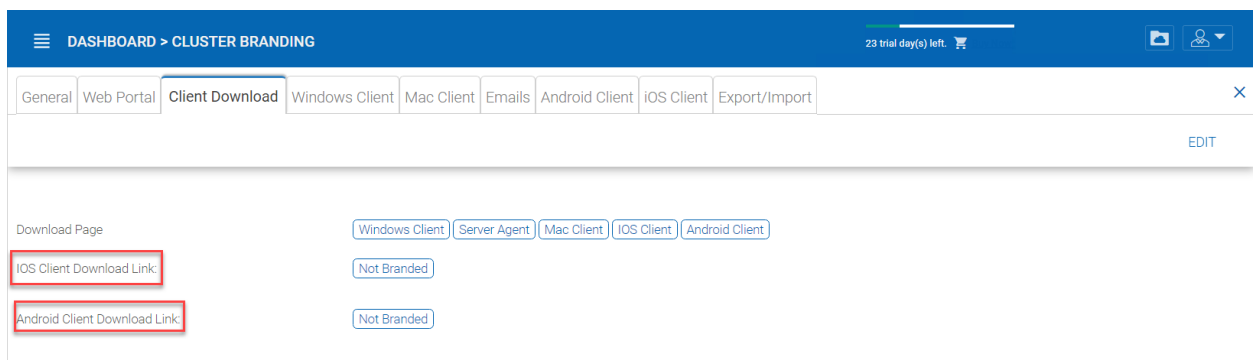
### 3.3.4 Windows Client

Cluster Manager > Cluster Branding > Windows Client



The screenshot shows the 'Client Download' settings page. The top navigation bar is blue with a hamburger menu icon, 'DASHBOARD > CLUSTER BRANDING', a progress bar indicating '23 trial day(s) left', and a user profile icon. Below the navigation bar is a tabbed interface with tabs for 'General', 'Web Portal', 'Client Download' (selected), 'Windows Client', 'Mac Client', 'Emails', 'Android Client', 'iOS Client', and 'Export/Import'. An 'EDIT' link is visible on the right. The main content area has a 'Download Page' section with buttons for 'Windows Client', 'Server Agent', 'Mac Client', 'iOS Client', and 'Android Client'. Below this are two sections: 'iOS Client Download Link:' and 'Android Client Download Link:', each with a 'Not Branded' button.

Fig. 24: CLIENT DOWNLOAD SETTINGS

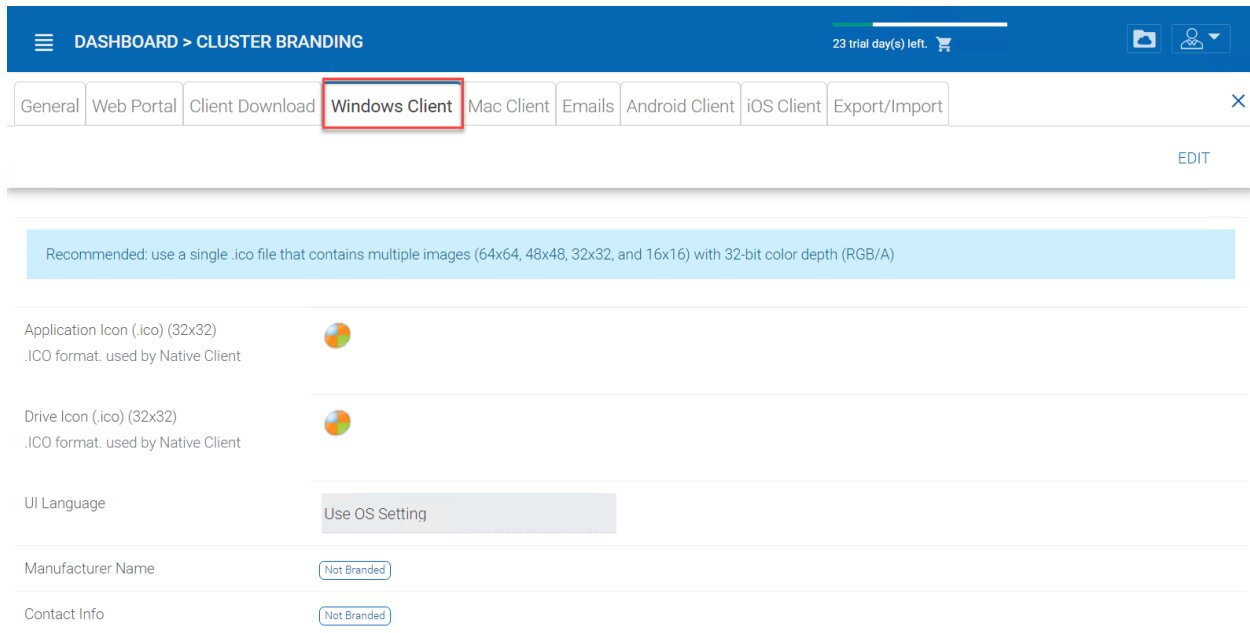


This screenshot is identical to the one above, showing the 'Client Download' settings page. However, in this version, the 'iOS Client Download Link:' and 'Android Client Download Link:' labels are highlighted with red rectangular boxes to indicate the specific settings being discussed in the accompanying figure.

Fig. 25: CLIENT DOWNLOAD LINKS SETTINGS

The application icon and drive icon URLs can be specified here. Also, you can put in your company name under ‘Manufacturer Name’ along with the ‘Contact Info’ email. You also have the option here to create your own branded MSI Windows client. You can also use your own code signing certificate in order to digitally sign the MSI package. The advantage of creating your own MSI client package is that when users download and install the Windows Client you provide, they will see your company name along with your branding during the client installation.

Windows client supports multiple languages. Some language packs are included and shipped with CentreStack. If you need to run the Windows client under a different language, you can set the UI Language there.



**DASHBOARD > CLUSTER BRANDING** 23 trial day(s) left.

General Web Portal Client Download **Windows Client** Mac Client Emails Android Client iOS Client Export/Import

EDIT

Recommended: use a single .ico file that contains multiple images (64x64, 48x48, 32x32, and 16x16) with 32-bit color depth (RGB/A)

Application Icon (.ico) (32x32)  
.ICO format. used by Native Client

Drive Icon (.ico) (32x32)  
.ICO format. used by Native Client

UI Language  
Use OS Setting

Manufacturer Name  
Not Branded

Contact Info  
Not Branded

Fig. 26: WINDOWS CLIENT BRANDING

Once you clicked the “Edit” button to edit the Windows Client branding information, you will be able to provide EULA (End User License Agreement) and Code Signing Certificate.

### EULA

This will be a RTF file format as input.

### Code Signing Certificate

You can acquire a code signing certificate from your code signing certificate vendor. Most SSL vendor also provide code signing certificate. Make sure you use SHA 256 (SHA2) as your digital signing certificate hash algorithm.

If your Code Signing certificate is already installed you can also use the option - Sign using cert in certificate store

## 3.3.5 Mac Client

You can configure the MAC client and MAC client installation package branding under here.

### Client Branding

### Installation Package Branding



The screenshot shows the 'Windows Client' branding settings page. The left sidebar contains navigation links: Dashboard, Tenant Manager, Cluster Branding (selected), Reports, Cluster Control Panel, Default Group Policy, and Cloud Backup and Restore. The top navigation bar shows 'DASHBOARD > CLUSTER BRANDING' with a trial timer and user profile. Below the navigation bar, tabs for 'General', 'Web Portal', 'Client Download', 'Windows Client' (selected), 'Mac Client', 'Emails', 'Android Client', 'iOS Client', and 'Export/Import' are visible. The main content area has buttons for 'BRAND MSI', 'RESET BRANDED PACKAGE', 'APPLY', and 'CANCEL'. A blue box contains a recommendation: 'Recommended: use a single .ico file that contains multiple images (64x64, 48x48, 32x32, and 16x16) with 32-bit color depth (RGB/A)'. The settings include:
 

- Application Icon (.ico) (32x32): .ICO format, used by Native Client. Button: 'Choose File'. Status: 'No file chosen'.
- Drive Icon (.ico) (32x32): .ICO format, used by Native Client. Button: 'Choose File'. Status: 'No file chosen'.
- UI Language: 'Use OS Setting'.
- Manufacturer Name: (empty text field).
- Contact Info: (empty text field).

Fig. 27: WINDOWS CLIENT BRANDING SETTINGS

The screenshot shows the 'Mac Client' branding settings page. The left sidebar is identical to the previous figure. The top navigation bar shows 'DASHBOARD > CLUSTER BRANDING' with a trial timer and user profile. Below the navigation bar, tabs for 'General', 'Web Portal', 'Client Download', 'Windows Client', 'Mac Client' (selected), 'Emails', 'Android Client', 'iOS Client', and 'Export/Import' are visible. The main content area contains a message: 'You can schedule a branding task from your partner account , we will brand the Mac Client automatically.' with an 'EDIT' link. The settings include:
 

- Mac Client Application Icon: Application icon in Mac Client Systray menu (128X128). Icon: (colorful circle icon).
- Mac Client Drive Icon: Mac Client Drive Icon (.icons format). Icon: (colorful circle icon).
- Mac Client Systray(Notification Area) Icon: Mac Client Systray icon displayed on Notification Area (16X16). Icon: (colorful circle icon).
- UI Language: 'Use OS Setting' with a dropdown arrow.

Fig. 28: MAC CLIENT BRANDING

You can brand the Mac software agent package as well. You will need to go to <https://www.centrestack.com/>, login as a partner and go to the “Branding” section to create a branding task. The task will be fulfilled and completed and a Mac software agent package will be available for download once the branding task completes. It may take a couple of days for the task to finish.

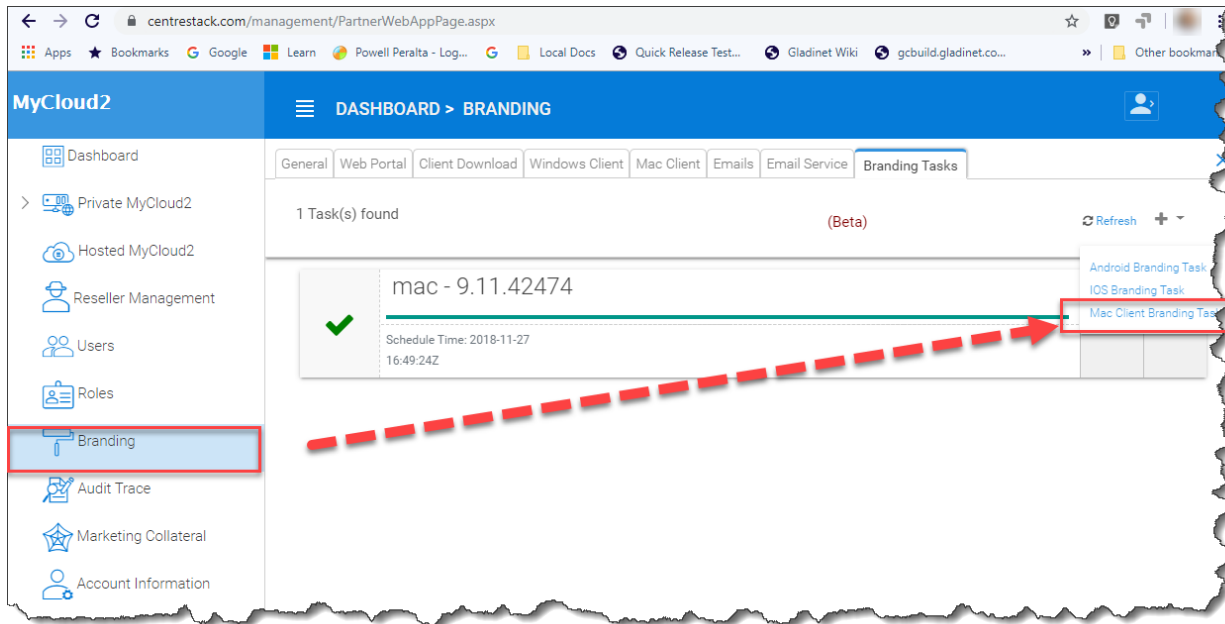


Fig. 29: MAC CLIENT BRANDING IN PARTNER PORTAL

**Note:** Mac software package branding is different from the Windows software package branding because the Mac software package branding will need to be done on a Mac machine. So the task will be created on the partner portal but will be completed asynchronously on a Mac machine.

### 3.3.6 Emails

There are many places in the Cluster Manager that need to contact the users via email. So the “Emails” tab is used to set up the email templates used for contacting users via email.

#### Welcome Email for New Tenant

This is the email sent to the new tenant when the tenant is created. The email is sent to the tenant administrator.

#### Welcome Email for New Team User

The team user is a regular user in a tenant. This is the email template that is sent to the user when the user account is created.

#### Welcome Email for New Guest User

Guest user is a regular user in a tenant that doesn't have a home directory associated. So the guest user can only operate within shared files and folders from other regular users. This is the email template that is sent to the guest user when the guest user's account was provisioned.

#### Email for File/Folder Share

This is the email sent to a user when the user is about to receive file/folder shares.

### Request a File

This is the email sent to a user when the user is about to receive an invitation to upload a file.

### Notify external user that shared file changed

When a shared file/folder changed, this is the email that is sent to the user who receives file/folder shares.

### Admin Reset User Password Email

This is the email that sent to a user when the user's password is reset.

### User Reset Password Email

This is the email that sent to a user when the user resets the password for himself/herself.

### New Sign-in Action Email

This is the email notification sent to the user when the user logs in from a specific machine.

### Settings

This is to set the reply email address. Typically the email is sent with the SMTP service set. However, if the reply address is different, you can set it here.

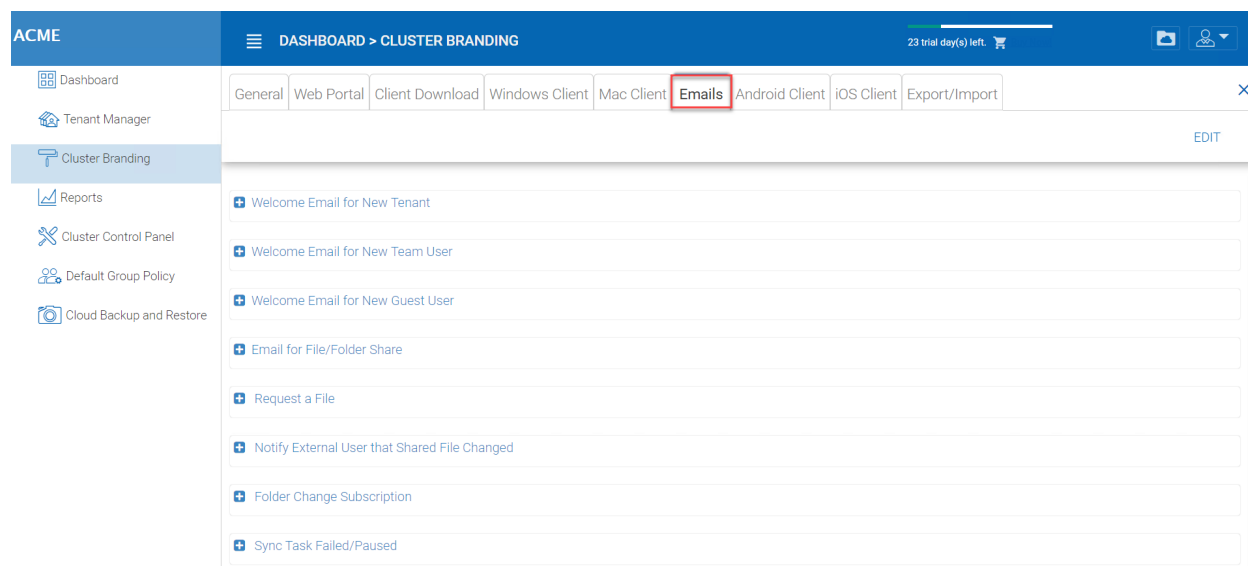


Fig. 30: EMAIL SETTINGS

## 3.3.7 Android Client

**Note:** Branding the android client can now be automated from your partner portal (<http://www.centrestack.com>). Please goto <http://www.centrestack.com> to brand the Android client.

The branding of Android client and iOS client is done from [www.centrestack.com](http://www.centrestack.com), instead of from your own server.

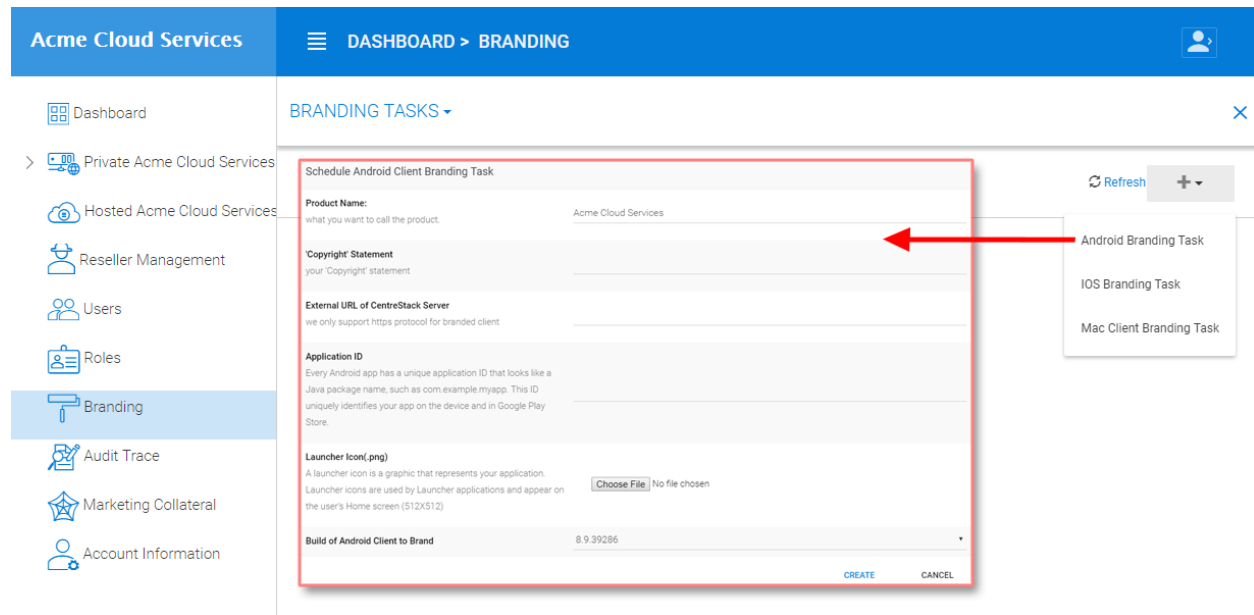


Fig. 31: ANDROID CLIENT BRANDING

### 3.3.8 iOS Client

**Note:** Branding of iOS client can now be automated from partner portal (<http://www.centrestack.com>).

The information here in this section is preserved for legacy reference. Please goto <http://www.centrestack.com> to brand iOS client.

As shown in the above picture, you can generate branding task and request for Android branding and iOS branding.

### 3.3.9 Export/Import

You can either export the branding settings to another cluster or you can import branding settings from another cluster in this cluster under this setting.

## 3.4 Reports

Cluster Manager > Reports

### 3.4.1 Upload Report

Upload report tab shows you graphs for all the uploads that have taken place in the last sixty minutes, 24 hours, 30 days and a whole week.

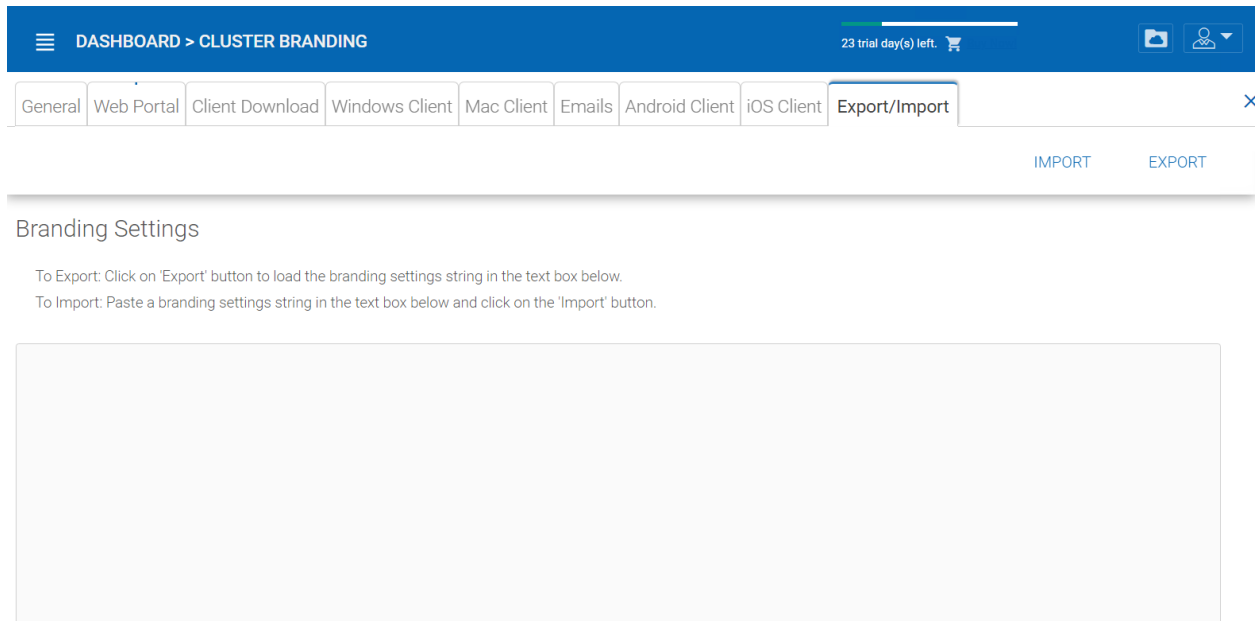


Fig. 32: EXPORT/IMPORT SETTINGS

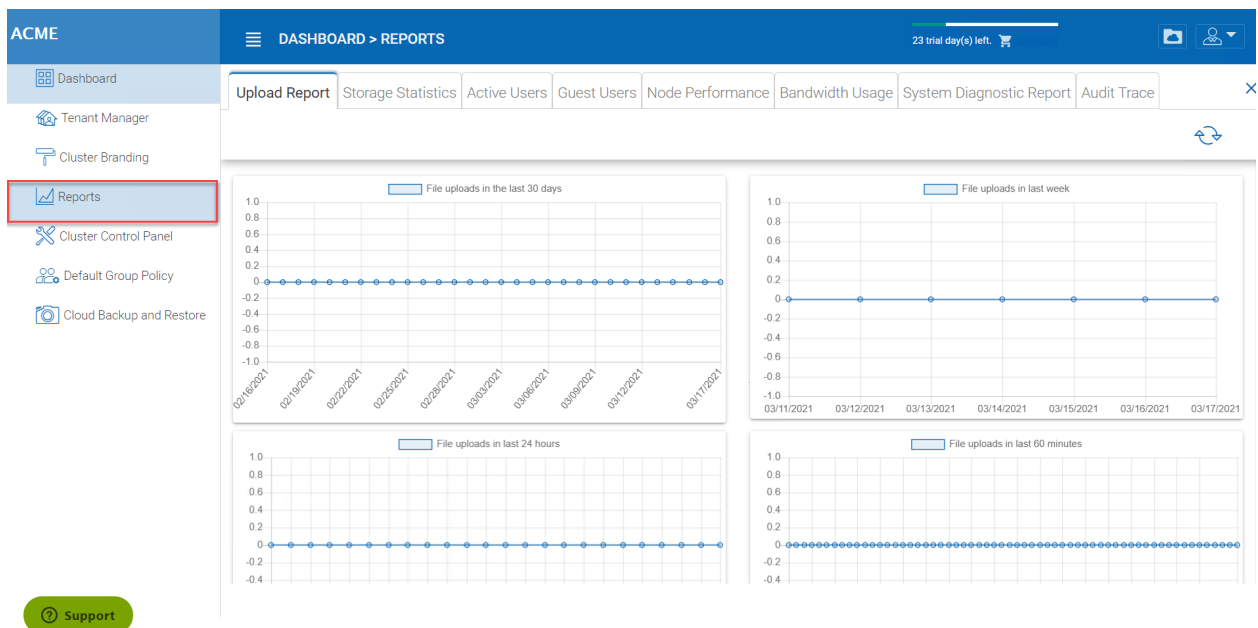


Fig. 33: UPLOAD REPORT

### 3.4.2 Storage Statistics

Under storage statistics, you can see a quick overview of the overall storage statistics, size distribution file type distribution pie charts, and users who have used the most storage so far.

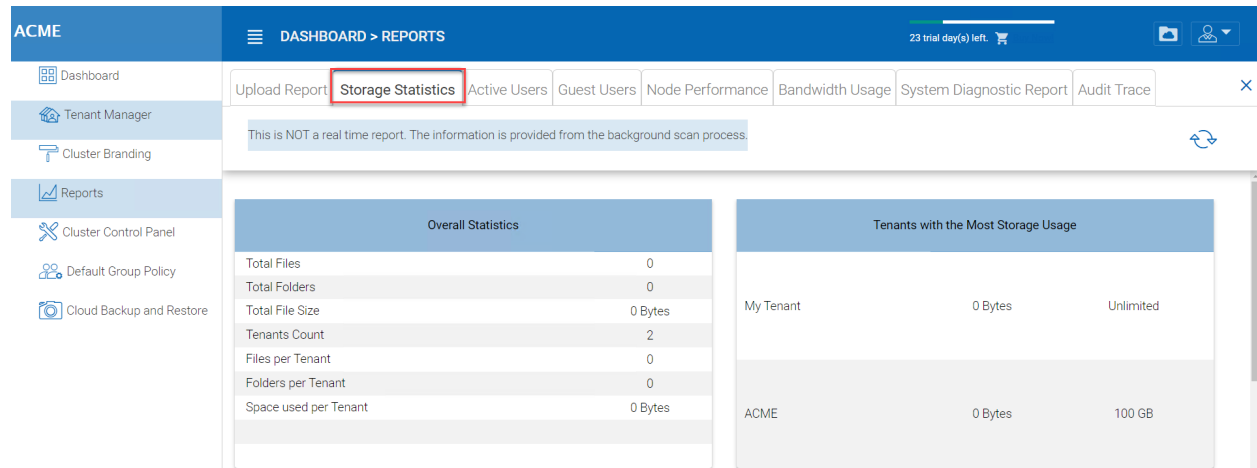


Fig. 34: STORAGE STATISTICS REPORT

### 3.4.3 Active Users

Active users reports the activity of users on the web portal. The active users report doesn't include users from windows client or other native clients because those users are more persistent (always there). To access this report, you can click on the active users section in the panel near the top of the screen.

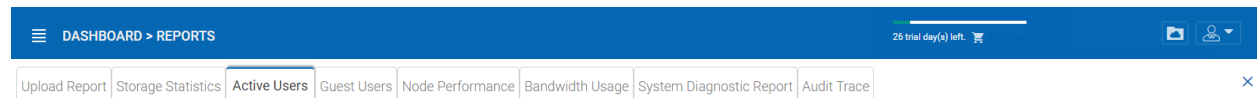


Fig. 35: ACTIVE USERS REPORT

### 3.4.4 Guest Users

Other reports are also available such as Guest Users, which are users that don't have a home directory but are invited to participate on some shared folders and shared files.

### 3.4.5 Node Performance

You can use the Node Performance to check out the worker node health and the database health.

#### Last Reported

You want to see this field has small numbers such as 6 seconds, 10 seconds. If you see sometime like 3 hours ago, that means the node is not reporting the health.

#### Total Requests Processed

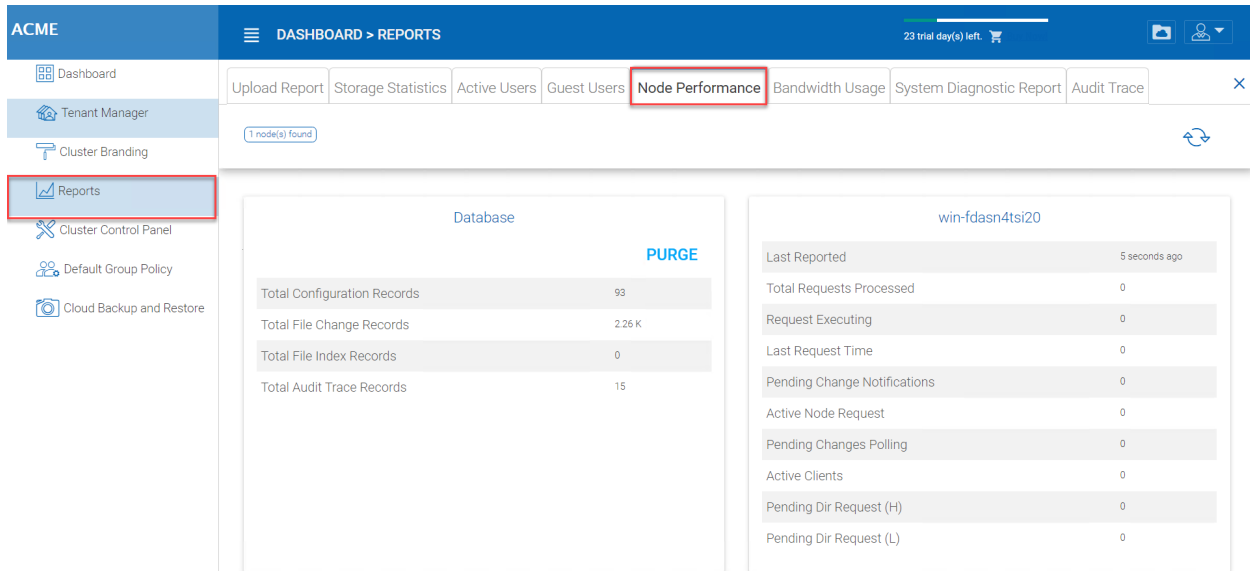


Fig. 36: NODE PERFORMANCE REPORT

You want to see this number as big as possible. This number is cumulative since the service was last re-started. So the bigger the number, the more stable the service is. Also when you have multiple worker nodes, you want to see the Total Requests distributed evenly among the worker nodes.

### Request Executing

You want to see this number as small as possible. This means the number of requests that are concurrently executing on the server. In general a number smaller than 100 is normal. Bigger than 100 is abnormal. Anything bigger than 20 will require investigation.

### Last Request Time

You want to see this number as small as possible. This means the number of milliseconds for the last request. In general, numbers smaller than 3000 or 5000 are normal, which translates to below 3-5 seconds.

### Pending Change Notification

For the files and folders that are changed, there is change notification written to the database. In general, you want to see the pending queue as short as possible.

### Active Node Request

These are the clients out there contacting the server. Usually it is just for reporting purposes.

### Pending Change Polling

These are the clients out there polling to see whether there are files and folders that have been changed. Usually the smaller the better.

### Active Clients

For reporting purpose.

### Pending Dir Request(H)

The pending directory listing calls from the remote clients to the Cluster Server. This is the high priority queue.

### Pending Dir Request(L)

The pending directory listing calls from the remote clients to the Cluster Server. This is the low priority queue.

**Note:** If you don't see the node performance report, check the **Internal URL** setting of each worker node.

Under reports you can look at the upload graphs and storage statistics.

### 3.4.6 Bandwidth Usage

This shows the overall bandwidth usage statistics as well as more granular tenant and user level statistics.

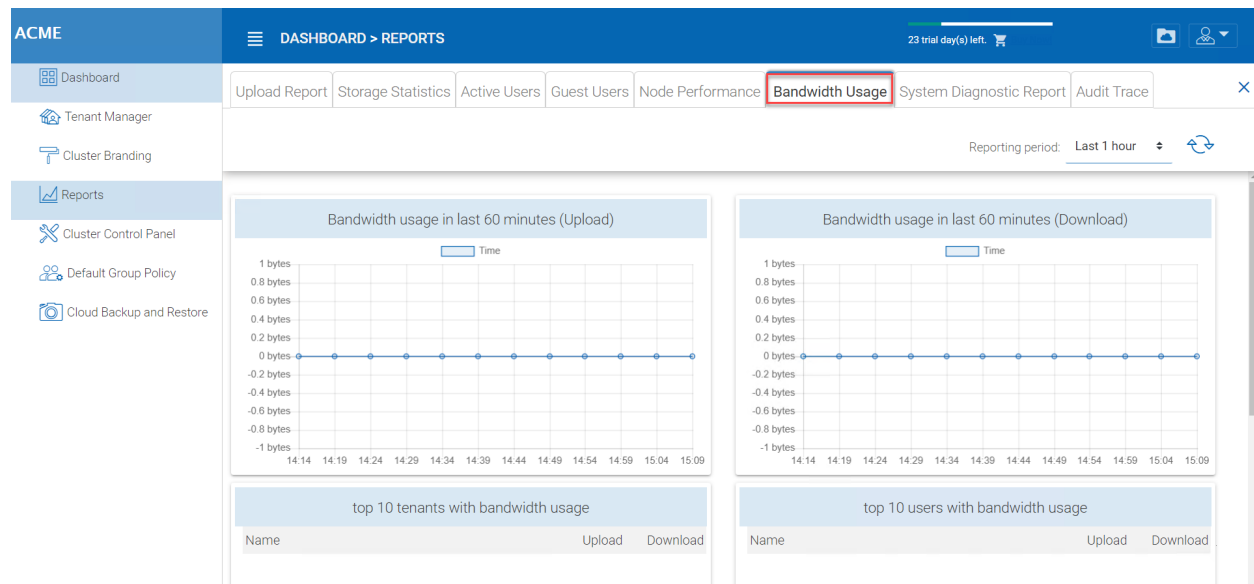


Fig. 37: BANDWIDTH USAGE REPORT

### 3.4.7 System Diagnostic Report

Click the Start Scanning button to generate system diagnostic report.

A sample system diagnostic report is shown below.

### 3.4.8 Audit Trace

This is a sample audit trace.

## 3.5 Cluster Control Panel

### 3.5.1 Cluster Admin

Cluster Manager > Cluster Control Panel > Cluster Admin



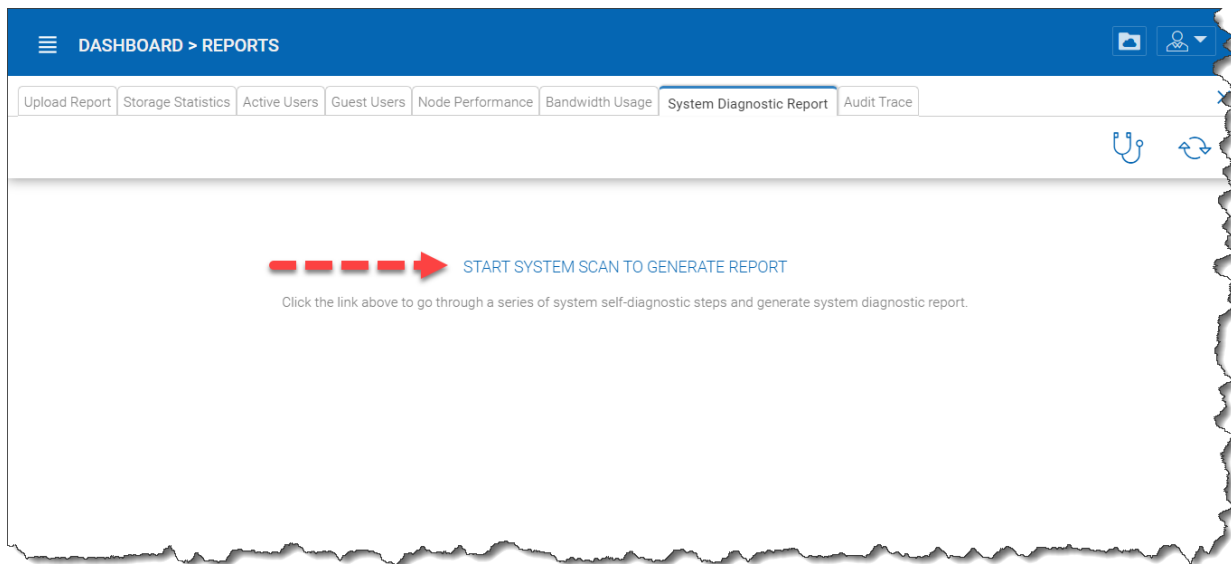


Fig. 38: GENERATE REPORT

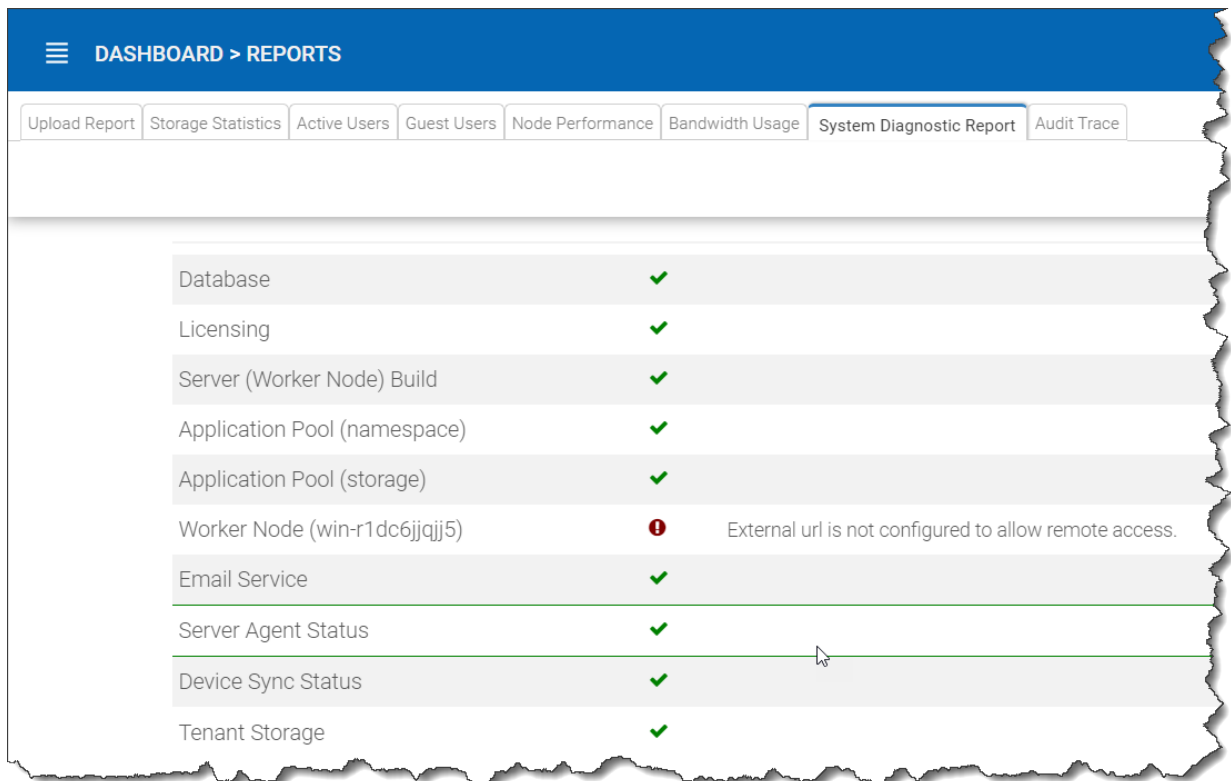


Fig. 39: SYSTEM DIAGNOSTIC REPORT

	Action	Trace	Time	Server Time	User Email	Full Name
1	Login_Success	admin@local,10.0.0.102,	2019-10-21 20:12:45Z	10/21/2019 13:12:45	admin@local	Default Cluster Admin
2	Login_Success	admin@local,10.0.0.102,	2019-10-21 17:59:46Z	10/21/2019 10:59:46	admin@local	Default Cluster Admin
3	Login_Success	admin@local,10.0.0.102,	2019-10-21 12:47:24Z	10/21/2019 05:47:24	admin@local	Default Cluster Admin
4	Add_User	delegate admin(dadmin@gladinet.com)	2019-10-18 19:15:25Z	10/18/2019 12:15:25	admin@local	Default Cluster Admin
5	Login_Success	admin@local,10.0.0.102,	2019-10-18 18:18:29Z	10/18/2019 11:18:29	admin@local	Default Cluster Admin
6	Login_Success	admin@local,10.0.0.102,	2019-10-18 18:14:22Z	10/18/2019 11:14:22	admin@local	Default Cluster Admin
7	Login_Failed	admin@local,10.0.0.102,AUTH_FAILED	2019-10-18 18:14:17Z	10/18/2019 11:14:17	admin@local	Default Cluster Admin

Fig. 40: AUDIT TRACE

Cluster Admin section is to change the properties of the default administrator and also to add additional people to be the cluster administrators. Access the Cluster Admin in the panel on the right of your Tenant Dashboard or from the Cluster Control Panel view.

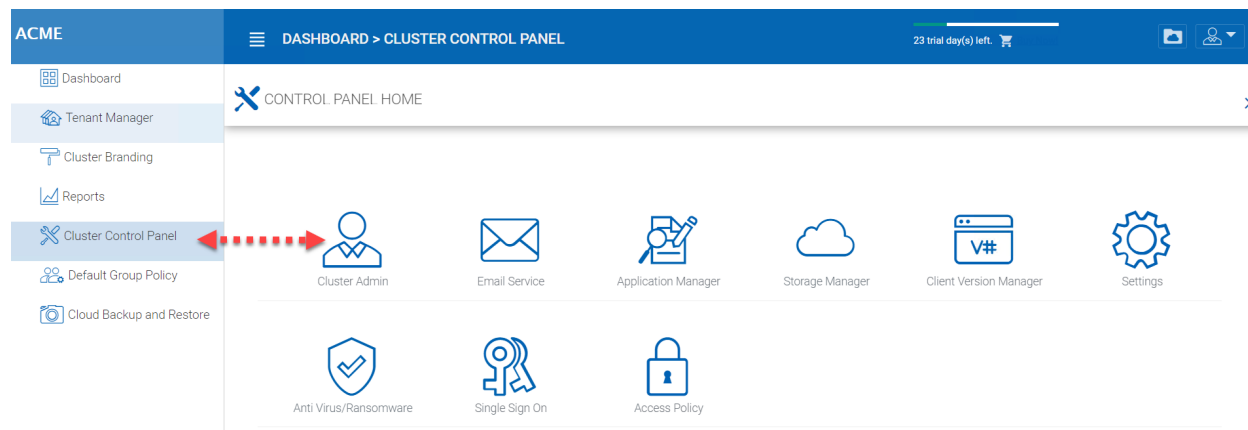


Fig. 41: CLUSTER ADMIN SETTINGS

### 3.5.2 Email Service

Cluster Manager > Cluster Control Panel > Email Service

There are many places in the CentreStack solution that the user needs to be contacted by Email. The Email service is used to set up the SMTP email service to send out the emails.

By default, it works out of box using the default email service with the Cluster Server's customer support email address as the sender.

It is recommended that the SMTP service be setup to use your own SMTP service to send out emails.

In the Authenticate User field, if your SMTP service doesn't require authentication, you can put dummy email in the field.

**Note:** For example, if your email service is on Office 365,

**:SMTP Server Address** smtp.office365.com

**:Use SSL** True

**:SMTP Server Port** 587

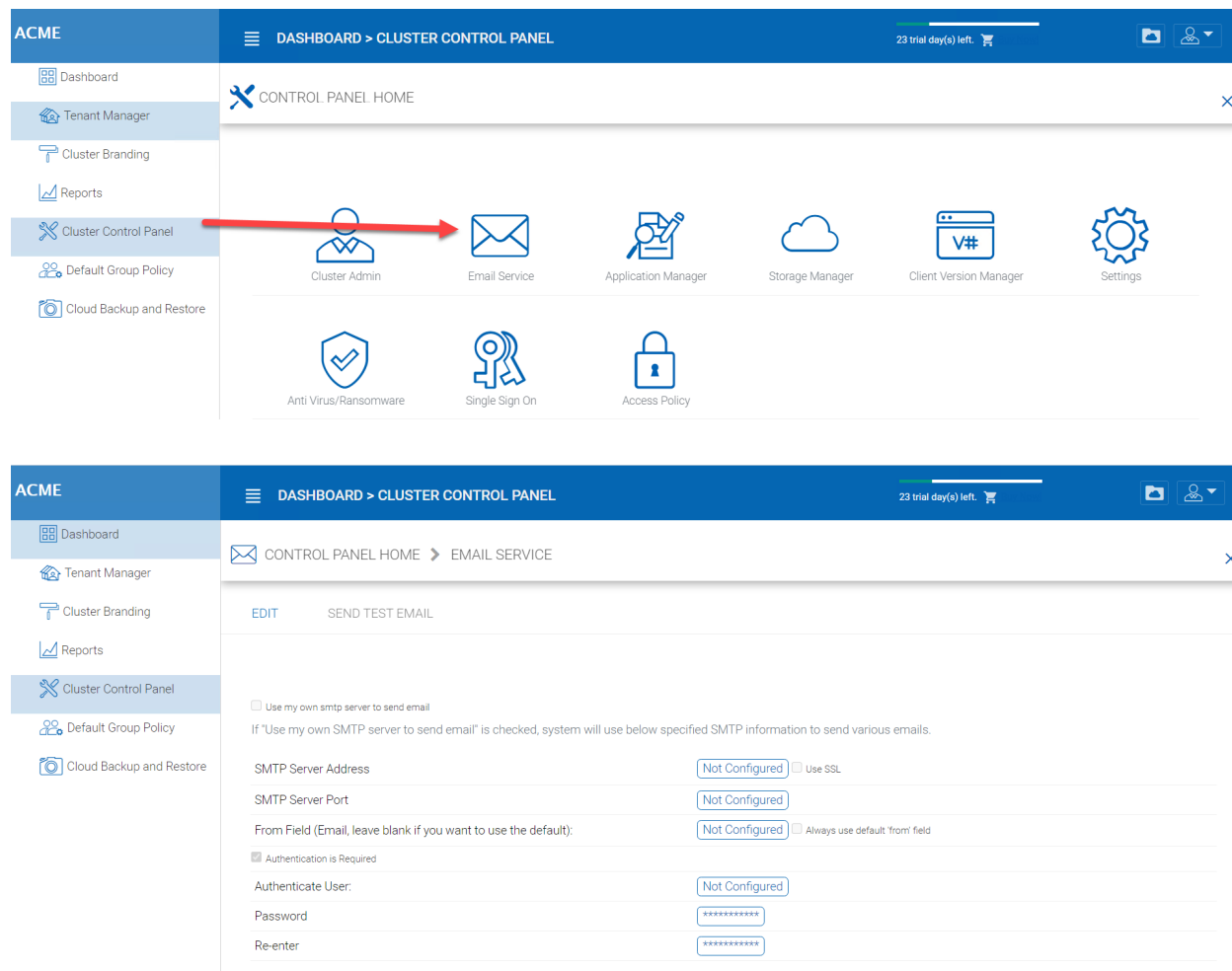


Fig. 42: EMAIL SERVICE SETTINGS

### 3.5.3 Application Manager

Cluster Manager > Cluster Control Panel > Application Manager

You can also configure Web Apps under 'Application Manager' tab in Cluster Settings. This will enable the users to edit documents using the web apps. The applications here only apply to web portal based editing.

Once an application is enabled, you will be able to see the context menu entry from the web based file and folder manager view.

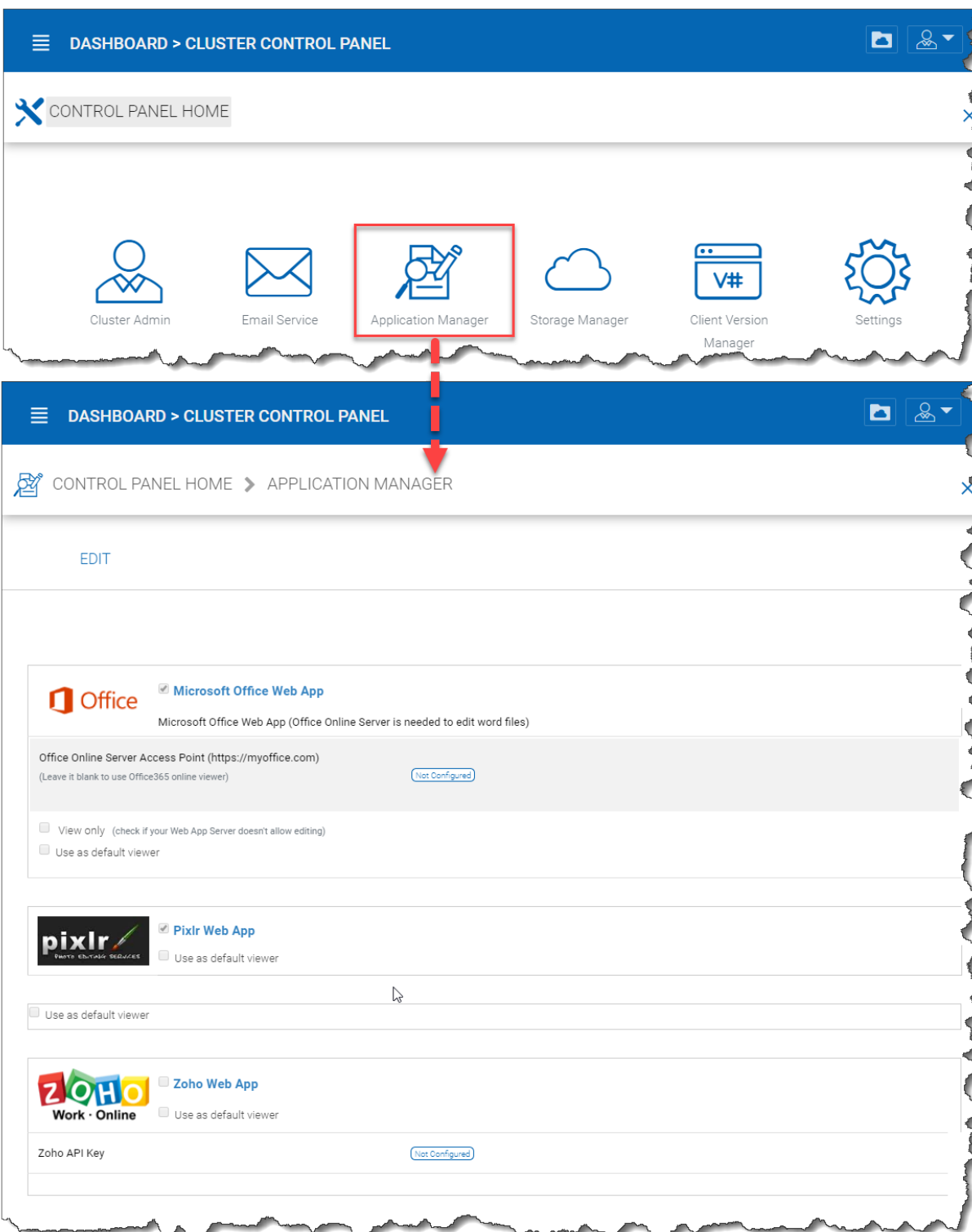


Fig. 43: APPLICATION MANAGER SETTINGS

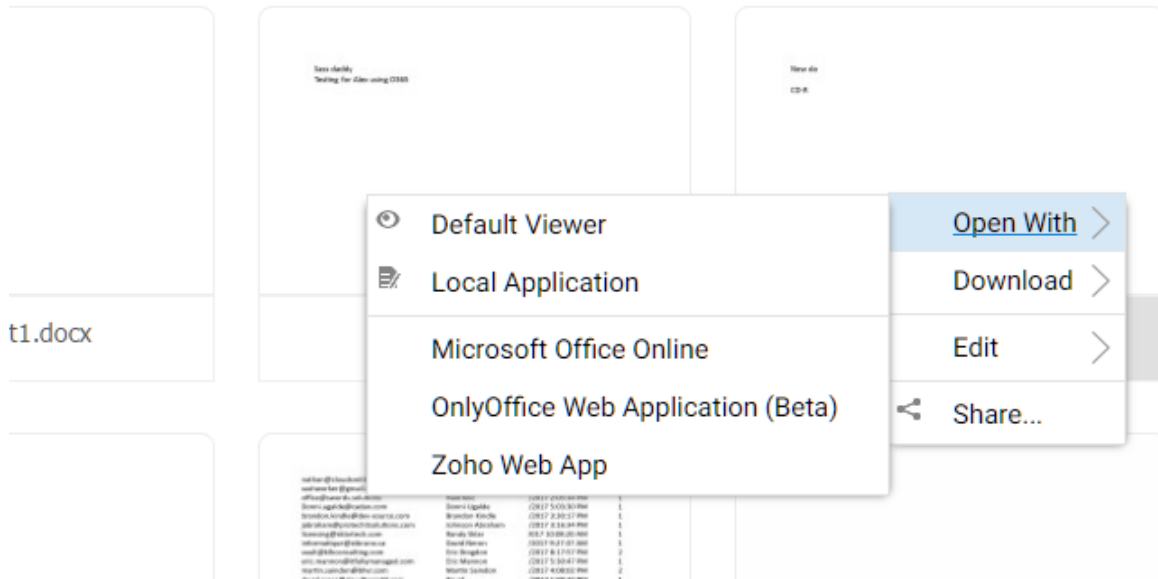


Fig. 44: APPLICATION CONTEXT MENU

### 3.5.4 Storage Manager

#### Google Drive and OneDrive Integration (Storage Manager)

##### OneDrive for Business Integration

In order to complete the OneDrive for Business Integration, you will first need to login to your company's Office 365 portal.

After that, click on the Admin tile and then on to the "Azure AD" section.

After that go to the Applications section of the company Azure AD web portal.

Add a "Web Application"

Sign On URL:

This can be set to the LoginPage.aspx for your Cluster Server.

Client ID:

This will be generated by Azure AD and you will need to copy it back to the configuration page of the Cluster Server.

App ID URI:

This can be the same as the Sign On URL

Reply URL:

This field can be <https://your-centrestack-server/management/storageconfig/SkyDriveCallback.aspx>

You will need to grant permissions according to the following pictures.

Office 365 SharePoint Online:

Windows Azure Active Directory:

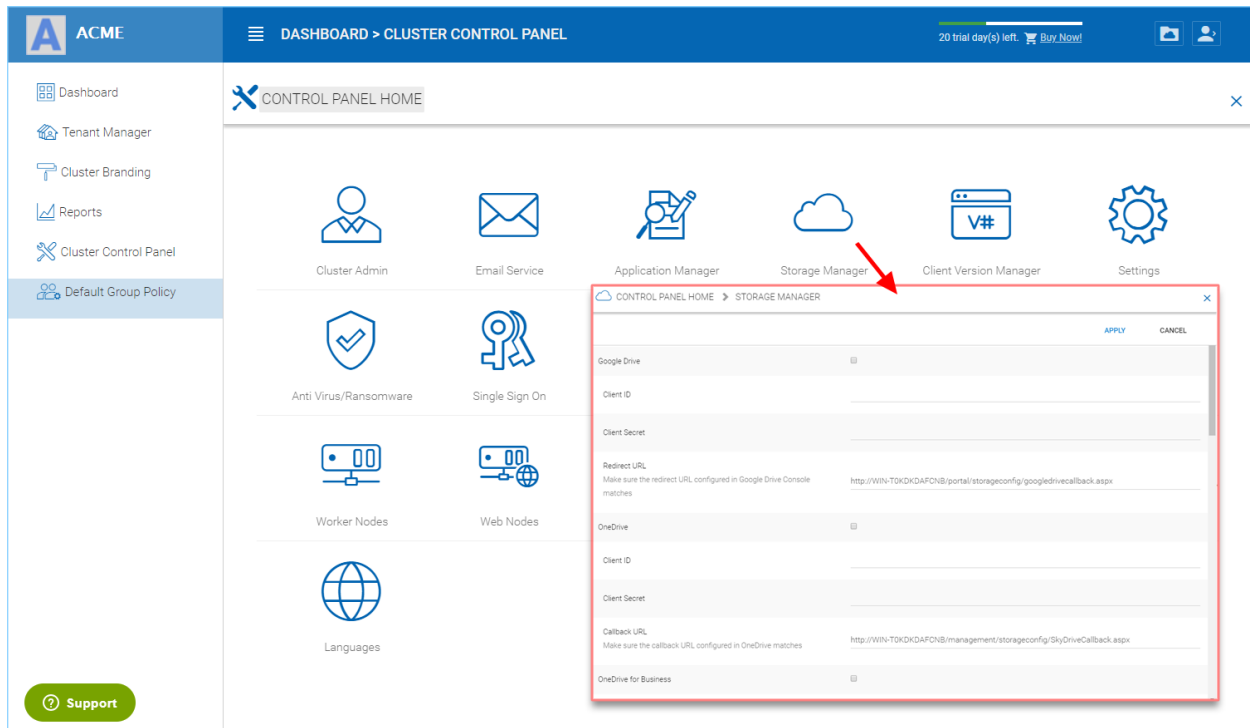


Fig. 45: CLOUD STORAGE MANAGER

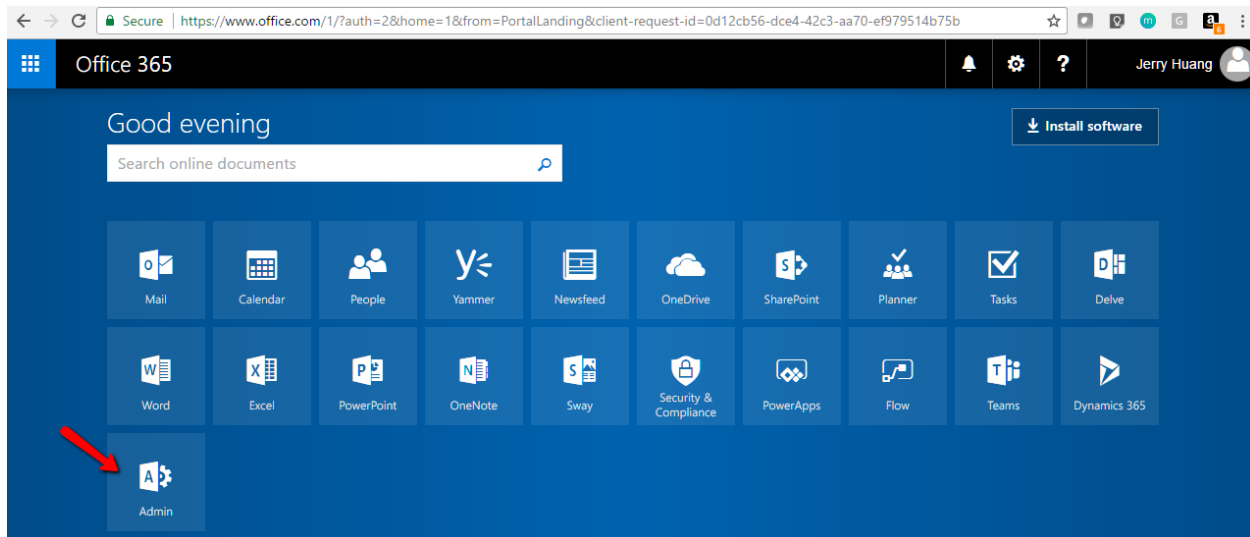


Fig. 46: MICROSOFT ONEDRIVE BUSINESS INTEGRATION

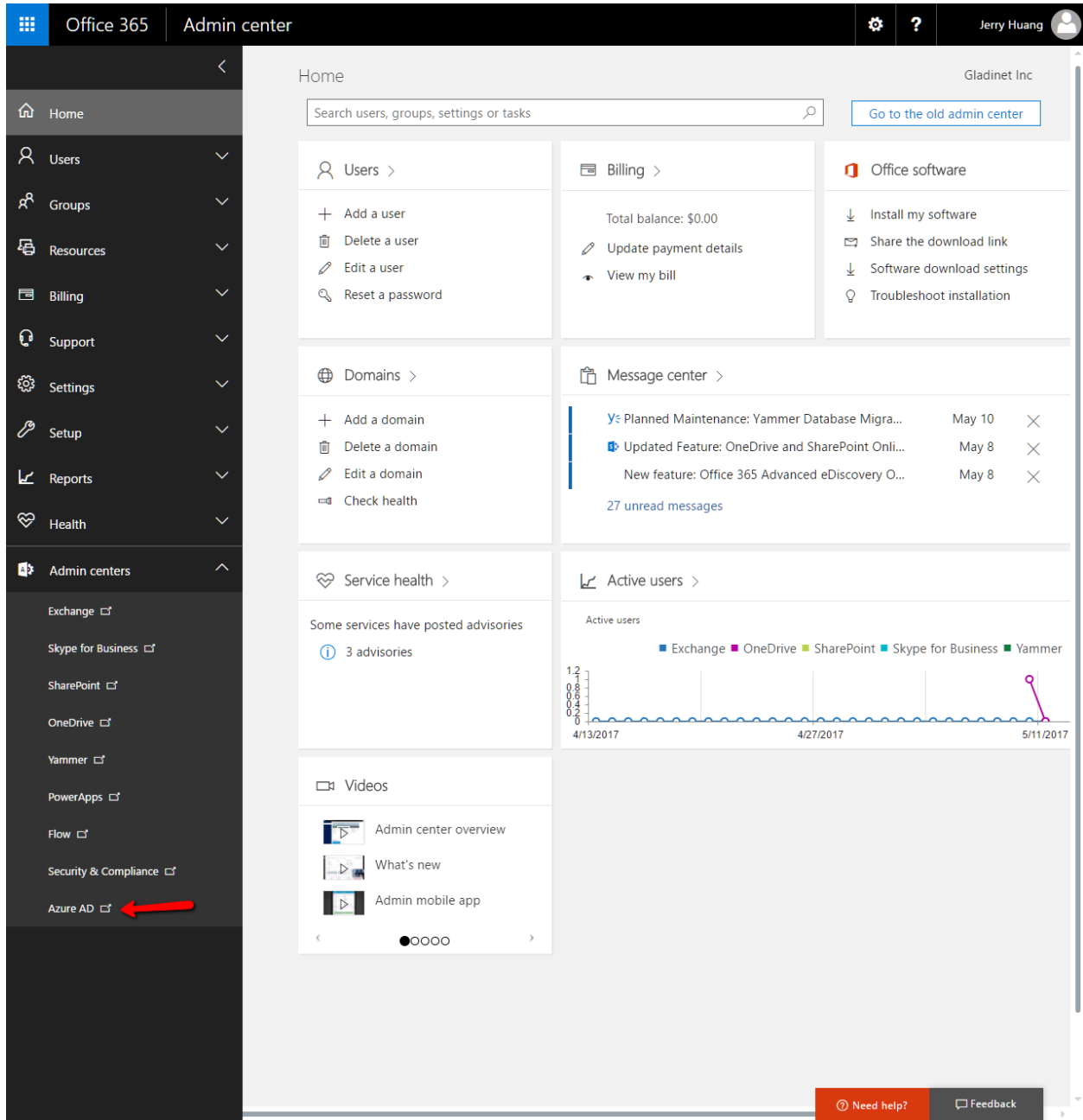


Fig. 47: AZURE AD SETTINGS

The screenshot shows the Microsoft Azure portal interface for the 'gladinet inc' tenant. The 'APPLICATIONS' tab is selected, indicated by a red arrow. The interface includes a sidebar with navigation icons, a top navigation bar with 'Check out the new portal' and 'Subscriptions', and a main content area with a search bar and a table of applications.

NAME	PUBLISHER	TYPE	APP URL
aaaaa	Gladinet Inc	Native client application	
CENTRESTACK	Gladinet Inc	Web application	http://192.168.2.11/portal/saml2.aspx/23Kx...
cluster sso	Gladinet Inc	Web application	https://office.centrestack.com/portal/saml2...
Console App for Azure AD	Gladinet Inc	Web application	http://localhost
Microsoft Azure Subscription Management		Web application	
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com/en-us/server-cio...
Microsoft Intune Enrollment	Microsoft Corporation	Web application	http://go.microsoft.com/fwlink/?LinkId=82...
Microsoft Power BI	Microsoft Corporation	Web application	https://powerbi.microsoft.com/
node4SSO	Gladinet Inc	Web application	https://node4.gladinet.com/portal/saml2.a...
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com/outlook/
Office 365 Management APIs	Microsoft Corporation	Web application	
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/sharepoint/
Office 365 Yammer	Microsoft Corporation	Web application	https://products.office.com/yammer/
Onedrive Biz	Gladinet Inc	Web application	http://my.gladinet.com/portal/loginpage.a...
onedrive biz labtech	Gladinet Inc	Web application	https://labtech.centrestack.com/portal/Log...
Outlook Groups		Web application	
Skype for Business Online (preview)	Microsoft Corporation	Web application	
SSODEMO	Gladinet Inc	Web application	http://192.168.2.11/portal/saml2.aspx/7W6...
SSOTest	Gladinet Inc	Web application	http://ssotest.gladinet.com/portal/saml2.as...
test one drive business integration	Gladinet Inc	Web application	https://labtech.centrestack.com/portal/Log...
test onedrive business labtech	Gladinet Inc	Web application	http://labtech.centrestack.com
test sso centrestack	Gladinet Inc	Web application	https://labtech.centrestack.com/portal/sam...
testgce	Gladinet Inc	Web application	https://testgce.gladinet.com/portal/saml2....
win2012-05	Gladinet Inc	Web application	http://win2012-05/portal/saml2.aspx

Fig. 48: AZURE APPLICATIONS SETTINGS



The screenshot displays the Microsoft Azure portal interface. At the top, the header shows 'Microsoft Azure' and a 'Check out the new portal' button. The user is logged in as 'admin@centrestack.com'. The left-hand navigation pane lists various services, with 'onedrive biz labtech' selected. The main content area is titled 'onedrive biz labtech' and includes tabs for 'DASHBOARD', 'USERS', 'CONFIGURE', and 'OWNERS'. The 'CONFIGURE' tab is active, showing the 'properties' section. This section contains several configuration fields: 'NAME' (onedrive biz labtech), 'SIGN-ON URL' (https://labtech.centrestack.com/portal/LoginPage.aspx), 'LOGO' (a blue square with a white cube icon), 'APPLICATION IS MULTI-TENANT' (YES/NO toggle set to NO), 'CLIENT ID' (d04ddc73-fd95-437c-ad40-22e478915692), and 'USER ASSIGNMENT REQUIRED TO ACCESS APP' (YES/NO toggle set to NO). Below the properties section is the 'keys' section, which shows a table with columns for 'VALID FROM', 'EXPIRES ON', and 'KEY VALUE'. The first row shows a key valid from 4/17/2017 to 4/17/2019. At the bottom of the page, there is a 'single sign-on' section and a dark blue footer bar with icons for 'NEW', 'VIEW ENDPOINTS', 'UPLOAD LOGO', 'MANAGE MANIFEST', and 'DELETE'.

Fig. 49: ONEDRIVE BIZ LABTECH SETTINGS

single sign-on

APP ID URI

REPLY URL  (ENTER)

permissions to other application

Office 365 SharePoint Online Application Permissions: 5 Delegated Permissions: 11

Windows Azure Active Directory Application Permissions: 0 Delegated Permissions: 1

Add application

Fig. 50: OFFICE 365 SHAREPOINT PERMISSIONS 1

single sign-on

APP ID URI

REPLY URL  (ENTER A REPLY URL)

permissions to other applications

Office 365 SharePoint Online Application Permissions: 5 Delegated Permissions: 11

Windows Azure Active Directory Application Permissions: 0 Delegated Permissions: 1

Add application

Fig. 51: OFFICE 365 SHAREPOINT PERMISSIONS 2

single sign-on

APP ID URI:

REPLY URL:  (ENTER A REPLY URL)

permissions to other applications

Application	Application Permissions	Delegated Permissions
Office 365 SharePoint Online	5	
Windows Azure Active Directory	0	1

[Add application](#)

Fig. 52: AZURE ACTIVE DIRECTORY SETTINGS

### 3.5.5 Client Version Manager

Cluster Manager > Cluster Control Panel > Client Version Manager

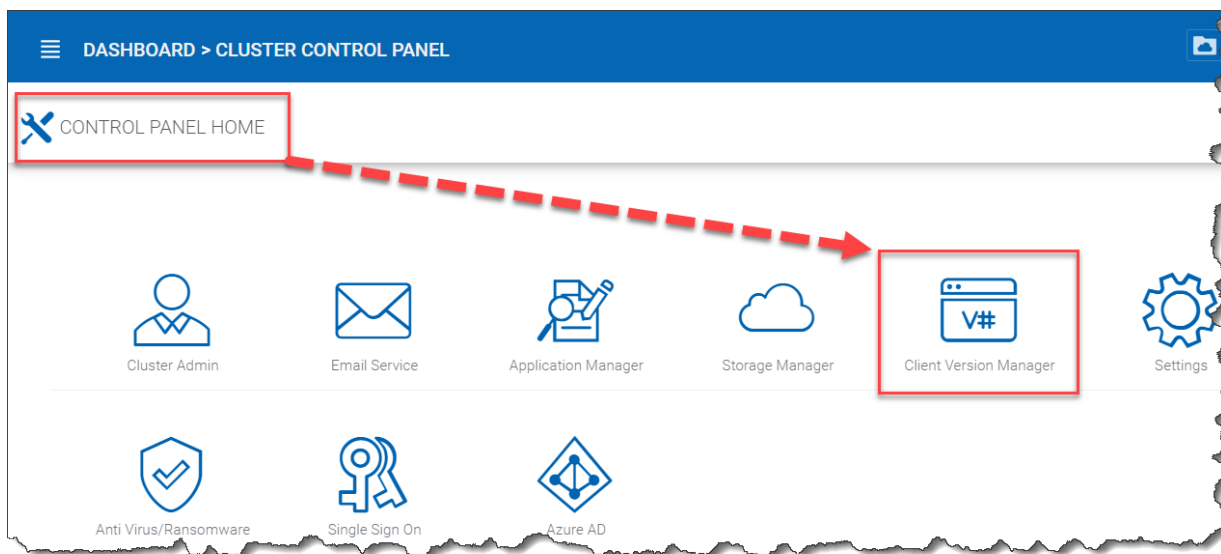


Fig. 53: CLIENT VERSION MANAGER

For Windows Client, Mac Client and Windows Server Agent, there is an auto client update feature. Each upgrade package contains the updated clients. By clicking on the Publish button [see (1) below], the newer package can be published to clients out there.

Every new Cluster Server upgrade contains the newer Windows client, Windows Server Agent and Mac Client. The Cluster users via manual download can get the clients that are included in the Cluster Server. However, for existing users with previously installed clients, those older clients will not auto upgrade until the newer client packages are published.

#### (2) Daily Upgrade Limit

This is a per-worker node setting. For example, if you have 2 worker nodes, and set the daily upgrade limit to 100, maximum 200 clients will be upgraded per day.

### (3) Apply to Users

This typically is used for testing prior to pushing the client out.

### (4) Do Not Apply to Users

This typically is used for testing prior to pushing the client out and to exclude certain users.

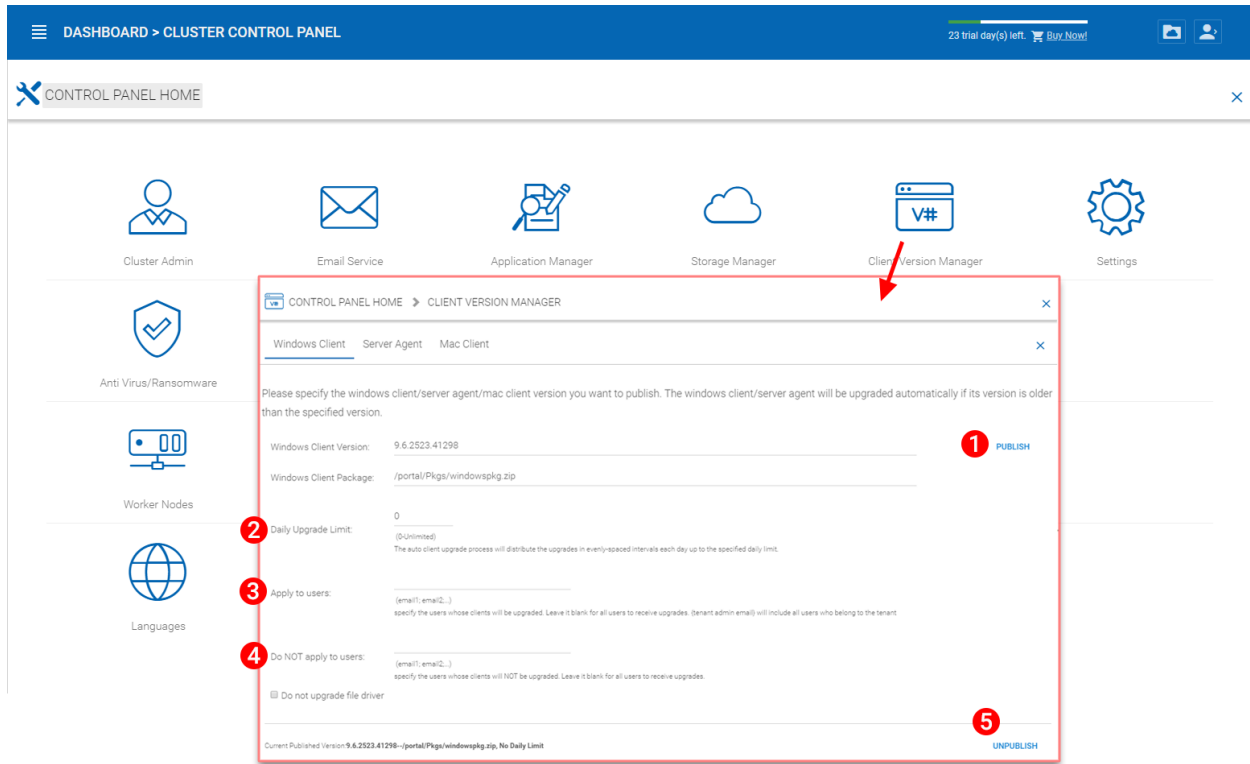


Fig. 54: WINDOWS CLIENT VERSION SETTINGS

**Note:** The windows client out there has a process running as a background windows service. The service will periodically check for a newer upgrade in about 1-2 hour intervals. Once a newer client package is published and discovered, the newer package will be downloaded. However, if the client is still actively running, the replacement and upgrade will not happen until the client application is stopped and restarted. This usually happens when the user logs off their Windows or restarts their desktop altogether.

