Ahsay Backup

Ahsay Cloud Backup Suite v8

Quick Start Guide

Ahsay Systems Corporation Limited

25 March 2021

Copyright Notice

Trademarks

Disclaimer

Revision History

Date	Descriptions	Type of modification
25 January 2021	Updated system architecture diagrams in Ch. 1.1; Added Ahsay Mobile in Ch. 1.2.2; Added permission requirement for agentless backup in Ch. 2.6; Added port 8081 in Ch. 4.3.1; Added SSL requirement in Ch. 4.4; Added Ahsay Push Notification in Ch. 4.6; Updated 2FA login in Ch. 6.1; Updated screenshots in Ch. 6.3, 6.4, 6.5, 6.7 and 6.8; Added Mobile Authentication setup in Ch. 6.6	New / Modification
5 February 2021	Updated TLS version and example in Ch. 4.5; Updated 2FA setup in Ch. 6.6.1 and 6.6.2; Added 2FA login in Ch. 6.6.5	New / Modification
11 February 2021	Updated diagrams in Ch. 1.1; Updated Ch. 7.3; Removed AhsayMOB in Ch. 1.1, 1.2.2 and 7.4	Modification
25 March 2021	Updated push notification in Ch. 4.6; Updated login instructions for TOTP only setup in Ch. 6.6.5	Modification

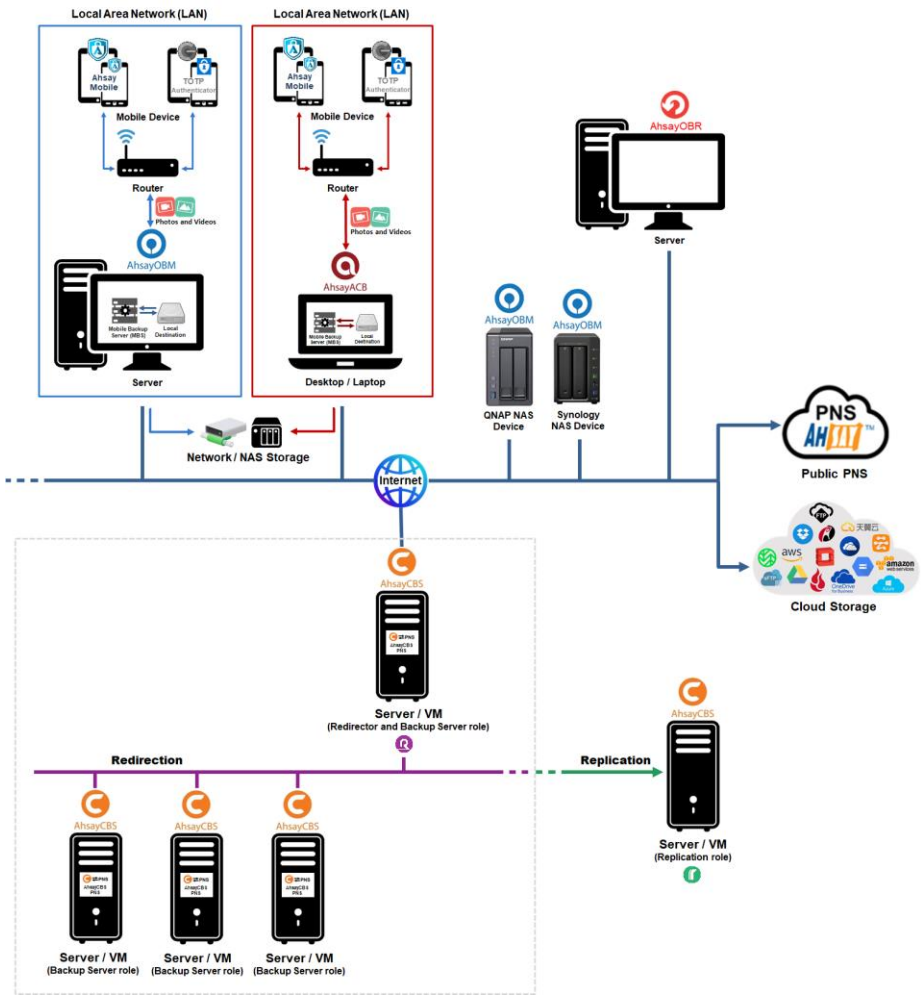
Table of Contents

1 Overview

1.1 System Overview

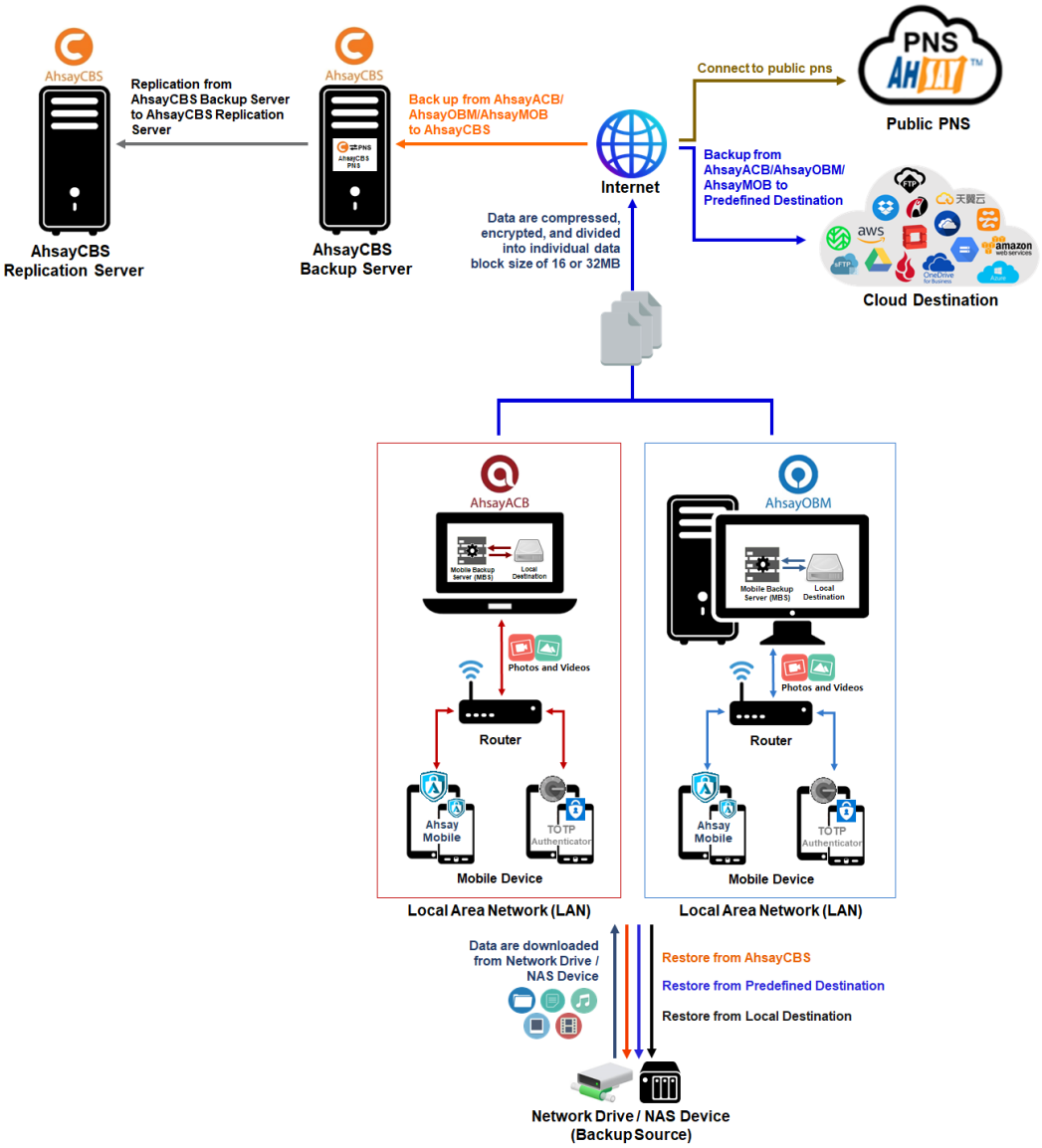
AhsayCBS consists of five core software components.

- AhsayOBM, AhsayACB and Ahsay Mobile are backup clients for installing on servers, desktops, laptop computers, or mobile devices that you need to back up.
- AhsayOBM, AhsayACB, AhsayOBR and Ahsay Mobile are restore clients for installing on servers, desktops, laptop computers, or mobile devices that you need to restore the backup data on.
- AhsayCBS is the server software which bundles a Backup Server, Replication Server and Redirector.
- Backup Server is the module that will host all the AhsayOBM/AhsayACB/Ahsay Mobile backup users and their backup data. It also performs Agentless Office 365 and Cloud File backups.
- Replication Server is the module to provide additional backup of the Backup Server.
- Redirector is the module to provide your backup environment with high scalability solution.

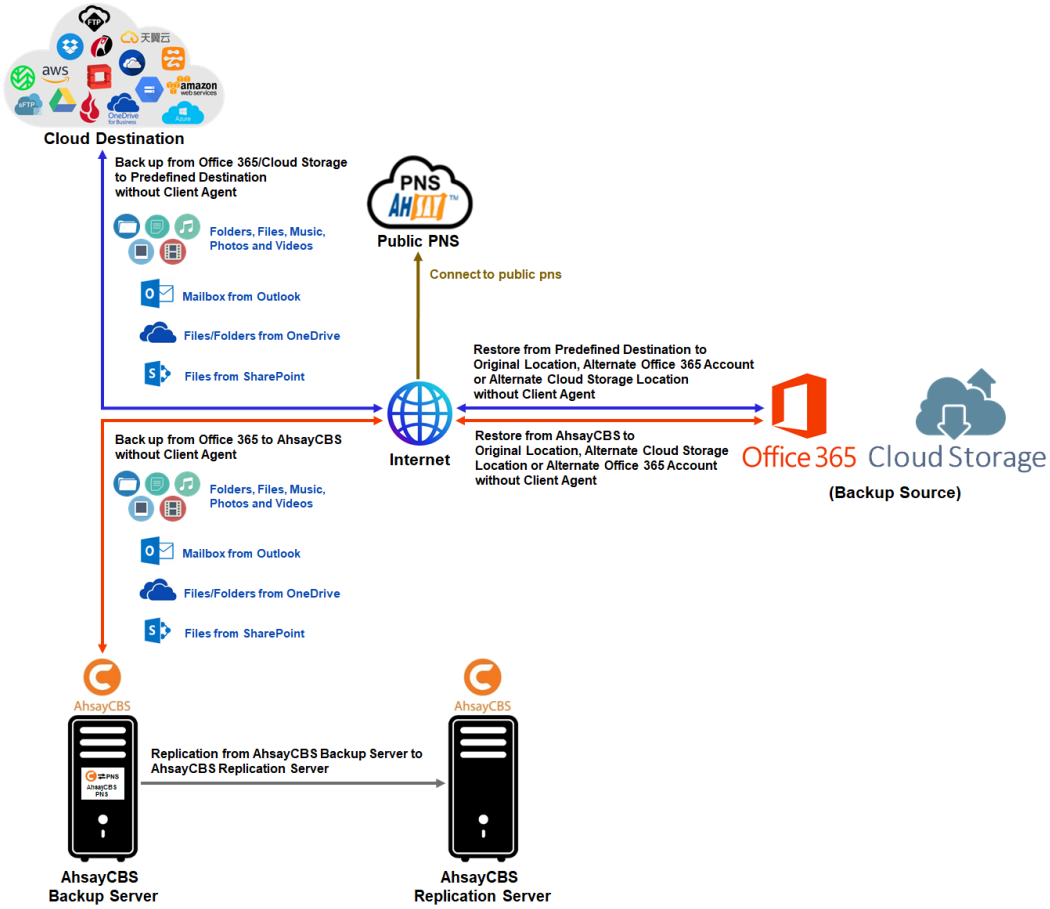


AhsayCBS has two types of setups:

- Agent based setup, wherein you will need AhsayOBM, AhsayACB and Ahsay Mobile to perform backup and restore.



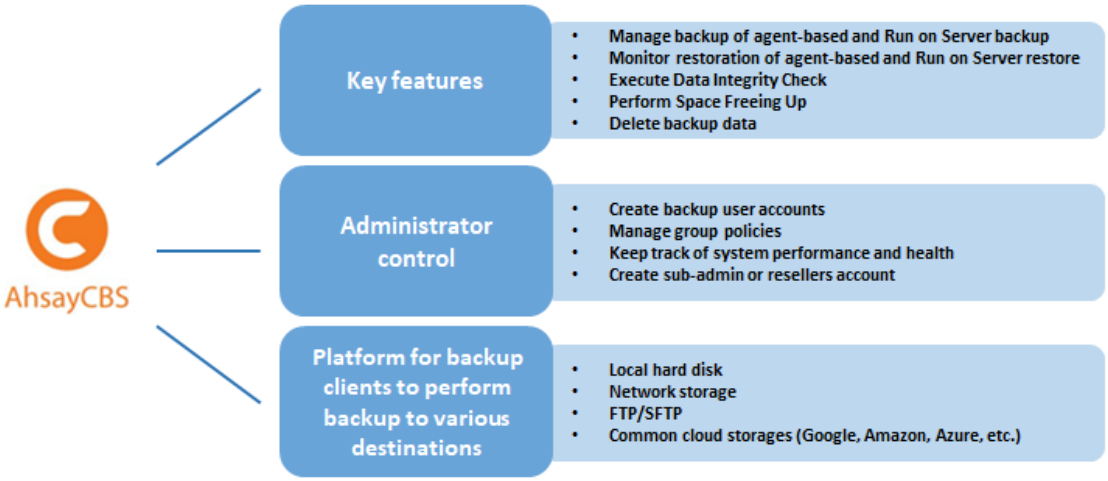
- Agentless setup for Office 365 and Cloud File where the AhsayCBS performs the backup and restore, no need for a backup client to be installed.

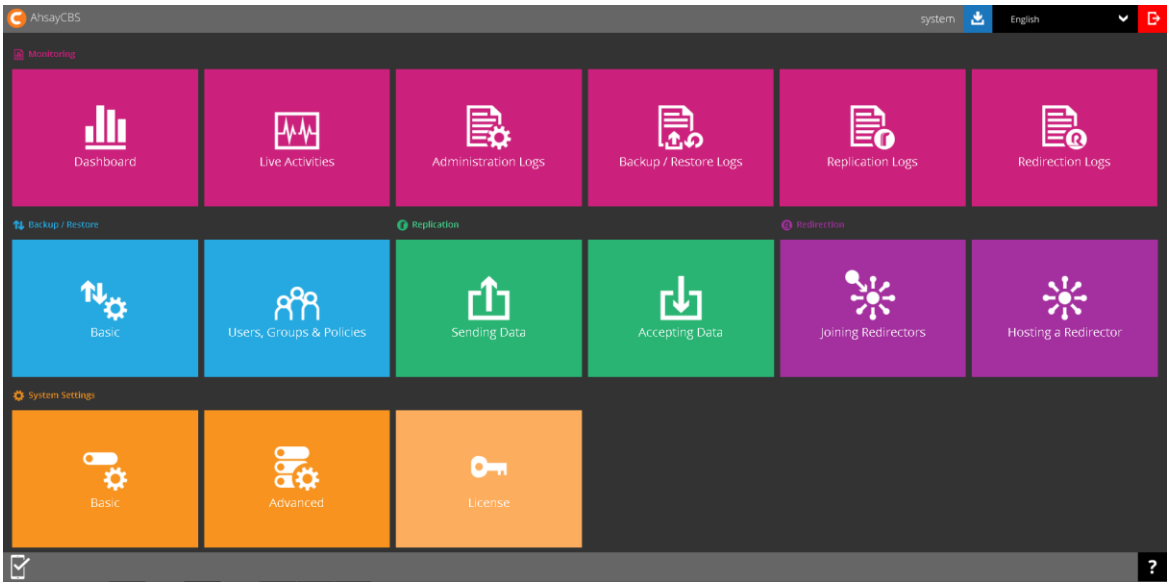


1.2 Software Component Overview

1.2.1 Backup Server

AhsayCBS is a web-based centralized management console for managing client-based backup, Run on Server backup, monitoring restoration, executing Data Integrity Check, performing Space Freeing Up and deleting backup data.

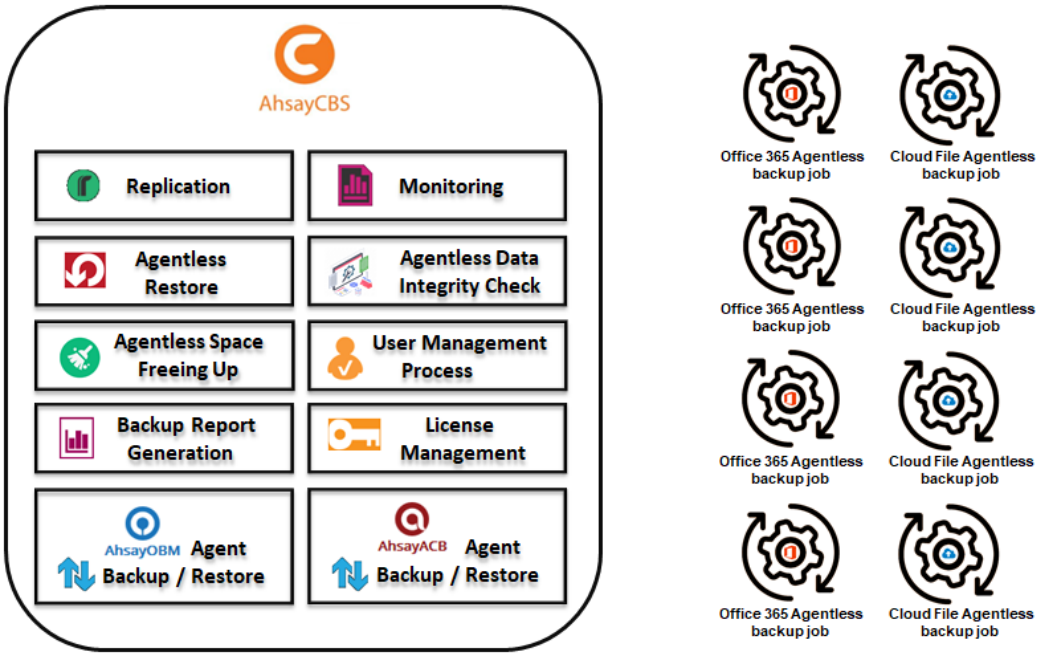




Starting with AhsayCBS v8.3.4.0, each Run on Server Office 365 and Cloud File backup job has a separate Java process with its own Java memory setting which is independent of the main AhsayCBS Java process.

The new Run on Server process only applies to backup jobs. Other processes like restore, data integrity check and space freeing up are still integrated with the AhsayCBS processes.

Run on Server Backup Process



1.2.2 Backup Client

We have three backup clients catering to customers with different needs. Below is a table providing a quick reference of the functionalities of the three backup clients.

			
Backup source	Back up files, databases and virtual machines such as: ➢ VMware ➢ Hyper-V ➢ Microsoft Exchange Database Availability Group (DAG) ➢ Microsoft Exchange Database ➢ Microsoft Exchange Mailbox ➢ Microsoft SQL Server ➢ Oracle Database ➢ Lotus Domino/Note ➢ MySQL ➢ MariaDB ➢ Windows System ➢ Windows System State ➢ ShadowProtect ➢ Synology NAS Devices ➢ Office365 ➢ Cloud File ➢ QNAP NAS Devices	Back up files, Outlook / Outlook Express / Windows Live mail, Windows System, IBM Lotus Note, Cloud File, Office365 mailbox, OneDrive and Sharepoint files.	Backup up photos and videos from an Android or iOS mobile device to AhsayOBM or AhsayACB.
Backup destination	Local and offsite destinations, e.g. local storage, on-premises backup server or backup server located in a datacenter, and common cloud		Local destination only, e.g. local storage or flash drive on the

	storages (Google, Amazon, Azure, etc.)	AhsayOBM or AhsayACB machine. Also possible for offsite destinations but involves a two-step process. For more information please refer to the AhsayOBM Quick Start Guide and AhsayACB Quick Start Guide.
Data encryption	All the backup data are compressed and encrypted before uploading to the Backup Server, while the restoration process requires downloading the compressed and encrypted data onto the client computer for decryption and decompression.	Photos and videos are uploaded in its original format; files can be viewed directly in the backup destination.

NOTE

Backup Sets with Run Direct restore and Granular restore enabled, both compression and encryption are disabled to optimize restore performance.

1.2.3 Restore Client

We have four restore clients (AhsayOBM/ AhsayACB/ Ahsay Mobile/ AhsayOBR) catering to customers with different needs. Below is a table providing a quick reference of the functionalities of AhsayOBR.

	AhsayOBR
Restore source	Restore files, databases and virtual machines such as: ➢ VMware ➢ Hyper-V ➢ Microsoft Exchange Database Availability Group (DAG) ➢ Microsoft Exchange Database ➢ Microsoft Exchange Mailbox ➢ Microsoft SQL Server ➢ Oracle Database ➢ Lotus Domino/Note ➢ MySQL

	➢ Windows System ➢ Windows System State ➢ ShadowProtect ➢ Office365 ➢ Cloud File ➢ MariaDB
Restore destination	The backup data will be restored to the devices running restore client

While you can still download Client Backup Agent (AhsayOBM/ AhsayACB) to restore data on computer, AhsayOBR gives a quick, direct and secure solution just for the data restore purpose. Below is a table comparing some major features of both tools, and the pros and cons of using them.

Feature	Tool	Pros	Cons
Installation	**AhsayOBR**	◉ No installation required ◉ Faster to launch	Required to launch every time when you use
	Client Backup Agent	One-time installation	Larger installer size hence longer installation time
Run Direct Restore	**AhsayOBR**	N/A	Run Direct restore for VMware and Hyper V servers is **NOT** supported. Since AhsayOBR is not a Client Backup Agent and therefore NFS is not bundled along with the software. NFS is a mandatory item for performing Run Direct restore for VMware and Hyper-V servers.
	Client Backup Agent	Support Run Direct restore for both VMware and Hyper-V servers.	N/A
OpenDirect Restore	**AhsayOBR** **Client Backup Agent**	OpenDirect restore allows you to view and download individual files from a compressed or image file, without having to restore compressed file or image file first. OpenDirect restore gives you the flexibility to restore selective file(s)	To ensure optimal restore performance, the backup of the files in an OpenDirect file backup set will **NOT** be encrypted and compressed, therefore, you may have to take these factors in consideration when

		quickly, so it saves you time and effort to achieve your restore goal.	selecting this restore option.
Granular Restore	**AhsayOBR** **Client Backup Agent**	In some cases, you may only need to restore a few individual file(s) from the guest VM, therefore, granular restore gives you a fast, convenient, and flexible tool to restore selected file(s) from a guest VM quickly.	To ensure optimal restore performance, the backup of the guest VM will **NOT** be encrypted and compressed, therefore, you may have to take this factor in consideration when using this restore method.
Cross platform usage	**AhsayOBR** **Client Backup Agent**	Although both tools are available for use on various platforms, e.g. Windows, Mac, Linux, etc., cross platform restore is **NOT** recommended. For example, files backed up on Windows are not recommended to restore on a Mac/Linux machine.	
Compatibility	**AhsayOBR**	Support restore of backup set created on either AhsayACB / AhsayOBM	N/A
	Client Backup Agent	N/A	Support restore of backup set created by the same type of Client Backup Agent only. E.g. backup set created on AhsayOBM can only be restored by AhsayOBM.

1.2.4 Replication Server

Replication Server offers close to real time replication of user data hosted on the Backup Server, so that when your live Backup Server is out of service, you can switch the Replication Server into Backup Server so as to keep your backup service uninterrupted. Aside from the Replication Server, you can also use cloud storage for replication. Alternatively, you can also choose to restore the backed up data from the Replication Server or cloud storage when your Backup Server machine is recovered.

1.2.5 Redirector

With the use of Redirector in conjunction with multiple Backup Server machines, it forms a cloud backup architecture for servicing as many backup customers as needed with a single public URL. All backup users will use the single URL as the initial contact server, even though they reside on different Backup Servers under different URLs. Thus, an online backup provider can add new Backup Server machines to serve new customers, or relocate existing backup accounts from one Backup Server to another easily without the need for the existing users to reconfigure the backup server address in AhsayOBM or AhsayACB.

IMPORTANT

For details regarding setup and configuration of the replication server and redirector, please refer to the **Administrator's Guide** via the URL below. Chapter 7 **Replication** and Chapter 8 **Configuring Redirector** would state the details of replication and redirector respectively.
https://www.ahsay.com/download/download_document_v8_cbs-admin.jsp

1.3 Run on Server (Agentless) Backup Process

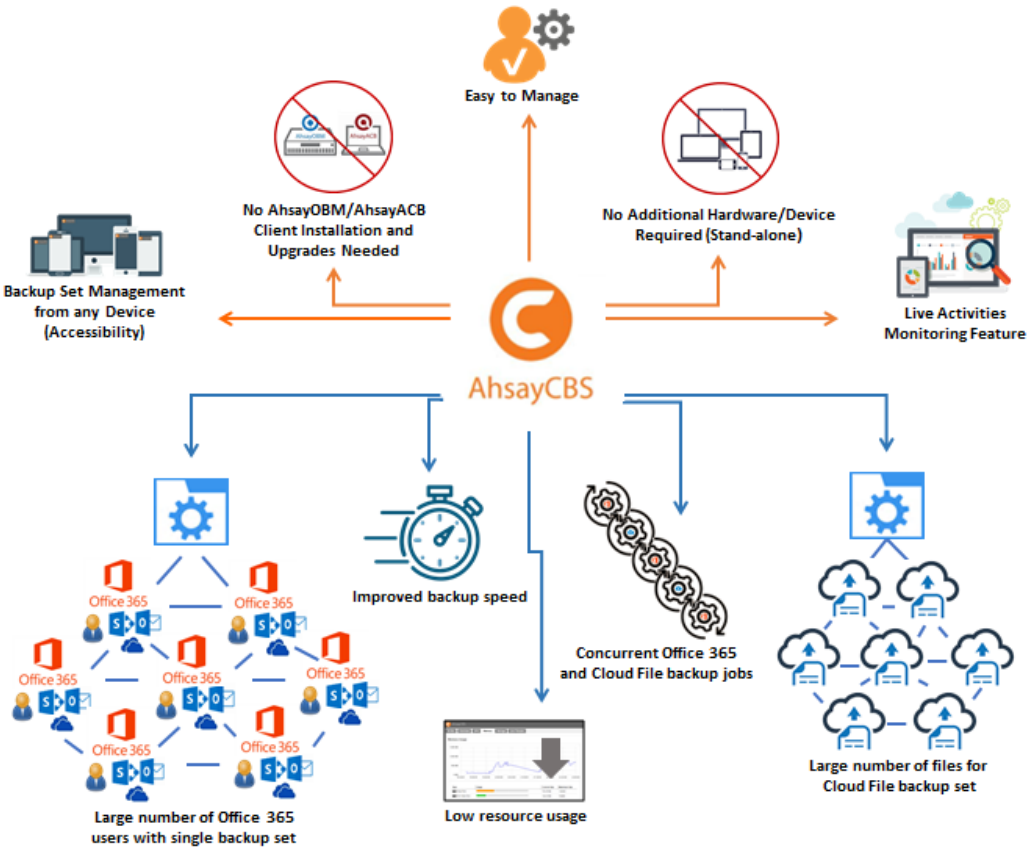
The Run on Server (Agentless) Office 365 and Cloud File backup jobs are now a separate Java process independent from the main AhsayCBS Java process. This means that Office 365 and Cloud File backup jobs will not utilize the Java memory resources of AhsayCBS Java process, as each backup job will run in its own independent Java process with its own dedicated Java memory setting. By default, each Run on Server backup job is assigned 1GB of Java memory. However, the Java memory allocation can be customized by the system administrator.

The previous limitations on maximum number of concurrent Run on Server (Agentless) Office 365 and Cloud File backup job on AhsayCBS has been removed, as more concurrent backups can be supported due to the improvements.

The changes made will improve the overall performance, stability, and scalability of AhsayCBS for Run on Server (Agentless) Office 365 and Cloud File backup jobs.

1.3.1 Why deploy agentless Office 365 and Cloud File backup

Run on Server (Agentless) backup process has been improved to make the backup experience better to meet the needs of the customers.



- **No AhsayOBM/AhsayACB client installation and upgrades needed**

  AhsayOBM and AhsayACB client installation is not required as backup jobs are running on the AhsayCBS server. Also, unlike the client backup agent, upgrading when a newer version becomes available is not necessary, as long as the AhsayCBS server version is upgraded by the backup service provider.

- **No additional hardware/device required**

  As the Run on Server (Agentless) backup set utilizes the resources of the AhsayCBS backup server, there is no need to provision additional physical or virtual machine to run the backup/restore which means the cost of each backup set is much lower than for an agent based Office 365 and Cloud File backup set.

- **Easy to manage**

  The AhsayCBS User Web Console offers you an easy-to-manage user interface. This will help you save time and it reduces the overall cost of support.

- **Backup set management from any device (Accessibility)**

  Backup/restore operation(s), backup set settings configuration, and backup/restore process monitoring can be done from any device as long as a web browser and internet connection are present in the device.

- **Live Activities Monitoring feature**

  The AhsayCBS User Web Console has a live activity monitoring feature which is used to keep track of the backup and restore job(s). The following operations can be performed using this feature:

  - View the status of the backup process that is currently running or finished within 1 hour
  - View the status of the restore process that is currently running or finished within 1 hour

- **Handle backups of large number of Office 365 users with a single backup set**

  Finish backup of a single Office 365 Run on Server (Agentless) backup set with 2000 users within 24 hours.

- **Handle backups of large number of files for Cloud File backup sets**

  Easily backup Cloud File Run on Server (Agentless) backup sets containing large number of files.

- **Improved Office 365 backup speed**

  The Office 365 backup speed has improved due to Office 365 Change API implementation.

- **Lower resource usage**

  The new Run on Server (Agentless) backup process has its own independent Java process, set at 1GB by default, which means it does not use the Java memory resources of the AhsayCBS Java process resulting in lower resource usage.

- **Improved capacity for each AhsayCBS server to handle more concurrent Office 365 and Cloud File backup jobs**

  Since the Run on Server (Agentless) backup process is now separate from the main AhsayCBS process, more concurrent Run on Server (Agentless) Office 365 and Cloud File backup jobs can be supported.

Please refer to the following user guide for the details about how to run agentless backup/ restore jobs using AhsayCBS user web console:

Cloud File Run on Server (Agentless) Backup and Restore Guide

Office 365 Run on Server (Agentless) Backup and Restore Guide

2 System Requirements

Before you install the AhsayCBS, please pay attention to the following system requirements and make sure that the requirements are met before getting started.

The AhsayCBS should be deployed on a machine supporting 64-bit multiple CPU and multiple cores environment. A 64-bit operating system will allow AhsayCBS to run on a 64-bit Java OpenJDK 1.8 platform, as 64-bit Java is capable of supporting sufficient capacity for future business expansion, to meet the need of existing customers and to support new AhsayCBS server features. It should also have the GNU C Library version 2.14 or higher installed to support the Java OpenJDK 1.8 platform.

When you deploy the AhsayCBS, please consider to assign a dedicated disk for the system home, user home and replication home. It is not suggested to install AhsayCBS on a disk which contains your operating system. Due to backup data growth this can quickly fill up the system drive which makes the operating system unstable and may even crash the AhsayCBS server.

2.1 Software Requirements

Refer to the following link for details of the operating systems, applications and databases supported by AhsayCBS.

FAQ: Ahsay Software Compatibility List (SCL) for version 8.1 or above

Refer to the following article for the list of compatible operating system for Granular Restore:

FAQ: Ahsay Software Compatibility List (SCL) for Granular and OpenDirect Restore

2.2 Hardware Requirements

You can deploy AhsayCBS server on a physical machine, on a virtual machine, or on a cloud environment. The server requirements are outlined in the following sections.

Refer to the following link for details of the hardware requirements needed to run AhsayCBS successfully.

FAQ: Ahsay Hardware Requirement List (HRL) for version 8.1 or above

2.2.1 AhsayCBS on Physical Machine

When you deploy a physical machine, please consider to purchase a more powerful machine. This will reduce the need for frequent hardware upgrades when your backup business grows, which will require services down time for hardware upgrades and data migration. If the AhsayCBS server is deployed for Office 365 and/or Cloud File Run on Server (Agentless) backups, the server needs to be of a higher specification; CPU and RAM, as the backup/restore jobs will be processed by the server itself.

It is a good idea to ensure your AhsayCBS server is equipped with some redundancy features, i.e. power supply, and is connected to a UPS (Uninterruptible Power Supply).

2.2.2 AhsayCBS on Cloud Environment

To host an AhsayCBS on cloud, the basic requirement would be similar with setting up a physical machine. It is more flexible when you need to increase memory size, process cores, and disk space. In addition, you will need to take the running cost of a server instance and network usage, which are considered as a hidden cost for the setup.

You can consider hosting a cloud server instance such as Amazon or Azure.

2.2.3 Additional Disk Storage

Connect a Direct-Attached Storage (DAS) with e.g. a 12 hard disk bays filled with 4TB hard disks via the SCSI interface, extra SCSI controller card required.

With the above setup, it should be able to handle 100 users with around 30TB of storage and a total of 1000 backup sets. With this server setup, it is not yet reaching the server's physical limitation. There are still other factors that may limit the growth of users, e.g.: network bandwidth. Also, it is easier to manage from administration point of view.

There are 2 assumptions:

- Each user has around 300GB of backup data, with constant 3% of changes daily.
- Each user account has configured 10 backup sets. These backup sets could be run on different machines and backup to the AhsayCBS at the same time.

AhsayOBM/AhsayACB backup clients are enhanced to utilize multiple threads for backup and restore. It is recommended to keep the maximum number of concurrent backup jobs on the AhsayCBS to 1000, to avoid potential performance problems.

Additional Storage on Cloud

Besides local storage, you can set up network storage, FTP/SFTP and common cloud storages (Google Drive, Dropbox, OneDrive, Rackspace, Wasabi etc.) for the AhsayCBS.

2.2.4 Additional Memory

The amount of RAM needed for the AhsayCBS server to run efficiently depends on:

- The memory required for the operating system to run efficiently.
- The type of backup jobs; agent based backup where the backup is processed on the customer machine or an agentless (Run on Server) backup job such as Office 365 or Cloud file backup where the backup job is processed by the AhsayCBS server itself.
    - Agent based backup

      As the agent based backup rely on AhsayOBM/AhsayACB backup client to process the backup, the Java heap size required is relatively small. For most AhsayCBS servers a setting of 4096M or 4GB of Java heap size is sufficient. The default Java heap size is 2048 or 2GB.

      For example, the AhsayCBS server will require a minimum of 8GB of RAM, 4GB (for the Operating System) + 4GB (for AhsayCBS service) = 8GM of RAM.

      For an AhsayCBS server hosting agent based backups, the Java heap size should not exceed 2/3 of RAM available to allow sufficient resources for the operating system.

      For instruction on how to configure the Java heap size, please refer to the AhsayCBS Administrator's Guide.

- Agentless backup

  Although the backup job is processed by the AhsayCBS server itself with each backup job having its own separate Java process and Java heap size, it is still recommended that the AhsayCBS service should have a Java heap size of 4096M or 4GB. As restore, data integrity check and space freeing up feature for agentless Office 365 and Cloud File backup sets will still utilize Java memory from the AhsayCBS service.

  For example, if the AhsayCBS server is hosting 20 agentless (Run on Server) Office 365 backup jobs, each backup job has a default Java heap size of 2048M or 2GB of memory. The AhsayCBS server will require 48GB of RAM. That is 40GB (for the 20 Office 365 backup jobs) + 4GB (for the Operating System) + 4GB (for AhsayCBS service) = 48GB of RAM.

  Although based on the estimated 48GB RAM usage, a server with 64GB RAM is sufficient. For an on-premises server, it is recommended to provision additional RAM to meet unexpected on-going requirements and future business growth.

  Please refer to Chapter 6.9 Setting up memory for Run on Server (Agentless) Backups for more information on how to set up memory of agentless backup job.

  WARNING

  Review usage regularly, if more backup sets are created then more RAM may need to be added.

  If there is not enough RAM to accommodate all agentless Office 365 & Cloud File backup jobs running concurrently, then some backup jobs will not run.

2.2.5 AhsayCBS on Virtual Environment

It is more flexible when you deploy AhsayCBS on virtual machine environment, as you can increase memory size, process cores according to the actual need.

If VM snapshots are not required, please try to delete or reduce the amount of snapshots stored on your disk. Please also check on the storage requirement on virtual environment.

Additional Storage on Cloud

Besides local storage on your virtual machine, you can set up network storage, FTP/SFTP and common cloud storages (Google Drive, Dropbox, OneDrive, Rackspace, Wasabi etc.) for the AhsayCBS.

2.2.6 AhsayCBS on Standby Server

To ensure you have a backup of your Backup Server in the event of any hardware issues. We recommend replicating your data on the Backup Server to the Replication Server.

In case you need to shut down your Backup Server for maintenance, you can simply switch your Replication Server to the Backup Server, and change the DNS record from your current Backup Server to the Replication Server.

The hardware requirement of the Replication Server would be similar as your Backup Server and usually configured with more storage than your Backup Server.

Although both Backup Server and Replication Server are bundled in AhsayCBS, both backup and replication services are activated post installation.

It is not recommended to configure and use both services on one machine, as they will compete for system resources, i.e. CPU, memory and storage. This could affect the performance and stability of your backup service. Also, it will completely defeat the purpose of Replication Server as a backup or standby server to your Backup Server.

Please also check the details on the replication setup.

2.3 Storage Requirements

When you are setting up storage for your AhsayCBS, please consider the following:

- Type of RAID to fit your requirement (for local physical server or virtual environment)
- If you are deploying the storage locally, you are required to set up storage with redundancy, such as RAID 5 or RAID 6. This is important especially when you are delivering a backup service with good disk performance as well as good fault tolerance.
- Dedicated storage location for the system, user home and replication home
- Physical storage, virtual storage, and cloud storage

2.3.1 Redundant Disk Setup for Physical and Virtual Storage

We would recommend setting a rack mount server with several hard disk bays and/or attach a DAS for future expansion.

When you are setting up a rack mount server with 10 4TB hard disks, you may have concerns whether formatting the disk volume with RAID 5 or RAID 6. The following table lists out the differences between the 2 disk array setup.

	RAID 5	RAID 6
Total capacity	Around 36TB	Around 32TB
Fault tolerance	1-drive failure	2-drive failure
Speed gain	9x read speed	8x read speed

As the cost of hard disk has reduced a lot nowadays, it is strongly recommended that you format your disk volume with RAID 6 that maximizes the protection.

Dedicated Storage on AhsayCBS

When you partition the disk in your new server, please consider to set up dedicated virtual disk volumes for operating system, application system, user homes and replication home (if Replication Server is enabled), respectively. It is a common practice that application system home, user homes and replication homes are not located in the system volume, which may fill up easily, causing the system to become unstable.

Space required for application system home with replication setup

If you have replication setup on the Backup Server, please consider to dedicate a volume for the application home with sufficient disk space to store the transaction log. As there is no exact formula for estimating the size of the application home, the amount of space used for the transaction log is dependent upon:

- The period of time that the replication reached the replay mode
- The amount of daily backup data uploaded to your backup server

For example, if daily customer backup jobs generate an average of 20GB of data. Your previous replication takes about 5 days to the replay mode, and then your application home partition will require at least 100GB (20GB x 5 days) of free disk space.

This is only a general rule of thumb, this estimation does not take into consideration the growth of daily backup data, or the accumulation of backup data on the backup server which will result in a longer time to reach replay mode.

Setup multiple dedicated disks for each replication receiver.

If your Replication Server has setup several replication by multiple Backup Server, it is recommended that each receiver is located on its own individual disk. The advantage of this type of setup is that it minimizes the I/O on each disk, therefore improving replication performance.

Also, if one of the Backup Servers suffers an outage, there is the option of swapping the disk to the affected Backup Server.

2.3.2 Physical Storage

If you plan to have physical backup server, you are expected to have a fast local backup storage such as local hard disks, DAS or SAN. It is a solution for your business which wants to host the backup data with your physical backup server in your server room or data center.

Please avoid using network storage such as NAS, share drive on another computer as the backup and restore performance is lower.

2.3.3 File System Tuning for Virtual Storage Environment

If your backup server and user's data are hosted on a virtual environment, you need to check on the following to make sure the performance has been optimized.

When you set up a disk to attach on a virtual machine, please consider choosing the "thick provisioning" option or the "allocate all disk space" option. This is because choosing "thin provisioning" or "non-allocate all disk space" option may slow down disk performance when the amount of data grows.

Please also consider running the user home on a dedicated virtual disk, which is configured on fast and non-busy physical disks.

2.3.4 Cloud Storage

If you are considering hosting your backup server instance with a commercial cloud services provider such as Google, Amazon, Azure etc., you need to set up cloud storage for your user home, predefined destination or replication home as well.

2.4 Requirements for Using AhsayCBS User Web Console

In order to use the AhsayCBS user web console, you need the following:

- **Internet connection**

  You need to have Internet connection to access the AhsayCBS user web console.

- **Web browsers**

  The AhsayCBS user web console runs with all major browsers such as Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari. Please make sure that you are using the latest version of the browser.

> **NOTE**
>
> You can also monitor live backup and restore activities on the AhsayCBS user web console of your mobile device.
>
> **OpenDirect restore** of file backup sets or **Granular Restore** for VMware and Hyper-V backup sets performed using Windows File Explorer will not show up on the **Restore Status** tab in **Live Activities**. **Restore Status** tab in **Live Activities** only applies to the restore performed directly through AhsayOBM/ AhsayACB/ AhsayOBR or AhsayCBS user web console.

2.5 Temporary folder size for agentless Office 365 and Cloud file backups

All agentless Office 365 and Cloud File backup sets use a temporary directory location on the user home for backup and restore.

Each agentless Cloud File backup job requires at least 100 MB of free space for the temporary files generated during the backup job.

For each agentless Office 365 backup job, the required free space for the temporary files generated during the backup job depends on two factors:

- the number of Office 365 users selected in each backup set, the required free space is calculated as 300 MB per Office 365 user.
- the number of concurrent Office 365 backup jobs running on the AhsayCBS server.

Example:

- If an AhsayCBS server has only one backup set with 500 Office 365 users, it will require 150 GB (500 x 300 MB) disk space on the user home drive for the temporary files generated during the backup job.
- If there are multiple Office 365 backup sets running concurrently on AhsayCBS, then the free space required will be the sum of all the Office 365 users. If they are located on the same user home drive then the temporary folder on that drive will require 540 GB of free space for the temporary files generated during the backup job.

  Backup set 1 with 200 Office 365 users (200 x 300 MB) = 60 GB

  Backup set 2 with 100 Office 365 users (100 x 300 MB) = 30 GB

Backup set 3 with 500 Office 365 users (500 x 300 MB) = 150 GB

Backup set 4 with 1000 Office 365 users (1000 x 300 MB) = 300 GB

The following are the default temporary directory locations for the different operating systems:

- in Windows – C:\\Program Files\AhsayCBS\user\%username%\temp (the default path of the user home)
- in Linux/FreeBSD – /usr/local/cbs/user/%username%/temp
- in AhsayUBS – /ubs/mnt/eslsfw/obsr/user/%username%/temp

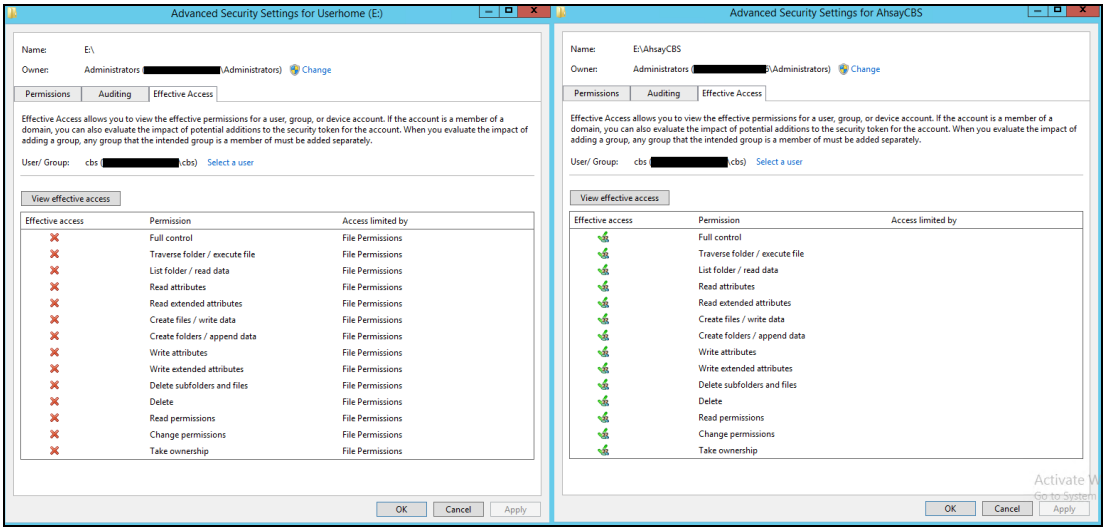
Ensure that the drive where the temporary directory is located has a lot of free space to accommodate all the agentless Office 365 and Cloud File backup jobs, especially if they will be running concurrently.

2.6 Permission Requirement for AhsayCBS on Windows with AhsayPRD for agentless backup

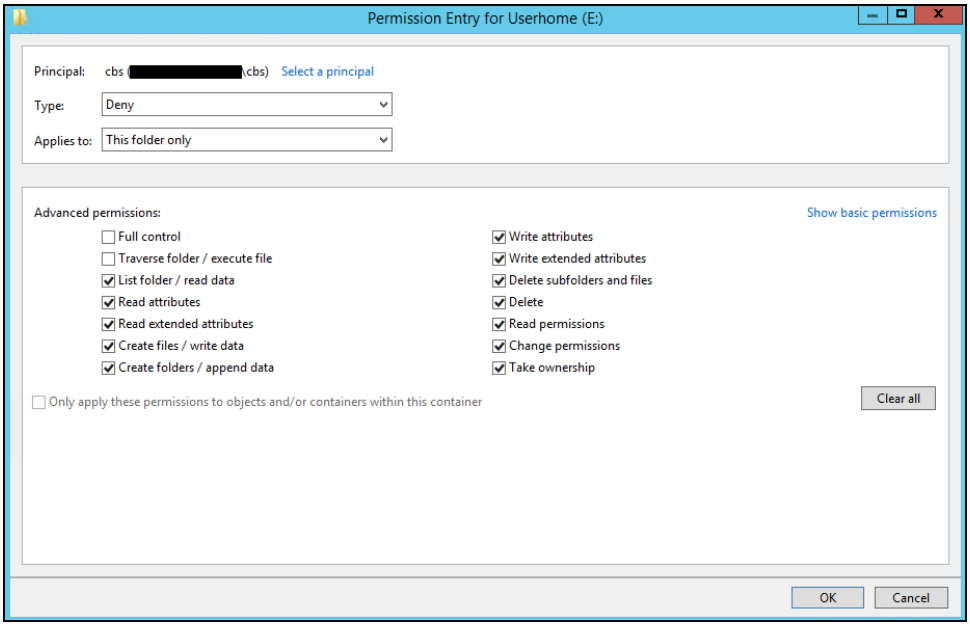
To ensure the AhsayCBS Windows service account has permission to access the user home folder of the AhsayCBS instance running with AhsayPRD, make sure the user account for the AhsayCBS service is granted permission to traverse folder / execute file for the Windows user running the AhsayCBS.

Please see below screenshots for reference:

The traverse folder / execute file in the advance security setting for the user home has no permission, it should be the same as the advanced security setting for AhsayCBS which is granted permission to traverse folder / execute file.



Make sure that the Traverse folder / execute file is granted permission.



3 Best Practices for Running Agentless Office 365 Backup

The following are some best practices we strongly recommend you follow before you start any Run on Server (Agentless) Office 365 backup and restore.

3.1 Recommended Number of Office 365 users on a Backup Set

To ensure that your Office 365 agentless backup set completes the backup job within 24 hours, it is recommended that a single Office 365 agentless backup set should not contain more than 2000 users. That is assuming that only small incremental daily changes will be made on the agentless backup set.

For a large number of Office 365 users that needs to be backed up, it is recommended that the users be divided into multiple backup sets. However, the actual number of Office 365 users in a single Office 365 agentless backup set may vary depending on the total number of Outlook, OneDrive and SharePoint items, as well as the total size of these items. The actual number of Office 365 users in a single Office 365 agentless backup set could be considerably less or could be more than 2000.

For details on the actual item count and size of the Office 365 user, it is recommended to check in the Microsoft 365 Admin Center. Please refer to How to view item count and storage used in Microsoft 365 Admin Center for more details.

Also, by splitting up the Office 365 users into separate backup sets, the more backup sets, a faster backup process can be achieved.

It is also a requirement that for every split backup set, it should have its own unique user account for authentication to minimize the probability of throttling from Microsoft.

For example, if there are 10 split Office 365 agentless backup sets, then there should be 10 unique user accounts for authentication.

For more detailed example, refer to Office 365 agentless backup set for a large number of Office 365 users.

3.2 Concurrent Backup Thread

The value of 4 concurrent backup threads is found to be the optimal setting for Agentless Office 365 backups to ensure the best backup performance, minimal resource usage, and lowest probability of throttling of AhsayCBS backup requests by Microsoft Office 365.

However, the number of concurrent backup threads can be increased if required. After increasing the number of threads, you should also increase the Java memory of the Agentless backup process as it is expected to consume more memory.

For more details on how to configure the number of threads for the Agentless Office 365 backup job please refer to How to configure backup threads on AhsayCBS.

For details on how to increase the Java memory of the Agentless backup process please refer to Setting up memory for Run on Server (Agentless) Backups

3.3 AhsayCBS server dedicated to Agentless Office 365 and Cloud File backup

The AhsayCBS server hosting the Agentless Office 365 and Cloud File backup should not host agent-based backups, so that all available server resources are dedicated to the Agentless Office 365 and Cloud File backups.

3.4 Compression Type Usage

It is recommended to use the Fast with optimization for local compression type for AhsayCBS Run on Server (Office 365 and Cloud file) backup jobs since it requires the lowest CPU usage which can reduce the overall server load.

Although the Fast with optimization for local compression consumes the least CPU utilization which increases the backup performance, it has the smallest compression ratio among all compression types thus may increase the overall file storage size and the backup set cost.

.

4 Network and Firewall Settings

4.1 Overview

In this section, we shall discuss the network and firewall settings required for the AhsayCBS. These include the access to the web interface, license activation, backup and restore processes, email port settings and replication port settings.

As a prerequisite, a fixed remote IP and internal IP are required for the AhsayCBS. Also, the firewall should support the TLSv1 cryptographic protocol.

4.2 Network Settings

4.2.1 Static IP Address

The use of dynamic IP addresses for AhsayCBS domain names may result in an unstable backup service, or replication process restarting whenever the IP address re-cycles.

A static IP address will ensure the remote IP address sent by AhsayCBS to the Ahsay license server will remain the same during daily routine license checks. This will avoid potential license errors, i.e. 1011 or 1012 license errors which could result in the automatic shutdown of your AhsayCBS service.

It is strongly recommended that you use a static IP address for your AhsayCBS server to ensure a stable and reliable backup service.

4.2.2 Network Load Balancing Configuration

For AhsayCBS servers which are configured with network load balancing, i.e. a dual WAN router or Round Robin routing. A static route should be configured for your AhsayCBS server connection to the Ahsay License Server (**lic.ahsay.com**). This will ensure the remote IP address sent by AhsayCBS to the Ahsay License Server will remain the same during daily routine license checks. This will avoid potential license errors, i.e. 1011 or 1012 license errors which could result to the automatic shutdown of your AhsayCBS service.

In addition, any switching between the two network connections will cause connection problems between Backup Server and Replication Server due to the change in IP address. This will result in the replication process restarting itself.

4.2.3 MAC Address

A valid MAC address is also needed as part of the license activation and validation process, otherwise the evaluation or production license keys will not be applied to AhsayCBS.

In Windows open a command prompt and type `ipconfig /all`. The MAC address will be displayed as the Physical Address.

```
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : w2k16R2-std
   Primary Dns Suffix  . . . . . . . :
```

```
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Private:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network
Connection #2
   Physical Address. . . . . . . . . : 00-0C-29-E4-A7-F4
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . :
fe80::b8c9:1b18:e502:59e6%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.10.12(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.252.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 419433513
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-EC-7D-6E-00-0C-
29-E4-A7-EA

   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Public:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network
Connection
   Physical Address. . . . . . . . . : 00-0C-29-E4-A7-EA
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . :
fe80::c920:be27:8595:e668%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.16.10.12(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.252.0.0
   Default Gateway . . . . . . . . . : 10.16.0.1
   DHCPv6 IAID . . . . . . . . . . . : 301993001
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-EC-7D-6E-00-0C-
29-E4-A7-EA

   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{9522CFAB-2A5A-45DB-B5E9-61D594C78BC2}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter isatap.{324988F8-C083-40FE-A532-9BC6BD88603B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #2
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

In Linux open a ssh and type `ifconfig`. The MAC address is the ether.

```
ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.16.30.2  netmask 255.252.0.0  broadcast 10.19.255.255
        inet6 fe80::49c2:9525:f44c:ff19  prefixlen 64  scopeid
0x20<link>
        ether 00:0c:29:fb:8d:39  txqueuelen 1000  (Ethernet)
        RX packets 1825484  bytes 1277510886 (1.1 GiB)
        RX errors 0  dropped 255  overruns 0  frame 0
        TX packets 987689  bytes 1043791281 (995.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 6394  bytes 7067982 (6.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6394  bytes 7067982 (6.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast
192.168.122.255
        ether 52:54:00:73:02:43  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

4.2.4 Test Connectivity

The AhsayCBS server must be able to ping its hostname and activate license key successfully to ensure that the SMTP server setting will work properly.

In Windows open a command prompt and type `hostname`. Then type `ping "hostname"`.

```
hostname
w2k16R2-std

ping w2k16R2-std

Pinging w2k16R2-std [fe80::b8c9:1b18:e502:59e6%15] with 32 bytes of
data:
Reply from fe80::b8c9:1b18:e502:59e6%15: time<1ms
Reply from fe80::b8c9:1b18:e502:59e6%15: time<1ms
Reply from fe80::b8c9:1b18:e502:59e6%15: time<1ms

Ping statistics for fe80::b8c9:1b18:e502:59e6%15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

In Linux/FreeBSD open a ssh and type `hostname`. Then type `ping "hostname"`.