If the Windows client software is actively running, the user may be seeing a message popup from the system tray area asking the user if they want to restart the client software and to receive the newer version.

Once a client is published for client auto upgrade, you can use Unpublish (5) to stop the client auto upgrade.

### Server Agent

Windows Server Agent can be separately published for auto upgrade.

### Mac Client

Mac client can be separately published for auto upgrade.

**DASHBOARD > CLUSTER CONTROL PANEL**

CONTROL PANEL HOME > CLIENT VERSION MANAGER

Windows Client **Server Agent** Mac Client

Please specify the windows client/server agent/mac client version you want to publish. The windows client/server agent will be upgraded automatically if its version is older than the specified version.

Server Agent Version:

Server Agent Package:

☐ Do not upgrade file driver ☐ Do not restart server agent after upgrade

**PUBLISH**

Current Published Version: 10.10.2865.45294--/portal/Pkgs/windowspkg.zip

Fig. 55: SERVER AGENT AUTO UPGRADE

**DASHBOARD > CLUSTER CONTROL PANEL**

CONTROL PANEL HOME > CLIENT VERSION MANAGER

Windows Client Server Agent **Mac Client**

Please specify the windows client/server agent/mac client version you want to publish. The windows client/server agent will be upgraded automatically if its version is older than the specified version.

Mac Client Version (OSX 10.13/10.14):

Mac Client Package:

**PUBLISH**

Current Published Version: 10.8.44514--/portal/Pkgs/Mac/MacClient.9.dmg.zip

Fig. 56: MAC CLIENT AUTO UPGRADE

### 3.5.6 Settings

Cluster Manager > Cluster Control Panel > Settings

Under cluster settings, you can configure auto-client update, web applications, and other settings like 2-Step Verification, multiple domain support, etc..

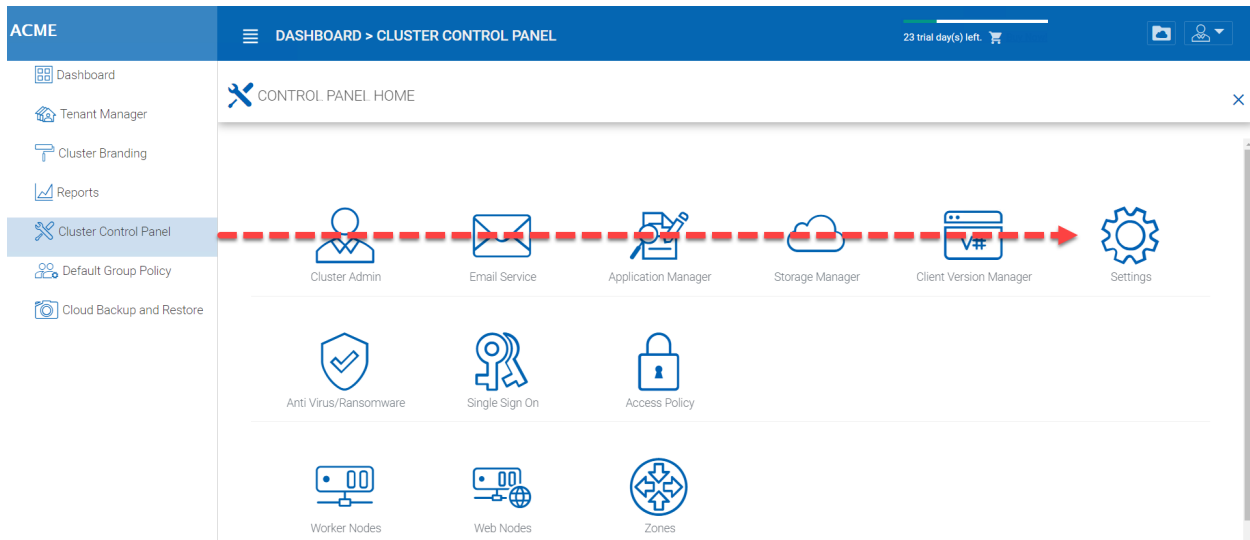


Fig. 57: CLUSTER SETTINGS

#### 3.5.6.1 Cluster Settings

Cluster Manager > Cluster Control Panel > Settings > Cluster Settings

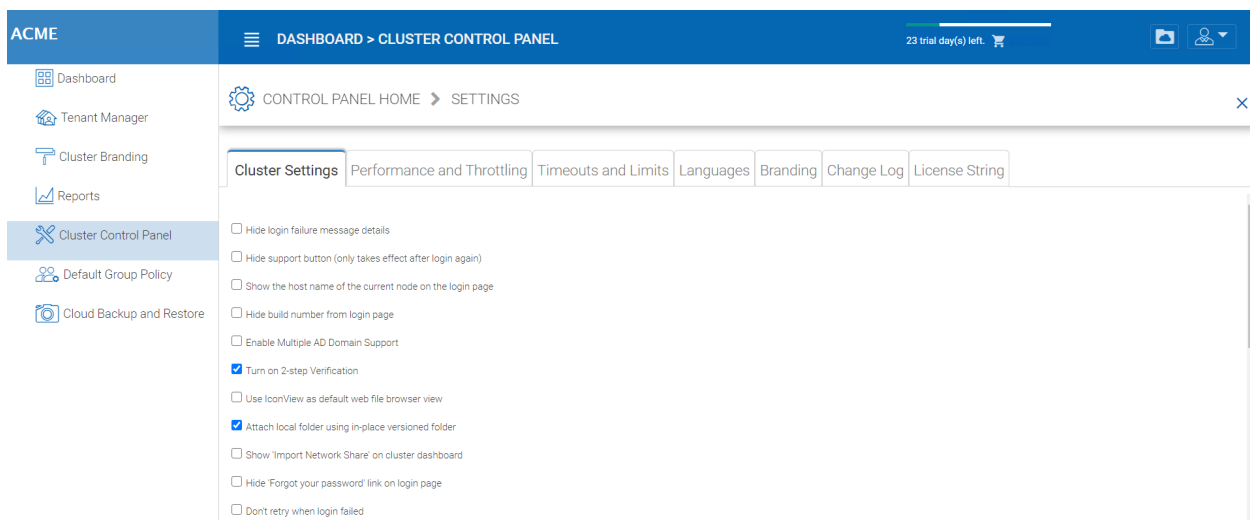


Fig. 58: CLUSTER SETTINGS PERMISSIONS

#### Hide Login Failure Message

When checked, the login failed message will be replaced by a very generic “Login Failed” message. When un-checked, it may return a more meaningful login error, such as user-not-found, authentication-error and

so on. This is a security feature if you don't want to give out too much information for hackers to guess a reason for authentication failure.

#### **Hide support button**

This hides the floating support icon.

#### **Hide build number from login page**

This controls the build number on the web portal login page.

#### **Enable Content Management Policies – Reserved**

#### **Show file dashboard by default**

#### **Hide 'Forgot your password' link on login**

Most often it is used when Active Directory integration is set. The user will need to do a forget-and-change password the normal Active Directory way instead of the way CentreStack provides. In this case, it is recommend to hide the "Forgot your password" link.

#### **Don't retry when login failed**

Most often it is used when the Active Directory user has low failed-count on lock-out policy. When the user's password is wrong, a few retries can lock out the user's Active Directory account. The retry feature can be used when there is no Active Directory lock out or when the lock out count is high.

#### **Show 'purge storage option' when delete user**

By default, when a user is deleted, the user's home directory storage content is not touched for later use or review. If it is desired to delete the user's content when the user is deleted, this can show the purge option.

#### **Enable Multiple AD Domain Support**

In the multi-tenant environment, you can always link one Active Directory to a tenant. However, in some cases, a single tenant may have multiple un-related Active Directories. In this case, Enable Multiple AD Domain support will be useful.

When you have multiple Active Directory from multiple forests in a specific tenant, you can turn on this option. The Cluster Server software is capable of automatically searching for domains in one single forest.

However, for multiple forests, the software will allow you to manually enter the root of each domain when this option is enabled.

---

**Note:** The AD support here is related to using LDAP for Active Directory connectivity.

If you are using "Server Agent" to connect to multiple Active Directories in proxy modes, you don't need to turn it on here.

---



---

**Note:** If I turned it on, where to see the change?

You will see the difference in the per-tenant Active Directory setting page. Instead of a single AD setup, you will see a table that allows you to add multiple rows, with each row represents a single Active Directory LDAP connection.

---

#### **Turn on 2-step Verification**

The Cluster Server supports Google Authenticator, Amazon Virtual MFA soft token for 2-step verification. When this setting is turned on, users will see the option to configure 2-step verification in their web portal.

#### **Don't send email notification to user when purge deleted content**

When the user delete files, they are not actually deleted immediately. The purge is asynchronous and scheduled at a later time. This setting controls the notification.

#### **Don't send email notification to admin when purge deleted content**

When the user deletes files, They are not actually deleted immediately. The purge is asynchronous and scheduled at a later time. This setting controls the notification to the administrator.

#### **Use 'Icon View' as default web file browser view**

Icon view is set when this setting is enabled. (The opposite is ListView)

#### **Use Ghost Script to generate PDF preview**

There are two ways in the system to generate PDF preview. This setting will force the system to use one way or the other. For example, force it to use Ghostscript to generate PDF preview.

#### **Preview pdf files with browser builtin viewer**

When selected, the PDF file will be rendered in the web browser on the web browser side. Otherwise, it is rendered on the server side first and shown to the end user in browser.

#### **Retrieve avatar from third party service (i.e. Google)**

This is a usability feature that users's picture can be queried from Google.

#### **Hide file extension in web file browser**

This setting will hide the file extension.

#### **Disable Windows Client Auto-Logon**

This is a security feature. The result is every time the windows client is done running, the next time the user tries to login, it will not remember the login token and the user will have to re-type the credential to get in.

#### **Use short url**

Use shorter URL for web links generated for file/folder sharing.

#### **Allow personal data tagging**

#### **Attach local folder using in place versioned folder**

When synchronize folders from remote PC/Mac to CentreStack, using in place versioned folder will make the folder keep the same folder structure as the folder that is being uploaded. Otherwise CentreStack manage the folder content on the server side in its own ways.

#### **Only allow access performance information from local host**

only allow accessing performance data from <http://localhost> and not from external URL.

#### **Show 'Import Network Share' on cluster dashboard**

#### **Web Browser Session Timeout (minutes, 0 - never timeout)**

This is the web browser session time out value. Default is set to 15 minutes. For default cluster administrator, we recommend increase this value to a bigger number so it is easier for web based management work not to time-out too soon.

#### **Native Client Token Timeout (days)**

For Windows client and Mac client, this defines the token time to live.

#### **Distributed Lock Idle Timeout (minutes, 0 - never timeout)**



This setting is related to automatic file locking. When a file is automatically locked, the machine that has the file locked will need to maintain a healthy heart beat with the Cluster Server. If the machine is offline (idle) and can't report back to the Cluster Server for a period of time, the lock that was automatically grabbed will need to be released.

If this is not desired, the user can always use manual “Check Out” to lock a file and that will not be subject to the timeout.

### Open third party web application in new window when the height of the web browser is less than

This is a usability feature. When using third party web application to edit documents in Cluster Server web browser file and folder view, if the web browser height is too short, the third party web application may not function properly.

### Max Device Count(Concurrent Device Count) for Each User (0-Unlimited)

This is the number of concurrent devices connected to the Cluster Server for each user. The default is not limited.

## 3.5.6.2 Performance and Throttling

Cluster Manager > Cluster Settings > Settings > Performance and Throttling

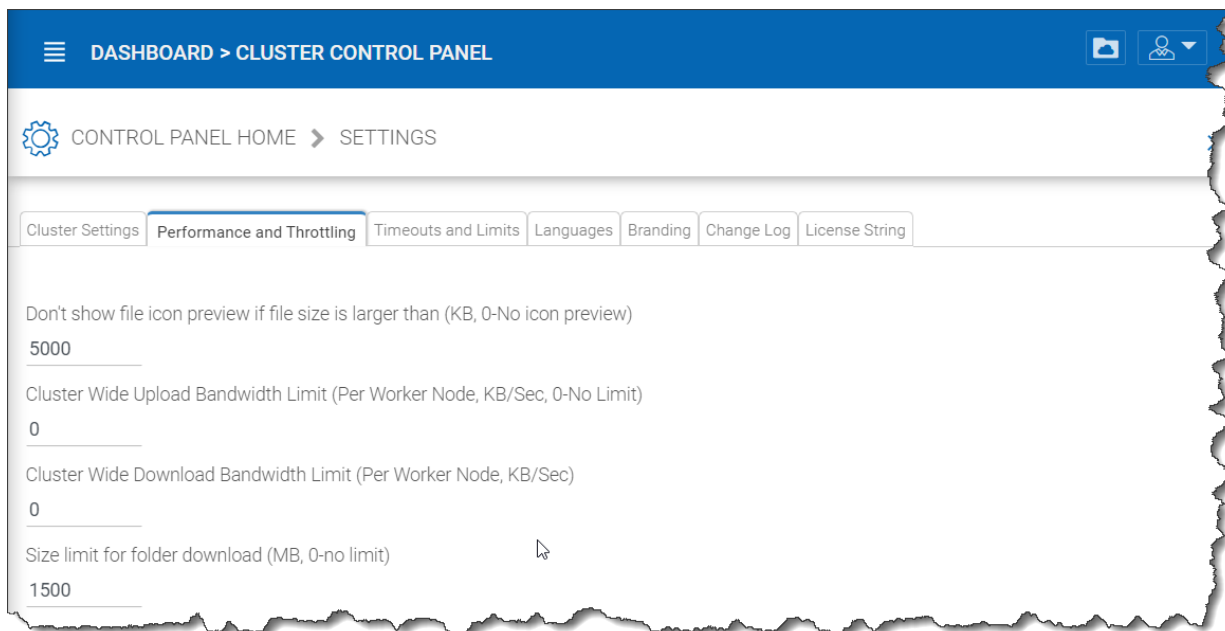


Fig. 59: PERFORMANCE THROTTLING

### Don't show file icon preview if file size is larger than(KB, 0-No icon preview)

This is used to control iconview thumbnail generation in the web browser files and folders view. The generation of thumbnail takes CPU power from the Cluster Server. For big files, the generation of thumbnail may negatively affect the system performance. So it is recommended to cap the feature to a certain image size.

### Cluster Wide Upload Bandwidth Limit(Per Worker Node, KB/Sec, 0-No Limit)

This is to limit upload bandwidth.

### Cluster Wide Download Bandwidth Limit(Per Worker Node, KB/Sec)

This is to limit download bandwidth.

### Size limit for folder download (MB, 0-no limit)

This is to prevent user downloading a very big folder and using up all the Cluster Server resources.

### 3.5.6.3 Timeouts and Limits

Cluster Manager > Cluster Control Panel > Settings > Timeouts and Limits

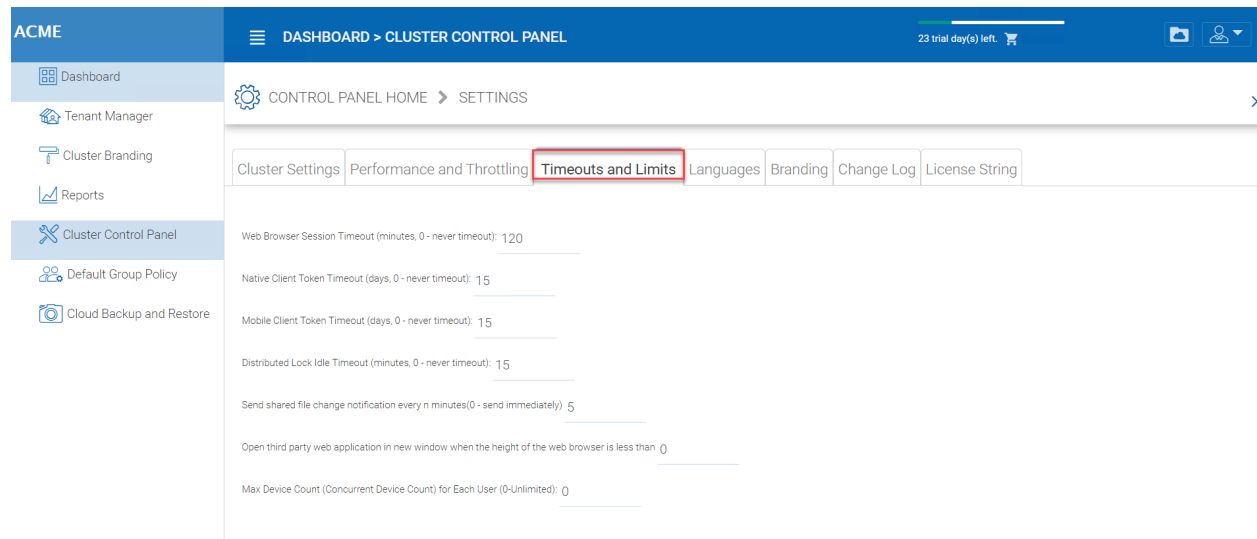


Fig. 60: TIMEOUTS AND LIMITS

### 3.5.6.4 Languages

Cluster Manager > Cluster Control Panel > Settings > Languages

This section sets up the web portal languages and also the client application languages for Windows client.

We have automated translation and provided the resource files that you can use to localize the web portal and clients in the language of your choice. If there are strings that not translated yet in the language you want, just go ahead and select the string and put in the translated string in the window for the language selected.

### 3.5.6.5 Branding

Cluster Manager > Cluster Control Panel > Settings > Branding

#### Don't Show Tutorial Videos

At different places in the web portal, there are tutorial videos. This setting is to hide those videos, which may have CentreStack references inside.

#### Enable Tenant Branding

Allow tenants in the system to have their own co-branding on a tenant-by-tenant basis. The branding can override the default Cluster wide branding when the solution is accessed via a specific URL. Most of the time, a wild card SSL certificate is used so the Cluster Server solution can be binded to different URL's within a common suffix.

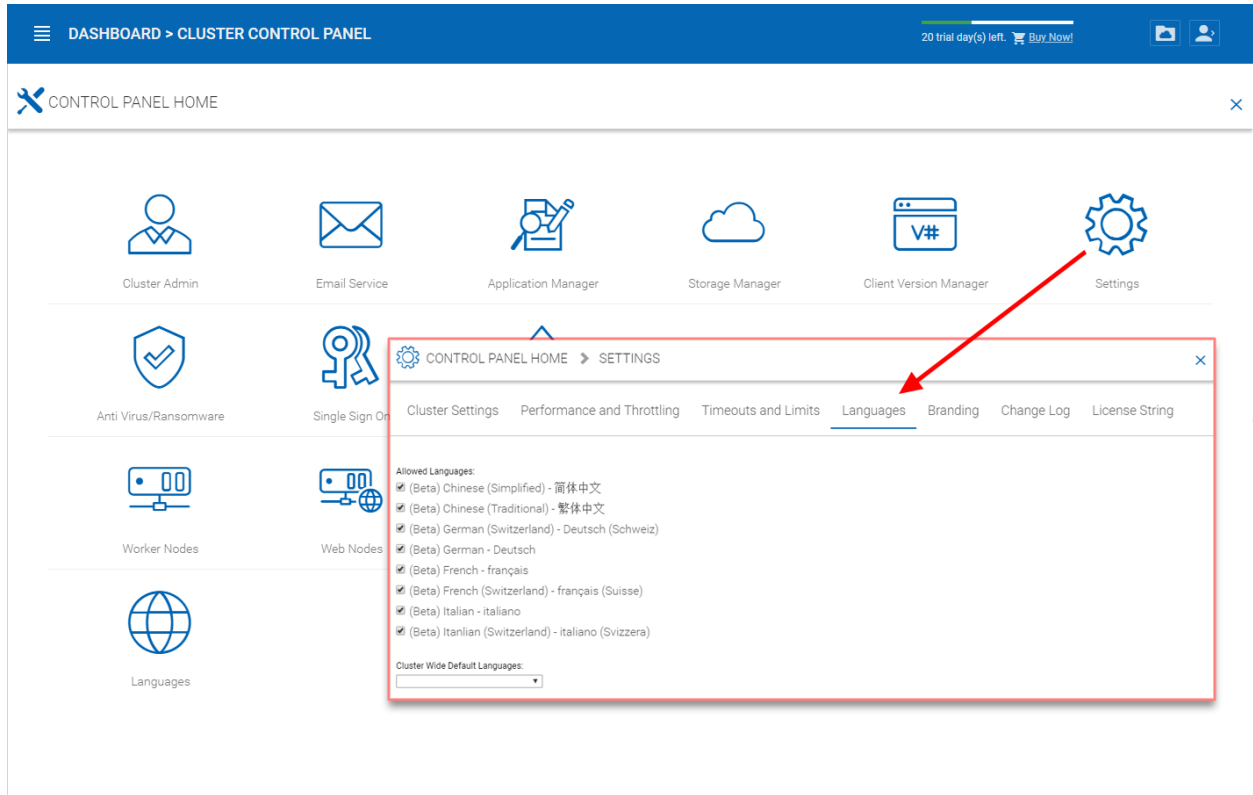
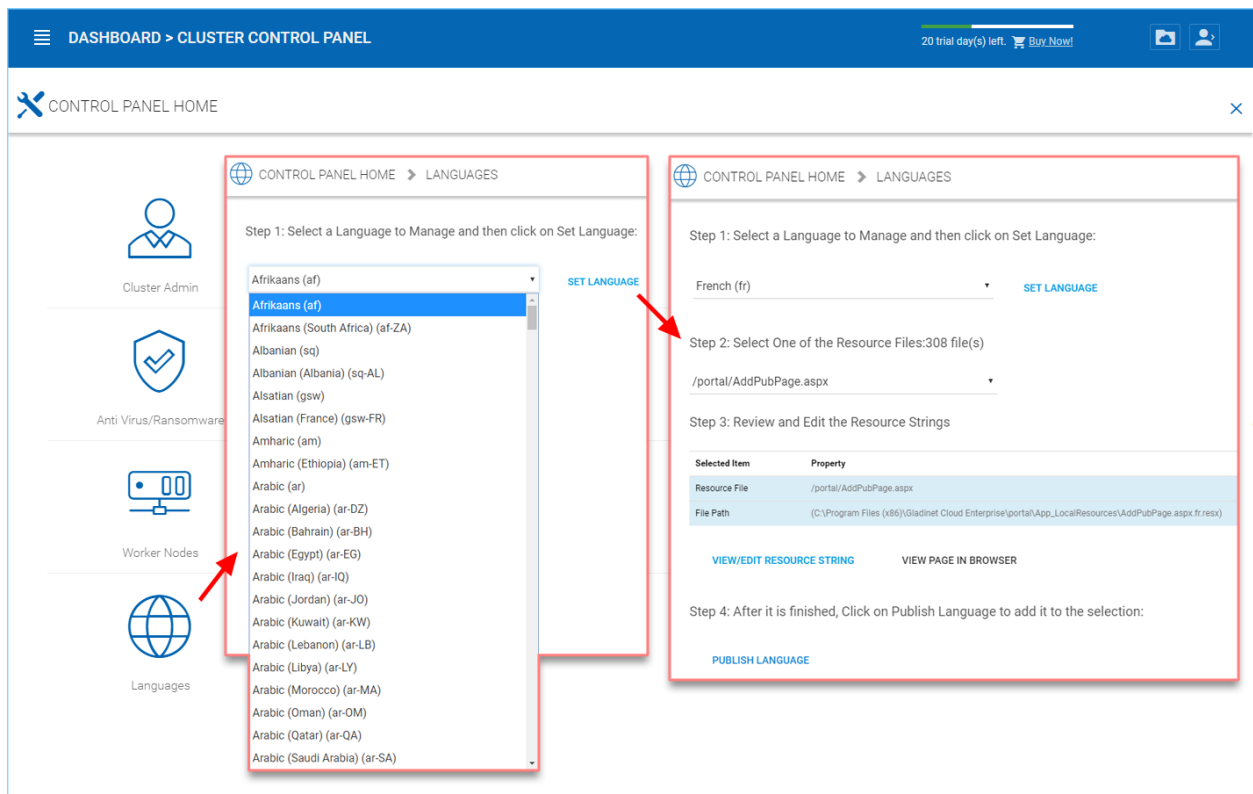


Fig. 61: LANGUAGE SETTINGS



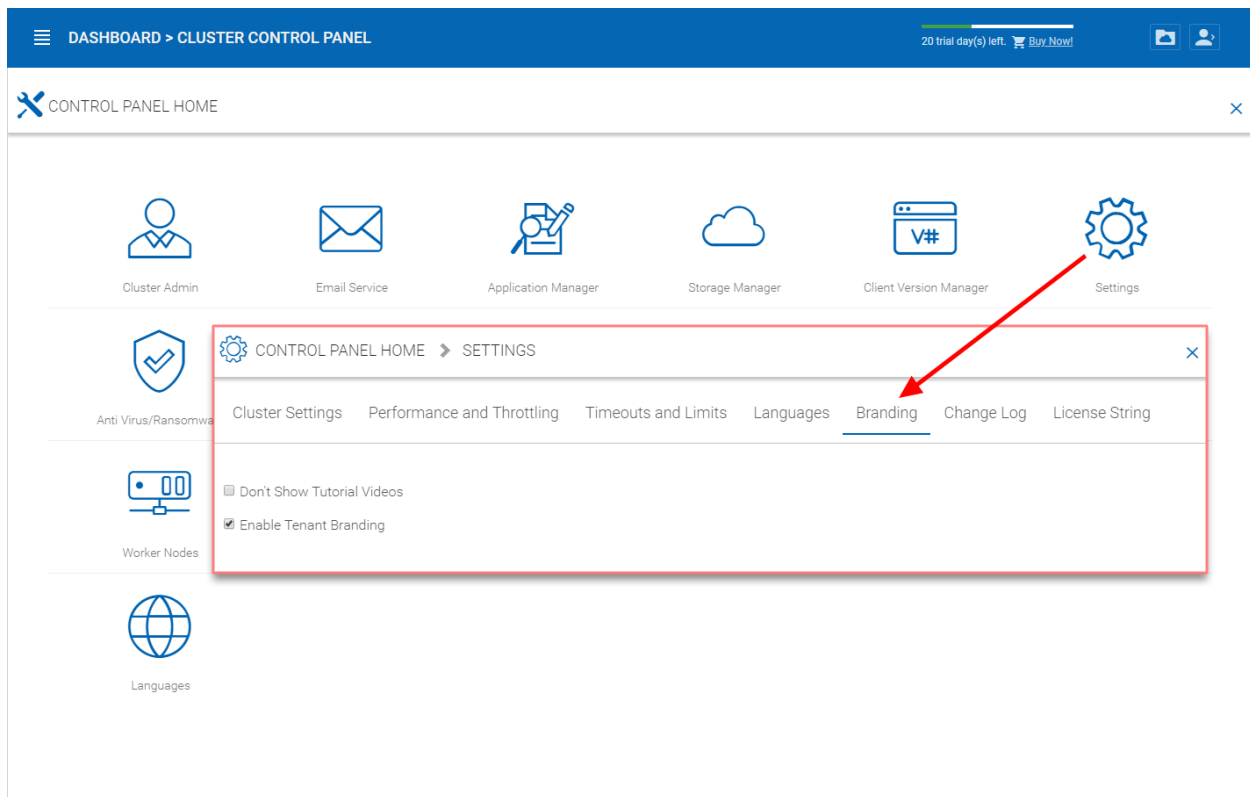


Fig. 62: ENABLE TENANT BRANDING

For example \*.mycompany.com , while tenant1.mycompany.com is for tenant 1's access.

### Only allow branded client to access

This can lock out the generic client and only allow the branded client to connect.

### Branding Id

This setting only applies to full-branding clients. For the full-branding client, it is possible to lock the full-branding clients to only connect to the branded Cluster Server. When set, it will lock out the white-label clients or other non-branding clients and will not allow them to connect.

### 3.5.6.6 Change Log

Cluster Manager > Cluster Settings > Settings > Change Log

#### Keep file change log for n days

This is a cluster wide retention policy for the file change log.

The file change log is in the SQL database, for deployments that are using SQL Express, it has size limitation for the database. In the deployment guide, there is option to split the file change log into MySQL database or split it to a different SQL database. This option typically is used to keep the size of SQL small.

---

**Note:** After the Cluster Server is running in production mode for a while, we recommend reviewing the file change log database table and the file index table to see how big those tables are.

---

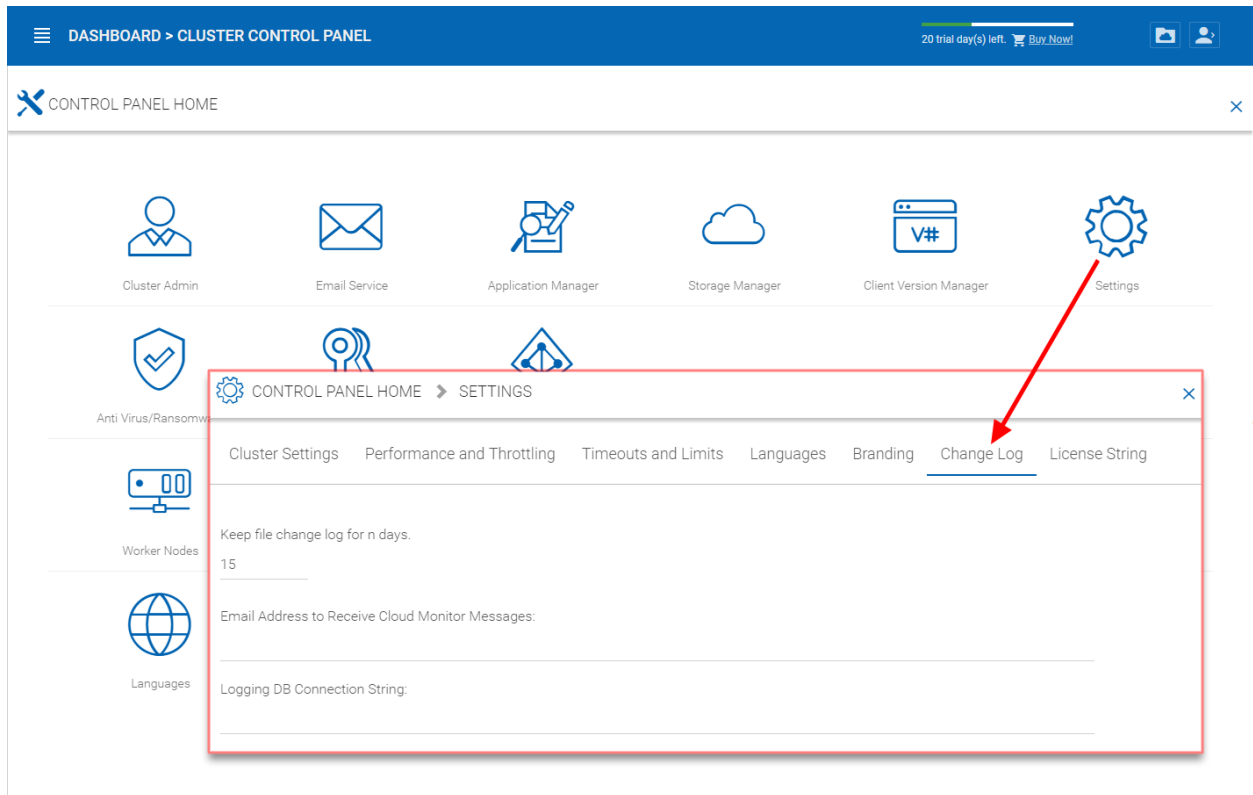


Fig. 63: CHANGE LOG SETTINGS

### Email Address to Receive Cloud Monitor Messages

From time to time, the cluster monitor service may send an email about the status and alerts.

### Logging DB Connection String

This is to split the file change log, device table, file index table and audit trace table out of the main database into a secondary database. The secondary database can be a Microsoft SQL Server or a MySQL Community server.

The Cluster Server database is split into the core part and the logging part. The core part can store the DB connection string that connects to the secondary database. This setting used to be in the web.config file.

### 3.5.6.7 License String

Cluster Manager > Cluster Settings > Settings > License String

**License String** – Reserved.

This is for Cluster Servers that are isolated from the Internet, can't be activated online and has to use a license string for offline activation.

## 3.5.7 Anti Virus

Cluster Manager > Cluster Settings > Anti Virus

You can enable anti-virus protection which will ensure that the files being uploaded via the Cluster Server are scanned by the selected anti-virus software.

You will first need to obtain the anti-virus service that is independent from the Cluster Server, and get it directly from the anti-virus vendor. After that, you can integrate the anti-virus service into the Cluster Server.

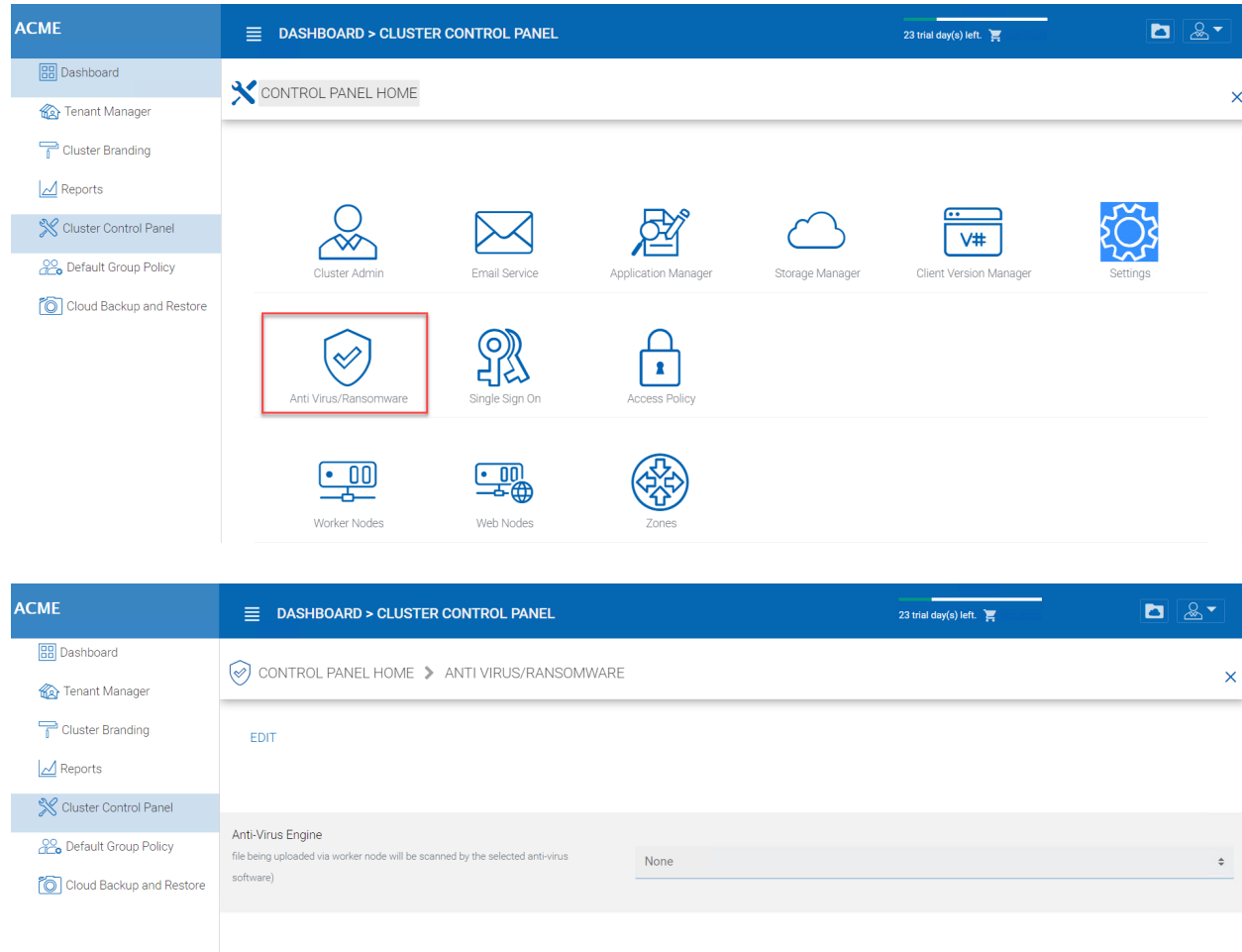


Fig. 64: ANTI-VIRUS SETTINGS

### 3.5.8 Worker Nodes

Cluster Manager > Cluster Control Panel > Worker Node

Cluster Server Farm has two types of nodes, one is “Worker Node” and the other is “Web Nodes”.

This type of node will contain services like Web Browser Based File Manager, Storage Service Connectors, and etc. Again, additional nodes can be added as the load increases. Because there is cache information located on each node, users will have an affinity to a single node once it is assigned. If the load balancer distributes users evenly to all worker nodes, the cache information may exist on all worker nodes.

#### Worker Node Settings

There are some settings that apply to all worker nodes. After you click on the “Settings” icon, the Advanced Settings panel will show.

#### Always force SSL on Login

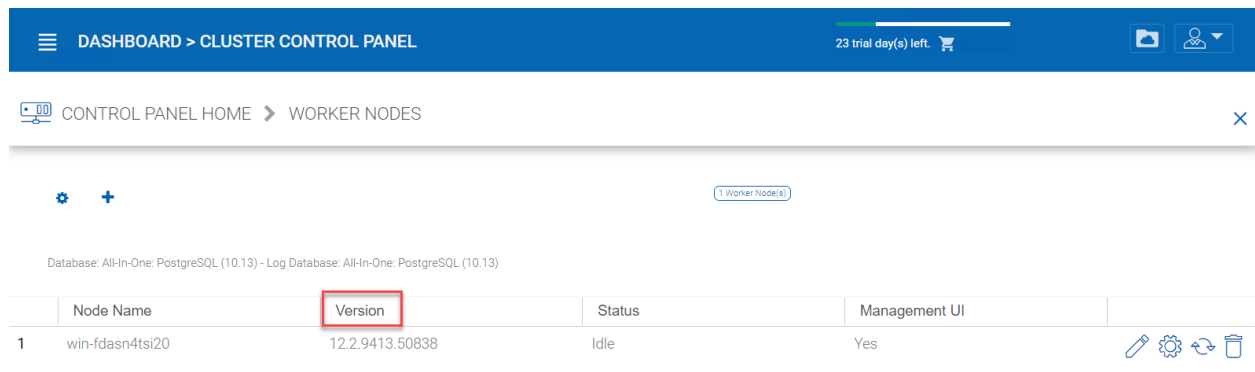
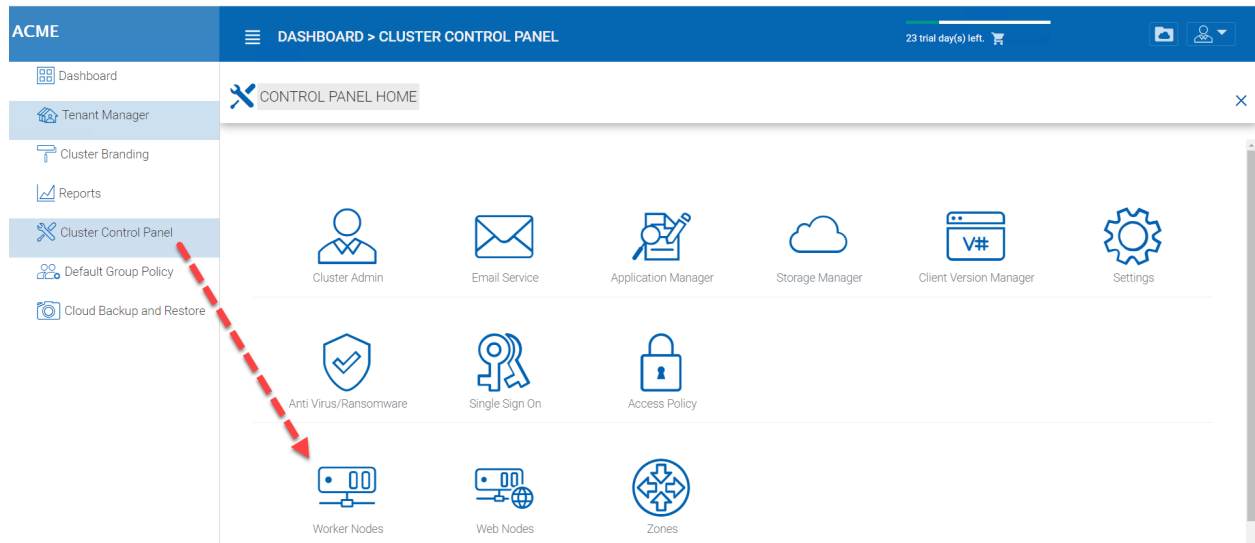


Fig. 65: CLUSTER SERVER FARM NODES

Fig. 66: SSL NOTICE

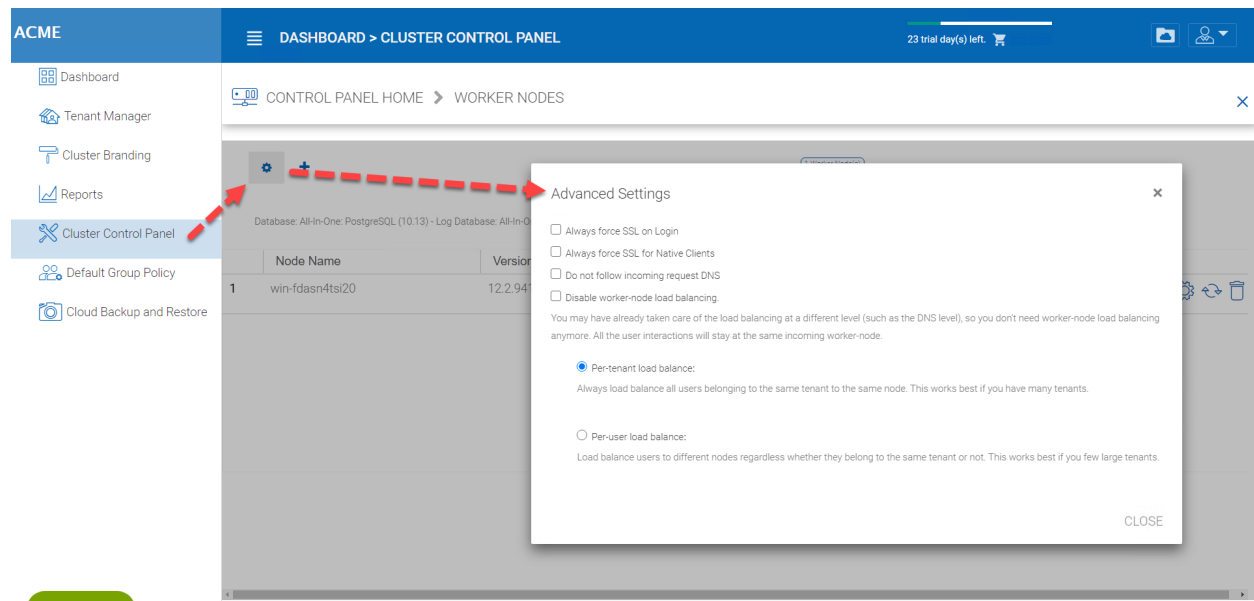


Fig. 67: WORKER NODE SETTINGS

In a production environment, almost 100% of the time you will need to check “Always force SSL on Login”. When this is checked and when CentreStack detects that the incoming connection is HTTP, it will do a redirect to HTTPS. If you turn on SSL, you will need to setup SSL certificate first.

However, if you have SSL-offload, such that SSL is offloaded to a hardware appliance, and after that, the incoming connection is HTTP between the hardware appliance and CentreStack. In this SSL-offload case, you will NOT check “Always force SSL on Login” because it will create an infinite redirect loop because the incoming connection is always HTTP as far as the CentreStack Server is concerned.

### Always force SSL for Native Clients

In a production environment, almost 100% of the time you will need to check “Always force SSL for Native Clients”.

Especially, in the case of SSL-Offload, you MUST check “Always force SSL for Native Clients”. Otherwise, the CentreStack Server may think that the incoming connection is HTTP so it will continue to encourage the native clients (such as Windows client) to use HTTP instead of using HTTPS.

---

**Note:** In iOS devices, the Application Transport Security may be enforced by the operating system and HTTPS must be used for an iOS Application to connect to the Cluster Server.

---

### Disable worker-node load balance

When you have your own load balancer, you will disable worker-node load balancing. The Cluster Server has built-in node-affinity load balancing, which can be per-tenant or per-user. When you have your own load balancer, you may have session-affinity or just simple round-robin, either one is fine.

---

### **Note:** How to add a worker node?

You just go ahead to install the Cluster Server during the installation and point the Cluster Server to the same database. Once the installation of the Cluster Server worker node is completed, reboot. The web portal page will pop up, asking you to add the worker node to the server farm.

---



**Warning:** What if you changed the Cluster Server's Host Name?

For Windows server 2012 and later Server OS, when a server is newly provisioned, it is typically named in host-name format similar (WIN-ABCDEFGH). Sometimes, it is desired to change the name in the Control Panel -> Systems. If the Cluster Server is already installed, changing the name will make the Cluster Server add itself again with the new name. So next time when you visit <http://localhost> on the Cluster Server after the server has been renamed, you will see the worker node section has both the node with the old name (which no longer exists) and the node with the new name (Which is current and good). In this case, you just need to simply remove the worker node with the old name.

## Worker Node Properties

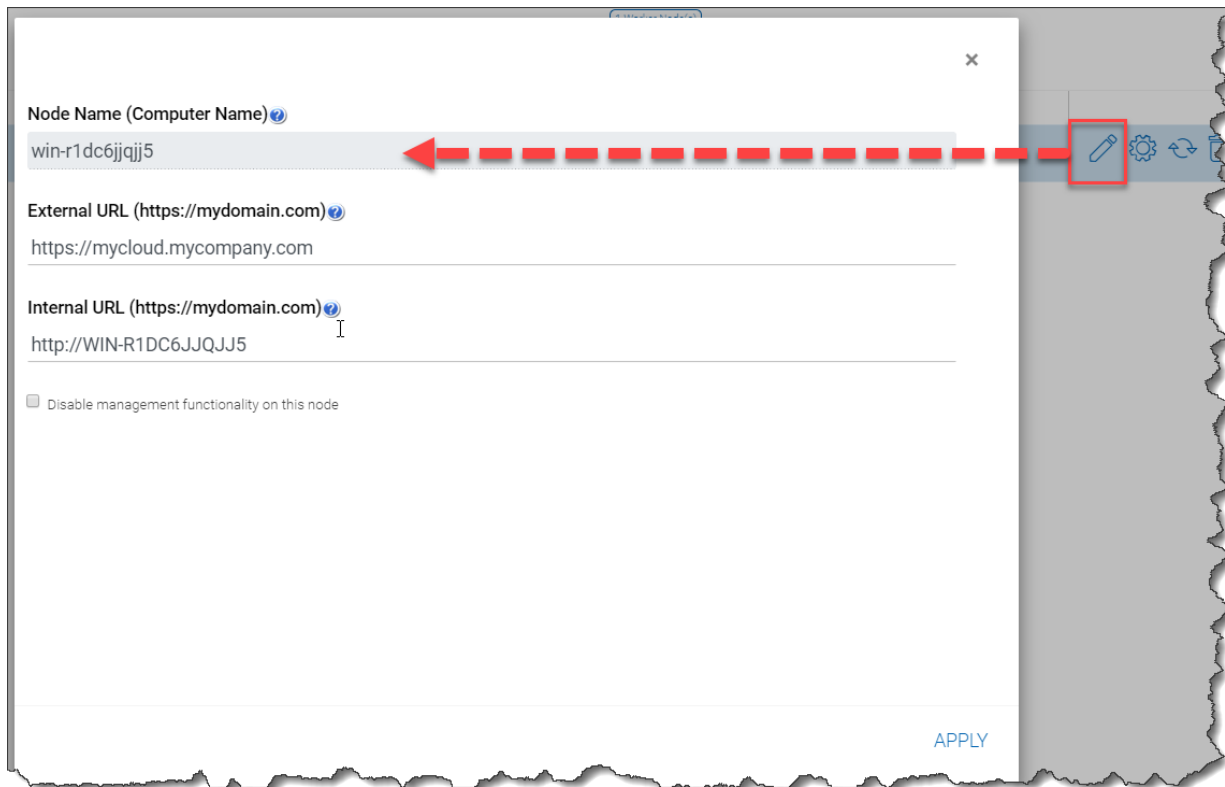


Fig. 68: WORKER NODE PROPERTIES

You may need to modify the worker node properties when you setup SSL and the DNS name for the cluster.

### Node Name

The **Node Name** needs to match the worker node's hostname. Sometimes, if you rename a worker node's Windows hostname (NETBIOS name) after the Cluster Server installation, upon reboot, the Cluster Server will pop up a web page, asking you to add the new worker node. In that case, you can go ahead and add the new worker node and then delete the old worker node.

### External URL

The **External URL** needs to match the worker node's external URL. In a production environment, this typically is in an <https://> format with the node's DNS name.

External URL is a critical property for Email templates. Once the Cluster Server installation is finished, the dashboard will have a warning message, 'External DNS has not been configured for this worker node.'

Some functionality may not work properly. Config Now'

The moment that you have finalized on the External DNS name of the Cluster Server, you must come here and configure the ExternalURL property for the Cluster Server.

### Internal URL

The **Internal URL** is the node's internal URL, typically in the form of <http://local-ip-address> format. In later Cluster Server builds, this property is hidden and there is no need to set it any more.

### Disable management functionality

You can create an internal facing worker node (that doesn't have an externalURL) and only allow management functionality on this worker node. This is a security feature.

### Edit Cloud Monitor Setting

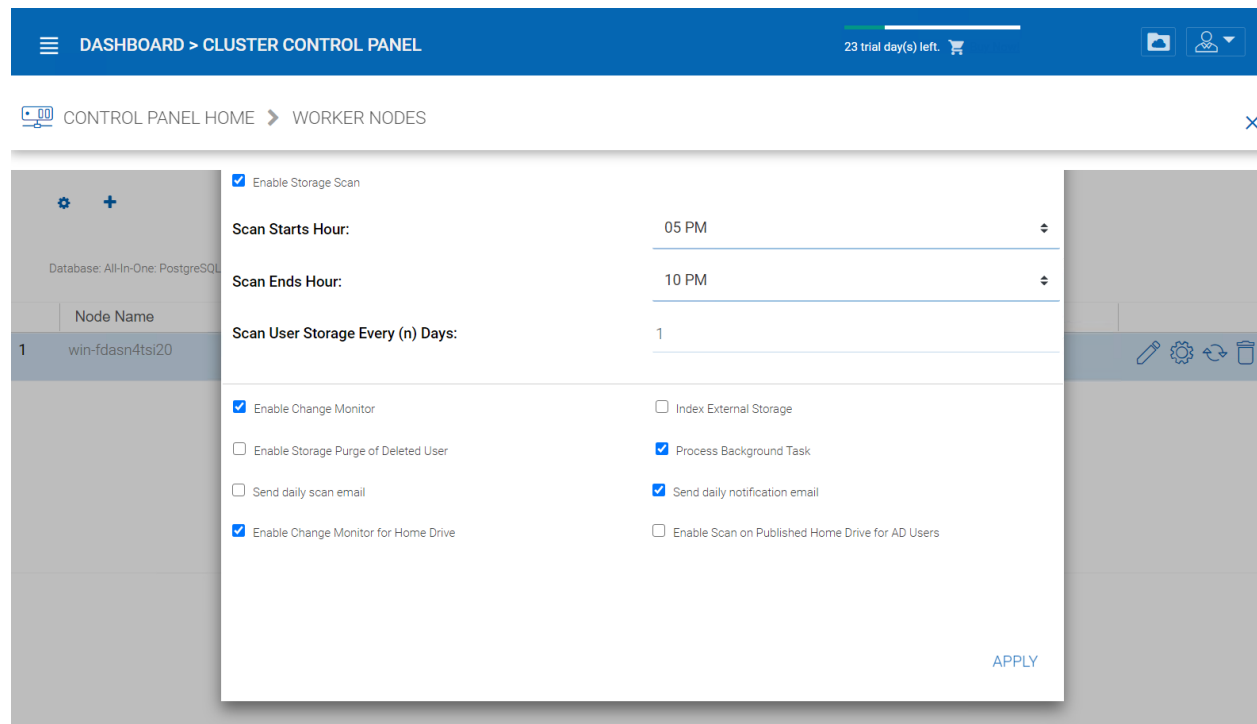


Fig. 69: CLOUD MONITOR SETTINGS

### Enable Storage Scan

Enables or disables storage scan on the worker node. On the worker node, there is a cloud monitor service. The service will be doing background monitoring and make scan storage from time to time to correct quota calculation and perform other maintenance tasks.

### Scan Starts Hour

Typically you will set the scan start time to sometime in the early morning like 1AM.

### Scan End Hour

Typically you will set the scan end time to sometime in the morning like 8AM before everyone comes to work. The main idea is to leverage idle time (when people are not at work) to do the scanning.

### Scan User Storage Every (n) Days

Typically you can set it to every week or every other week. so a number between 7 to 15 is reasonable.

### Enable Change Monitor

Enable change monitor monitors the attached local storage such as storage from file server network share and report file change notification to remotely connected clients. This usually is required if your users are both modifying documents directly from the backend attached network share and also from the front end Cluster access clients.

### Index External Storage

This setting will index storage services added via the “Storage Manager”. The index will be written to the files table in the database.

### Enable Storage Purge of Deleted User

When a user is deleted from the system, the user’s home directory is not immediately removed. And a lot of times, you don’t want to delete it at all. For example, a user is deleted from the Cluster Server, but the user may still continue to use the files and folder directly from the network.

### Process Background Task

Whether this specific node will process background task.

### Enable Change Monitor for Home Drive

If Active Directory Home Drive integration is on, this will allow the Cluster Server to monitor the changes on the home drive and notify remote client agents that the files/folders have changed.

### Send daily scan email

If the storage scan is enabled, a daily scan email will be sent to the cluster administrator about the result of the scan.

## 3.5.9 Web Node

Cluster Manager > Cluster Control Panel > Web Node

---

**Note:** In a small deployment, there is no need to have web nodes. You can go straight to worker nodes since worker nodes by defaults are web nodes too.

---

The Account Management, Sign-in and Load-balancing services will be installed on this physical machine (or virtual machine). Depending on the load, you may need 1 to N such nodes. Normally, we recommend for every web front node, you can have 10+ worker nodes. When you have small deployments, you can skip web front nodes and combine them into worker nodes. All the installation work is the same. If you do not need web front node, you do not need to assign them in the cluster manager.

### Example:

- ACME Corporation deploys two web front nodes node1.acme.com and node2.acme.com. Each node is running a copy of the Cluster Server connecting to the same SQL database.
- ACME Corporation acquires a domain name (DNS) of cloud.acme.com which is load balanced to node1.acme.com and node2.acme.com.

When Users point their browsers to <https://cloud.acme.com> it is directed to one of the nodes login page.

---

**Note:** NOTE 1: If you have hardware load balancing available, you do not need to use web nodes at all.

---

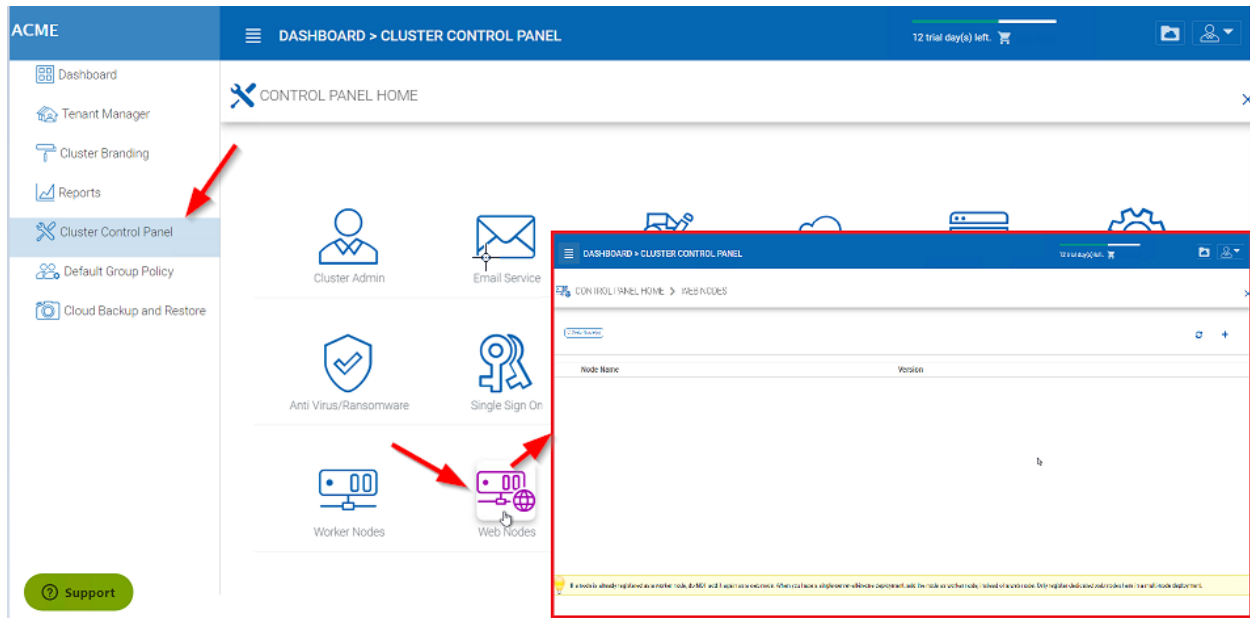


Fig. 70: WEB NODE

NOTE 2: Windows 2012/R2 comes with Network Load Balancing (NLB). If you use NLB, you do not need web nodes at all.

Basically, if you have any existing load balancer, you can omit web nodes.

### 3.5.10 Zones

Cluster Manager > Cluster Control Panel > Zones

The concept of zone is to associate your worker nodes with the location of the storage. When you think about zones, you will think about your storage location first.

For example, I have storage in LA so I have an LA zone. I also have storage in NY so I have a NY Zone.

You can have worker nodes from different zones as well and assign users to specific zone. If user's home directory is coming from LA zone, the user will need to be assigned to LA zone.

## 3.6 Default Group Policy

Cluster Manager > Default Group Policy

Default group policy can be applied to all tenants in the cluster. However, if the tenant also defines its own group policy, the tenant policy can over ride cluster wide default group policy.

Please reference the Group Policy in the tenant administrator section for full list of policy items.

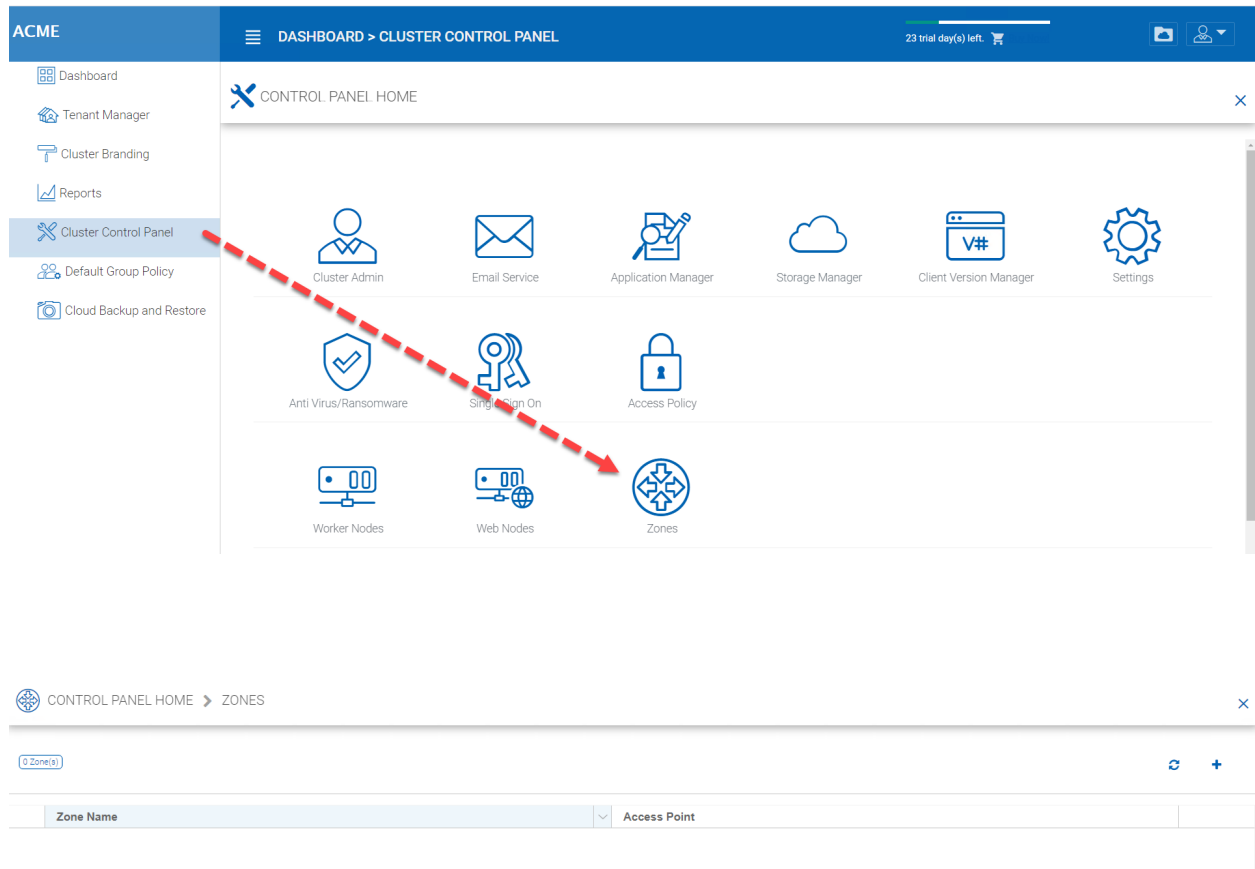


Fig. 71: CONTROL PANEL STORAGE ZONES EDITOR

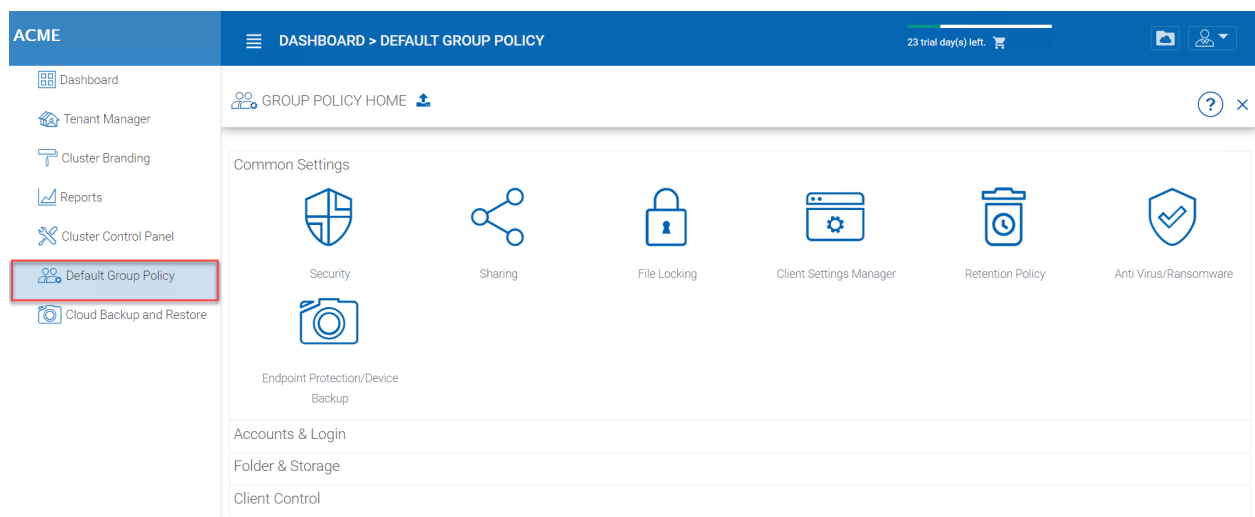


Fig. 72: GROUP POLICY SETTINGS



## Tenant Administration

**Note:** A tenant is usually mapped to a company, or a division of a company, an organization or in the case of MSP managed organization, a service provider would call them clients. Basically, a tenant is a management scope that represents an organization.

Tenant manager scope is defined for tenant administrators. 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.

Tenant Manager is completely web-based.

From the Cluster Manager Dashboard, you can access the Tenant Manager by choosing it in the left-side menu (1). This menu can be toggled on and off by clicking the “hamburger” menu in the top left corner of the Dashboard.

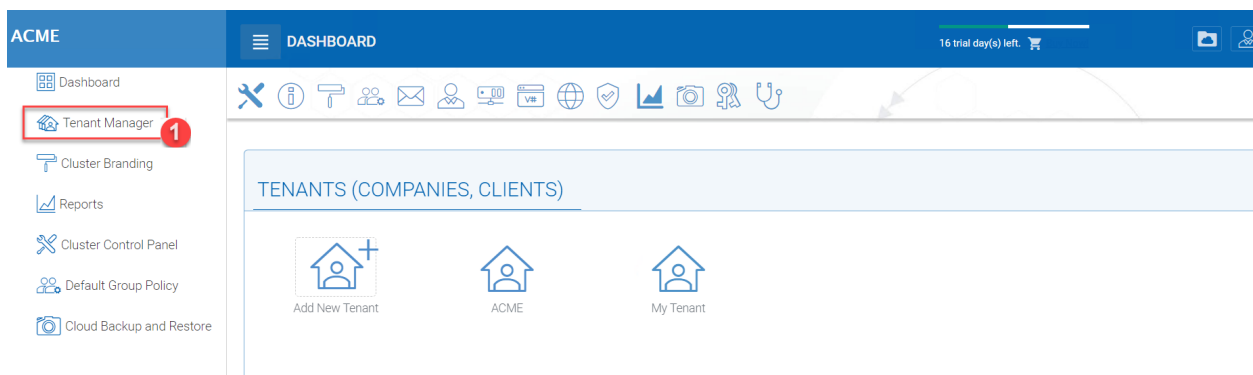


Fig. 1: CLUSTER SERVER DASHBOARD

Once you have selected the Tenant Manager in the left-side menu, you can access the management console directly by clicking the “Default Tenant” icon. You can also log in directly to the web portal as the tenant administrator instead of the default cluster administrator to get to the tenant administrator management web interface.

**Note:** At a high level, the Cluster Administrator and Tenant Manager have almost identical controls for the Tenants within their scope; however, the Tenant Manager settings will always take precedence and override Cluster Administrator settings. Tenant Managers can give permission for Cluster Administrator to manage their tenants by enabling this option in Group Policy > Common Settings > Security. “The Allow Cluster Admin to manage my tenant” is by default checked.

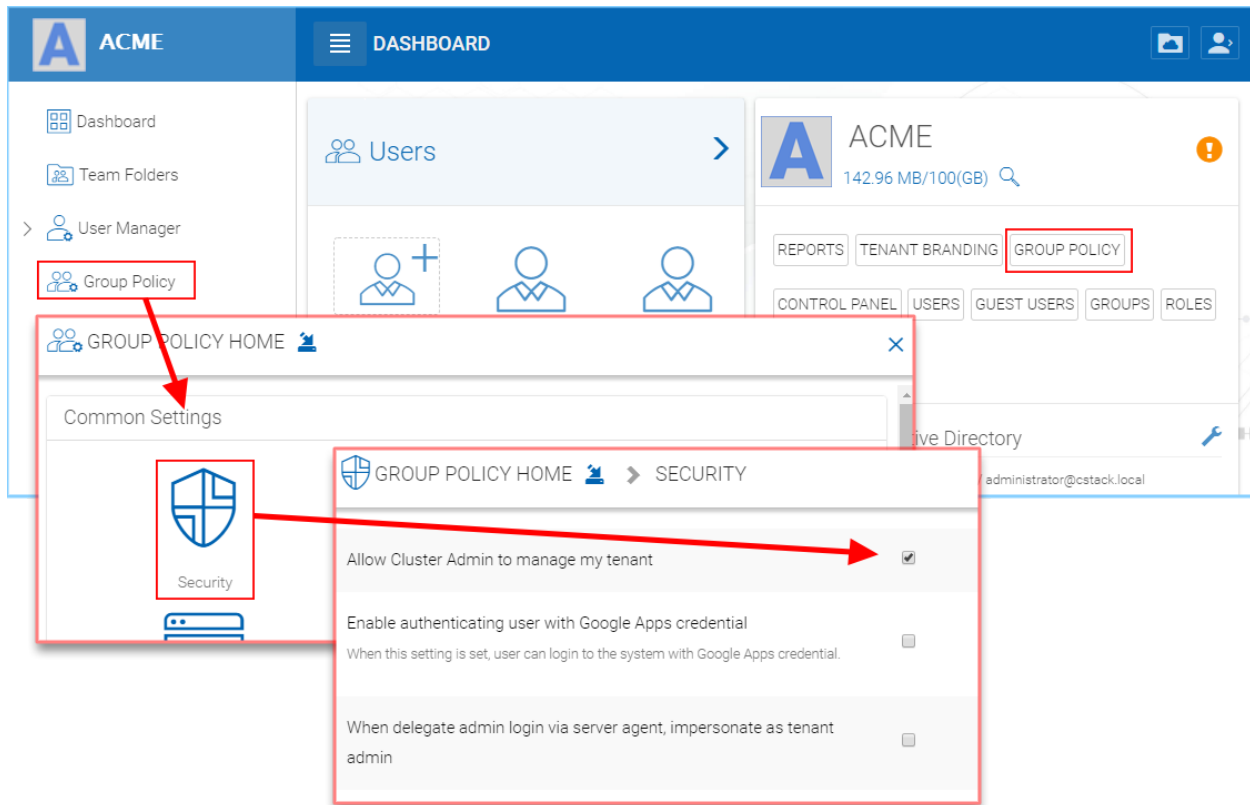


Fig. 2: TENANT GROUP POLICY > SECURITY

## 4.1 Tenant Dashboard

Tenant Manager > [Tenant] > Tenant Dashboard

You can navigate to different sections of Tenant Administration using the navigation menu at the top (1).

On the right side of the tenant manager web interface, if the screen is wide enough, there is a right side panel that has 4 items (icons always visible at the top of the Tenant Dashboard), Cloud Backup, Local Active Directory, Remote Active Directory and Backend Storage. Otherwise

## 4.2 Cloud Backup

Tenant Manager > [Tenant] > Cloud Backup

Cloud backup allows you to backup team folders in the tenant and also folders on devices attached to the tenant.