```
#  hostname
freebsd11

# ping freebsd11
PING freebsd11 (10.16.30.21): 56 data bytes
64 bytes from 10.16.30.21: icmp_seq=0 ttl=64 time=0.073 ms
64 bytes from 10.16.30.21: icmp_seq=1 ttl=64 time=0.086 ms
64 bytes from 10.16.30.21: icmp_seq=2 ttl=64 time=0.097 ms
-- freebsd11 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.073/0.083/0.097/0.009 ms
```

4.3 Firewall Settings

4.3.1 Ports and Settings

After you have finished setting up your AhsayCBS server, please ensure you have updated your firewall settings to allow network traffic through the following ports:

Port	Description
80	HTTP port for incoming backup and restore traffic, and browsing the AhsayCBS web interface.
443	HTTPS port for incoming backup and restore traffic, and browsing the AhsayCBS web interface.
8081	Default port used by AhsayCBS for Run on Server (Agentless) Office 365 and Cloud File backup on local IP address 127.0.0.1. If the default port is occupied, then AhsayCBS will automatically acquire the next available free port from 8081 to 9080. If all ports in that range are occupied, then AhsayCBS service is stopped.
25	Outgoing SMTP port to the SMTP server.
111	Port Mapper
1058	Mount Port ** Required for Run Direct on AhsayCBS
2049	Port for NFS Service
Any incoming TCP port(s)	Any incoming TCP port(s) used by previous version of replication receiver(s), e.g. 9444, 9445…

4.3.2 TCP Ports 80 and 443

It is recommended to expose only TCP ports 80 and 443 to the public on your firewall. Please consult the user's manual of your firewall for more information on how to do so.

4.3.3 SMTP Server

AhsayCBS supports SMTP server which use either TLS v1.0, v1.1 or v1.2.

4.3.4 Restricting Access on Administration Panel

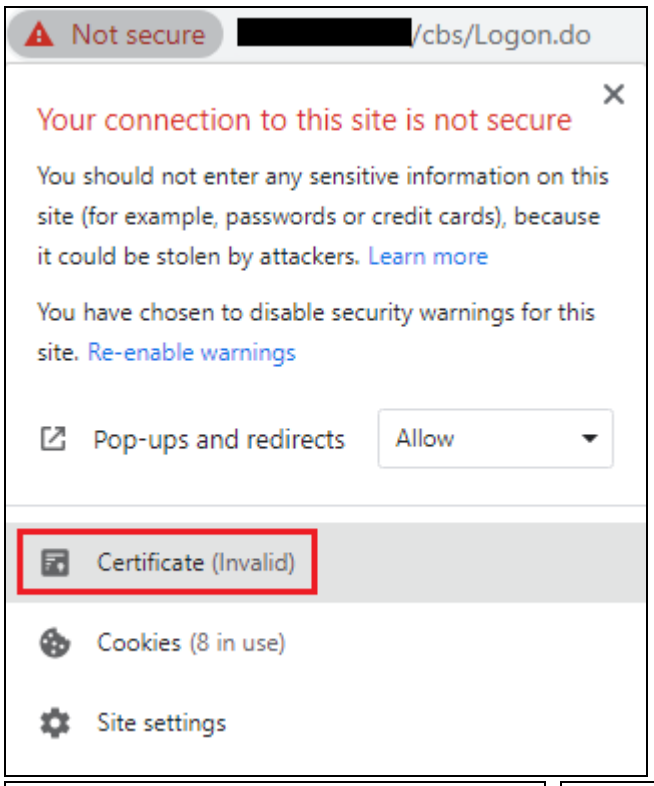
If you do not wish to offer your client access to the AhsayCBS console to manage their accounts, it is recommended to implement IP address restrictions to harden the security. You may do this by restricting a range of IP addresses which can access your AhsayCBS console. For more information please refer to Chapter 5.1.1.5 on page 41 of the AhsayCBS v8 Administrator's Guide.

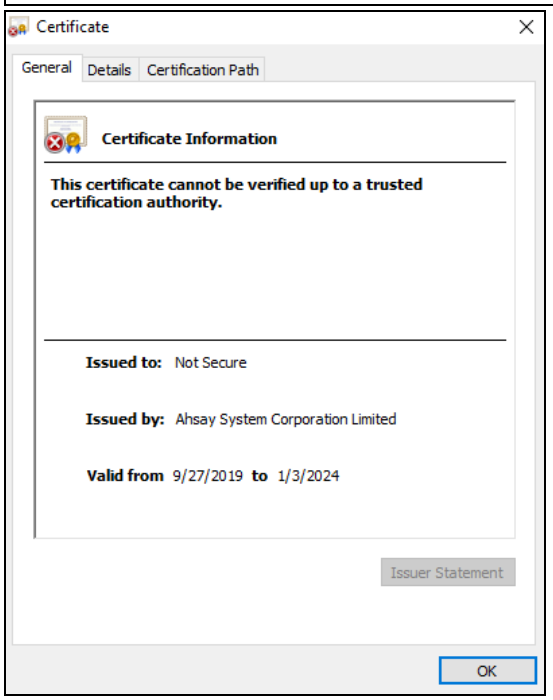
4.3.5 Replication Using Cross Over Cable

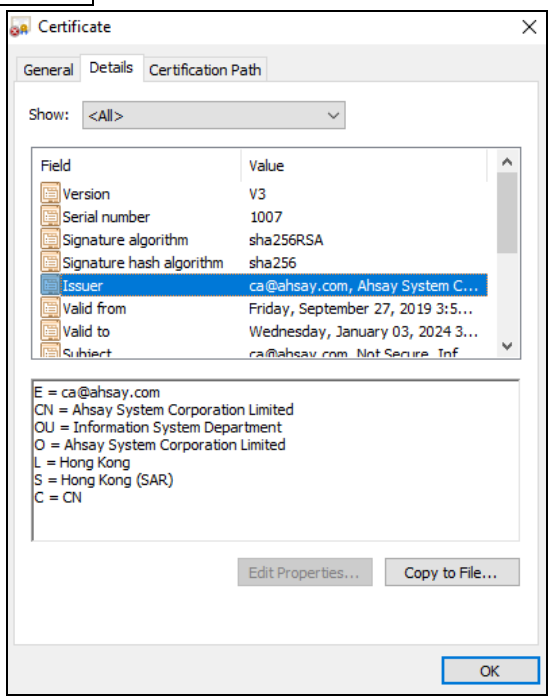
It is not recommended to set up a Backup Server and a Replication Server using a cross over cable for replication, which will result in connection and performance issues.

If the Backup Server and the Replication Server are located on the same site they should be connected via a switch.

4.4 Certificate Settings







As the certificate provided by Ahsay System Corporation Limited is the dummy certificate, which means it can only be used for testing and evaluation but not for production use. So please purchase the offical trusted certificate before using AhsayCBS.

NOTE

A valid SSL certificate from a trusted CA is also required if you are going to use Two-Factor Authentication with https protocol. Otherwise, you will have to use http instead which means all AhsayOBM/AhsayACB users with Two-Factor Authentication enabled will need to connect using http as well.

You can refer to the following article for trusted certificate authority (CA) certificates list for AhsayCBS version 8.1.0.24. or above:
https://wiki.ahsay.com/doku.php?id=public:8028_faq:trusted_ca_list_for_v8&s

Please refer to AhsayCBS v8 Administrator's Guide for more details about the certification. You can also refer to the folowing link to search about the details about SSL certificate installation:
https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_services_express-installation-services_ssl

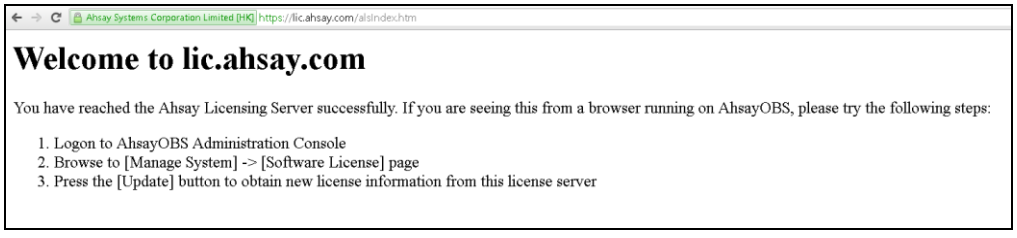
4.5 Ahsay License Server

The AhsayCBS server is required to access the Internet to connect to our license server **lic.ahsay.com** using the https protocol in order to activate the trial license key or validate a purchase key.

Please ensure the firewall outbound connection settings are enabled and the TLSv1.2 setting is allowed.

- **Windows**

  To verify connection to the Ahsay license server, please open a browser on the Windows machine and load https:/lic.ahsay.com in a browser. If the connection is successful, you will see the following screen.



- **Linux**

  To verify connection to the Ahsay license server, use the **`telnet`** command. If the connection is successful, you will see the following message.

```
# telnet lic.ahsay.com 443
Trying 203.186.85.237...
Connected to lic.ahsay.com.
Escape character is '^]'.
```

To verify TLSv1.2 is enabled, use **`openssl s_client`** command. If TLSv1.2 is enabled, you will see the following message.

```
# openssl s_client -connect lic.ahsay.com:443 -tls1_2

CONNECTED(00000003)

depth=3 C = US, O = "The Go Daddy Group, Inc.", OU = Go Daddy
Class 2 Certification Authority

verify return:1

depth=2 C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com,
Inc.", CN = Go Daddy Root Certificate Authority - G2

verify return:1

depth=1 C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com,
Inc.", OU = http://certs.godaddy.com/repository/, CN = Go Daddy
Secure Certificate Authority - G2

verify return:1

depth=0 1.3.6.1.4.1.311.60.2.1.3 = HK, businessCategory = Private
Organization, serialNumber = 0498825, C = HK, L = Lai Chi Kok, O
= Ahsay Systems Corporation Limited, CN = ahsay.com

verify return:1

---

Certificate chain

 0 s:/1.3.6.1.4.1.311.60.2.1.3=HK/businessCategory=Private
Organization/serialNumber=0498825/C=HK/L=Lai Chi Kok/O=Ahsay
Systems Corporation Limited/CN=ahsay.com

   i:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com,
Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure
Certificate Authority - G2

 1 s:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com,
Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure
Certificate Authority - G2

   i:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./CN=Go
Daddy Root Certificate Authority - G2

 2 s:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./CN=Go
Daddy Root Certificate Authority - G2

   i:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2
Certification Authority

 3 s:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2
Certification Authority

   i:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2
Certification Authority

---

Server certificate

-----BEGIN CERTIFICATE-----

MIIH8DCCBtigAwIBAgIJANK9EdRBepEyMA0GCSqGSIb3DQEBCwUAMIG0MQswCQYD

VQQGEwJVUzEQMA4GA1UECBMHQXJpem9uYTETMBEGA1UEBxMKU2NvdHRzZGFsZTEa

MBgGA1UEChMRR29EYWRkeS5jb20sIEluYy4xLTArBgNVBAsTJGh0dHA6Ly9jZXJ0

cy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5LzEzMDEGA1UEAxMqR28gRGFkZHkgU2Vj

dXJlIENlcnRpZmljYXRlIEF1dGhvcml0eSAtIEcyMB4XDTIwMDIyODAxMjI1NFoX

DTIyMDQxNDEzMjQwM1owgakxEzARBgsrBgEEAYI3PAIBAxMCSEsxHTAbBgNVBA8T

FFByaXZhdGUgT3JnYW5pemF0aW9uMRAwDgYDVQQFEwcwNDk4ODI1MQswCQYDVQQG
```

EwJISzEUMBIGA1UEBxMLTGFpIENoaSBLb2sxKjAoBgNVBAoTIUFoc2F5IFN5c3Rl
bXMgQ29ycG9yYXRpb24gTGltaXRlZDESMBAGA1UEAxMJYWhzYXkuY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzVy+OD4alpafXwiOYEKQikNFbMvu
2hysHv6t6g3rX2dBOrtboCWwP9RZOV2g4x5DIRZj7duR2wjhAY0HaE3DN3fr6TnL
FJPwg+7IYTt4sd7ovtHJDE1PcEuizjyL2k6XRxcoRajTzAMXDTLZsyJNuRNMSusa
TVWpHyhgpXk+D1FgOg2DaPojuYLPW/TkolbFMvj08BBOYqYrcRfV6y+Syz0/PeZ+
Gb9+kkVB+FP4pJMDxv/vlFtbakJDIpbtr01VfgjLHqh0gMMBTnrxsBXrLvhv2GHi
3Lr7TNJb7Hf4JAs9cR3w0kkK1cCK1vvyokQ2QNLEYwexbi+4QMpfpQXd/wIDAQAB
o4IEDDCCBAgwDAYDVR0TAQH/BAIwADAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYB
BQUHAwIwDgYDVR0PAQH/BAQDAgWgMDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly9j
cmwuZ29kYWRkeS5jb20vZ2RpZzJzMy0xNS5jcmwwXAYDVR0gBFUwUzBIBgtghkgB
hv1tAQcXAzA5MDcGCCsGAQUFBwIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFk
ZHkuY29tL3JlcG9zaXRvcnkvMAcGBWeBDAEBMHYGCCsGAQUFBwEBBGowaDAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMEAGCCsGAQUFBzAChjRo
dHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvZ2RpZzIu
Y3J0MB8GA1UdIwQYMBaAFEDCvSeOzDSDMKIz1/tss/C0LIDOMIH5BgNVHREEgfEw
ge6CCWFoc2F5LmNvbYINd3d3LmFoc2F5LmNvbYIPZm9ydW0uYWhzYXkuY29tgg1s
aWMuYWhzYXkuY29tghB3d3cudWsuYWhzYXkuY29tghVwYXJ0bmVycy11cy5haHNh
eS5jb22CDnNob3AuYWhzYXkuY29tgg1pZHAuYWhzYXkuY29tgg1wY3AuYWhzYXku
Y29tghB3d3cuYWhzYXkuY29tLmNugg1sbXAuYWhzYXkuY29tghVwYXJ0bmVycy11
ay5haHNheS5jb22CFXBhcnRuZXJzLmFoc2F5LmNvbS5jboIMa2IuYWhzYXkuY29t
MB0GA1UdDgQWBBQU/GniKbSMjgEmaqndKdtzS0DqlDCCAX0GCisGAQQB1nkCBAIE
ggFtBIIBaQFnAHUApLkJkLQYWBSHuxOizGdwCjw1mAT5G9+443fNDsgN3BAAAAFw
iWO3kgAABAMARjBEAiA+hEdDmd5DpqSzX43y7ri9ByGIyN3cuzzZG+bUbxMeZQIg
PhPHCcuSpHmdZPdiqzd9dkoFfT1a7mBZgA5X/Qn8sXIAdwDuS723dc5guuFCaR+r
4Z5mow9+X7By2IMAxHuJeqj9ywAAAXCJY7tKAAAEAwBIMEYCIQDyF8exjOGxWWqn
WjJsCIMdmhNa5TQP4P7S0eILTZxTQQIhAIsb+1B1r2xKnxyfO/5Gjzozgf71RNd2
y5j52nS3fjQ5AHUAVhQGmi/XwuzT9eG9RLI+x0Z2ubyZEVzA75SYVdaJ0N0AAAFw
iWO9ogAABAMARjBEAiBoPXKsSdkni3BlFRpz01zcyW6o+GOGbNKM+3JAFBoFrwIg
TNKIG8+hkzknLcbhJIJRj8ivOSZxYhYt0wtnfSxKXsIwDQYJKoZIhvcNAQELBQAD
ggEBAHtl3dePp2Plp8VLRr8xhpHM76K8u1HBBxF/Joucv68vmelCN+1mY7Z7sloI
0lz4tGBh51DK8gerVKUrSgxFk4W/E5PVc0QMpoK6rr8DpwOGbShjSyfGvkAOOwem
tv8L7rEtVIldWS1n+oeDPlLOB92RBxWUhiXt8QE9GpV4pPcKrMgNACkoWQZxDKYW
JNNhwsTomktzu0sLO0yJFhGGmq1htV/RCx7LJ6gZl7/fLcFtzVrd27elaA+iQhEb
oCmwZgnijIT49EE6pY0octFYRtEm2GCcq79rAqzVPJnWWaOdbzSwJaurtliCyyZ+
/7/2hEy9EtpStmAf9KVeUglC76c=

-----END CERTIFICATE-----

subject=/1.3.6.1.4.1.311.60.2.1.3=HK/businessCategory=Private Organization/serialNumber=0498825/C=HK/L=Lai Chi Kok/O=Ahsay Systems Corporation Limited/CN=ahsay.com

issuer=/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2

```
No client certificate CA names sent
Server Temp Key: ECDH, prime256v1, 256 bits
---
SSL handshake has read 6137 bytes and written 373 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID:
6C1B0AEEE18BC2A83599A8058564E766063AA3AC87CBA6797EDED5BC77F900F5
    Session-ID-ctx:
    Master-Key:
3F2E8F3E9F0F5AA3719F07B91B91D0685878D1C9E7A4D2B79F53ED640350C3624
D4ED338A6A2397C095E2F1186BF6C5C
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - 1b ed e6 48 ab 80 f9 a7-f8 0b f1 1d bc 93 70
ab   ...H..........p.
    0010 - 94 8b dc ab da 60 57 90-5d ea 10 14 66 c5 80
62   .....`W.]...f..b
    0020 - b2 f1 ba e0 49 fc 48 b6-4b 11 46 bb b9 e7 dd
d8   ....I.H.K.F.....
    0030 - 12 28 36 85 3d 2c bf 1a-61 e9 76 1a 10 d1 d2
f1   .(6.=,..a.v.....
    0040 - e1 28 74 5e 1a 1a 0b 73-d2 c8 4f de 6e e1 d2
6f   .(t^...s..O.n..o
    0050 - ee 6b 63 e7 ad dd d4 9c-b7 c4 08 19 9e 2c fd
d7   .kc..........,..
    0060 - c1 7e 65 dc 29 f1 26 d7-48 7b 29 d1 88 17 f5
e6   .~e.).&.H{).....
    0070 - 49 2c 50 bf 4c 90 25 ac-34 c1 be 40 00 33 0c 65
I,P.L.%.4..@.3.e
    0080 - cf f9 13 a8 c2 d7 82 cf-b2 bc d6 ff 7b 15 9b
6e   ............{..n
    0090 - d9 ce 58 77 a2 c2 e2 c9-e4 2d a5 a0 e4 29 fd
a6   ..Xw.....-...)..
    00a0 - 2c 21 af bf da 3e 75 38-71 45 e4 0f 4f 36 6a
58   ,!...>u8qE..O6jX
```

```
    Start Time: 1612168629
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
closed
```

- **FreeBSD**

  To verify connection to the Ahsay license server, use the **`fetch`** command. If the connection is successful, you will see the following message.

```
# fetch https://lic.ahsay.com/alsIndex.htm
alsIndex.htm                                    100% of  782  B
3336 kBps 00m00s
```

  You also need to open the alsIndex.htm to verify the contents. You can open it by using a text editor like vi.

```
# vi alsIndex.htm
<html>^M
<head>^M
<meta http-equiv="Content-Type" content="text/html;
charset=windows-1252">^M
<meta http-equiv="Content-Language" content="en-us">^M
<meta name="GENERATOR" content="Microsoft FrontPage 4.0">^M
<meta name="ProgId" content="FrontPage.Editor.Document">^M
<title>Welcome to lic.ahsay.com</title>^M
</head>^M
<body>^M
<h1>Welcome to lic.ahsay.com</h1>^M
<p>You have reached the Ahsay Licensing Server successfully. If
you are seeing this from a browser running on AhsayOBS, please
try the following steps: </p>^M
<ol>^M
  <li>Logon to AhsayOBS Administration Console</li>^M
  <li>Browse to [Manage System] -&gt; [Software License]
page</li>^M
  <li>Press the [Update] button to obtain new license information
from this license server</li>^M
</ol>^M
^M
</body>^M
</html>^M
```

4.6 Ahsay Push Notification Server

The Ahsay push notification server is needed to receive push notifications in your mobile device to log in to AhsayCBS, AhsayOBM and AhsayACB when using Ahsay Mobile for Two-Factor Authentication.

4.6.1 AhsayCBS public IP address

The AhsayCBS public IP address or domain must be resolvable locally on the AhsayCBS server, i.e. ping your-cbs-server.com on the AhsayCBS server itself must be successful

Example:

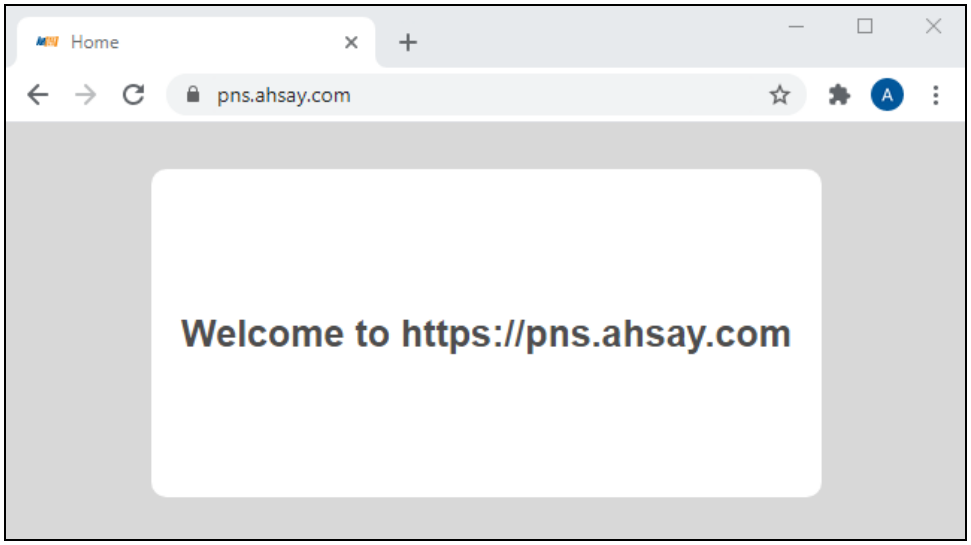
```
C:\ping your-cbs-server.com

Pinging 125.2.17.44 with 32 bytes of data:
Reply from 125.2.17.44: bytes=32 time<1ms TTL=128
Reply from 125.2.17.44: bytes=32 time<1ms TTL=128
Reply from 125.2.17.44: bytes=32 time<1ms TTL=128
Reply from 125.2.17.44: bytes=32 time<1ms TTL=128

Ping statistics for 125.2.17.44:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:

    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4.6.2 Firewall configuration

Please ensure the firewall is configured to allow outbound connections to pns.ahsay.com via port 80 and 443.

- **Windows**

  To verify connection to the Ahsay push notification server, please open a browser on the Windows machine and load https:/pns.ahsay.com in a browser. If the connection is successful, you will see the following screen.



- **Linux and FreeBSD**

  To verify connection to the Ahsay push notification server, use the **`telnet`** command. If the connection is successful, you will see the following message.

```
# telnet pns.ahsay.com 443
Trying 52.168.142.119...
Connected to pns.ahsay.com.
Escape character is '^]'.
```

- **AhsayUBS**

  To verify connection to the Ahsay push notification server, use the **`fetch`** command. If the connection is successful, you will see the following message.

```
# fetch --no-verify-peer https://pns.ahsay.com/
fetch: https://pns.ahsay.com/: size of remote file is not known
fetch.out                                             1291  B
5384 kBps 00m00s
```

  To check the contents of fetch.out use the `cat` command.

```
# cat fetch.out
<!DOCTYPE HTML>
<html>
    <head>
        <title>Home</title>
        <meta http-equiv="Content-Type" content="text/html;
charset=UTF-8" />
        <style>
            body {
                margin: 0;
                padding: 0;
                font-family: Arial, Helvetica, sans-serif;
            }
            .container {
                height: 100vh;
                display: flex;
                flex-direction: column;
                align-items: center;
                justify-content: center;
                background: #d8d8d8;
            }
            .content {
                border-radius: 10px;
                background: #FFF;
                min-height: 200px;
                min-width: 200px;
                padding: 10px 20px;
```

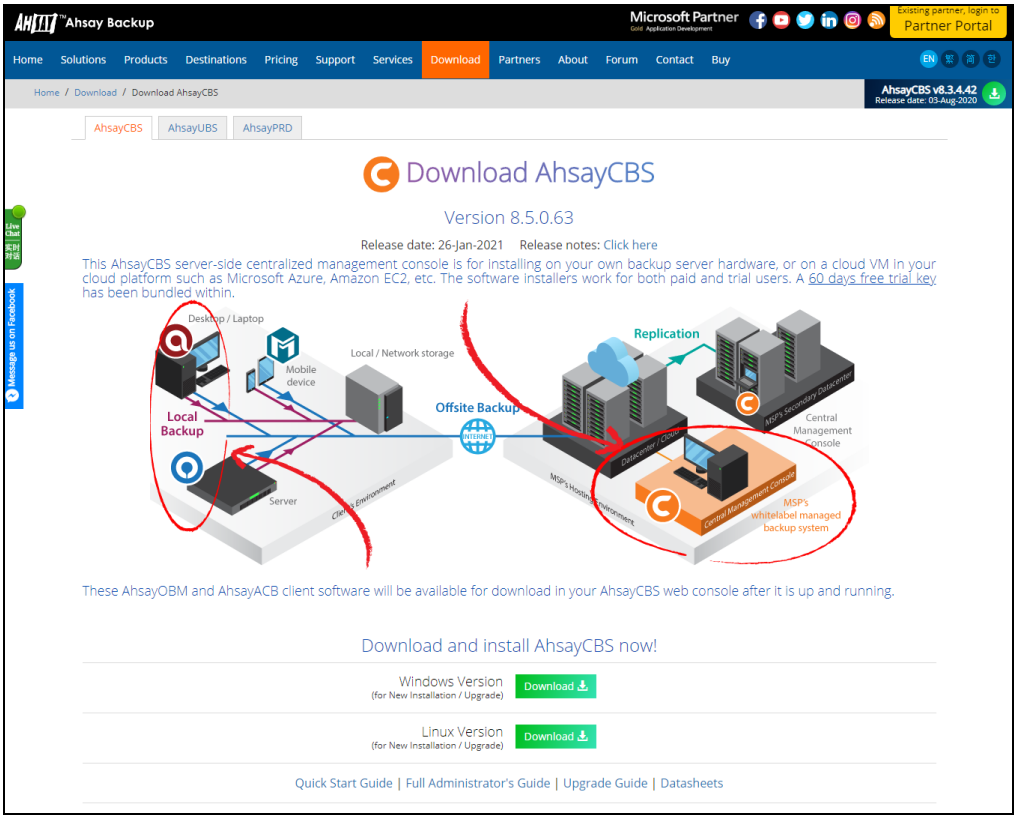
```
                display: flex;
                justify-content: center;
                align-items: center;
            }
            .title {
                font-size: 25px;
                font-weight: bold;
                color: #4d4d4d;
            }
        </style>
    </head>
    <body>
        <div class="container">
            <div class="content">
                <div class="title">Welcome to
https://pns.ahsay.com</div>
            </div>
        </div>
    </body>
```

5 Download and Install AhsayCBS

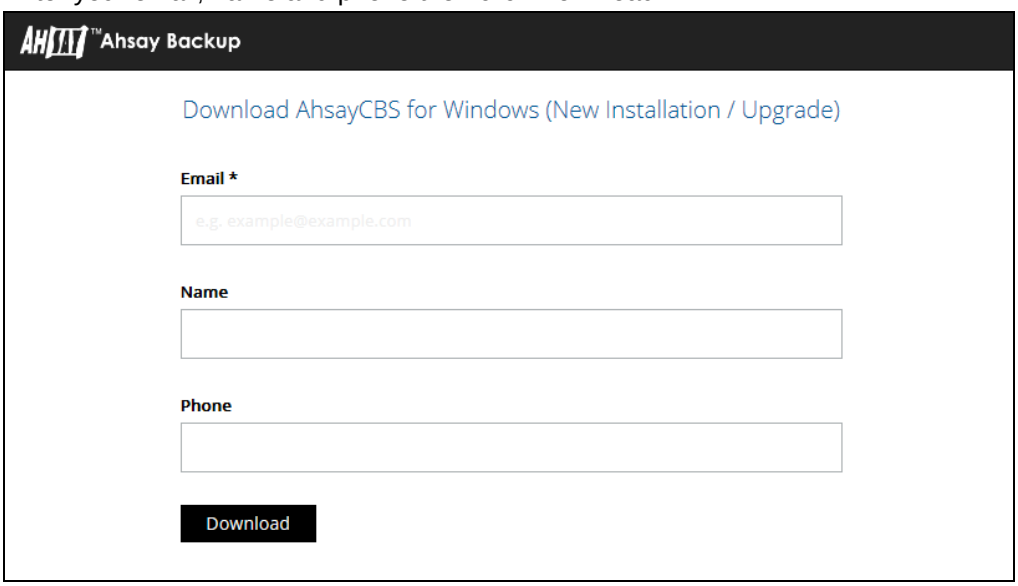
5.1 Installation on Windows

1. Log in as admin on your Windows machine.

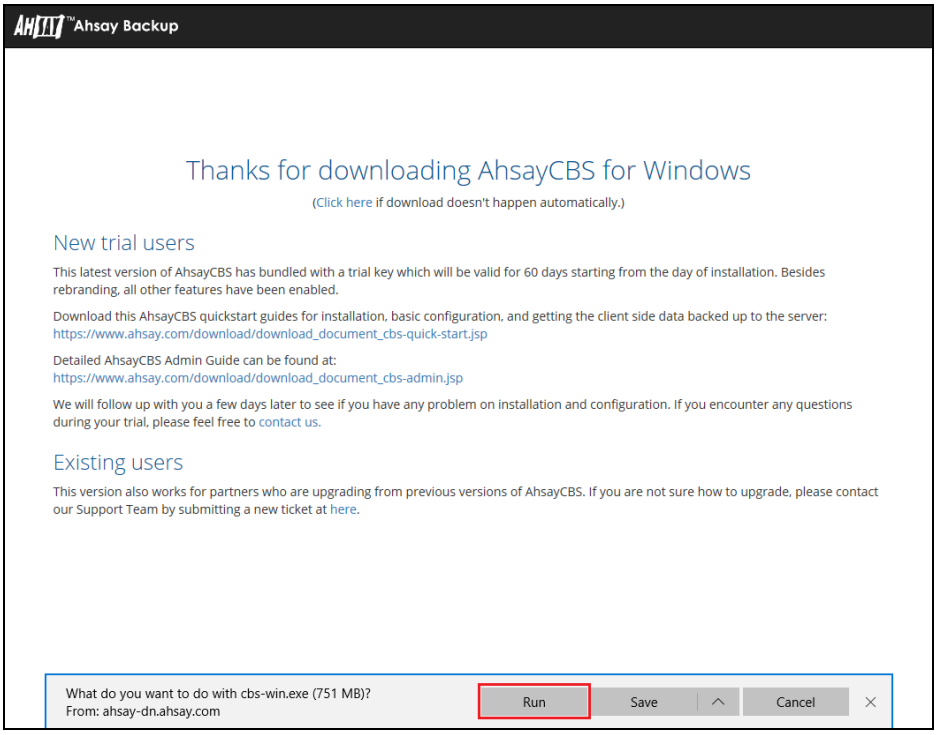
2. In a browser, download the AhsayCBS installation package **cbs-win.exe** from the Ahsay website by clicking the Download button.



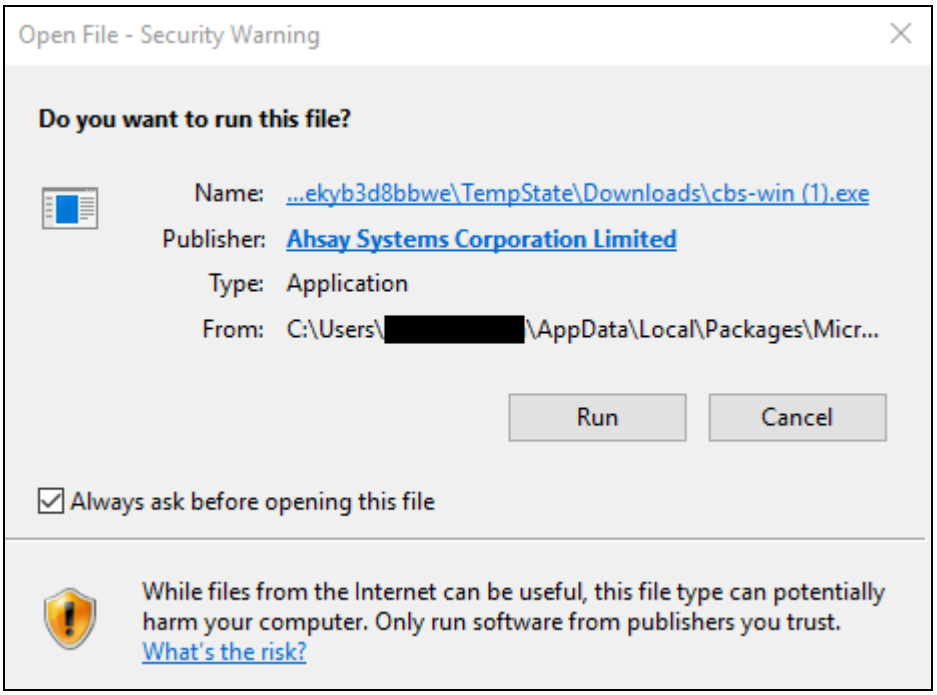
3. Enter your email, name and phone then click Download.



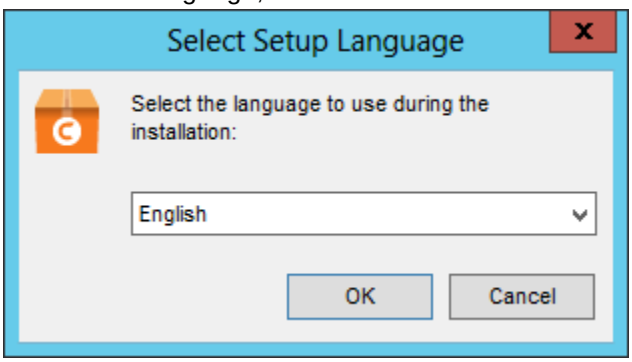
4. Click on Run to start the download.



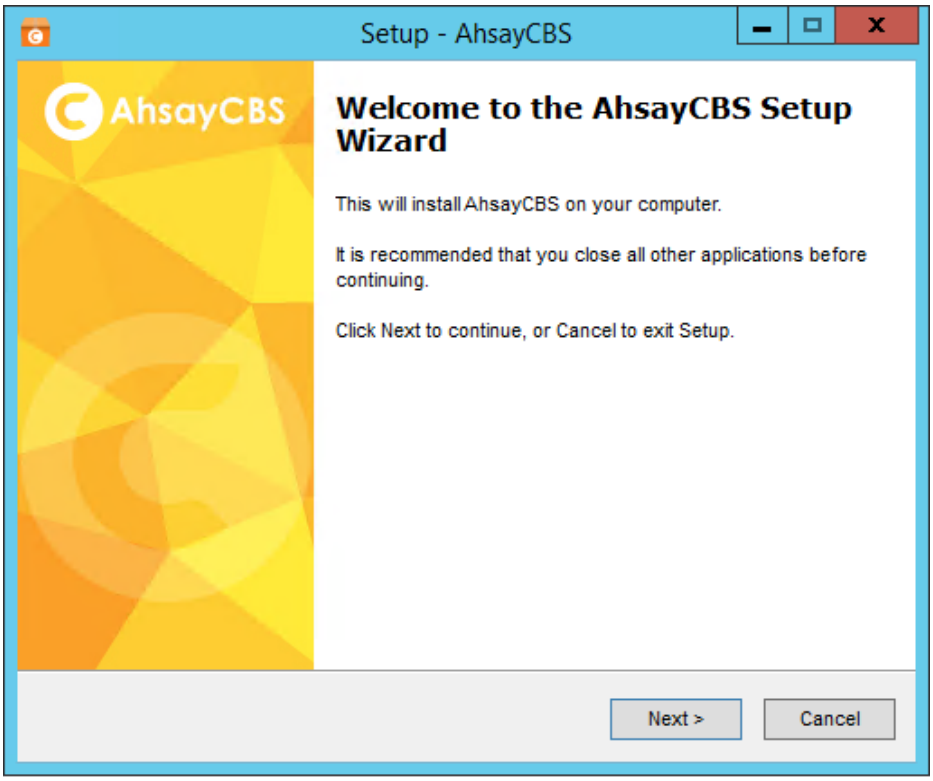
5. Run the downloaded installer.



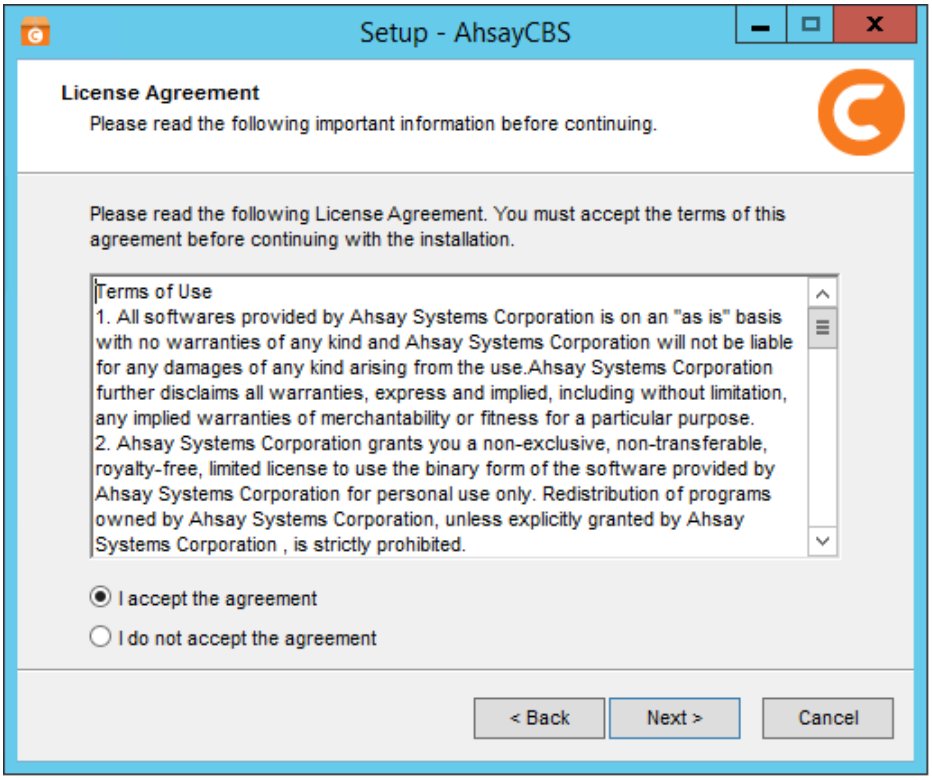
6. Choose the language, and then click **OK** to continue.



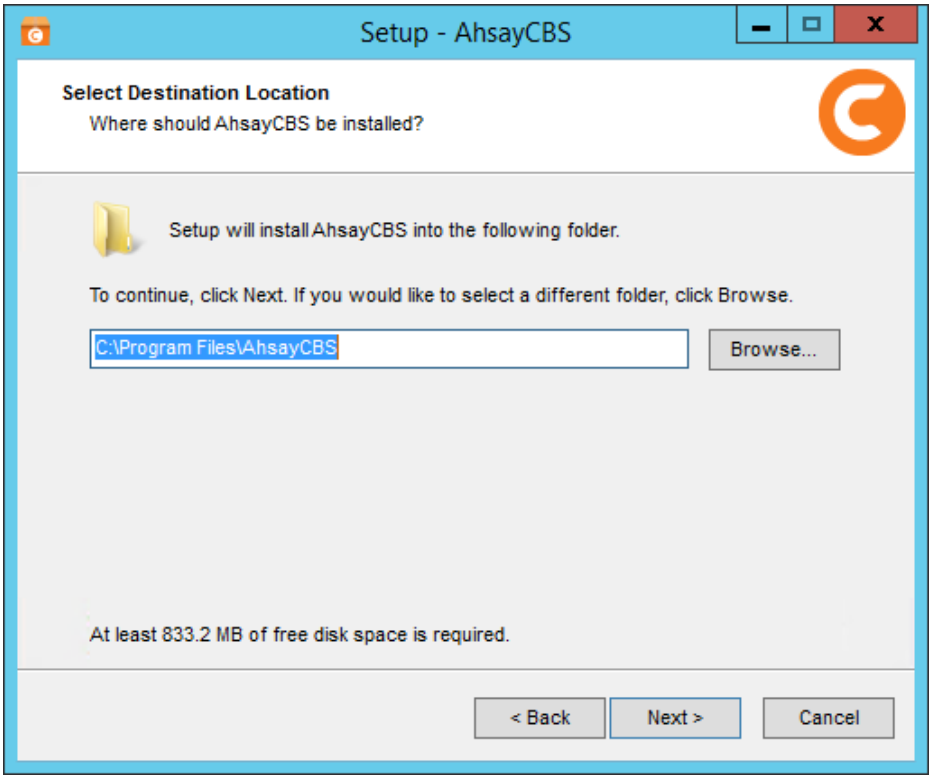
7. Click **Next** to continue.



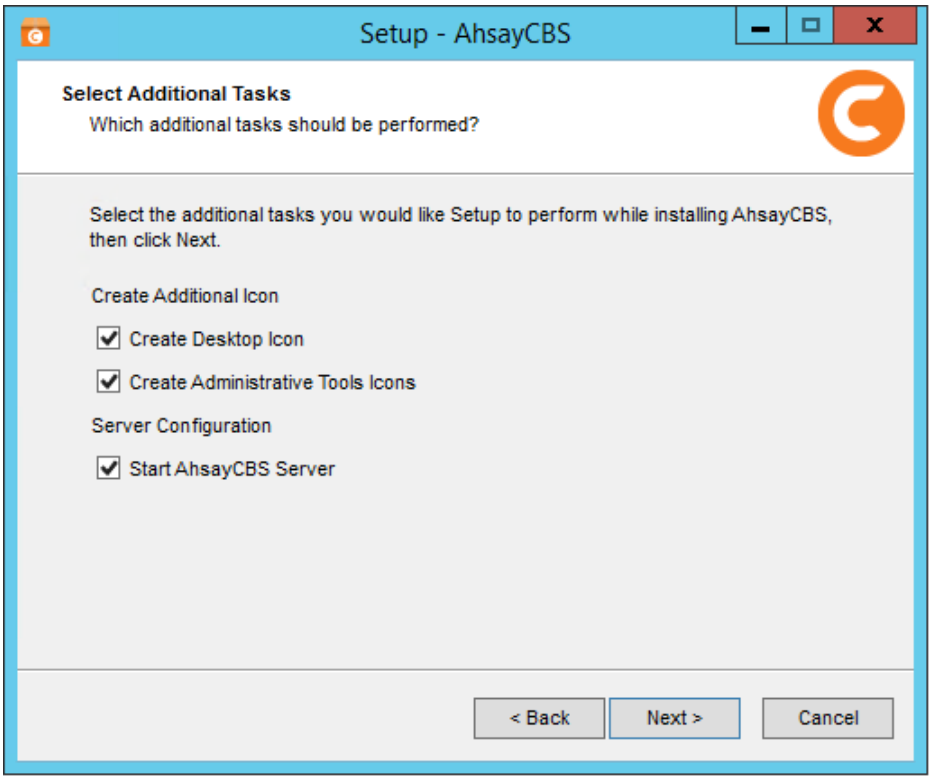
8. Select **I accept the agreement** after reading the license agreement. Then, click **Next** to continue.



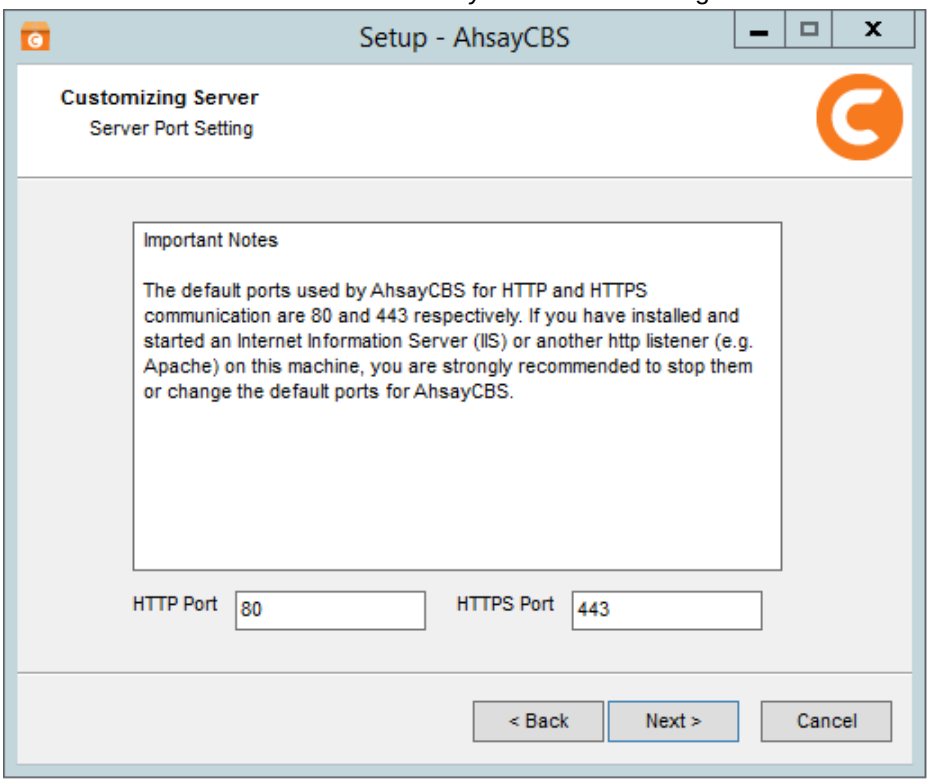
9. Choose the installation directory. Then, click **Next** to continue.



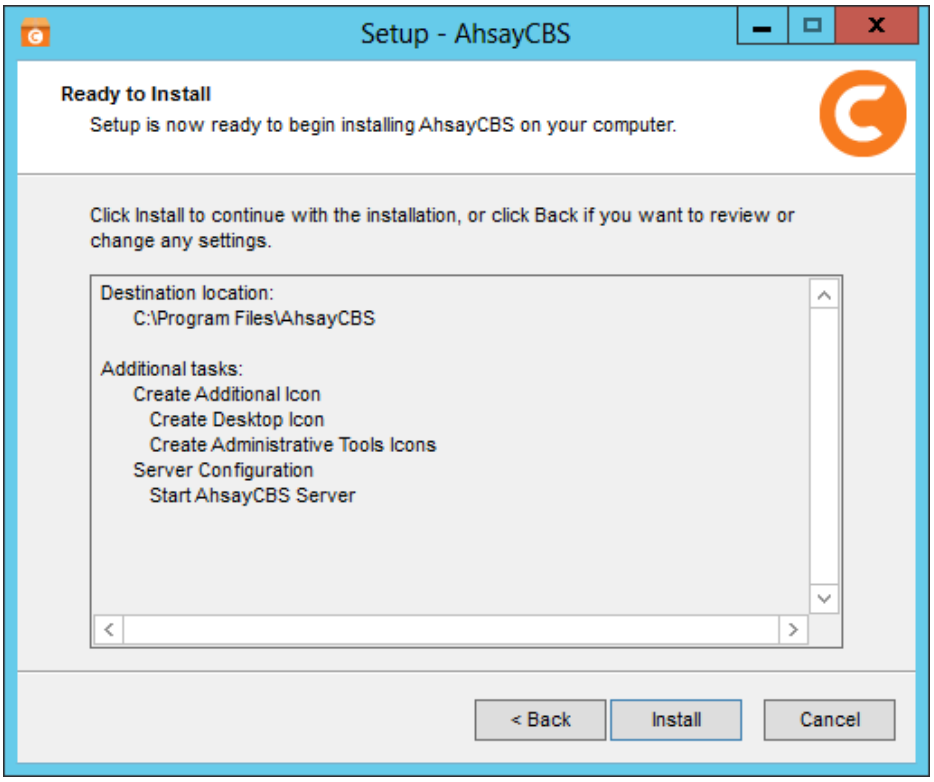
10. Click **Next** to continue.



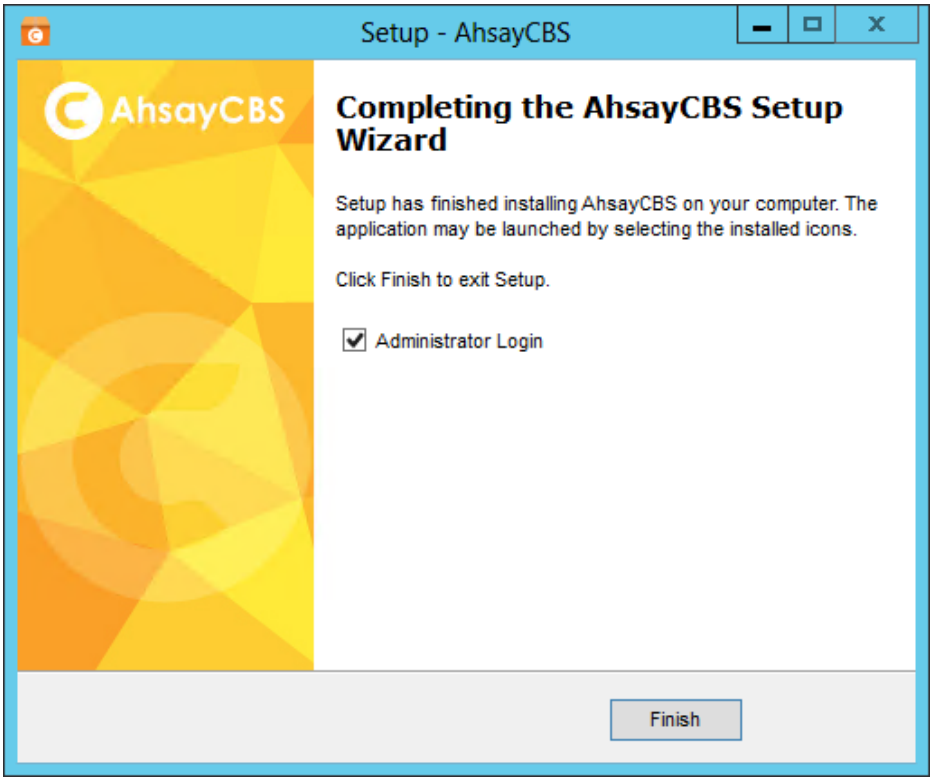
11. Enter the ports to be used by AhsayCBS. By default, the ports are 80 and 443 (HTTP and HTTPS respectively). If these ports have been used by other applications, e.g. Microsoft IIS, Apache or other applications, please use alternative ports such as 8080 and 8443. Click **Next** to continue when you are done setting.



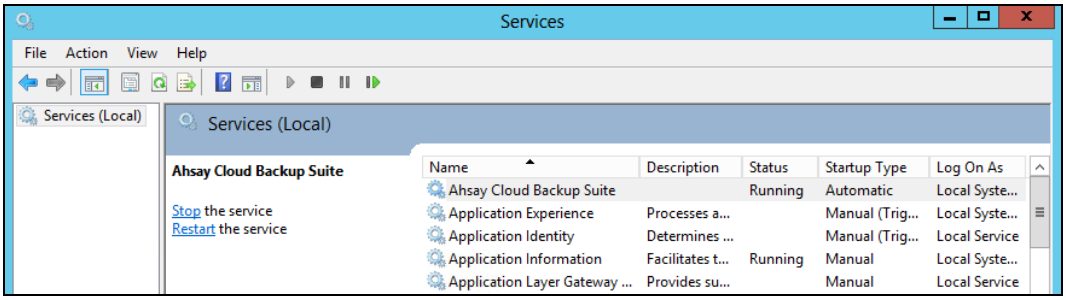
12. Click **Install** to start the installation.

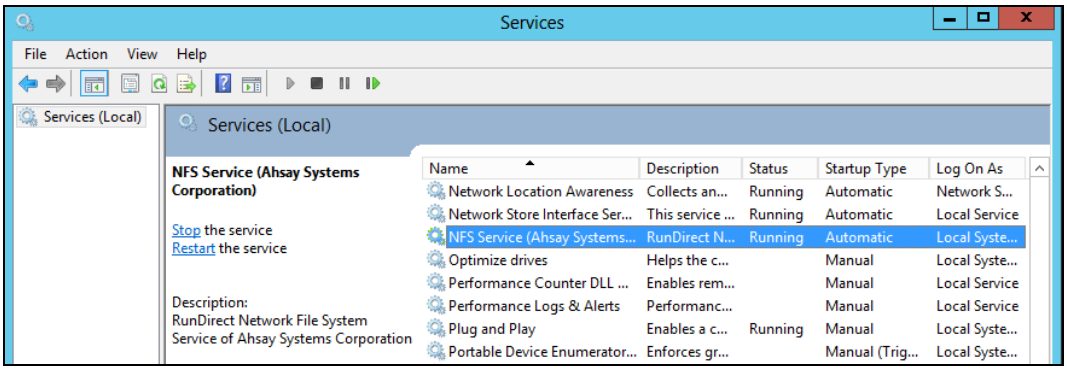


13. Click **Finish** to complete the installation.

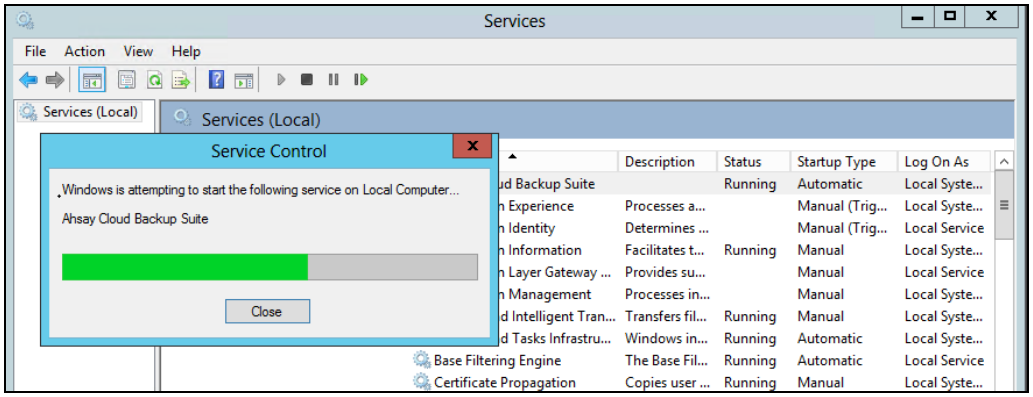


14. Run `services.msc` to open **Services** from Windows to confirm that the AhsayCBS service has started. In the following screen shot, the status of **Ahsay Cloud Backup Suite** is "**Running**" and the status of the **NFS Service (Ahsay Systems Corporation)** is "**Running**".





- When you need to reset the service of an item, select the item (e.g. **Ahsay Cloud Backup Suite**) and then press **Restart** in the left pane. Alternatively, after selecting the item, press **Stop** and then press **Start**.



15. Open Command Prompt and type the following command to check whether AhsayCBS is listening to pre-defined **http** and **https** ports. The default port values are 80 and 443 respectively.

```
netstat -an|more
```

16. You will get a list of all active connections. You can see clearly that AhsayCBS is listening to both ports 80 and 443.

```
C:\Users\Administrator>netstat -an|more
Active Connections

Proto      Local Address     Foreign Address     State
TCP        0.0.0.0:80        0.0.0.0             LISTENING
TCP        0.0.0.0:135       0.0.0.0             LISTENING
```

```
TCP        0.0.0.0:443        0.0.0.0          LISTENING
TCP        0.0.0.0:445        0.0.0.0          LISTENING
TCP        0.0.0.0:3389       0.0.0.0          LISTENING
```

For AhsayCBS servers hosting Run on Server (Agentless) Office 365 and Cloud File backups, ensure that AhsayCBS is listening to port 8081 (default) on local IP address 127.0.0.1.

```
C:\Users\Administrator>netstat -an|more
Active Connections

Proto      Local Address     Foreign Address     State
TCP        127.0.0.1:8081    0.0.0.0           LISTENING
TCP        127.0.0.1:49157   127.0.0.1:49158   ESTABLISHED
TCP        127.0.0.1:49158   127.0.0.1:49157   ESTABLISHED
TCP        127.0.0.1:49159   127.0.0.1:49160   ESTABLISHED
TCP        127.0.0.1:49160   127.0.0.1:49159   ESTABLISHED
```

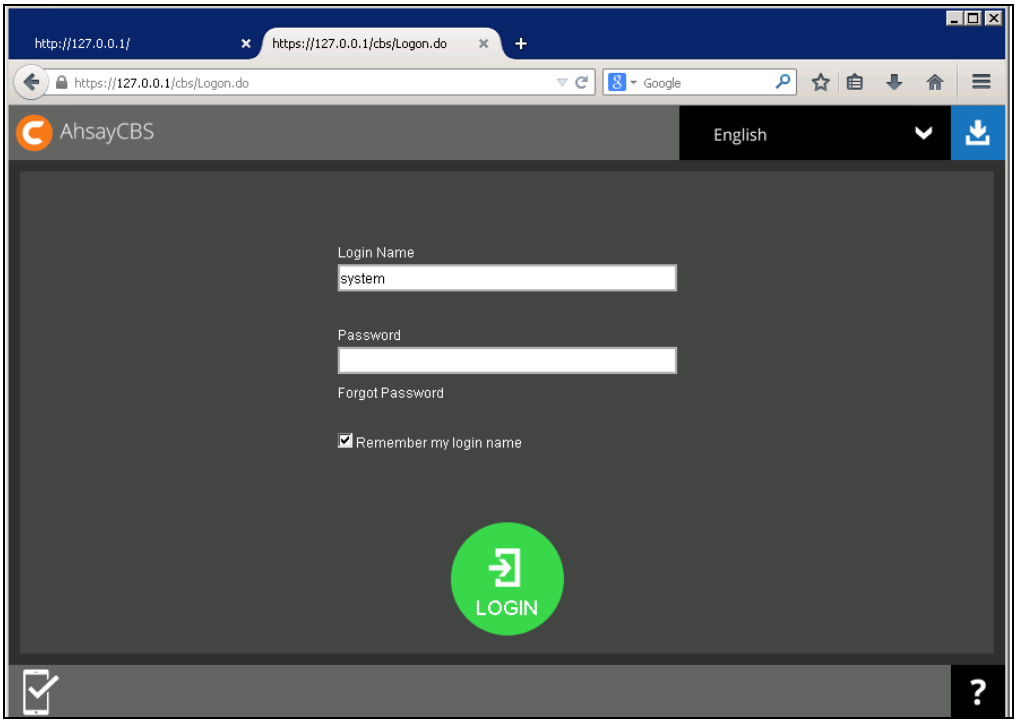
17. Use the `hostname` and `ping` commands to check whether the hostname is resolvable. The following shows that the hostname is resolvable.

```
C:\Program Files\AhsayCBS\nfs\bin>hostname
w7-pro

C:\Program Files\AhsayCBS\nfs\bin>ping w7-pro

Pinging w7-pro [fe80::2ccf:4d81:c65c:805d%14] with 32 bytes of data:
Reply from fe80::2ccf:4d81:c65c:805d%14: time<1ms
Reply from fe80::2ccf:4d81:c65c:805d%14: time<1ms
Reply from fe80::2ccf:4d81:c65c:805d%14: time<1ms
Reply from fe80::2ccf:4d81:c65c:805d%14: time<1ms

Ping statistics for fe80::2ccf:4d81:c65c:805d%14:
        Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Program Files\AhsayCBS\nfs\bin>
```

If the hostname is not resolvable, add the corresponding hostname information to the "hosts" file found at "C:\Windows\System32\drivers\etc".

Otherwise, the SMTP server setting on the AhsayCBS may not work properly.

18. After successful installation, you can access the login page by opening **localhost** (https://127.0.0.1/cbs/Logon.do) in a browser.

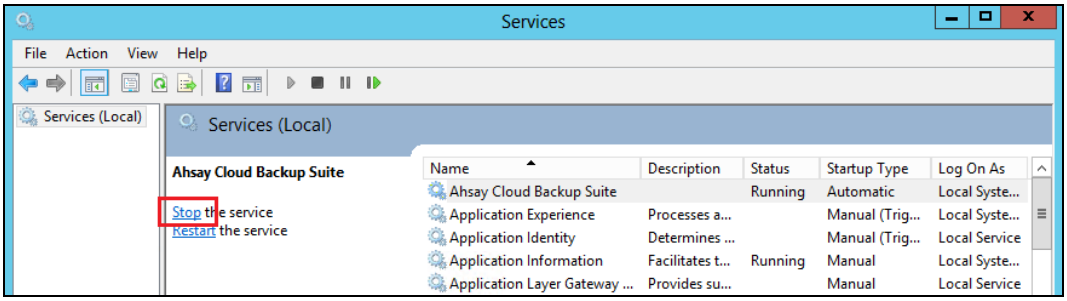


5.2 Upgrade on Windows

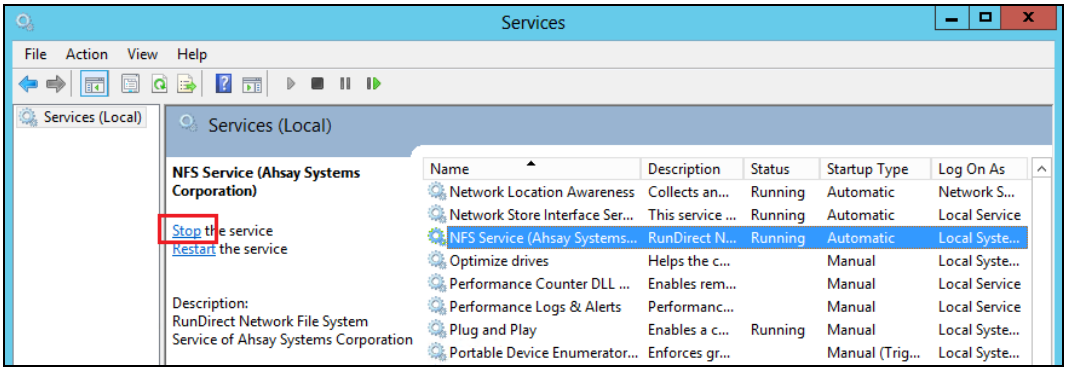
1. Log in as admin on your Windows machine

2. Download the latest version of AhsayCBS installation package. For instructions on how to download, please refer to the previous section.