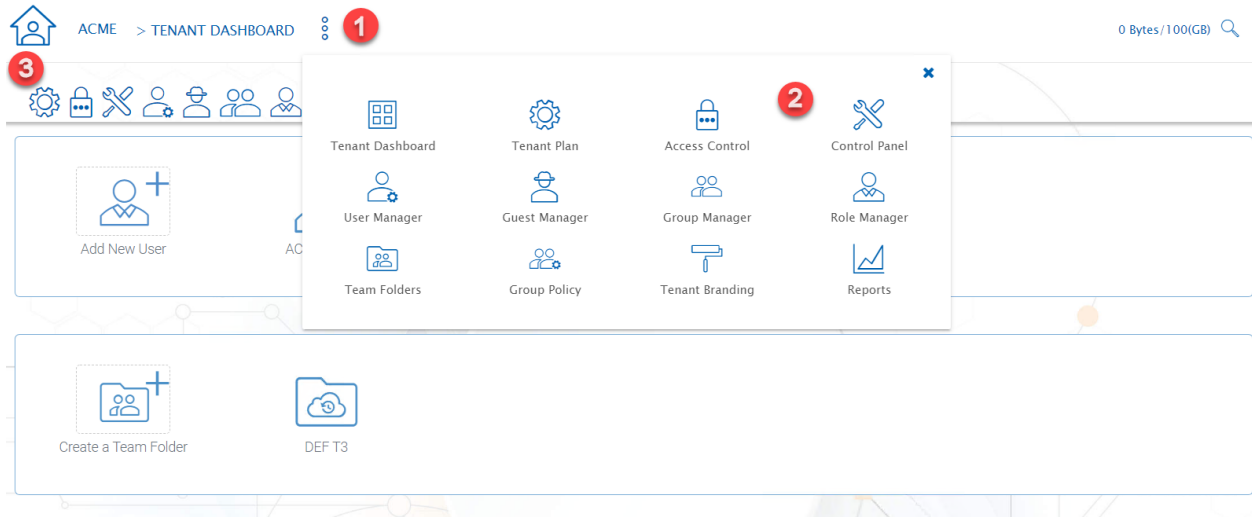


Fig. 3: TENANT DASHBOARD MENUS

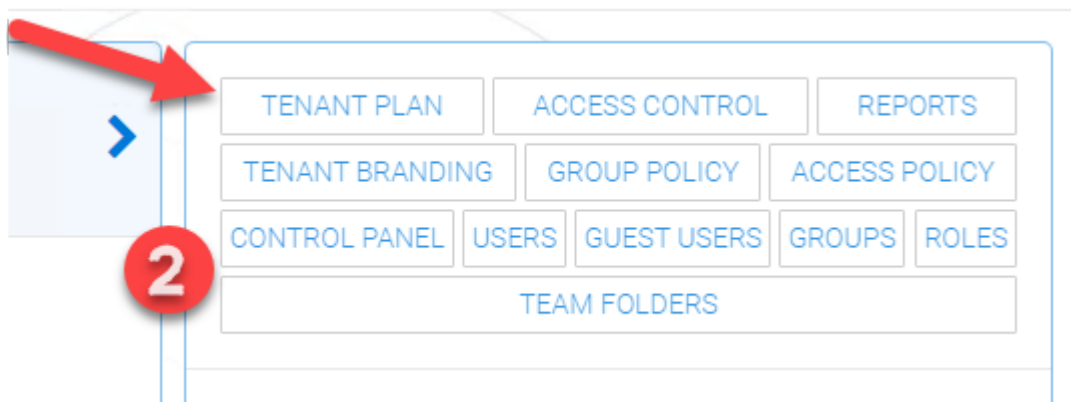


Fig. 4: TENANT DASHBOARD QUICK LINKS

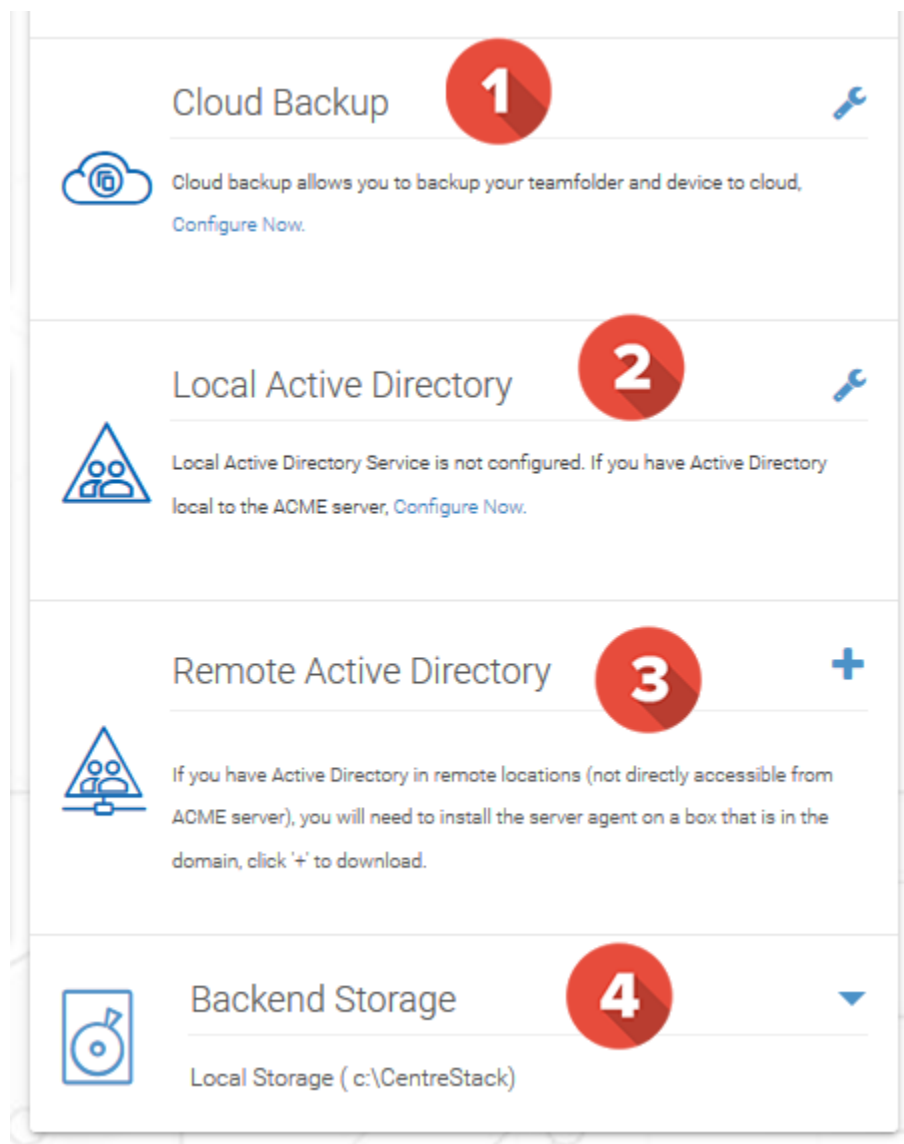


Fig. 5: RIGHT PANEL

## 4.3 Active Directory

If the tenant's infrastructure is in the same local area network as the Cluster Server, the Active Directory can be directly accessed and integrated from the "Local Active Directory" page. The integration is done over LDAP protocol.

However, if the tenant's infrastructure is away from the Cluster Server, it is recommended using "Server Agent" to connect both the tenant's file server and Active Directory to the Cluster Server.

**Tip:** If your Active Directory is away from the Cluster Server over the Internet, skip the "Local Active Directory" section but use the "Remote Active Directory" instead.

Use LDAP AD Setting only if the AD is in the same Local Area Network.

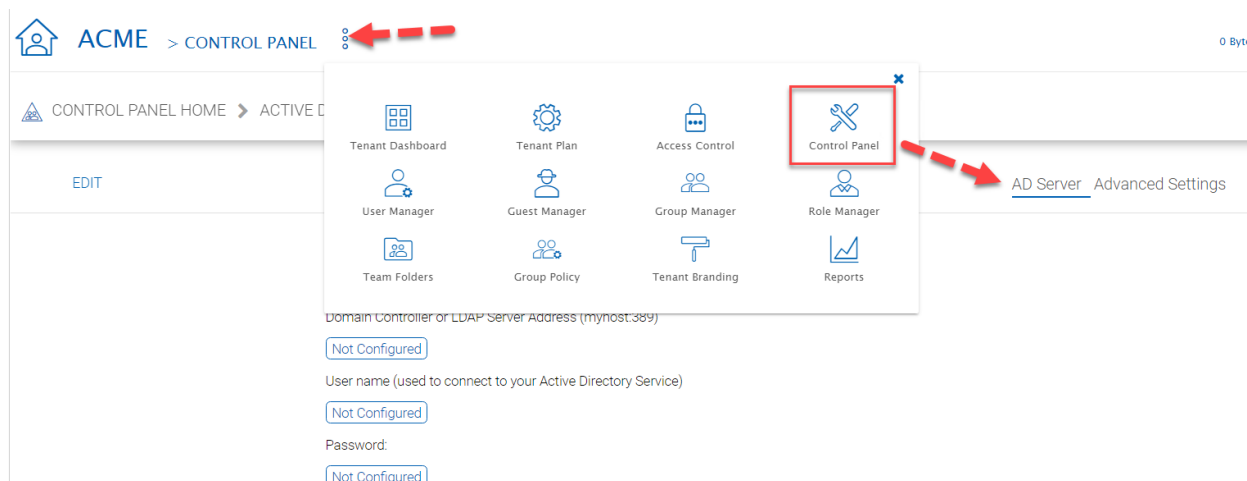


Fig. 6: ACTIVE DIRECTORY SETTINGS

**Note:** The difference between using LDAP to connect Active Directory and using "Server Agent" to connect Active Directory:

By using LDAP to connect Active Directory, the assumption is that the LDAP is local in the local area network so the speed is very fast and also very reliable. So a lot of the calls and queries are directly passing through to Active Directory.

By Using Server Agent to connect Active Directory, the assumption is that the Active Directory is in a remote location and over the Internet so the access speed may not be fast and the Internet may not be 100 percent up and reliable. So the server agent replicates Active Directory related information over to the Cluster Server.

### 4.3.1 Local Active Directory

Tenant Manager > [Tenant] > Local Active Directory

The connection to local active directory is via LDAP over Local Area Network. If the active directory infrastructure is in the same network as the Cluster Server, this is a convenient way to connect to the active directory.

### 4.3.2 Remote Active Directory

```
Tenant Manager> [Tenant] > Remote Active Directory
```

If the active directory is away from the Cluster Server, (for example, the active directory is on-premise inside a client's building, while the Cluster Server is in a data center) it is recommended to use Server Agent to connect the remote active directory.

---

**Note:** If the client/customer's Active Directory is in a remote location, you can use "Server Agent" to connect the Active Directory (and replicate remote File Server Network Share to the Cluster Server. You don't need to configure LDAP in the remote Active Directory case.

---

## 4.4 Backend Storage

```
Tenant Manager> [Tenant] > Backend Storage
```

Each tenant has a default backend storage. Tenant user (team user)'s home storage and other shared storage space can be allocated from the default backend storage.

---

**Tip:** You can think of the Tenant Backend Storage as a "Black Box" managed by the Cluster Server and you shall always use the Cluster Server interface to interact with the content inside the storage. If you can't take this "Black Box" approach for the tenant's root backend storage, you can use the following other methods via the team folders, such as import file server network share.

---

However, if you already have a file server that will provide the storage, it is recommended to use "Import Network File Shares" to mount the file server network share to the tenant's storage space. In this case, you can leave the "Default Storage" as is, or point it to an empty location and treat it as a black box storage managed at the Cluster Server level.

To access the Tenant Storage Manager, click the 3-dot menu on the bottom right of the Tenant Dashboard (Backend Storage section).

---

**Note:** You can mount different storage services into a single namespace (folder structure). For example, if you have multiple Amazon S3 buckets, you can mount them all in. If you have multiple OpenStack Swift accounts, you can mount them all in as well. If you have multiple file server network shares, you can add them to the storage manager.

---

---

**Note:** The cluster manager can define whether or not the Storage Manager is exposed to the tenant administrator.

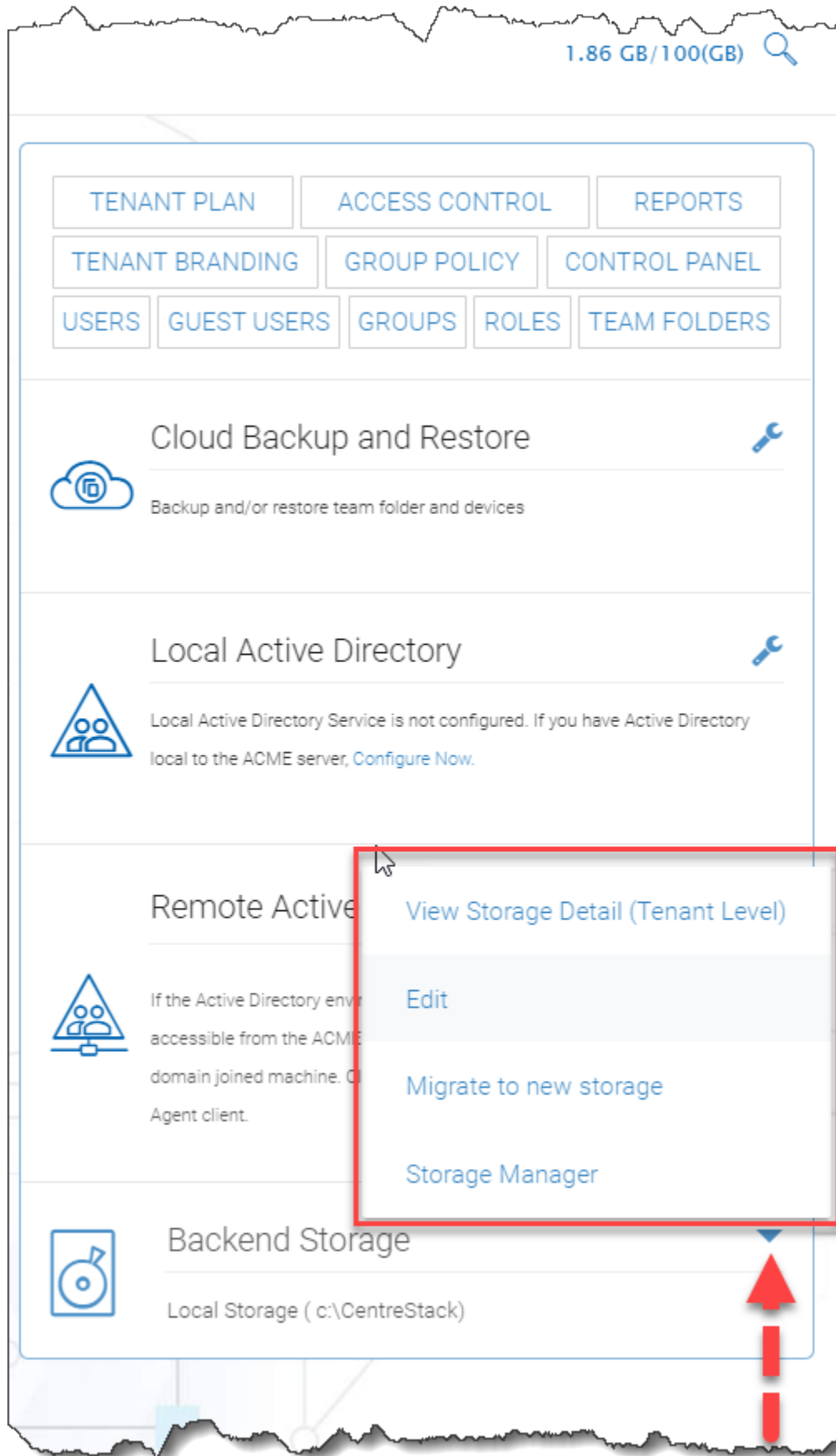
---

### 4.4.1 Home Storage

Home storage is the most important property in the tenant manager. It is used in many ways. For example, the users' home directory can be set up under the home storage (if the user's active directory home directory property is not used).

---

**Note:** In the field, one of the common mistakes is that a tenant's root network share is mapped directly to the home directory of the tenant. The home directory can not be shared from the root, so if your end goal is to turn the network



#### 4.4. Backend Storage

Fig. 7: STORAGE MANAGER ACCESS

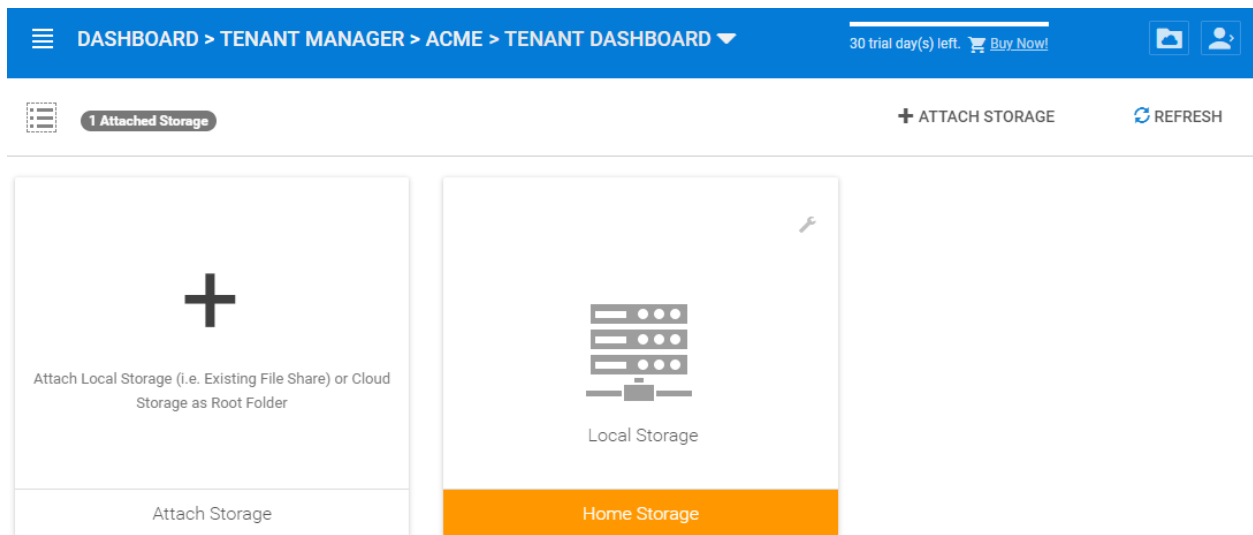


Fig. 8: STORAGE MANAGER SETTINGS

DASHBOARD > TENANT MANAGER > ACME > TENANT DASHBOARD
EDIT

30 trial day(s) left. Buy Now!

Local Storage Location (C:\myfolder or \\myfilesrvr\myshare):

c:\CentreStack\D8F45A62-81AA-49D8-AB63-7A0BA7CC682E\d01012d1-8c03-4ce1-bbef-d42bbb100d0a

User Name (for local storage access):

gladuser

Password (for local storage access):

☐ Always access the storage using the logged in user's identity

The specified user will be used to verify and access the storage for the admin account. When the above checkbox is selected, the storage will always be accessed using the team-user's Active Directory identity when the storage is published as a team folder. Non-Active Directory users will access the storage using the specified user account.

☐ The share is from a Linux/Unix/ZFS Server

☐ The share is a DFS share

☒ Enable In-Place Versioning

Warning! Branding materials, such as images and installer packages, are stored in the tenant's default storage. If the branding was configured before changing the storage location, it will need to be reset and re-configured.

APPLY
CANCEL

Fig. 9: EDITING HOME STORAGE SETTINGS

share directly into a team folder, you are better off mapping the home directory to another location, and later attach the network share as a secondary folder and turn that secondary folder into a team folder.

## 4.4.2 Attach Storage

Storage is an important component in the Cluster Server. you can connect the tenant to a specific storage service. For example, you can connect it to local file server storage; you can also connect the tenant to cloud storage services such as Amazon S3, Windows Azure, and OpenStack Swift.

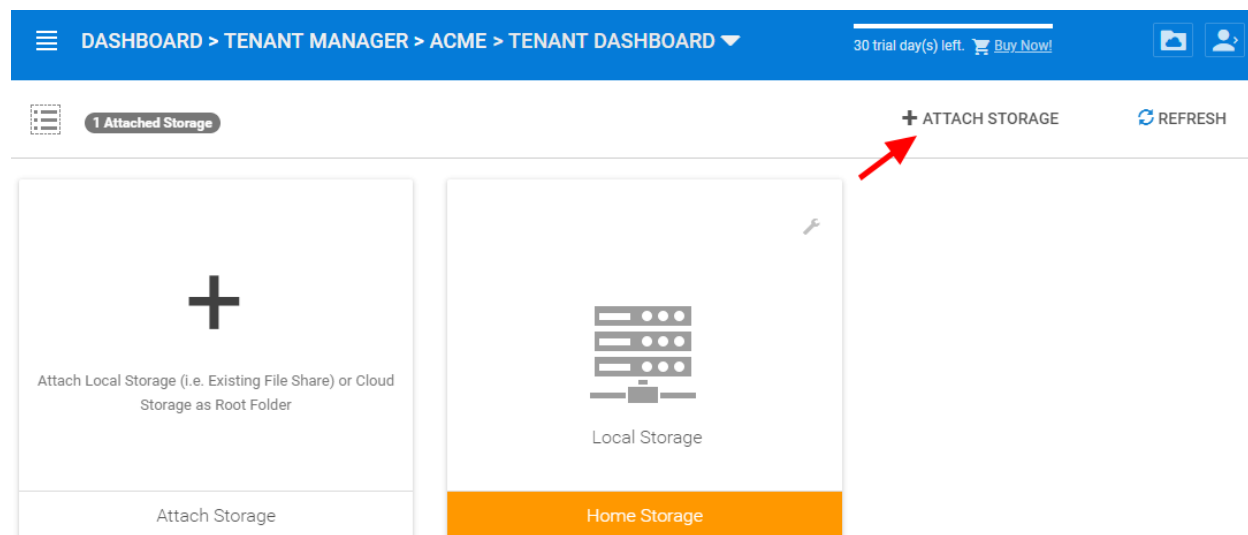


Fig. 10: ATTACH STORAGE

After clicking the “Attach Storage” button, the Cluster Server will take some time to discover file servers in the local area network and also provide a section to add cloud storage.

### 4.4.2.1 File Servers

In the File Servers in Local Area Network section, the Cluster Server will contact Active Directory or contact network browser in the local area network to try to find file servers in the local area network. Most of the time, if firewalls and network connections are properly configured, the file server can be easily added to the system.

However, sometimes, there are some situations such as the DNS system or the NETBIOS system not being ready. In that case, the file server may be discovered but it may not be connected, you can use the Manual Configuration to manually connect to the file server.

#### Root Folder Name

The Root folder name is the top-level folder name that will show up in the tenant administrator’s folder structure. We recommend the folder name being descriptive and follow the normal Windows path recommendations (For example, certain characters that are not allowed).

**Note:** Remember this folder is only showing to the tenant administrator, it is not published to the team user yet. When it is time to publish the folder to the tenant users, the name that the tenant user will see can also be defined. It is recommended that if later on, the folder is to be published as a team folder, then the name for the team folder should

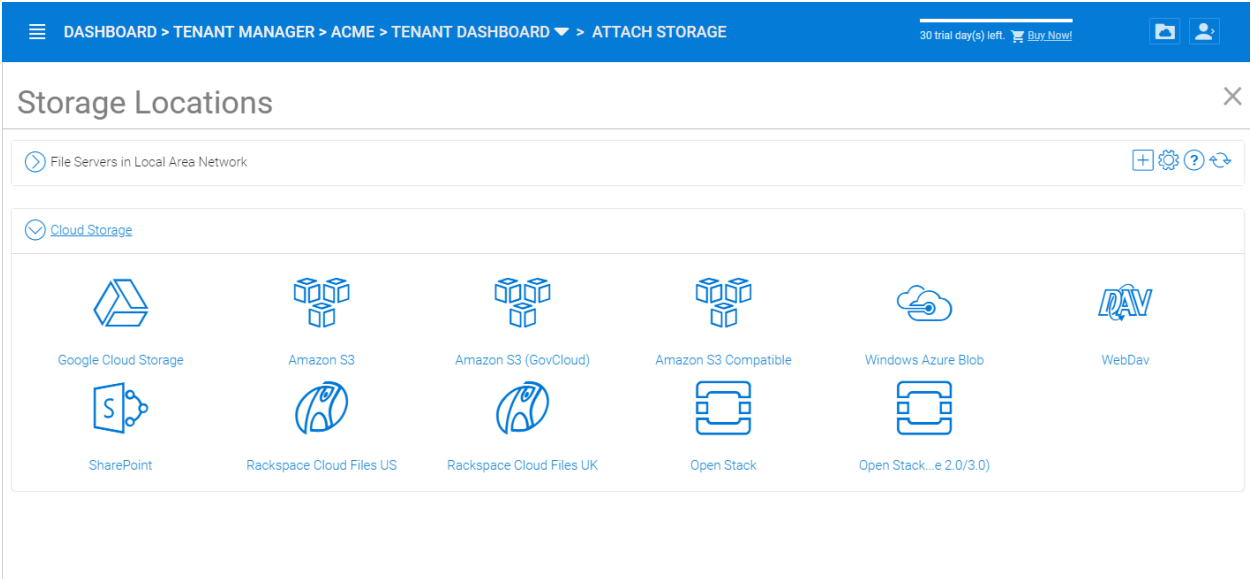


Fig. 11: TYPES OF ATTACHED STORAGE

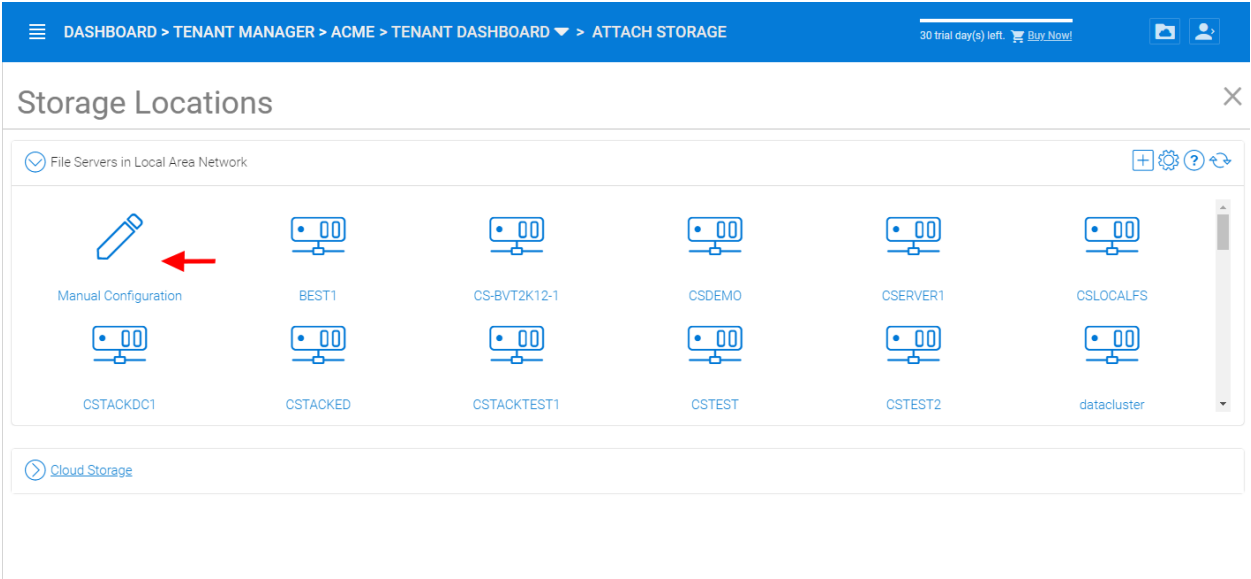


Fig. 12: LOCAL AREA NETWORK (LAN) STORAGE



**DASHBOARD > TENANT MANAGER > ACME > TENANT DASHBOARD > ATTACH STORAGE** 30 trial day(s) left. [Buy Now!](#)

Root Folder Name  
This is the name of the top level folder in your cloud.

Local Storage Location (C:\myfolder or \\myfileserver\myshare):

User Name (for local storage access):  
acmeadmin@mailinator.com

Password (for local storage access):  
.....

☐ Always access the storage using the logged in user's identity  
The specified user will be used to verify and access the storage for the admin account. When the above checkbox is selected, the storage will always be accessed using the team-user's Active Directory identity when the storage is published as a team folder. Non-Active Directory users will access the storage using the specified user account.

☐ The share is from a Linux/Unix/ZFS Server  
☐ The share is a DFS share  
☐ Enable In-Place Versioning

BACK CREATE CANCEL

Fig. 13: LAN ACCESS CREDENTIALS

be the same as the folder name here. It is recommended but not necessary to have the root folder name the same as your published team folder name.

#### 4.4.2.2 Local Storage

This is the file server UNC path or local windows folder path that you will connect into the tenant administrator's root folder structure. The idea here is you will take this folder and mount the folder to the tenant administrator's root folder structure with the name described in the "Root Folder name".

##### User Name

The user name is the Windows username, either it being local Windows user or global Active Directory user, this is a Windows account that is capable of accessing the "Local Storage Location".

##### Password

This is the password for the Windows user above.

**Note:** We recommend this Windows user and his credential be set up as a service account, meaning the password isn't subject to the maximum password days via local security policy. The reason being, that, when it is time to rotate or change the user password, the connection here may be broken until the password is updated to match.

##### "Always access the storage using logon user identity"

When you have Active Directory Integration, and mount an existing file server network share in, you can select "Always access the storage using logon user identity" so the ACL (NTFS Permission) on the file server share will be used natively. The access permission will be checked natively against the user's Active Directory identity that is defined by the NTFS permission.

This option only applies to the “Local Storage” such as network share, DFS share, local folder, and etc.

**“The share is from a Linux/Unix/ZFS server”**

Most of the time, you don’t want to check this flag because your file server share shall behave like a normal Windows Server share, even if it doesn’t come from a Windows Server.

In some small SOHO network storage devices, it may only allow one connection from one IP address, so if that is the case, you want to check this flag. Most of the time, you just don’t need to check this when the network share is capable of taking multiple connections/sessions from one single machine.

**“This share is a DFS share”**

If the share is a DFS share, you will check this checkbox, because DFS share has an extra layer of translation to translate back down to normal file server shares. This flag tells the Cluster Server to do an extra DFS translation back to SMB share before connecting to the share.

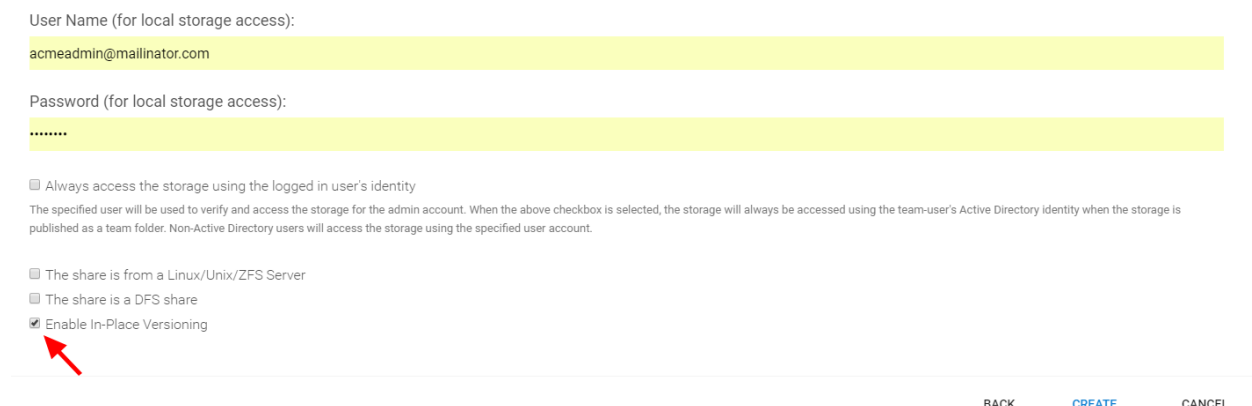
**“Enable Inplace Versioning”**

The underlying file server network share may not have explicit version control (it may have volume shadow copy for other purposes). This will add Cluster Server version control to the file server network share. It is independent of and not related to the volume shadow copy.

---

**Note:** In place versioning will put the older version of the file into a \_\_ver\_\_ subfolder in the same folder structure making the name for In-Place Versioning so the folder structure is maintained as-is, while extra old copies of the file will be stored in a specific subfolder.

---



The screenshot shows a configuration form with the following elements:

- User Name (for local storage access):** acmeadmin@mailinator.com
- Password (for local storage access):** ..... (masked)
- ☐ Always access the storage using the logged in user's identity  
The specified user will be used to verify and access the storage for the admin account. When the above checkbox is selected, the storage will always be accessed using the team-user's Active Directory identity when the storage is published as a team folder. Non-Active Directory users will access the storage using the specified user account.
- ☐ The share is from a Linux/Unix/ZFS Server
- ☐ The share is a DFS share
- ☒ Enable In-Place Versioning (highlighted with a red arrow)

At the bottom right, there are three buttons: BACK, CREATE (in blue), and CANCEL.

Fig. 14: IN-PLACE VERSIONING

Here is a demo video showing the result of “Enable Inplace Versioning” when the root folder (‘forward slash’) is mounted with the “Inplace versioning” enabled.

#### 4.4.2.3 Cloud Storage

Besides local storage, you can also mount cloud storage into the system. If you have Amazon S3, or Amazon S3 compatible storage service, or if you have OpenStack Swift or OpenStack Swift compatible storage, you can connect it into the system. You can see the full list of storage services supported, including SoftLayer Object Storage, Google Cloud Storage, Microsoft Azure storage, and more.

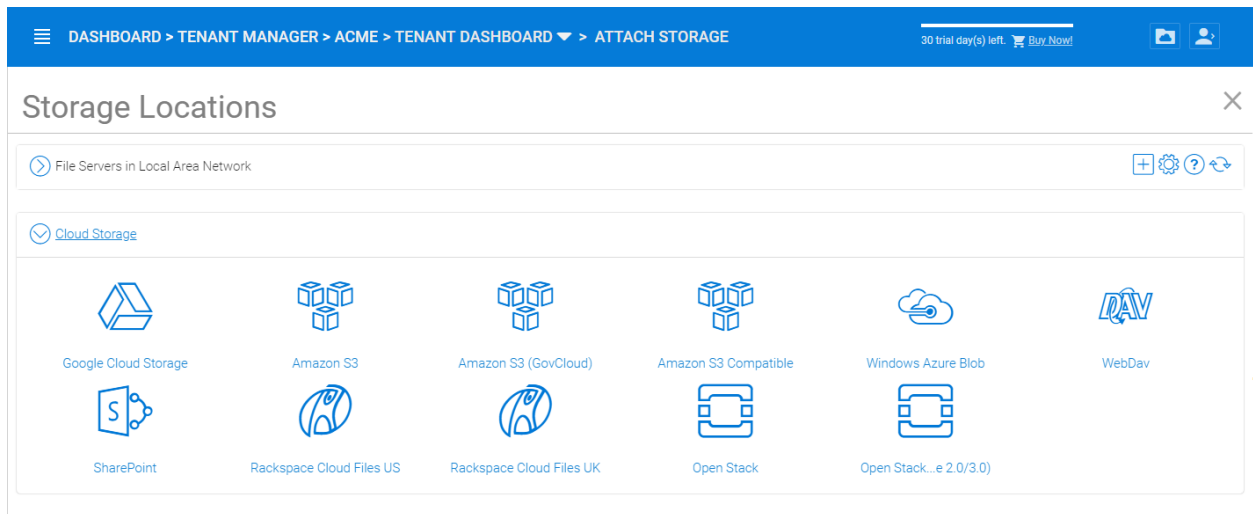


Fig. 15: CLOUD STORAGE OPTIONS

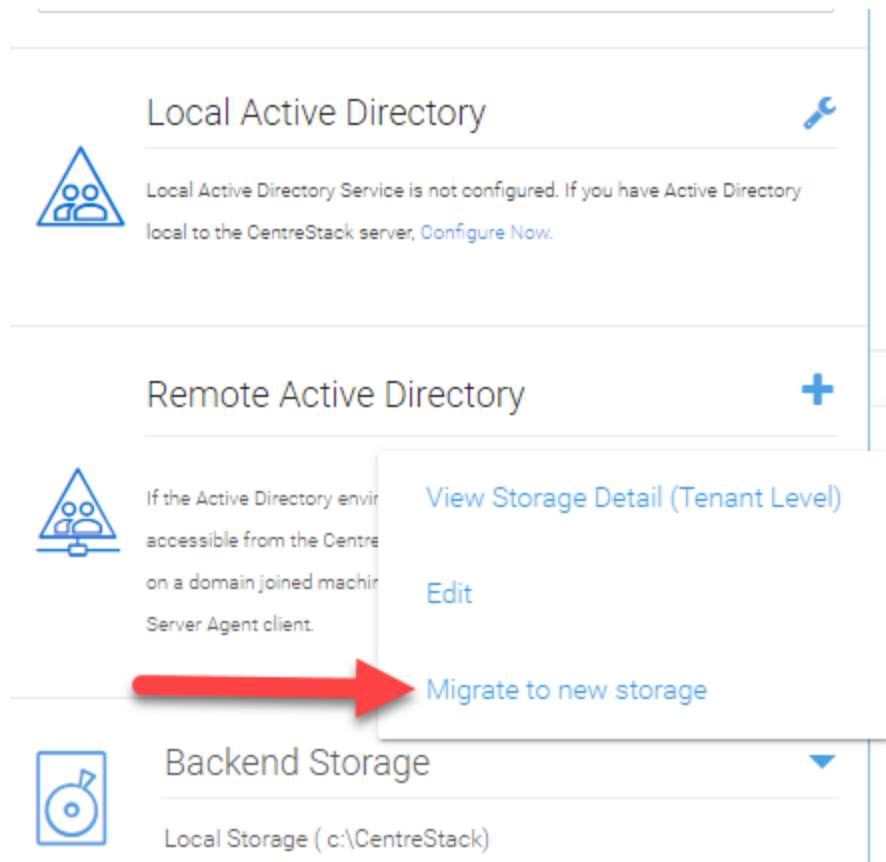


Fig. 16: CLOUD STORAGE MIGRATE

### 4.4.3 Migrate to New Storage

Once the tenant backend storage is set, we don't recommend changing it until it has to be changed (e.g., migrate to other location). However when you are just setting up the tenant, you can decide where your tenant's storage location is and can change between local file server storage or remote cloud storage service.

There are two types of storage migrations.

#### 1. Migrate data to a different location in the same type of storage:

- Identify the location of the current storage
- Copy the content to the new location (for example, you can use `xcopy` . from the old location to the new location
- Login to web portal as Cluster Admin.
- Go to Tenant Manager -> Manage the specific Tenant -> Backend Storage and click on edit to point to the new location

#### 2. Migrate data to a different type of storage:

- Go to the registry using regedit
- Go to `HKLM\SOFTWARE\Gladinet\Enterprise\` and add a new string value called 'CanChangeDefaultStorage' and set the value to 'True' and reboot
- Edit the storage type using new icon to edit storage under Cluster ManagerTenant Manager

**Note:** It is not recommended that you modify registry settings. Create a backup of the registry before modifying any registry settings.

## 4.5 Tenant Plan

Tenant Manager > [Tenant] > Tenant Plan

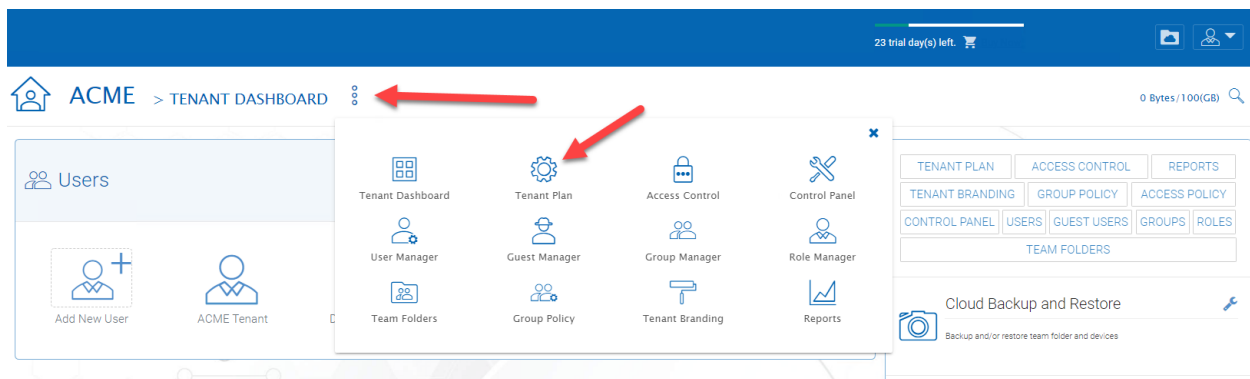
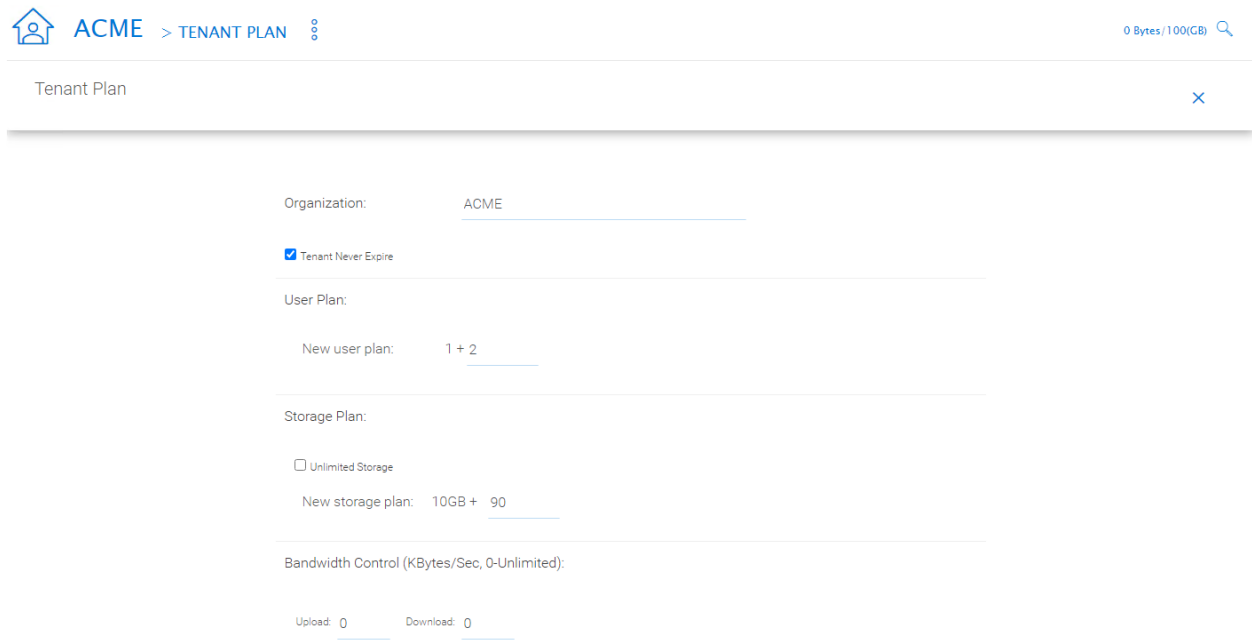


Fig. 17: TENANT PLAN SETTINGS

Here in the Tenant Plan section, you can change the tenant's user plan and storage plan, and also control the bandwidth usage for the tenant.



Tenant Plan

Organization: ACME

☒ Tenant Never Expire

User Plan:

New user plan: 1 + 2

Storage Plan:

☐ Unlimited Storage

New storage plan: 10GB + 90

Bandwidth Control (KBytes/Sec, 0-Unlimited):

Upload: 0 Download: 0

Fig. 18: TENANT PLAN SETTINGS

## 4.6 Access Control

Tenant Manager > [Tenant] > Access Control

In the Admin Access Control, the cluster administrator can decide the division of work between cluster administrators and the specific tenant administrator. A lot of times, the cluster administrator will help with setting things up. In this case, the cluster administrator can take away some of the administrative work from the tenant administrator.

**Note:** For example, if the cluster administrator is a Managed Service Provider (MSP), the tenant admin can be an admin user from a specific client (customer).

Or, if the cluster administrator is an enterprise IT directory, the tenant admin can be a specific division of the enterprise.

### Allow tenant to attach external cloud storage

If checked, in the tenant administrator's management console, the "Storage Manager" will show and allow tenant administrator to mount (attach) external storage.

If the cluster administrator is setting it up for the tenant, the cluster administrator can take away this privilege.

### Edit tenant administrator info

The Cluster administrator can decide whether to allow the tenant administrator to edit its own information, such as change email.

### Allow tenant to edit branding settings

The Cluster administrator can decide whether to allow tenant administrator to have its own branding.

### Do not show GDPR consent form

Access Control

Tenant Administrative Control:  
There are certain features you can expose to tenant administrators, such as setup LDAP for Active Directory or mount extra external storage services. Select the checkboxes for the following features that you would like to expose to the tenant administrator.

- ☒ Allow tenant to attach external cloud storage
- ☒ Edit tenant administrator info
- ☒ Allow tenant to edit branding settings
- ☐ Do not show GDPR consent form
- ☐ Allow tenant to increase the user plan automatically
- ☐ Disable Active Directory integration
- ☐ Multi AD Domain Support
- ☒ View and edit group policy
- ☐ Disable file/folder sharing
- ☐ Hide migration option
- ☒ Allow creation of guest users
- ☒ Show Data-At-Rest Encryption configuration page (Requires empty storage container)
- ☒ Allow tenant to edit LDAP setting

Fig. 19: ACCESS CONTROL SETTINGS

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. There are regulations about collecting user information and software needs to provide consent form. If you have customers in the EU, it is recommended to show the consent form.

#### Allow tenant to increase user plan automatically

The Cluster administrator can decide whether to allow the tenant to grow the user count automatically.

#### Disable Active Directory integration

If checked, this will remove AD integration for this tenant.

#### Multi AD Domain Support

Support multiple Active Directories in a single tenant (current tenant).

Multiple Active Directory forests support. This is not a common option because most of the time, the tenant has one forest (which can have multiple sub domains). In the case when the tenant has several Active Directory domains that are not related, multiple LDAP connection can be set up this way.

**Tip:** If you have single AD forest but contains multiple sub-domain AD domain controller, you don't need to turn on Multi-AD support. Instead, you just point the LDAP to the root forest domain controller and the root forest domain controller will find and identify the sub-domains.

#### View and edit group policy

The Cluster administrator can decide whether to show the group policy section to this tenant.

#### Disable file/folder sharing

Disable file and folder sharing from tenant level.

#### Hide migration option

Migration option refers to migrating remote file server(s) from remote customer location(s) to the Cluster Server. Not all clients (customers) have remote file servers, so this tenant level option may not apply all the time.

#### Allow tenant to edit LDAP setting

In the case the tenant's infrastructure is in the same LAN (Local Area Network) as the Cluster Manager, the tenant's Active Directory can be directly connected via LDAP to the Cluster Server.

If the cluster administrator is setting it up for the tenant, cluster administrator can take away this privilege.

### Show Data-At-Rest Encryption (DARE) configuration page (Requires empty storage container)

If the tenant has the required encryption of the data in the cloud (Cluster Server side), a DARE configuration page can be shown upon the first usage to set it up.

### Allow creation of guest users

The Cluster administrator can control whether to allow the specific tenant to have guest users.

## 4.7 Control Panel

Tenant Manager > [Tenant] > Control Panel

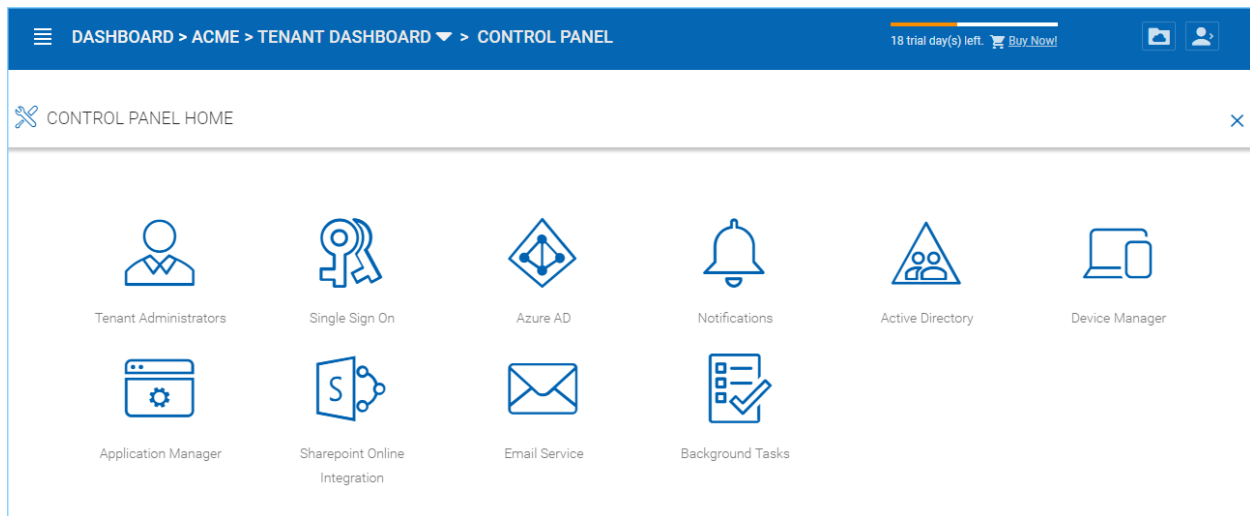


Fig. 20: TENANT MANAGEMENT CONTROL PANEL

### 4.7.1 Administrator Information

Tenant Manager > [Tenant] > Control Panel > Tenant Administrators

In the administrator information page, the cluster administrator can help the tenant manager change their email and user name if they need to, and to also setup delegated administrators.

The delegated administrators that are setup at the cluster level are users who are already in the Cluster Server and will be helping out the management of this specific tenant. Access these settings by clicking "Control Panel" and choose the "Tenant Administrators" icon.

You can define a group of users here to delegate the administration of tenants to other users.

**Note:** Delegated administrators have two different roles. First of all, they are not the default administrator in the tenant so normally they are just normal team users in the tenant.

However, they can elevate themselves into the admin role by clicking the elevation icon that is available to delegated administrators.

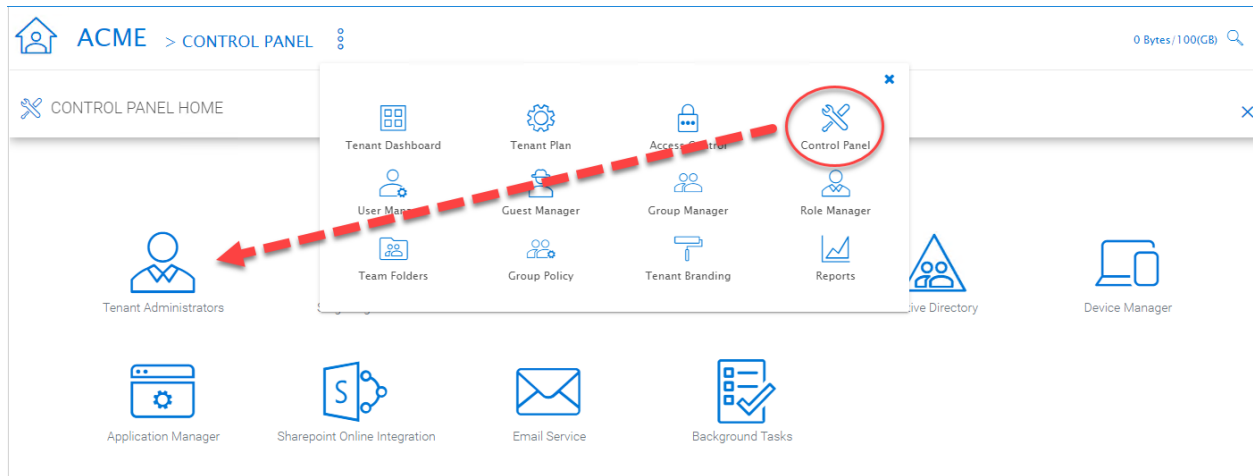


Fig. 21: TENANT ADMINISTRATORS

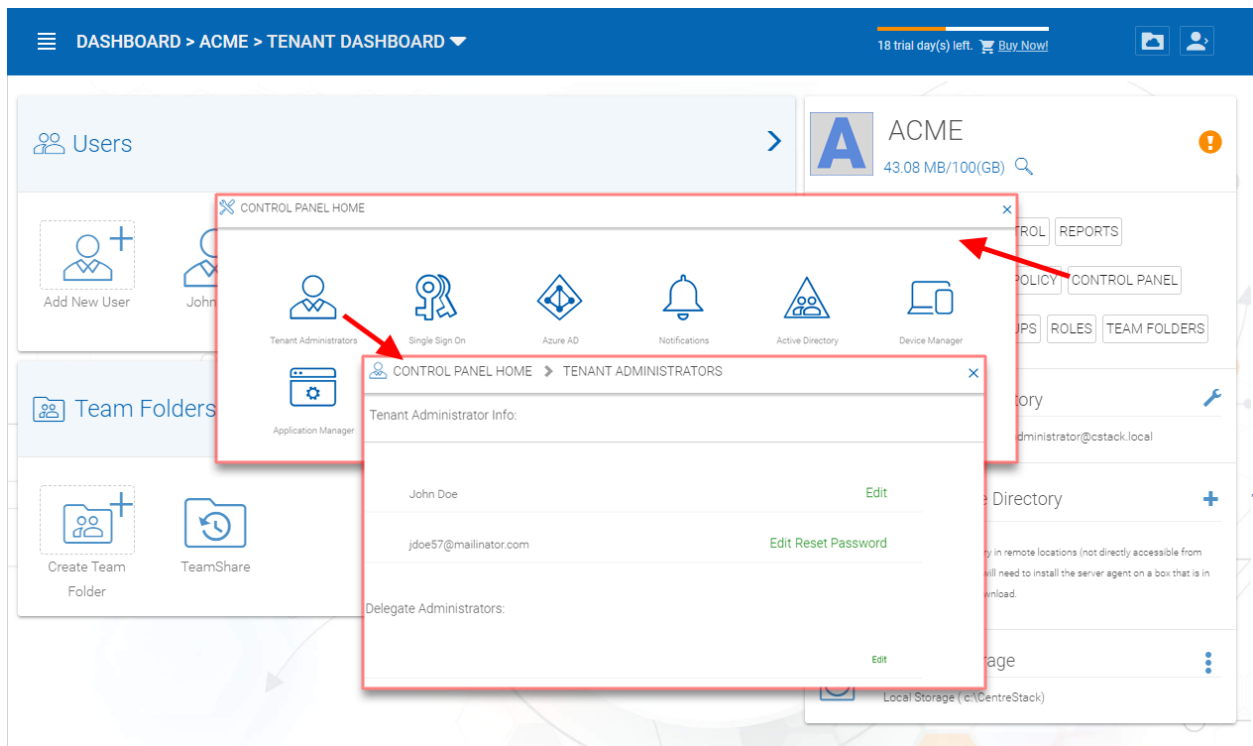


Fig. 22: ADDING/EDITING TENANT ADMINISTRATORS



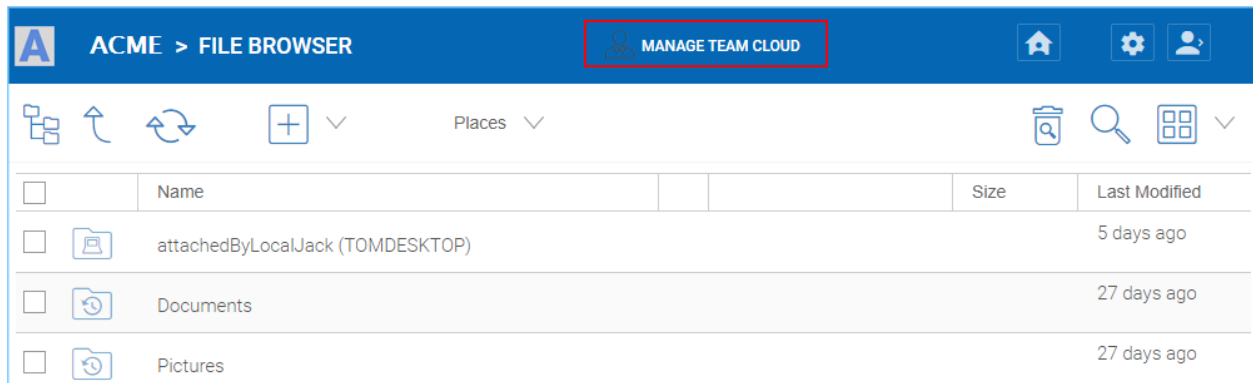


Fig. 23: MANAGE TEAM CLOUD SETTINGS

## 4.7.2 Notifications

Tenant Manager > [Tenant] > Control Panel > Notifications

The cluster administrator can use the notification manager to help the tenant setup notification events. The tenant administrator will receive email notifications for the events subscribed.

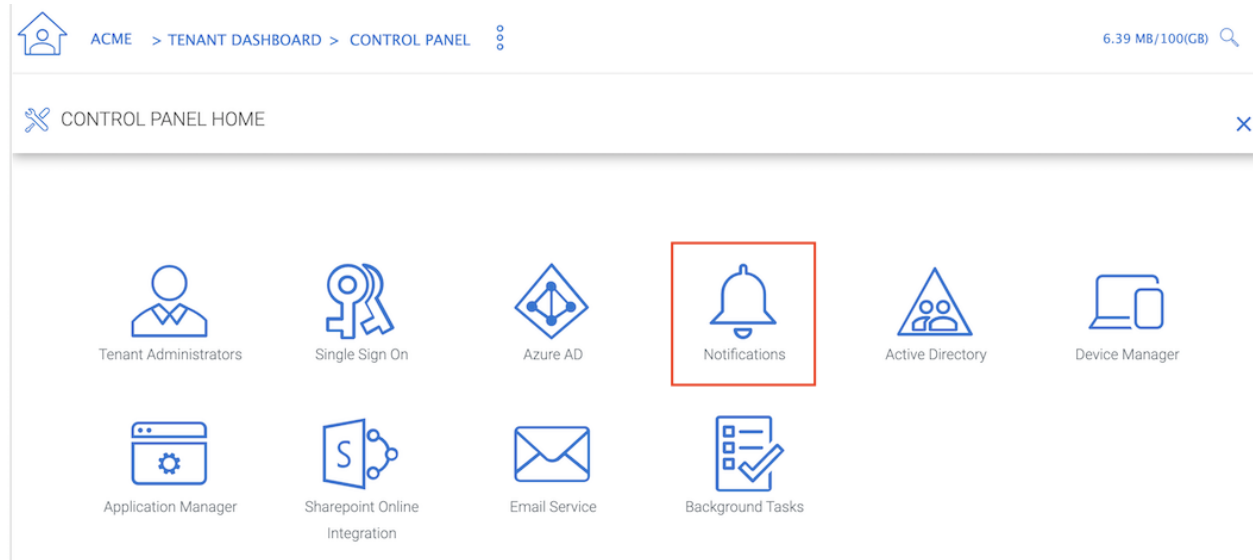


Fig. 24: NOTIFICATIONS

### 4.7.2.1 Settings

#### Send Daily Notification Email

When set, the system will send email notification daily about the events you are interested (Select below).

- File Changes
- Audit Trace

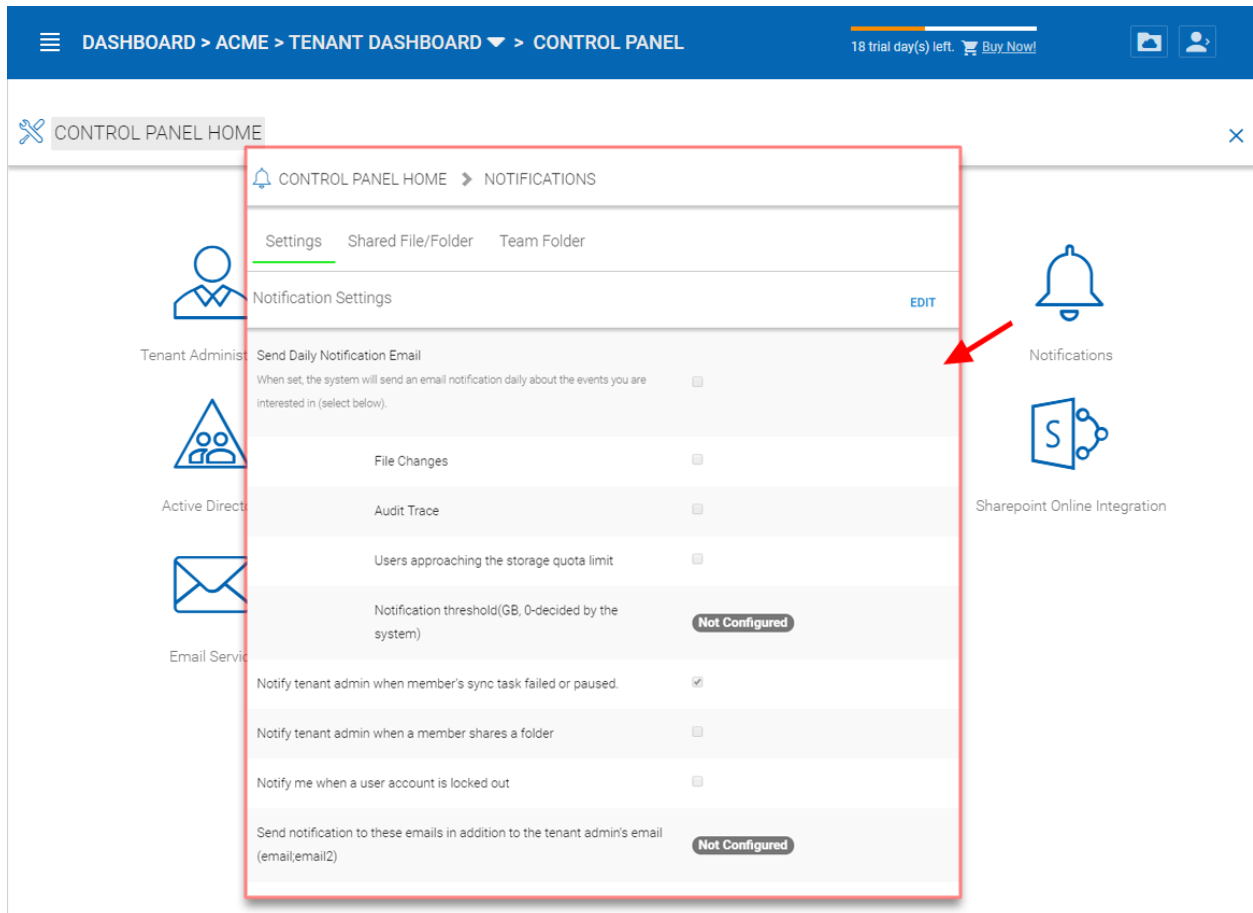


Fig. 25: NOTIFICATION SETTINGS

- Users approaching the storage quota limit
- Notification threshold

**Notify tenant admin when member's sync task failed or paused**

**Notify tenant admin when a member shares a folder**

**Notify me when a user account is locked out**

**Do not show file change notifications on Windows and Mac client**

**Send notification to these emails in addition to tenant admin's email (email;email2)**

This is used for additional administrators to receive email notification.

#### 4.7.2.2 Shared File/Folder



Fig. 26: SHARES SUBSCRIPTIONS

Notification regarding modified/downloaded shared files and folders.

#### 4.7.2.3 Team Folder

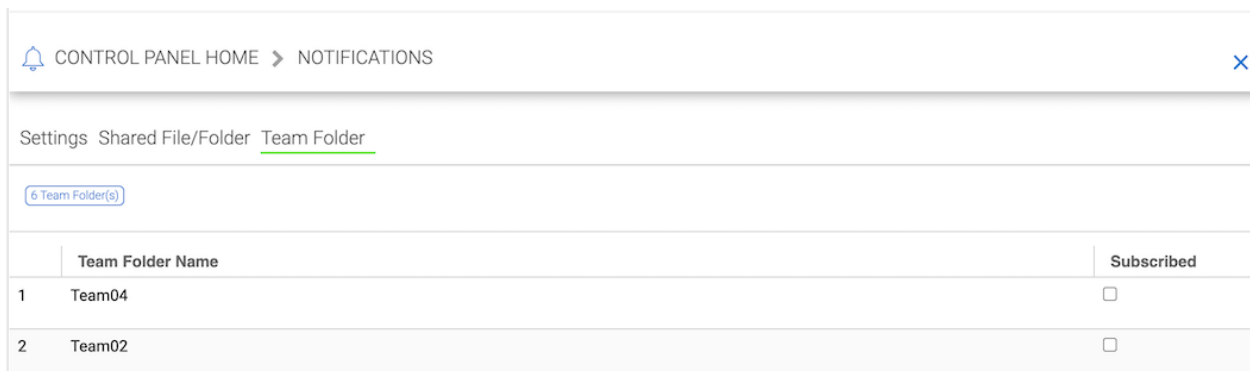


Fig. 27: TEAM FOLDER SUBSCRIPTIONS

Administrators can use this setting to receive notifications when changes occur in Team Folders.

### 4.7.3 Active Directory

Tenant Manager > [Tenant] > Control Panel > Active Directory

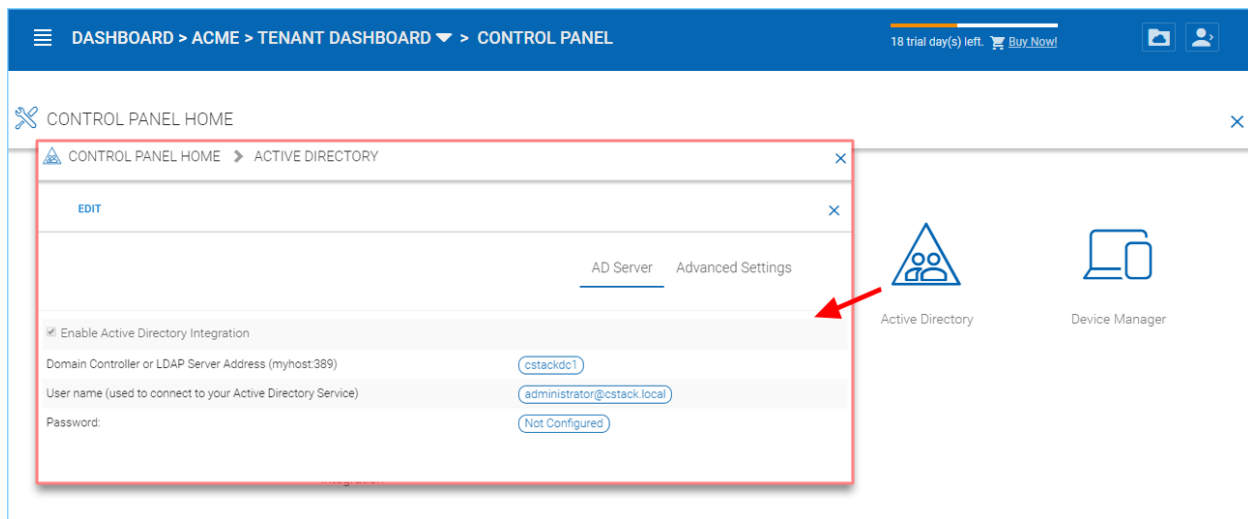


Fig. 28: CONTROL PANEL AD SERVER SETTINGS

#### 4.7.3.1 AD Server

##### Enable Active Directory Integration

You will check this when you want to integration with Active Directory.

**Note:** There are two different ways to integrate with Active Directory. One way is here, using the Lightweight Directory Access Protocol (LDAP) connection. The other way is to leverage the server agent software. The server agent software is capable of connecting a remote Active Directory.

##### Domain Controller Address

The domain controller's address, typically in the form of DNS name.

##### User Name

This is recommended to be a service account (password never expire, account never disable" so the user will be able to query LDAP for users and authenticate users on the login user's behave.


##### Password

This is the password for the service account for the "User Name" field.

#### 4.7.3.2 Advanced Settings

##### Friendly Domain Name

(i.e. **mydomain.com**, the domain name you see in Active Directory tools) This is typically the domain name you see in the Microsoft Domain and User tool. It needs to be exact match of the domain name. Otherwise, you will see error message about "referral is required", which translates to the domain controller didn't match the domain name and need to refer you to somewhere else for another domain name.


[CONTROL PANEL HOME](#) > [ACTIVE DIRECTORY](#)

[EDIT](#)

AD Server

Advanced Settings

Friendly Domain Name (i.e. mydomain.com, the domain name you see in Active Directory tools)

[cstack.local](#)

☐ Enable LDAPS for secure access

Only include users and groups from the following Organizational Units (e.g. OU=ou1,OU=ou2. Leave this blank to include all OUs)

[Not Configured](#)

☐ Allow Switching to Global Catalog If needed

☐ Disable Nested Groups (Enabling it may slow down your access to cloud)

☐ This is the root of the AD Forest and contains multiple sub-domains(☐ Discover domain controller IP at runtime)

☐ Don't allow user auto-creation

☐ Publish user's home drive

When unchecked, the user home drive space will be allocated from enterprise storage. When checked, existing user home drives will be automatically published from Active Directory.

Fig. 29: CONTROL PANEL AD ADVANCED SETTINGS

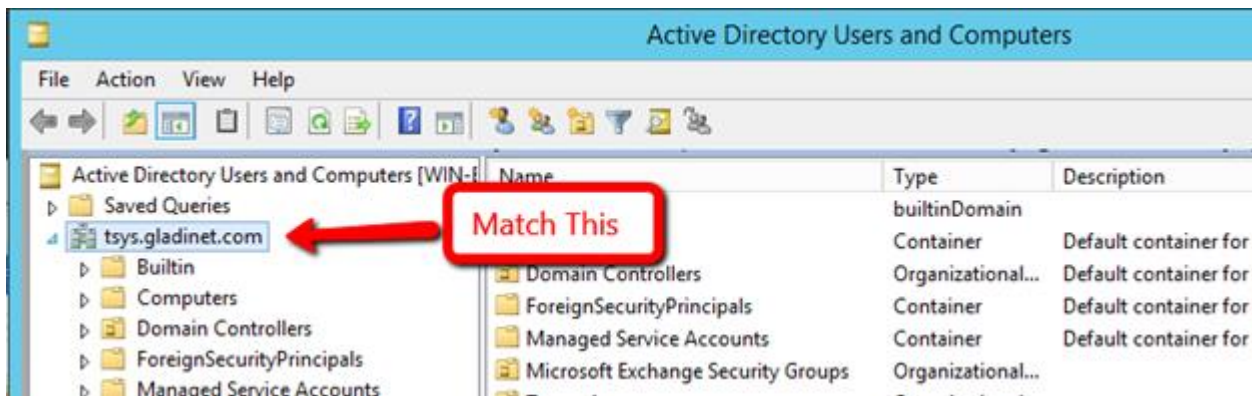


Fig. 30: FRIENDLY DOMAIN NAME EXAMPLE

### Enable LDAPS for secure access

Disabled by default. Enable this if you are using SSL security on the domain.

### Only include users and groups from the following Organizational Units

(e.g. OU=ou1,OU=ou2. Leave this blank to include all OUs) When you type in the organization unit, you don't need to type the domain part any more. It just need the Organization Unit part of the string. This is allowed for only single Organization Unit specified in its distinguishedName format without the domain suffix.

### Allow Switching to Global Catalog If needed

Disabled by default. For some organization that has multiple domain, sometimes there is a Global Catalog that stores everything inside. This may be required if you have such situation.

### Disable Nested Groups

Not checked by default. **(Activating this checkbox may slow down your access to cloud)** Normally you will activate this option if you have many groups.

### This is the root of the AD Forest and contains multiple sub-domains

The Cluster Server supports multiple domains in the same AD forest. You will need to point to the root of the AD and it is capable of finding all the sub-domains if you enable the **Discover domain controller IP at runtime** sub-option.

### Don't allow user auto-creation

By default, the Enterprise package is capable of creating users upon first login into the web portal. However, for big enterprise, they may want to control the pace of adding users to the system so they will disable this feature.

### Publish user's home drive

When unchecked (default), the user home drive space will be allocated from enterprise storage. When checked, existing user home drives will be automatically published from Active Directory.

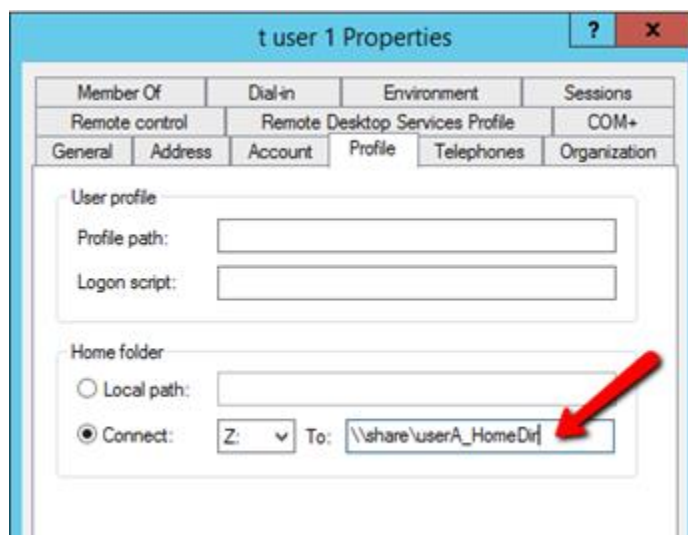


Fig. 31: USER'S PROFILE HOME FOLDER SETTING

## 4.7.4 Device Manager

Tenant Manager > [Tenant] > Control Panel > Device Manager

The cluster administrator can look at the devices that have the client agent software installed and connected in the specific tenant.

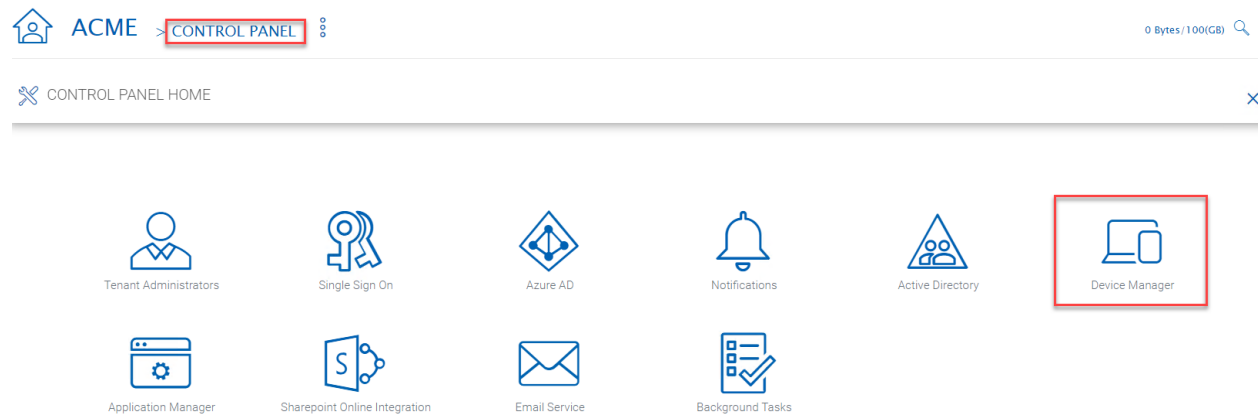


Fig. 32: DEVICE MANAGER

This feature is used to control BYOD (Bring your own device). For some organization, they want to control who can bring what device into the system. This is the tool to control that and allow/disallow on a device by device basis.