3. Run `services.msc` to open **Services** from Windows to stop the AhsayCBS service.



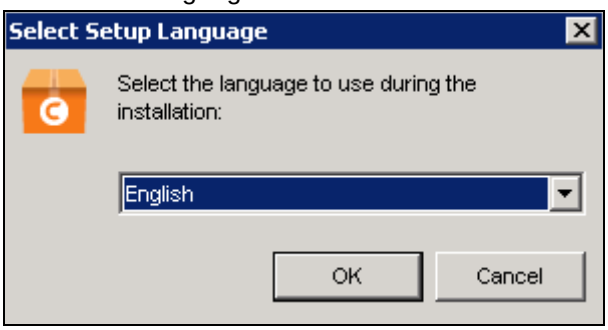
4. Also stop the NFS service.



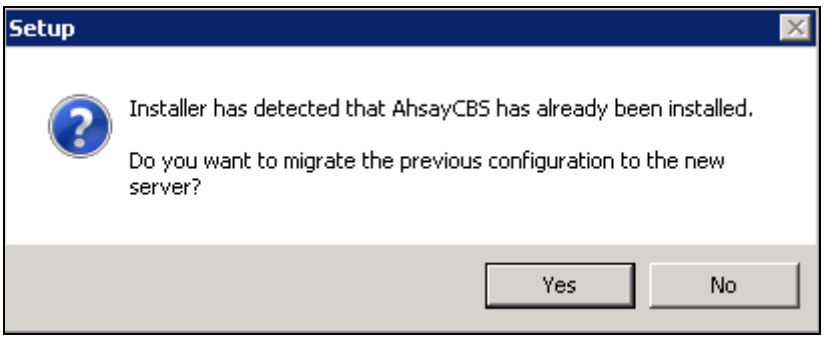
5. Remove the folder %AhsayCBS_HOME%\system\cbs\Installers, since this contains Branded installers which will be out of date upon AhsayCBS upgrade.

6. Double-click the downloaded cbs-win.exe to start the AhsayCBS setup wizard.

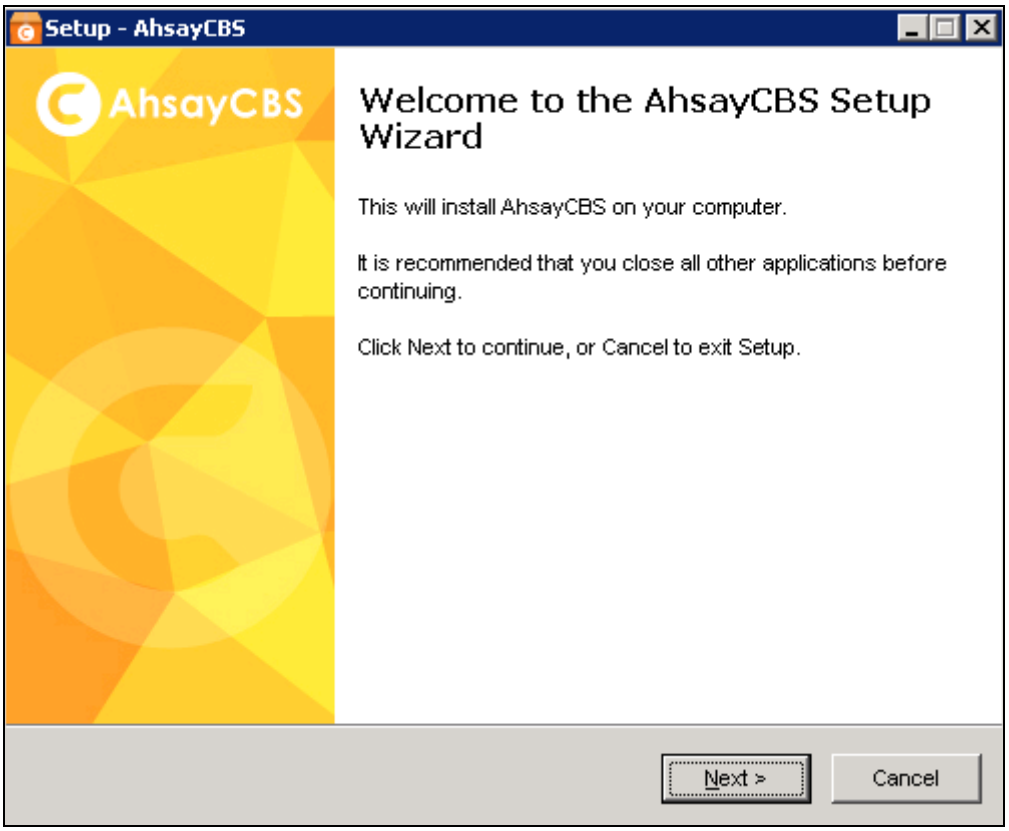
7. Choose the language then click **OK** to continue.



8. Click **Yes**, if you want to migrate your configuration to the new server. Otherwise, click **No**.

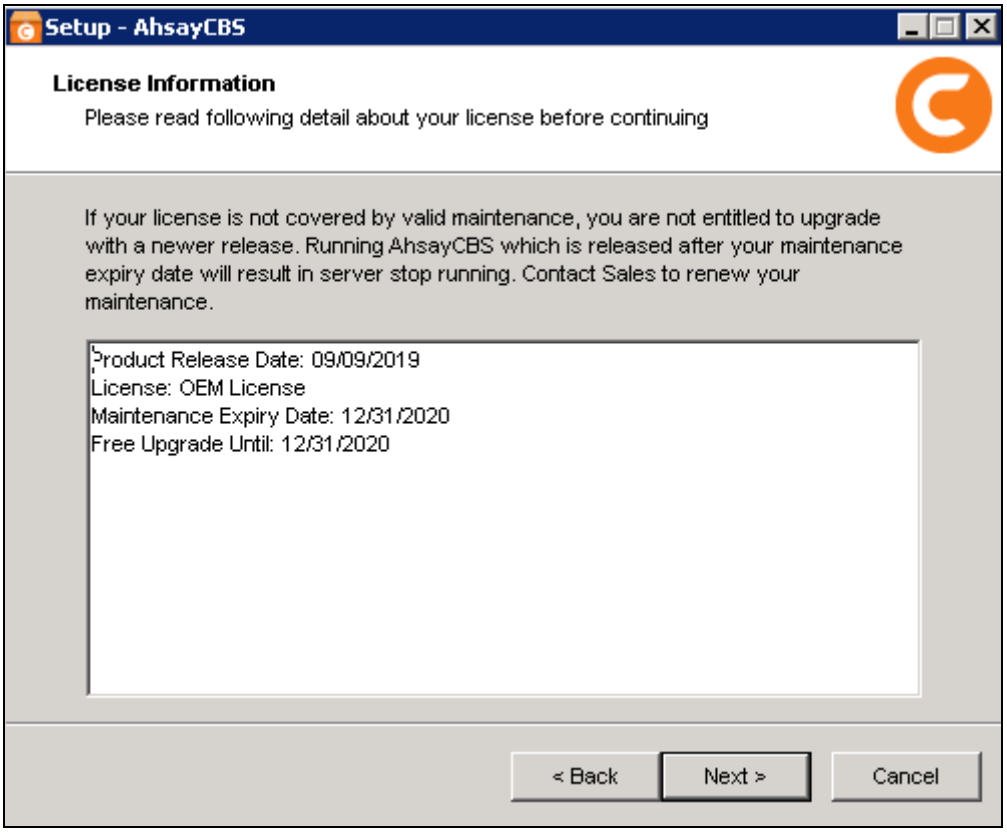


9. Click **Next** to proceed.

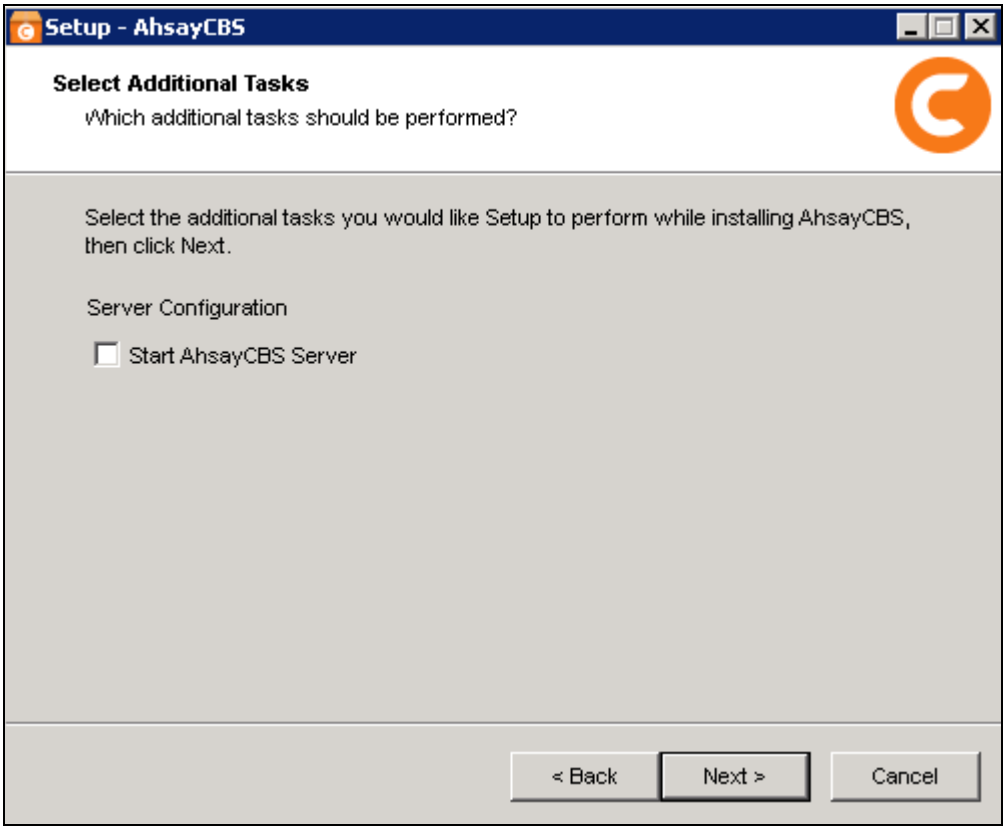


10. Select **I accept the agreement** after reading the license agreement. Then, click **Next** to continue.

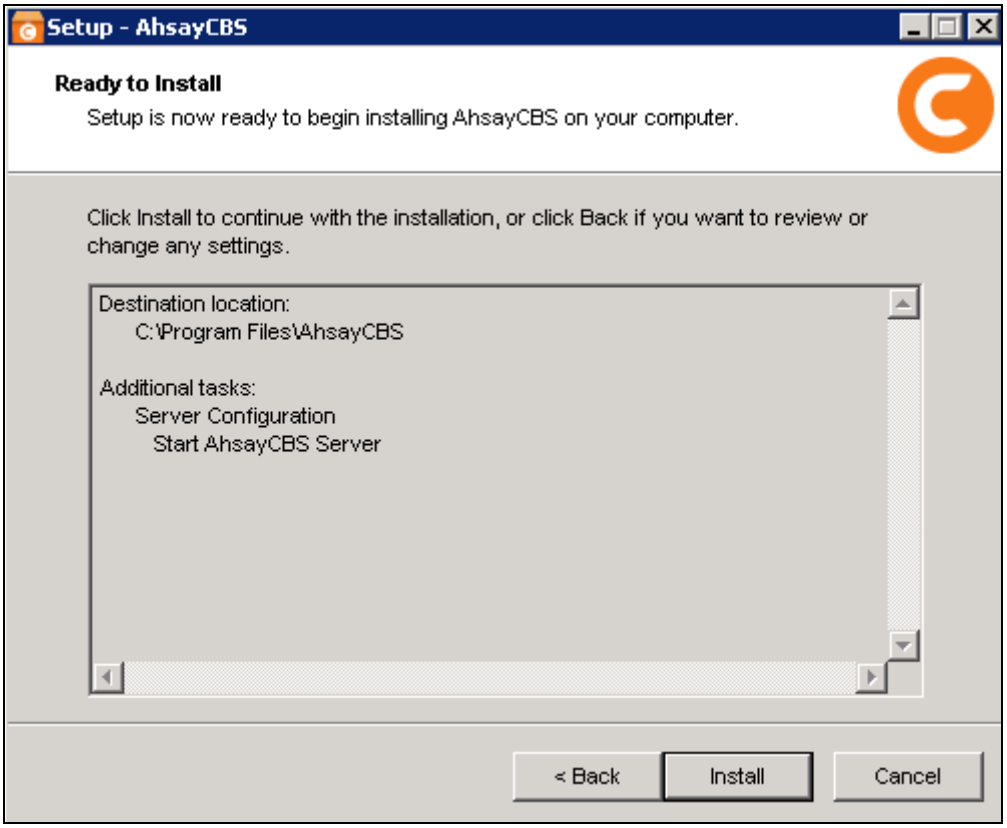
11. The system will check the validity of your maintenance license before proceeding with the installation. Click **Next** to continue.



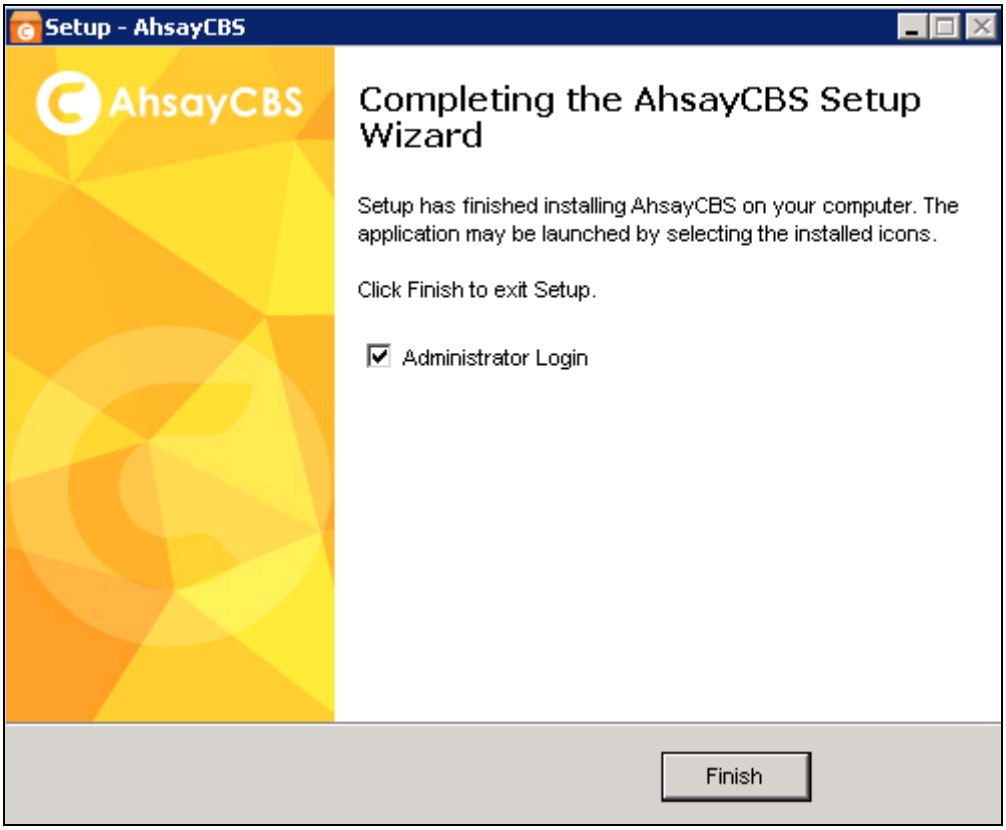
12. Deselect the **Start AhsayCBS Server** option. Click **Next** to continue.



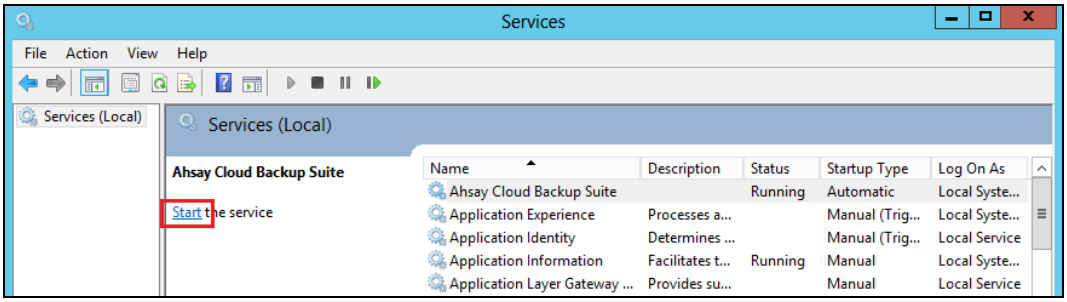
13. Click **Install** to start the upgrade.



14. Click **Finish** to complete the upgrade.

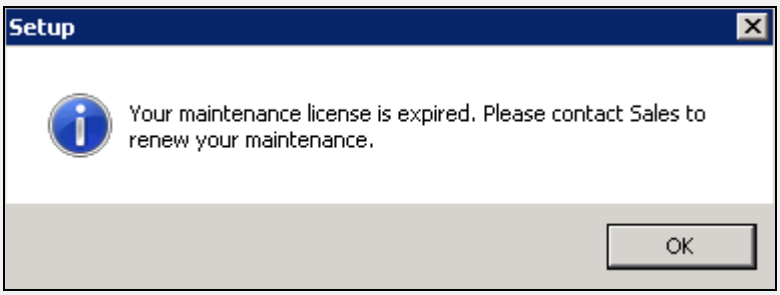


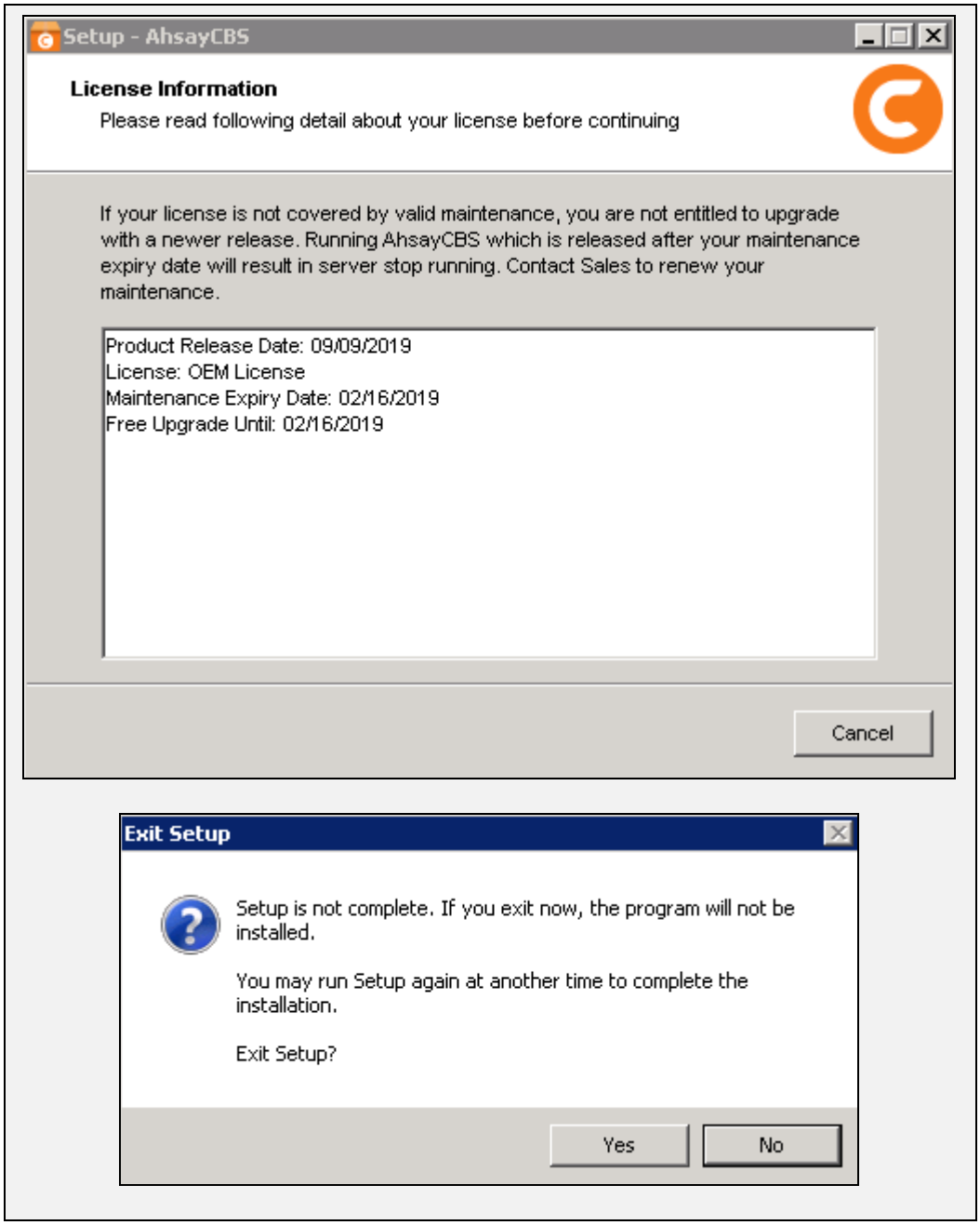
15. Run `services.msc` to open **Services** from Windows to start the AhsayCBS service.



NOTE

Before upgrading to the latest version of AhsayCBS make sure that your license key has a valid support maintenance otherwise installation will fail. You will receive the following messages if you have an expired maintenance license.

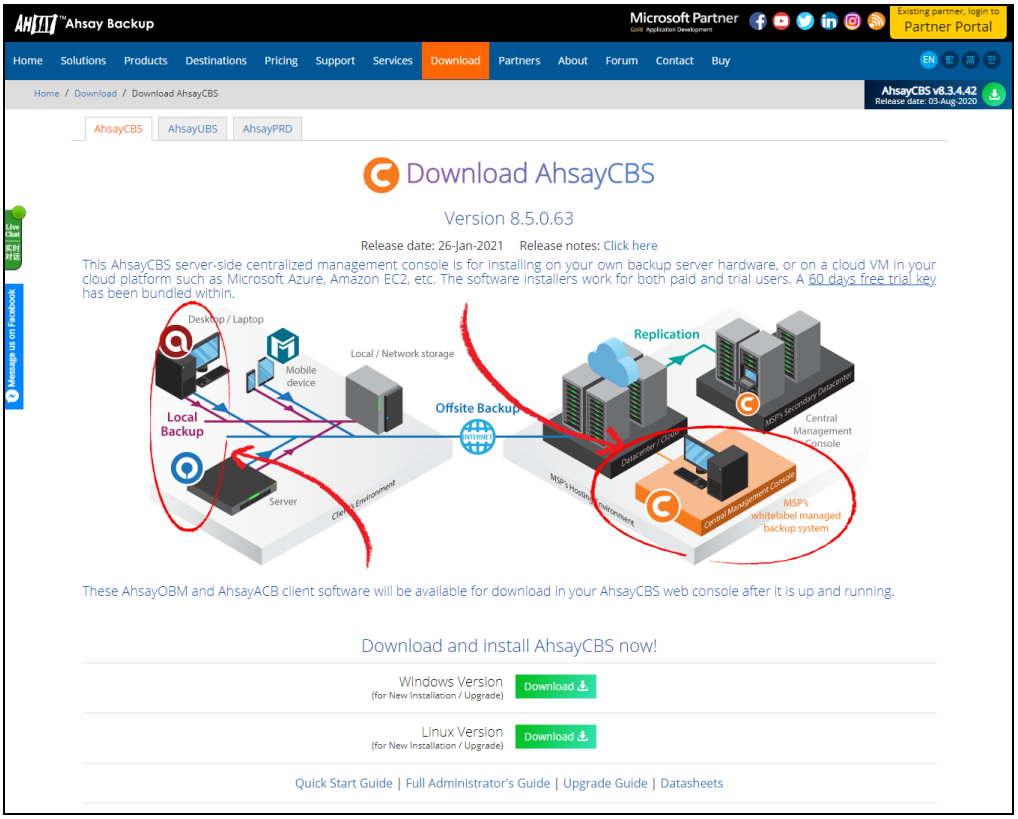



Setup - AhsayCBS
License Information
Please read following detail about your license before continuing
If your license is not covered by valid maintenance, you are not entitled to upgrade with a newer release. Running AhsayCBS which is released after your maintenance expiry date will result in server stop running. Contact Sales to renew your maintenance.
Product Release Date: 09/09/2019
License: OEM License
Maintenance Expiry Date: 02/16/2019
Free Upgrade Until: 02/16/2019
Cancel
Exit Setup
Setup is not complete. If you exit now, the program will not be installed.
You may run Setup again at another time to complete the installation.
Exit Setup?
Yes
No

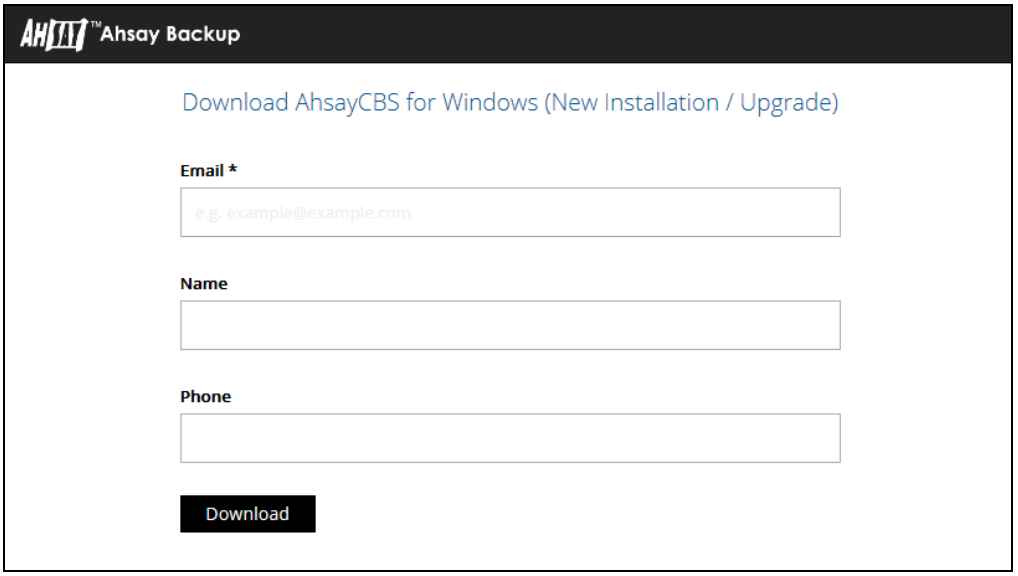
5.3 Installation on Windows Server Core

1. If the Windows Server Core machine does not have a web browser installed, find the download link of the AhsayCBS installation package **cbs-win.exe** from another machine with a web browser so it can be used in the Windows Server Core machine. Otherwise, use the web browser on the Windows Server Core machine to download the AhsayCBS installation package.

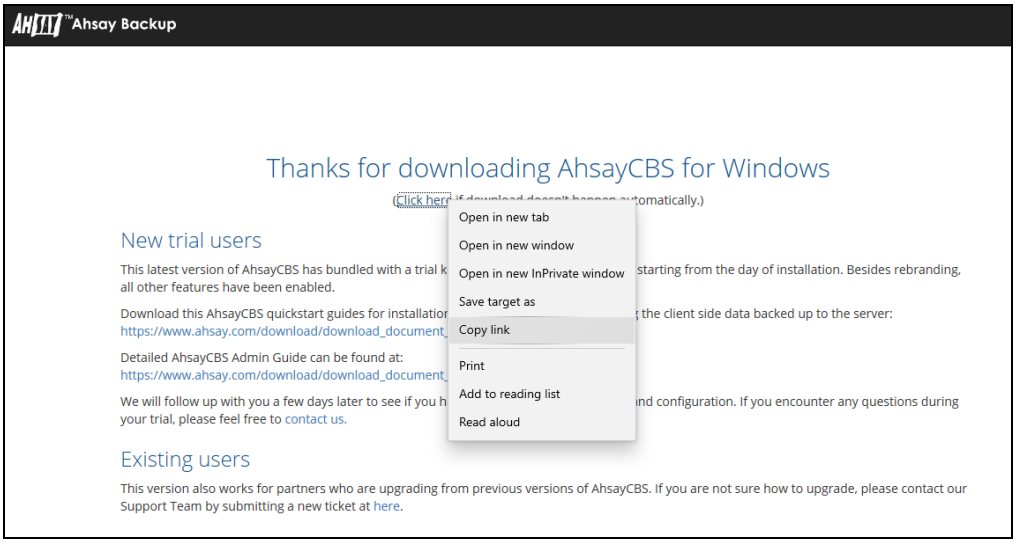
   In a web browser, find the download link of the AhsayCBS installation package **cbs-win.exe** from the Ahsay website by clicking on the Download button.



2. Enter your email, name and phone then click Download.

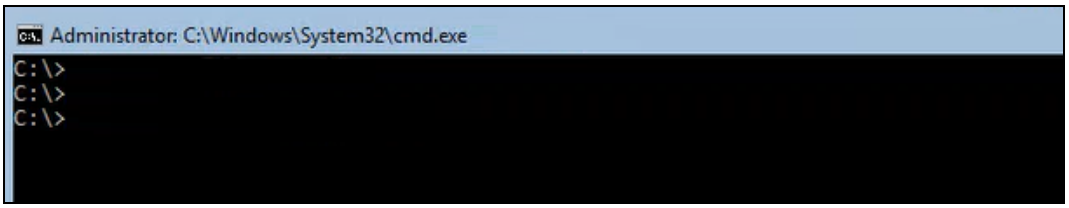


3. Right-click on the Click here link then select Copy link.



Example: `http://ahsay-dn.ahsay.com/v8/81150/cbs-win.exe`

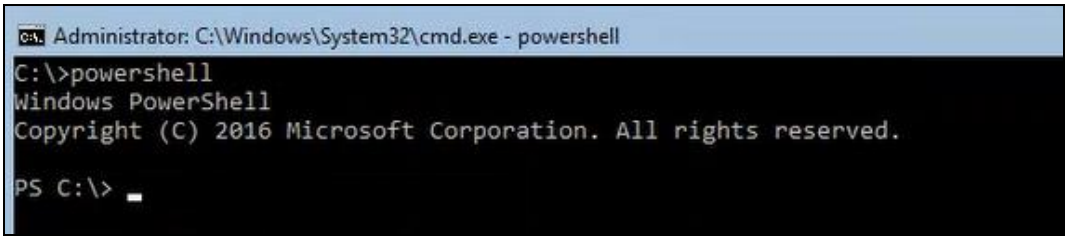
4. Log in to the Windows Server Core and start the command prompt.



5. Type in the following command to enter PowerShell.

```
C:\> powershell
```

After successfully entering PowerShell the prompt will change to PowerShell prompt:



6. Use the following command to download the online AhsayCBS installer to Windows Server Core `C:\temp` folder.

```
PS C:\> Invoke-WebRequest http://ahsay-
dn.ahsay.com/v8/81150/cbs-win.exe -Outfile 'c:\temp\cbs-win.exe'
```

Example: `Invoke-WebRequest http://ahsay-dn.ahsay.com/v8/81150/cbs-win.exe -Outfile 'c:\temp\cbs-win.exe'`

NOTE

The above command will download the AhsayCBS installer to the path of *"C:\temp"*.

You can change the download path of the file, which is *"C:\temp\"* to another path, but **DO NOT** change the filename of the AhsayCBS installer downloaded, i.e. *"cbs-win.exe"*.

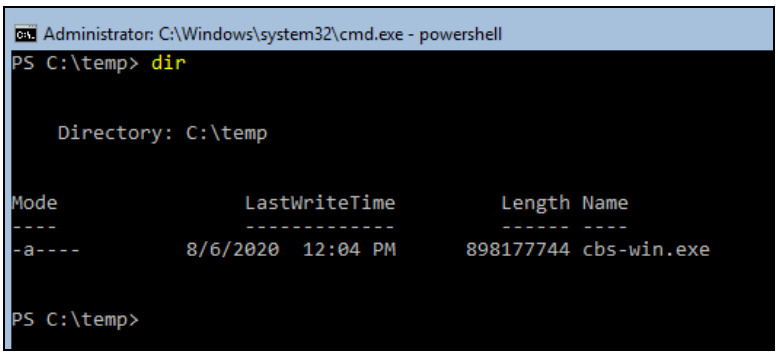
7. During downloading of AhsayCBS installer the following message will be displayed:

```
Writing web request
   Writing request stream... (Number of bytes written: 3223857)
```

After completing the download of the AhsayCBS installer the screen above would disappear. Press **Enter** button to continue.

8. Verify the AhsayCBS installer is downloaded using the following command.

```
PS C:\temp> dir
```



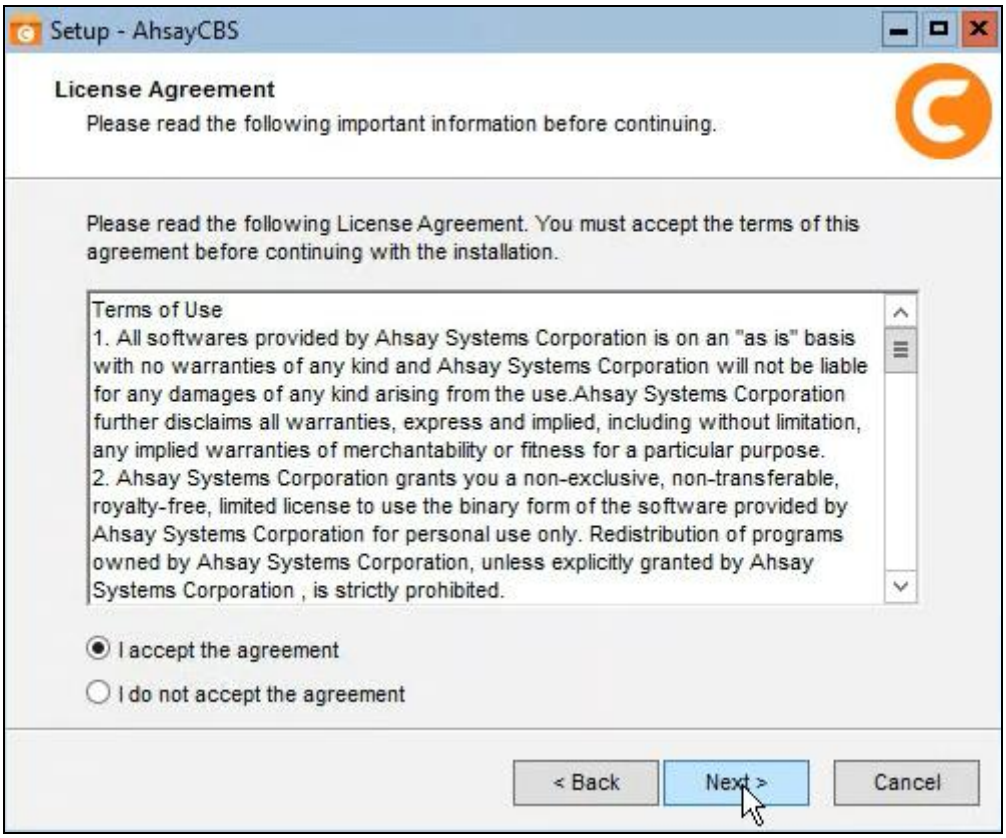
9. Use the following command to execute the installer:

```
PS C:\> C:\temp\cbs-win.exe
```

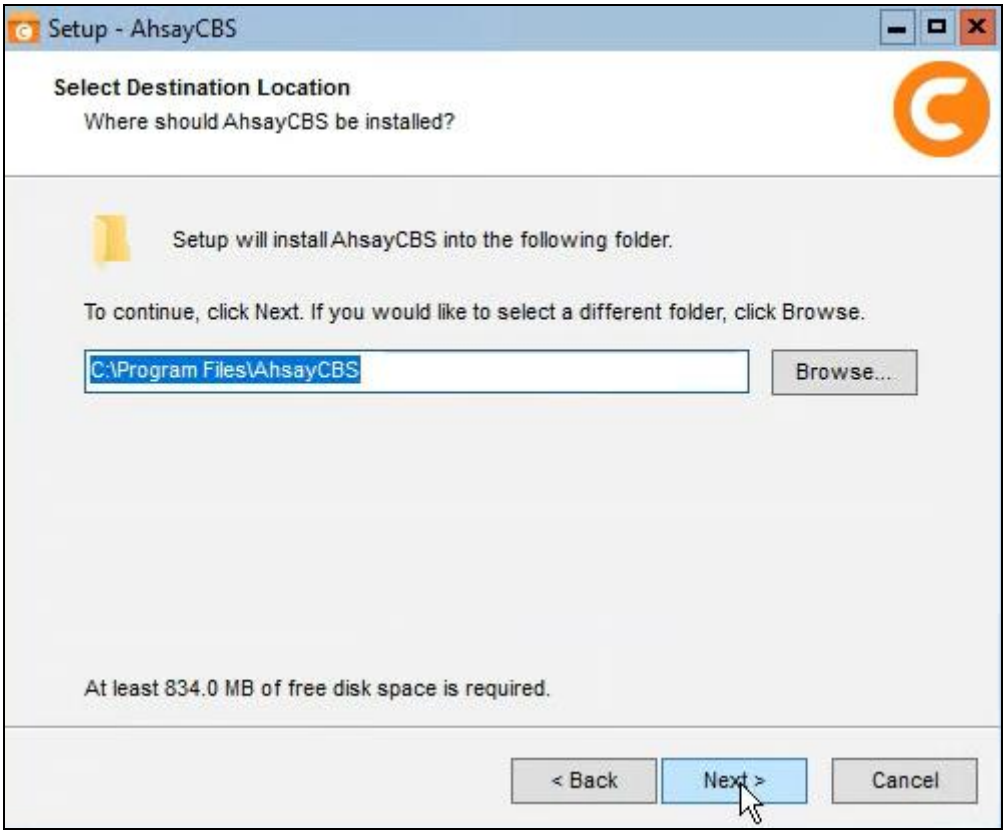
10. When the Select Setup Language window is shown, select the language then click **OK** to continue.

11. In the AhsayCBS Setup Wizard click **Next** to continue.

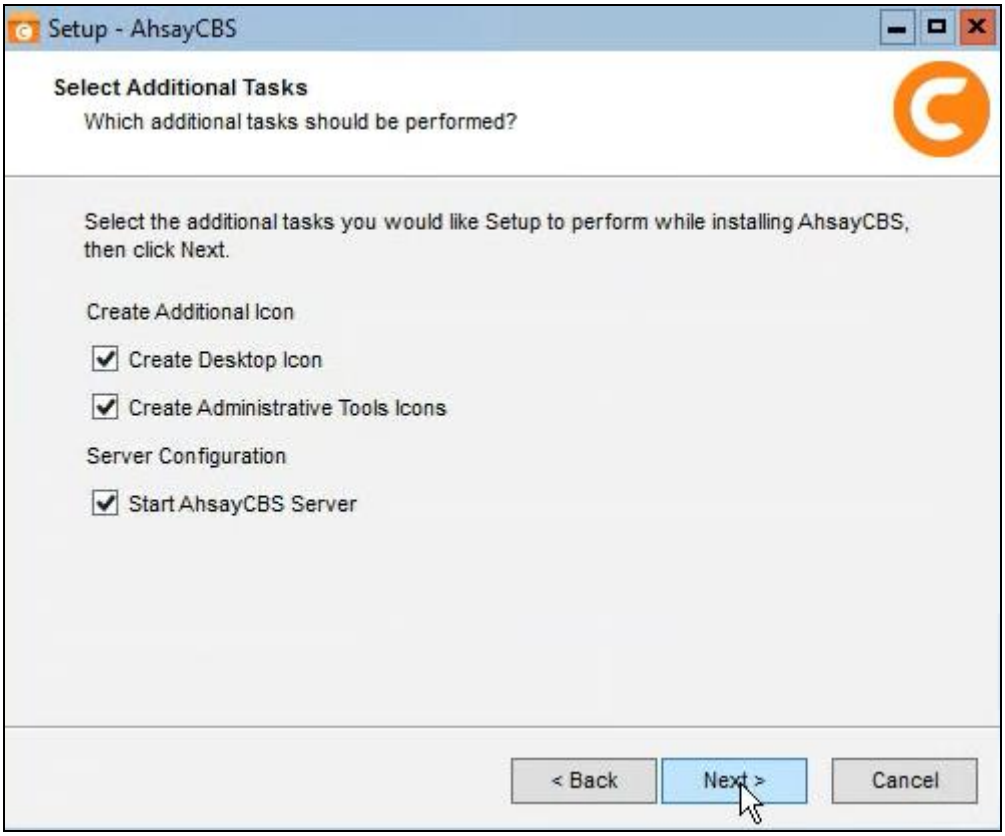
12. Select “I accept the agreement” after reading the license agreement. Then click Next to continue.



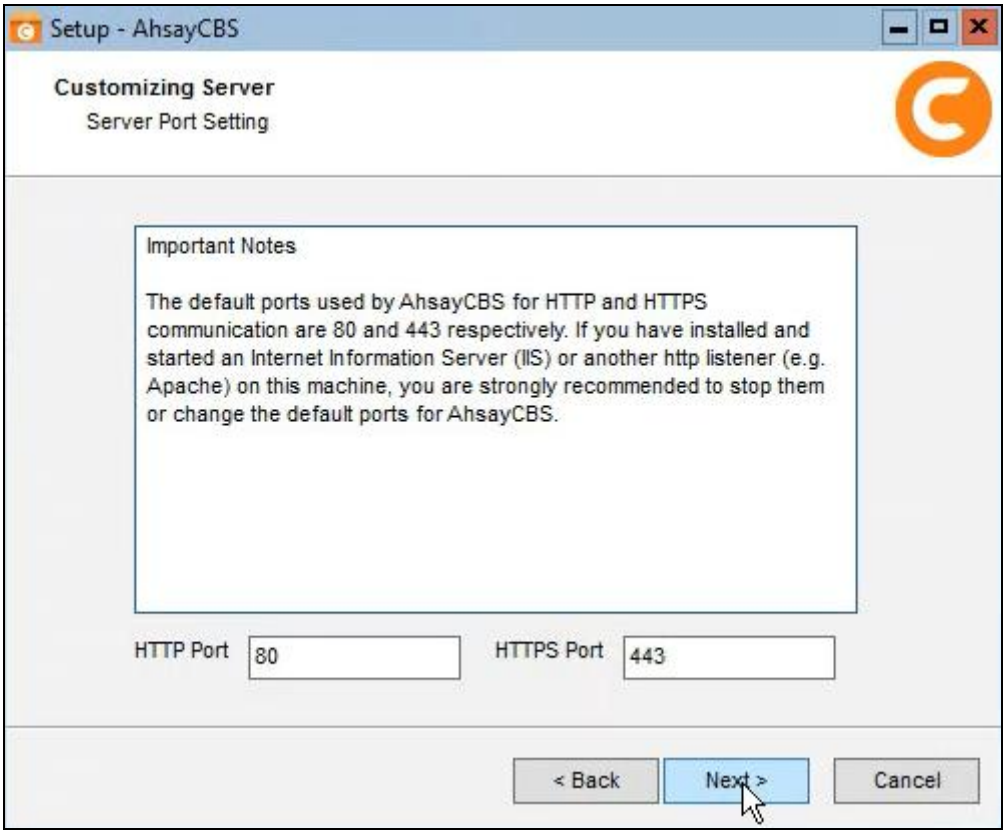
13. Choose the installation directory. Then click Next to continue.



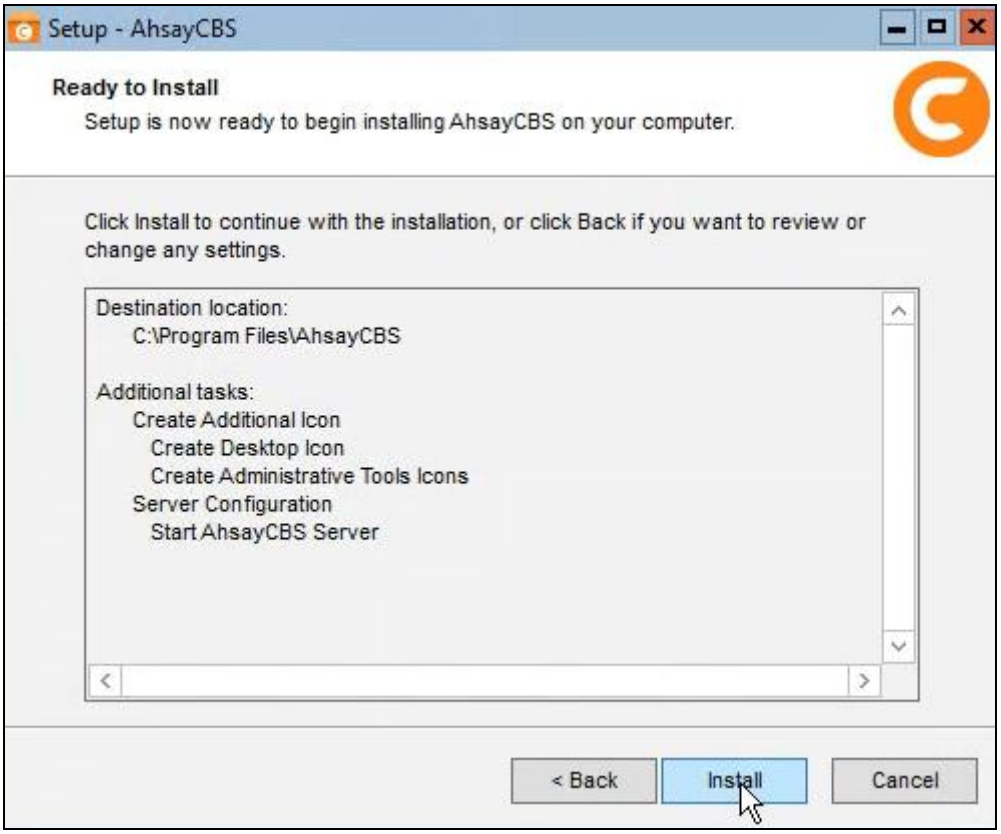
14. Select the additional tasks that will be performed. Then click Next to continue.



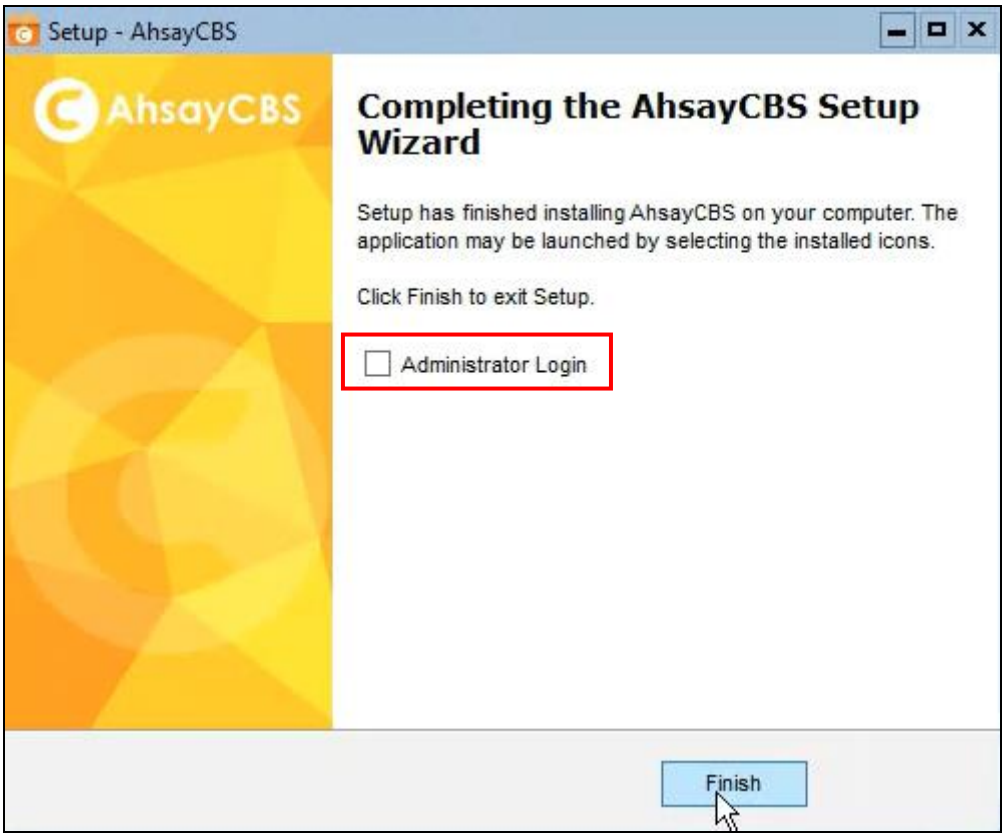
15. Enter the ports to be used. Then click Next to continue.



16. Click Install to start installation.

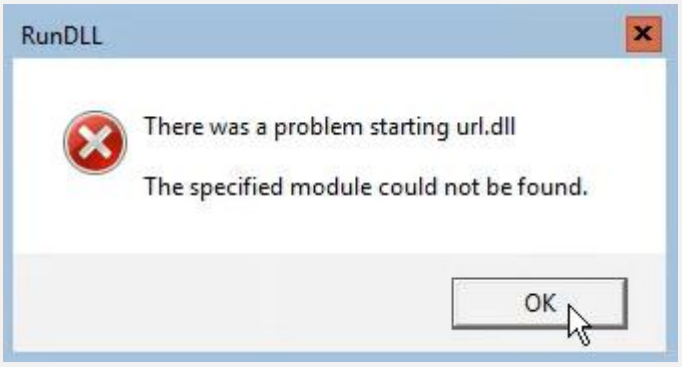


17. Untick the Administrator Login checkbox. Then click Finish to complete the installation.



NOTE

If you forgot to untick the "Administrator Login" option before clicking **Finish** you will get a rundll error. You can ignore this message since the missing url.dll is only used to launch the AhsayCBS web console in a browser.



18. After installation, check whether the AhsayCBS services are running. There are two methods to check the services status. In the following screen shot, the status of **Ahsay Cloud Backup Suite** is "**Running**" and the status of the **NFS Service (Ahsay Systems Corporation)** is "**Running**".

Method 1: Use PowerShell command prompt:

```
PS C:\> Get-Service -DisplayName 'Ahsay Cloud Backup Suite'

Status        Name               DisplayName
------        ----               -----------
Running       ahsaycbs           Ahsay Cloud Backup Suite
```

or

```
PS C:\> Get-Service -Name 'ahsaycbs'

Status        Name               DisplayName
------        ----               -----------
Running       ahsaycbs           Ahsay Cloud Backup Suite
```

and

```
PS C:\> Get-Service -DisplayName 'NFS Service (Ahsay Systems
Corporation)'

Status        Name               DisplayName
------        ----               -----------
Running       OBNfsServer        NFS Service (Ahsay Systems
Corp
```

or

```
PS C:\> Get-Service -Name 'OBNfsServer'

Status        Name               DisplayName
------        ----               -----------
Running       OBNfsServer        NFS Service (Ahsay Systems
Corp
```

If the services are not running, use the command to start the service.

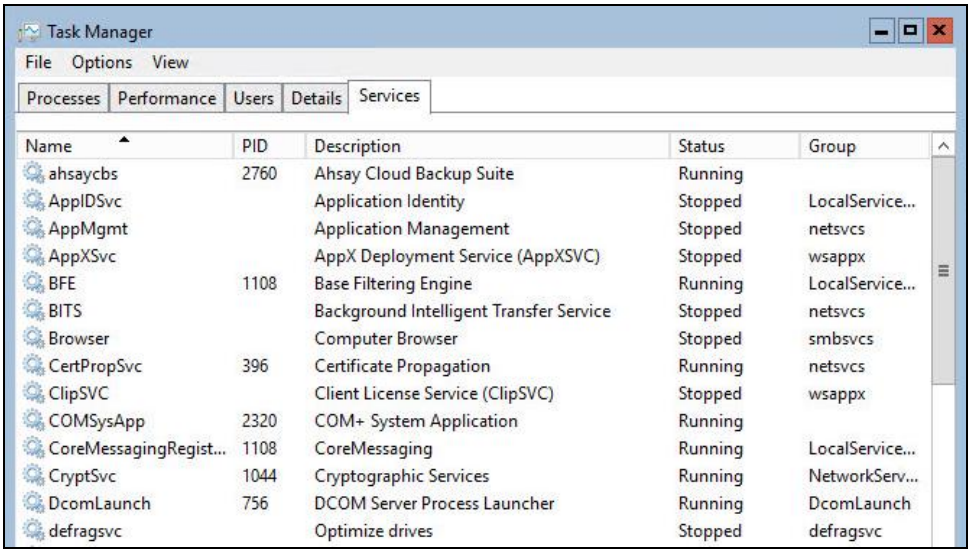
```
PS C:\> Start-Service -DisplayName 'Ahsay Cloud Backup
Suite'

PS C:\> Start-Service -DisplayName 'NFS Service (Ahsay
Systems Corporation)'
```

Method 2: Use GUI:

i. Use the following command to open task manager.

```
PS C:\> taskmgr
```

ii. **Task Manager** should appear. Navigate to **Services**.



Name	PID	Description	Status	Group
ahsaycbs	2760	Ahsay Cloud Backup Suite	Running	
AppIDSvc		Application Identity	Stopped	LocalService...
AppMgmt		Application Management	Stopped	netsvcs
AppXSvc		AppX Deployment Service (AppXSVC)	Stopped	wsappx
BFE	1108	Base Filtering Engine	Running	LocalService...
BITS		Background Intelligent Transfer Service	Stopped	netsvcs
Browser		Computer Browser	Stopped	smbsvcs
CertPropSvc	396	Certificate Propagation	Running	netsvcs
ClipSVC		Client License Service (ClipSVC)	Stopped	wsappx
COMSysApp	2320	COM+ System Application	Running	
CoreMessagingRegist...	1108	CoreMessaging	Running	LocalService...
CryptSvc	1044	Cryptographic Services	Running	NetworkServ...
DcomLaunch	756	DCOM Server Process Launcher	Running	DcomLaunch
defragsvc		Optimize drives	Stopped	defragsvc

iii. Ensure the following services exist and running.

Name	PID	Description	Status
ahsaycbs	2760	Ahsay Cloud Backup Suite	Running

Name	PID	Description	Status
OBNfsServer	1776	NFS Service (Ahsay Systems Corporation)	Running

If the services are not running, right click to start.

19. Also check if AhsayCBS is listening to the pre-defined http and https ports, which are 80 and 443. The following shows that AhsayCBS is listening to both ports.

```
PS C:\> netstat -an|more

Active Connections

Proto      Local Address          Foreign Address        State
TCP        0.0.0.0:80             0.0.0.0:0              LISTENING
TCP        0.0.0.0:135            0.0.0.0:0              LISTENING
TCP        0.0.0.0:443            0.0.0.0:0              LISTENING
TCP        0.0.0.0:445            0.0.0.0:0              LISTENING
TCP        0.0.0.0:2179           0.0.0.0:0              LISTENING
```

For AhsayCBS servers hosting Run on Server (Agentless) Office 365 and Cloud File backups, ensure that AhsayCBS is listening to port 8081 (default) on local IP address 127.0.0.1.

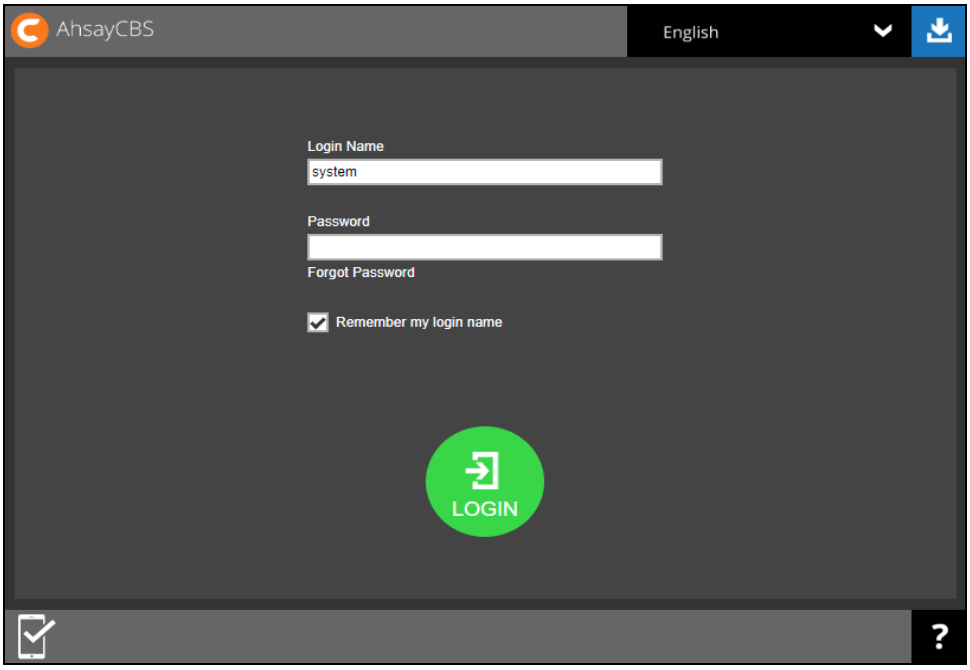
```
PS C:\> netstat -an|more

Active Connections

Proto      Local Address          Foreign Address        State
```

```
TCP        127.0.0.1:8081         0.0.0.0:0              LISTENING
TCP        127.0.0.1:49157        127.0.0.1:49158        ESTABLISHED
TCP        127.0.0.1:49158        127.0.0.1:49157        ESTABLISHED
TCP        127.0.0.1:49159        127.0.0.1:49160        ESTABLISHED
TCP        127.0.0.1:49160        127.0.0.1:49159        ESTABLISHED
```

20. Check if the hostname is resolvable. The following shows that the hostname is resolvable.

```
PS C:\> hostname
w2k16-hyperv

PS C:\> ping w2k16-hyperv
Pinging w2k16-hyperv [fe80:78f8:2b59:3931:38ce%7] with 32
bytes of data:
Reply from fe80:78f8:2b59:3931:38ce%7: time<1ms
Reply from fe80:78f8:2b59:3931:38ce%7: time<1ms
Reply from fe80:78f8:2b59:3931:38ce%7: time<1ms
Reply from fe80:78f8:2b59:3931:38ce%7: time<1ms

Ping statistics for Reply from fe80:78f8:2b59:3931:38ce%7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

21. After successful installation you can access the login page by opening https://<your-backup-server> in a browser.



5.4 Installation on Linux

Pre-requisite requirements:

Make sure the GNU C Library is installed on Linux to support AhsayCBS NFS service. The version should at least be 2.14.

- To check for the GNU C Library version:
  - Login to the AhsayCBS server as root
  - Check the version by using the ldd --version command

```
# ldd --version
ldd (GNU libc) 2.17
Copyright (C) 2012 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.
There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.
Written by Roland McGrath and Ulrich Drepper.
```

If the version is lower than 2.14 see instruction below on how to install the GNU C Library.

- Install GNU C Library:
  - Login to the AhsayCBS server as root
  - make installation

Example: on CentOS/Redhat

```
yum group install 'Development Tools'
```

Example: on Ubuntu

```
apt-get install build-essential
```

- Ahsay CBS installation path: /usr/local/cbs

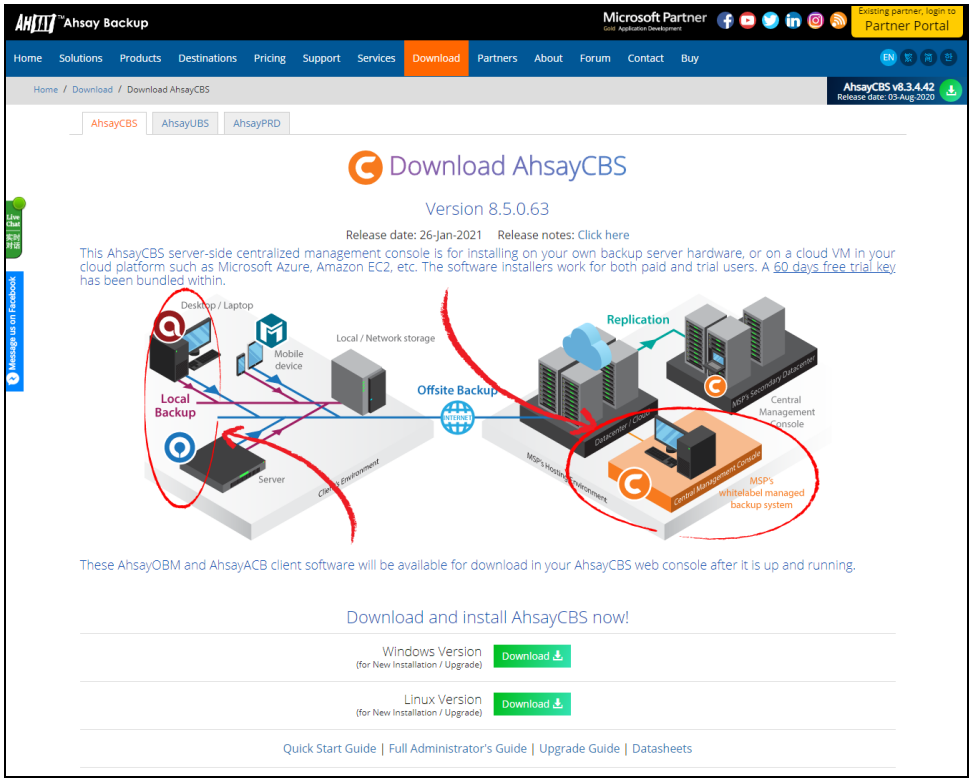
1. Log in as root on your Linux machine.