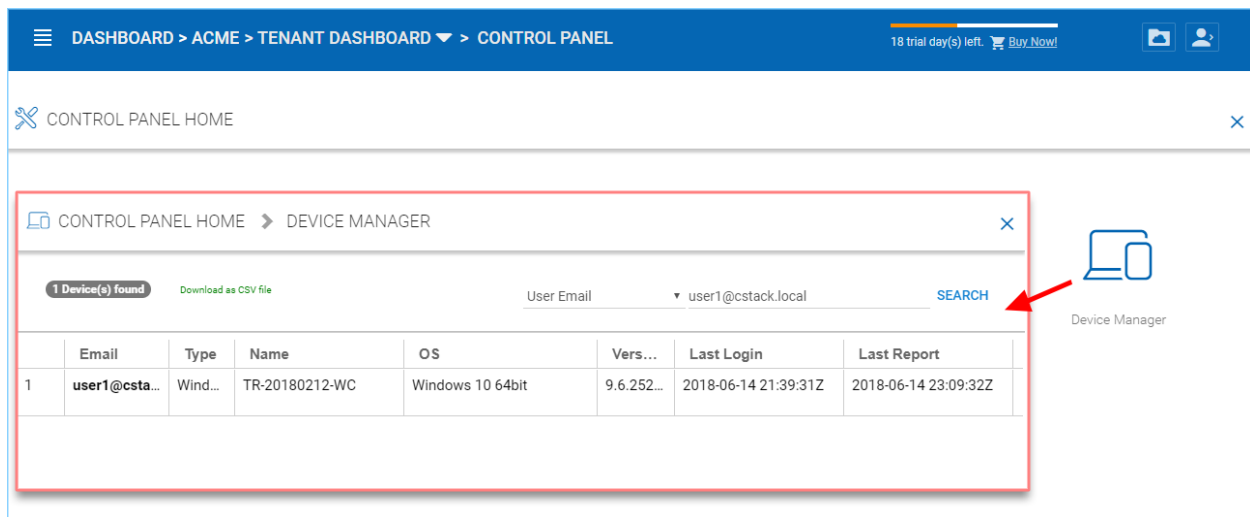


Fig. 33: DEVICE MANAGER SETTINGS

## 4.7.5 Application Manager

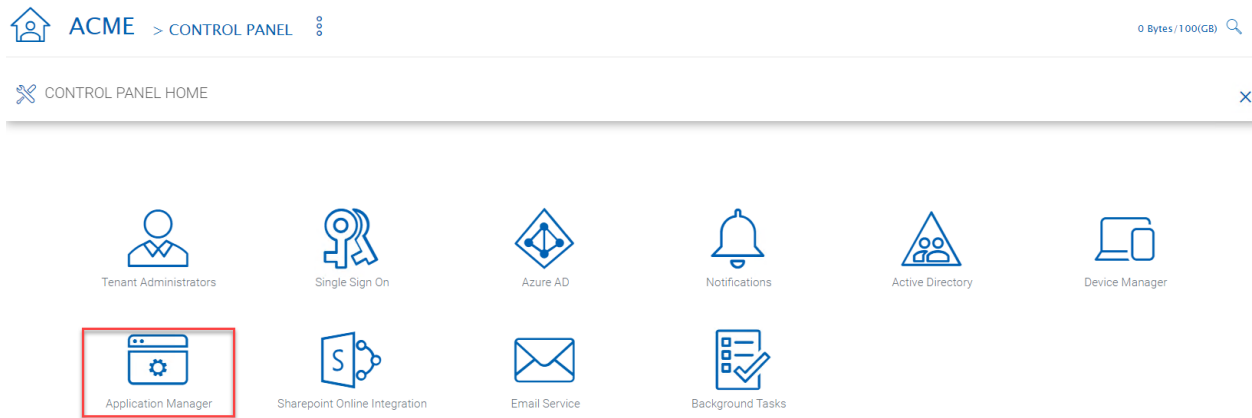
Tenant Manager > [Tenant] > Control Panel > Application Manager

The cluster administrator can look at the application manager for the specific tenant.

Here are the 4 different applications that can be setup on a per-tenant basis.

- Microsoft Office Web App

- Pixlr Web App
- Zoho Web App



## 4.7.6 Background Tasks

Tenant Manager > [Tenant] > Control Panel > Background Tasks

There are three different kind of background tasks that may take a long time to finish:

1. Data Seeding - copying data into CentreStack
2. Storage Scan - do a full scan to calculate storage consumption
3. Tenant Storage Migration - move tenant storage from location A to location B
4. Anchor Migration - move data out of Anchor and into CentreStack

The cluster administrator can help the tenant seed the data. For example take data into a USB drive and take it to the same local area network as the Cluster Server and see the data into the tenant storage.

### Add New Data Seeding Task

Tenant Manager > [Tenant] > Background Tasks > Add New Data Seeding Task

Data Seeding is to take a folder from a source location and seed it into a team folder.

On the left of the dialog, it is the source folder path information.

On the right side of the dialog, it is the target team folder information.

If you are seeding the data into a brand new team folder, you will first go into the team folder area and create a new team folder with empty content inside, and then come back to data seeding page and select it from the team folder drop down.

## 4.8 User Management

### 4.8.1 Regular User

Tenant Manager > [Tenant] > User Manager

In the Documentation, the regular user is often referenced as “Team User”.



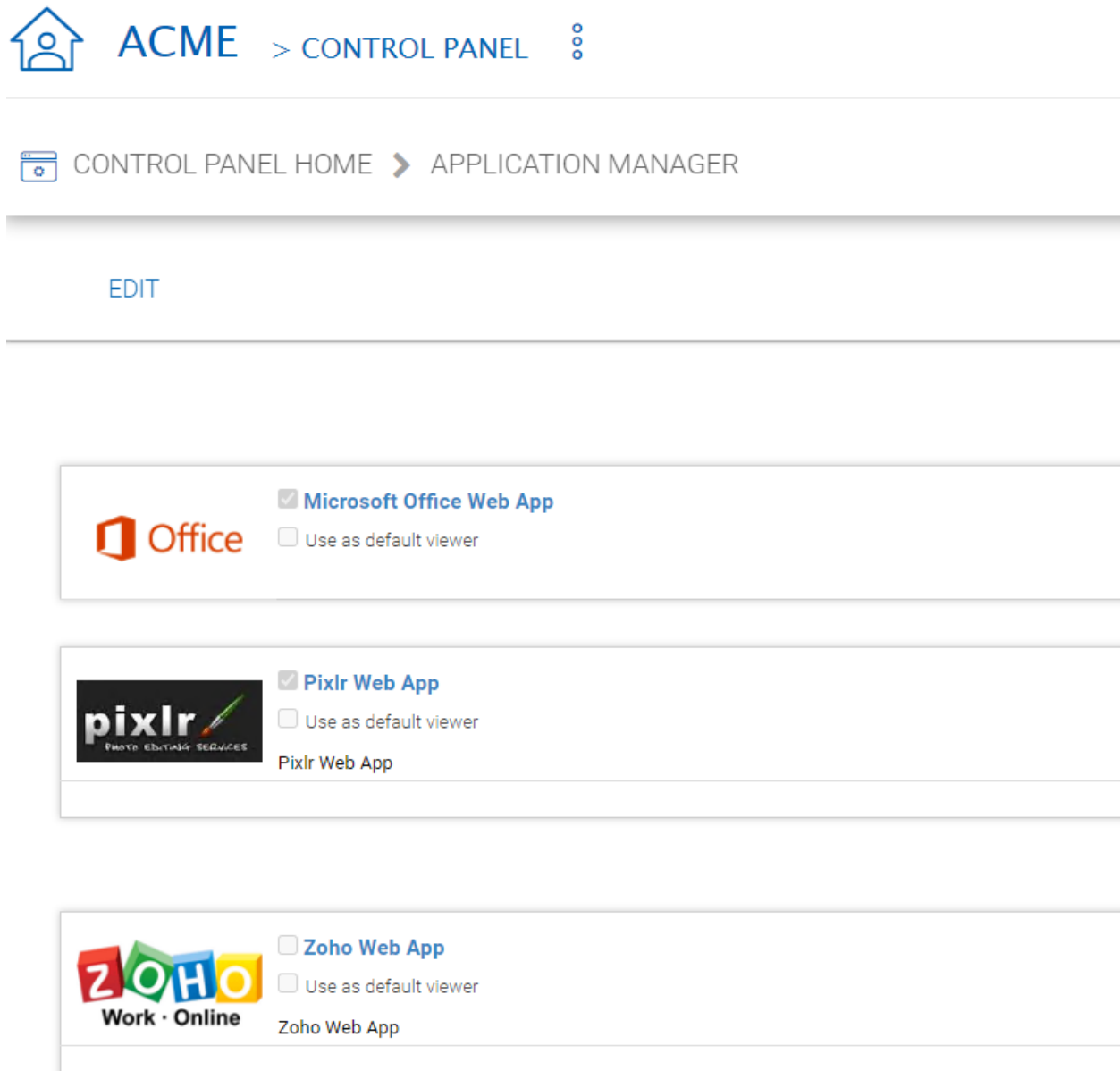


Fig. 34: APPLICATION MANAGER

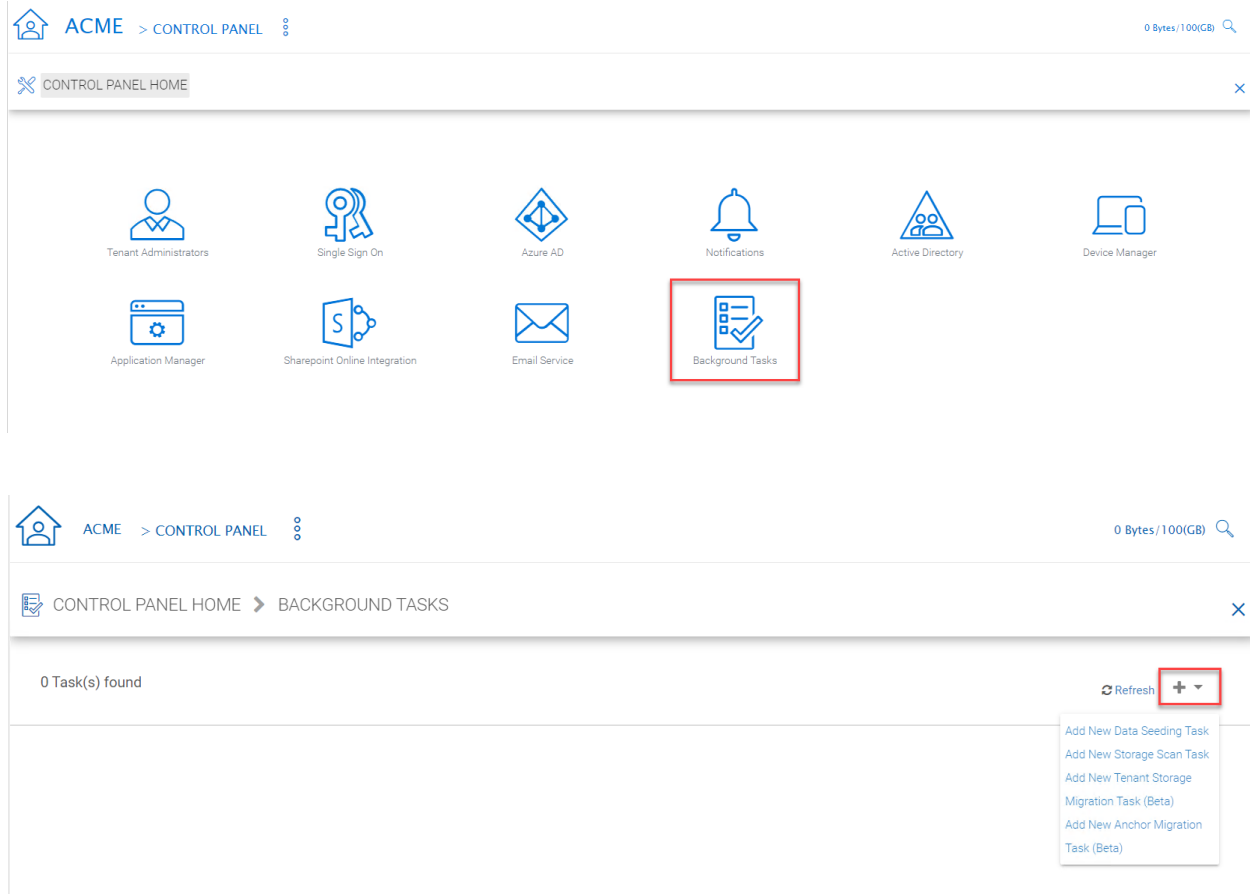


Fig. 35: BACKGROUND TASKS

The screenshot shows the 'DATA SEEDING' form. It includes a 'Description' field, a 'Source (From)' section with sub-fields for 'Local Storage Location (C:\myfolder or \myfiles\server\myshare):', 'User Name (for local storage access):', and 'Password (for local storage access):', and a 'Target (To)' field. A green arrow points from the 'Source (From)' section to the 'Target (To)' field, which contains 'DEF T3'. At the bottom, there is a 'CREATE' button highlighted with a red box and a 'CANCEL' button. A blue banner at the bottom left states 'Data seeding may not start immediately.'

Fig. 36: DATA SEEDING

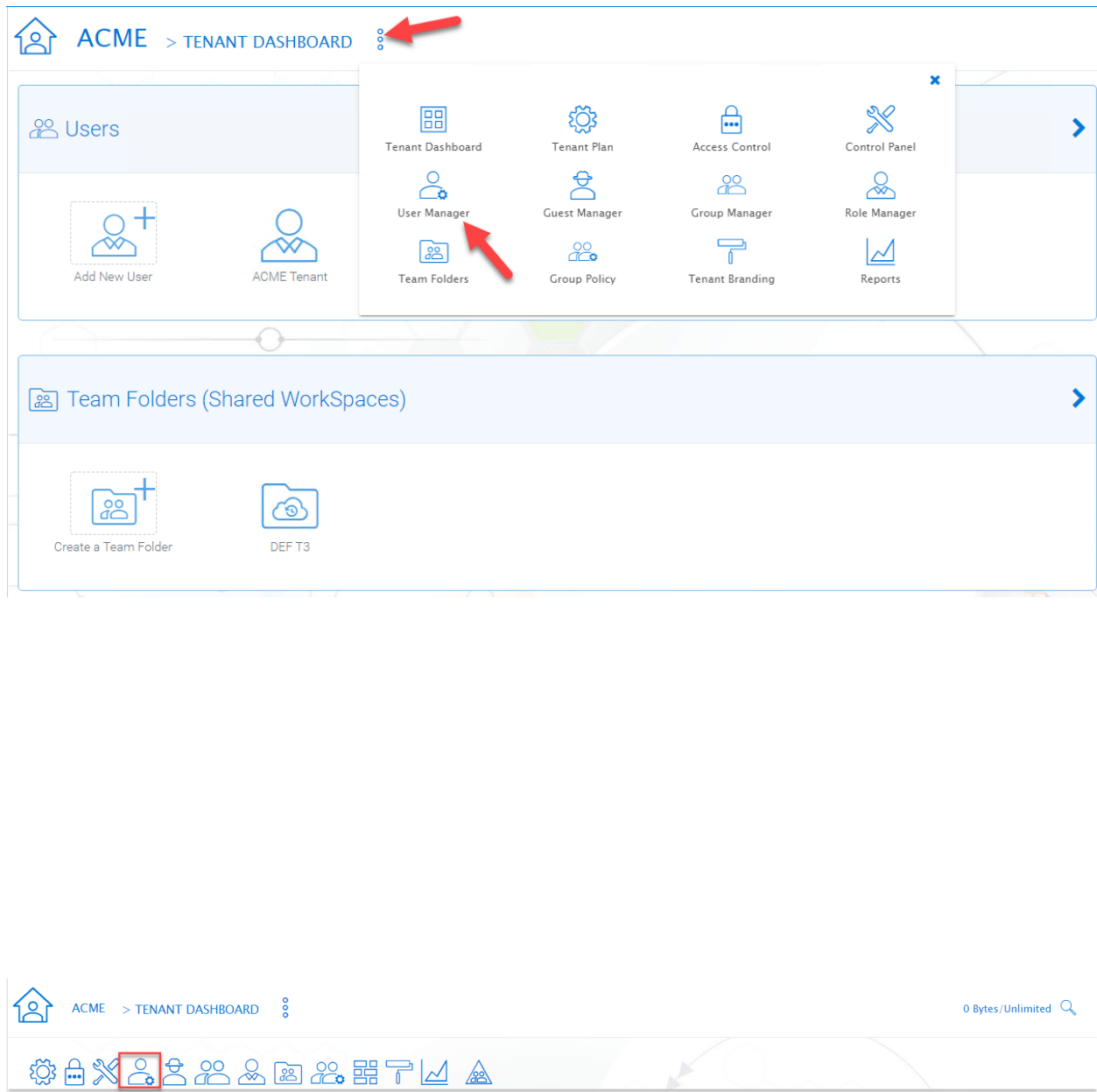


Fig. 37: TENANT ADMIN > USER MANAGER

These are the users that have full privilege of home directory, sharing and other features.

User Manager also have a list view:

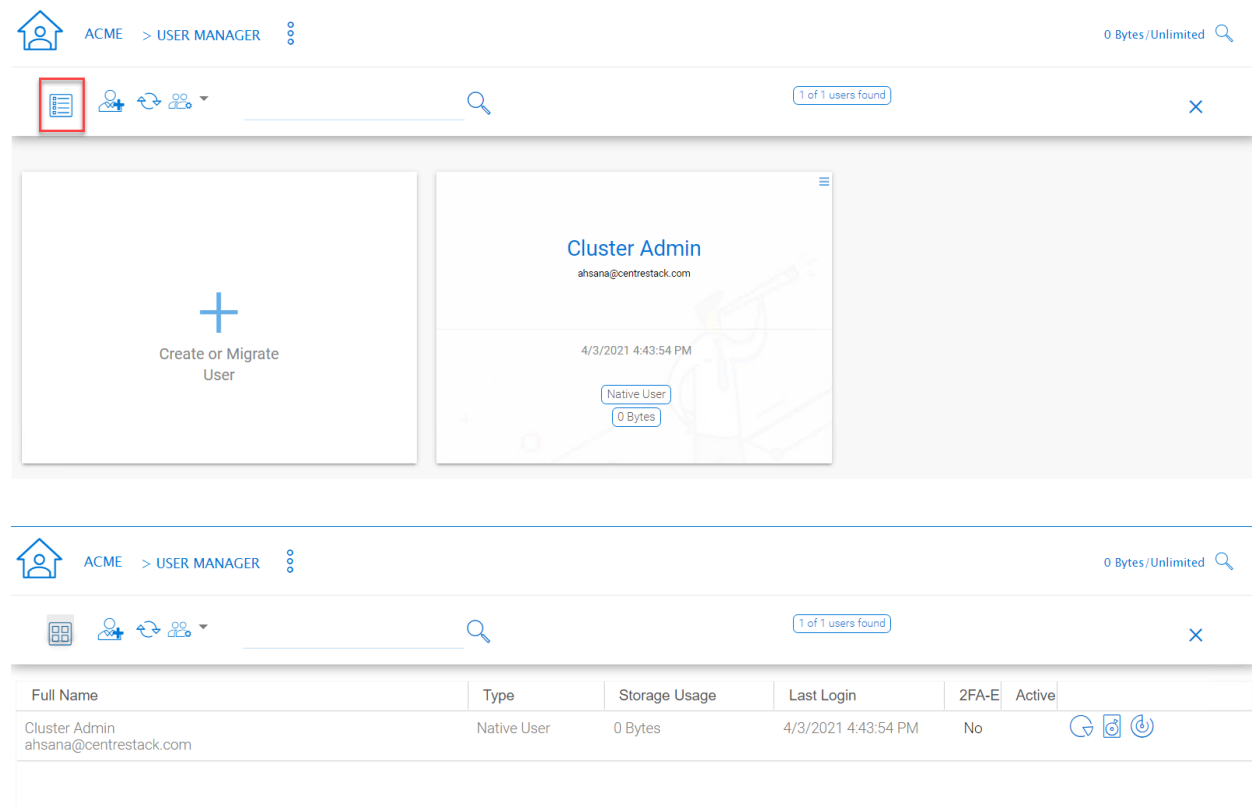


Fig. 38: USER MANAGER LIST/ICON VIEW TOGGLE

If you have Active Directory, normally these are the users in the Active Directory.

- Native User

These are the users that are created manually with an email.

- AD User

These are the users that are imported from Active Directory via LDAP.

- Proxied AD User

These are the users that are imported from Server Agent, where the file server agent is remote and away from the Cluster Server in the customer's site. The customer's Active Directory domain is also remote, and the file server itself (where server agent is installed) is in the remote Active Directory.

### User's File and Folder List

An admin can view a user's file and folder list using the drive icon (3) for the user in Management Console User Manager.

First switch the icon view (1) to detail view (2) and click the drive icon (3) next to the user you are examining. This will open a new window (4) where you can view the files.

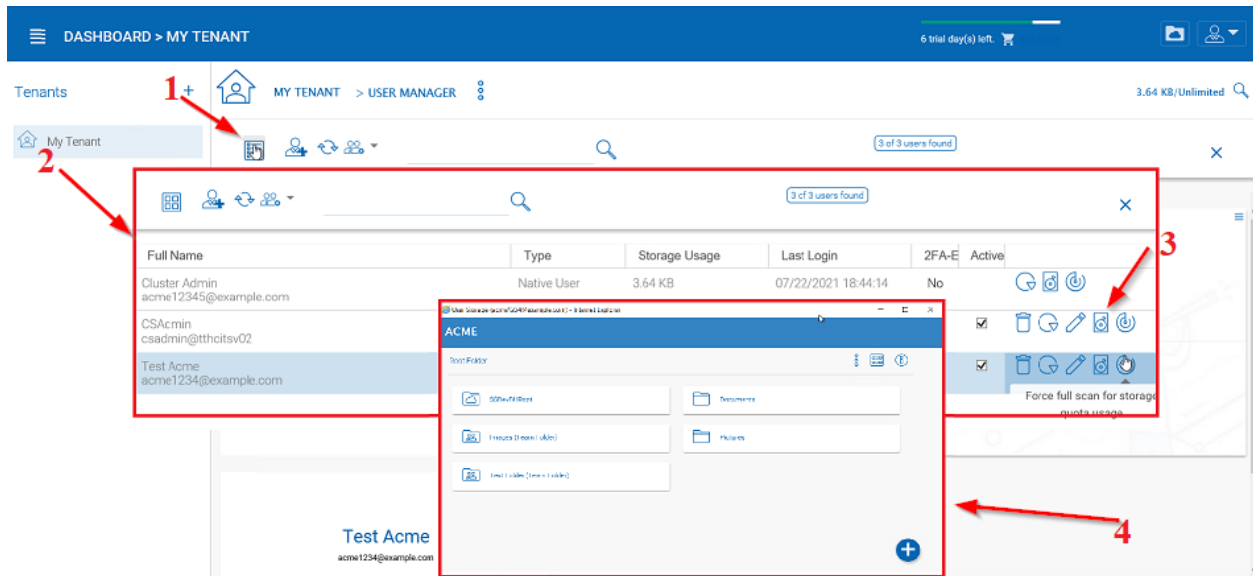


Fig. 39: VIEWING A USER'S FILE AND FOLDER LIST

## 4.8.2 Guest User

Tenant Manager > [Tenant] > Guest Manager

Guest users are users that don't have a home directory. The only folder they have is "Files Shared with Me". So they rely on other "Regular User" sharing files and folders with them before they can do anything. If nobody is sharing anything with a guest user, the guest user doesn't have any read/write permission to any folder.

The primary reason for guest user to exist is to have a secure way for external user to collaborate and edit documents.

## 4.8.3 Group Manager

Tenant Manager > [Tenant] > Group Manager

When you have Active Directory integration, you will leverage the Active Directory group instead of using Group Manager here. This group manager is to create a group of users in a simple way. It is not as complicated as Active Directory (such as supporting nested groups) but make it easy for non-Active Directory users. This is native Cluster group. In the product, you may also see AD group from the user selection user interface and Proxied AD group from the user related interface. The AD group and the proxied AD group are not the same as the group mentioned here.

## 4.8.4 Role Manager

Tenant Manager > [Tenant] > Role Manager

The Role Manager is to provide role based administration. For example, you may want to provide read-only permissions to some users. You can also assign some group policies to some groups of users. More and more policy items are added to the role manager so in addition to only use role manager for administration, it can be also used to define policy items for users.

When creating a role, there are 4 different sections

- Sharing
- Policies

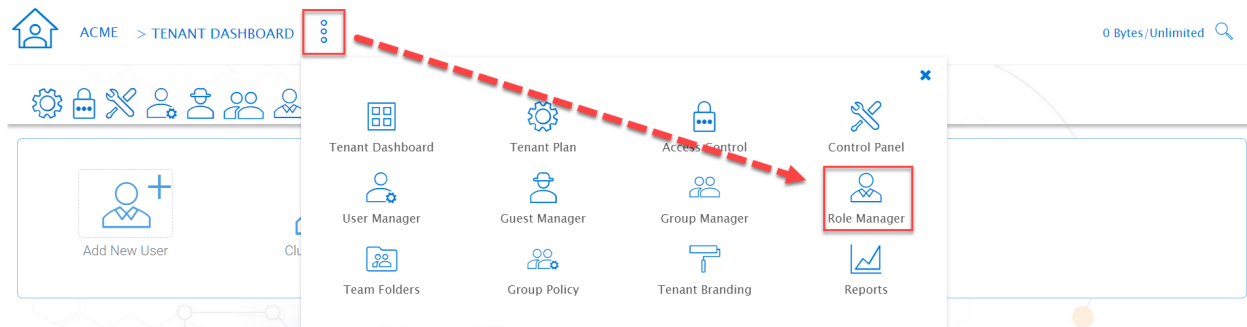
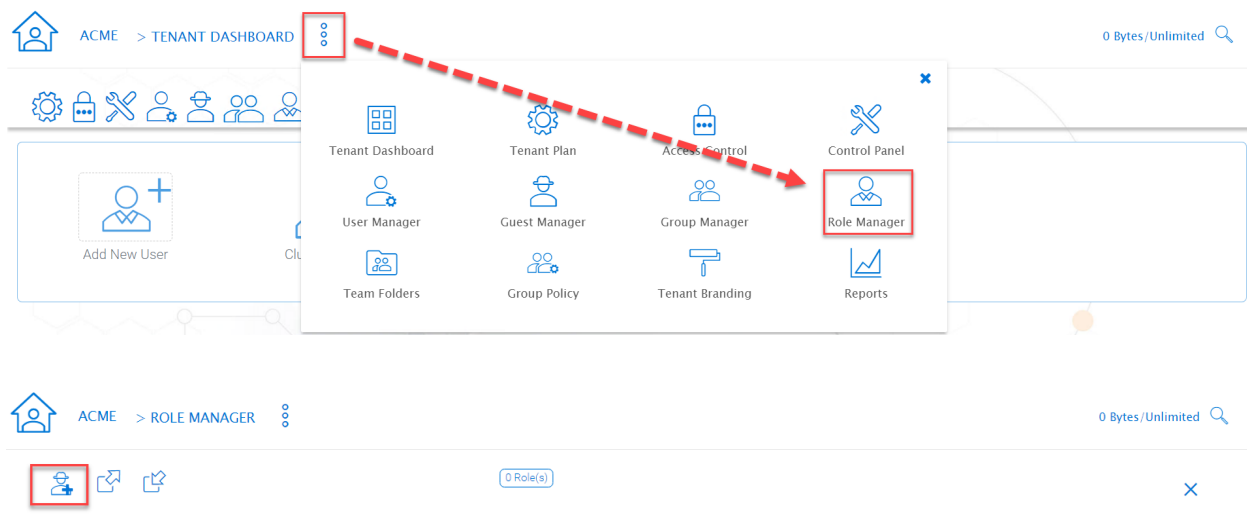


Fig. 40: ROLE MANAGER ENTRY

- Permissions
- Assigned Users/Groups

### Create New Role

You can define areas in the tenant administrator's management console and assign it into a role.



No roles have been created

### Policies

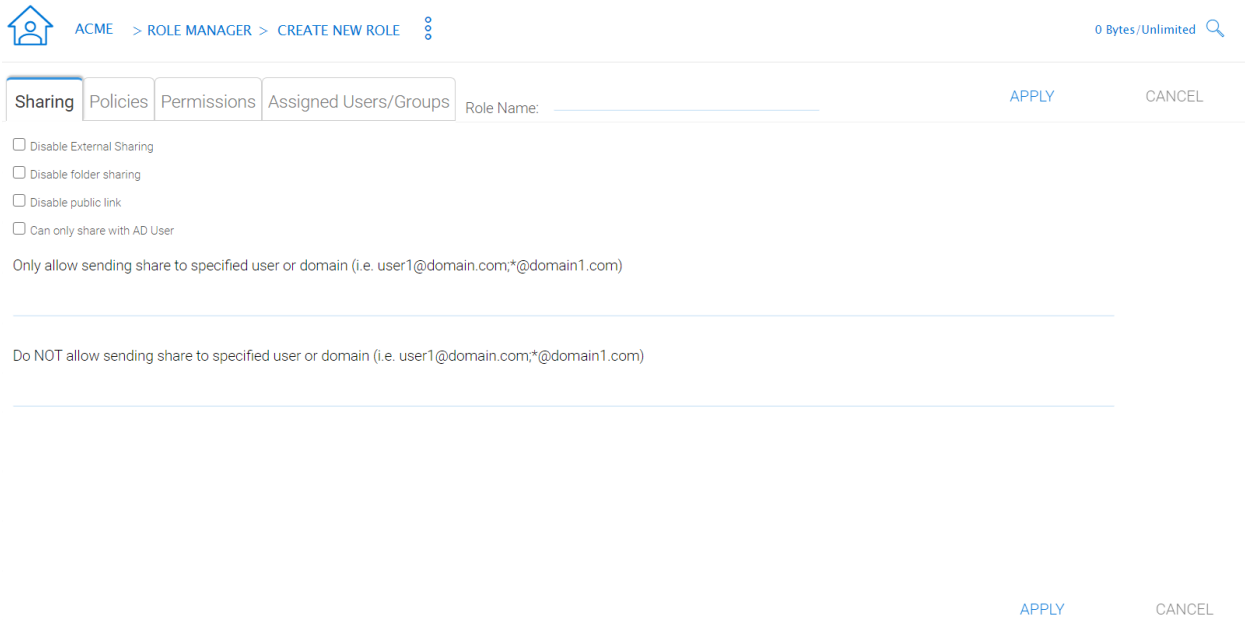
additional policies for the role.

### Permissions

Additional Permissions that can be assigned to a role.

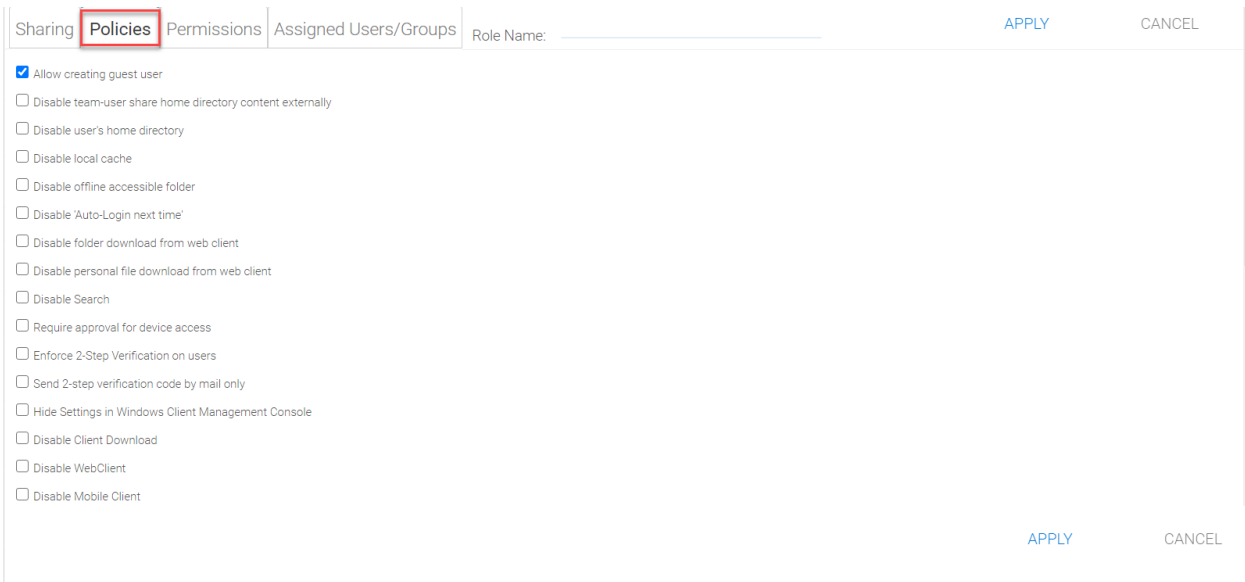
### Assigned Users/Groups

After the content of the role is all set, users and groups can be assigned to a role.



The screenshot shows the 'CREATE NEW ROLE' page in the CentreStack Role Manager. The breadcrumb navigation is 'ACME > ROLE MANAGER > CREATE NEW ROLE'. The top right shows '0 Bytes / Unlimited' and a search icon. The page has four tabs: 'Sharing' (selected), 'Policies', 'Permissions', and 'Assigned Users/Groups'. Below the tabs is a 'Role Name:' field. The 'Sharing' tab contains several checkboxes: 'Disable External Sharing', 'Disable folder sharing', 'Disable public link', and 'Can only share with AD User'. Below these is a text input field for 'Only allow sending share to specified user or domain (i.e. user1@domain.com;\*@domain1.com)'. At the bottom right, there are 'APPLY' and 'CANCEL' buttons.

Fig. 41: ROLE MANAGER SHARING



The screenshot shows the 'CREATE NEW ROLE' page in the CentreStack Role Manager, specifically the 'Policies' tab. The breadcrumb navigation is 'ACME > ROLE MANAGER > CREATE NEW ROLE'. The top right shows '0 Bytes / Unlimited' and a search icon. The page has four tabs: 'Sharing', 'Policies' (selected), 'Permissions', and 'Assigned Users/Groups'. Below the tabs is a 'Role Name:' field. The 'Policies' tab contains a list of checkboxes: 'Allow creating guest user' (checked), 'Disable team-user share home directory content externally', 'Disable user's home directory', 'Disable local cache', 'Disable offline accessible folder', 'Disable 'Auto-Login next time'', 'Disable folder download from web client', 'Disable personal file download from web client', 'Disable Search', 'Require approval for device access', 'Enforce 2-Step Verification on users', 'Send 2-step verification code by mail only', 'Hide Settings in Windows Client Management Console', 'Disable Client Download', 'Disable WebClient', and 'Disable Mobile Client'. At the bottom right, there are 'APPLY' and 'CANCEL' buttons.

Fig. 42: ROLE MANAGER POLICIES

ACME > ROLE MANAGER > CREATE NEW ROLE

0 Bytes/Unlimited

Sharing Policies **Permissions** Assigned Users/Groups Role Name: \_\_\_\_\_ APPLY CANCEL

Operation	View	Add	Edit	Delete
Team Folders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Groups	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest Users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group Policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Active Directory Settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Branding	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reports	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Client Device Manager	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

APPLY CANCEL

Fig. 43: ROLE MANAGER PERMISSIONS

ACME > ROLE MANAGER > CREATE NEW ROLE

0 Bytes/Unlimited

Sharing Policies Permissions **Assigned Users/Groups** Role Name: \_\_\_\_\_ **+** APPLY CANCEL

User Name	Email	
[BuiltInGroup] All AD Users	N/A	✕

Fig. 44: ROLE MANAGER ASSIGNED USERS/GROUPS



## 4.9 Team Folders

Tenant Manager > [Tenant] > Team Folders

The team folder concept is like a network share, meaning you can define a folder and then add users and groups to the folder and thus turn it into a team shared folder. The team folder will show up in the user's folder list when the user is added to the team folder.

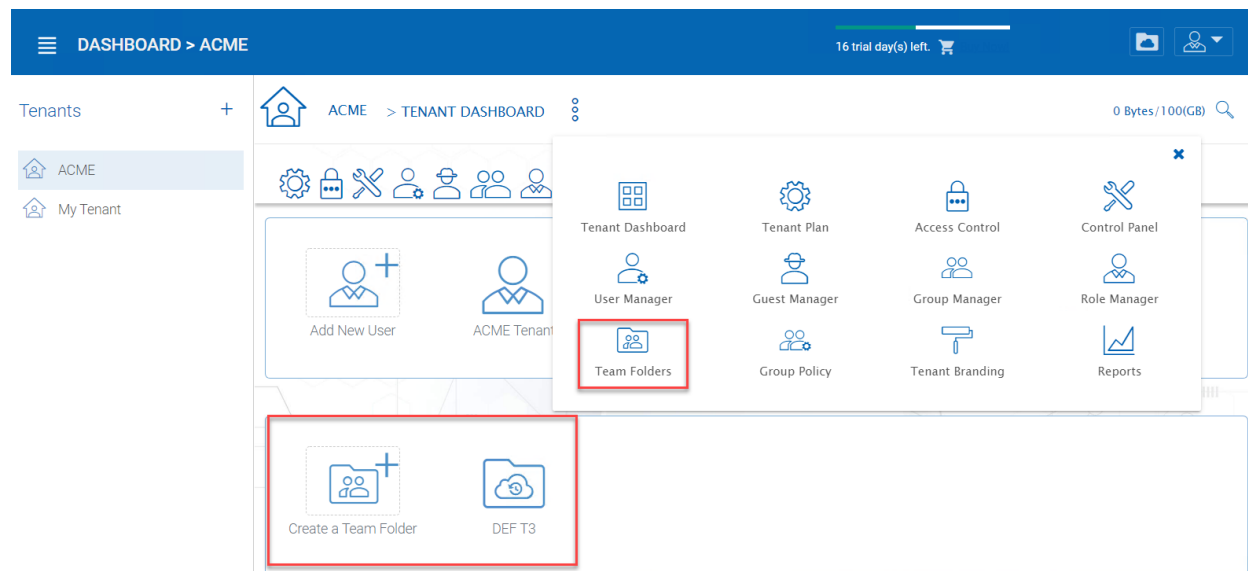


Fig. 45: ENTER TEAM FOLDER SECTION

When the server agent is in use, the team folder can be mapped directly to a network share from the server where the server agent is installed.

When a directly connected network share is used, a team folder can be mapped to an SMB/CIFS network share directly.

You can also turn any existing folder into a team folder.

A Team folder has a tenant administrator scope so the team folder related sharing is limited to the users inside the tenant.

---

**Note:** By default, the files and folders that the administrator can see is hidden away from the regular team user until those folders are published to the team users.

---

Team Folders (Shared Work Space) are used for team-share collaborations. Generally, Team Folders are converted from File Server Network shares. Other Team Folder sources can be Google Storage, Amazon S3 (or S3 Compatible), Amazon Cloud, Windows Azure Blob, WebDav, SharePoint, Rackspace (US or UK) and OpenStack or you can create new folders under the Tenant's root storage.

In the team folders page, you can manage team shares, folder permissions and the underlying storage configuration.

### 4.9.1 Create Team Folder

Tenant Manager > [Tenant] > Team Folders > Add New Team Folder

You can click on the "+" sign to create a new team folder.

Once it is clicked, it shows four main sources of team folder, among other options:

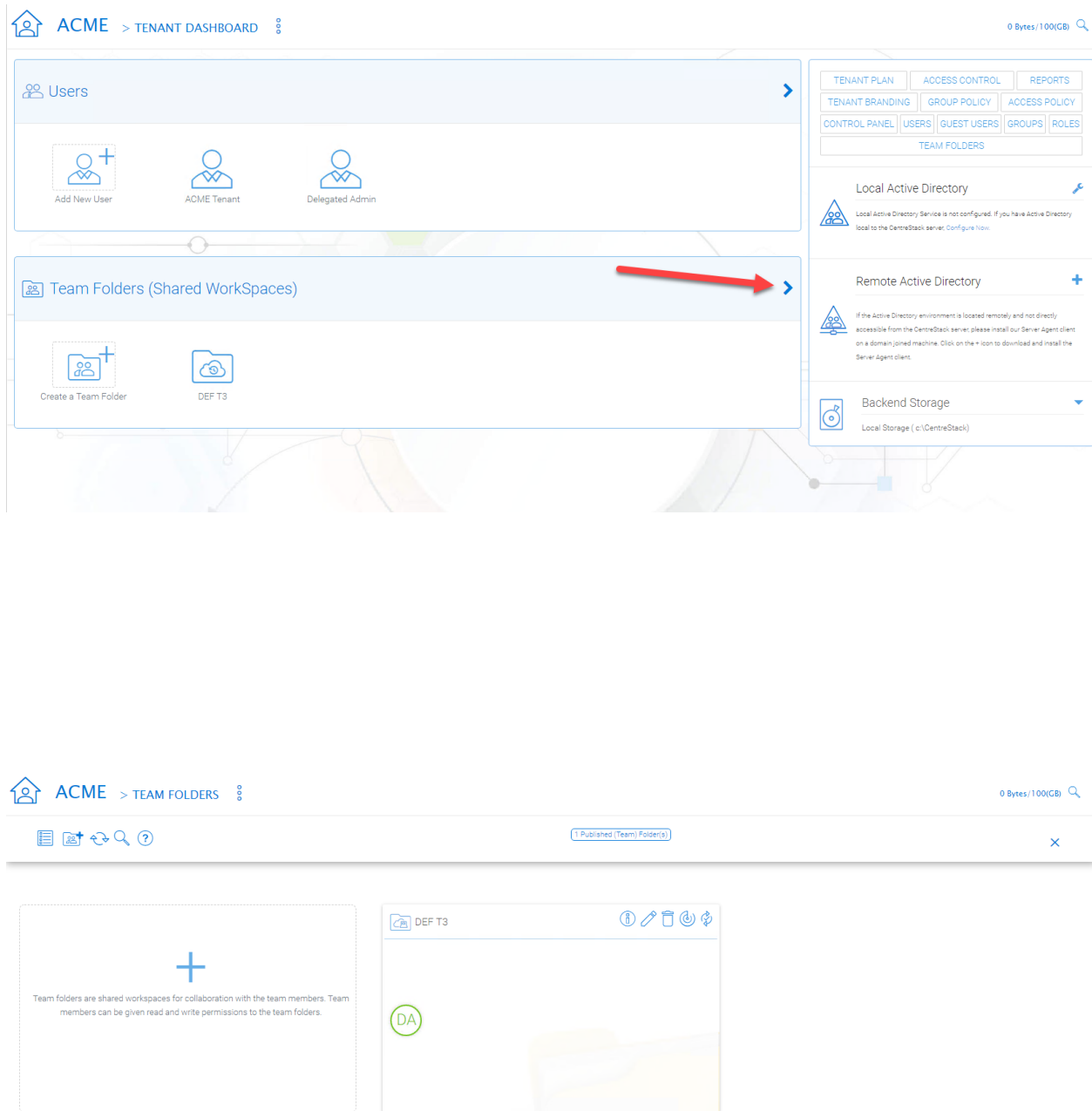


Fig. 46: MANAGING TEAM SHARES

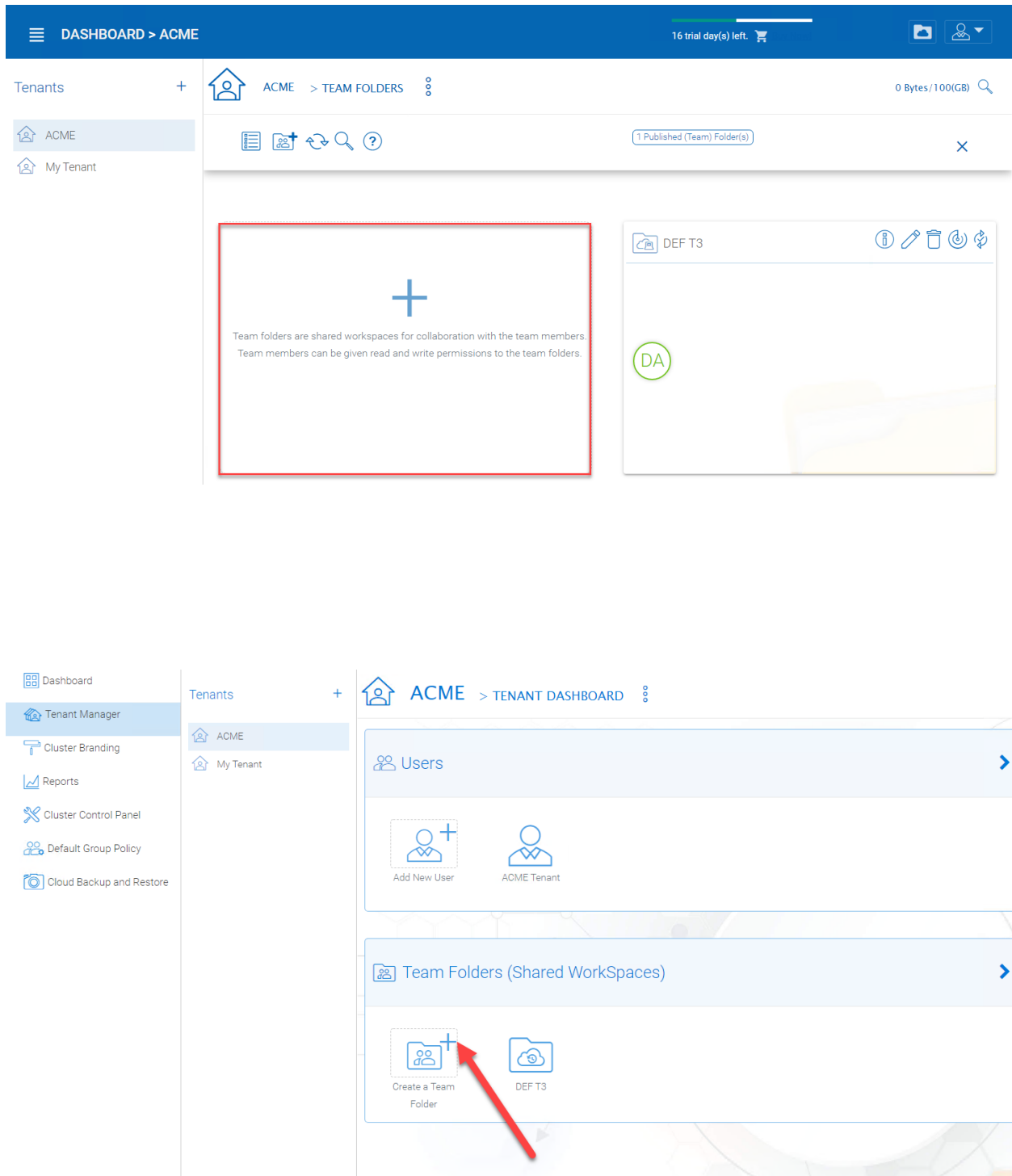


Fig. 47: ADDING A TEAM FOLDER

- Existing Tenant Storage (default location)
- File Servers in Local Area Network
- Remote File Servers
- Cloud Storage

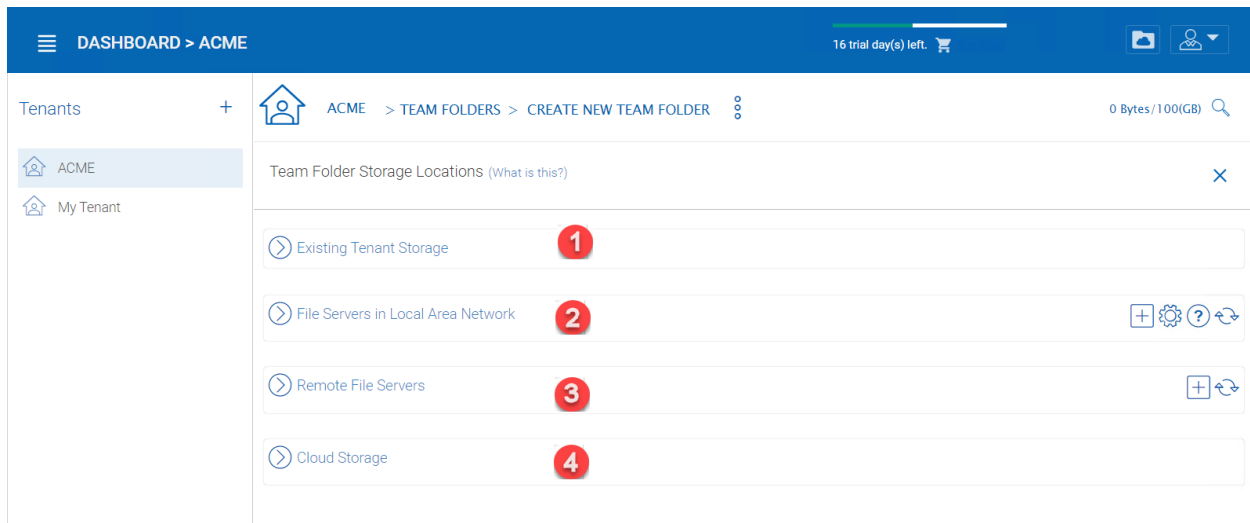


Fig. 48: TEAM FOLDER LOCATIONS

### Existing Tenant Storage (default location)

When you pick this option to create a team folder, the team folder will be created from the default storage from scratch with an empty team folder. Usually when you want to have a team folder that is brand new and empty, you can pick this option.

Another use case is “Existing Folder(s)”, in which you can pick several existing folders, which physically may not be in the same folder, but you can logically arrange them into the same team folder. For example, you may want to have a short term project that put “Building A”, “Blue Print A”, “Budget A”, three different folders from three different places into one logical

### File Servers in Local Area Network

When you have files and folders from the local area network (LAN), you can convert the network share directly into a team folder in the Cluster Server. It is a one-to-one relationship between a team folder and a network share. When you pick this option, most of the time, the Active Directory server for this tenant is also in the same Local Area Network.

### Publish Tenant Home Storage As a Team Folder



By default, the tenant’s root storage folder is not published to any team user. To use an analogy, it is like a C: drive on a Windows File Server, by default it is not published as a network share to users. However, if you want to make it available to users, you can pick this option.


### Remote File Server



When you have server agents installed on remote file servers, those file servers will be visible and the network shares from remote file servers will be imported to the Cluster Server.

### Cloud Storage

You can also pick Cloud Storage as this team folder’s underlying storage. As shown in the following picture, you can pick Amazon S3, Windows Azure Blob, OpenStack Swift, and other cloud storage services.

 DASHBOARD > > TENANT DASHBOARD 

20 trial day(s) left.  [Buy Now!](#)

 [Existing Tenant Storage](#)

 **Default Tenant Storage**  
Create a new team folder from scratch using default storage. It will be empty to start with and you can put files and folders inside later.

 **Existing Folder(s)**  
Create a new team folder by selecting one or more existing folders. Those selected folders will show up inside the team folder.

 **Publish Tenant Home Storage As a Team Folder**  
The tenant's home storage will be published to users in the same tenant so they can see file and folder contents from the home storage. Some specialized folder such as folders from remote file servers or remote cloud storage services are not included in this scope.

 File Servers in Local Area Network    

 Remote File Servers  

 Cloud Storage

Fig. 49: EXISTING TENANT STORAGE

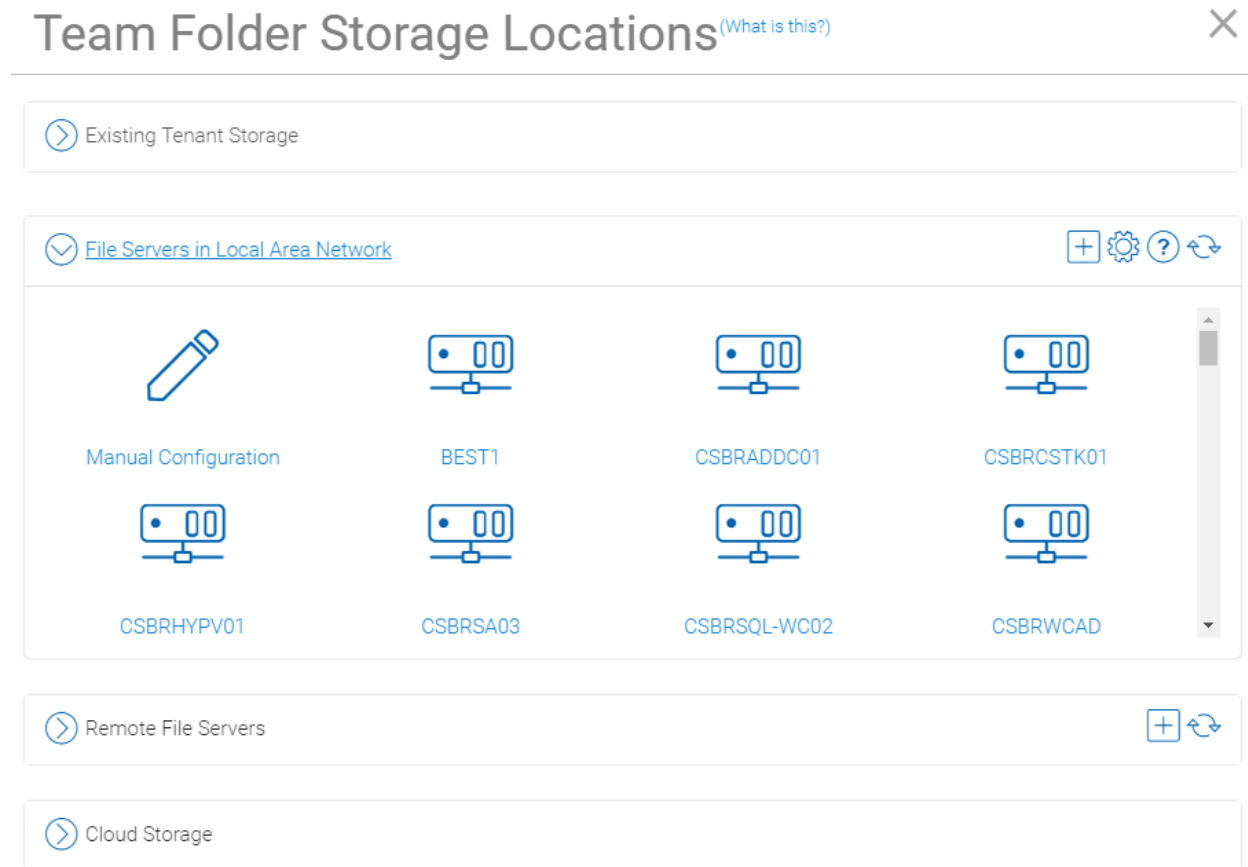


Fig. 50: LAN-BASED TEAM FOLDER

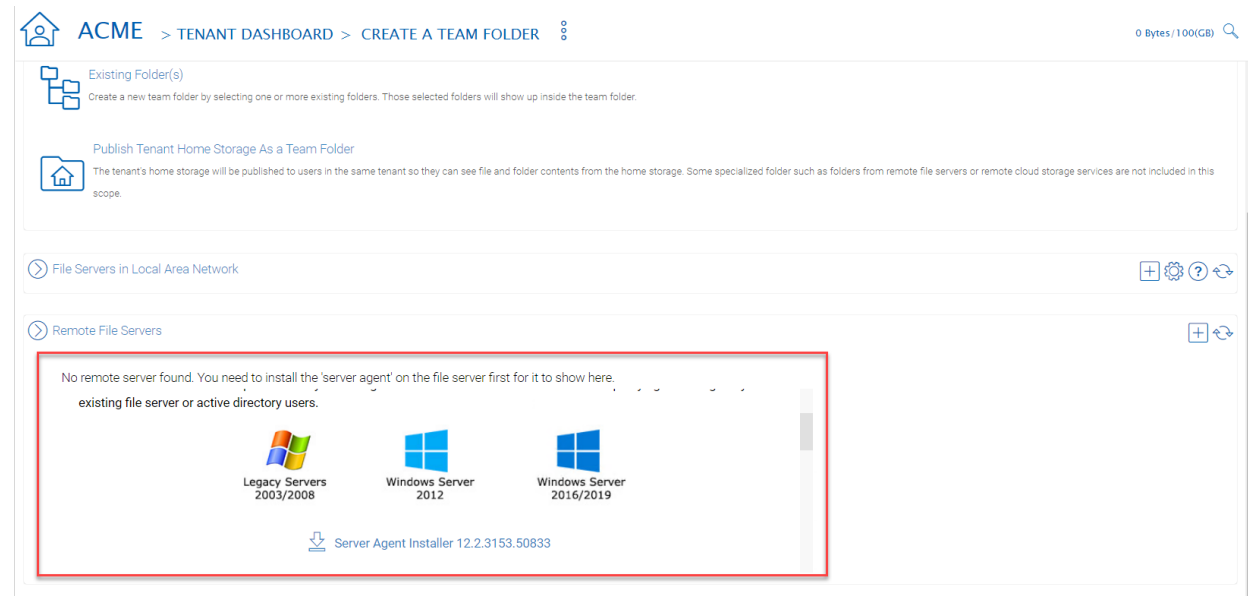


Fig. 51: REMOTE TEAM FOLDER

## Team Folder Storage Locations (What is this?)



> Existing Tenant Storage

> File Servers in Local Area Network



> Remote File Servers



✓ [Cloud Storage](#)



Google Cloud Storage



Amazon S3



Amazon S3 (GovCloud)



Amazon S3 Compatible



Windows Azure Blob



WebDav



SharePoint



Rackspace Cloud Files US



Rackspace Cloud Files UK



Open Stack



Open Stack...e 2.0/3.0)

Fig. 52: CLOUD-BASED TEAM FOLDER

## Team Folder Properties

### 4.9.2 Team Folder Information

Tenant Manager > [Tenant] > Team Folders > {Pick a Team Folder} > info button

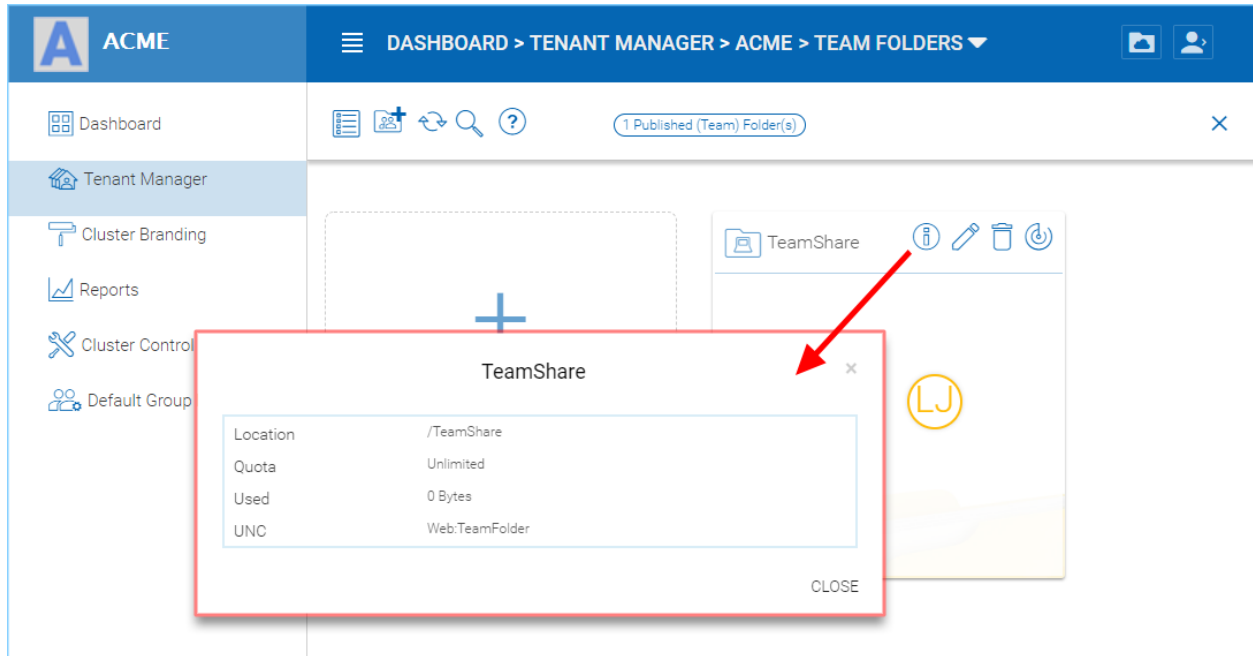


Fig. 53: TEAM FOLDER INFORMATION ACCESS

### 4.9.3 Collaborators

Tenant Manager > [Tenant] > Team Folders > {Pick a Team Folder} > edit button > Collaborators

In the Collaborators section, you can define:

**User List:** The users and groups that are assigned to the team folder. The users with the owner flag will be able to manage the users.

### 4.9.4 External Sharing

Tenant Manager > [Tenant] > Team Folders > {Pick a Team Folder} > edit button > External Sharing

You can see what folders and files have been shared and control access to those files from this setting.

### 4.9.5 Access Policy

Tenant Manager > [Tenant] > Team Folders > {Pick a Team Folder} > edit button > Access Policy

You can enable an access policy through this tab.



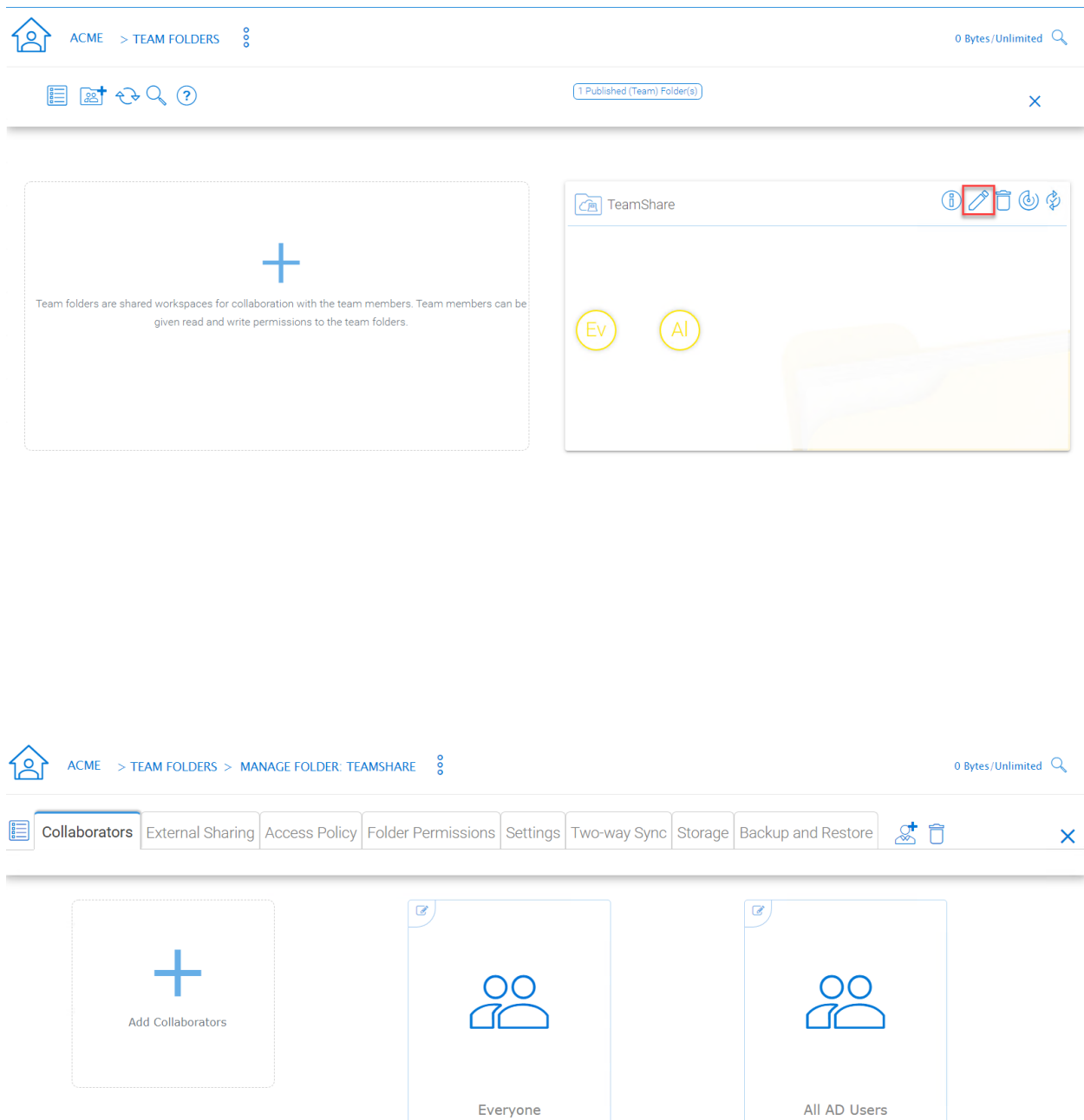


Fig. 54: EDITING FOLDER PERMISSIONS

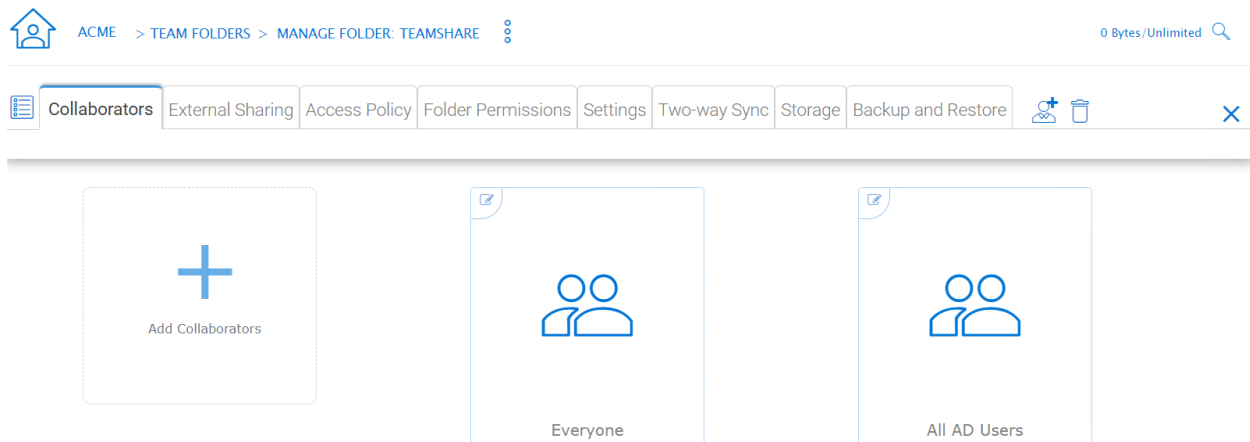


Fig. 55: TEAM FOLDER PERMISSION SETTINGS

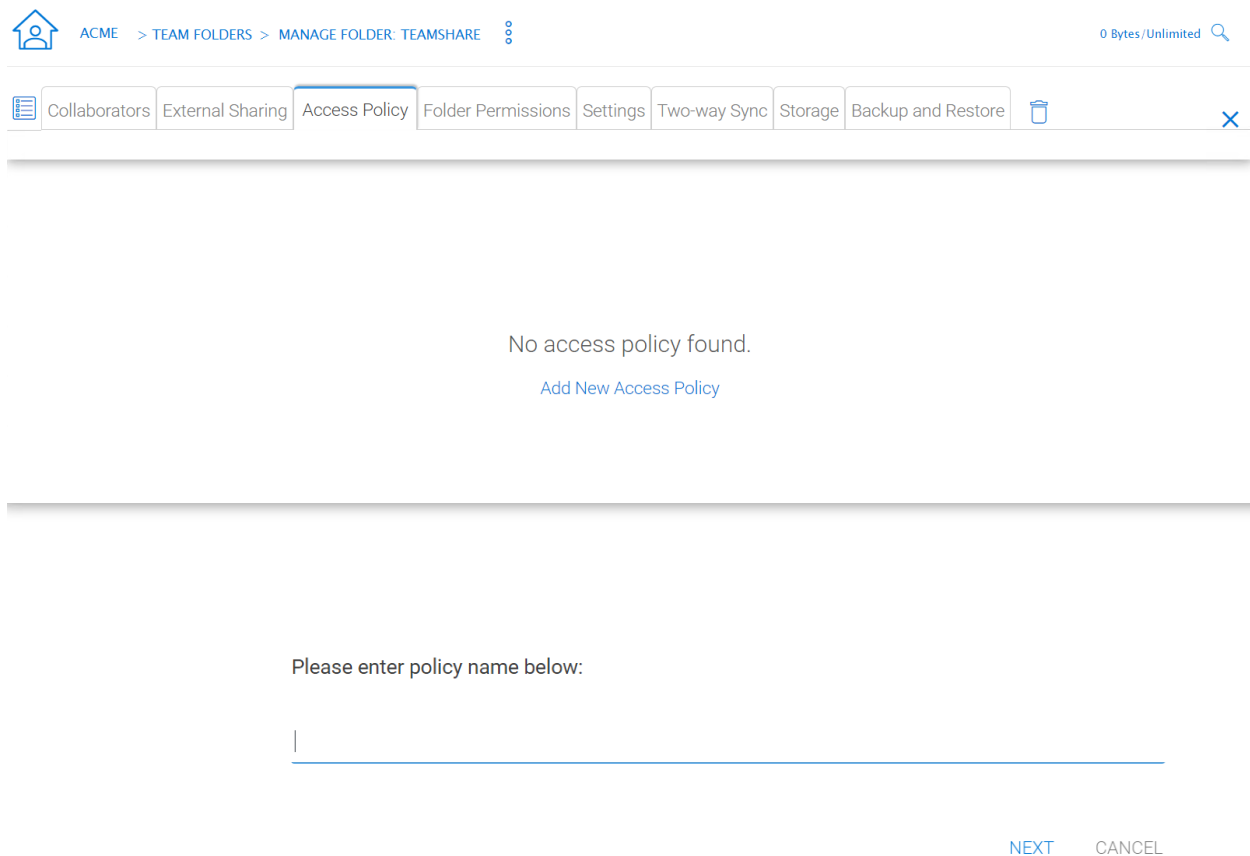


Fig. 56: Client Access Policies

Define customized access policies to restrict and allow access based on the device location. For example, a company can enable access from the internet to only Windows clients and web clients. IT can configure allow or deny client access policies from the following locations:

Access from the internet, access from local network, access from Anywhere, access from customer-defined networks, deny access from customer defined networks.

The above allow and deny client access policies can be configured for the following clients:

web client, web management, windows client, mac client, mobile client.

Please enter access condition:

Access from Internet

Access from Internet

Access from Local Network

Access from Anywhere

Access from Customer-Defined Network

Not Access from Customer-Defined Network

BACK NEXT CANCEL

ACME > TEAM FOLDERS > MANAGE FOLDER: TEAMSHARE

Collaborators External Sharing Access Policy Folder Permissions Settings Two-way Sync Storage Backup and Restore

Allow following checked permission(s)

☒ Visible

☒ Permission to list files

☒ Permission to read files

☒ Permission to create/update files/folders

☒ Permission to delete files/folders

☐ Secure data room

BACK COMMIT CANCEL

IT can also prevent data loss and data leakage of important company confidential shares by configuring 'Share Access Policies' for external users who are not company employees. Again, IT can configure allow or deny shares access policies from the following locations:

-Access from the internet -Access from local network -Access from Anywhere -Access from customer-defined networks -Deny access from customer defined networks

The above allow and deny share access policies can be configured with the following conditions:

-Visible -Permissions to list files -Permissions to read files -Permissions to create or update files and folders -Permissions to delete files and folders -Secure data room

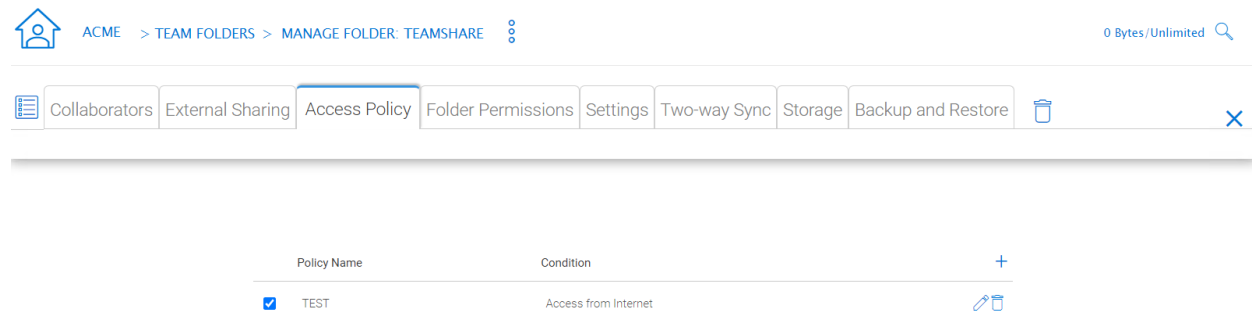


Fig. 57: Share Access Policy

## ACCESS POLICY SETTINGS

## 4.9.6 Folder Permissions

Tenant Manager > [Tenant] > Team Folders > {Pick a Team Folder} > edit button > Folder Permissions

You can browse to different sub-folders and define the folder permission. The folder permissions defined here represent the Cluster Server side of the permission.

If you are leveraging native Active Directory/NTFS permission from a file server, you don't need to define any permissions here.

**Note:** You can think of the permissions as two different gates controlling the access to files and folders. The first gate is defined here as the Cluster Server Folder Permission. After this permission check, there is still a check at the file server level (which is the NTFS permission).