```
login as: root
root@10.21.4.28's password:
Last login: Mon Jan 14 14:13:21 2019 from mis-hq-
249.ahsayhqt.local
[root@cos6x ~]#
```

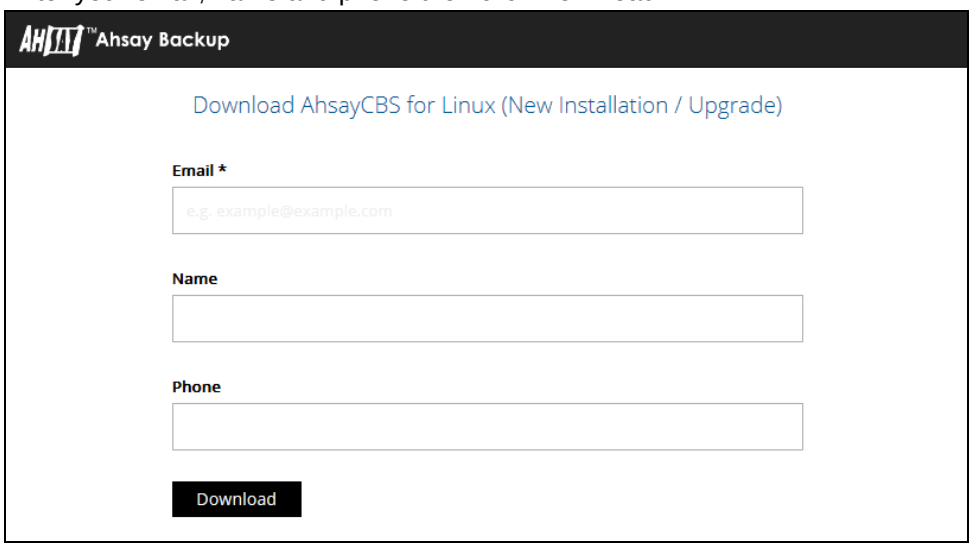
2. Make a directory in `/usr/local/cbs`

```
# mkdir /usr/local/cbs
```

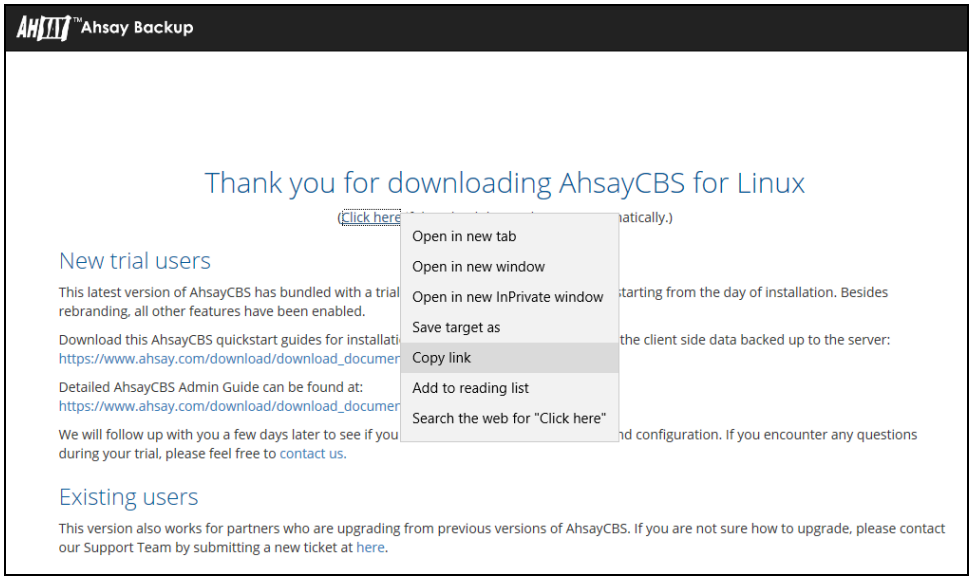
3. In a browser, download the AhsayCBS installation package cbs-nix.tar.gz from the Ahsay website by clicking on the Download button.



4. Enter your email, name and phone then click Download.



5. Right-click on the **Click here** link then select **Copy link**.



6. Go to the cbs directory you created then download the installation package cbs-nix.tar.gz with the `wget` command, then run `tar` as follows:

```
# cd /usr/local/cbs
# wget http://ahsay-dn.ahsay.com/v8/83442/cbs-nix.tar.gz
     --2020-08-11 15:22:33--  http://ahsay-
     dn.ahsay.com/v8/83442/cbs-nix.tar.gz
     Resolving ahsay-dn.ahsay.com (ahsay-dn.ahsay.com)...
     54.192.16.115, 54.192.16.107, 54.192.16.60, ...
     Connecting to ahsay-dn.ahsay.com (ahsay-
     dn.ahsay.com)|54.192.16.115|:443... connected.
     HTTP request sent, awaiting response... 200 OK
     Length: 1041735214 (886993M) [application/x-gzip]
     Saving to: 'cbs-nix.tar.gz'

     100%[======================================>]
     928,881,759 7.41MB/s   in 2m 12s

2020-08-11 15:23:35 (11.9 MB/s) - 'cbs-nix.tar.gz' saved
[1041735214/1041735214]
# tar xvfz cbs-nix.tar.gz
```

7. After the tar process, install and start AhsayCBS using the `install.sh` command:

```
# /usr/local/cbs/bin/install.sh
```

8. When AhsayCBS installation is started, the following output will appear:

```
# sh install.sh
Log Time: Tuesday, 11 August, 2020 03:31:11 PM PST

Verifying current user privilege ...
Current user has enough privilege to "install".

Start configuration on Generic Linux Platform (Linux)
Using CBS_HOME /usr/local/cbs
Current Directory: "/usr/local/cbs".
```

```
Created symlink "java" to "java-linux-x64".
Minimum supported JVM version: 1.8
Current JVM version is supported for installation.
/usr/local/cbs
Get Startup path for NIX type OS
Installing [ Ahsay Cloud Backup Suite ]
[ Ahsay Cloud Backup Suite ] Service Script created at
/usr/local/cbs/bin/cbs
Please provide the path to the service script!
Install Service for NIX type OS
Using init script path /etc/init.d
Using run level script path /etc
Copying script cbs to /etc/init.d
Copying systemd unit file cbs.service to
/etc/systemd/system
Creating symbolic link to run levels
You may start this service by:

sh "/etc/init.d/cbs" start &

[ Ahsay Cloud Backup Suite ] setup completed!
Migrate from previous version
/usr/local/cbs
Get Startup path for NIX type OS
RDR_HOME
OBS_HOME
OBSR_HOME
RPS_HOME
Run MigrateV6 script
Startup [ Ahsay Cloud Backup Suite ]
Run MigrateV7 script
------------------------------------------------------------
-------------
You may set SYSTEM_DEBUG=0 to disable the debug message
------------------------------------------------------------
-------------
Current User Name   : root
Using SYSTEM_TYPE   : linux
Using SYSTEM_ARCH   : x86_64
Using PHYSICAL_MEM  : 3936 (MB)
------------------------------------------------------------
-------------
Using CBS_HOME      : /usr/local/cbs
Using JAVA_HOME     : /usr/local/cbs/java
Using CATALINA_HOME : /usr/local/cbs/tomcat
Using JAVA_OPTS     :
-Djava.library.path=/usr/local/cbs/lib/LinX64 -
DCATALINA_PID=/var/run/obsr.pid -Xrs -Xms512m -Xmx2048m -
Xss384k -XX:MetaspaceSize=96m -XX:MaxMetaspaceSize=256m -
XX:MaxDirectMemorySize=512m -XX:NewRatio=3 -
XX:SurvivorRatio=32 -XX:MinHeapFreeRatio=20 -
XX:MaxHeapFreeRatio=80 -XX:+PrintGCDetails -
XX:+PrintGCDateStamps -XX:+UseConcMarkSweepGC -
XX:+UseCMSInitiatingOccupancyOnly  -
XX:CMSInitiatingOccupancyFraction=85 -
XX:+ScavengeBeforeFullGC  -XX:+CMSScavengeBeforeRemark -
Dsun.net.inetaddr.ttl=3600 -Dnetworkaddress.cache.ttl=3600
-Dsun.net.inetaddr.negative.ttl=300 -
Dnetworkaddress.cache.negative.ttl=300 -
```

```
Dsun.nio.PageAlignDirectMemory=true -
Djava.net.preferIPv4Stack=true -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogM
anager -
Djava.util.logging.config.file=conf/logging.properties -
Dtc.work.path=work -Dtc.log.path=logs -
Djavax.servlet.context.tempdir=work -
Djdk.nio.maxCachedBufferSize=262144 -Dfile.encoding=UTF-8
-Dsun.jnu.encoding=UTF-8
Using CATALINA_OPTS :
Using CATALINA_PID  : /var/run/obsr.pid
------------------------------------------------------------
-------------
Starting AhsayCBS service
Started [ Ahsay Cloud Backup Suite ]
Installing [ NFS Service (Ahsay Systems Corporation) ]
[ NFS Service (Ahsay Systems Corporation) ] Service Script
created at /usr/local/cbs/nfs/bin/cbsnfs
Please provide the path to the service script!
Install Service for NIX type OS
Using init script path /etc/init.d
Using run level script path /etc
Copying script cbsnfs to /etc/init.d
Copying systemd unit file cbsnfs.service to
/etc/systemd/system
Creating symbolic link to run levels
You may start this service by:

sh "/etc/init.d/cbsnfs" start &

[ NFS Service (Ahsay Systems Corporation) ] setup
completed!
Startup [ NFS Service (Ahsay Systems Corporation) ]
Starting NFS Service (Ahsay Systems Corporation)
Started [ NFS Service (Ahsay Systems Corporation) ]
```

NOTE

On some Linux systems, the installation may appear to pause after displaying Starting AhsayCBS service. If this occurs, press the space bar to complete the installation.

9. Check if Java is running on AhsayCBS with the `ps -ef|grep java` command. The following output shows that Java is running on AhsayCBS.

```
# ps -ef|grep java
root       64573       1   0 Aug10 ?        00:05:14
/usr/local/obm/jvm/bin/bschJW -Xms128m -Xmx768m -
Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=.
-cp .:./cbs.jar cbs /usr/local/obm
root       72956       1 31 16:40 pts/0    00:01:37
/usr/local/cbs/java/bin/java -
Djava.util.logging.config.file=/usr/local/cbs/conf/loggin
g.properties -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLog
Manager -Djava.library.path=/usr/local/cbs/lib/LinX64 -
DCATALINA_PID=/var/run/obsr.pid -Xrs -Xms512m -Xmx2048m -
Xss384k -XX:MetaspaceSize=96m -XX:MaxMetaspaceSize=256m -
```

```
XX:MaxDirectMemorySize=512m -XX:NewRatio=3 -
XX:SurvivorRatio=32 -XX:MinHeapFreeRatio=20 -
XX:MaxHeapFreeRatio=80 -XX:+PrintGCDetails -
XX:+PrintGCDateStamps -XX:+UseConcMarkSweepGC -
XX:+UseCMSInitiatingOccupancyOnly -
XX:CMSInitiatingOccupancyFraction=85 -
XX:+ScavengeBeforeFullGC -XX:+CMSScavengeBeforeRemark -
Dsun.net.inetaddr.ttl=3600 -
Dnetworkaddress.cache.ttl=3600 -
Dsun.net.inetaddr.negative.ttl=300 -
Dnetworkaddress.cache.negative.ttl=300 -
Dsun.nio.PageAlignDirectMemory=true -
Djava.net.preferIPv4Stack=true -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLog
Manager -
Djava.util.logging.config.file=conf/logging.properties -
Dtc.work.path=work -Dtc.log.path=logs -
Djavax.servlet.context.tempdir=work -
Djdk.nio.maxCachedBufferSize=262144 -Dfile.encoding=UTF-8
-Dsun.jnu.encoding=UTF-8 -
Djdk.tls.ephemeralDHKeySize=2048 -
Djava.protocol.handler.pkgs=org.apache.catalina.webresour
ces -
Dorg.apache.catalina.security.SecurityListener.UMASK=0027
-Dignore.endorsed.dirs= -classpath
/usr/local/cbs/tomcat/bin/bootstrap.jar:/usr/local/cbs/to
mcat/bin/tomcat-juli.jar -Dcatalina.base=/usr/local/cbs -
Dcatalina.home=/usr/local/cbs/tomcat -
Djava.io.tmpdir=/usr/local/cbs/temp
org.apache.catalina.startup.Bootstrap start

root       73098   72431  0 16:45 pts/0    00:00:00 grep
--color=auto java
```

10. Check if NFS Service is running on AhsayCBS with the `ps -ef|grep nfs` command. The following output shows that NFS Service is running on AhsayCBS.

```
# ps -ef|grep nfs
root       73019       1  0 16:40 pts/0    00:00:00
/usr/local/cbs/nfs/bin/NfsLinX64 -logfile
/usr/local/cbs/nfs/log/debug.log -pidfile /var/run/cbsnfs.pid
root       73115   72431  0 16:48 pts/0    00:00:00 grep --
color=auto nfs
```

11. Check if the process for rotating logs is running on AhsayCBS with the `ps -ef|grep rotatelogs` command. The following output shows that the rotate logs process is running on AhsayCBS.

```
# ps -ef|grep rotatelogs
root       72955       1  0 16:40 pts/0    00:00:00
/usr/local/cbs/bin/LinX64/rotatelogs -f
/usr/local/cbs/logs/console_%Y-%m-%d.log 86400
root       73118   72431  0 16:49 pts/0    00:00:00 grep --
color=auto rotatelogs
```

12. Check if AhsayCBS is listening to the pre-defined **http** and **https** ports, i.e. ports **80** and **443** with the `netstat -pan|more` command. The following output shows that AhsayCBS is listening to both ports.

```
# netstat -pan|more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign
Address             State       PID/Program name
tcp        0      0 0.0.0.0:111                 0.0.0.0:*
LISTEN      1478/rpcbind
tcp        0      0 0.0.0.0:80                  0.0.0.0:*
LISTEN      3736/java
tcp        0      0 0.0.0.0:22                  0.0.0.0:*
LISTEN      1746/sshd
tcp        0      0 127.0.0.1:60024             0.0.0.0:*
LISTEN      3736/java
tcp        0      0 127.0.0.1:25                0.0.0.0:*
LISTEN      1822/master
tcp        0      0 0.0.0.0:443                 0.0.0.0:*
LISTEN      3736/java
tcp        0      0 0.0.0.0:54178               0.0.0.0:*
LISTEN      1569/rpc.statd
tcp       86      0 10.16.4.28:33250
203.186.85.237:443          CLOSE_WAIT  3736/java
tcp       86      0 10.16.4.28:60738
203.186.85.237:443          CLOSE_WAIT  3736/java
tcp       52      0 10.16.4.28:22
192.168.7.104:1318          ESTABLISHED 14322/0
tcp       86      0 10.16.4.28:33251
203.186.85.237:443          CLOSE_WAIT  3736/java
tcp        0      0 :::111                      :::*
LISTEN      1478/rpcbind
tcp        0      0 :::22                       :::*
LISTEN      1746/sshd
tcp        0      0 :::45846                    :::*
LISTEN      1569/rpc.statd
udp        0      0 0.0.0.0:5353                0.0.0.0:*
1527/avahi-daemon:
udp        0      0 0.0.0.0:111                 0.0.0.0:*
1478/rpcbind
udp        0      0 0.0.0.0:897                 0.0.0.0:*
1569/rpc.statd
udp        0      0 0.0.0.0:44431               0.0.0.0:*
1527/avahi-daemon:
udp        0      0 0.0.0.0:10000               0.0.0.0:*
3736/java
udp        0      0 0.0.0.0:805                 0.0.0.0:*
1478/rpcbind
udp        0      0 0.0.0.0:43587               0.0.0.0:*
1569/rpc.statd
udp        0      0 :::111                      :::*
1478/rpcbind
udp        0      0 :::805                      :::*
1478/rpcbind
udp        0      0 :::42700                    :::*
1569/rpc.statd
```

For AhsayCBS servers hosting Run on Server (Agentless) Office 365 and Cloud File backups, ensure that AhsayCBS is listening to port 8081 (default) on local IP address 127.0.0.1.

```
# netstat -pan|more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign
Address         State
PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*
LISTEN
6506/java
tcp        0      0 127.0.0.1:8081          0.0.0.0:*
LISTEN
6506/java
tcp        0      0 0.0.0.0:22              0.0.0.0:*
LISTEN
4341/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*
LISTEN
4571/master
tcp        0      0 0.0.0.0:443             0.0.0.0:*
LISTEN
6506/java
```

13. Use the `hostname` and `ping` commands to check whether the hostname is resolvable. The following shows that the hostname is resolvable.

```
# hostname
centos7
# ping centos7
PING centos7 (10.16.4.28) 56(84) bytes of data.
64 bytes from centos7 (10.16.4.28): icmp_seq=1 ttl=64 time=17.1 ms
64 bytes from centos7 (10.16.4.28): icmp_seq=2 ttl=64 time=0.095 ms
64 bytes from centos7 (10.16.4.28): icmp_seq=3 ttl=64 time=0.098 ms
64 bytes from centos7 (10.16.4.28): icmp_seq=4 ttl=64 time=0.081 ms
64 bytes from centos7 (10.16.4.28): icmp_seq=5 ttl=64 time=0.095 ms
64 bytes from centos7 (10.16.4.28): icmp_seq=6 ttl=64 time=0.081 ms

--- centos7 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5001ms
rtt min/avg/max/mdev = 0.081/2.936/17.169/6.365 ms

[root@centos7 ~]#
```

If the hostname is not resolvable, add the corresponding hostname information to the “hosts” file found at “/etc”.

Otherwise, the SMTP server setting and license key activation on the AhsayCBS may not work properly.

14. Check if cbs and cbsnfs are present with the `ls -la /etc/rc.d/rc[2-5].d/*cbs*` command. The following output shows that cbs and cbsnfs are present on AhsayCBS. These files are needed to enable the cbs and nfs service to start automatically after the machine has been rebooted.

```
# ls -la /etc/rc.d/rc[2-5].d/*cbs*
lrwxrwxrwx. 1 root root 15 Aug 11 16:40 /etc/rc.d/rc2.d/S99cbs ->
/etc/init.d/cbs
lrwxrwxrwx. 1 root root 18 Aug 11 16:40 /etc/rc.d/rc2.d/S99cbsnfs
-> /etc/init.d/cbsnfs
lrwxrwxrwx. 1 root root 15 Aug 11 16:40 /etc/rc.d/rc3.d/S99cbs ->
/etc/init.d/cbs
lrwxrwxrwx. 1 root root 18 Aug 11 16:40 /etc/rc.d/rc3.d/S99cbsnfs
-> /etc/init.d/cbsnfs
lrwxrwxrwx. 1 root root 15 Aug 11 16:40 /etc/rc.d/rc4.d/S99cbs ->
/etc/init.d/cbs
lrwxrwxrwx. 1 root root 18 Aug 11 16:40 /etc/rc.d/rc4.d/S99cbsnfs
-> /etc/init.d/cbsnfs
lrwxrwxrwx. 1 root root 15 Aug 11 16:40 /etc/rc.d/rc5.d/S99cbs ->
/etc/init.d/cbs

lrwxrwxrwx. 1 root root 18 Aug 11 16:40 /etc/rc.d/rc5.d/S99cbsnfs
-> /etc/init.d/cbsnfs
```

For newer Linux versions (e.g. CentOS 8, Red Hat Enterprise 8, Ubuntu 20.04 LTS), service startup after the machine has been rebooted is managed using systemd. Check if cbs and cbsnfs services are configured to startup automatically after reboot or power on with the `systemctl status cbs` and `systemctl status cbsnfs` commands.

```
# systemctl status cbs
● cbs.service - Service to run CBS
     Loaded: loaded (/etc/systemd/system/cbs.service; enabled;
     vendor preset: enabled
     Active: active (exited) since Fri 2020-08-07 10:25:15 PST;
     4 days ago
  Main PID: 692 (code=exited, status=0/SUCCESS)
       Tasks: 0 (limit: 4657)
     Memory: 286.2M
     CGroup: /system.slice/cbs.service

Aug 07 10:26:09 ubuntu20 sh[692]: Using PHYSICAL_MEM  : 3936 (MB)
Aug 07 10:26:09 ubuntu20 sh[692]: ------------------------------
--------------------------->
Aug 07 10:26:09 ubuntu20 sh[692]: Using CBS_HOME      :
/usr/local/cbs
Aug 07 10:26:09 ubuntu20 sh[692]: Using JAVA_HOME     :
/usr/local/cbs/java
Aug 07 10:26:09 ubuntu20 sh[692]: Using CATALINA_HOME :
/usr/local/cbs/tomcat
Aug 07 10:26:09 ubuntu20 sh[692]: Using JAVA_OPTS     : -
Djava.library.path=/usr/local/cbs/l>
Aug 07 10:26:09 ubuntu20 sh[692]: Using CATALINA_OPTS :
Aug 07 10:26:09 ubuntu20 sh[692]: Using CATALINA_PID  :
/var/run/obsr.pid
Aug 07 10:26:09 ubuntu20 sh[692]: ------------------------------
--------------------------->
Aug 07 10:26:09 ubuntu20 sh[692]: Starting AhsayCBS service
```

```
# systemctl status cbsnfs
● cbsnfs.service - Service to run CBSNFS
     Loaded: loaded (/etc/systemd/system/cbsnfs.service;
     enabled; vendor preset: enabled
     Active: active (exited) since Fri 2020-08-07 10:25:15 PST;
     4 days ago
  Main PID: 693 (code=exited, status=0/SUCCESS)
       Tasks: 0 (limit: 4657)
     Memory: 1.4M
     CGroup: /system.slice/cbsnfs.service

Aug 07 10:25:15 ubuntu20 systemd[1]: Started Service to run
CBSNFS.

Aug 07 10:25:15 ubuntu20 sh[693]: Starting NFS Service (Ahsay
Systems Corporation)
```

If the cbs and cbsnfs services are not starting up automatically after reboot or power on, for example when "`systemctl status`" return the following results:

```
# systemctl status cbs
● cbs.service - Service to run CBS
     Loaded: loaded (/etc/systemd/system/cbs.service; disabled;
     vendor preset: enabled
     Active: inactive (dead)
```

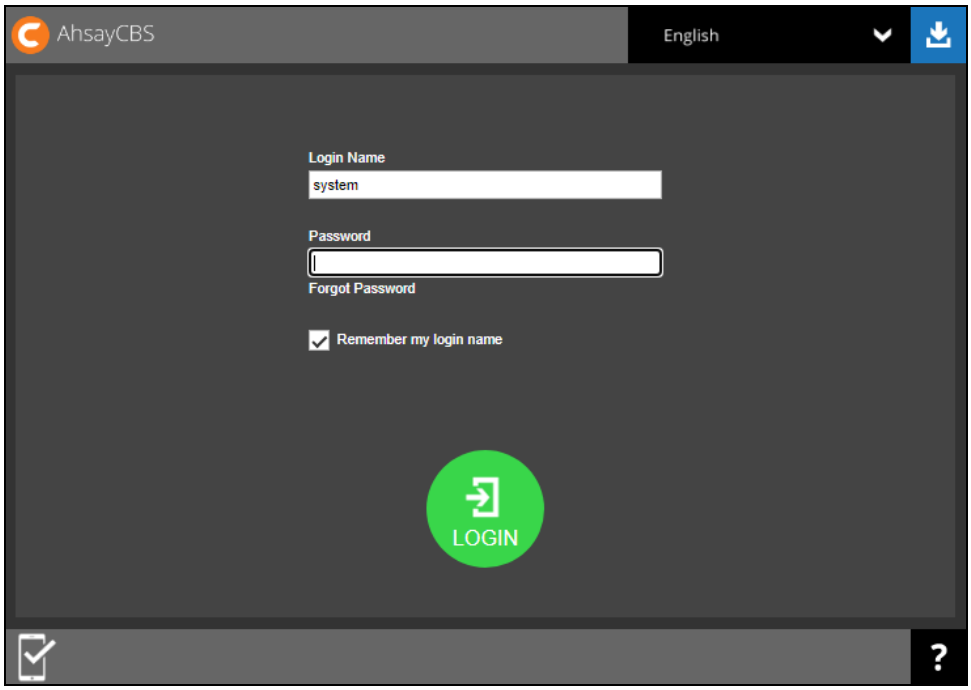
```
# systemctl status cbsnfs
● cbsnfs.service - Service to run CBSNFS
     Loaded: loaded (/etc/systemd/system/cbsnfs.service;
     disabled; vendor preset: enabled
     Active: inactive (dead)
```

It is recommended to enable them using the following commands: `systemctl enable cbs` and `systemctl enable cbsnfs`

```
# systemctl enable cbs
Synchronizing state of cbs.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable cbs
```

```
# systemctl enable cbsnfs
Synchronizing state of cbsnfs.service with SysV service script
with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable cbsnfs
```

15. After successful installation, you can access the login page by opening `https://<your-backup-server>` in a browser.



5.5 Installation on FreeBSD

Pre-requisite requirements:

Make sure OpenJDK Version 1.8 has been installed beforehand since the user will be asked to enter the location of the java 1.8 home. Also OpenJDK8 and GNU C Library must be installed on FreeBSD to support AhsayCBS NFS service.

- Install GNU C Library:
  - Login to the AhsayCBS server as root
  - Change working directory to /usr/ports/misc/compat9x and add additional ports.