In practice, usually it is done one way or the other. If you have decided to use NTFS natively, you can leave the permission settings here empty and not defined.

## 4.9.7 Settings

Tenant Manager > [Tenant] > Team Folders > {Pick a Team Folder} > edit button > Settings

Here is a look at the details of the Team Folder Settings:

### Disable further sharing

Don't allow users to share out team folder contents.

### Create CIFS Share

If there are server agents connected to the tenant, create a CIFS share on the file server agent server as a standard Windows network share.

### Disable Offline Access

Don't allow Windows clients or Mac clients to mark their folders as offline from within the team folder.

### Synchronize folder permission automatically

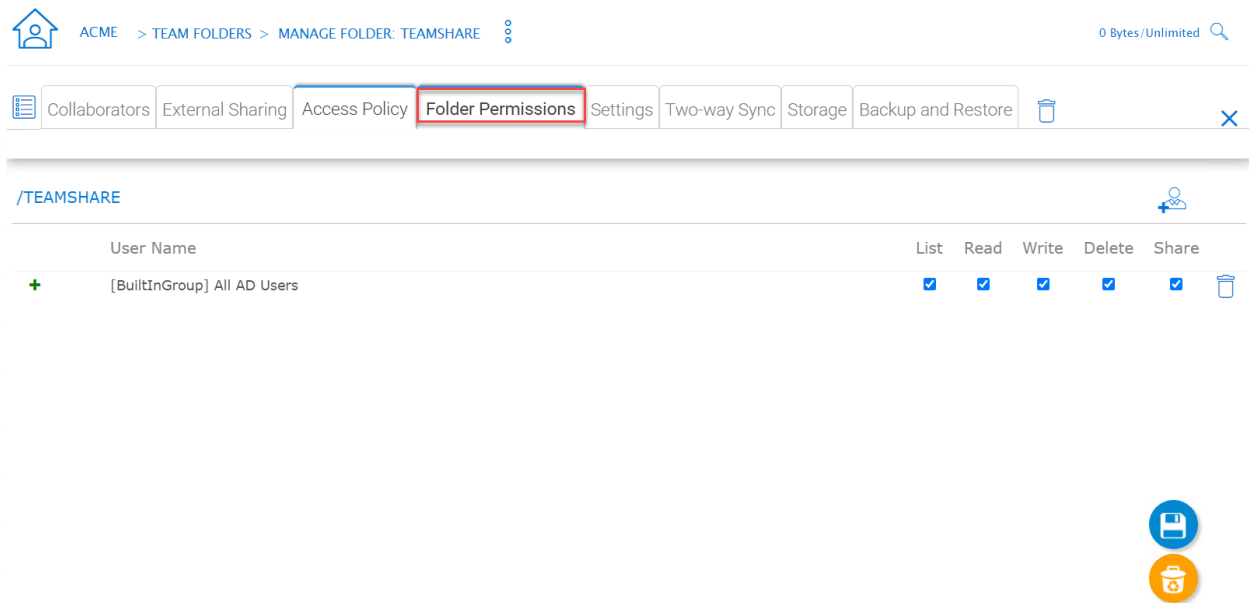


Fig. 58: TEAM FOLDER PERMISSION SETTINGS

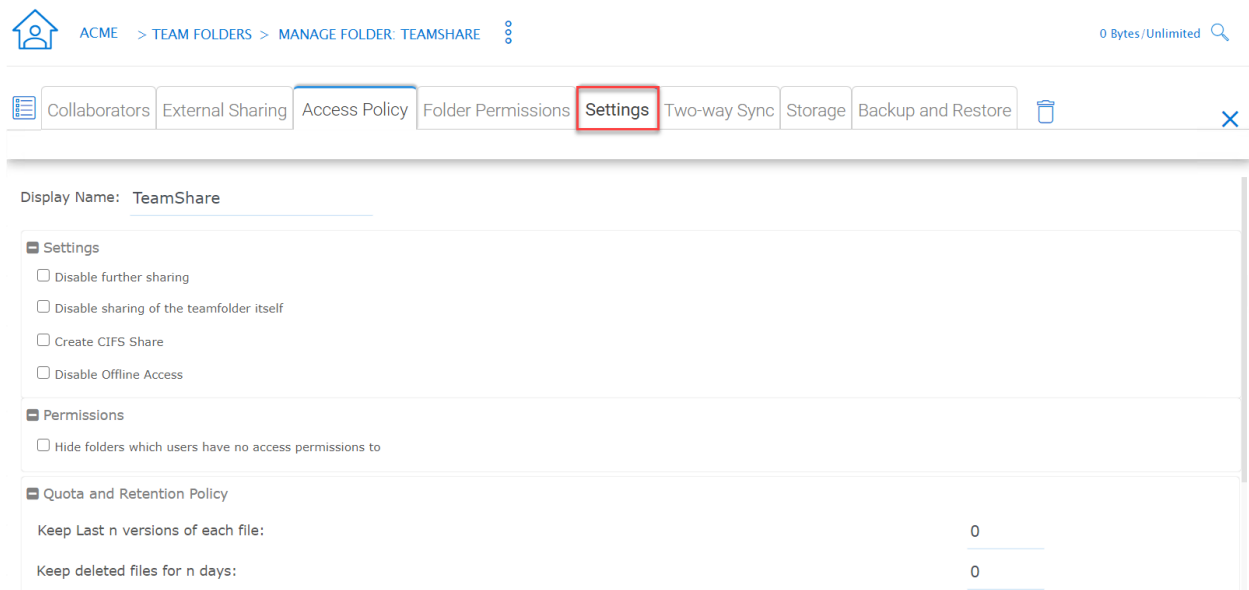
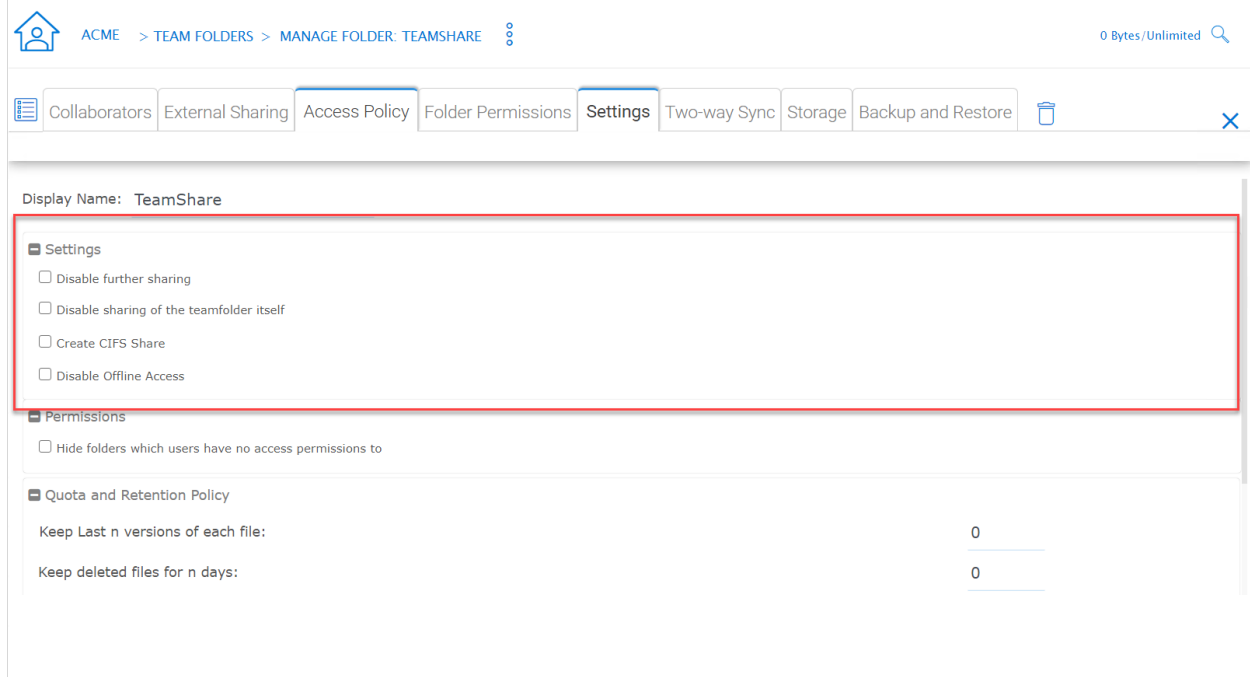


Fig. 59: TEAM FOLDER SETTINGS OVERVIEW



ACME > TEAM FOLDERS > MANAGE FOLDER: TEAMSHARE 0 Bytes/Unlimited

Collaborators External Sharing Access Policy Folder Permissions **Settings** Two-way Sync Storage Backup and Restore

Display Name: TeamShare

**Settings**

- ☐ Disable further sharing
- ☐ Disable sharing of the teamfolder itself
- ☐ Create CIFS Share
- ☐ Disable Offline Access

**Permissions**

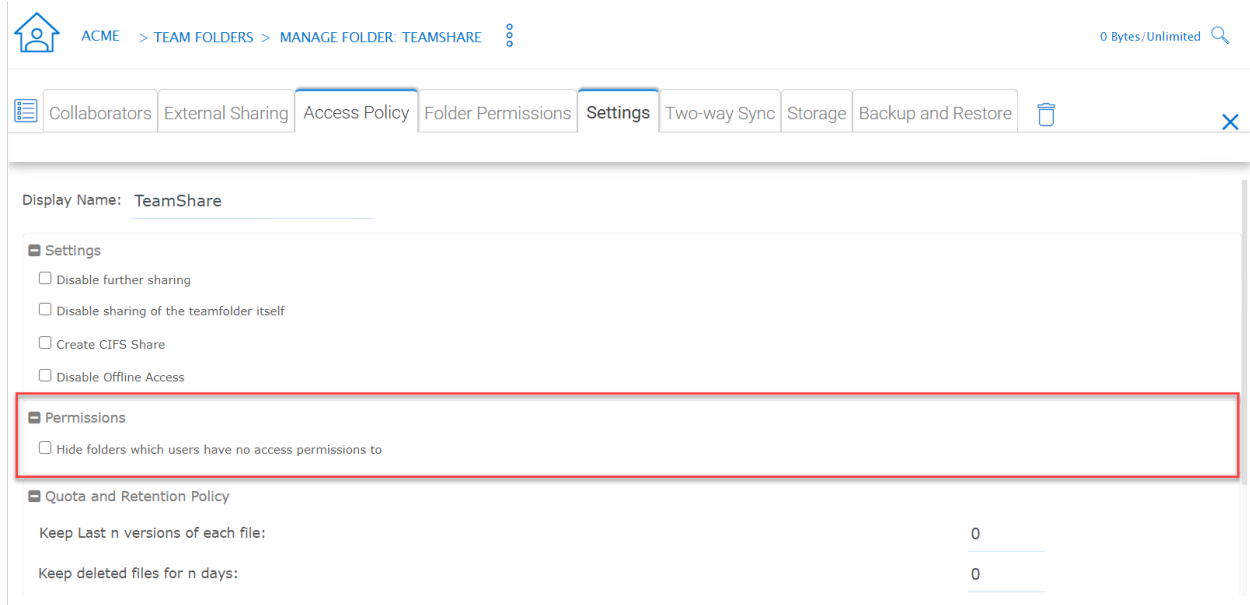
- ☐ Hide folders which users have no access permissions to

**Quota and Retention Policy**

Keep Last n versions of each file: 0

Keep deleted files for n days: 0

Fig. 60: TEAM FOLDER SETTINGS DETAIL



ACME > TEAM FOLDERS > MANAGE FOLDER: TEAMSHARE 0 Bytes/Unlimited

Collaborators External Sharing Access Policy Folder Permissions **Settings** Two-way Sync Storage Backup and Restore

Display Name: TeamShare

**Settings**

- ☐ Disable further sharing
- ☐ Disable sharing of the teamfolder itself
- ☐ Create CIFS Share
- ☐ Disable Offline Access

**Permissions**

- ☐ Hide folders which users have no access permissions to

**Quota and Retention Policy**

Keep Last n versions of each file: 0

Keep deleted files for n days: 0

Fig. 61: TEAM FOLDER SETTINGS - PERMISSIONS

If the folder is coming from a file server agent, sync the NTFS permission over to the cloud side. This is emulating NTFS permission with the CentreStack Server is away from the file server across the Internet.

### Don't show folder users doesn't have permissions to access

Hide the folder instead of showing users folders that they will receive "Access Denied".

### Quota and Retention Policy

Team folder can have a per-team folder retention policy.

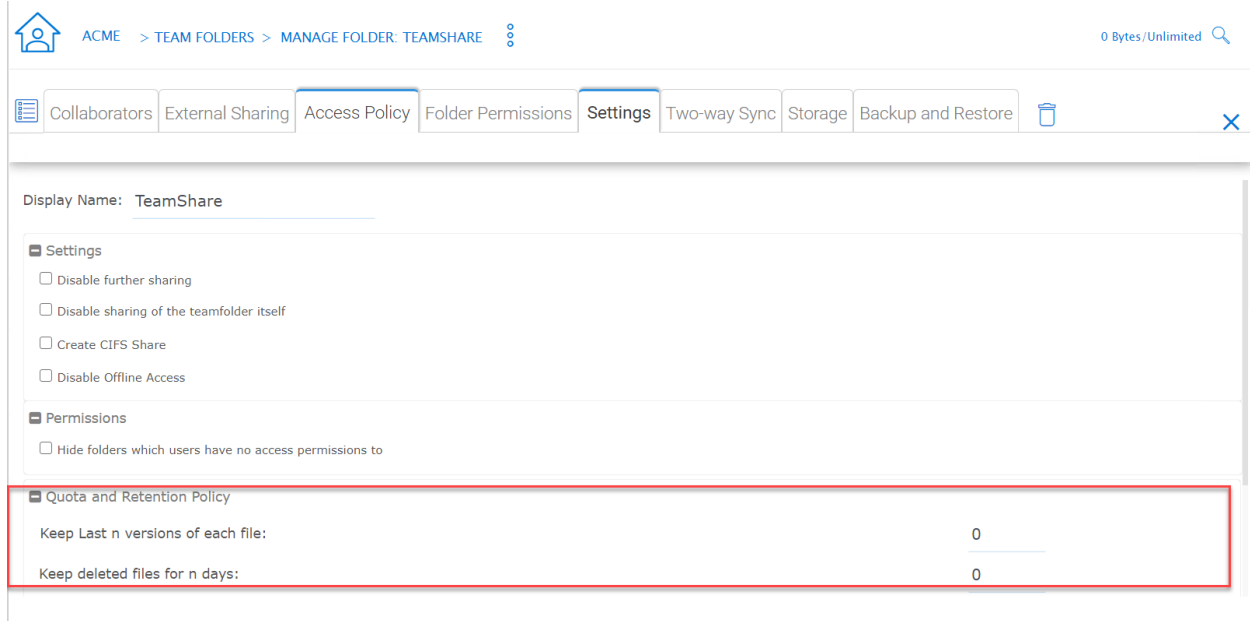


Fig. 62: QUOTA AND RETENTION POLICY

## 4.10 Group Policy

Tenant Manager > [Tenant] > Group Policy

### 4.10.1 Common Settings

Tenant Manager > [Tenant] > Group Policy > Common Settings

#### 4.10.1.1 Security

Tenant Manager > [Tenant] > Group Policy > Common Settings > Security

#### Allow Cluster Admin to manage my tenant

when enabled, the cluster-admin will be able to use the "Manage Tenant" link to manage the tenant in the tenant manager. This is very convenient for cluster administrators (typically system administrators from service providers) to provide management work to the tenant.

#### Enable Authenticating User with Google Apps Credentials

when enabled, users can login using Google Apps credentials.

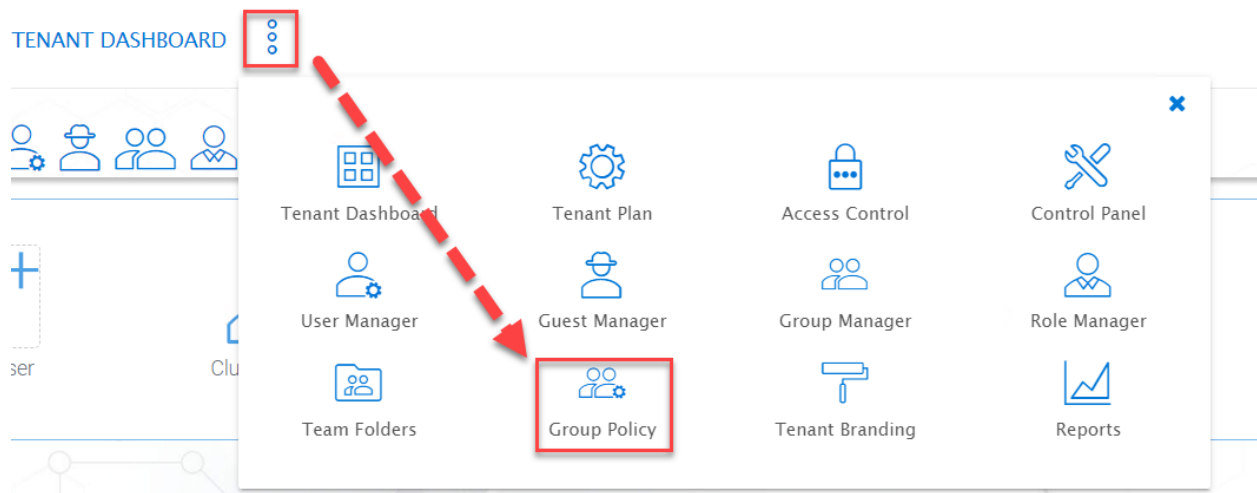


Fig. 63: GROUP POLICY SETTINGS

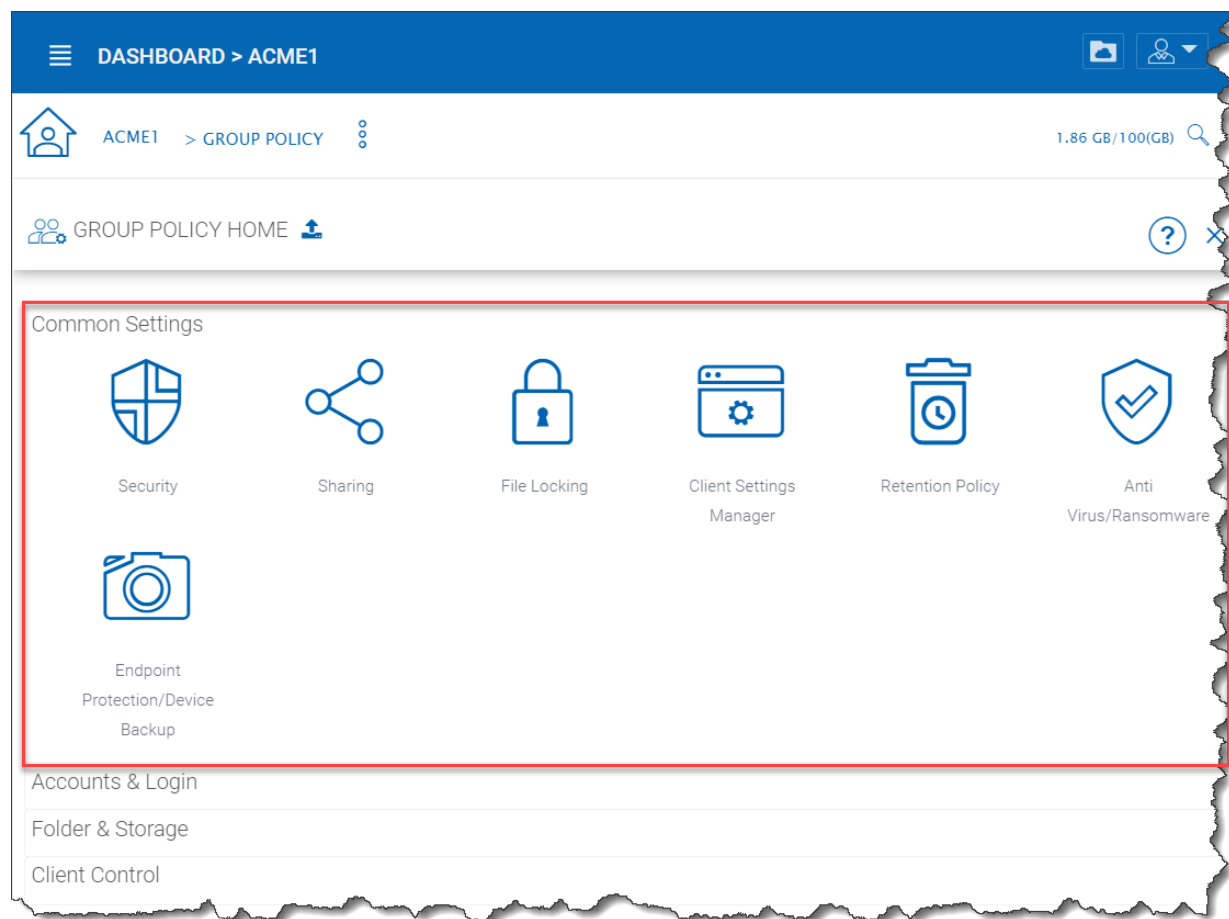






Fig. 64: GROUP POLICY COMMON SETTINGS



 ACME > GROUP POLICY 

 GROUP POLICY HOME  > SECURITY

Allow Cluster Admin to manage my tenant	<input type="checkbox"/>
Notify user when email is changed	<input checked="" type="checkbox"/>
Disable remote assistance	<input type="checkbox"/>
Enable authenticating user with Google Apps credential <small>When this setting is set, user can login to the system with Google Apps credential.</small>	<input type="checkbox"/>
When delegate admin login via server agent, impersonate as tenant admin	<input type="checkbox"/>
File upload and download must go through worker node <small>When this option is enabled, uploading files and downloading files will always go through worker node.</small>	<input checked="" type="checkbox"/>

Fig. 65: GROUP POLICY SETTINGS

### **When delegate admin login via server agent, impersonate as tenant admin**

Server agents typically need to sync to the default tenant administrator. It is recommended when a delegate administrator setup a server agent, it needs to impersonate the default tenant administrator.

### **File upload and download must go through worker node**

(This setting may only be available from cluster administrator side)

For Amazon S3 type of cloud storage/object storage, it is recommended NOT to force file upload and download going through worker nodes, because Amazon S3 is good for offload the upload/download between the access clients and the backend Amazon S3 storage. However, for OpenStack Swift storage, depending on how it is set up, you may want to turn this on to force File Upload/Download going through worker node for security reasons.

This setting may be checked by default. However, based on your configuration, it may not need to be checked.

For example, if you are using file server network share as the storage location, the upload and download has to go through worker node anyway, so there is no need to check this checkbox.

There may be some situations that this setting must be checked. For example, you may be using native object storage such as Amazon S3 for storage. However, your company policy may disable direct access to Amazon S3. So in this case, you will have to route traffic through the worker node.

## **4.10.1.2 Sharing**

Tenant Manager > [Tenant] > Group Policy > Common Settings > Sharing

### **Users must login to access the content in ‘Files shared with me’ folder**

When sharing files and folders with users, you can force the sharing to create guest accounts for users that are not already in the system. It is more secure when asking the receiver of the share to sign in to receive shared items. This disables anonymous sharing.

If this setting is not enabled, users can share files and folders to an outside email address without requiring outside users to create a guest user account.

### **Disable user’s ability to share home directory content externally**

This feature disables the ability for a regular user to share home directory contents for security reasons.

### **Enable Internal Public Share URL**

If you have an internal public share you can use this setting to enable it.

When this is enabled, it will use the Internal URL property to generate a web link for shared file/folder.

### **Disable Public Link**

This will disable the public web link feature in the sharing dialog.

### **Show guest user creation option**

When enabled this shows the guest user creation option which you will see when ‘Sharing’ a file or folder by email. This is how you can provide full edit capability to a guest user, as they must be logged in to modify a file or folder in the CentreStack.

### **Enable distribution group detection in file/folder sharing’s user interface**

With active directory integration, sometimes you want to share files and folders with a distribution group. This feature allows detection of distribution group and expands the group so the sharing will be done with the users in the group, instead of using the group as a single user.

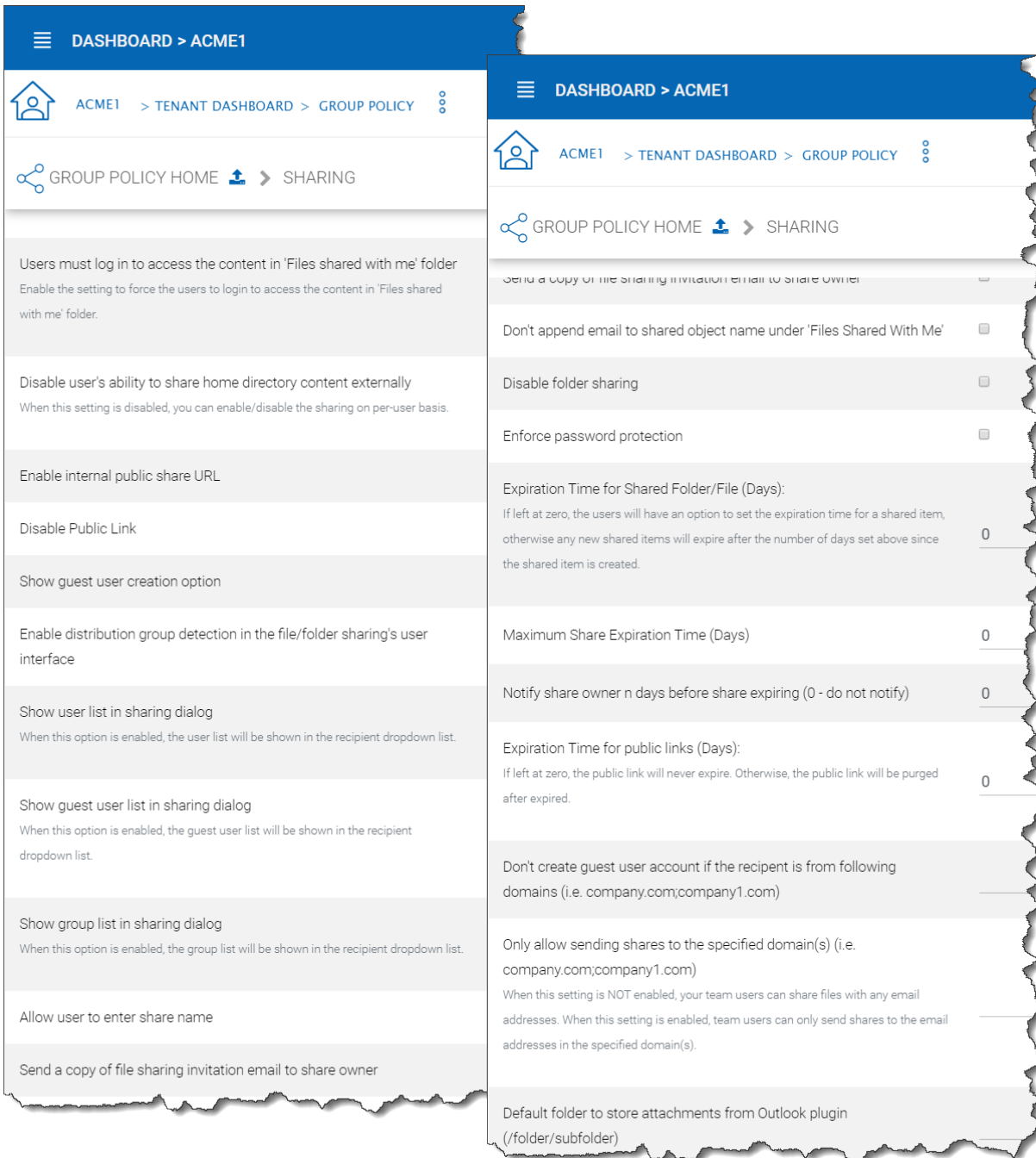


Fig. 66: GROUP POLICY SHARING SETTINGS

#### **Show user list in sharing dialog**

When enabled, the user list will be displayed in the recipient's dropdown list.

#### **Show guest user list in sharing dialog**

When this option is enabled, the guest user list will be shown in the recipient dropdown list.

#### **Show group list in sharing dialog**

When this option is enabled, the group list will be shown in the recipient dropdown list.

#### **Allow user enter share name**

By default the file name or folder name is used for the share name. However, if user has many same name folders or files. Sharing them out sometimes many not know which is which. This setting allows user to change share name. For example, when sharing out a "Documents" folder, it can be named "Documents in top level folder".

#### **Send a copy of file sharing invitation email to share owner**

When sending the file-sharing email, sending a copy (CC) to the owner of the share (usually the sender of the email)

#### **Don't append email to shared object name under 'Files Shared With Me'**

When enabled, emails won't show next to object names in 'Files Shared With Me' view.

#### **Disable folder sharing**

When enabled users will not be able to share folders.

#### **Enforce password protection**

When enabled all users (including guest users) will be required to use complex password protection.

#### **Expiration Time for Shared Folder/File (Days):**

When set, during the file/folder sharing wizard, the expiration time dropdown selection will not be shown, it will be pre-set to expiration set in here.

#### **Maximum Share Expiration Time (Days):**

When set, this creates an upper limit to the time a share will be available, which forces all shares to expire when this limit is reached.

#### **Notify share owner n days before share expiring (0 - do not notify)**

Notify the sender (owner) of the share before share expiration.

#### **Expiration Time for public links (Days):**

If left as zero, public link will never expires, otherwise the public link will be purged after expired.

#### **Don't create a guest user account if the recipient is from the following domains (i.e. company.com;company1.com)**

Blacklist guest emails from the domains listed here. Do not allow sharing to these domains.

#### **Only allow sending shares to the specified domain**

You can further limit the sharing to some domain instead of random email. For example, if your primary collaboration target is with ACME corporation and you can limit the sharing to your domain and also ACME domain.

#### **Only allow sending shares to the specified domain(s) (i.e. company.com;company1.com)**

When it is set, the external sharing can only be shared to the white-list of email domains (which represent external partners, clients and etc)

#### Default folder to store attachments from Outlook plugin (/folder/subfolder)

Allows you to designate where Outlook attachments are saved.

### 4.10.1.3 File Locking

Tenant Manager > [Tenant] > Group Policy > Common Settings > File Locking File Locking can be accessed from the following location in the Tenant Dashboard's Group Policy section.

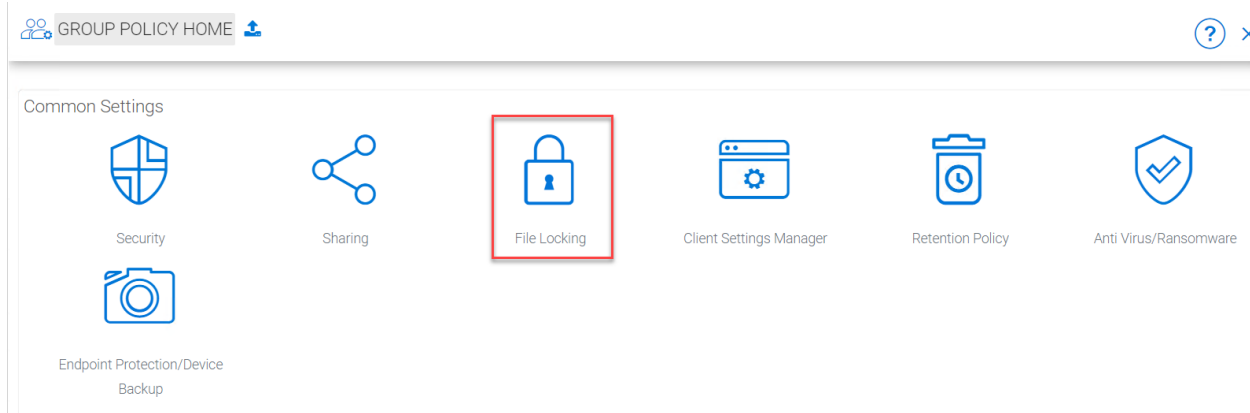


Fig. 67: GROUP POLICY FILE LOCKING

After you click the “File Locking” icon, here is the screen for the file locking settings details.

Settings under file locking applies to all clients which include desktop clients as well as server agent clients.

#### Enable Distributed locking when accessing files

In the Cluster Server, there are two ways to lock files, one is manually by right-clicking on a file and select “Check out”. The other way is automatic based on certain binary executables. For example, you can see Microsoft Office executable files like winword.exe and so on.

#### Lock file exclusively

When enabled, the locked file will be locked exclusively. When disabled, the other user who is trying to open the locked file will be notified about the lock status, but will still be able to open the file.

#### Automatically open file in read only mode when file is locked and “Lock file exclusively” is not checked.

When this setting is enabled (default), a second attempt to open a locked file will result in the file opening in read-only mode. If “Lock file exclusively” is checked, then second user will not be able to open a locked file.

#### Delay sync until file is unlocked

It is recommended to check this setting. Most users have the habit to save files in the middle of editing. You don’t want these edits to go every time to the cloud for these intermediate saves. You want to do a save to the cloud at the end like a grand finale. So you can delay sync until the file is unlocked.

#### Unlock file after file is uploaded

After the file is uploaded, unlock the file.

#### Lock file natively on network shares

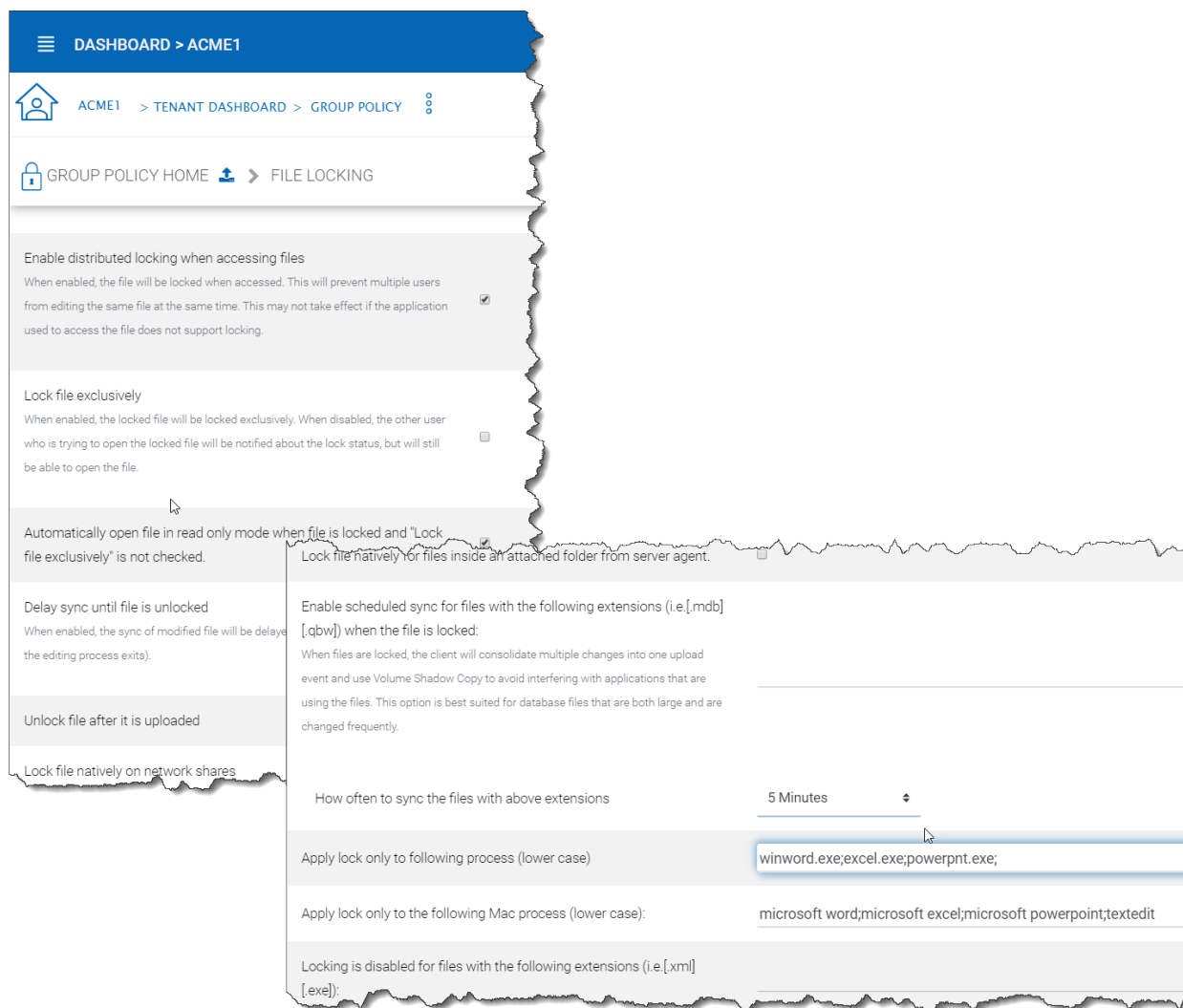


Fig. 68: FILE LOCKING SETTINGS

When a file is locked in the CentreStack, if the file is from an attached network share, the CentreStack lock will be converted into a native file system lock on the network share. This provides locking interoperability between the CentreStack and the underlying file system network share.

#### Enable scheduled sync for files with following extensions (i.e.[.mdb][.qbw]) when the file is locked”

When files are locked, the client will consolidate multiple changes into one upload event and use Volume Shadow Copy to avoid interfering with applications that are using the files. Typically this applies to database files that are constantly in use and constantly actively writing (commit) to the database file.

#### How often to sync the files with above extensions

This setting allows you to control the interval of synchronization that takes place on the above file extensions.

#### Apply lock only to the following processes (Lower case)

You can specify the processes here for which locking should be applied. By default, locking is enabled for Microsoft Word, Excel, and PowerPoint.

#### Apply lock only to the following MAC processes”(Lower case)

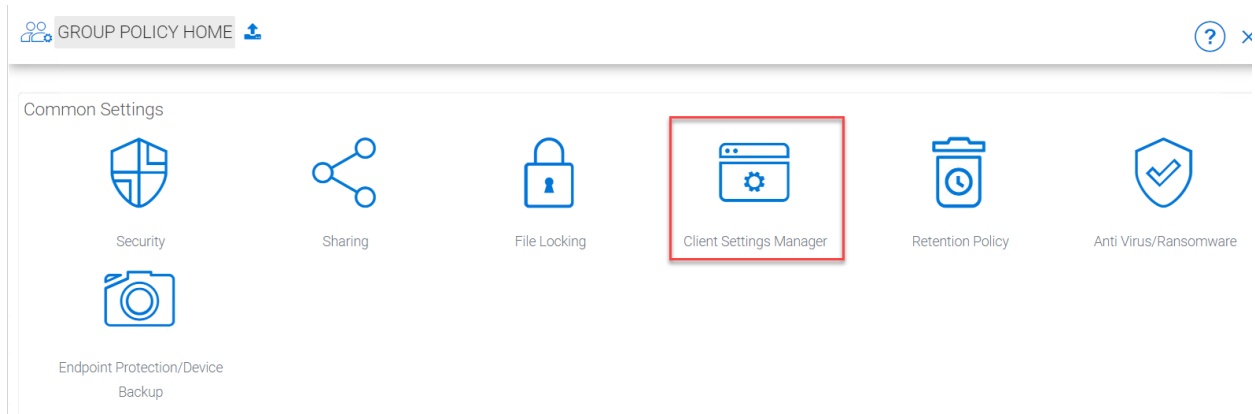
You can specify the processes here for which locking should be applied. By default, locking is enabled for Microsoft Word, Excel, PowerPoint and MAC text editor.

#### Locking is disabled for files with the following extensions (i.e.[.xml][.exe])

You can use this setting to specify which file types will be ignored with regard to the file-locking feature.

### 4.10.1.4 Client Settings Manager

Tenant Manager > [Tenant] > Group Policy > Common Settings > Client Setting Manager



#### 4.10.1.4.1 Sync Throttle

##### Enable Throttle Sync

When disabled (default) all Sync Throttle settings in this section are disabled. Must be enabled to activate the following settings.

##### Sync Throttled Upload Bandwidth (KB/s, 0-Unlimited)

This setting controls the upload bandwidth from the client machine.

##### Sync Throttled Download Bandwidth (KB/s, 0-Unlimited)

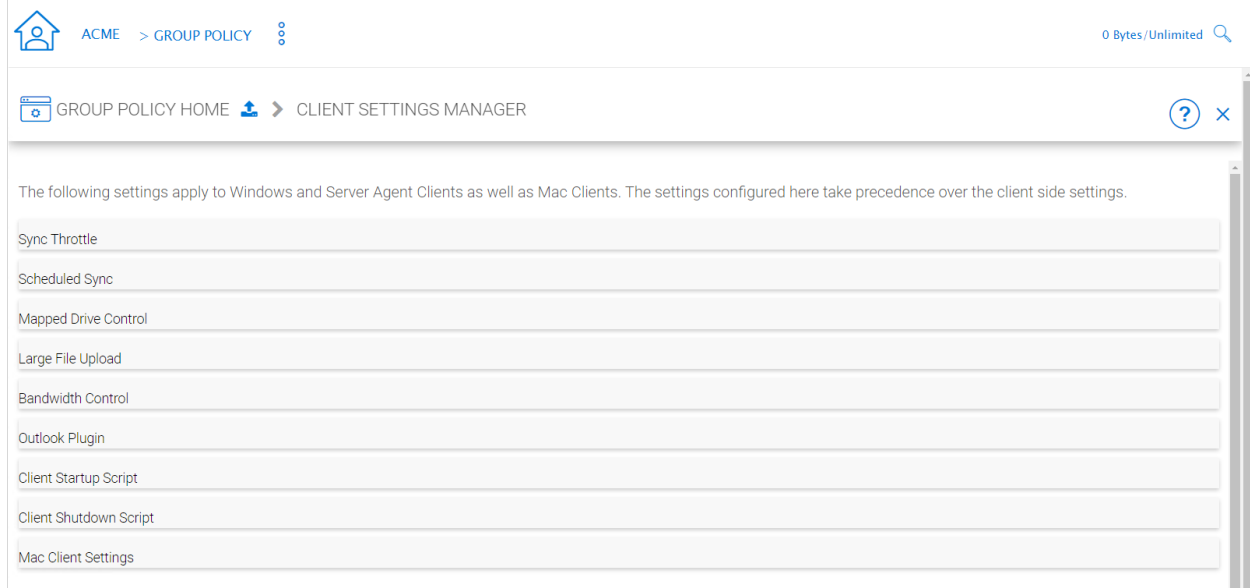


Fig. 69: GROUP POLICY CLIENT SETTING MANAGER

Sync Throttle	
Enable Throttle Sync When enabled, the following settings will apply.	<input type="checkbox"/>
Sync Throttled Upload Bandwidth (KB/s, 0-Unlimited):	0
Sync Throttled Download Bandwidth (KB/s, 0-Unlimited):	0
Full Speed Sync Stop Hour (default 7:00):	7
Full Speed Sync Start Hour (default 20:00)	20

Fig. 70: SYNC THROTTLE SETTINGS



This setting controls the download bandwidth from the client machine.

#### Full Speed Sync Stop Hour (default 7:00)

Full speed sync means multiple thread concurrent upload or download. This is typically good for after hour activity. We recommend default setting stop at 7am so when people return to work, the full speed sync stops so to give back more bandwidth to users who may be using the Internet for other purposes.

#### Full Speed Sync Start Hour (default 20:00)

Similar to the above setting, we recommend start full speed sync after working hours.

### 4.10.1.4.2 Scheduled Sync

#### Enable Scheduled Sync

On the client side, in addition to a mapped drive (or a mac mounted volume), there is also functionality about folder synchronization. This setting can control when to sync. For example, if the business has limited bandwidth to the Internet, avoid doing synchronization during the working hours can save bandwidth.



Fig. 71: SCHEDULED SYNC SETTINGS

### 4.10.1.4.3 Mapped Drive Control

#### Hide Large File Download Tracker (popup progress window on the bottom-right when downloading large files)

This is usually good for usability but people may find it annoying if download is popping up a download progress dialog at the lower right corner.

#### Always Allow Picture Preview

Windows Explorer may want to download pictures in the background to generate thumbnails. This consumes bandwidth and may slow system down until all the preview thumbnails are generated. By default the client program disables the preview. However you can re-enable it.

#### Always Allow PDF Preview

Windows Explorer may want to download PDFs in the background to generate thumbnails. This consumes bandwidth and may slow system down until all the preview thumbnails are generated. By default the client program disables the preview. However you can re-enable it.

Mapped Drive Control	
Hide Large File Download Tracker (popup progress window on the bottom-right when downloading large files)	<input type="checkbox"/>
Always Allow Picture Preview	<input type="checkbox"/>
Always Allow PDF Preview	<input type="checkbox"/>
Allow shortcuts	<input type="checkbox"/>
When starting the client, open the mounted drive automatically	<input type="checkbox"/>
In OneDrive, only show files	
Disable "Check Out"	<input type="checkbox"/>
Encrypt Local Cache	<input type="checkbox"/>
Disable AutoCad Optimization	<input type="checkbox"/>

Fig. 72: MAPPED DRIVE CONTROL SETTINGS

**Allow shortcuts**

Allow shortcuts (.lnk) files

**When starting the client, open the mounted drive automatically**

Enabling this opens the mounted drive in Windows Explorer when the client starts.

**Do not show file change notifications**

This is another feature that shows file change notification at the lower right-hand corner of the Windows desktop. People may find it annoying if the change notification comes in quite often.

**Do not show file in-place editing/preview disabled notifications**

This feature also shows file change notifications at the lower right-hand corner of the Windows desktop. People may find it annoying if the change notification comes in quite often.

**Enable Inplace Open Zip File**

Windows Explorer has a zip built-in extension that can open a zip file when double-clicked on. It may be good for the local drive but for cloud drive, that means the zip file is unzipped and re-upload back into the cloud. By default client application disables opening zip files directly in the cloud drive.

**Enable Single Sign On with login windows user identity**

Enable Single Sign-On with Login Windows User Identity - For a Windows client agent running on a Windows Desktop machine, the login windows user's identity will be used for single sign-on to the CentreStack account.

**Max Size of Zip File Allowed to Open In-place (MB)**

Limits the size of a Zip File that can be opened in-place.

**Max Size of File Allowed to Generate Thumbnail (MB)**

Limits the size of Files that can be used in the generation of thumbnails.

**Cloud Drive Label**

What do you want to call your windows client drive.

**Drive Letter**

What do you want to give the drive letter to the client application.

**Cache Size Limit (MB)**

The Windows client maintains a client-side cache of this size (0 - unlimited)

**Minimal free disk space (GB)**

This setting is used to establish a minimum amount of disk space used for the windows client drive.

**Purge logging db n days old (0 - don't purge)**

This limits how many days of logging are kept in the Windows client cache.

**Mount Drive in global space (Windows Client Only)**

A drive mounted in the global space will not be subject to UAC (User Account Control) limitations, such as when legacy applications are required to run with administrative privilege and cannot see the drive guarded by the UAC. On the other hand, drives that are mounted in the global space are visible to any other users who log in on the same Windows machine at the same time.

**In offline mode, only show files that are cached and available locally**

Typically there will be place-holder files and representative icons created for all of the files in the client drive. If this setting is enabled, only locally stored files will be shown.

**Disable “Check Out”**

Turn off the “Check Out” feature and remove it from the right-click context menu.

**Encrypt Local Cache**

Once enabled, when a file is downloaded to cache, it is encrypted in place. When an authorized user then accesses the file from the (M:) Mapped Cloud Drive, CentreStack automatically decrypts it on the fly and then returns it to the user.

**Disable AutoCad Optimization**

By default, there is an AutoCAD optimization that delays the synchronization of the updated .dwg file and schedules it to sync upwards to the cloud at a later time. Use this setting to disable this AutoCad optimization and make saving AutoCAD .dwg files act the same as saving other regular files and lets .dwg file behavior follow other policy settings.

**4.10.1.4.4 Large File Upload****Enable chunk uploading when file size larger than (MB)**

Uploading a single large file can be disrupted by an Internet glitch. This setting breaks large files into smaller chunks to increase the success rate.

**Chunk file in the unit of (MB)**

Works with the above setting to establish what size the chunks will be in as they are transferred.

**Use Volume Shadow Copy to Upload Files being Opened**

Large File Upload	
Enable chunk uploading when file size larger than (MB):	<input type="text" value="50"/>
Chunk file in the unit of (MB):	<input type="text" value="50"/>
Use Volume Shadow Copy to Upload Files being Opened	<input type="checkbox"/>

Fig. 73: LARGE FILE UPLOAD SETTINGS

There is pro and con of using this flag. When file is open by other application, the file usually is locked and can't be uploaded until the file is closed. However using volume shadow copy can still upload the file. The down side is when the volume shadow copy happens, the file is not known to be in a consistent state.

#### 4.10.1.4.5 Endpoint Protection

Endpoint Protection	
Backup "My Documents" folder	<input type="checkbox"/>
Backup to location (Leave empty for default location. ) myroot/{email} or {samAccountName} or {upn}/My Documents	<input type="text"/>
Backup "My Pictures" folder	<input type="checkbox"/>
Backup to location (Leave empty for default location. ) myroot/{email} or {samAccountName} or {upn}/My Pictures	<input type="text"/>

Fig. 74: ENDPOINT PROTECTION SETTINGS

##### Backup "My Documents" folder

Forces files in "My Documents" to be backed-up to the cloud.

##### Backup to location (Leave empty for default location. e.g., myroot/{email} or {samAccountName} or {upn}/My Pictures)

Allows you to set an alternative storage location for the above setting.

##### Backup "My Pictures" folder

Forces files in "My Pictures" to be backed-up to the cloud.

##### Backup to location (Leave empty for default location. e.g., myroot/{email} or {samAccountName} or {upn}/My Pictures)

Allows you to set an alternative storage location for the above setting.

#### 4.10.1.4.6 Bandwidth Control

Bandwidth Control:	
Download Bandwidth Limit (KB/s, 0-Unlimited):	0
Upload Bandwidth Limit (KB/s, 0-Unlimited):	0
Number of File Transfer Threads:	5

Fig. 75: BANDWIDTH CONTROL SETTINGS

##### Download Bandwidth Limit (KB/s, 0 - Unlimited)

This is download bandwidth control.

##### Upload Bandwidth Limit (KB/s, 0 - Unlimited)

This is upload bandwidth control.

##### Number of File Transfer Threads

This is the number of concurrent upload/download allowed (default is 5).

#### 4.10.1.4.7 Outlook Plugin

Outlook Plugin	
Prompt for conversion only when the file is larger than n KB (0 - unlimited)	0
Default folder to store attachments from Outlook plugin (/folder/subfolder)	
Link expiration time	<div>Never</div> <div>Never</div> <div>One day</div> <div>One week</div> <div>One month</div> <div>Six months</div> <div>One year</div>
Client Startup Script	
Client Shutdown Script	
Mac Client Settings	

Fig. 76: OUTLOOK PLUGIN SETTINGS

##### Prompt conversion only when file is larger than n KB (0 - unlimited)

For smaller files, it may be as well to just use the native outlook attachment.

**Default folder to store attachments from Outlook plugin (/folder/subfolder)**

Allows you to set a storage location for the above setting.

**Link expiration time**

Allows Outlook share link to last indefinitely or expire in a specified timeframe (e.g., never, one day, one week, one month, six months, one year).

#### 4.10.1.4.8 Client Startup Script

After the Windows client is completely started and finished loading, a command line script can be run. You can be upload that script here. For example, a script to map an additional drive letter to a specific folder inside the cloud drive.

#### 4.10.1.4.9 Client Shutdown Script

Right before the Windows client is completely shutdown and finished running, a command line script can be run. You can upload that script here. For example, a script to clean up any reference to folders and files inside the cloud drive.

#### 4.10.1.4.10 Mac Client Settings

**Do not show Mac Client sync status pop up dialog**

This is usually good for usability but people may find it annoying if the file status is popping up a progress dialog at the lower right corner.

**Start Mac Client automatically**

(Enabled by default.) If this is disabled, the Mac Client must be started manually.

#### 4.10.1.5 Retention Policy

Tenant Manager > [Tenant] > Group Policy > Common Settings > Retention Policy

The cloud monitoring service on the Cluster Server will be responsible for the retention policy. The settings of the retention policy are described below.

**Keep last n version(s) of files in versioned folder**

This setting lets you decide how many versions of files to keep in the version folder. (0 - let system decide, also apply to “attached local folder”)


**Only purge versioned files that are more than n day(s) old**



This is a security feature. For example, there is a virus modified the same file many times so it created many versions causing good old versions to be scheduled for deletion. However, with this set, the good old versions will be kept for at least the amount of days so give enough time to recover. (0 - purge old versions once they exceed the version limit, regardless of the version lifespan)



**Keep deleted files in versioned folder and/or Trash Can for n day(s)**

When a file is deleted in the version folder, it is not actually deleted. It will be kept for several days defined here. The same policy also apply to

**Keep file change log for n day(s)**


**DASHBOARD > ACME1**


ACME1 > TENANT DASHBOARD > GROUP POLICY



GROUP POLICY HOME  > RETENTION POLICY

Keep last n version(s) of files in versioned folder. 0 - let system decide, also apply to 'attached local folder'	0
Only purge versioned files that are more than n day(s) old: 0 - Purge old versions once they exceed the version limit, regardless of the version lifespan	0
Purge previous versions that are more than n day(s) old: Purge old versions that meets the criteria, regardless if it exceeds version limit. 0 - do not purge based on file time	0
Keep deleted files in versioned folder and/or Trash Can for n day(s). 0 - let system decides	90
Keep file change log for n day(s). 0 - don't purge file change log	15
Keep audit trace for n day(s). 0 - don't purge audit trace	0
Hide purge option from web file browser (not applicable to tenant administrator)	<input checked="" type="checkbox"/>
Don't send email notifications when purging deleted content	<input type="checkbox"/>
Include deleted but not yet purged items in storage quota	<input type="checkbox"/>

file change log is the biggest database table and could be growing without trimming. You can decide how often you want to trim the table.

---

**Note:** There is also a cluster setting about the file change log length. The cluster setting overrides the per-tenant setting.

---

#### **Keep audit trace for n day(s)**

audit trace log is stored in a local device directory and keeps a record of high-level activity from a device (e.g., windows client, server agent). This setting limits the number of days that are stored in the local database file.

#### **Hide purge option from web file browser (not applicable to tenant administrator)**

Do not show the purge window to users when deleting content.

#### **Don't send email notifications when purging deleted content**

There are times when an admin would not want to send or see delete email notifications for purged contents.

#### **Include deleted but not yet purged items in storage quota**

Allows you to decide if you want to include not visible (purged) files in the storage quota that is used.

### **4.10.1.6 Anti Virus**

Tenant Manager > [Tenant] > Group Policy > Common Settings > Anti Virus

#### **Only allow the following processes to update files (empty: allow all, separate using semicolon (;), i.e. win-word.exe;excel.exe)**

This is a white list of applications that are allowed to update files. The applications that are not in the list will not be able to upload files.

#### **The following executables will not be allowed to open files directly from the cloud drive (i.e. qbw32.exe;excel.exe)**

This is the opposite of the above policy. The applications in this list will be denied.

#### **Disable a device if the device changes more than n files in 10 minutes**

When users are using the cloud drive in a normal way. Human speed will not be able to generate large amount of file upload.

#### **Ignore the following processes when applying the above policy**

This is a white list of files that will not be monitored for the activity described above. (e.g., qbw32.exe; excel.exe)

#### **Disable uploading of files whose named contain the following text patterns**

When file name text contains the following strings, the files will not be uploaded. (e.g., badfile1; badfile2)


#### **Disable uploading of files whose names start with the following strings**



When the starting text of files contain these strings, the files will not be uploaded. (e.g., bad1; bad2)



#### **Disable uploading of files whose names end with the following strings**

When the ending text of files contain these strings, the files will not be uploaded. (e.g., bad1; bad2)



 DASHBOARD > ACME1

 ACME1 > TENANT DASHBOARD > GROUP POLICY 

 GROUP POLICY HOME  > ANTI VIRUS/RANSOMWARE

Only allow the following processes to update files (empty: allow all, separate using semicolon (;), i.e. winword.exe;excel.exe)

The following executables will not be allowed to open files directly from the cloud drive (i.e. qbw32.exe;excel.exe)

Disable a device if the device changes more than n files in 10 minutes

Ignore the following processes when applying the above policy (i.e. qbw32.exe; excel.exe)

Disable uploading of files whose named contain the following text patterns  
i.e. badfile1;badfile2

Disable uploading of files whose names start with the following strings  
i.e. bad1;bad2

Disable uploading of files whose names end with the following strings  
i.e. bad1;bad2

Fig. 78: ANTI VIRUS SETTINGS

## 4.10.2 Account & Login

Tenant Manager > [Tenant] > Group Policy > Account & Login

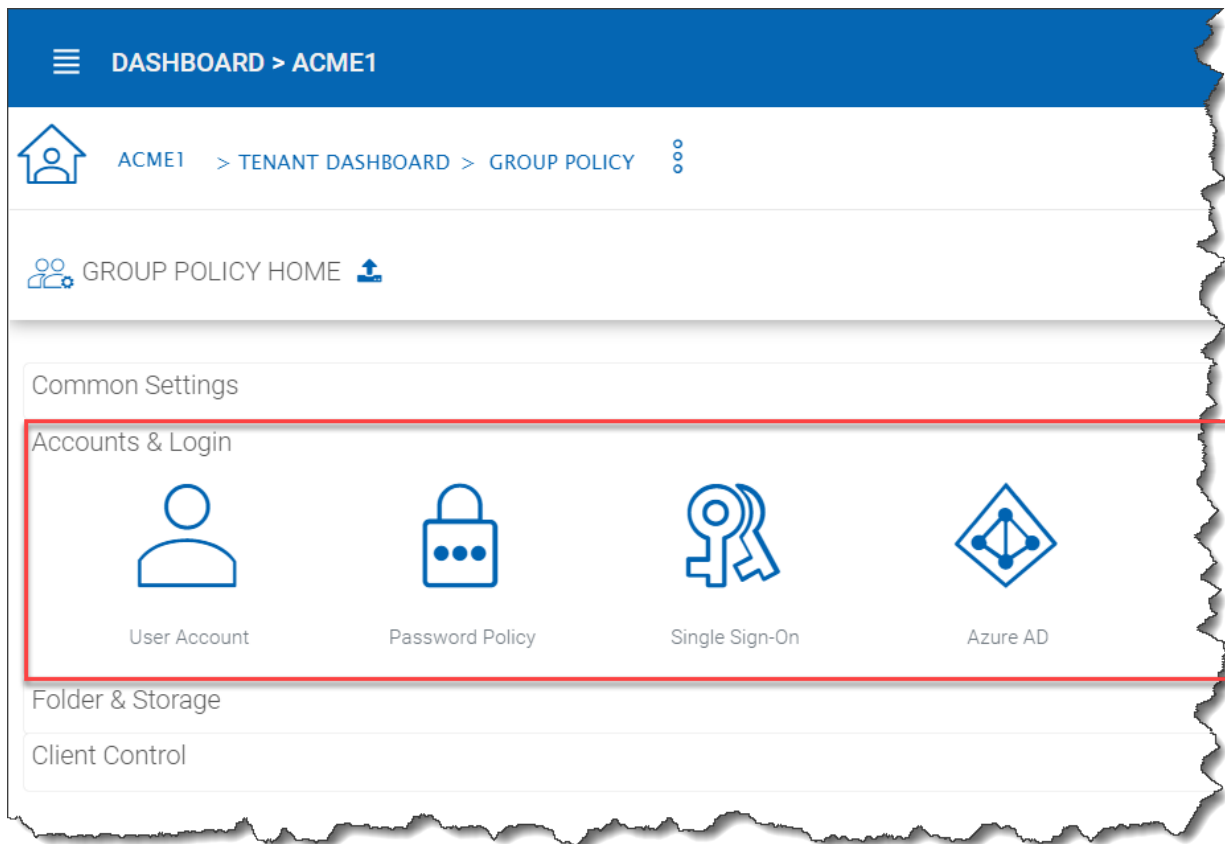


Fig. 79: ACCOUNT AND LOGIN SETTINGS

### 4.10.2.1 User Account Settings

Tenant Manager > [Tenant] > Group Policy > Account & Login > User Account

This is how “User Account” settings looks when “2-Step Verification is not turned on by the Cluster Manager.

#### 4.10.2.1.1 Guest User

##### Allow creation of guest user

When enabled (default), you will allow creating of guest user when team user share files or folders with external users. When disabled, the file/folder sharing is limited to regular users only or anonymous users only.

#### 4.10.2.1.2 Account Info

##### Allow user to edit account info

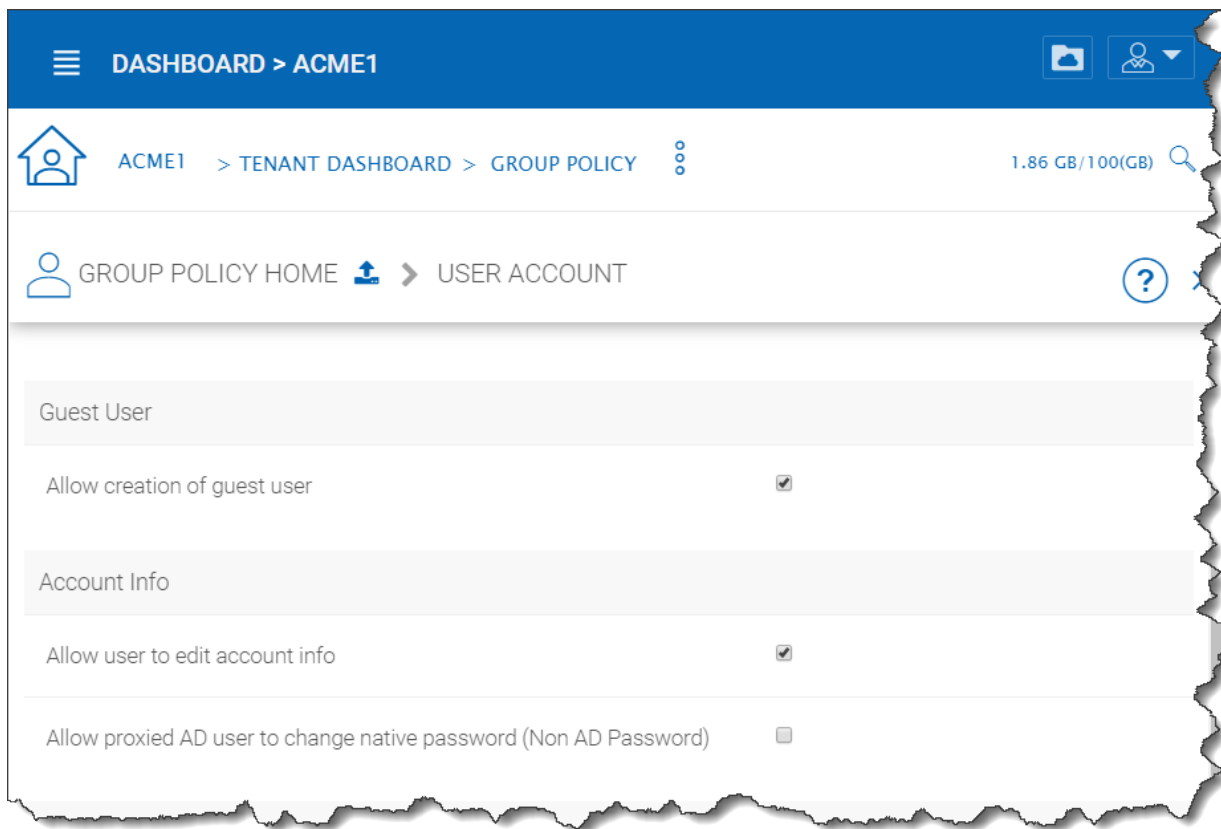


Fig. 80: GROUP POLICY USER ACCOUNT SETTINGS

When enabled (default), this setting allows users to edit their account information.

#### Allow proxied AD user to change native password (Non AD Password)

Proxied AD user refers to Active Directory users from remote server agent machine. Normally the initial password and changed password are synchronized from the server agent side periodically so the end user is always using the same Active Directory credentials to log in. However, there may be cases when you want the user to break away from the old Active Directory and setup credential natively on CentreStack.

#### 4.10.2.1.3 2-Step Verification

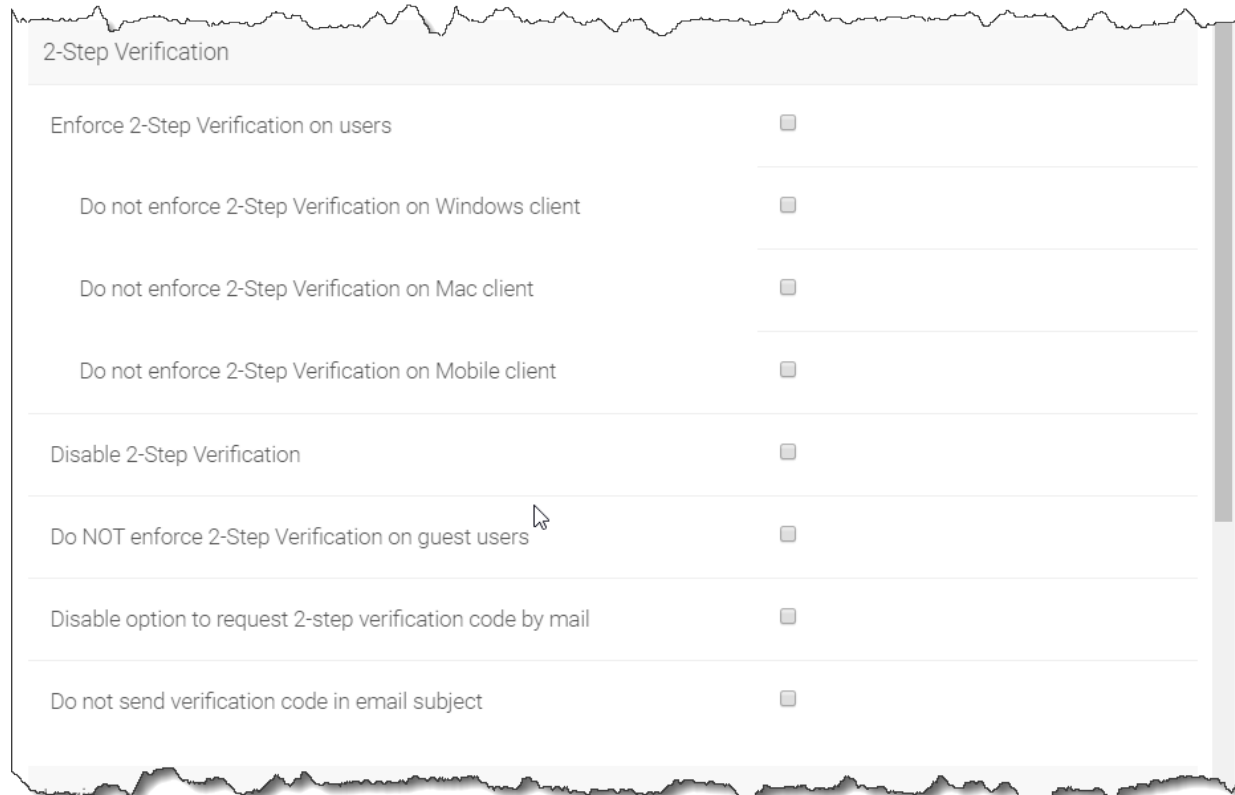


Fig. 81: GROUP POLICY USER ACCOUNT SETTINGS (Cont.)

#### Enforce 2-Step Verification on users

Enforce 2-step verification will force the users to setup 2-step verification via Google Authenticator, Microsoft Authenticator, Amazon MFA or any app that supports the same 2-step verification algorithm.

#### Do not enforce 2-Step Verification on Windows client

Tuning on windows client whether to enforce 2-step verification

#### Do not enforce 2-Step Verification on Mac client

Tuning on mac client whether to enforce 2-step verification

#### Do not enforce 2-Step Verification on Mobile client

Tuning on windows client whether to enforce 2-step verification

**Disable 2-Step Verification**

Disable 2-step verification. One possible use case is when 2-step verification is no longer needed or 2-step verification needs to be disabled temporarily.

**Do NOT enforce 2-Step Verification on guest users**

Guest users may have a set of credentials to login to receive shared files and folders. This policy define whether to enforce 2-step verification for them.

**Disable option to request 2-step verification code by email**

If user doesn't have the 2-step verification app on the mobile device, the alternative is to send the code to user's email.

**Do not send verification code in email subject**

If the code has to be sent over email, don't send the code in the subject line.

**4.10.2.1.4 Login Control**

Login Control		
Account Lockout Threshold (0 - never lockout):	0	The Account lockout threshold sets the number of invalid logon attempts that are allowed before an account is locked out.
Enforce progressively longer waiting times after invalid logon attempts	<input type="checkbox"/>	
Send email notification when logging in from a new location/device	<input type="checkbox"/>	
Native Client Token Timeout (days, 0 - never timeout):	15	
Web Browser Session Timeout (minutes, 0 - never timeout):	120	
Max Device Count (Concurrent Device Count) for Each User (0-Unlimited):	120	

Fig. 82: GROUP POLICY USER ACCOUNT SETTINGS (Cont.)

**Account Lockout Threshold (0 - never lockout)**

You can specify the Account lockout threshold limit here. The limit specified will be the number of invalid logon attempts that will be allowed before an account is locked out. Default is 0 (never lockout).

**Enforce progressively longer waiting times after invalid logon attempts**

Disabled by default. Under login control, you can also enforce progressively longer waiting times after invalid logon attempts.

#### **Send email notification when logging in from a new location/device**

Disabled by default. Another setting under login control is the 'Send email notification when login from new location/device'. This setting will send an email to users whenever a different device or location is used to login.

#### **Native Client Token Timeout (days, 0 - never timeout)**

Determines if and when the Native Client Token will timeout, in days. Default is 15 days.

#### **Web Browser Session Timeout (minutes, 0 - never timeout)**

Determines if and when the Web Browser Session timeout, in minutes, will occur. Default is 120 minutes.

### **4.10.2.2 Password Policy**

Tenant Manager > [Tenant] > Group Policy > Account & Login > Password Policy

Here you can adjust your password policy settings.

#### **Enforce password policy for non-AD users**

By default, non-AD users are not enforced to use this policy when setting their password. Enable this to enforce the following rules.

#### **Minimum password length**

Require the password to contain a certain number of characters as a minimum. Default is 8.

#### **Users must change password every n days (0 - never)**

Force users to change their passwords every so many days. Default is 0 (never).

#### **Must contain upper case characters**

Enforce the use of upper-case characters in the password. Default is enabled.

#### **Must contain lower case characters**

Enforce the use of lower-case characters in the password. Default is enabled.

#### **Must contain base10 digits (0-9)**

Enforce the use of base10 digits in the password. Default is enabled.

#### **Must contain non-alphanumeric characters: (e.g., ~ ! @ # \$ % ^ &)**

Enforce the use of special non-alphanumeric characters when creating a password. Default is enabled.

### **4.10.2.3 Single Sign-On**

Tenant Manager > [Tenant] > Group Policy > Account & Login > Single Sign-On

Single Sign on via SAML is a per-tenant setting.

Single Sign-On is available using SAML authentication.

When it comes to Single Sign-On support via SAML, there are always two parties.

- One is the IdP (the identity provider)
- and the other is SP (service provider)

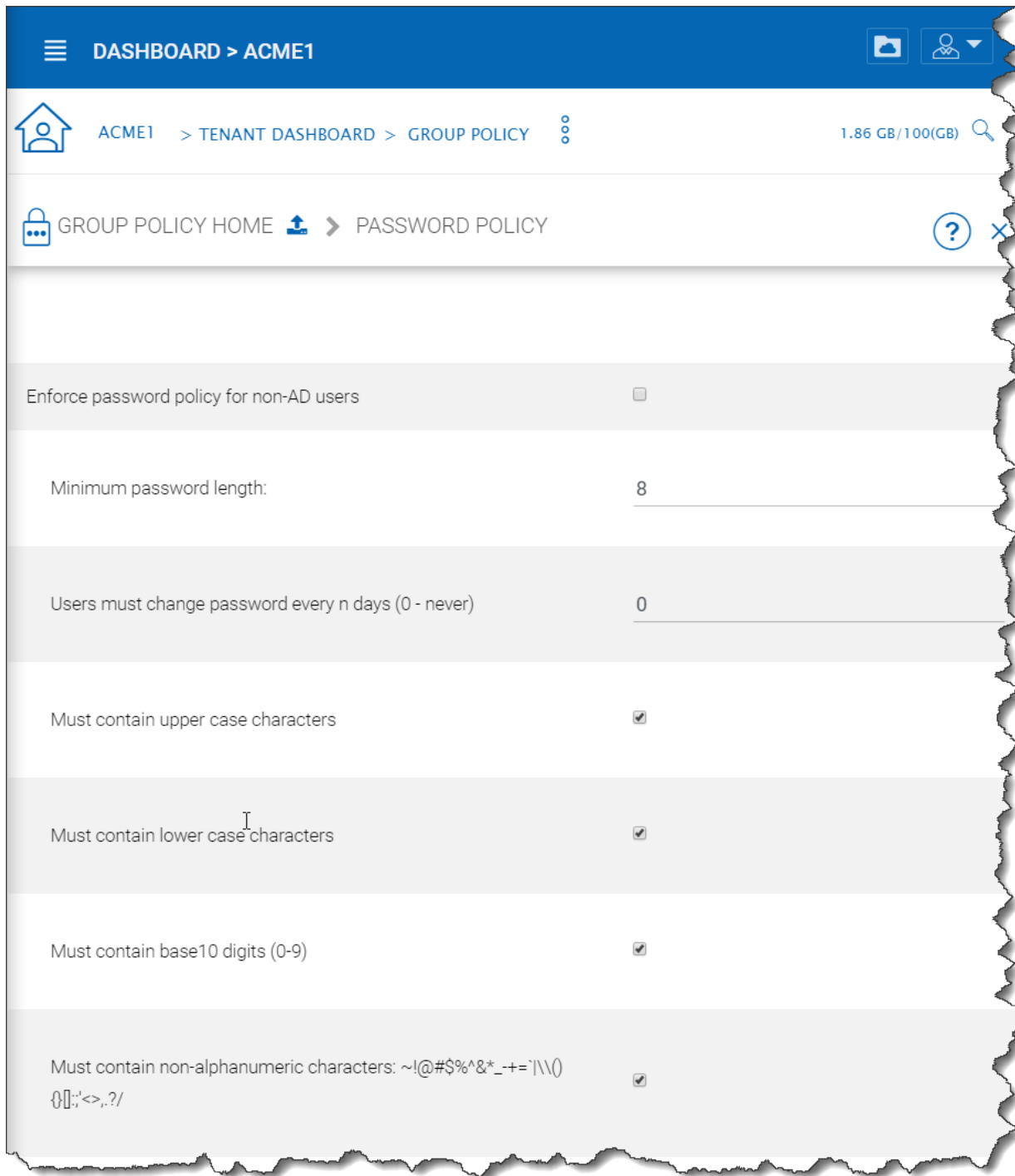


Fig. 83: PASSWORD POLICY SETTINGS

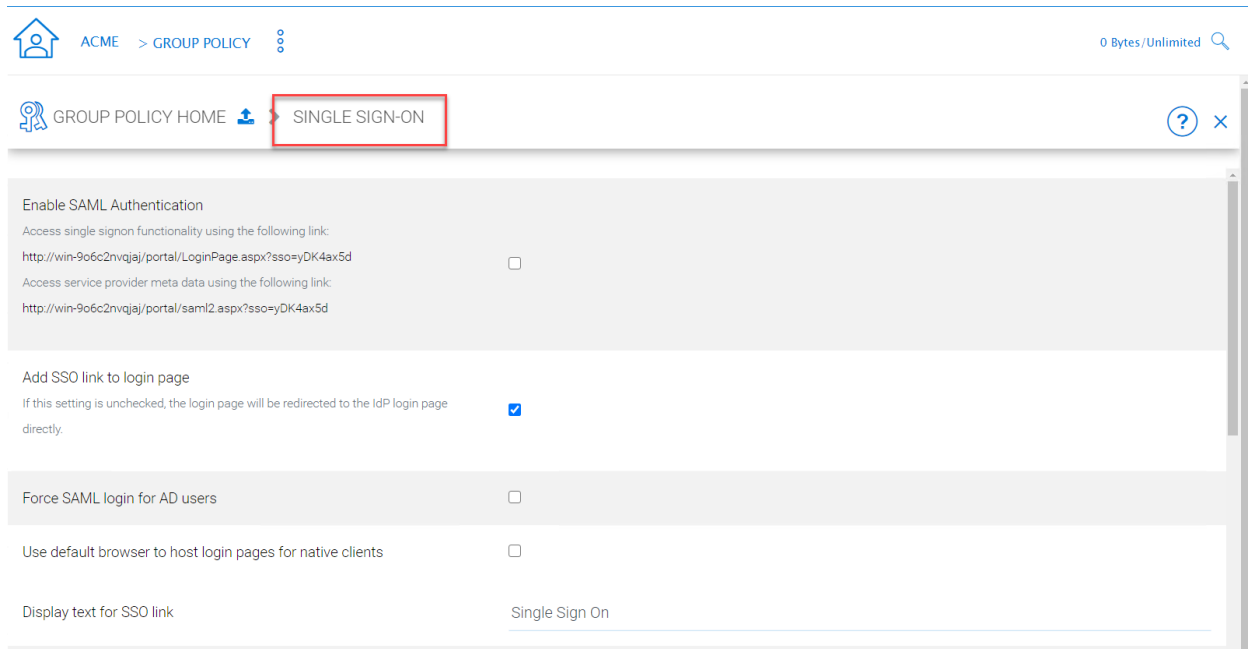


Fig. 84: ACCESSING TENANT GROUP POLICY SETTINGS

A user will be registered with the identity provider and use the service from service provider. The setup here is to allow service provider (the Cluster Server) to use an identity provider.

The SAML single sign on setup is mostly about matching parameters from the identity provider to the identity consumer (service provider). As shown in the screen capture, There are three types of identity provider, “Azure AD”, “AD FS”, and “others (generic)” that pretty much covers the most used ones and the most generic ones.

### Others (Generic SAML)

Here, The IdP will be a public IdP such as SSOCircle and the SP will be the Cluster Server. The SSOCircle is used as an example to set up the IdP; it can work with other IdP as well.

In a multi-tenant Cluster Server deployment each tenant may want to have its own SSO service. Therefore, the Single Sign On is a per-tenant setting.

### Step 1: Register the Cluster Server at IdP

IdP will need to register the Cluster Server as a service provider (SP) by importing the SP’s meta data. You will find the Cluster’s metadata at the following location (per-tenant setting).

We can use the following xml to register the Cluster as an SP at SSOCircle:

Now at the SSOCircle, need to add a new service provider:

In the next screen we can paste in the xml from the Cluster side, set the FQDN to the URL contained within the XML, and check the 3 parameters, the FirstName, LastName and Email.

Now the SSOCircle side of the registration is done.

### Step 2: Register SSOCircle at the Cluster Server side

The IdP registration and SP registration is a two-way I trust you and now you trust me kind of manual setup.

The meta data from the SSOCircle look like this and it can be imported to the Cluster Server.



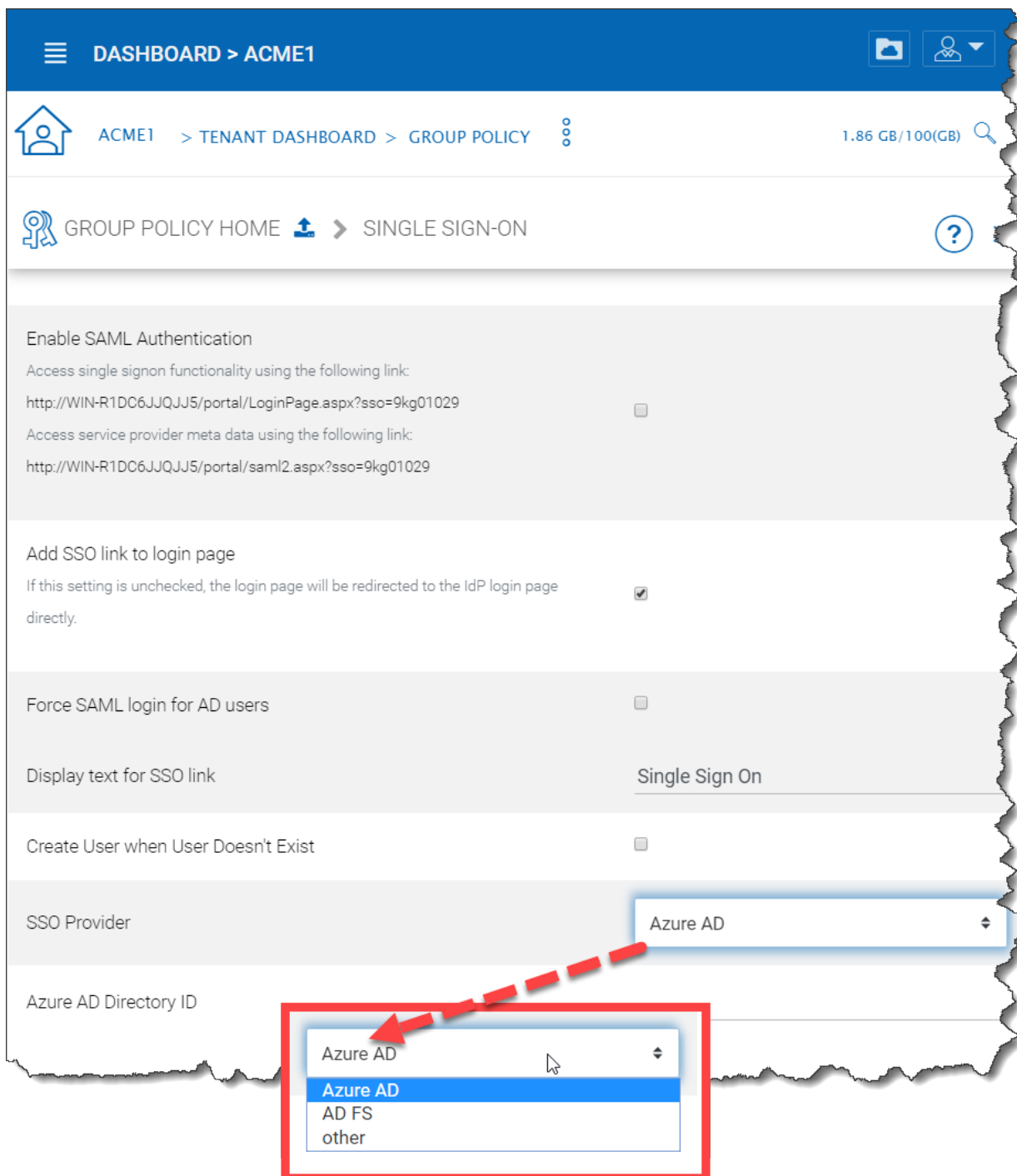


Fig. 85: SINGLE SIGN ON (SSO) SETTINGS

Access service provider meta data use following link:

<https://labtech.centrestack.com/portal/saml2.aspx?sso=I5F4UI9I>

Fig. 86: SERVICE PROVIDER META DATA LINK

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" entityID="https://labtech.centrestack.com/portal/saml2/I5F4UI9I">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:AssertionConsumerService index="0" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://labtech.centrestack.com/portal/saml2.aspx"/>
  </md:SPSSODescriptor>
  <md:Organization>
    <md:OrganizationName xml:lang="en">CentreStack</md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="en">CentreStack</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="en">
      https://labtech.centrestack.com/portal/LoginPage.aspx?sso=I5F4UI9I
    </md:OrganizationURL>
  </md:Organization>
</md:EntityDescriptor>
```

Fig. 87: REGISTER CLUSTER SERVER AS AN SP AT SSOCIRCLE

Logout

My Profile

My SAML Federations

My OpenID Trust

My Certificate Status

My Certificate  
Enrollment

My Certificate  
Enrollment PKCS#10

My Certificate  
Revocation

**Manage Metadata**

My Audit

My Debug

My Subscriptions

## Manage your Service Provider Metadata

### Service Provider Metadata

☐ <https://labtech.centrestack.com/portal/saml2/I5F4UI9I>

Remove Metadata

[Add new Service Provider](#)

[SSOCircle Public IDP Metadata](#)

Fig. 88: ADD A SERVICE PROVIDER AT SSOCIRCLE

Logout  
My Profile  
My SAML Federations  
My OpenID Trust  
My Certificate Status  
My Certificate Enrollment  
My Certificate Enrollment PKCS#10  
My Certificate Revocation  
Manage Metadata  
My Audit  
My Debug  
My Subscriptions

## Service Provider Metadata import

User ID: jhuang

Enter the FQDN of the ServiceProvider ex.: sp.cohos.de

Attributes sent in assertion (optional)

☐ FirstName

☐ LastName

☐ EmailAddress

Insert your metadata information

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:xsi="urn:oasis:names:tc:SAML:2.0:assertion" entityID="https://labtech.centrestack.com/portal/saml2/SP46092">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:AssertionConsumerService index="0" binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://labtech.centrestack.com/portal/saml2.asp"/>
  </md:SPSSODescriptor>
  <md:Organization>
    <md:OrganizationName xml:lang="en">Centrestack</md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="en">Centrestack</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="en">
      http://labtech.centrestack.com/portal/page.page.aspx?c=1544094
    </md:OrganizationURL>
  </md:Organization>
</md:EntityDescriptor>
```

Fig. 89: INSERT YOUR METADATA INFORMATION

Logout  
My Profile  
My SAML Federations  
My OpenID Trust  
My Certificate Status  
My Certificate Enrollment  
My Certificate

## Manage your Service Provider Metadata

### Service Provider Metadata

☐ <https://labtech.centrestack.com/portal/saml2/15F4UI9I>

[Add new Service Provider](#)

[SSOCircle Public IDP Metadata](#)

Fig. 90: MUTUAL TRUST SP REGISTRATION



Fig. 91: EXAMPLE OF SSOCIRCLE META DATA

Inside the meta data from SSOCircle, you will see there is a HTTP-Redirect URL, that will be the URL we use to register the IdP. And also register the 3 parameters (FirstName, LastName, EmailAddress) from the IdP.

### Step 3: Login at the IdP, but use service at SP

As the summary, the IdP and SP register each other's meta data, register each other's URL and parameters. After that, it will be single signon at the IdP side. The login will be at the IdP side, and after login, it will redirect back to the SP side.

#### 4.10.2.4 Azure AD

Tenant Manager > [Tenant] > Group Policy > Account & Login > Azure AD

Azure AD integration allows users to use their Azure AD credentials to login to the Cluster Server, including web portal and native clients.

You will still need to create Azure AD users as if they were local Cluster users first. After that, you can enable Azure AD integration.

To enable Azure AD integration, you will need to create an Azure AD native client application.

You will need the client id from the Azure Native Client Application

You will give the Azure Native Client Application full read permission to the following two items

- Azure Active Directory
- Microsoft Graph API

You will also need the domain name

#### 4.10.3 Folder & Storage

Tenant Manager > [Tenant] > Group Policy > Folder & Storage

The screenshot shows the 'SINGLE SIGN ON' settings page. The top navigation bar includes 'DASHBOARD > ACME > TENANT DASHBOARD > GROUP POLICY'. A trial timer shows '18 trial day(s) left' with a 'Buy Now!' button. The page title is 'GROUP POLICY HOME > SINGLE SIGN ON'. The settings are organized into sections:

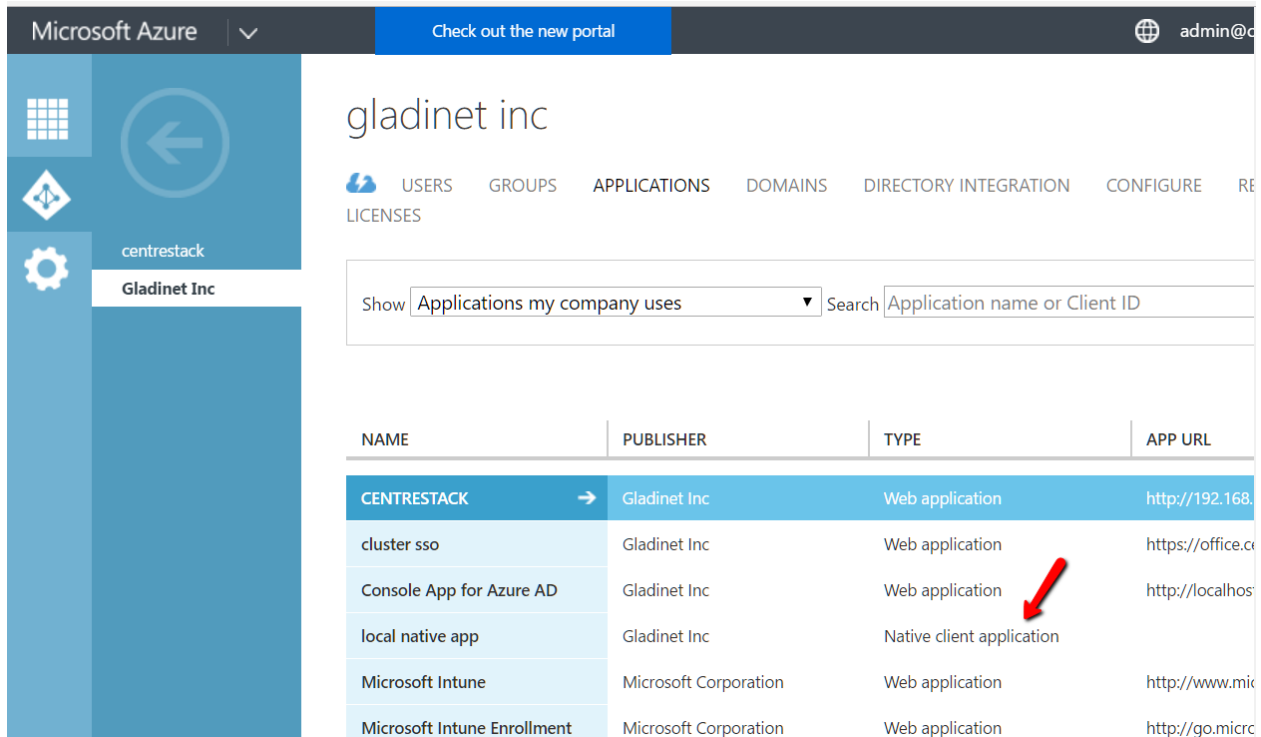
- Enable SAML Authentication:** Includes links for single signon functionality and service provider meta data.
- Add SSO link to login page:** A checkbox that is checked. A note states: 'If this setting is unchecked, the login page will be redirected to the IdP login page directly.'
- Display text for SSO link:** A text input field containing 'Single Sign On'.
- Create User when User Doesn't Exist:** A checkbox that is unchecked.
- IdP End Point URL:** A text input field for the URL of the Identity Provider.
- IdP Email Parameter:** A text input field for the email parameter name.
- IdP Given Name Parameter:** A text input field for the given name parameter name.

On the right side, there is a 'settings cont.' link and a modal window titled 'IdP Surname Parameter' with a text input field for the 'Surname Parameter Name in Identity Provider'. Below this is another modal window titled 'IdP Meta Data' for 'Identity Provider Metadata in XML Format'.

Fig. 92: SINGLE SIGN ON SETTINGS

The screenshot shows the 'SAML Consent Page'. On the left is a sidebar menu with links: Logout, My Profile, My SAML Federations, My OpenID Trust, My Certificate Status, My Certificate Enrollment, My Certificate Enrollment PKCS#10, My Certificate Revocation, and My Metadata. The main content area has the title 'SAML Consent Page' and the text: 'Please proof that you are not a ROBOT and click "continue"'. Below this is a link to 'Buy SSO Circle Premium Account' and another line of text: 'or any other hosted or SSOCheck enabled option: IDP Pricing or SSOCheck API'. A reCAPTCHA widget is present with the text 'I'm not a robot' and a 'Continue SAML Single Sign On' button.

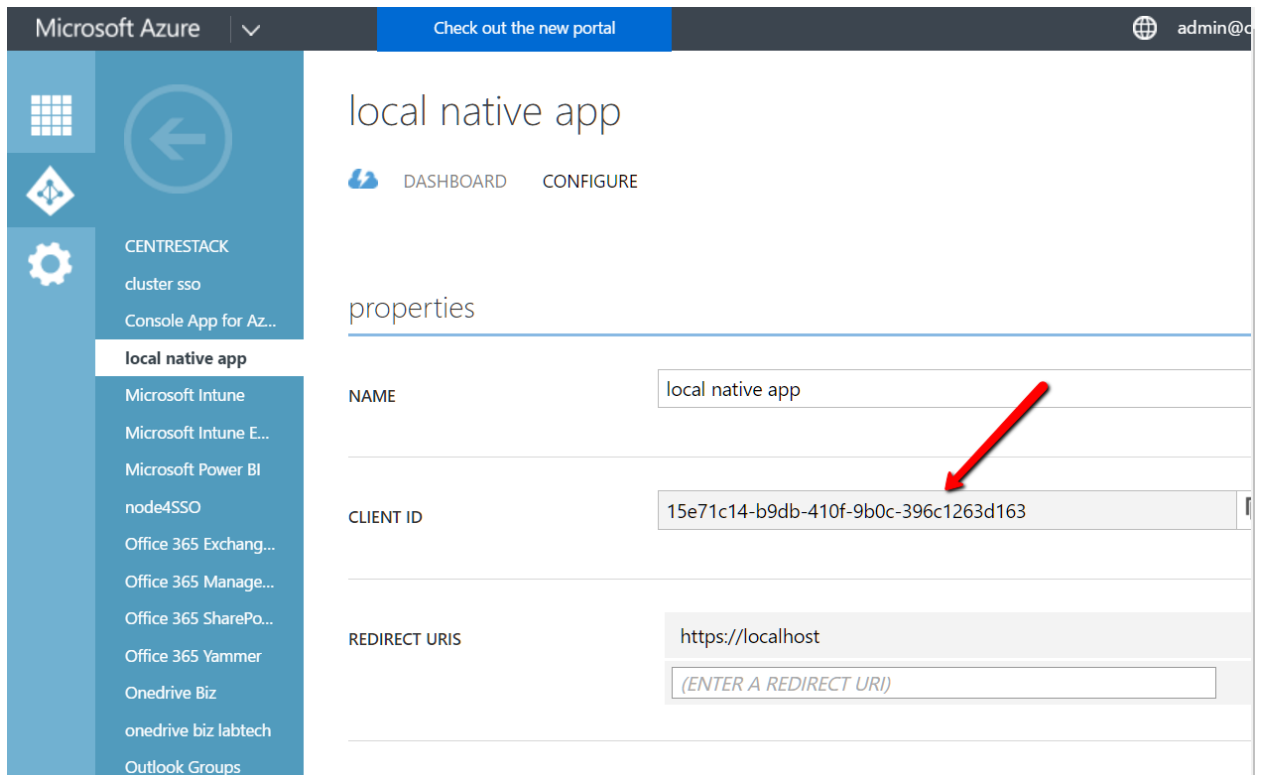
Fig. 93: IDP SIDE SINGLE SIGNON



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation icons and the text 'centrestack' and 'Gladinet Inc'. The main content area is titled 'gladinet inc' and includes tabs for 'USERS', 'GROUPS', 'APPLICATIONS', 'DOMAINS', 'DIRECTORY INTEGRATION', 'CONFIGURE', and 'RE'. Below these tabs is a search bar with the text 'Show Applications my company uses' and a search input field containing 'Application name or Client ID'. A table lists applications with columns 'NAME', 'PUBLISHER', 'TYPE', and 'APP URL'. The 'local native app' entry is highlighted, and a red arrow points to it.

NAME	PUBLISHER	TYPE	APP URL
CENTRESTACK	Gladinet Inc	Web application	http://192.168...
cluster sso	Gladinet Inc	Web application	https://office.c...
Console App for Azure AD	Gladinet Inc	Web application	http://localhost...
local native app	Gladinet Inc	Native client application	
Microsoft Intune	Microsoft Corporation	Web application	http://www.mic...
Microsoft Intune Enrollment	Microsoft Corporation	Web application	http://go.micr...

Fig. 94: ENABLE AZURE AD INTEGRATION



The screenshot shows the Microsoft Azure portal interface for the 'local native app' configuration page. The left sidebar contains navigation icons and the text 'CENTRESTACK', 'cluster sso', 'Console App for Az...', 'local native app', 'Microsoft Intune', 'Microsoft Intune E...', 'Microsoft Power BI', 'node4SSO', 'Office 365 Exchang...', 'Office 365 Manage...', 'Office 365 SharePo...', 'Office 365 Yammer', 'Onedrive Biz', 'onedrive biz labtech', and 'Outlook Groups'. The main content area is titled 'local native app' and includes tabs for 'DASHBOARD' and 'CONFIGURE'. Below these tabs is a section titled 'properties' with a table containing the following fields:

NAME	local native app
CLIENT ID	15e71c14-b9db-410f-9b0c-396c1263d163
REDIRECT URIS	https://localhost
	(ENTER A REDIRECT URI)

A red arrow points to the 'CLIENT ID' field.

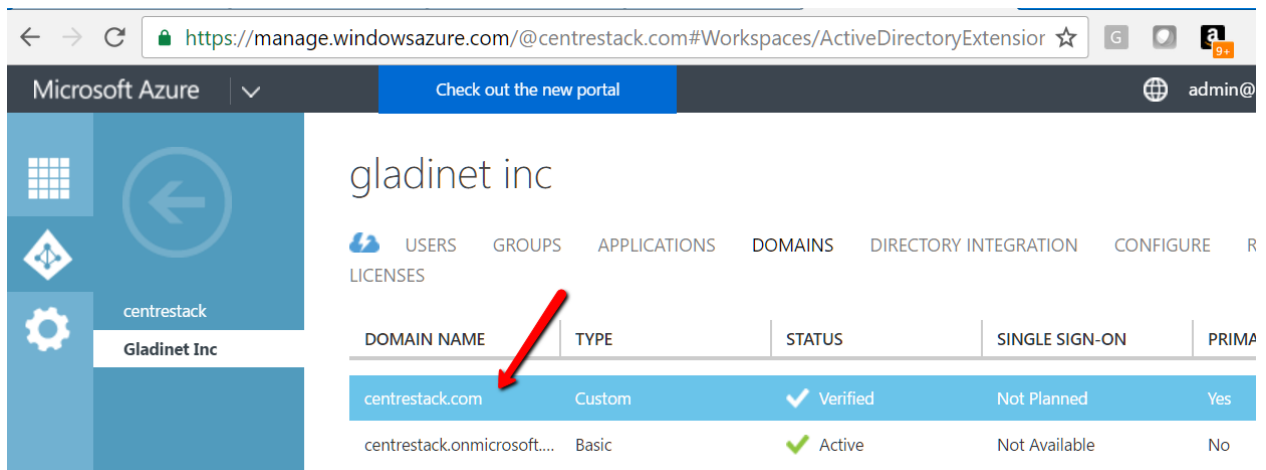
Fig. 95: AZURE CLIENT ID FIELD

## permissions to other applications

Office 365 Exchange Online	Delegated Permissions: 1
Microsoft Graph	Delegated Permissions: 1
Windows Azure Active Directory	Delegated Permissions: 1

Add application

Fig. 96: AZURE PERMISSIONS TO OTHER APPLICATIONS



The screenshot shows the Microsoft Azure portal interface for 'gladinet inc'. The left sidebar contains navigation icons for 'centrestack' and 'Gladinet Inc'. The main content area displays a table of domain settings. A red arrow points to the 'centrestack.com' domain entry.

DOMAIN NAME	TYPE	STATUS	SINGLE SIGN-ON	PRIMA
centrestack.com	Custom	✓ Verified	Not Planned	Yes
centrestack.onmicrosoft....	Basic	✓ Active	Not Available	No

Fig. 97: AZURE DOMAIN SETTING

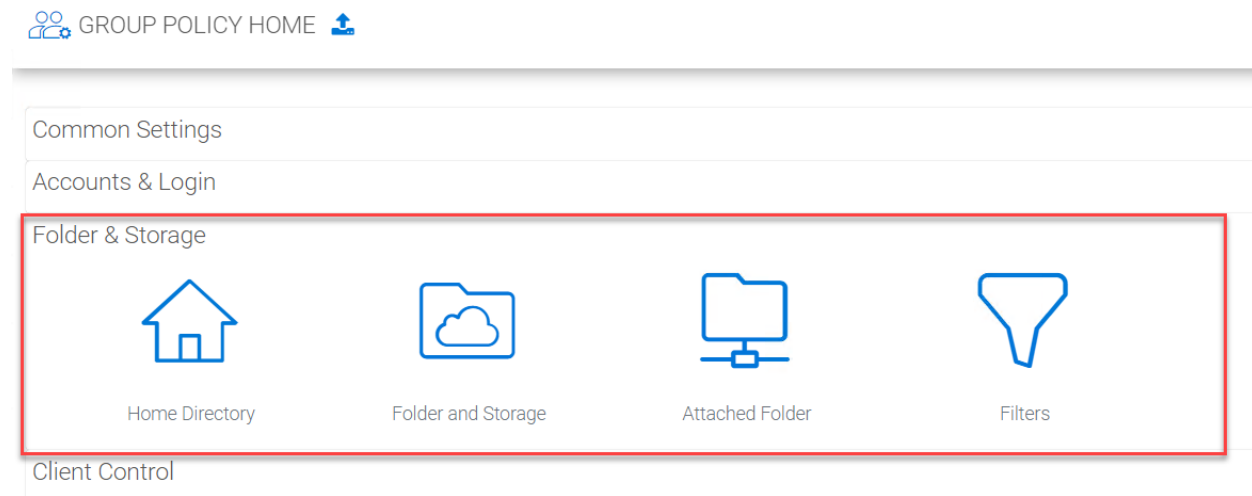


Fig. 98: FOLDER AND STORAGE PANEL

#### 4.10.3.1 Home Directory

Tenant Manager > [Tenant] > Group Policy > Folder & Storage > Home Directory

##### Default Storage quota

This policy will not affect existing user and their quota. It can affect a newly created user for the default storage quota.

##### Create default folders

When the new user account is provisioned, the default root folder is empty.

“Create default folder (Documents, Pictures)” will make the root folder look less empty and more user-friendly. This hints at how to organize files and folders in the cloud.

##### Use user email to generate home directory name

The home directory name will be created using user’s email address.

By default, it is user’s GUID that is used to create user’s home directory.

##### Use user’s sAMAccountName to generate home directory names for Active Directory users

This option supports clients and servers from previous versions of Windows that use Security Account Manager (SAM) type user accounts.

##### Publish user’s home drive

When unchecked, the user home drive space will be allocated from enterprise storage. When checked, existing user home drives will be automatically published from Active Directory.

##### Mount user’s home drive as a top level folder.

Without this option, the user’s home drive from active directory mapping will become the root folder in CentreStack. However, if the user also have network shares mapped into CentreStack, those network shares will appear as top level folders. So in this use case, mapping user’s home folder as a top folder is more in parallel to the other network shares.



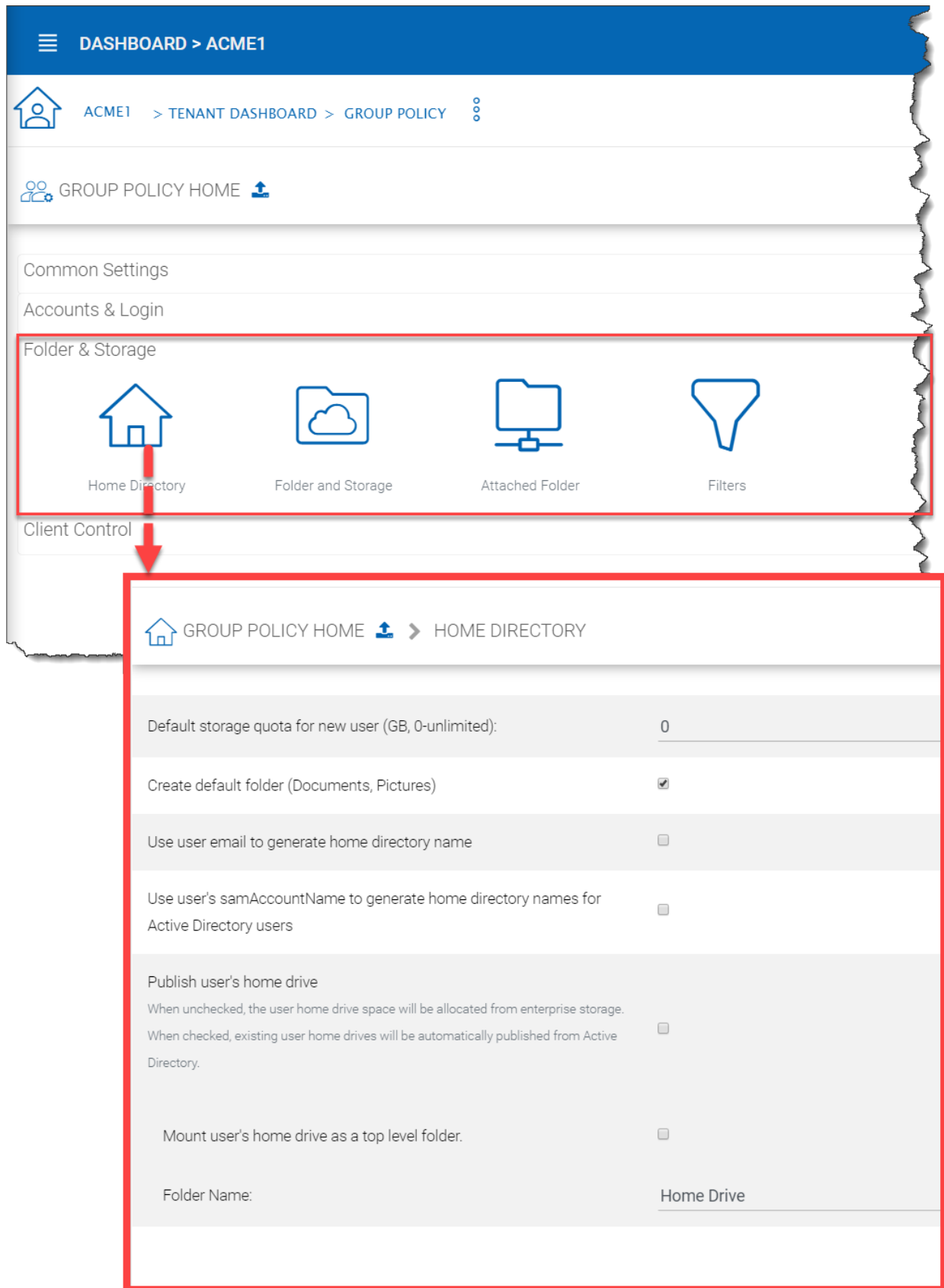


Fig. 99: HOME DIRECTORY SETTINGS

### 4.10.3.2 Folder and Storage

Tenant Manager > [Tenant] > Group Policy > Folder and Storage

These are the settings available to the tenant manager in the Folder and Storage view.

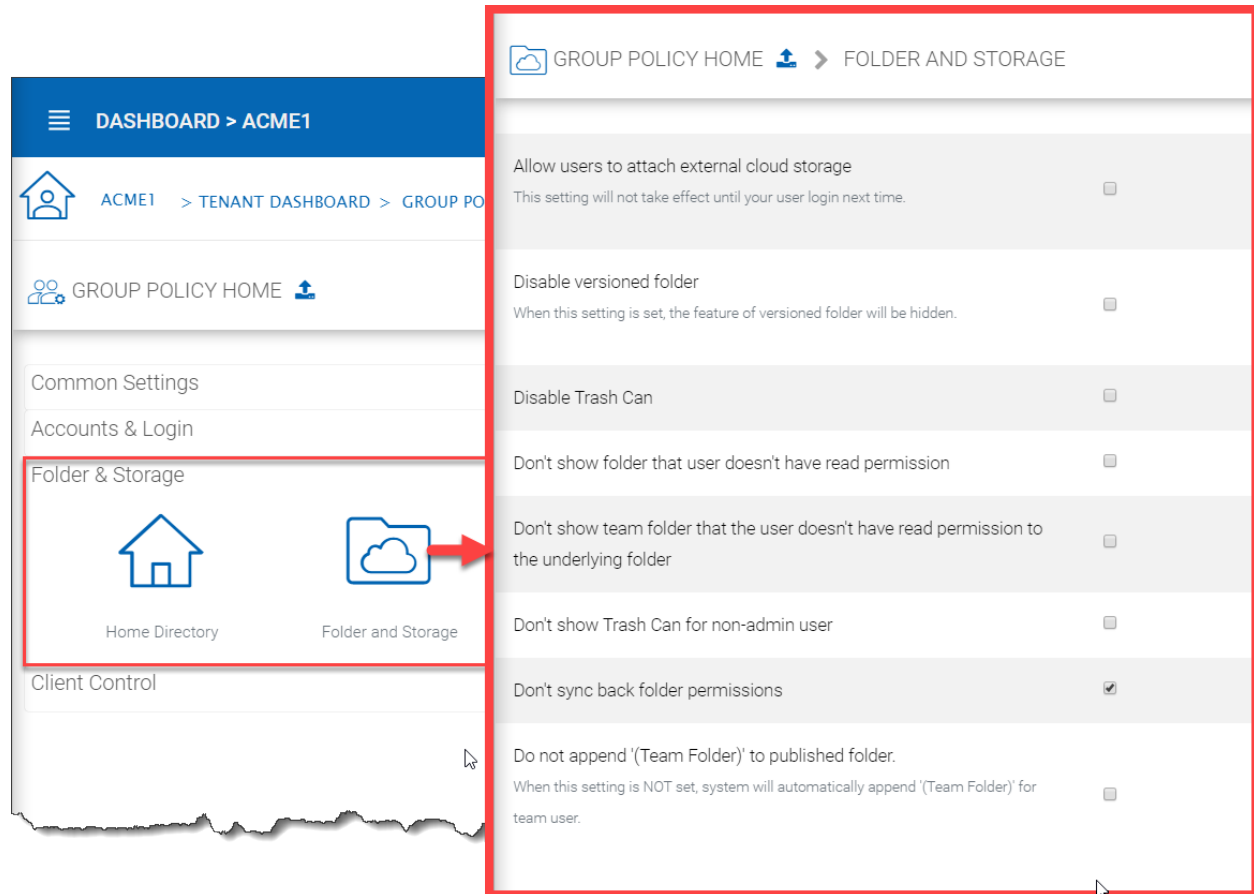


Fig. 100: FOLDER AND STORAGE SETTINGS

#### Allow users to attach external cloud storage

when checked, you will allow users to see storage manager and allow them to attach external storage such as their own Amazon S3 bucket into the system.

#### Disable Versioned folder

Normally you will NOT disable versioned folder. Because versioned folder is the supporting feature for “Two-way sync locally attached folder”. If you disable versioned folder, you will lose the two-way synchronization folder feature as well.

#### Disable Trash Can

For folders that are not under version control, a deleted file will be moved into Trash Can. If this feature is not useful, you can disable it.

#### Don't show folder that user doesn't have read permission

With native Active Directory integration and with network share as backend storage, the user's permission to the folders are checked natively. When this option is set, for those folders that users doesn't have read permission, the folder will be hidden.

### **Don't show team folder that the user doesn't have read permission to the underlying folder**

In the folder listing, if the user don't have read permission, sometimes it is better off not to show the folder to the user.

### **Don't show Trash Can for non-admin user**

Trash Can is a virtual folder that shows up at the web browser portal only. This setting controls whether or not to show it for regular team user.

### **Don't append (Team Folder) to published folders**

A team folder by default, when showing up in a team user's folder list, it will have "(Team Folder)" appended to the end of the folder name to signify it is a team folder. This feature allows a team folder showing up as it is without the (Team Folder) suffix. The use case is that when a network share is mounted and then turned into a team folder, since the users are already familiar with the network share in its original name, so it is not necessary to append (team folder) to the folder name. You shouldn't change this setting in the middle of operation because if users have pending upload/download, changing the name could cause those tasks to fail.

## **4.10.3.3 Attached Folder**

Tenant Manager > [Tenant] > Group Policy > Folder & Storage > Attached Folder

### **Disable backup/attach local folder from client device**

Attached Local Folders are two-way synchronization folders. In order to do version backup and two-way synchronization, there are multiple folder structures created in the backend storage. Some organization doesn't need this feature and want the users to work exclusively with the cloud drive.

### **Enable Snapshot backup for server agent**

It is a feature related to server agent on Windows 2003-2012 servers.

### **Allow syncing empty files**

By default, empty file (0-byte) will be skipped for syncing in attached folder. when enabled, those files will be synchronized.

### **Allow syncing of hidden files**

Hidden files by default will not sync.

### **Allow executable files (.exe)**

Executable files by default will not sync.

### **Allow ISO files (.iso)**

Executable files by default will not sync.

### **Allow backup files(.bck, .bkf, .rbf, .tib)**

**Allow VMs (.hdd, .hds, .pvm, .pvs, .vdi, .vfd, .vhd, .vmc, .vmdk, .vmem, .vmsd, .vmsn, .vmss, .vmtm, .vmwarevm, .vmx, .vmxf, .vsv, .nvram, .vud, .xva)**

### **Allow application folders**

Application folder by default will not sync.

### **Allow application data folders**

Application data folder by default will not sync.

### **Enable scheduled sync for files with following extensions**

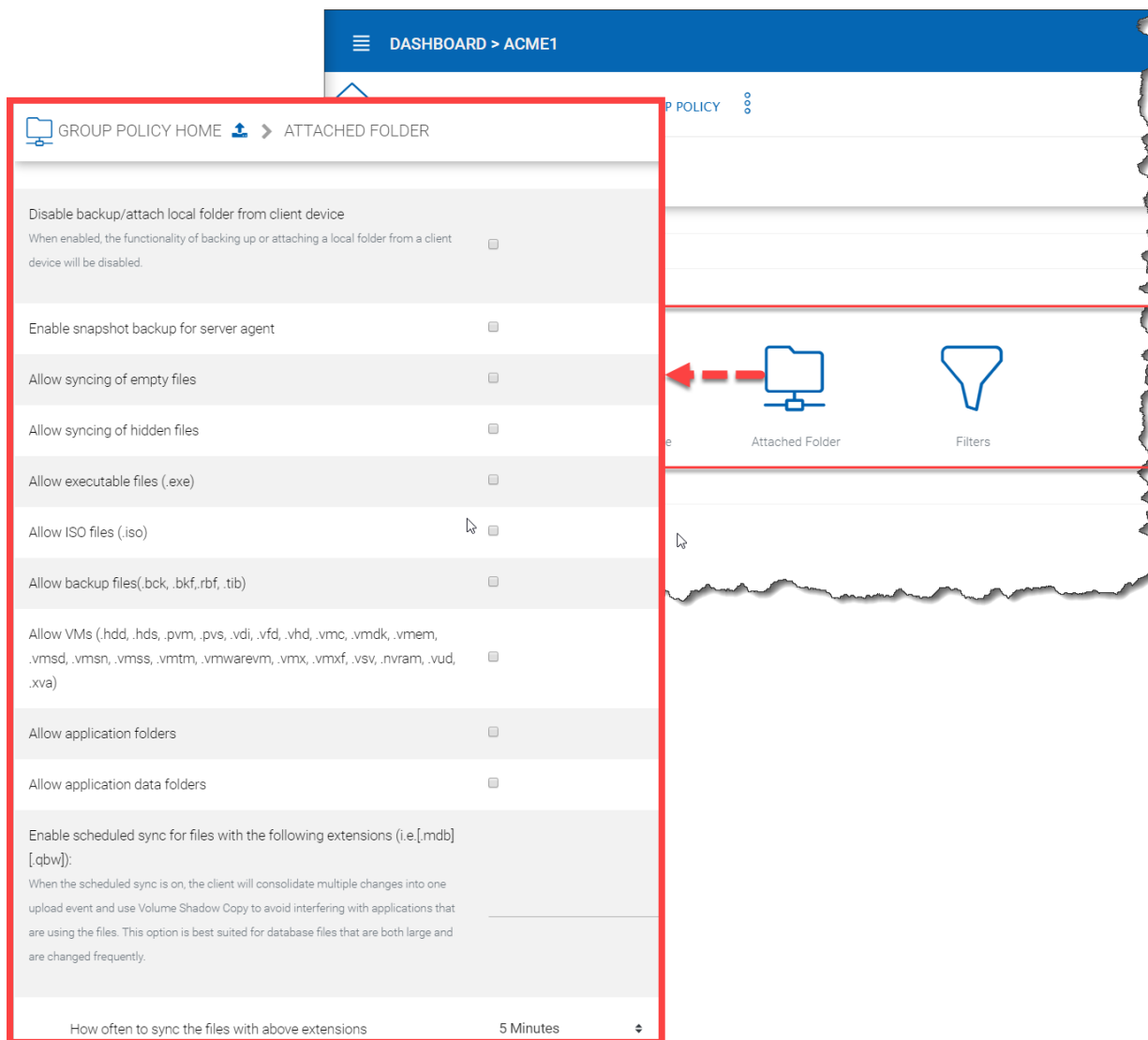


Fig. 101: ATTACHED FOLDER SETTINGS

this is to help sync/upload frequently changed file such as Microsoft access database or QuickBook files. These type of files typically are constantly open (thus prevent other application to hold on to them) and also changed frequently. So you can define the time period to check back on these type of files and use volume shadow copy to upload these files.

#### 4.10.3.4 Filters

Tenant Manager > [Tenant] > Group Policy > Folder & Storage > Filters

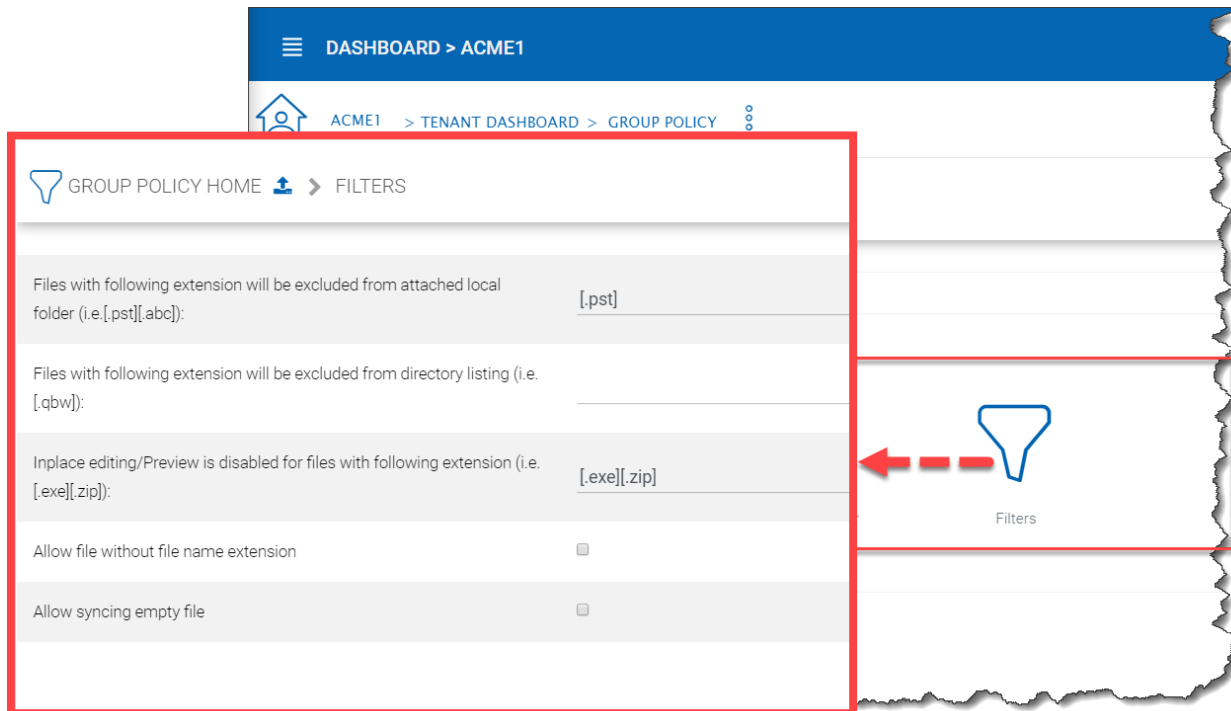


Fig. 102: GROUP POLICY FILTER SETTINGS

##### Files with the following extensions will be excluded from attached local folder

You can stop certain file types from being uploaded. For example .pst files. These are local outlook email files, which is not necessary to upload into the cloud storage because usually it is backed up by an exchange server.

##### Files with following extensions will be excluded from directory listing (i.e.[.qbw])

You can specify the executables which should not be listed under a user's directory.

##### In-place editing/Preview is disabled for files with following extension

Windows Explorer has a habit to peek into large files to generate thumbnail and present other information. It may not be a good fit for cloud drive files because each peek will generate a download from cloud.

##### Allow file without file name extension

Allow files without extension suffix to synchronize.

##### Allow syncing empty file

This is the same setting as in the "Attached Folder" section.

## 4.10.4 Client Control

### 4.10.4.1 Web Portal

Tenant Manager > [Tenant] > Group Policy > Client Control > Web Portal

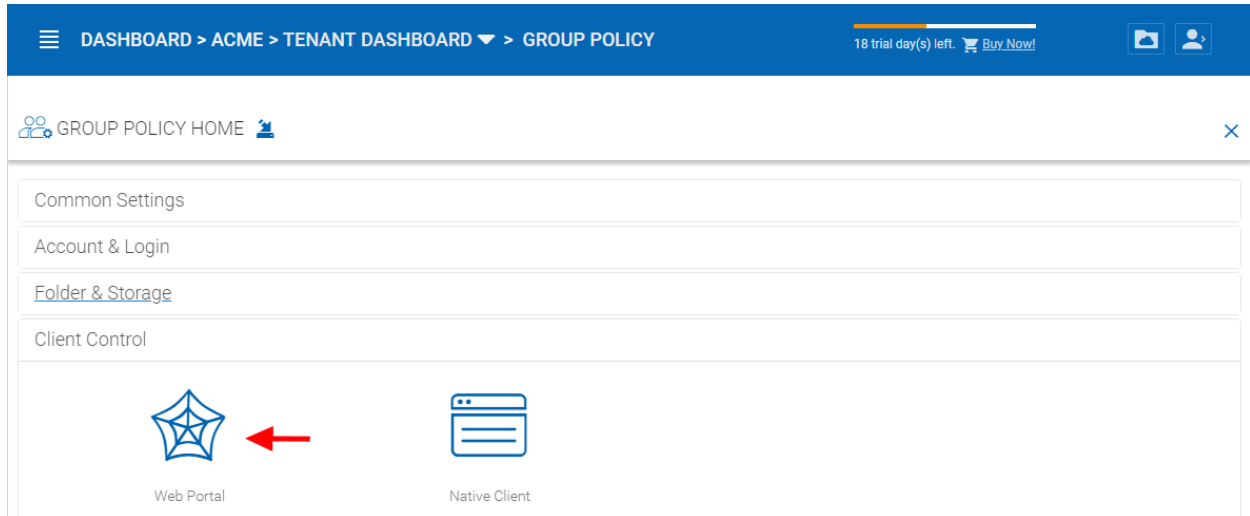


Fig. 103: WEB PORTAL PANEL

#### Disable folder download from web client

Disabled by default. The folder download from web client will zip up the folder and download it. It is CPU intensive so if you don't want it to be consuming too much CPU, you can disable it using this setting.

#### Disable Search

Disabled by default. If you don't need the search by file name feature, you can check this setting to disable it.

#### Web Browser - Disable Java Uploader

Some organization standardized on web browser, for example, all web browser are HTML5 compliant. In this case, Java Uploader is not necessary and could be confusing to support when different users have different Java version installed.

#### Web Browser - Disable Flash Uploader

Some organization standardized on web browser, for example, all web browser are HTML5 compliant. In this case, Flash Uploader is not necessary and could be confusing to support when different users have different Flash version installed. Different kind of web browser may also have different levels of Flash support, causing different behavior.



#### Web Browser - Disable Local Uploader

Admin can also disable local uploaded in which case the upload will happen using the browser directly.

#### Enable Tabbed-Browsing in User Manager

When enabled, the user manager will order users by their last name so if you have many users, you have an easy to access way to find the users.

#### Only show search interface in User Manager


GROUP POLICY HOME

> WEB PORTAL

Disable folder download from web client	
When enabled, the functionality of downloading a folder as a zip file from the web client will be disabled.	<input type="checkbox"/>
Disable Search	<input type="checkbox"/>
Web Browser - Disable Java Uploader	<input checked="" type="checkbox"/>
Web Browser - Disable Flash Uploader	<input checked="" type="checkbox"/>
Web Browser - Disable Local Uploader	<input checked="" type="checkbox"/>
Enable Tabbed-Browsing in User Manager	<input type="checkbox"/>
Only show search interface in User Manager	<input type="checkbox"/>
Show tutorial page for non-admin users	<input type="checkbox"/>
Show team folder level permissions in team folder publishing dialog	<input type="checkbox"/>
Disable 'Publish Tenant Home Storage As a Team Folder'	<input type="checkbox"/>
Confirm before moving via drag-and-drop	<input type="checkbox"/>
Show left tree view by default	<input type="checkbox"/>
Do not show "recent activities"	<input type="checkbox"/>
Show "link to local" option to non-admin user	<input type="checkbox"/>
Show max count of file/folder items	1000

Fig. 104: WEB PORTAL SETTINGS

When you have even more users, Tabbed-Browsing can't handle it any more, you can enable search-only interface.

#### **Show tutorial page for non-admin users**

Display tutorial page for regular users when they login to the web portal.

#### **Show team folder level permissions in team folder publishing dialog**

The advanced setting refers to “Create CIFS Share”, “Disable further sharing”, and “Disable Offline Access” settings.

#### **Disable ‘Publish Tenant Home Storage As a Team Folder’**

This feature can be hidden in Tenant Management Console > Team Folder > Add New Team Folder

#### **Confirm before moving via drag-and-drop**

In web portal, sometimes there can be accidental drag and drop, in this case, having a confirmation dialog can help prevent accidental drag and drop.

#### **Show left tree view by default**

Disabled by default. When enabled left-tree is displayed when you log in to the web portal.

#### **Do not show “recent activities**

Disabled by default. When enabled “recent activities” is not visible in the Show/Hide Info Panel on the right side of the Web Portal File Browser.

#### **Show ‘link to local’ option to non-admin user**

Disabled by default. When enabled, non-admin user will have access to the “**Link to Local**” option in the Sharing and Collaboration tab under the Show/Hide Info Panel on the right side of the Web Portal File Browser.

#### **Show max count of file/folder items**

Default files to show is 1,000. Some customers may have a very flat folder that has more than one thousand files. It is not recommended to have a cloud system have flat folder structure like this. But if customer has many files in a flat folder. This setting can be used to show all files by increasing this number as needed.

### **4.10.4.2 Native Client**

Tenant Manager > [Tenant] > Group Policy > Client Control > Native Client

#### **Create a shortcut in the documents library**

Enabled by default. This is a convenience feature to add a link to documents library to the cloud drive.

#### **Create shortcut on desktop**

Enabled by default. Same as above but the shortcut is on the desktop.

#### **Hide Settings in Windows Client Management Console**

Disabled by default. The Settings in the Windows client may be viewed as “too much information for normal user”. If that is the case, enabling this option will hide those settings.

#### **Don't Allow Setting Changes in Windows Client Management Console**

Disabled by default. When disabled the Windows Client user can change the settings in the Windows Client Management Console.

#### **Disable Windows client in-place drag & drop uploading**



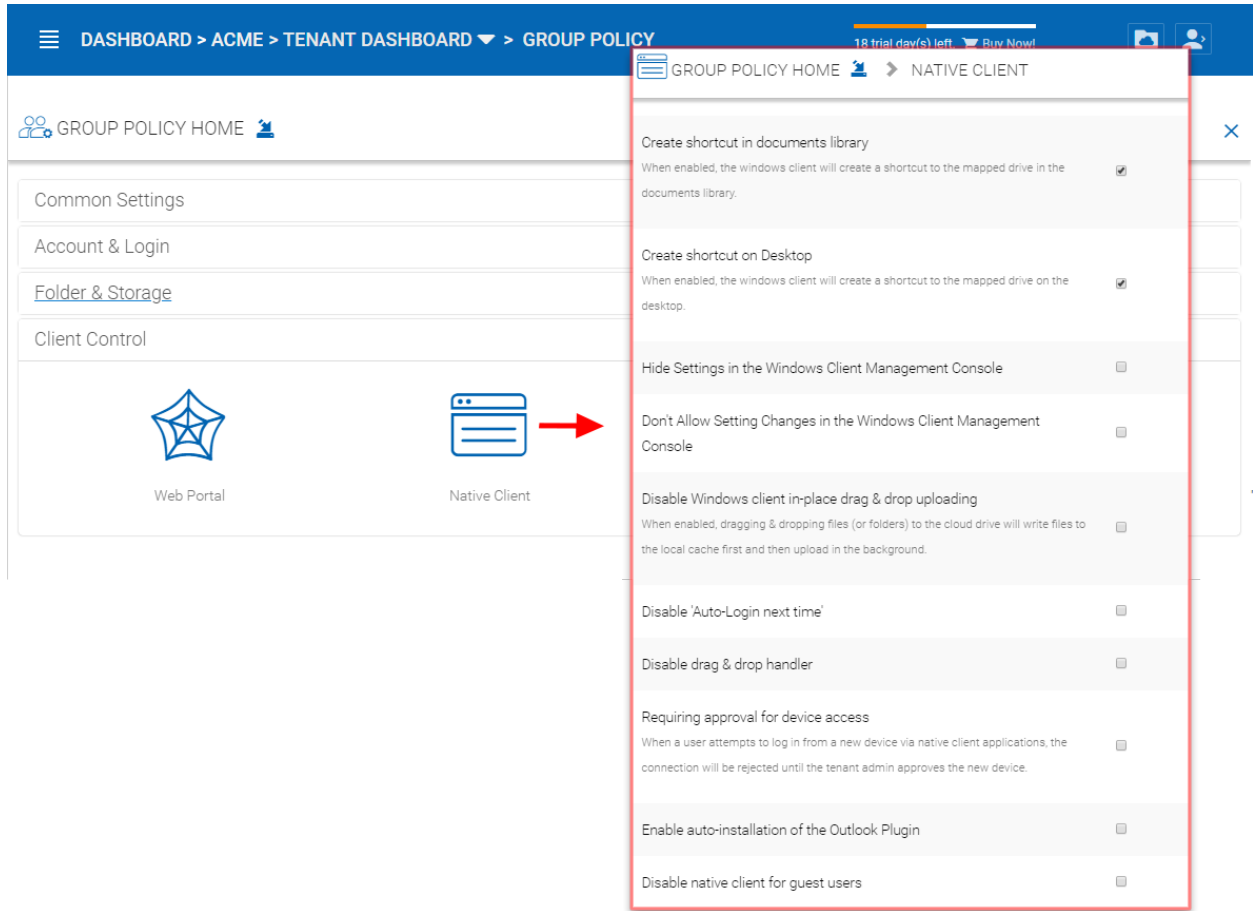


Fig. 105: NATIVE CLIENT SETTINGS

Unchecked by default. When enabled, dragging & dropping files (or folders) to the cloud drive will write files to the local cache first and then upload in the background.

#### **Disable Auto-Login next time**

Unchecked by default. When you want the user to type in username/password every time they login to the Windows client, you can check this to disable auto-login.

#### **Disable drag & drop handler**

Unchecked by default. If you check this option, the Windows file drag and drop will take over, this typically means the files will be copied into cache before upload, thus resulting in two copies of files being uploaded.

#### **Requiring approval for device access**

Disabled by default. When a user attempts to log in from a new device via native client applications, the connection will be rejected until the tenant admin approves the new device. The approval can be done from the “Client Device Manager”

#### **Enable auto-install of Outlook Plugin**

Disabled by default. The Cluster Server Windows Desktop client comes with an Outlook plug-in. If this option is enabled, the Outlook plugin will be enabled upon client startup.

#### **Disable native client for guest users**

Unchecked by default. For guest users, don’t allow them to use native client, so the guest users can only use web browser files and folder view.

### **4.10.5 Export/Import**

You can also export the group policy settings to other clusters in the environment or import existing settings from another cluster.

## **4.11 Tenant Branding**

```
Tenant Manager > [Tenant] > Tenant Branding
```

The cluster administrator can help the tenant do the tenant-specific branding in the partner portal.

The branding is applied by the customized URL. You can think of the customized URL as a primary key to retrieve all tenant related branding information.

If per-tenant branding is enabled, The tenant branding section will be available.

#### **Customized URL for your business**

Typically the customize URL is a sub domain of the Cluster Server. For example, if the Cluster Server is at <https://cloud.mycompany.com>, the sub domain can be <https://acme1.mycompany.com>

In Windows 2012 and above (the server that has the Cluster Server running), it also allows SNI (Server name indicator) in the SSL certificate binding. So it is possible to bind multiple SSL certificates to the same IIS server. In this case, the Customized URL can be a fully qualified domain name.

**Warning:** If you set up per-tenant branding, make sure the customized URL is specific to each tenant and also the URL is different from the default URL.

If you don’t want to setup per-tenant branding, disable it in cluster settings and setup cluster-wide branding instead.

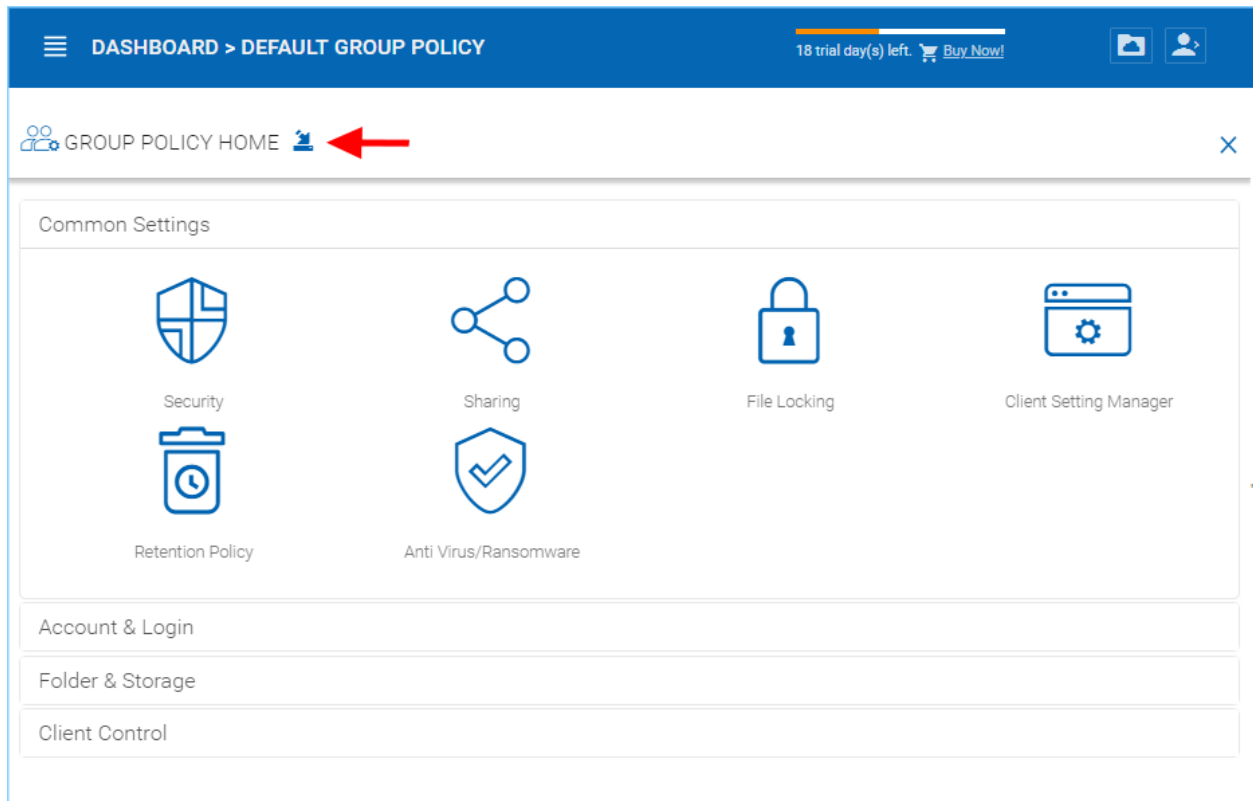
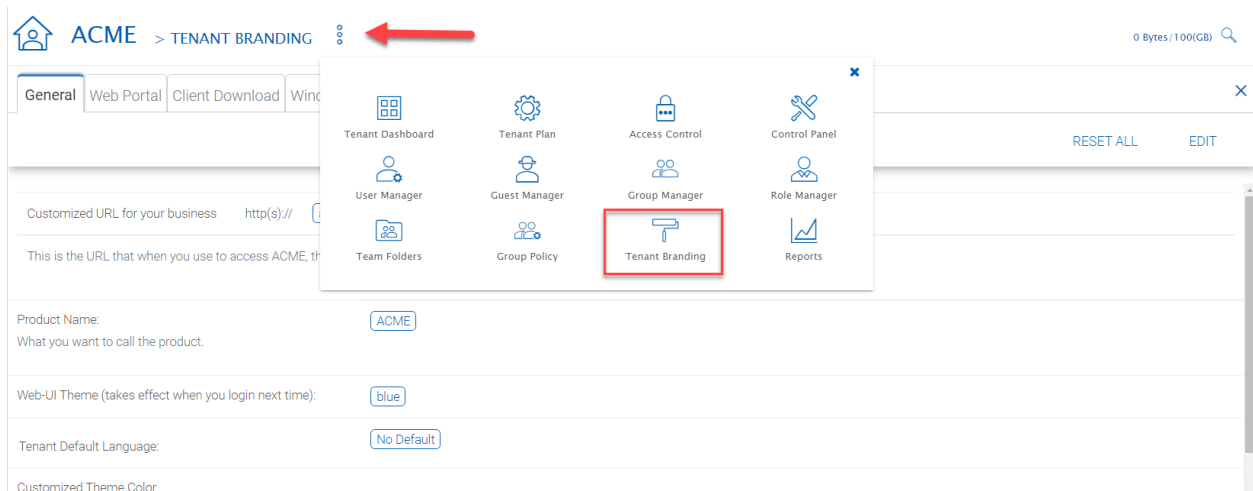


Fig. 106: EXPORT/IMPORT ICON LOCATION



ACME > TENANT BRANDING 0 Bytes/Unlimited

General Web Portal Client Download Windows Client Mac Client Emails Email Service

RESET ALL EDIT

Customized URL for your business http(s):// Not Branded /portal/loginpage.aspx

This is the URL that when you use to access CentreStack, the following branding settings will apply.

Product Name: Not Branded  
What you want to call the product.

Web-UI Theme (takes effect when you login next time): blue

Tenant Default Language: No Default

Customized Theme Color

Fig. 107: PER-TENANT BRANDING OPTIONS

## 4.12 Reports

Tenant Manager > [Tenant] > Reports

The cluster administrator can look at the tenant specific reports for the tenant.

The Reports section has the following sub categories

- Upload Report
- Storage Statistics
- Bandwidth Usage
- Team Folders
- Shared Objects
- Audit Trace
- File Change Logging
- Folder Permissions
- Distributed Locks
- Pending Purged Folders

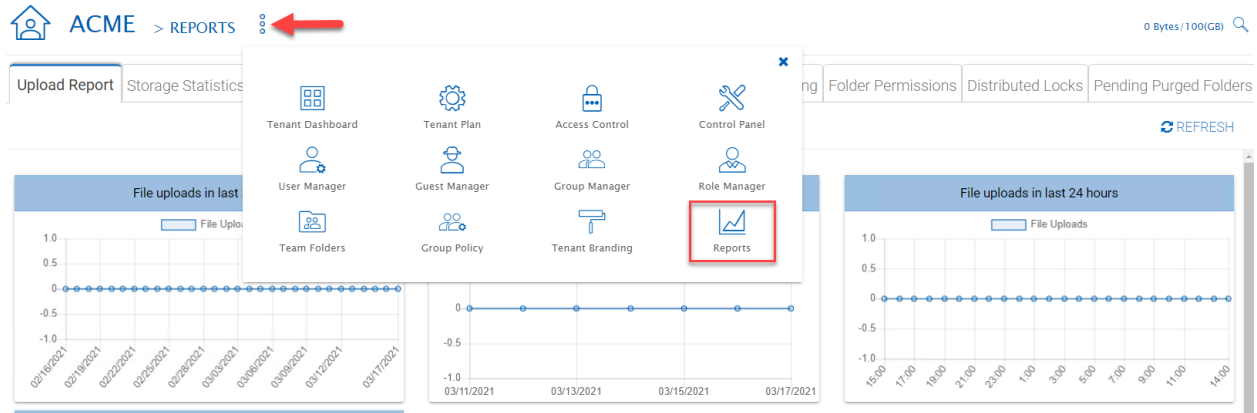


Fig. 108: TENANT MANAGER REPORTS

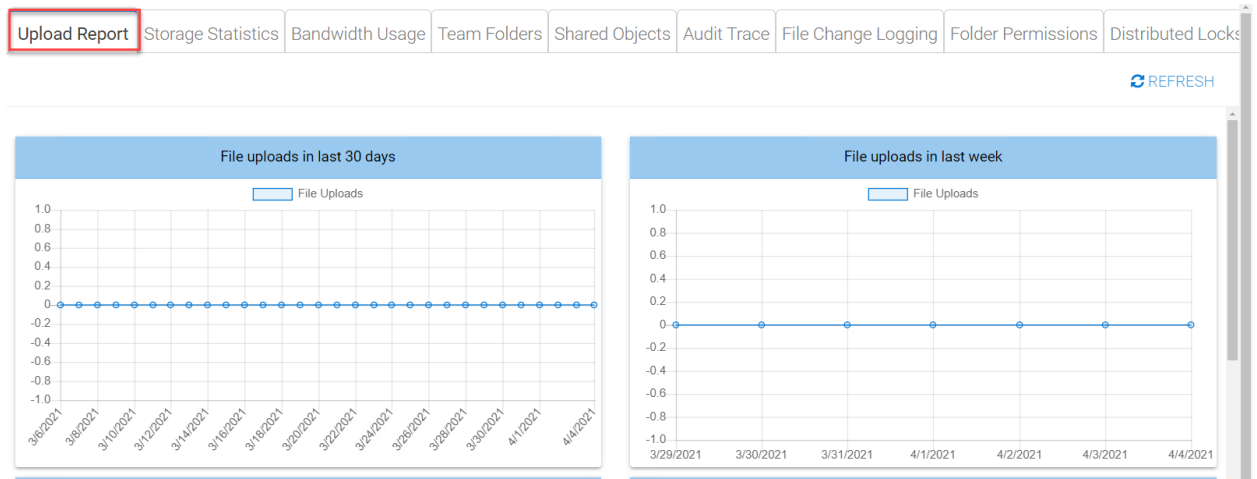


Fig. 109: UPLOAD REPORT

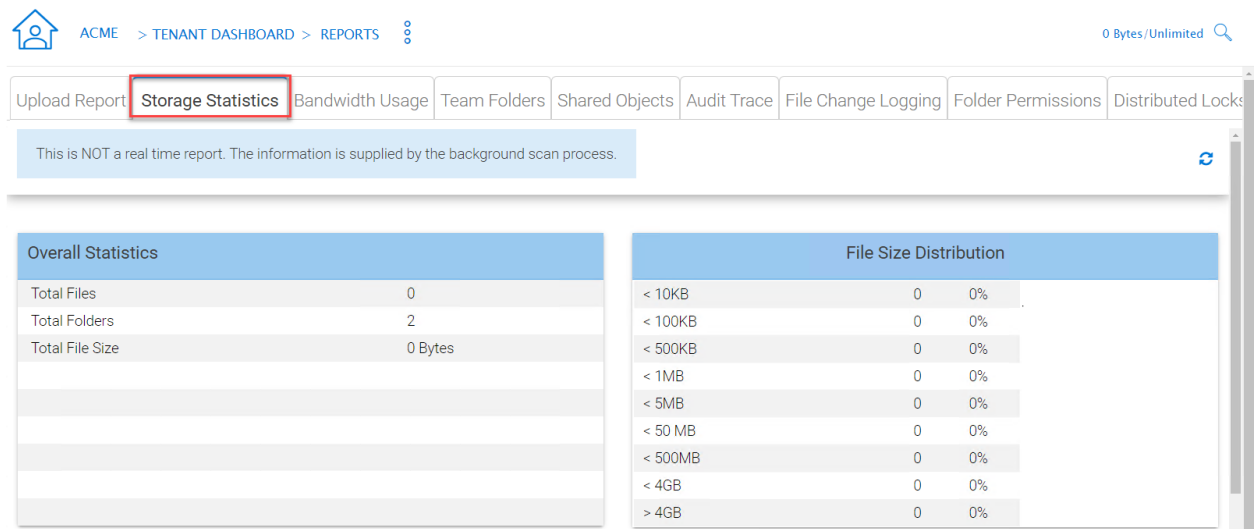


Fig. 110: STORAGE STATISTICS REPORT

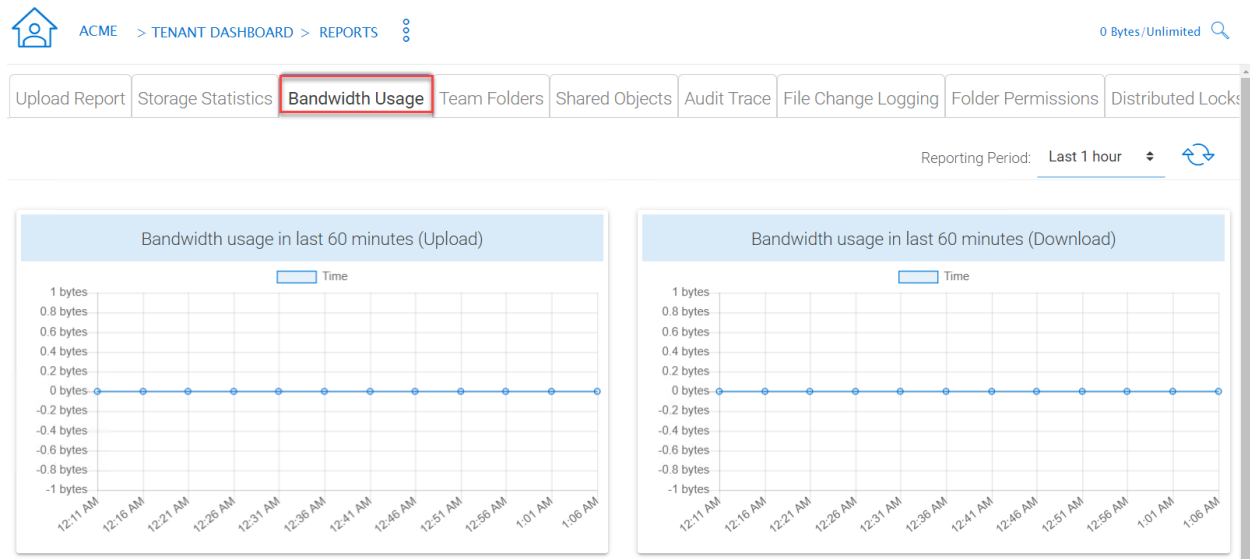


Fig. 111: BANDWIDTH USAGE REPORT

1 Published (Team) Folder(s)

User Name	Email	Read	Write	Owner
All AD Users	[Built In Group]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Everyone	[Built In Group]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Fig. 112: TEAM FOLDERS REPORT

### 4.12.1 Upload Report

### 4.12.2 Storage Statistics

### 4.12.3 Bandwidth Usage

### 4.12.4 Team Folders

### 4.12.5 Shared Objects

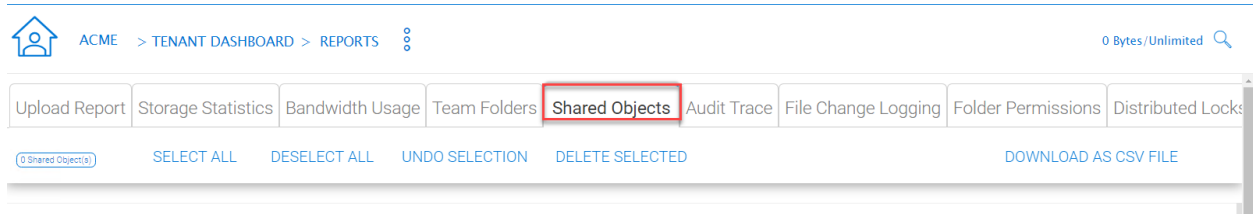


Fig. 113: SHARED OBJECTS REPORT

### 4.12.6 Audit Trace

Audit trace contains the management events, such as login success, login fail , shared a folder and etc.

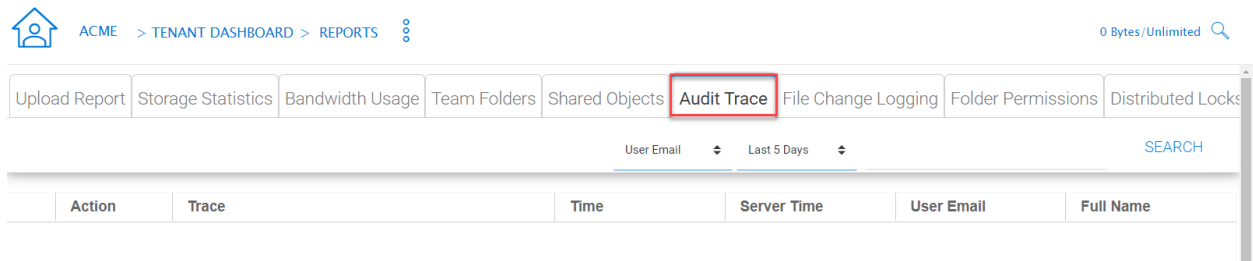


Fig. 114: AUDIT TRACE REPORT

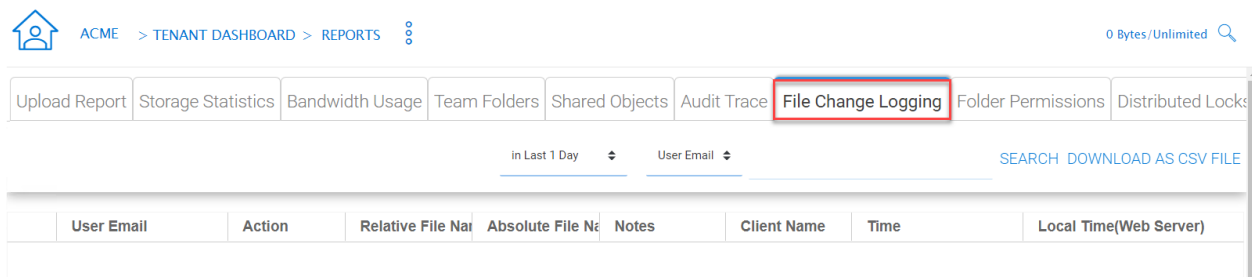
### 4.12.7 File Change Log

File change log is capable of search for user's file change history. It is most useful when helping user troubleshoot issues. For example, you can point to the file change log and say, you deleted this file on this day.

### 4.12.8 Folder Permissions

### 4.12.9 Distributed Locks

### 4.12.10 Pending Purged Folder



ACME > TENANT DASHBOARD > REPORTS

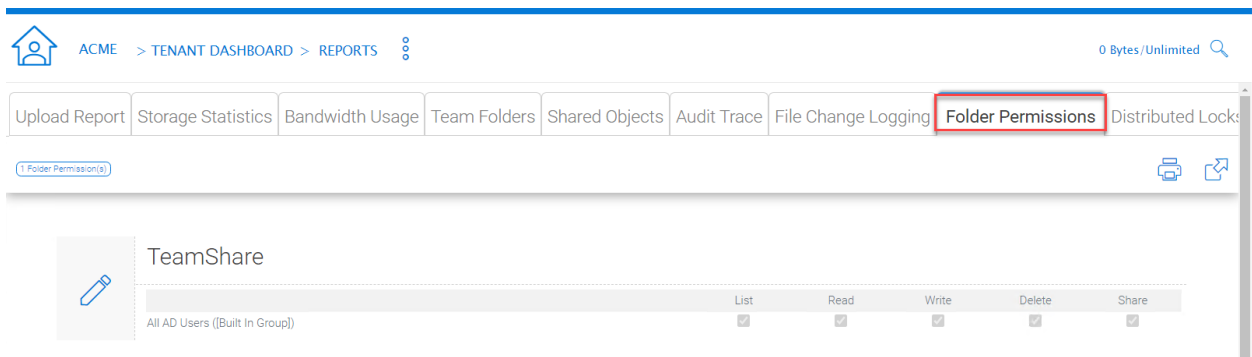
0 Bytes/Unlimited

Upload Report Storage Statistics Bandwidth Usage Team Folders Shared Objects Audit Trace **File Change Logging** Folder Permissions Distributed Locks

in Last 1 Day User Email SEARCH DOWNLOAD AS CSV FILE

User Email	Action	Relative File Name	Absolute File Name	Notes	Client Name	Time	Local Time (Web Server)
------------	--------	--------------------	--------------------	-------	-------------	------	-------------------------

Fig. 115: FILE CHANGE LOGGING REPORT



ACME > TENANT DASHBOARD > REPORTS

0 Bytes/Unlimited

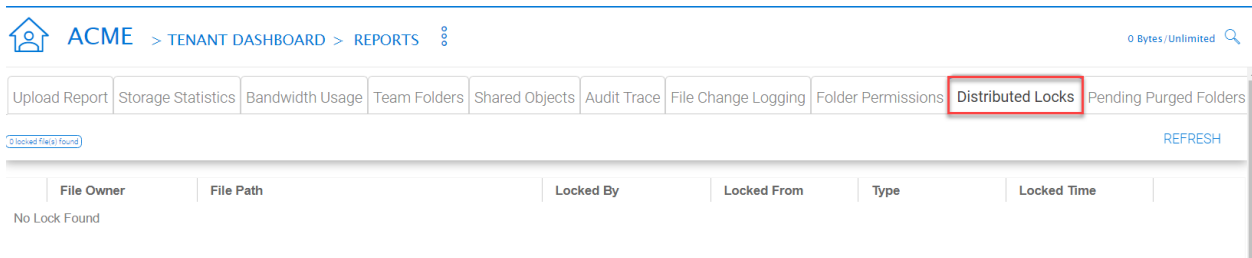
Upload Report Storage Statistics Bandwidth Usage Team Folders Shared Objects Audit Trace File Change Logging **Folder Permissions** Distributed Locks

1 Folder Permission(s)

TeamShare

	List	Read	Write	Delete	Share
All AD Users ([Built In Group])	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Fig. 116: FOLDER PERMISSIONS REPORT



ACME > TENANT DASHBOARD > REPORTS

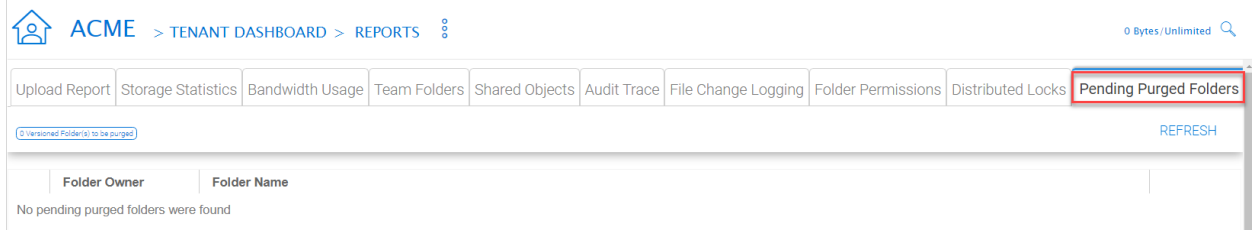
0 Bytes/Unlimited

Upload Report Storage Statistics Bandwidth Usage Team Folders Shared Objects Audit Trace File Change Logging Folder Permissions **Distributed Locks** Pending Purged Folders

0 Locked File(s) found REFRESH

File Owner	File Path	Locked By	Locked From	Type	Locked Time
No Lock Found					

Fig. 117: DISTRIBUTED LOCKS REPORT



ACME > TENANT DASHBOARD > REPORTS

0 Bytes/Unlimited

Upload Report Storage Statistics Bandwidth Usage Team Folders Shared Objects Audit Trace File Change Logging Folder Permissions Distributed Locks **Pending Purged Folders**

0 Versioned Folder(s) to be purged REFRESH

Folder Owner	Folder Name
No pending purged folders were found	

Fig. 118: PENDING PURGED FOLDER REPORT



### 5.1 Connect Your File Server

The way to connect the file servers are different, depending on where the file server is.

The file server can be sitting in the same Local Area Network (LAN) as the CentreStack Server. In this case, the direct network share connection is the best. Usually, this is combined with setting up a direct LDAP connection to the Active Directory.

The file server can also be remote, away from the CentreStack server and at the customer's premise. In this case, the best is to use a file server agent. File server agent will be installed on the file server, and it is capable of connecting the customer's Active Directory and syncing both folder content and active directory over HTTPS. In this case, in the user interface, you will see "Proxied AD User" to indicate that the Active Directory user or group is coming from the file server agent.

The best way to start using a file server agent to connect to a remote file server is to start with the migration wizard from the web portal.

### 5.2 Files and Folder Permission

If your files and folders are on a file server in the same Local Area Network (LAN) as the CentreStack server, the best way to manage file and folder permission is to delegate it 100% to the NTFS permission. In the "Storage Manager", when attaching local storage, there is an option "Always access the storage using logon user identity", This option can be used to delegate file/folder permission check directly to NTFS.

If you are not using native NTFS permission. For example, you are on cloud storage services such as Amazon S3 or OpenStack Swift, you can use CentreStack folder permission.

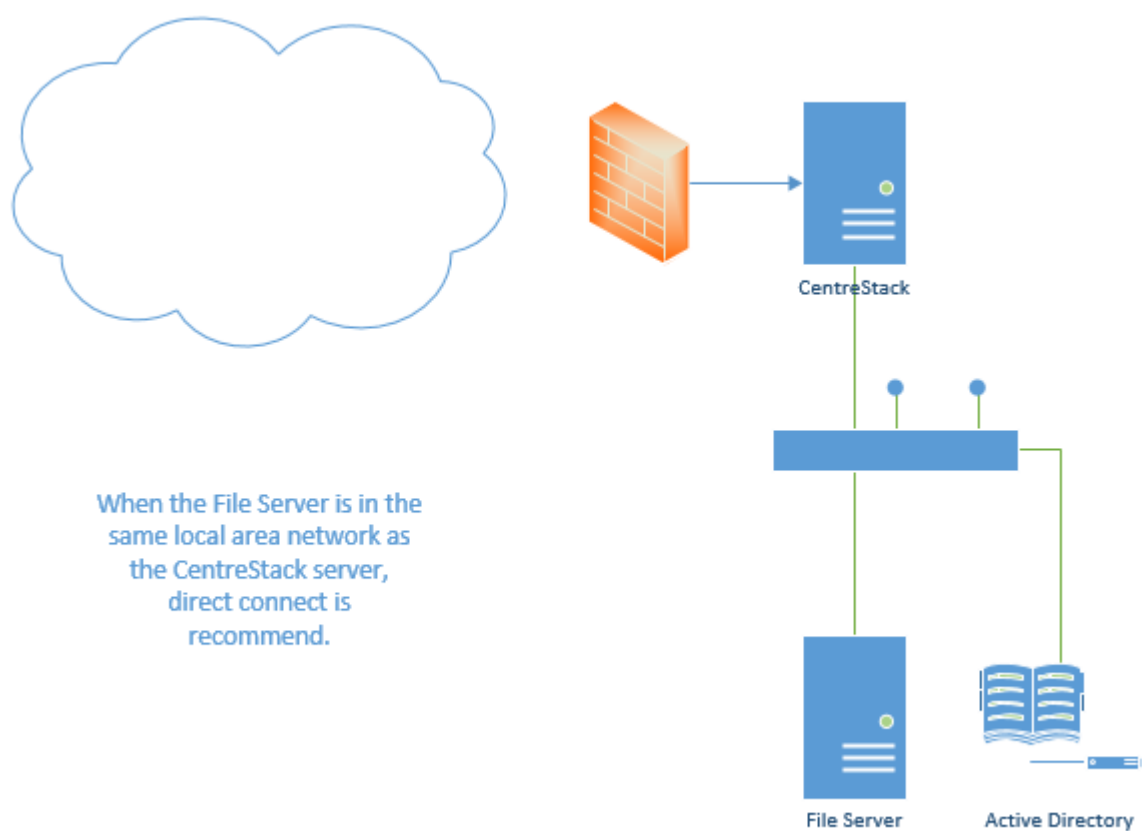


Fig. 1: FILE SERVER CONNECTION

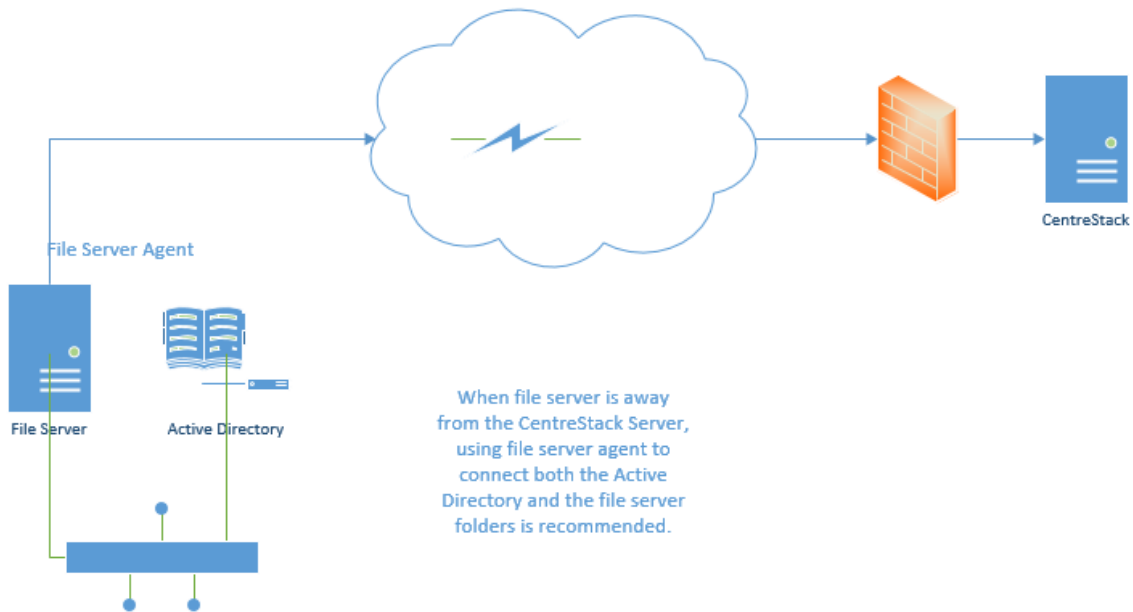


Fig. 2: SERVER AGENT CONNECTION

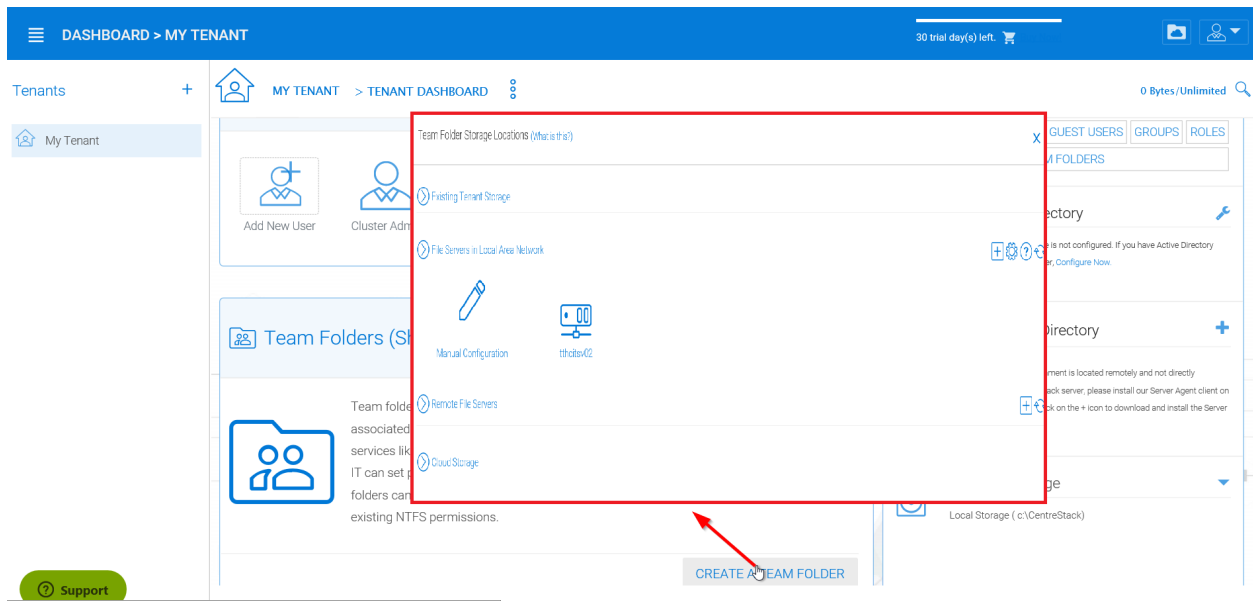


Fig. 3: TEAM FOLDER STORAGE LOCATIONS

☒ Always access the storage using logon user identity

The specified user will be used to verify the storage and will also be used to access the storage for the admin account. when above checkbox is checked, the storage will always be accessed using team-user's Active Directory identity when the storage is published as a team folder. Non-Active Directory user will access using the specified user account.

☐ The share is from a Linux/Unix/ZFS Server

☐ The share is a DFS share

☒ Enable Inplace Versioning

Fig. 4: FILE AND FOLDER PERMISSIONS SETTINGS

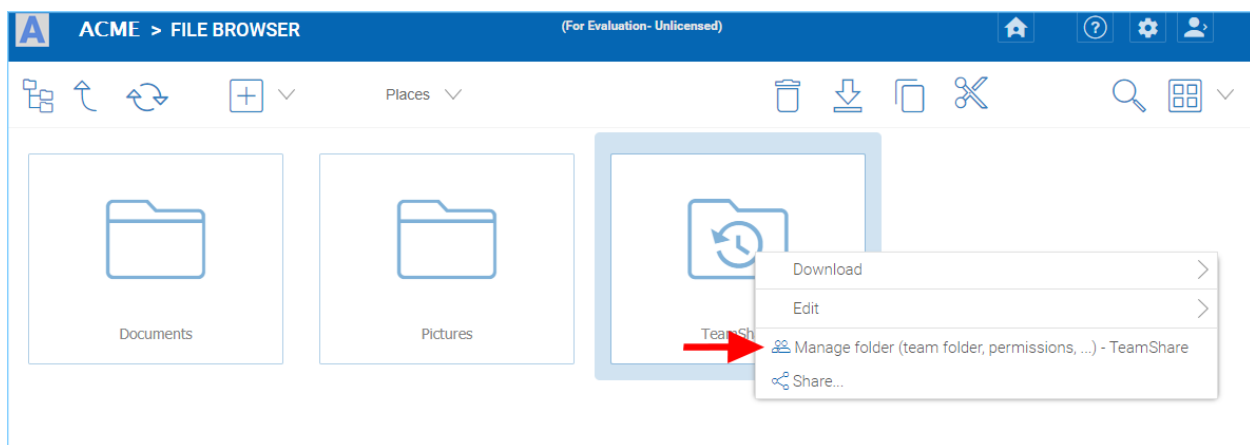


Fig. 5: MANAGE FOLDER SETTINGS

## 5.3 Setting up Active Directory

When the Active Directory is in the Local Area Network (LAN), LDAP can be used to connect to the Active Directory. There are several cases here,

- Sometimes you want the user account to be automatically provisioned so it is easy for the administrator.
- Sometimes you want the user account to be limited to a specific AD group, but still automatically provision the user's account when the users are in the AD group.
- Sometimes you want the user account to be limited to a specific Organization Unit.

### 5.3.1 AD account auto provision

This is the default setting in the Advanced -> Active Directory Settings.

As long as the “Don't allow user auto-creation” is not checked, Active Directory users will be allowed to go to the web portal and log in. The first time the user logs in, its CentreStack account will be automatically provisioned.

The screenshot shows the 'DASHBOARD > AD SETTINGS' page. The 'Advanced Settings' tab is selected. The 'Enable Active Directory Integration' checkbox is checked. The 'Domain Controller or LDAP Server Address (myhost:389)' is set to 'cstackdc1'. The 'User name (used to connect)' and 'Password' fields are present. A red box highlights the 'Don't allow user auto-creation' checkbox, which is currently unchecked. A red arrow points to this checkbox from the 'Advanced Settings' tab label.

AD Server Advanced Settings

☒ Enable Active Directory Integration

Domain Controller or LDAP Server Address (myhost:389) cstackdc1

User name (used to connect)

Password:

Friendly Domain Name (i.e. mydomain.com, the domain name you see in Active Directory tools) cstack.local

☐ Enable LDAPS for secure access

Only include users and groups from the following Organizational Units (e.g. OU=ou1,OU=ou2. Leave this blank to include all OUs)

☐ Allow Switching to Global Catalog If needed

☐ Disable Nested Groups (Enabling it may slow down your access to cloud)

☐ This is the root of the AD Forest and contains multiple sub-domains(☐ Discover domain controller IP at runtime)

☐ Don't allow user auto-creation

☐ Publish user's home drive

When unchecked, the user home drive space will be allocated from enterprise storage. When checked, existing user home drives will be automatically published from Active Directory.

Fig. 6: USER AUTO-CREATION SETTING

### 5.3.2 AD account auto provision, limiting to Organization Unit

The organization unit field can be used to further limit the Active Directory user account that can be automatically provisioned.

The screenshot shows the 'DASHBOARD > AD SETTINGS' interface. The 'Advanced Settings' tab is selected. The 'Enable Active Directory Integration' checkbox is checked. The 'Domain Controller or LDAP Server Address (myhost:389)' is set to 'cstackdc1'. The 'User name (used to connect)' and 'Password' fields are present. A red box highlights the 'Only include users and groups from the following Organizational Units (e.g. OU=ou1,OU=ou2. Leave this blank to include all OUs)' field, with a red arrow pointing to it from the left. Another red arrow points from the 'AD Server' tab to the 'Advanced Settings' tab. Other settings include 'Friendly Domain Name (i.e. mydomain.com, the domain name you see in Active Directory tools)' set to 'cstack.local', 'Enable LDAPS for secure access' (unchecked), 'Allow Switching to Global Catalog If needed' (unchecked), 'Disable Nested Groups (Enabling it may slow down your access to cloud)' (unchecked), 'This is the root of the AD Forest and contains multiple sub-domains (Discover domain controller IP at runtime)' (unchecked), 'Don't allow user auto-creation' (unchecked), and 'Publish user's home drive' (unchecked). A note at the bottom states: 'When unchecked, the user home drive space will be allocated from enterprise storage. When checked, existing user home drives will be automatically published from Active Directory.'

Fig. 7: LIMIT TO ORGANIZATION UNIT SETTING

The format of the organization unit is the OU's distinguishedName minus the DC suffix.

For example, the following OU's property is: distinguishedName => OU=tenant11,DC=tsys,DC=gladinet,DC=com when it is put into the OU field, the DC suffix can be removed so only OU=tenant11 is required.

**Note:** OU=tenant11

### 5.3.3 AD account auto provision, limiting to a specific AD group.

From the user manager, you can import the AD group and the users in the AD group will be able to get the account automatically provisioned.

Here is a demo video for Import AD group.

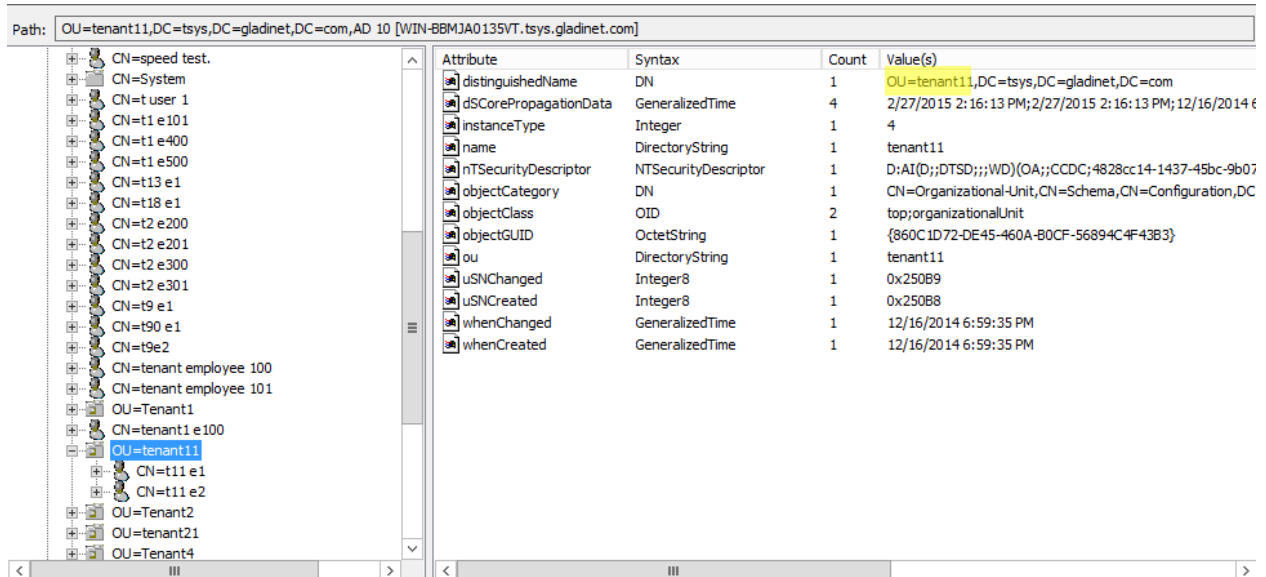


Fig. 8: OU PROPERTY LOCATION

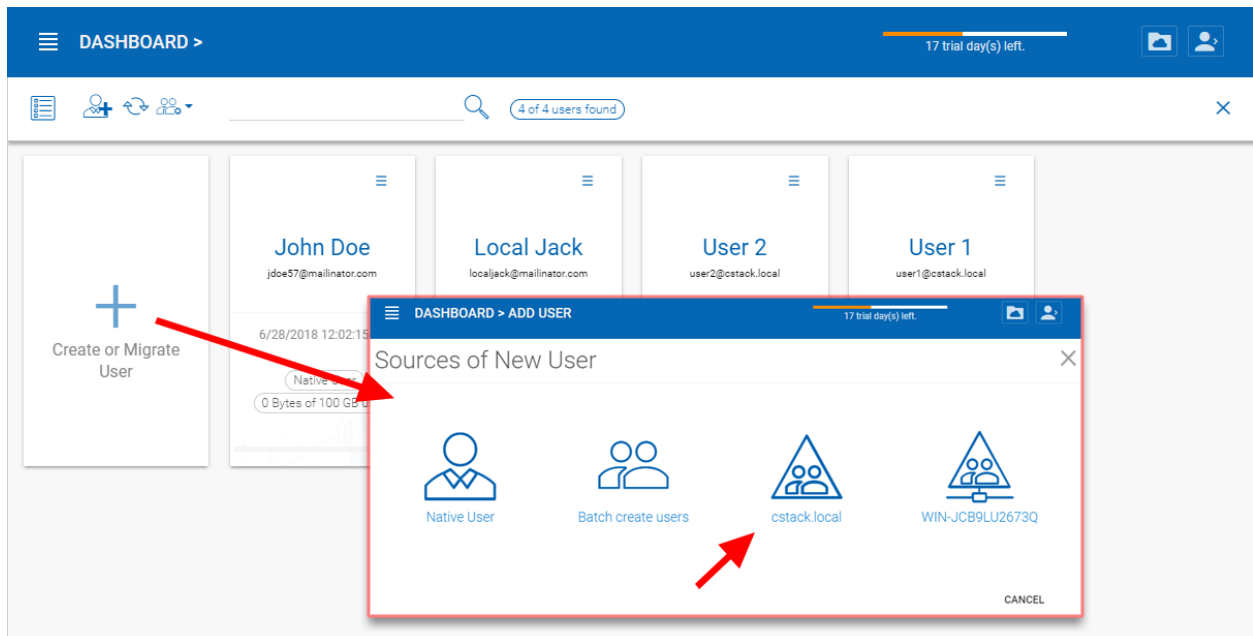


Fig. 9: MIGRATING USERS FROM ACTIVE DIRECTORY

## 5.4 Setting up Offline Folder

In a team collaboration environment, there are several best practices related to offline folder management.

Here are several parameters for consideration:

### 5.4.1 Team Folder Offline Settings

If you have a big team folder or several team folders that are quite big, it is not a good practice to enable the team folder offline from the root. Instead, you can choose not to enable offline or just enable a subset of sub-folders that are relatively small and at the same time, used more often. If you want to enable a subset of sub-folders within team folders for offline access, you can start by going to the folder permission section. You can access this by selecting the folder (1), in the pulldown menu (2) select “Folder Permissions”, then select the edit settings icon (3) and finally select “Enable offline access for native Client” (4), and apply the change.

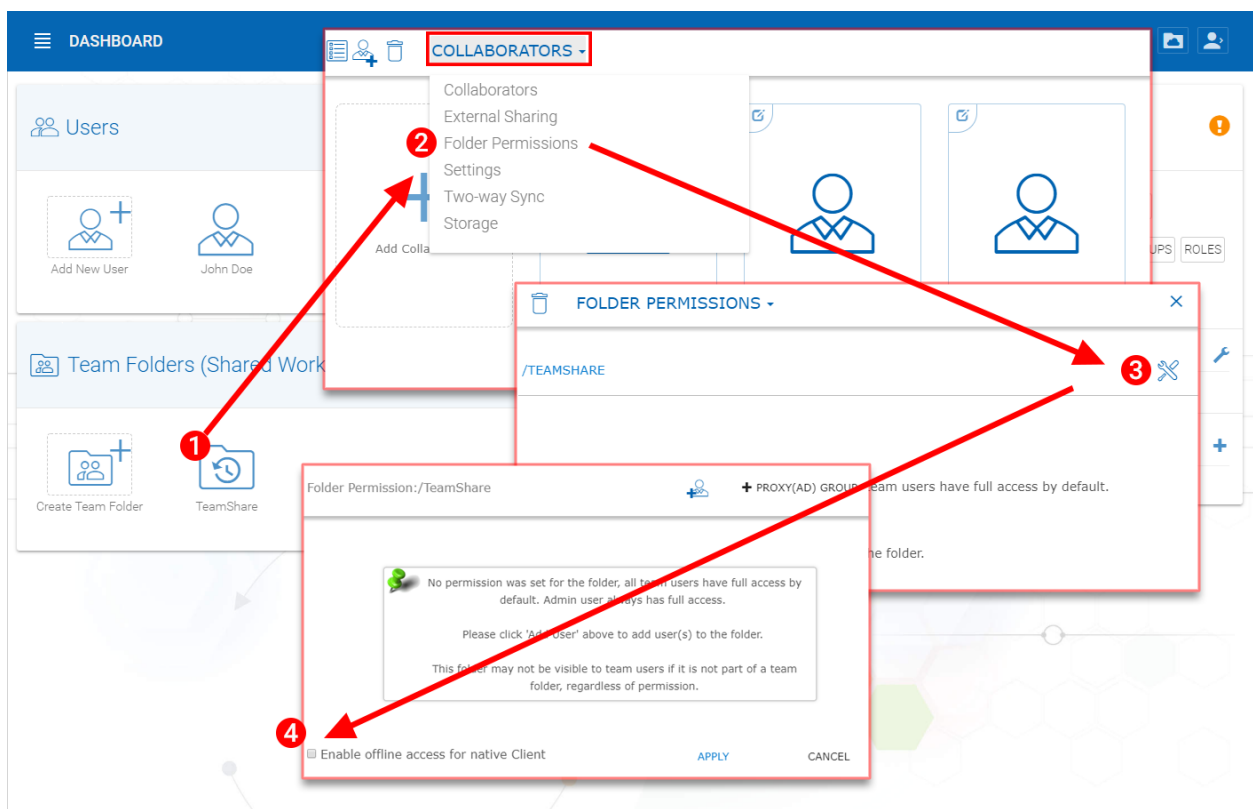


Fig. 10: ENABLING OFFLINE ACCESS FOR NATIVE CLIENT

If you want to disable offline access for the team folder completely, you can change the setting from the Team Folder section by choosing the “Settings” option below (1) in the drop-down menu and selecting the “Disable Offline Access” option (2). Don’t forget to save your changes (3).

### 5.4.2 User Offline Settings

Upon creating users in the CentreStack system (including users imported from Active Directory), there is an offline flag upon user creation.



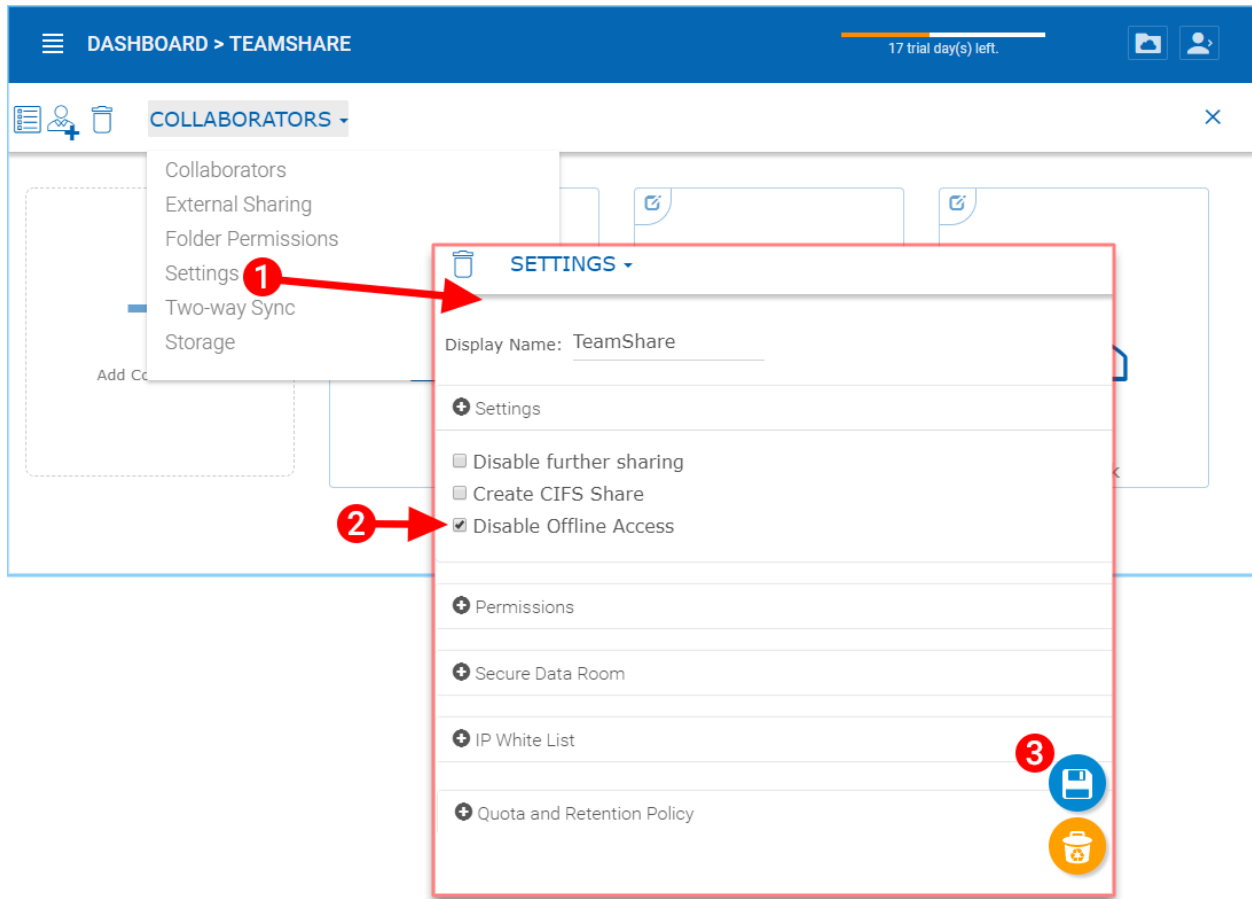


Fig. 11: DISABLING OFFLINE ACCESS FOR TEAMSHARE

Normally, we don't recommend checking the "Enable offline access for all folders" flag, because it will try to download every single file for the user when the user is connected, which can use a lot of bandwidth and slow things down.

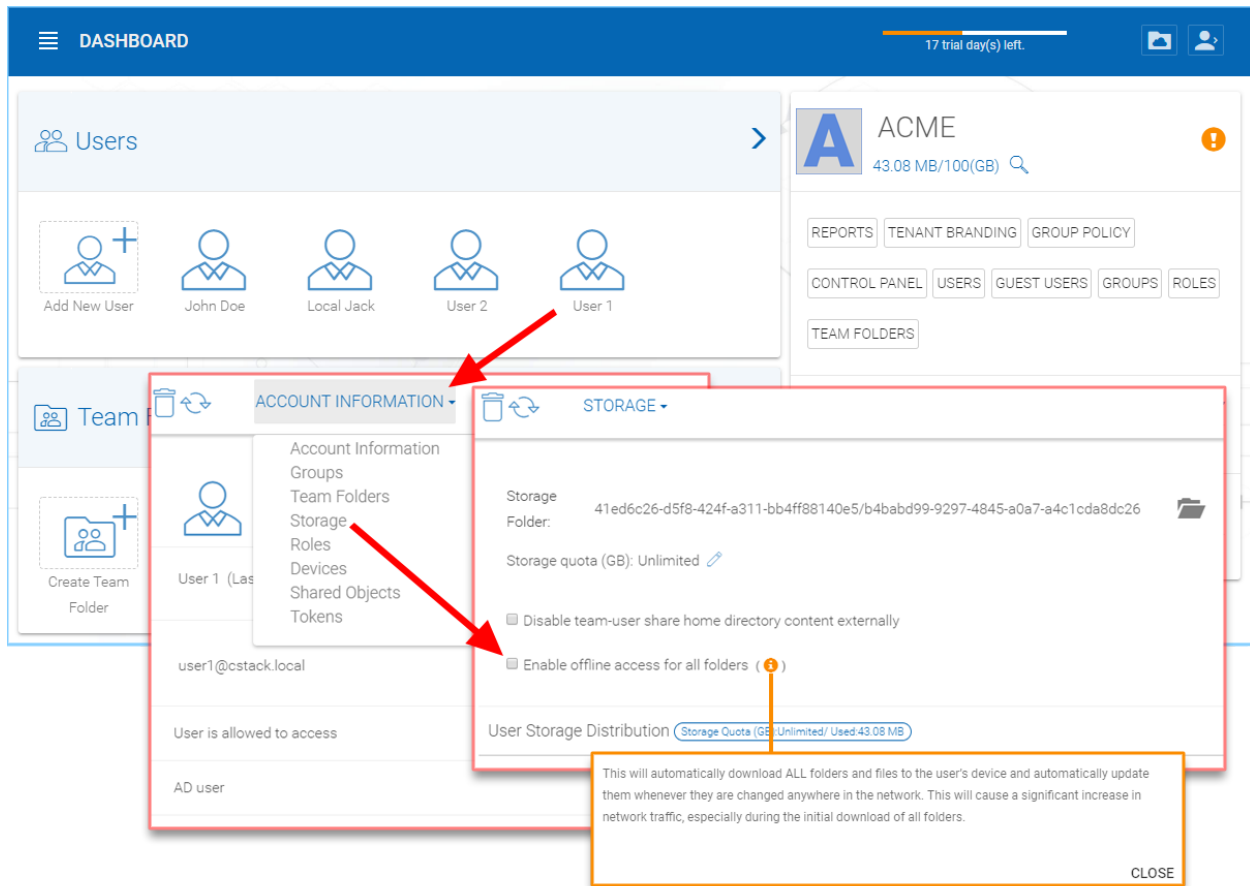


Fig. 12: ENABLING PER-USER OFFLINE ACCESS

**Note:** This will automatically download ALL folders and files to the user's device and automatically update them whenever they have changed anywhere in the network. This will cause a significant increase in network traffic, especially during the initial download of all folders.

Without it, the user can still pick and choose which folder to mark as offline.

### 5.4.3 User Manual Offline Settings

During regular usage of the files and folders, users can mark folders as offline.

### 5.4.4 Summary

Administrators can manage the tenant-wide offline policy related to team folders and users. In the case where team folder size is small and user size is small, an administrator can enable the offline flag to push files and folders to user's devices.

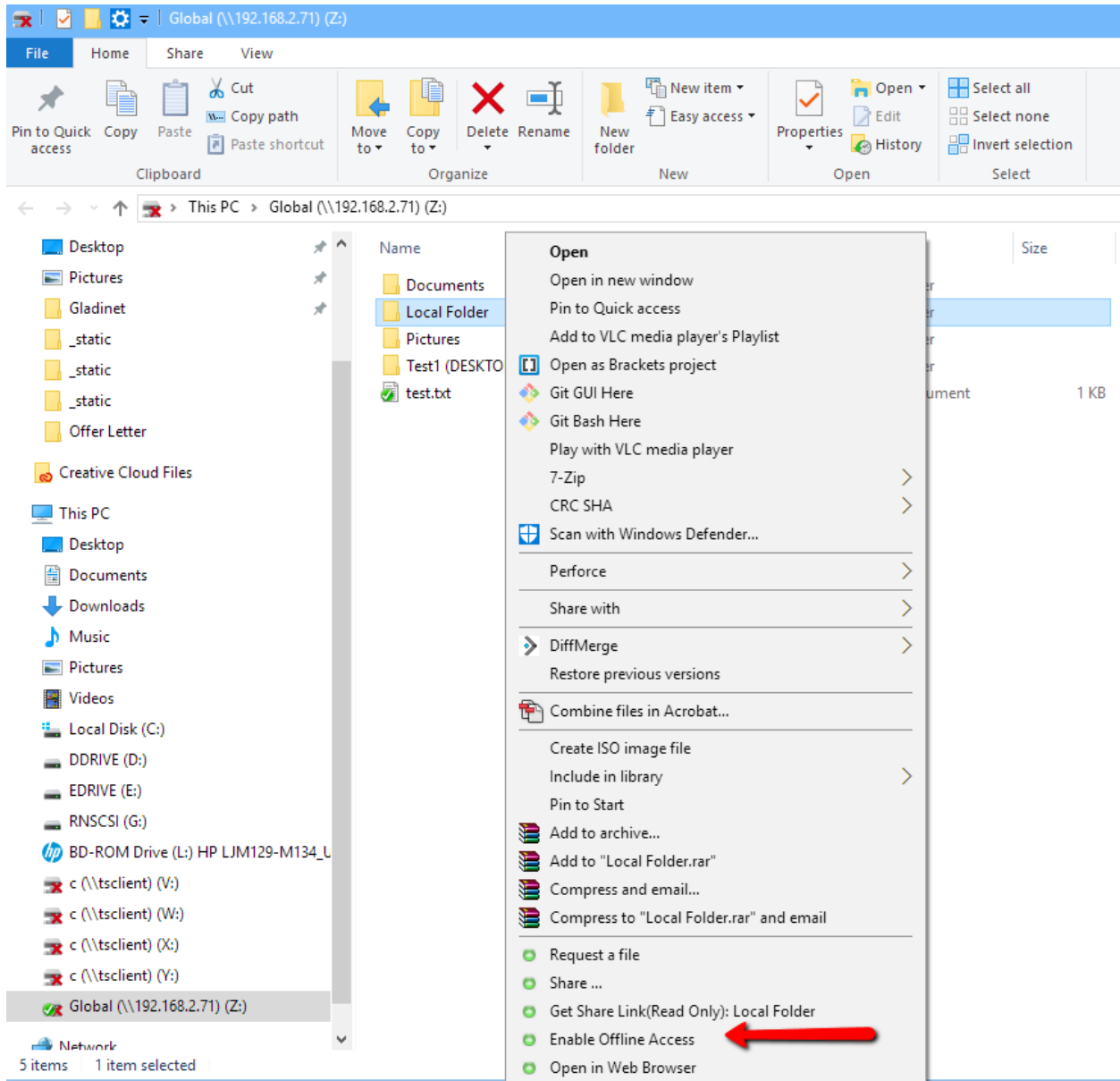


Fig. 13: ENABLE OFFLINE ACCESS AT THE CLIENT LEVEL

However, in the case where the team folder size is big and the user number is not small, we recommend the administrator enables as few offline flags/settings as possible on the administration side. Users can still do offline management themselves within their working folder on a case-by-case basis.

## CHAPTER 6

---

### Cloud Backup

---

---

**Note:** CentreStack's Cloud Backup allows you to turn your CentreStack server into a backup appliance or create a self-hosted backup solution with the ability to backup endpoints and restore folder permissions.

---

In this section, we'll review how to enable backup for file shares and endpoint devices and review how the files in the backup can be accessed and restored.

#### Enabling Cloud Backup

Cloud Backup is enabled on a cluster-wide basis. Instead of purchasing an expensive backup appliance, your CentreStack server will assume the role of the virtual appliance, allowing you to create your self-hosted backup service or leverage CentreStack's hosted environment to secure the offsite copies of your data.

#### Backing Up File Shares

You can backup file shares from the local file server using your CentreStack server as a conduit to CentreStack's backup cloud, or you can define your cloud backup target if you'd like to some other storage service.

#### Backing Up Endpoint Devices

Folders and file shares on remote PCs and servers will be backed up using the existing CentreStack agents to take advantage of existing HTTPS/SSL connections that have been rigorously architected to maintain connectivity and reliability.

#### Cloud Backup Access and Restore

Easily restore any files and folders or access them directly. For example, when you backup files and folders to CentreStack's backup cloud, they can also be accessed directly from <https://backup.centrestack.com>

The following data flow illustrates how the basic architecture functions for this solution.

---

**Note:** Traditionally, enterprises use backup appliances on-premises to receive backup sources from servers and desktops around the company network. It is a very secure setup because the backup data sits inside the appliance.

---

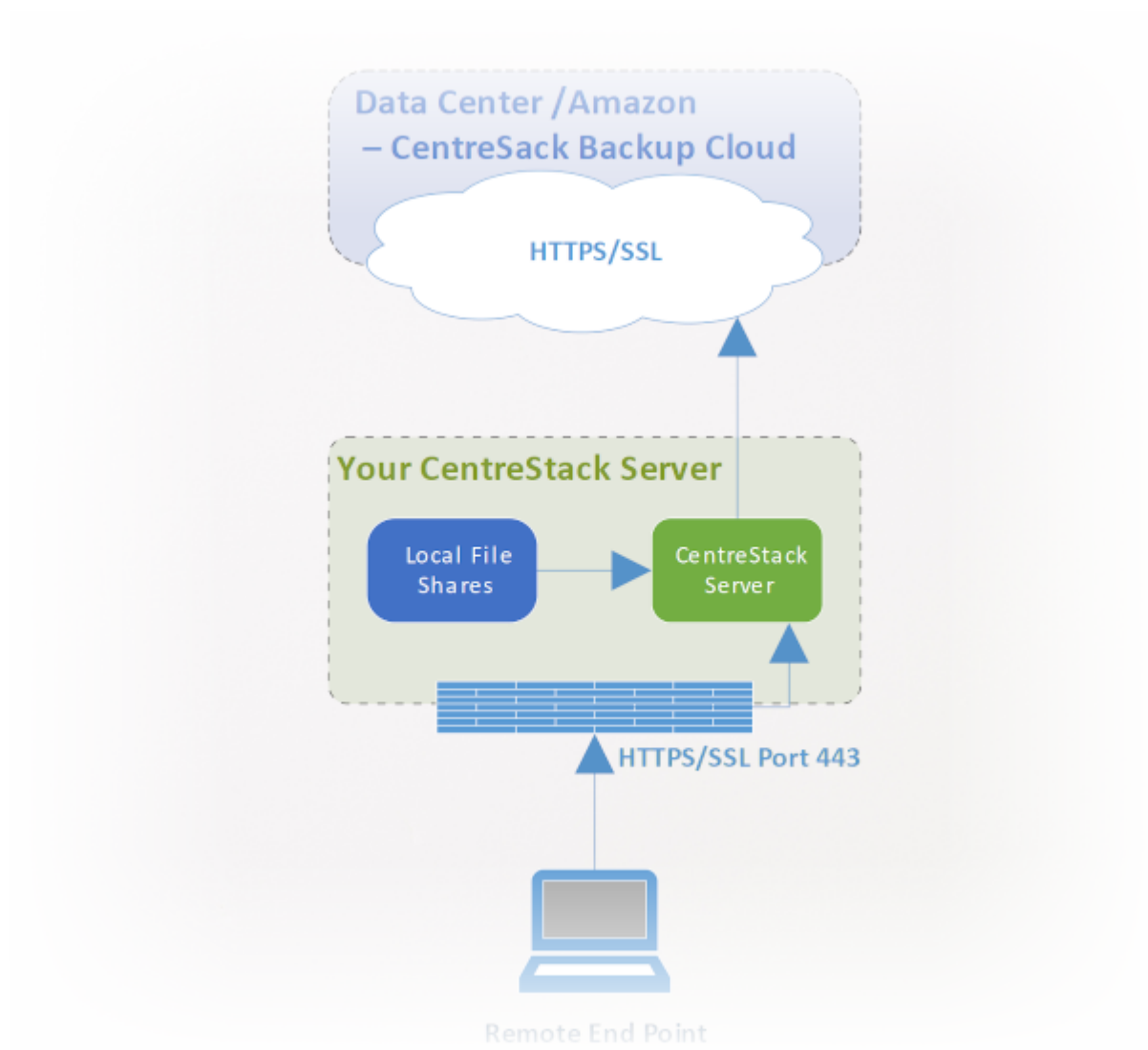


Fig. 1: CLOUD BACKUP ARCHITECTURE

However, it poses a challenge for remote devices because remote devices are not always inside the company network and the VPN (a virtual private network) from remote devices are not always on to observe certain backup schedules.

On the other hand, cloud backup solutions like Carbonite and CrashPlan can backup remote devices to the cloud directly, solving the problem for remote backup. However, the backup destination is in an opaque location, controlled by a 3rd party. This becomes problematic when there are business policies to prevent data replication to locations controlled by 3rd parties.

CentreStack cloud backup solves both these problems. First of all, the CentreStack server maintains connectivity with remote PCs and file servers via HTTPS/SSL so the connection is always on. This means that remote PCs and file servers can always leverage CentreStack's communication channel and data channel to back up through the CentreStack backup appliance. And since CentreStack's cloud backup is storage agnostic, allowing you to backup to a storage service under your control, you can now provide continuous backups of your file servers and endpoints to a storage service under your control, or the CentreStack defaults.

## 6.1 Enabling Cloud Backup

CentreStack Partner Portal > Backup Manager

Login to the partner portal from <https://centrestack.com>. On the dashboard, click 'Backup Manager' and select the CentreStack clusters you want to backup.

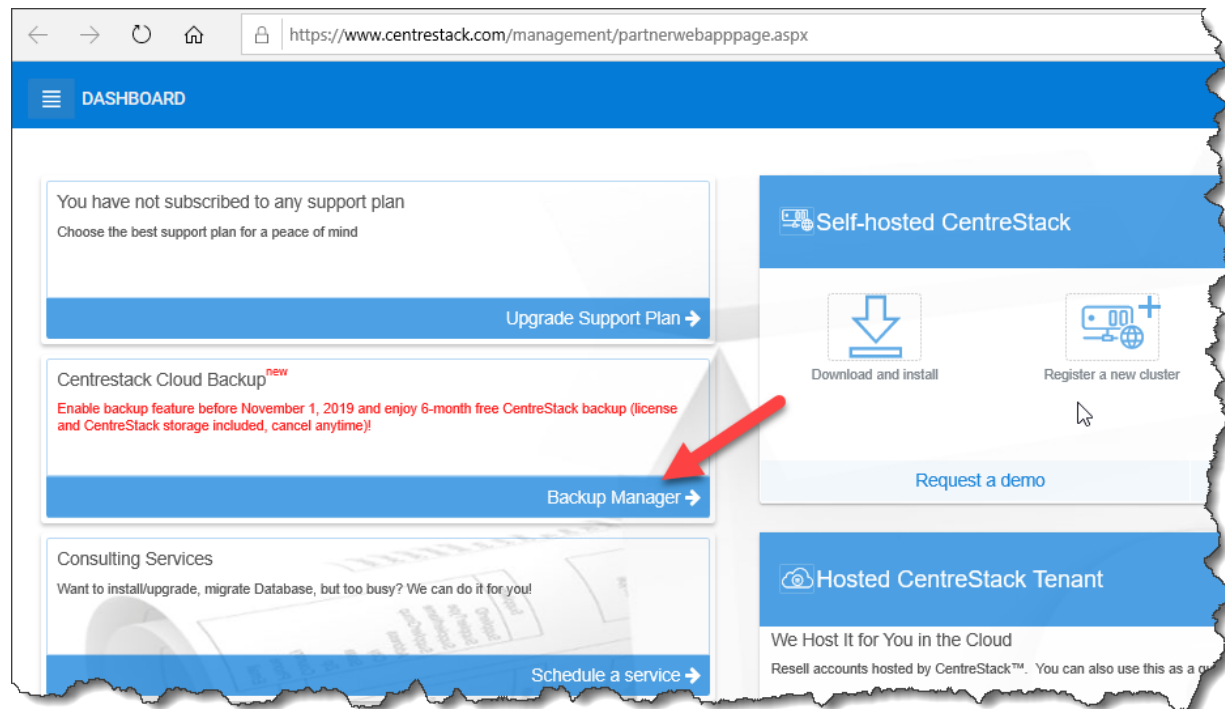
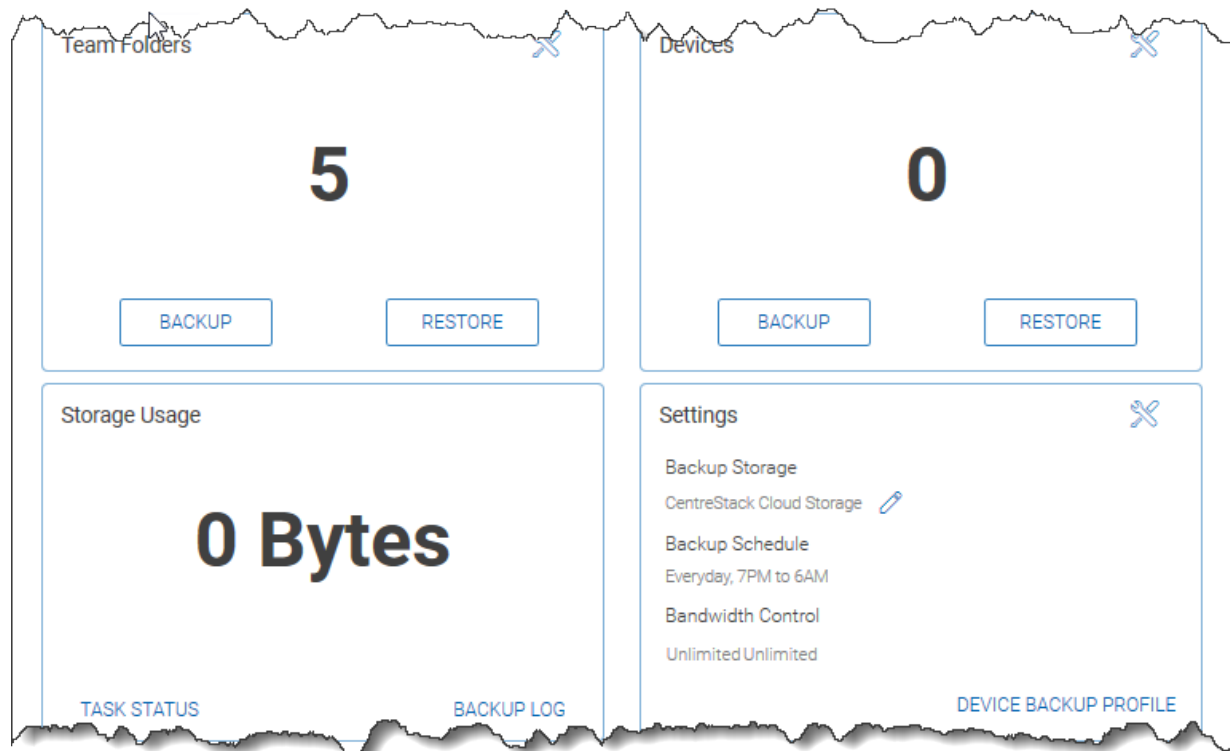
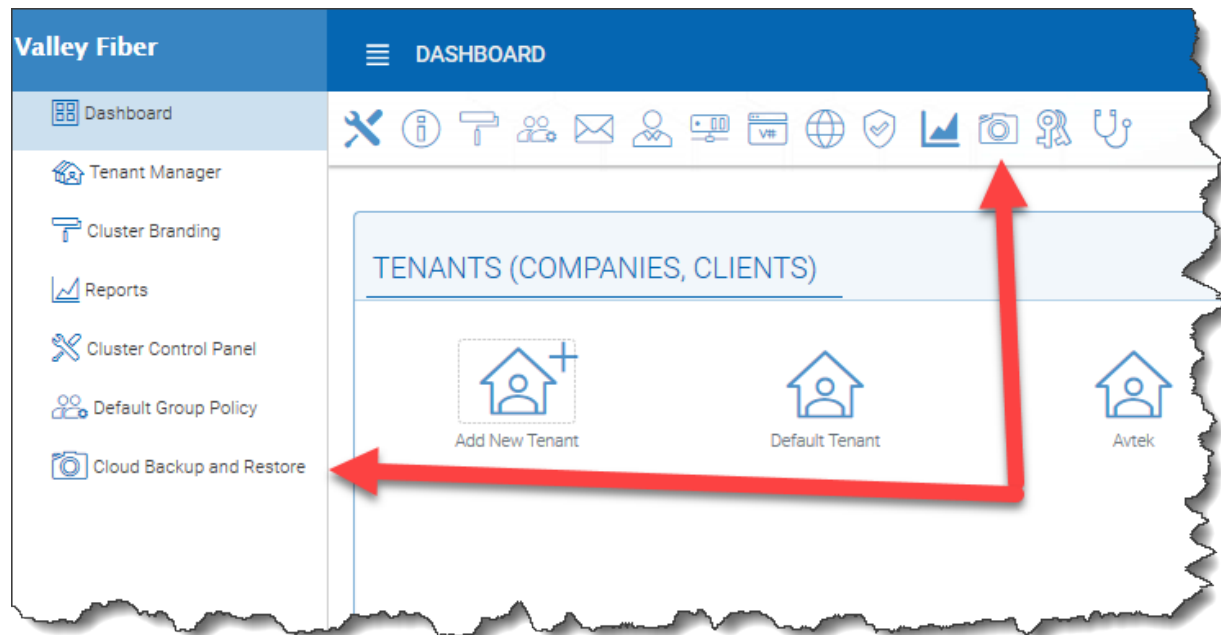


Fig. 2: ENABLING CLOUD BACKUP FROM PARTNER PORTAL

Once Cloud Backup has been enabled for the cluster, you can log in to the cluster management portal as the cluster-admin. Click on the 'Cloud Backup and Restore' icon in the top menu.

You should see the Cloud Backup Summary page.



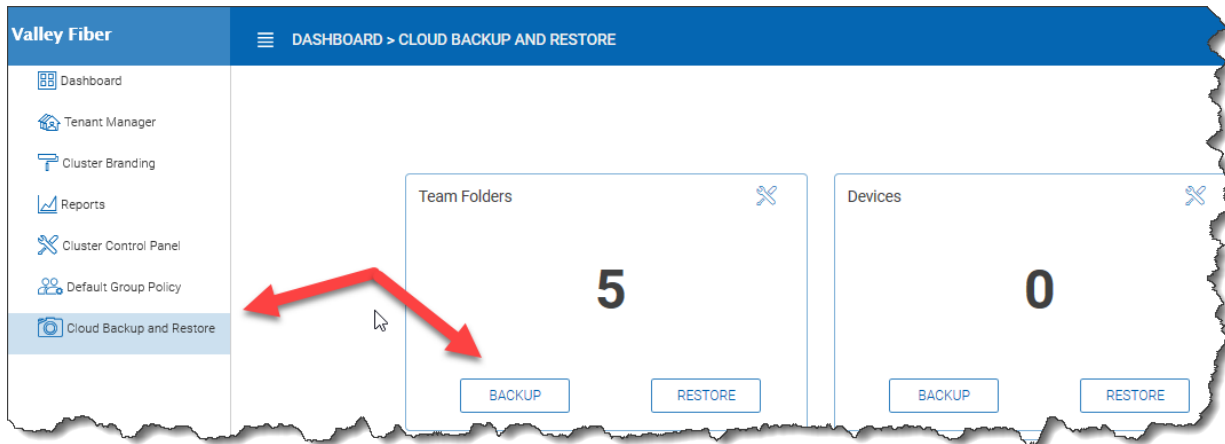


## 6.2 Cloud Backup for Team Folders

Cloud Backup works with any type of team folder, regardless of how they were created and can be initiated by the cluster-admin or tenant admin.

### 6.2.1 Enabling Cloud Backup for Team Folders

As a cluster administrator, go to the Dashboard of the Management Console and select 'Cloud Backup and Restore' from the left panel. Here you will see 'Team Folders' and 'Devices'.



Click on the 'BACKUP' button to see a list of team folders in the tenant which have not been backed up. Select the team folders to backup and then click 'BACKUP SELECTED'.

You can also follow this process as a cluster administrator but will first be prompted to select a tenant before seeing the list of team folders that haven't been configured for backup.

### 6.2.2 Cloud Backup Snapshots

Once enabled, Cloud Backup is stored in Snapshots. The snapshot must be initially seeded and new snapshots will be created to capture updates to the data set. Data can be restored from any snapshot.

#### Seeding a Snapshot

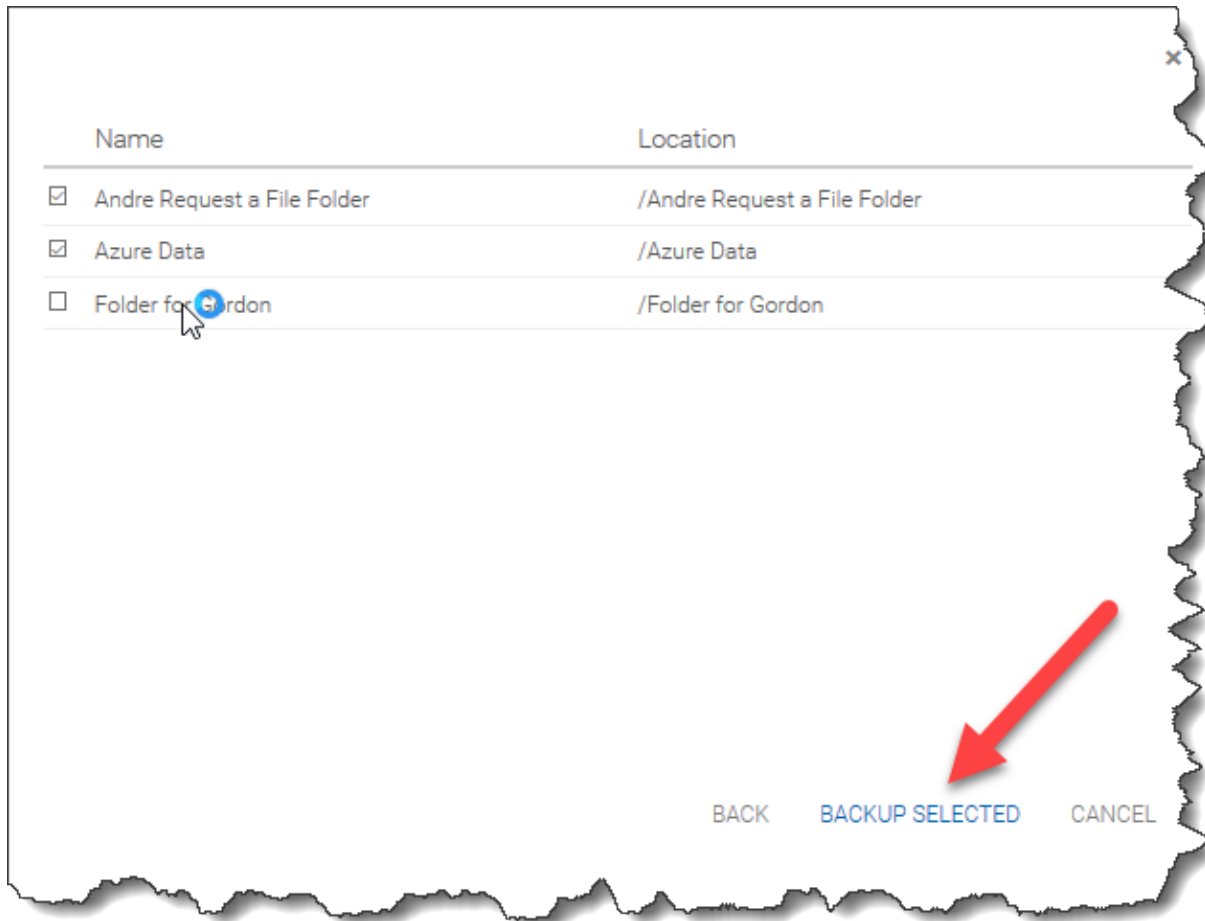
Click the 'Details' icon in 'Team Folders', select the team folder you'd like to restore, and click the detail icon. Click 'Force Initial Seeding Now':

#### Browsing a Snapshot

To browse a snapshot, click the icon that looks like an eye on the right side of the listed snapshot. You can then navigate through the folder hierarchy in the snapshot to download and restore files and folders using the action icons at the top left of the page. Checkboxes are provided to filter the list of objects that action will be applied to:

#### Downloading and Restoring from a Snapshot

For example, in the image below, you can click the highlighted icon to restore the selected items:



First select a tenant (who owns a team folder to backup)



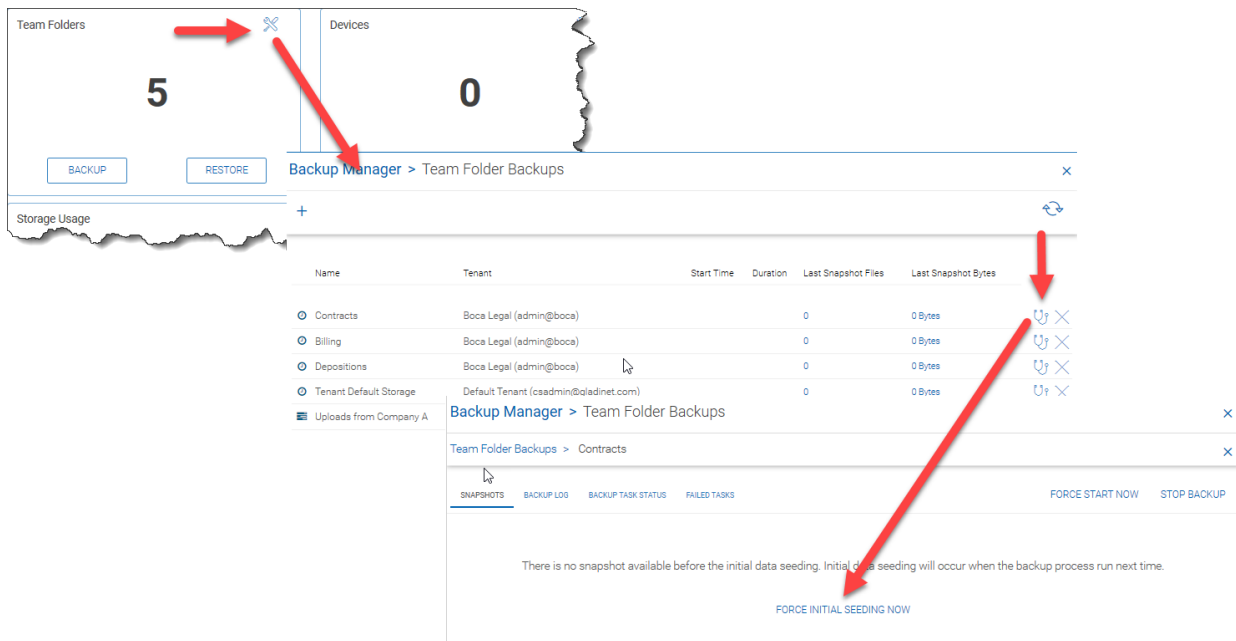


Fig. 3: SEEDING A BACKUP SNAPSHOT

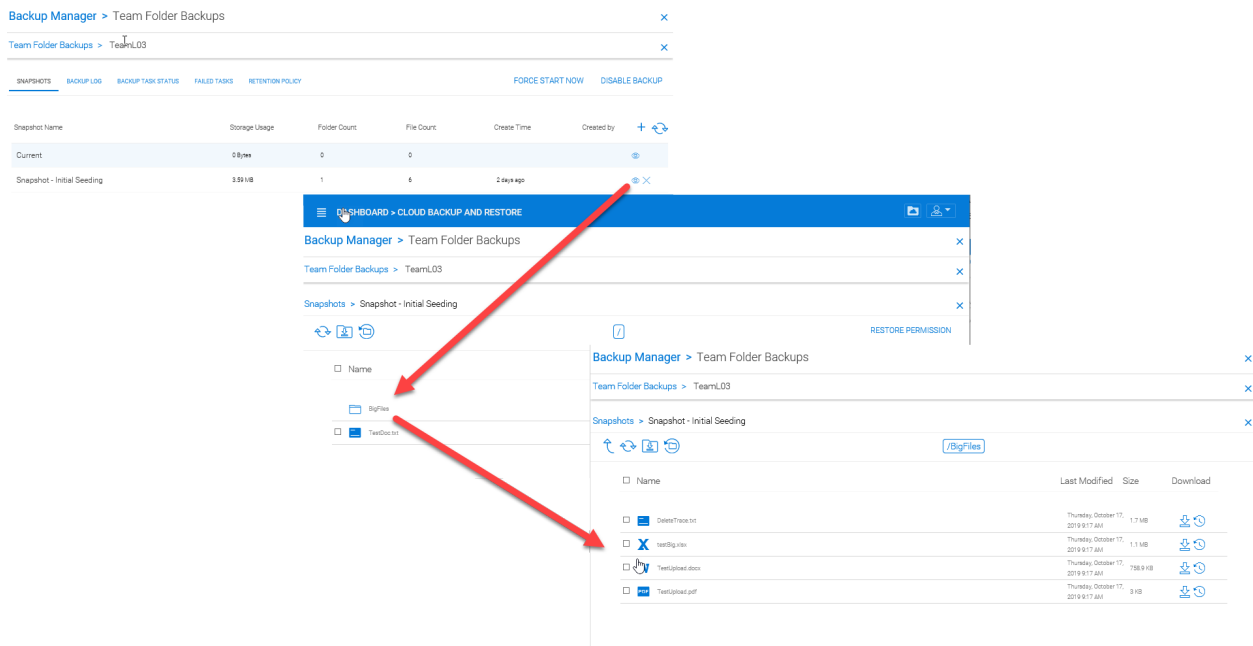


Fig. 4: BROWSING A BACKUP SNAPSHOT

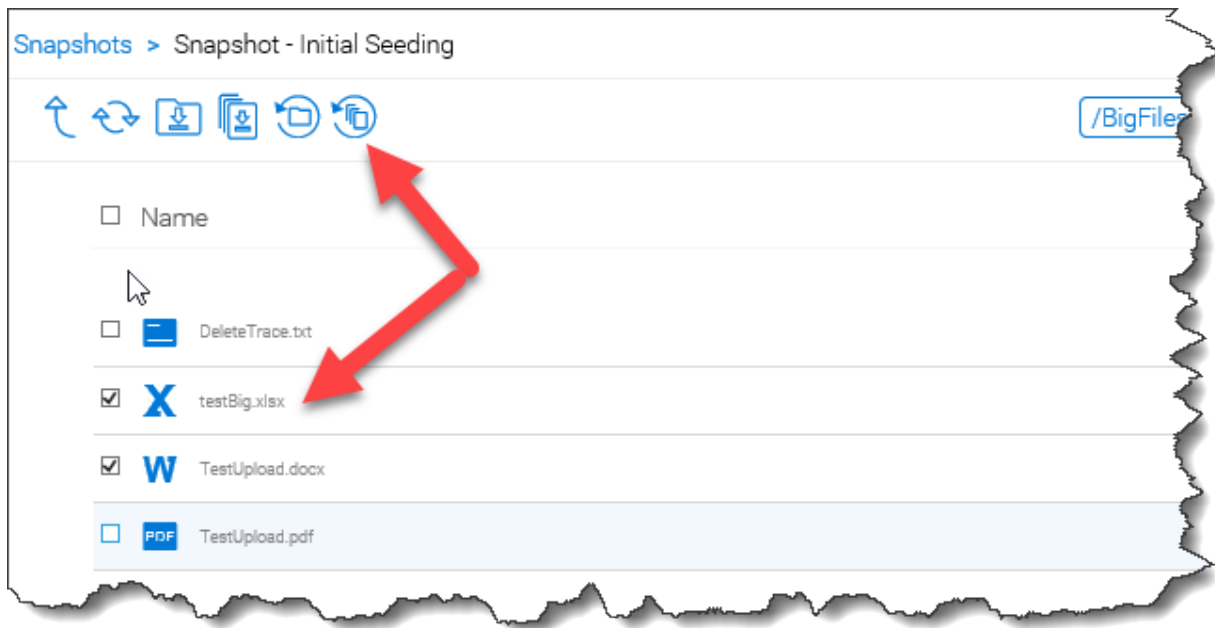


Fig. 5: RESTORING FROM A BACKUP SNAPSHOT

### 6.2.3 Disabling Cloud Backup for Team Folders

To disable Cloud Backup for a team folder, simply click the 'X' beside its backup listing:

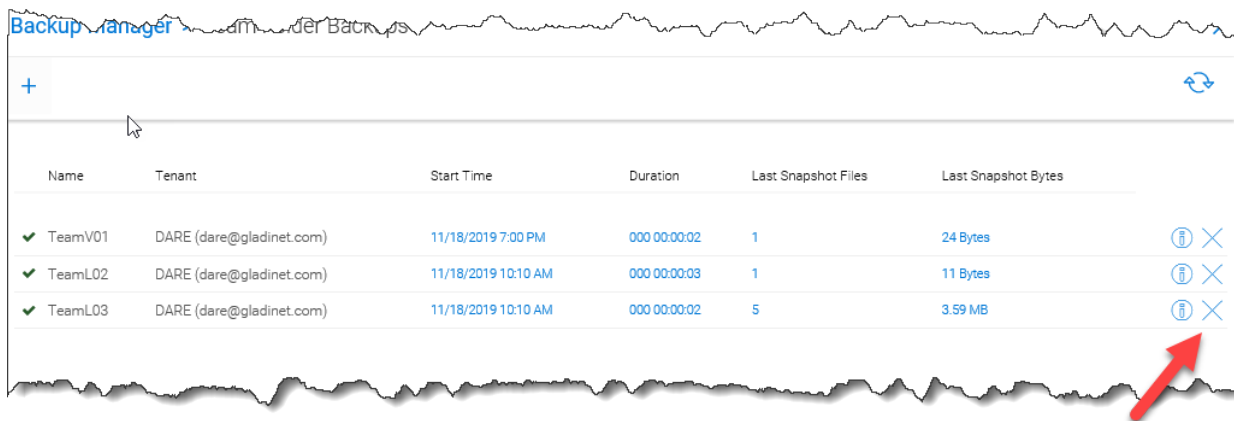


Fig. 6: DISABLING CLOUD BACKUP FOR A TEAM FOLDER

## 6.3 Cloud Backup for Endpoint Devices

Before an endpoint can be backed up, a backup profile must be created. This profile specifies which folders need to be backed up on each endpoint device. In this section, we'll review how to create backup profiles, assign them to devices and manage the resulting backups and restores.

### 6.3.1 Create a Device Backup Profile

Cluster Management Console > Cloud Backup and Restore

As the cluster-admin on the web portal, go to 'Cloud Backup and Restore'. Under 'Settings', click 'Device Backup Profile' and then open the profile list. Click 'Add' to create a new backup profile.

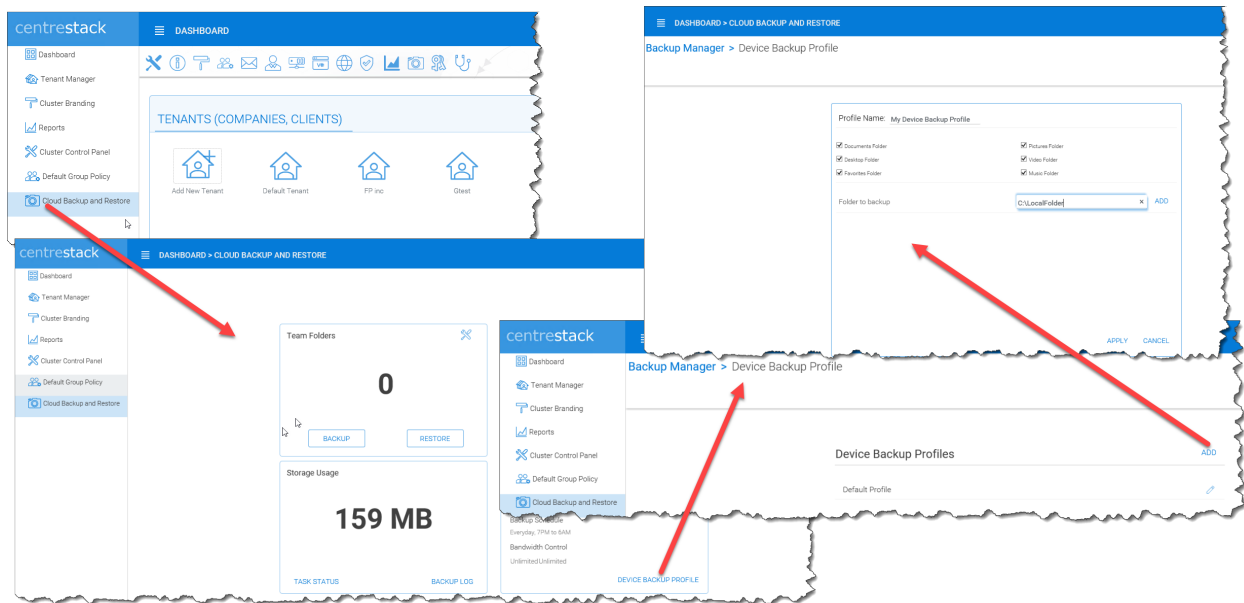


Fig. 7: CREATE BACKUP PROFILE

Use the backup profile to select which of the pre-defined folders need to be backed up on each device. These include Documents, a Desktop, Favorites, and Pictures. Any folder can be added to the profile by entering its path under 'Folder to backup' and clicking 'ADD':

### 6.3.2 Configure Devices for Backup

Cluster Management Console > Cloud Backup and Restore

As the cluster-admin on the web portal, go to 'Cloud Backup and Restore'. Click 'Backup' under 'Devices'.

Click on the 'Search by:' dropdown list to find the device(s) you want to backup:

---

**Note:** You could alternatively enumerate by devices by selecting 'Status' and searching for all accepted devices.

---

After selecting the backup device, you'll see that the number of device backups has now increased by 1.

### 6.3.3 Restoring from Device Backups

Cluster Management Console > Cloud Backup and Restore

As the cluster admin on the web portal, go to 'Cloud Backup and Restore'. Click 'Restore' under 'Devices'.

Click on the 'Search by:' dropdown list to find the device(s) you want to backup:

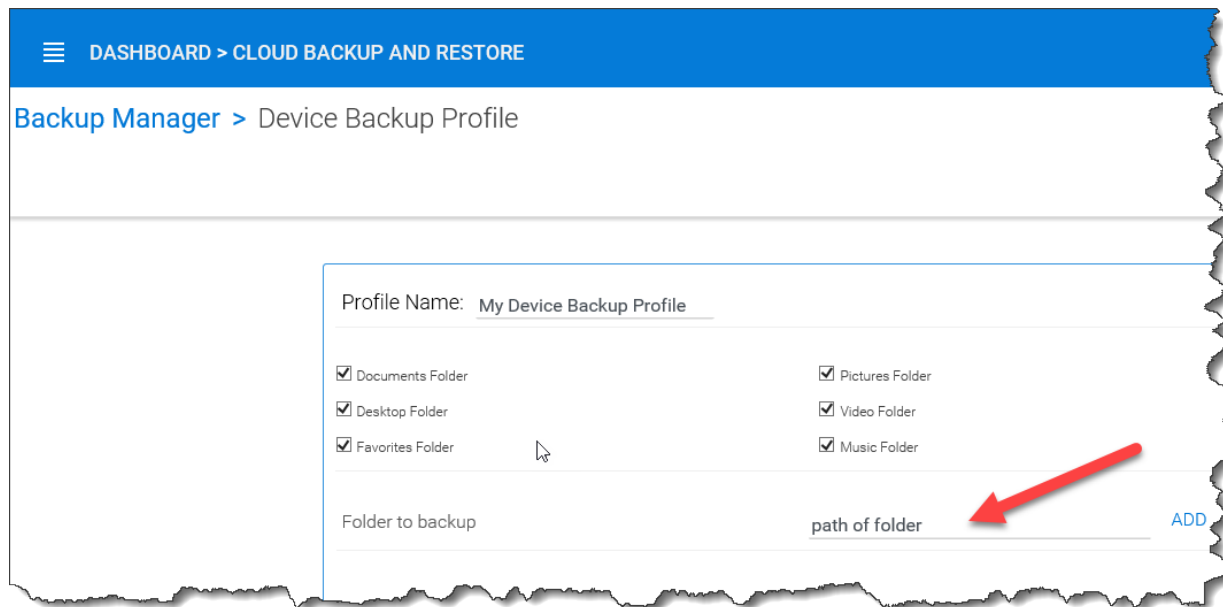


Fig. 8: SELECT FOLDERS FOR BACKUP

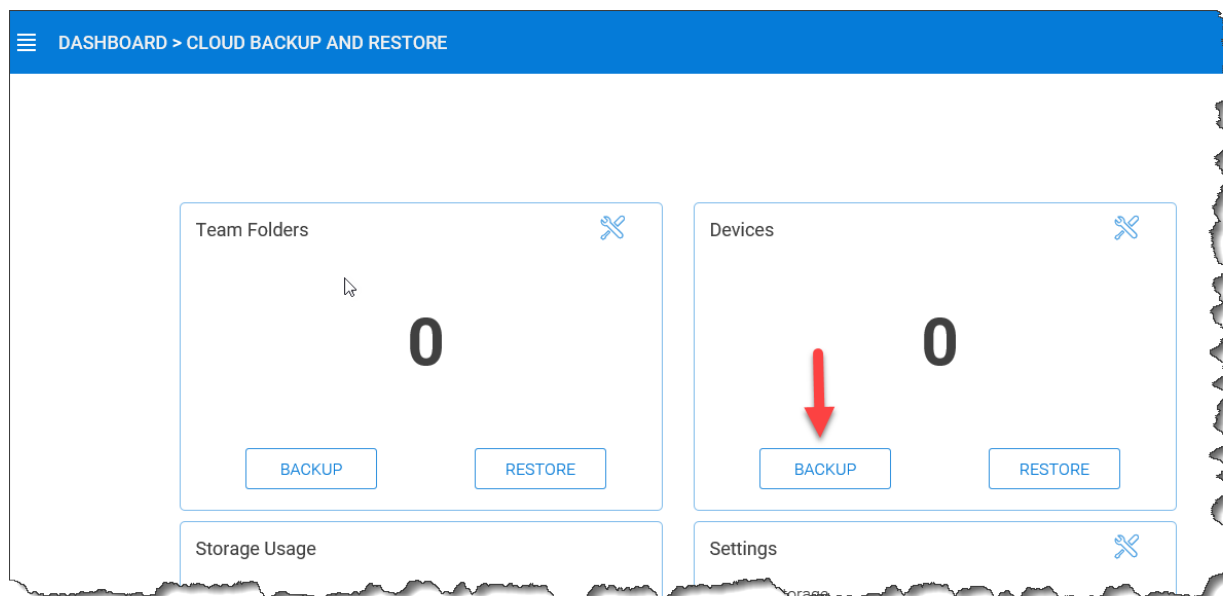


Fig. 9: SELECT BACKUP DEVICES

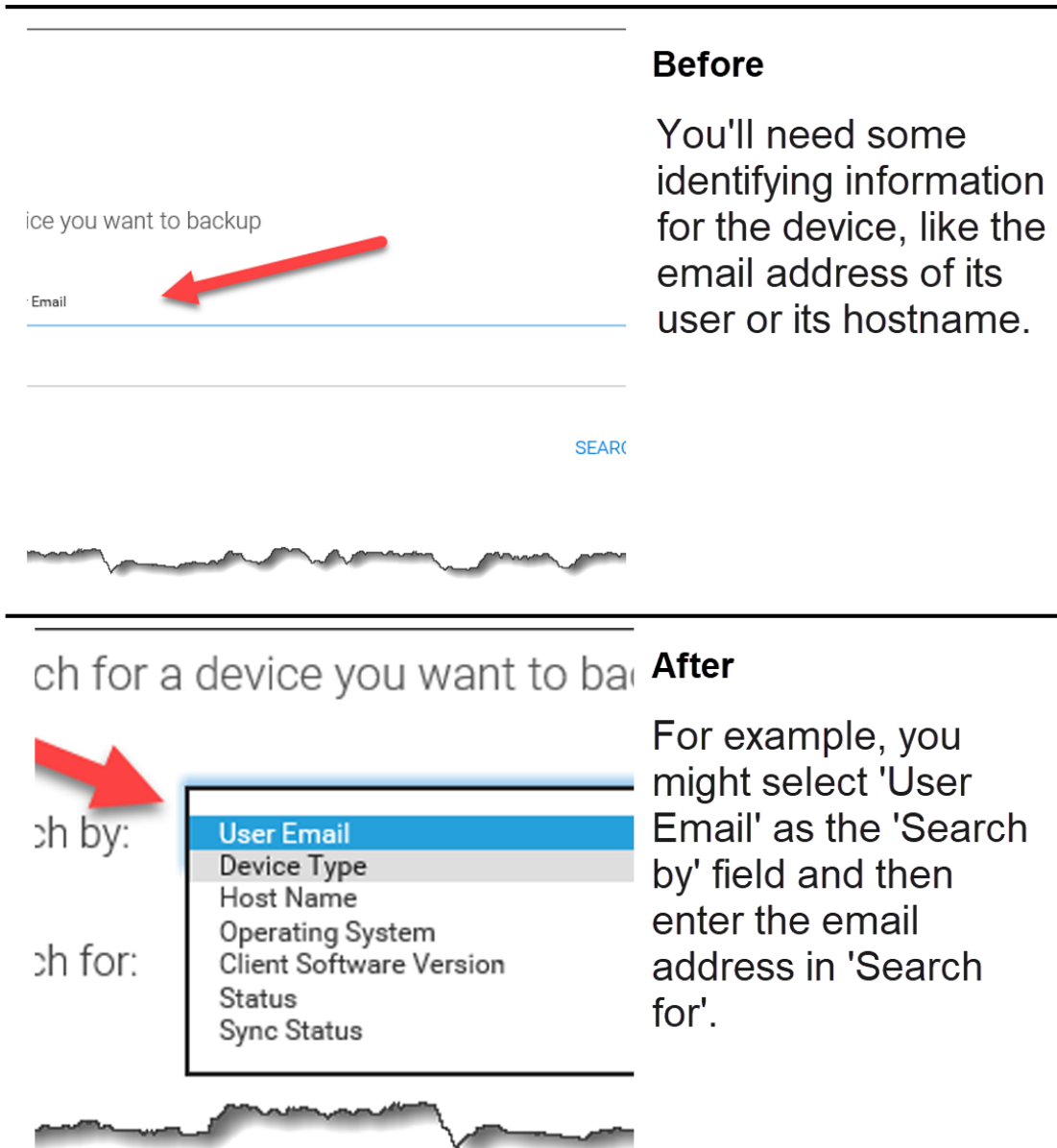


Fig. 10: FIND BACKUP DEVICES

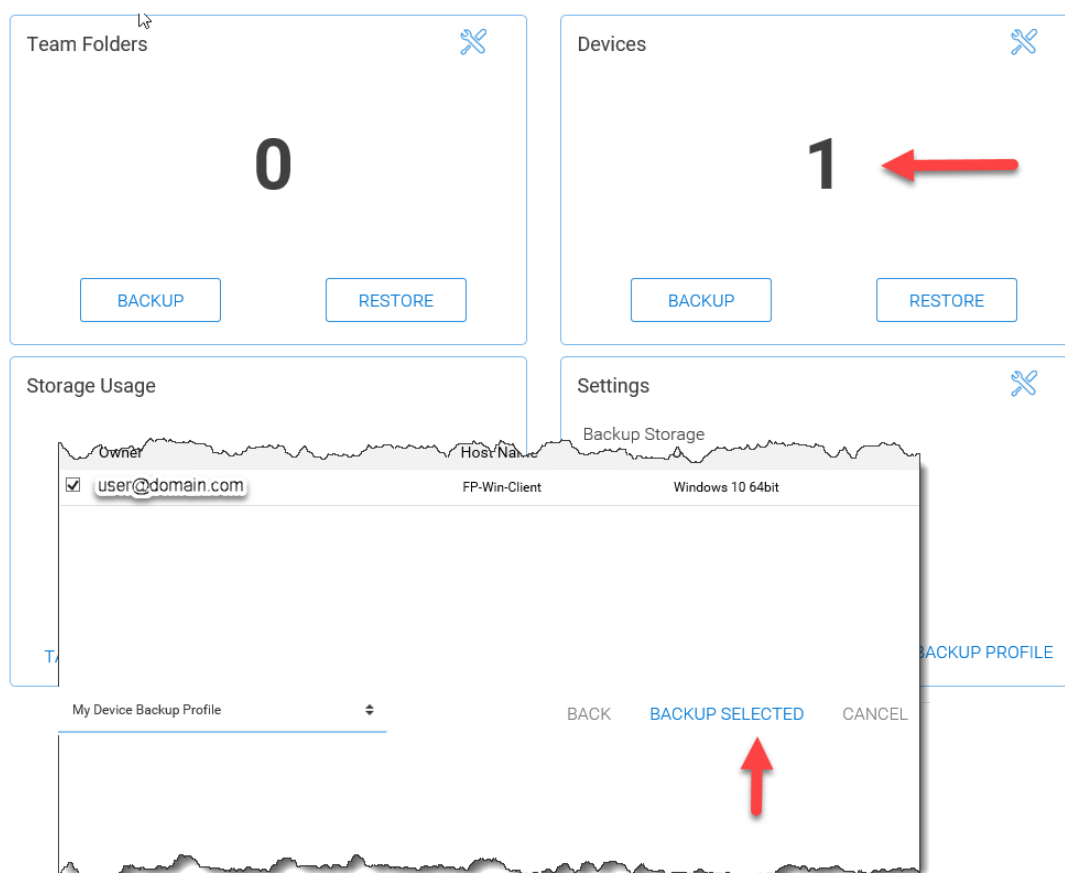


Fig. 11: DEVICES ADDED



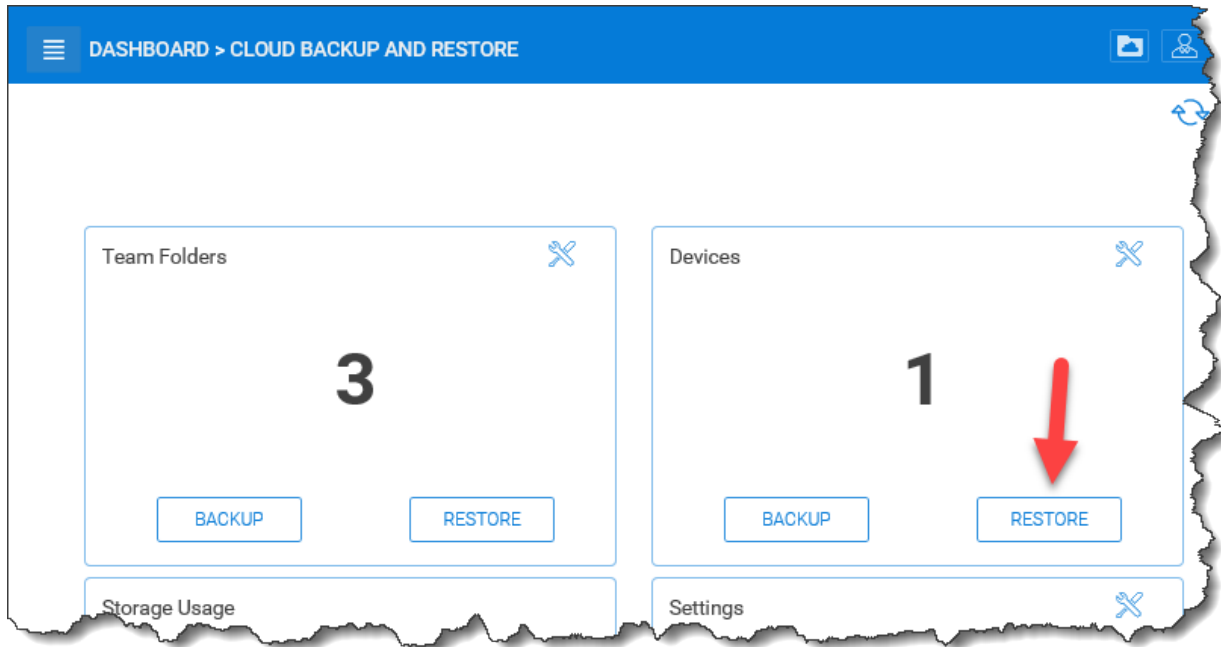


Fig. 12: RESTORE BACKUP DEVICES

---

**Note:** You could alternatively enumerate by devices by selecting ‘Status’ and searching for all accepted devices.

---

After selecting the backup device, you’ll see two options, ‘Local’ and ‘Cloud’.

CentreStack implements Cloud Backup for endpoint devices by first syncing the device to a special team folder and then backing up that team folder to the CentreStack backup cloud. So you have the option of restoring the device from the team folder, which is stored locally on the backend storage for the tenant, or from the copy which has been backed up to the backup cloud hosted by CentreStack.

After selecting ‘Local’, you will be prompted to select a date and time that you’d like to restore to. If you also select “Restore subfolders recursively”, the folder will be restored to the last version on or before the specified date and time.

After selecting ‘Cloud’, you will be prompted to select a snapshot that you’d like to restore from.

---

**Note:** The cloud-based restore is approached differently because the cloud backup is based on snapshots whereas the local team folder is just a versioned folder leveraging the standard restore process for any versioned folder in CentreStack.

---

## 6.4 Cloud Backup Access

The CentreStack architecture provides the option to store backups in a location of your choosing. When these backups are store in the CentreStack Backup Cloud, as shown below, they can be accessed by logging in to [backup.centrestack.com](https://backup.centrestack.com)

To access the backup, navigate to <https://backup.centrestack.com> and login with your normal credentials to access files using CentreStack’s standard browser interface:

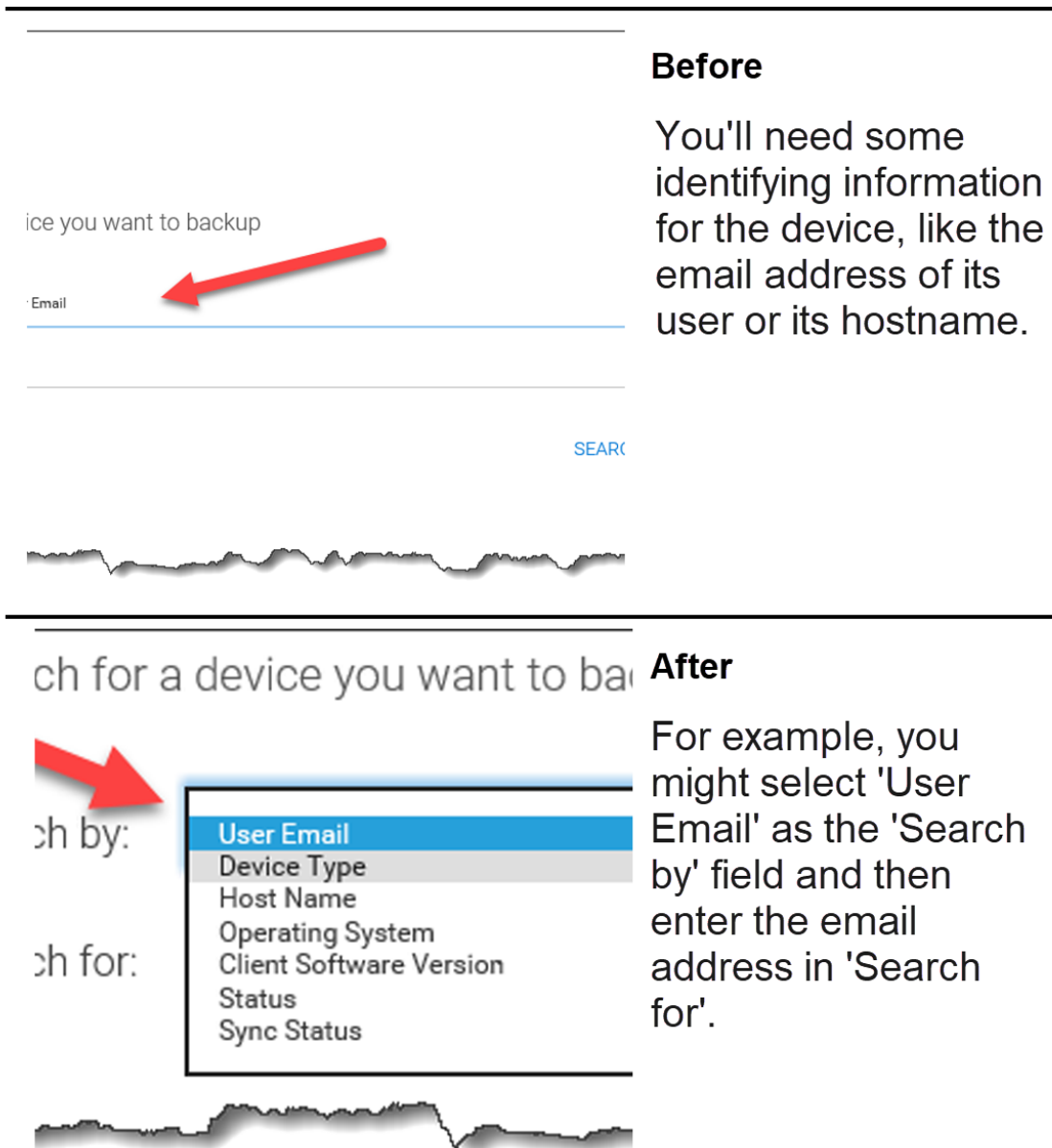


Fig. 13: FIND BACKUP DEVICES TO RESTORE

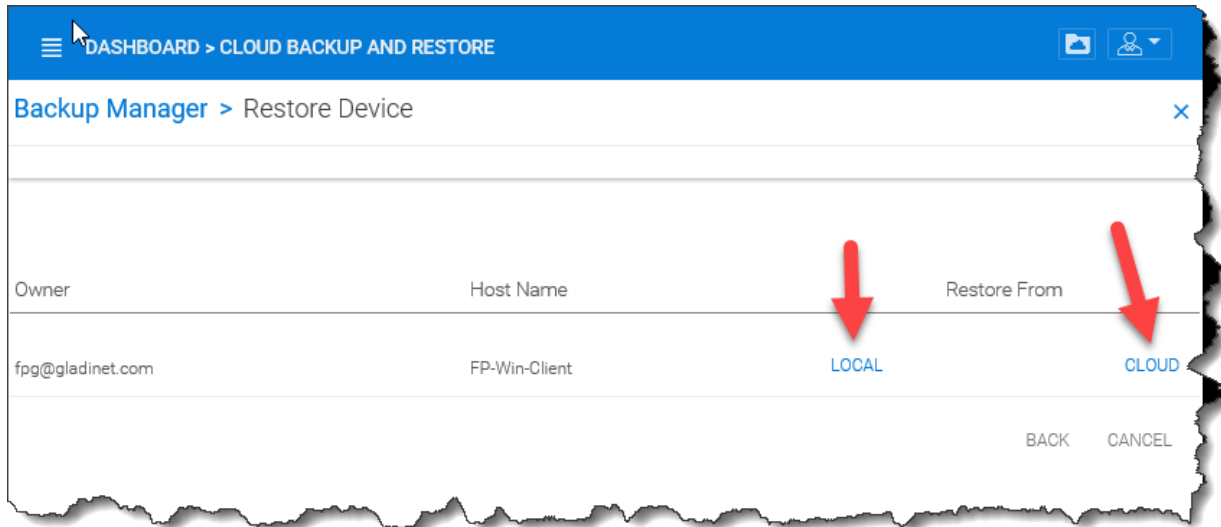


Fig. 14: RESTORE FROM LOCAL OR CLOUD BACKUP

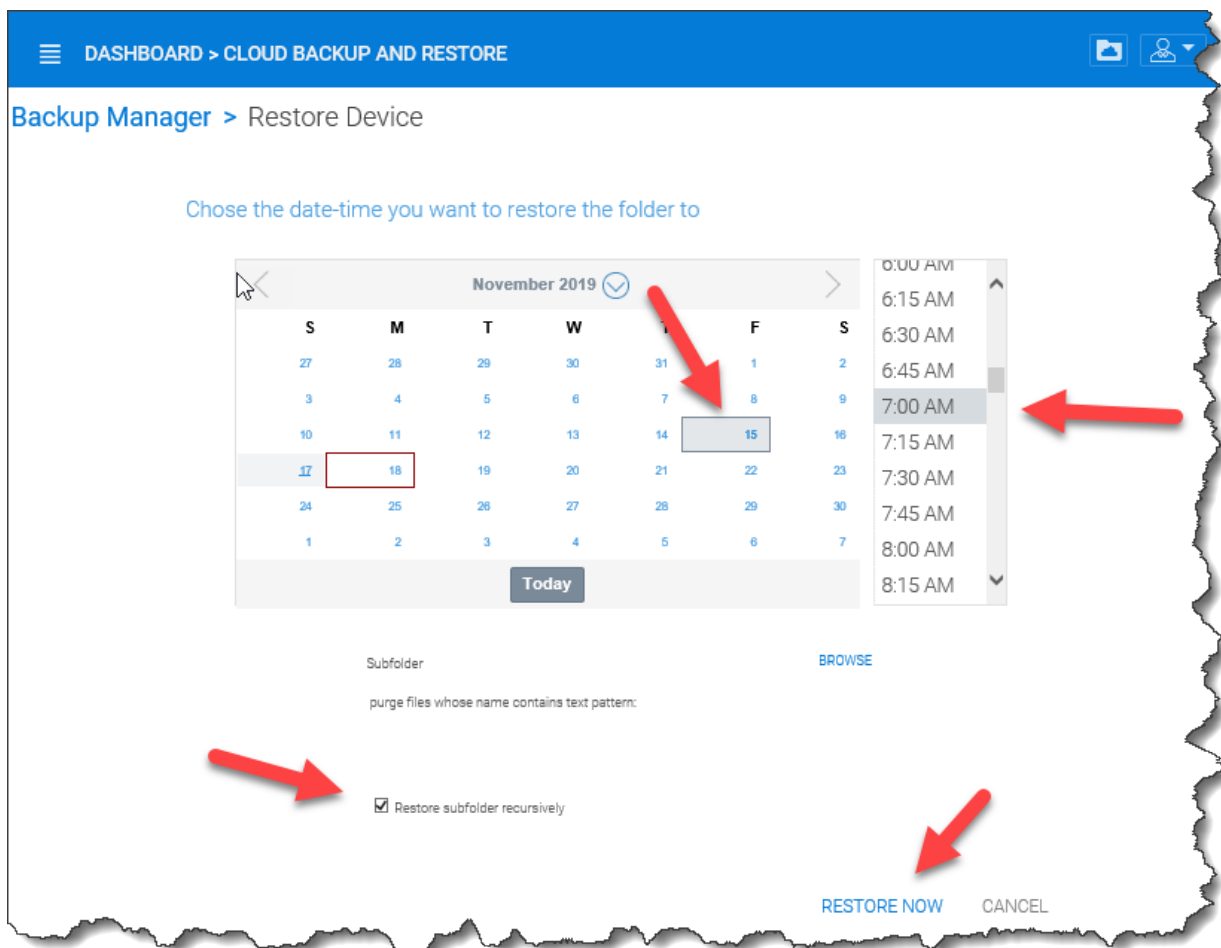


Fig. 15: SELECT DATE AND TIME FOR VERSION BASED LOCAL RESTORE

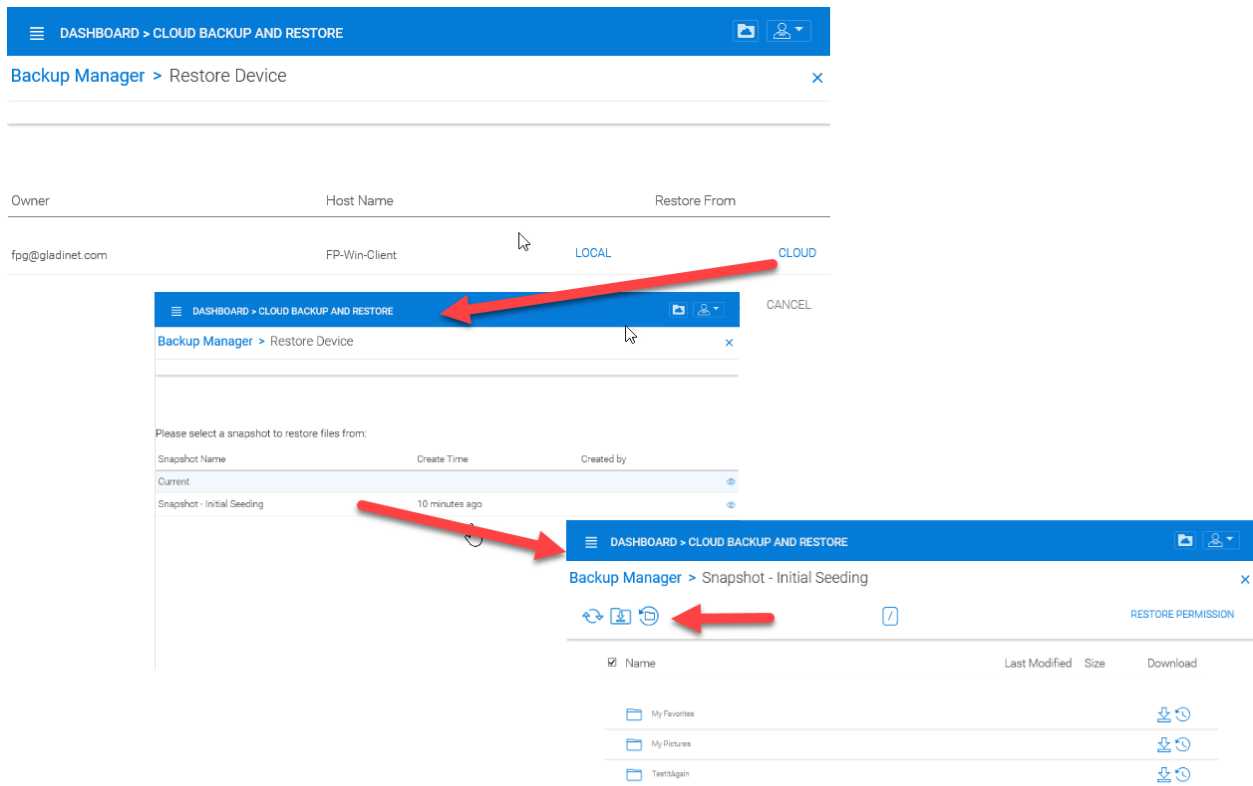


Fig. 16: SELECT CLOUD SNAPSHOT TO RESTORE FROM

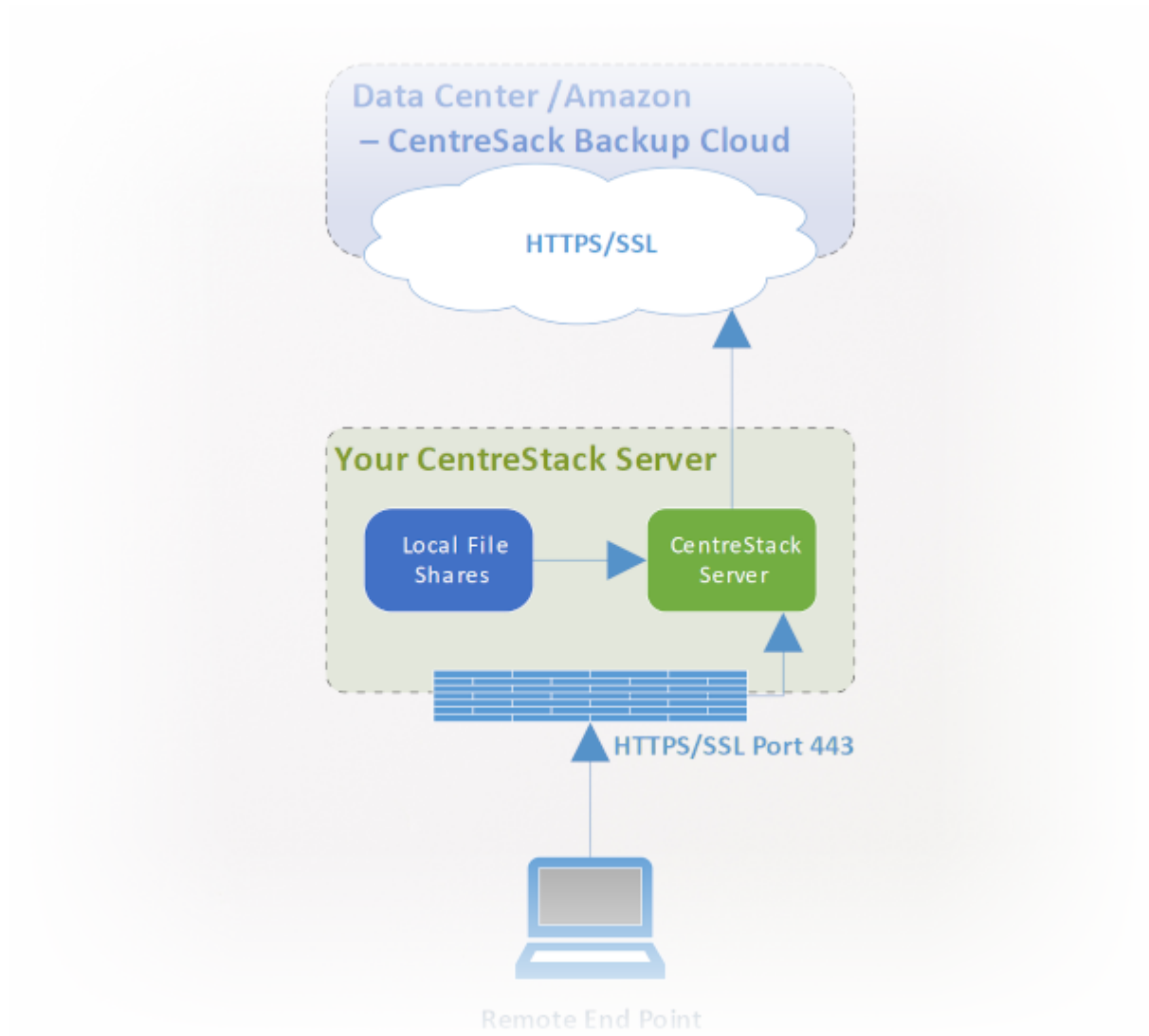


Fig. 17: CLOUD BACKUP ARCHITECTURE

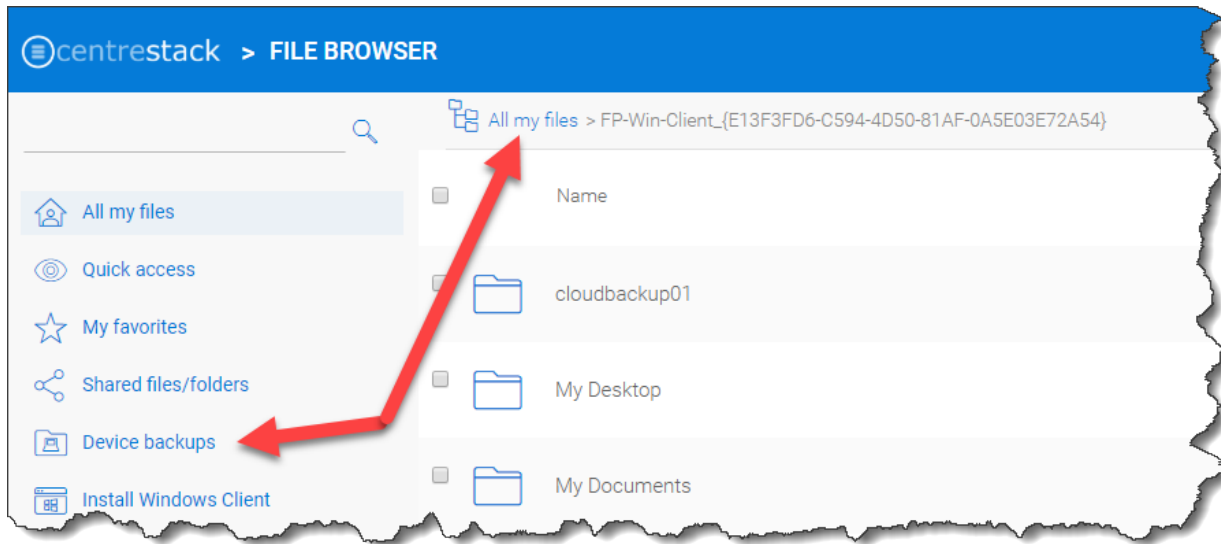


Fig. 18: CLOUD BACKUP ACCESS

As indicated in the image above, you'll find your team folder backups under 'All My Files' and there's a shortcut to your device backups that can be leveraged.

**Note:** The device backup is accessed differently from the local CentreStack cluster and CentreStack Cloud Backup. When a user logs into the cluster, the device backup can be accessed from 'Device Backup' as shown in the image above. But when logged into `backup.centrestack.com`, 'Device Backup' is no longer meaningful and the backup will be found under a folder whose name combines the name of the client machine with a GUID.

## 6.5 Cloud Backup Settings

Cloud Backup and Restore > Settings

CentreStack Cloud Backup is highly configurable, allowing you to determine where the backups will be stored when they will be scheduled, which folders should be backed up by default on the endpoints, and so forth. Most of these settings can be found in the 'Settings' section of the Cloud Backup Dashboard as shown below.

### 6.5.1 Enable Device Backup for All Users

Cloud Backup and Restore > Settings > Detail

As a cluster administrator, go to Cloud Backup and Restore and then navigate to Settings and Details. Go to 'Other Settings' to enable 'Backup all devices with below profile'. Select a profile and then click on 'Save Changes'.

**Note:** You must first create a device backup profile that can be attached to all devices. See below for details.

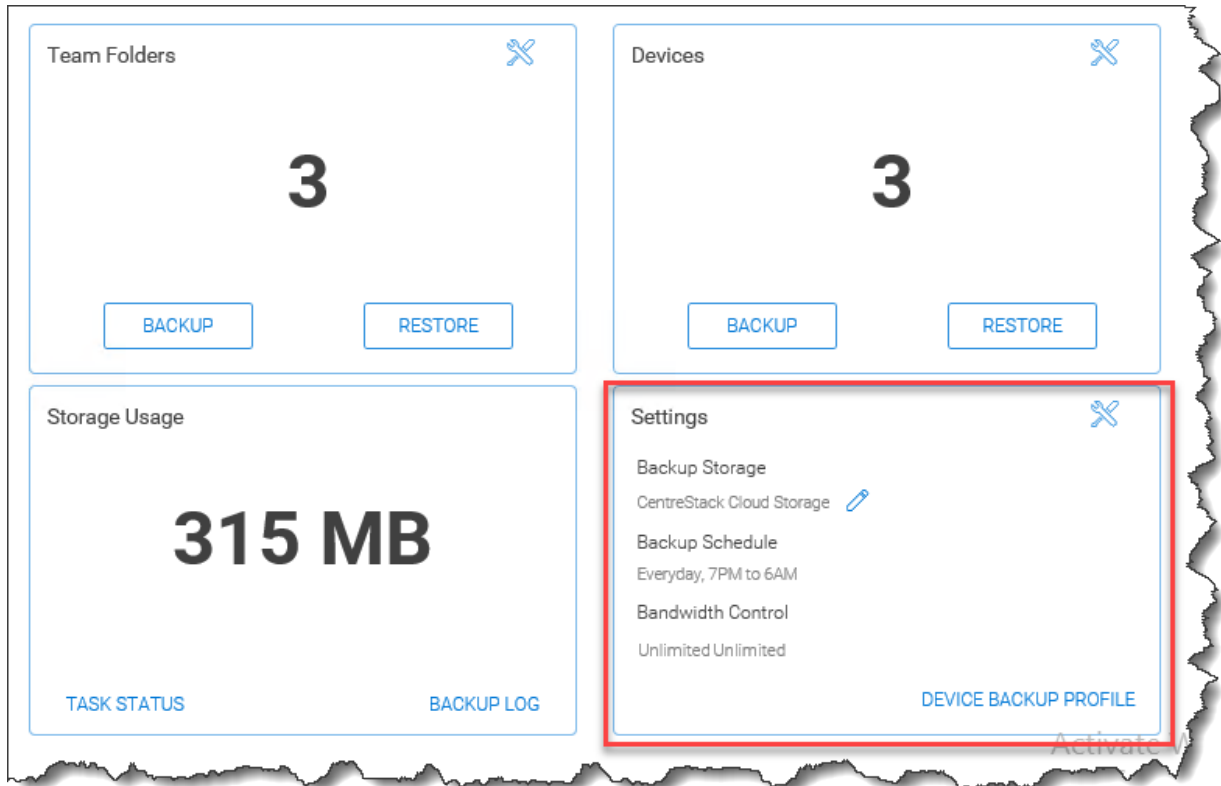


Fig. 19: CLOUD BACKUP SETTINGS

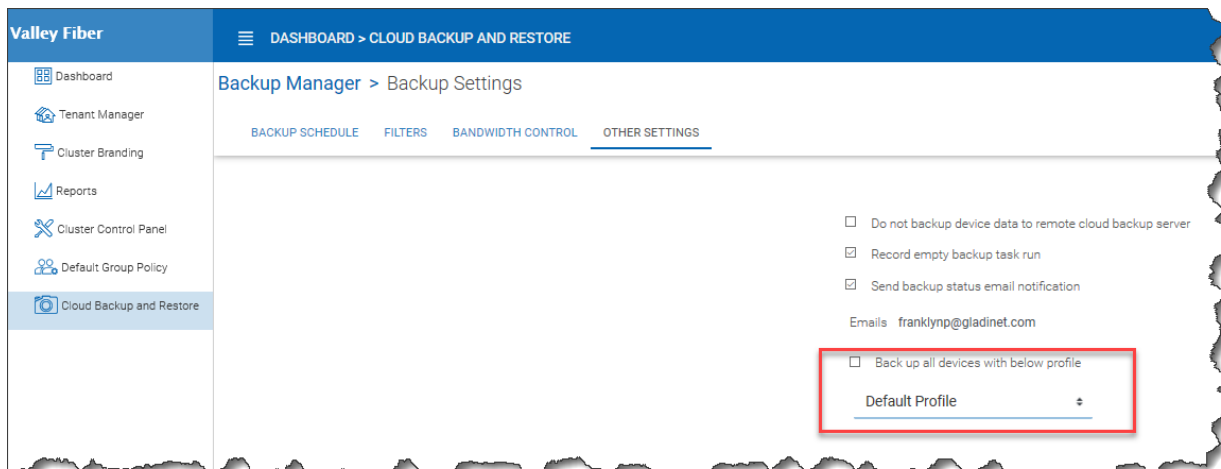


Fig. 20: ENABLE DEVICE BACKUP FOR ALL USERS

## 6.5.2 Change Backup Storage

Cloud Backup and Restore > Settings > Backup Storage

Endpoint devices are first synchronized to a team folder called \$\$DeviceBackupRoot. That team folder will then be backed up to one of three locations depending on the selections below.

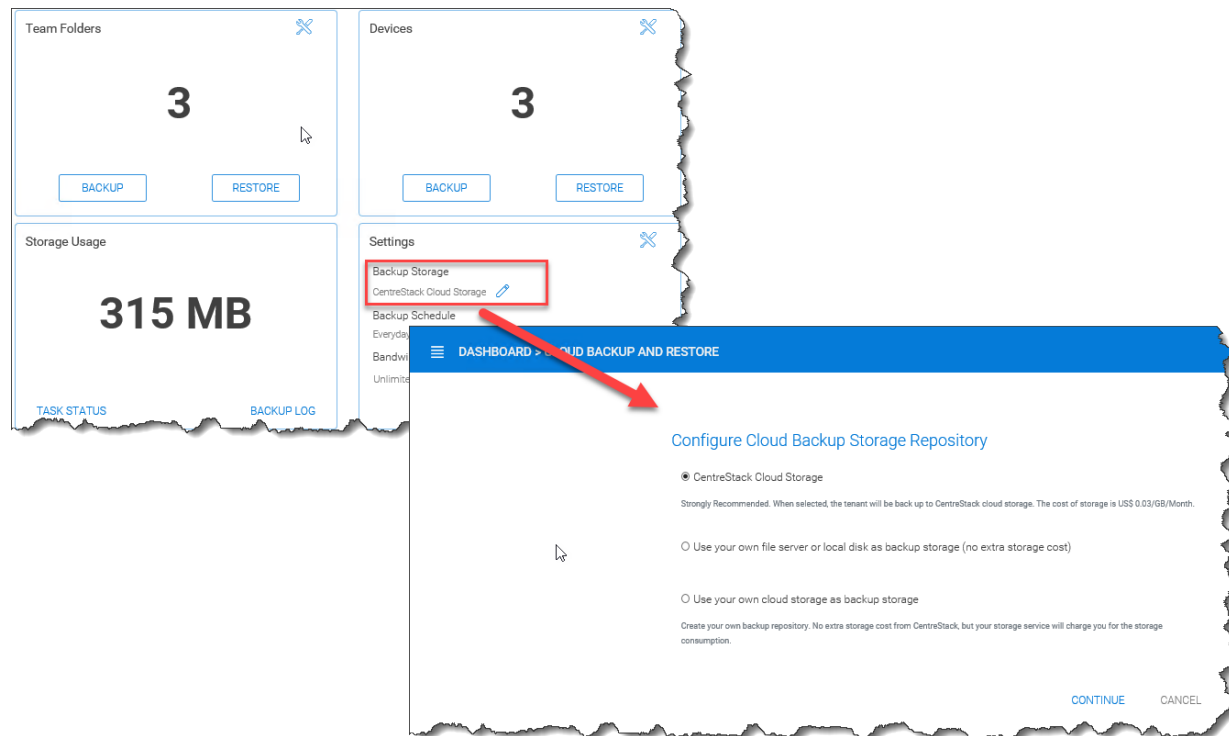


Fig. 21: CHANGE BACKUP STORAGE LOCATION

The preferred location is CentreStack Cloud Storage. When this option is selected, devices in the tenant will get backed up to CentreStack cloud storage. You may also choose to store the backups in your cloud storage account or on a local disk.

**Note:** CentreStack Cloud is strongly recommended because it is optimized for use with CentreStack endpoint backups. For example, the backups stored in CentreStack’s Backup Cloud are also available for access by connecting to <https://backup.centrestack.com>. With this approach, you can leverage the CentreStack cloud for business continuity and high availability instead of having to manage a more complex CentreStack deployment. In other words, you’re getting the benefits of self-hosting without fully assuming the costs of scaling out for reliability, availability, and durability.

## 6.5.3 Disable Backup to the Remote Backup Server

Cloud Backup and Restore > Backup Settings > Details

Click the tool icon to open Settings details and navigate to ‘Other Settings’. Click the checkbox labeled, ‘Do not backup device data to remote cloud backup server’. After doing this, device backup data will no longer be uploaded to the CentreStack Backup Cloud (currently <https://backup.centrestack.com>)



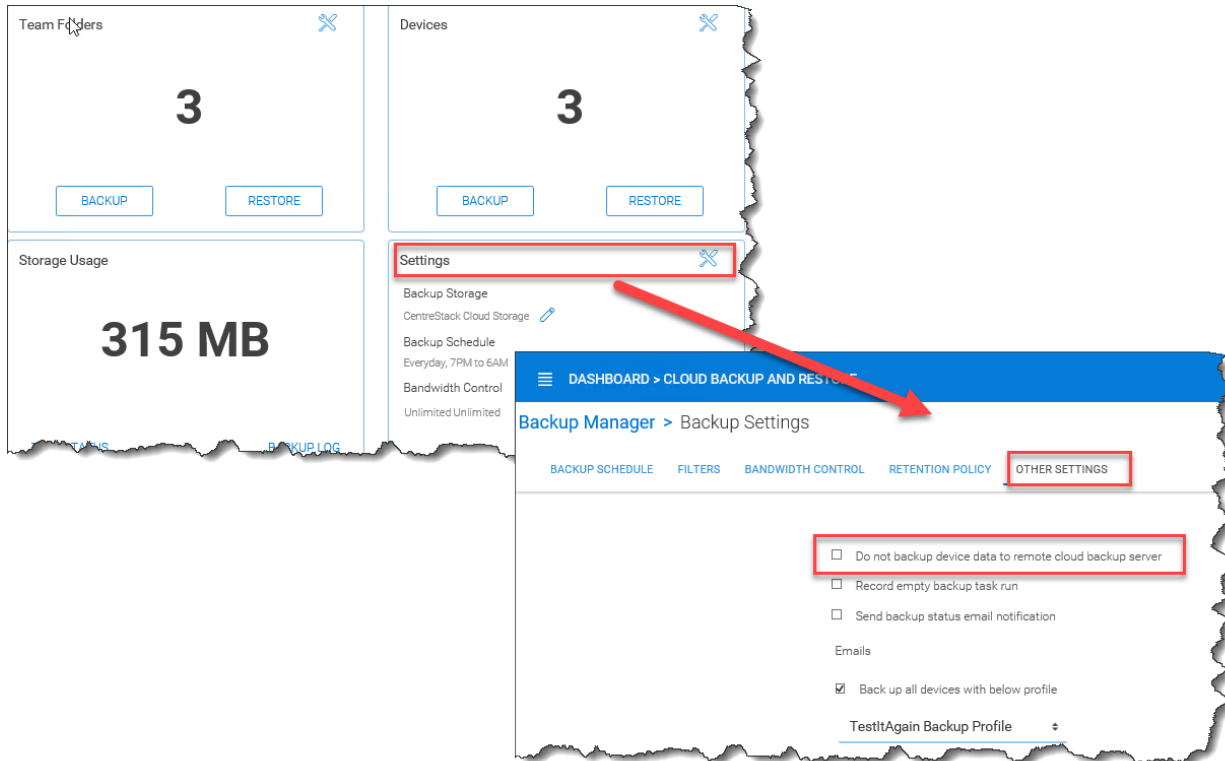


Fig. 22: DISABLE CLOUD REPLICATION FOR DEVICE BACKUP

## 6.5.4 Filters for Files and Folders

Cloud Backup and Restore > Backup Settings > Details

By default, the device backup snapshots will filter out the file types listed in the 'Filters' section of 'Backup Settings' and must be explicitly enabled. For example, select 'Allow ISO files (.iso)' to have ISO files included in each snapshot.

## 6.5.5 Cloud Backup Schedules

Cloud Backup and Restore > Backup Settings > Details

The current cloud backup schedule is displayed in the settings section as shown below.

Click the tool icon in the upper right corner of that section to modify the schedule. The backups can be configured to run continuously or on a daily, weekly, or monthly basis. In each case, you will select the desired time frames or intervals of operation.

## 6.5.6 Device Backup Profiles

Cluster Management Console > Cloud Backup and Restore

As the cluster-admin on the web portal, go to 'Cloud Backup and Restore'. Under 'Settings', click 'Device Backup Profile' and then open the profile list. Click 'Add' to create a new backup profile.

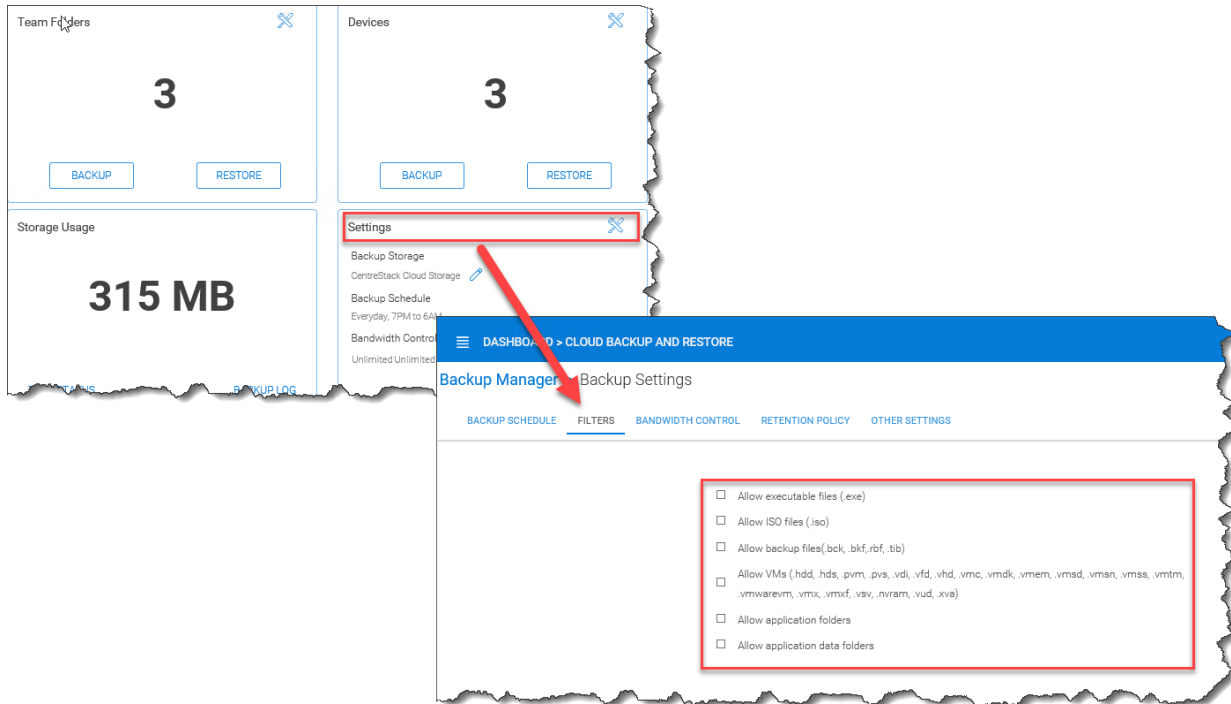


Fig. 23: CONFIGURE FILTERS FOR FILES AND FOLDERS

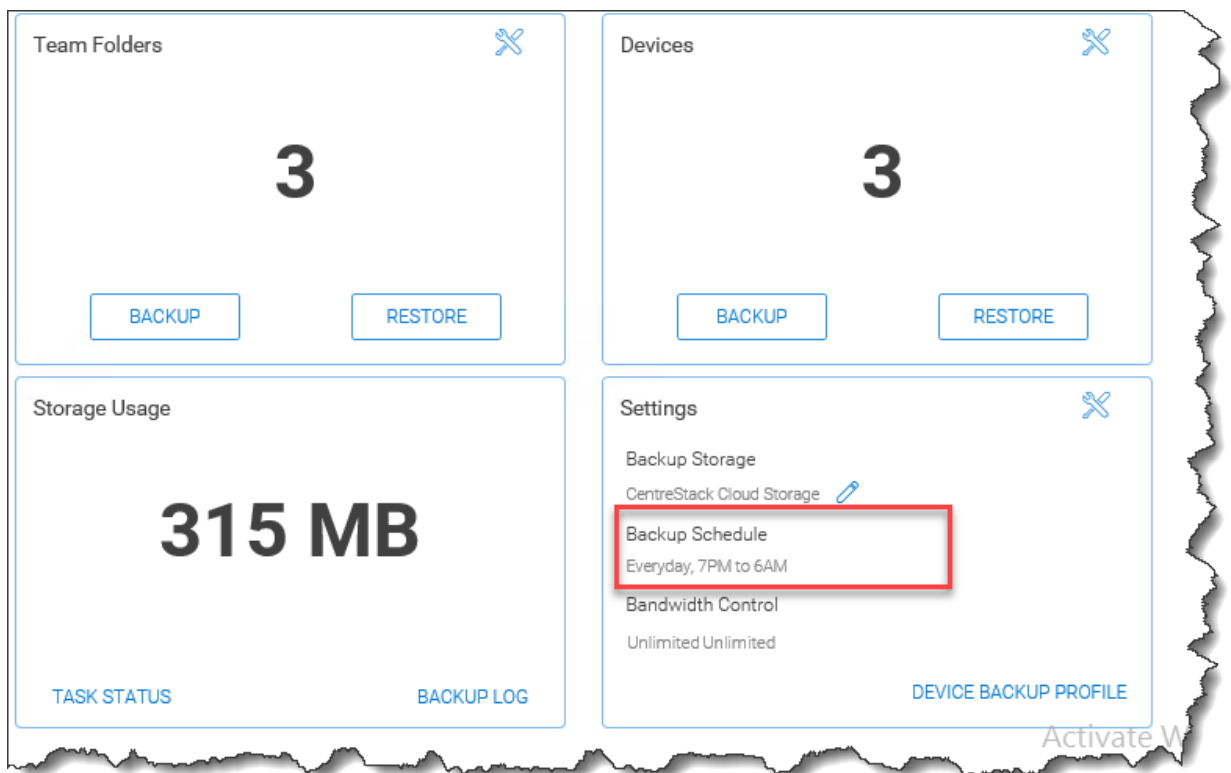


Fig. 24: VIEW CLOUD BACKUP SCHEDULE

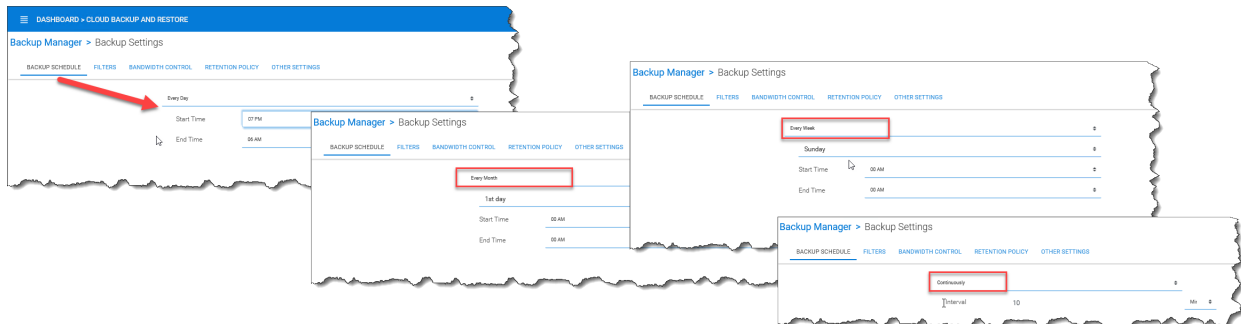


Fig. 25: ADJUST CLOUD BACKUP SCHEDULE

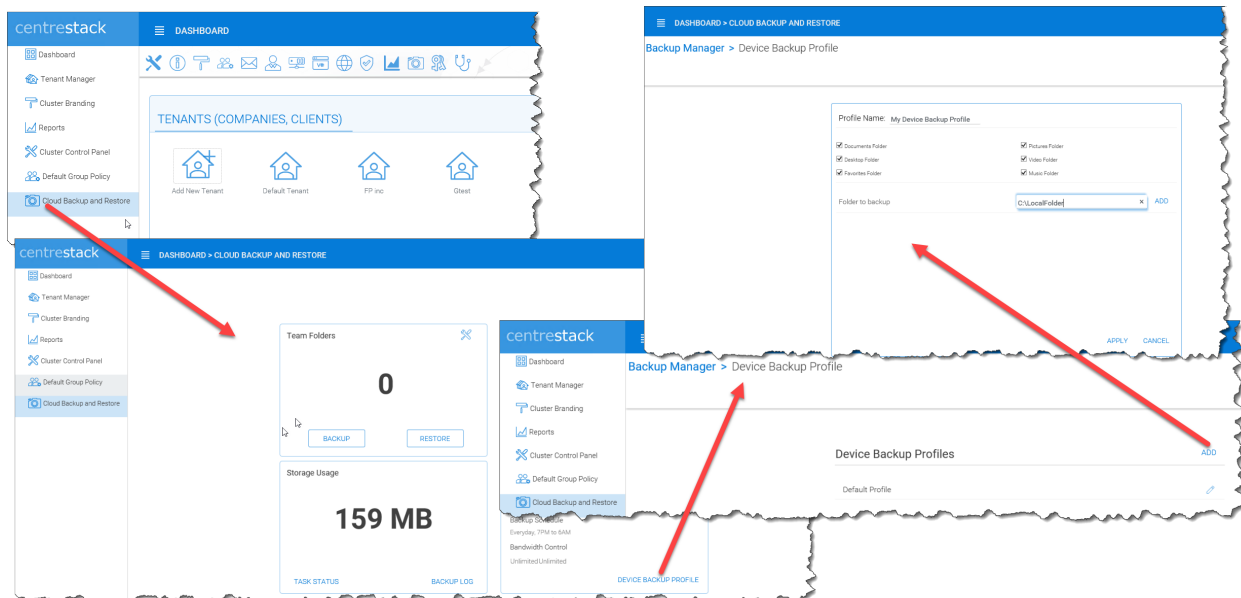


Fig. 26: CONFIGURE DEVICE BACKUP PROFILES

## 6.5.7 Cloud Backup Bandwidth Control

Cloud Backup and Restore > Backup Settings > Details

The current cloud backup bandwidth limits are displayed in the settings section as shown below.

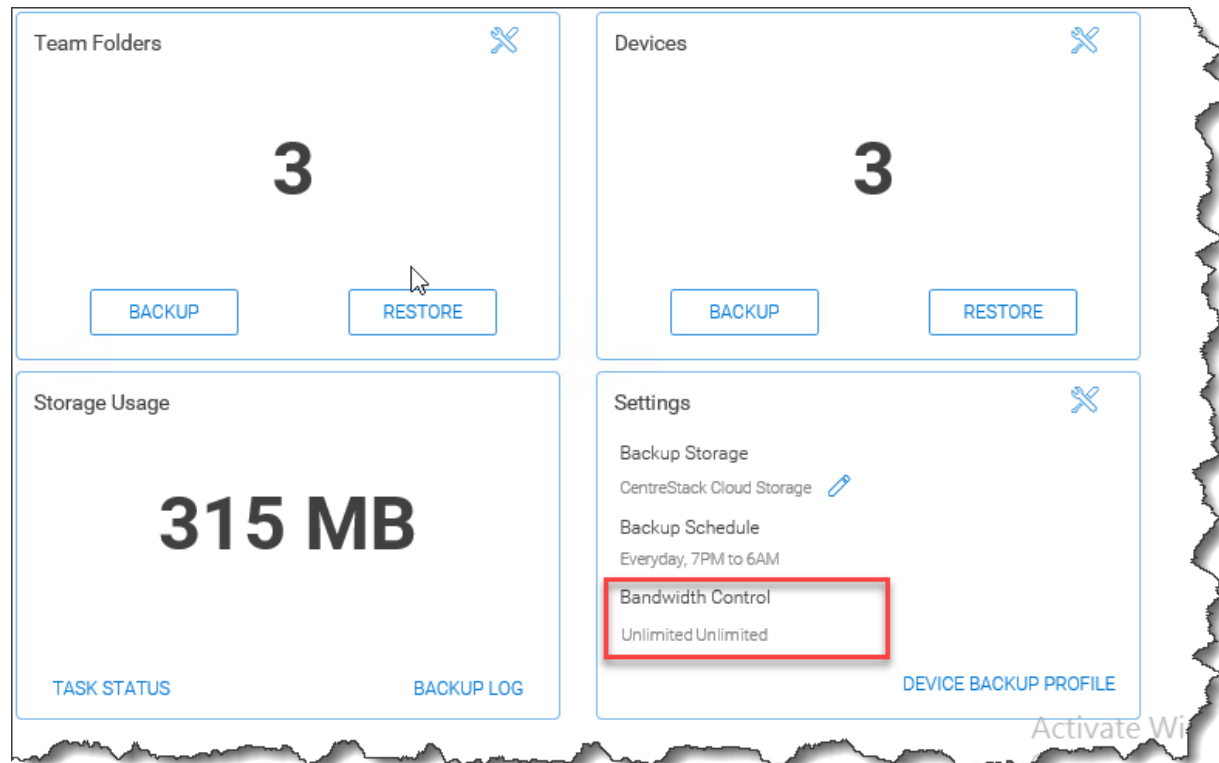


Fig. 27: VIEW CLOUD BANDWIDTH LIMITS

Click the tool icon in the upper right corner of that section to modify the limits. Specify the maximum bandwidth to be consumed during day and night times.

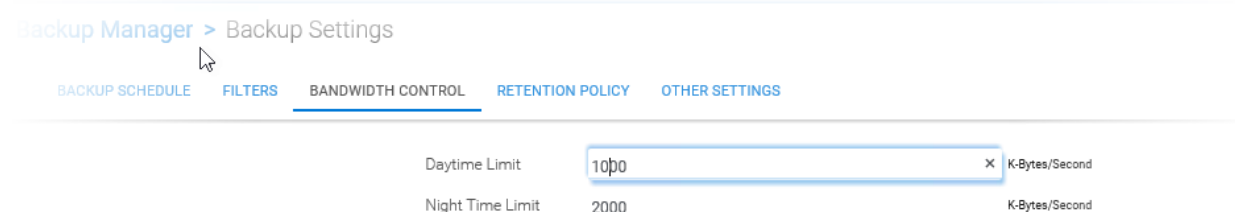


Fig. 28: ADJUST CLOUD BANDWIDTH LIMITS

**Note:** Bandwidth limits are in kilobytes per second (kB/s) and 1kB/s = 0.008 Mbps So a setting of 1000 translates to 8 Mbps.

## 6.5.8 Cloud Backup Retention Policies

Cloud Backup and Restore > Backup Settings > Details

There are three retention policies. “Keep last n snapshots” defines the maximum snapshots allowed at any given time. However, this setting may be overridden by the value of “Keep snapshots for at least n days” if it is not 0. For example, you may want to only keep the last 2 snapshots available, but if the system is configured to keep a snapshot for at least 30 days, a daily snapshot could result in 30 snapshots being created before any are deleted.

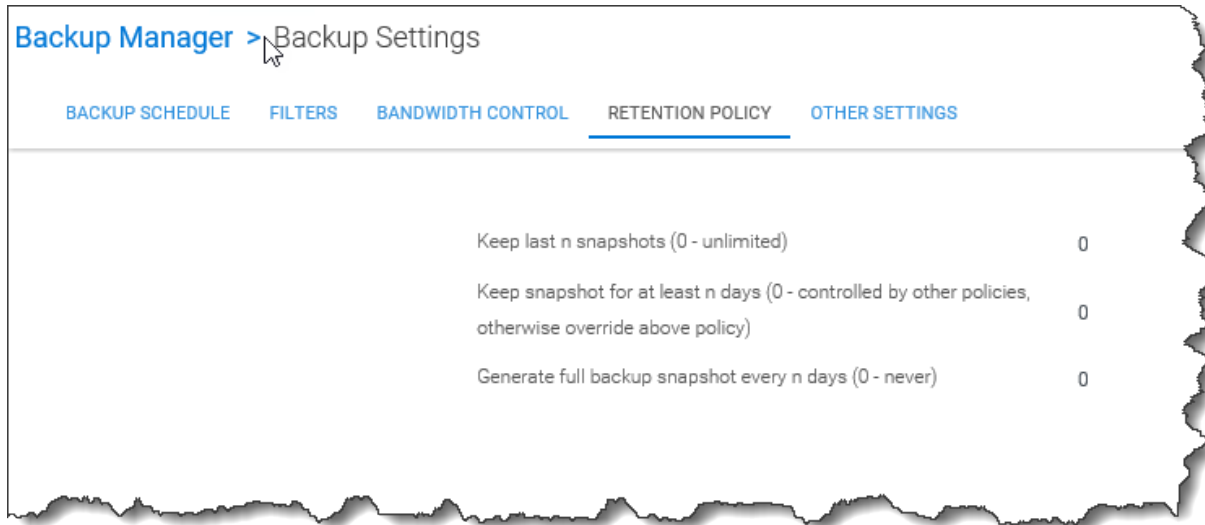


Fig. 29: DEFINE RETENTION POLICIES



## CHAPTER 7

---

### Indices and tables

---

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