```
cd /usr/ports/misc/compat9x
```

  - make installation

```
make install distclean
```

- Ahsay CBS installation path: /usr/local/cbs
- OpenJDK installation path: /usr/local/openjdk8

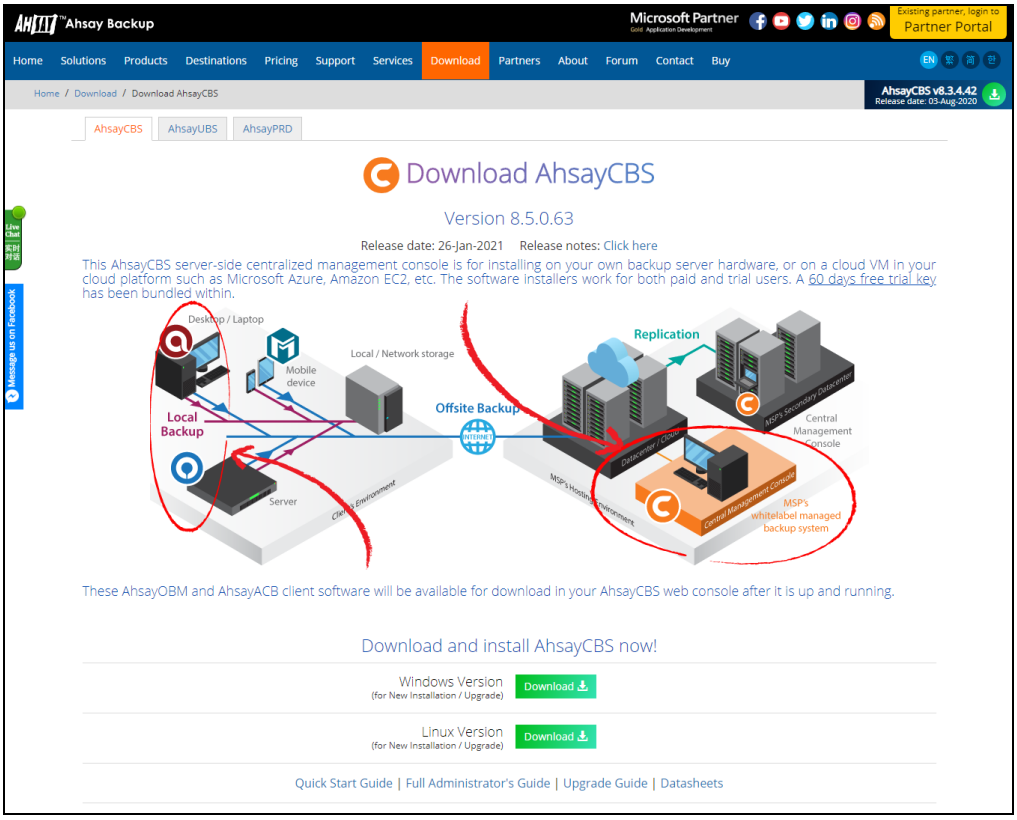
1. Log in as root on your FreeBSD machine.

```
login as: root
Using keyboard-interactive authentication.
Password for root@fbsd10-4-45:
```

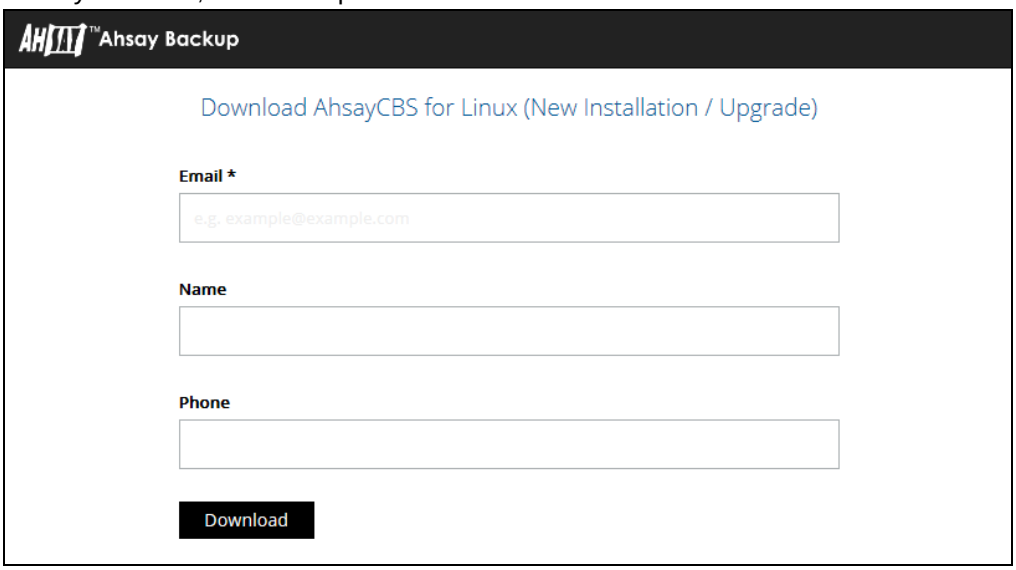
2. Create a directory `/usr/local/cbs` for the AhsayCBS installation.

```
mkdir -p /usr/local/cbs
```

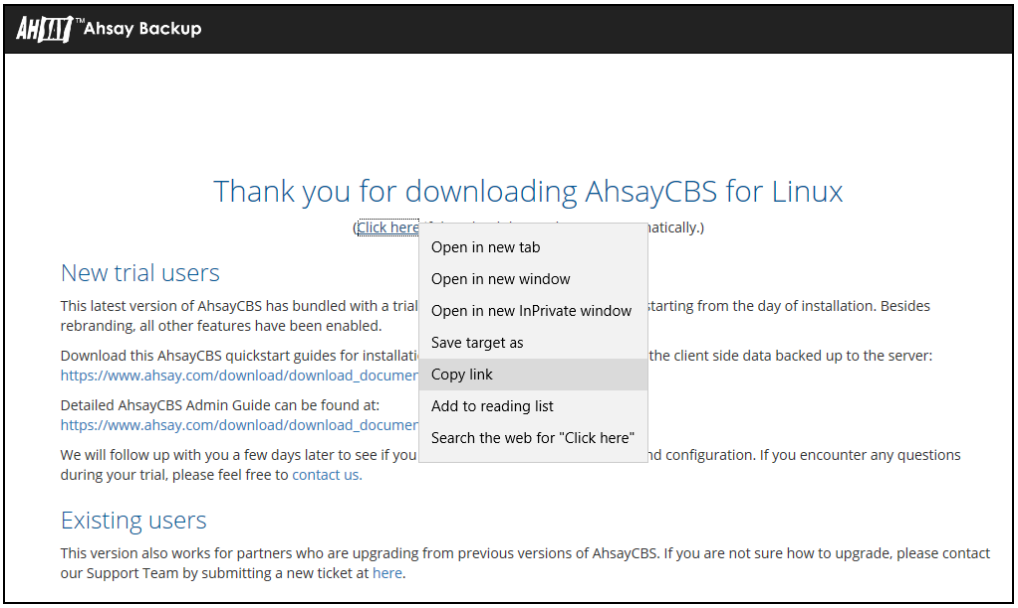
3. In a browser, download the AhsayCBS installation package **cbs-nix.tar.gz** from the Ahsay website by clicking on the Download button.



4. Enter your email, name and phone then click Download.



5. Right-click on the Click here link then select Copy link.



6. Go to the cbs directory you created then download the installation package cbs-nix.tar.gz with the `fetch` command.

```
# cd /usr/local/cbs
# fetch http://ahsay-dn.ahsay.com/v8/83030/cbs-nix.tar.gz
cbs-nix.tar.gz                                  100% of  933
MB   383 kBps 41m33s
```

7. Unzip and extract the installation files with the following `tar` command.

```
# tar xvfz cbs-nix.tar.gz
```

8. Go to the `/usr/local/cbs/bin` directory.

```
# cd /usr/local/cbs/bin
```

9. To execute the installation file, type the following command:

```
# sh install.sh
```

10. When asked to enter the java 1.8 home, type the following: `/usr/local/openjdk8` which is the location of your java 1.8 home but the path may be different depending on the installed java.

```
Log Time: Thu Apr  4 10:32:17 HKT 2019

Verifying current user privilege ...
Current user has enough privilege to "install".

Start configuration on BSD distribution Platform
(FreeBSD)
Using CBS_HOME /usr/local/cbs
Please enter your java 1.8 home:
/usr/local/openjdk8
```

11. After successful installation, the screen will look like the following:

```
Copy java 1.8 from /usr/local/openjdk8
Current Directory: "/usr/local/cbs".
Created symlink "java" to "jvm".
Minimum supported JVM version: 1.8
Current JVM version is supported for installation.
Installing [ Ahsay Cloud Backup Suite ]
[ Ahsay Cloud Backup Suite ] Service Script created at
/usr/local/cbs/bin/cbs
Please provide the path to the service script!
Install Service for BSD type OS
Copying script cbs to /usr/local/etc/rc.d
You may start this service by:

sh "/usr/local/etc/rc.d/cbs" start &


[ Ahsay Cloud Backup Suite ] setup completed!
Migrate from previous version
/usr/local/cbs
Get Startup path for BSD type OS
RDR_HOME
OBS_HOME
OBSR_HOME /usr/local/cbs
RPS_HOME
Run MigrateV6 script
Startup [ Ahsay Cloud Backup Suite ]
Run MigrateV7 script
------------------------------------------------------------
------
You may set SYSTEM_DEBUG=0 to disable the debug message
------------------------------------------------------------
-------------
Current User Name   : root
Using SYSTEM_TYPE   : bsd
Using SYSTEM_ARCH   : amd64
Using PHYSICAL_MEM  : 4063(MB)
------------------------------------------------------------
-------------
Using CBS_HOME      : /usr/local/cbs
Using JAVA_HOME     : /usr/local/cbs/java
Using CATALINA_HOME : /usr/local/cbs/tomcat
Using JAVA_OPTS     : -
Djava.library.path=/usr/local/cbs/lib/FbdX64 -
DCATALINA_PID=/var/run/obsr.pid -Xrs -Xms512m -Xmx2048m -
Xss384k -XX:PermSize=96m -XX:MaxPermSize=160m -
XX:MaxDirectMemorySize=512m -XX:NewRatio=3 -
XX:SurvivorRatio=30 -XX:MinHeapFreeRatio=20 -
XX:MaxHeapFreeRatio=80 -XX:+PrintGCDetails -
XX:+PrintGCDateStamps -XX:+UseParNewGC -
XX:+UseConcMarkSweepGC -XX:+CMSParallelRemarkEnabled -
XX:+UseCMSInitiatingOccupancyOnly  -
XX:CMSInitiatingOccupancyFraction=85 -
XX:+ScavengeBeforeFullGC  -XX:+CMSScavengeBeforeRemark -
XX:PerfDataSamplingInterval=500 -
Dsun.net.inetaddr.ttl=3600 -Dnetworkaddress.cache.ttl=3600
-Dsun.net.inetaddr.negative.ttl=300 -
Dnetworkaddress.cache.negative.ttl=300 -
```

```
Dsun.nio.PageAlignDirectMemory=true -
Djava.net.preferIPv4Stack=true -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogM
anager -
Djava.util.logging.config.file=conf/logging.properties -
Dtc.work.path=work -Dtc.log.path=logs -
Djavax.servlet.context.tempdir=work
Using CATALINA_OPTS :
Using CATALINA_PID  : /var/run/obsr.pid
-------------------------------------------------------
-------------
Starting AhsayCBS service
Started [ Ahsay Cloud Backup Suite ]
Installing [ NFS Service (Ahsay Systems Corporation) ]
[ NFS Service (Ahsay Systems Corporation) ] Service Script
created at /usr/local/cbs/nfs/bin/cbsnfs
Please provide the path to the service script!
Install Service for BSD type OS
Copying script cbsnfs to /usr/local/etc/rc.d
You may start this service by:

sh "/usr/local/etc/rc.d/cbsnfs" start &

[ NFS Service (Ahsay Systems Corporation) ] setup
completed!
Startup [ NFS Service (Ahsay Systems Corporation) ]
Starting NFS Service (Ahsay Systems Corporation)
Started [ NFS Service (Ahsay Systems Corporation) ]
```

12. Check if Java is running on AhsayCBS with the `ps -a|grep java` command. The following output shows that Java is running on AhsayCBS.

```
# ps -a|grep java
59569  2  I    23:08.38 /usr/local/cbs/java/bin/java -
Djava.util.logging.config.file=/usr/local/cbs/conf/logging
.properties -Djava.util.logging.manager=org.apache.j
65139  2  R+    0:00.00 grep java
```

13. To check the details of the parameters and values used by the Java process, use the `procstat -c {process ID}` command. The following output shows the details of the Java process.

```
# procstat -c 59569
  PID COMM             ARGS
59569 java             /usr/local/cbs/java/bin/java -
Djava.util.logging.config.file=/usr/local/cbs/conf/logging
.properties -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogM
anager -Djava.library.path=/usr/local/cbs/lib/FbdX64 -
DCATALINA_PID=/var/run/obsr.pid -Xrs -Xms512m -Xmx2048m -
Xss384k -XX:MetaspaceSize=96m -XX:MaxMetaspaceSize=256m -
XX:MaxDirectMemorySize=512m -XX:NewRatio=3 -
XX:SurvivorRatio=32 -XX:MinHeapFreeRatio=20 -
XX:MaxHeapFreeRatio=80 -XX:+PrintGCDetails -
XX:+PrintGCDateStamps -XX:+UseConcMarkSweepGC -
XX:+UseCMSInitiatingOccupancyOnly -
XX:CMSInitiatingOccupancyFraction=85 -
XX:+ScavengeBeforeFullGC -XX:+CMSScavengeBeforeRemark -
```

```
Dsun.net.inetaddr.ttl=3600 -Dnetworkaddress.cache.ttl=3600
-Dsun.net.inetaddr.negative.ttl=300 -
Dnetworkaddress.cache.negative.ttl=300 -
Dsun.nio.PageAlignDirectMemory=true -
Djava.net.preferIPv4Stack=true -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogM
anager -
Djava.util.logging.config.file=conf/logging.properties -
Dtc.work.path=work -Dtc.log.path=logs -
Djavax.servlet.context.tempdir=work -
Djdk.nio.maxCachedBufferSize=262144 -Dfile.encoding=UTF-8
-Dsun.jnu.encoding=UTF-8 -Djdk.tls.ephemeralDHKeySize=2048
-
Djava.protocol.handler.pkgs=org.apache.catalina.webresourc
es -
Dorg.apache.catalina.security.SecurityListener.UMASK=0027
-Dignore.endorsed.dirs= -classpath
/usr/local/cbs/tomcat/bin/bootstrap.jar:/usr/local/cbs/tom
cat/bin/tomcat-juli.jar -Dcatalina.base=/usr/local/cbs -
Dcatalina.home=/usr/local/cbs/tomcat -
Djava.io.tmpdir=/usr/local/cbs/temp
org.apache.catalina.startup.Bootstrap start
```

14. Check if NFS Service is running on AhsayCBS with the `ps -a|grep nfs` command. The following output shows that NFS Service is running on AhsayCBS.

```
# ps -a|grep nfs
40359  0- S     0:40.09 /usr/local/cbs/nfs/bin/NfsFbdX64 -
logfile /usr/local/cbs/nfs/log/debug.log -pidfile
/var/run/cbsnfs.pid
65555  3  R+    0:00.00 grep nfs
```

15. Check if the process for rotating logs is running on AhsayCBS with the `ps -a|grep rotatelogs` command. The following output shows that rotate logs process is running on AhsayCBS.

```
# ps -a|grep rotatelogs
59568  2  I     0:00.51
/usr/local/cbs/bin/FbdX64/rotatelogs -f
/usr/local/cbs/logs/console_%Y-%m-%d.log 86400
65656  3  S+    0:00.00 grep rotatelogs
```

16. Check if AhsayCBS is listening to both pre-defined http and https ports (i.e. Ports 80 and 443) with the `netstat -an|more` command. In the following screenshot, AhsayCBS is listening to both ports:

```
# netstat -an|more
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address
(state)
tcp4       0      0 127.0.0.1.60024        *.*
LISTEN
tcp4      85      0 10.16.4.45.36242
203.186.85.237.443     CLOSE_WAIT
tcp4       0      0 10.16.4.45.443
10.20.1.37.51021       ESTABLISHED
tcp4      85      0 10.16.4.45.60497
```

```
203.186.85.237.443     CLOSE_WAIT
tcp4       0      0 *.443                  *.*
LISTEN
tcp4       0      0 *.80                   *.*
LISTEN
tcp4       0      0 10.16.4.45.22
192.168.7.104.3983     ESTABLISHED
tcp4       0      0 10.16.4.45.22
192.168.7.104.3956     ESTABLISHED
tcp4       0      0 10.16.4.45.22
192.168.7.117.4617     ESTABLISHED
tcp4       0      0 10.16.4.45.952
192.168.22.40.2049     ESTABLISHED
tcp4       0      0 10.16.4.45.788
192.168.22.40.2049     ESTABLISHED
tcp4       0      0 *.44097                *.*
LISTEN
tcp6       0      0 *.31178                *.*
LISTEN
tcp4       0      0 127.0.0.1.25           *.*
LISTEN
tcp4       0      0 *.22                   *.*
LISTEN
tcp6       0      0 *.22                   *.*
LISTEN
udp4       0      0 *.10000                *.*
udp4       0      0 *.51313                *.*
udp4       0      0 *.5353                 *.*
udp4       0      0 *.514                  *.*
udp6       0      0 *.514                  *.*
```

For AhsayCBS servers hosting Run on Server (Agentless) Office 365 and Cloud File backups, ensure that AhsayCBS is listening to port 8081 (default) on local IP address 127.0.0.1.

```
# netstat -an|more
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address
(state)
tcp4       0      0 *.443                  *.*
LISTEN
tcp4       0      0 *.80                   *.*
LISTEN
tcp4       0      0 127.0.0.1.8081         *.*
LISTEN
tcp4       0      0 10.16.30.21.27873
125.5.184.206.80       SYN_SENT
tcp4       0      0 10.16.30.21.22
192.168.12.1.56311     ESTABLISHED
tcp4       0      0 127.0.0.1.25           *.*
LISTEN
tcp4       0      0 *.22                   *.*
LISTEN
tcp6       0      0 *.22                   *.*
LISTEN
udp4       0      0 *.10000                *.*
udp4       0      0 *.514                  *.*
udp6       0      0 *.514                  *.*
```

17. Use the hostname and ping commands to check whether the hostname is resolvable. The following shows that the hostname is resolvable.

```
root@freebsd11:~ # hostname
    freebsd11
    root@freebsd11:~ # ping freebsd11
    PING freebsd11 (10.90.30.21): 56 data bytes
    64 bytes from 10.90.30.21: icmp_seq=0 ttl=64 time=0.267 ms
    64 bytes from 10.90.30.21: icmp_seq=1 ttl=64 time=0.344 ms
    64 bytes from 10.90.30.21: icmp_seq=2 ttl=64 time=0.238 ms
    64 bytes from 10.90.30.21: icmp_seq=3 ttl=64 time=0.226 ms
    64 bytes from 10.90.30.21: icmp_seq=4 ttl=64 time=0.269 ms
    64 bytes from 10.90.30.21: icmp_seq=5 ttl=64 time=0.259 ms
    ^C
    --- freebsd11 ping statistics ---
    6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.226/0.267/0.344/0.038 ms
```

If the hostname is not resolvable, add the corresponding hostname information to the "hosts" file found at "/etc".

Otherwise, the SMTP server setting on the AhsayCBS may not work properly. Also, AhsayCBS may not be able to connect to the Ahsay license server.

18. Check if cbs and cbsnfs are enabled in the /etc/rc.conf file with the `cat /etc/rc.conf` command. The following output shows that cbs and cbsnfs are enabled.

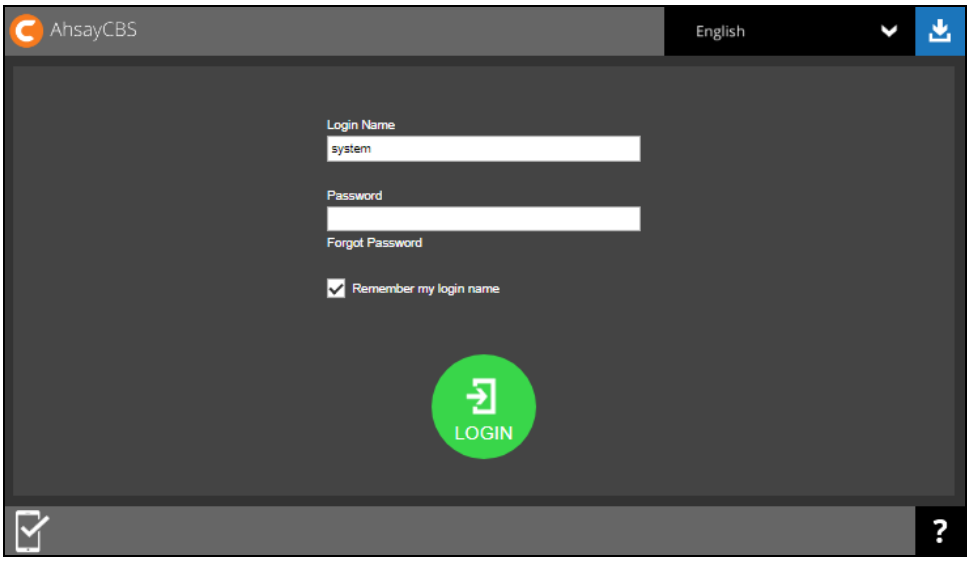
```
# cat /etc/rc.conf
root@freebsd11:~ # cat /etc/rc.conf
hostname="freebsd11"
ifconfig_em0="inet 10.16.30.21 netmask 255.252.0.0"
defaultrouter="10.16.0.1"
sshd_enable="YES"
# Set dumpdev to "AUTO" to enable crash dumps, "NO" to
disable
dumpdev="AUTO"
firewall_enable="NO"
cbs_enable="YES"
cbsnfs_enable="YES"
obmscheduler_enable="YES"
```

19. Check if cbs and cbsnfs are present in /usr/local/etc/rc.d directory with the `ls -la /usr/local/etc/rc.d` command. The following output shows that cbs and cbsnfs are available. These files will enable the cbs and nfs service to automatically start after the machine has been rebooted.

```
# ls -la /usr/local/etc/rc.d
root@freebsd11:~ # ls -la /usr/local/etc/rc.d
total 56
drwxr-xr-x   2 root  wheel    512 Apr  4 10:33 .
drwxr-xr-x  16 root  wheel    512 Dec 13 12:41 ..
-rwxr-xr-x   1 root  wheel    849 Apr  4 10:33 cbs
-rwxr-xr-x   1 root  wheel    983 Apr  4 10:33 cbsnfs
-r-xr-xr-x   1 root  wheel    789 Feb 25  2017 dbus
-r-xr-xr-x   1 root  wheel   2573 Feb 25  2017 hald
-rwxr-xr-x   1 root  wheel    714 Jan 22 11:59
obmscheduler
```

```
-rwxr-xr-x   1 root  wheel  27714 Mar  8  2017 vmware-
tools.sh
```

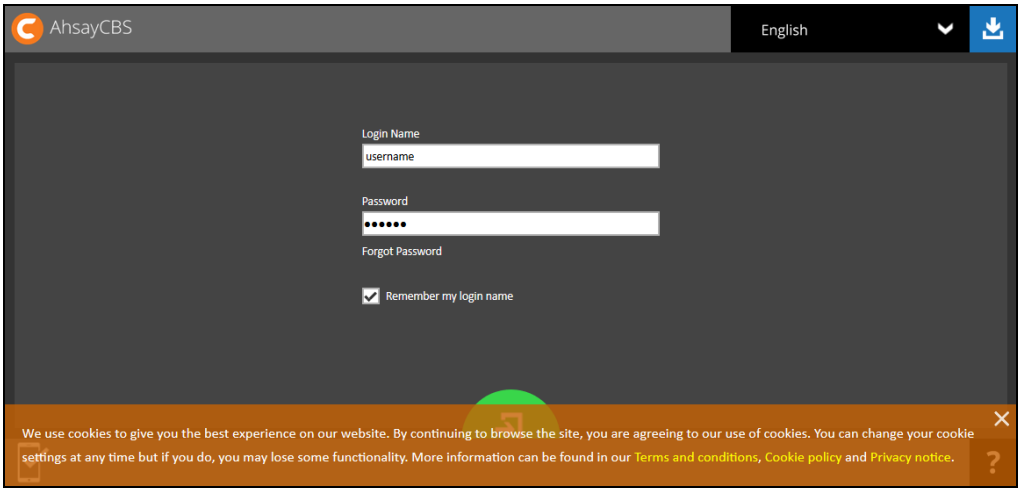
20. After successful installation, you can access the login page by opening `https://<your-backup-server>` in a browser.



6 Basic Setup and Configuration

6.1 Activating License

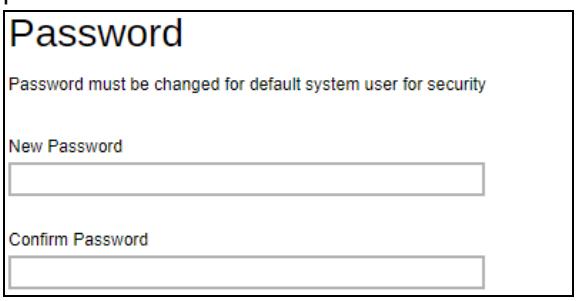
1. Open AhsayCBS from your browser, e.g. https://<your-backup-server>.



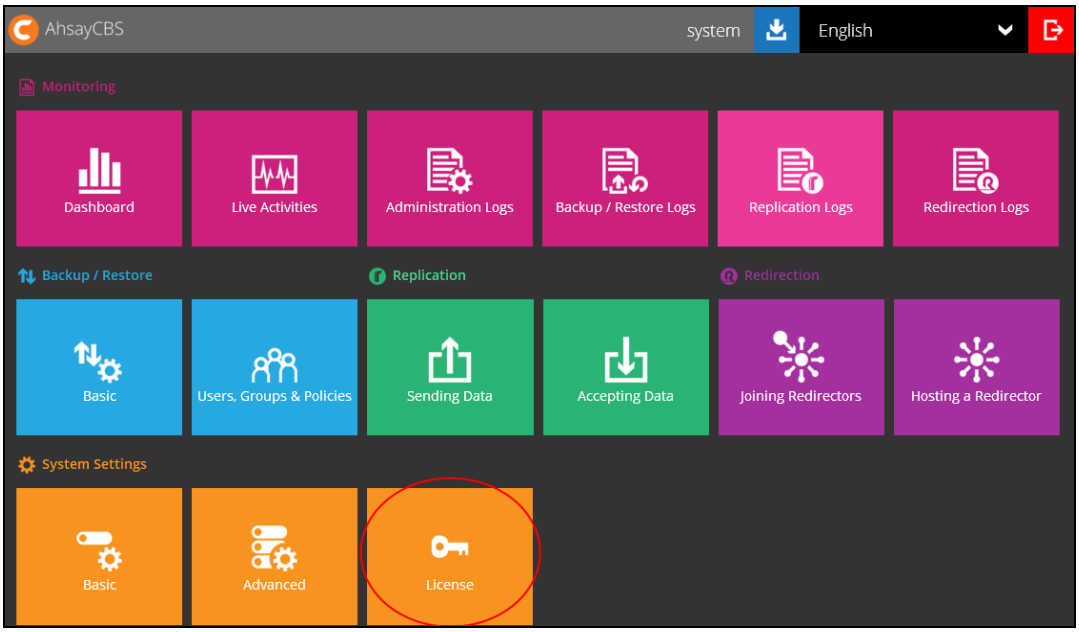
2. Log in to the AhsayCBS with the following default credentials.

   - Login name: system
   - Password: system

3. Only for first time login, starting with v8.3.4.0 and onwards, the user will be asked to change the password before they can proceed. Enter the new password and confirm password. Click  to save.

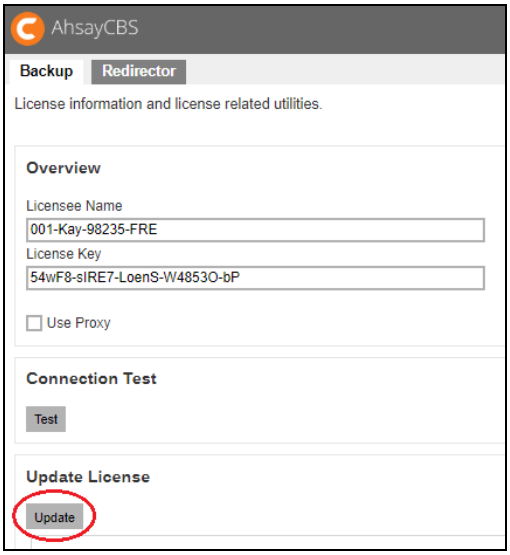


4. To activate the license, click the **License** icon.

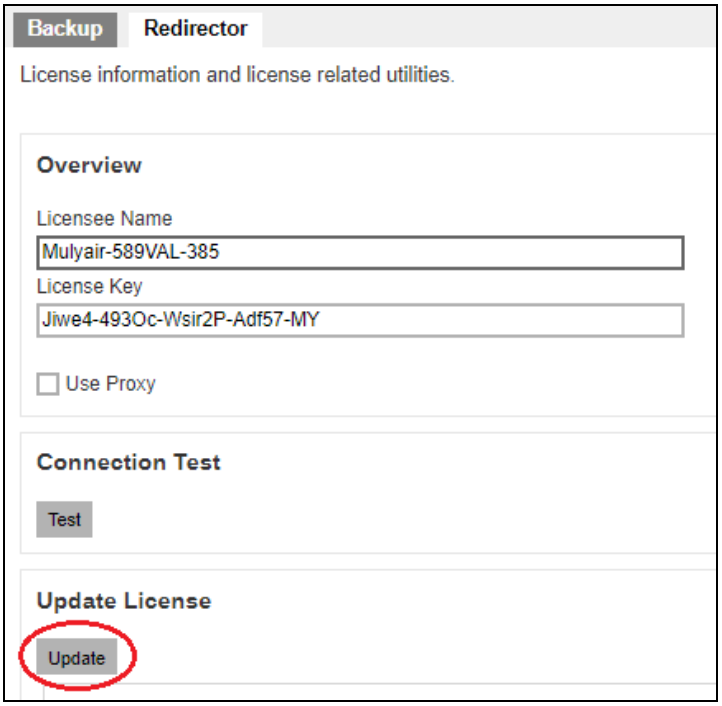


5. Applying the license key

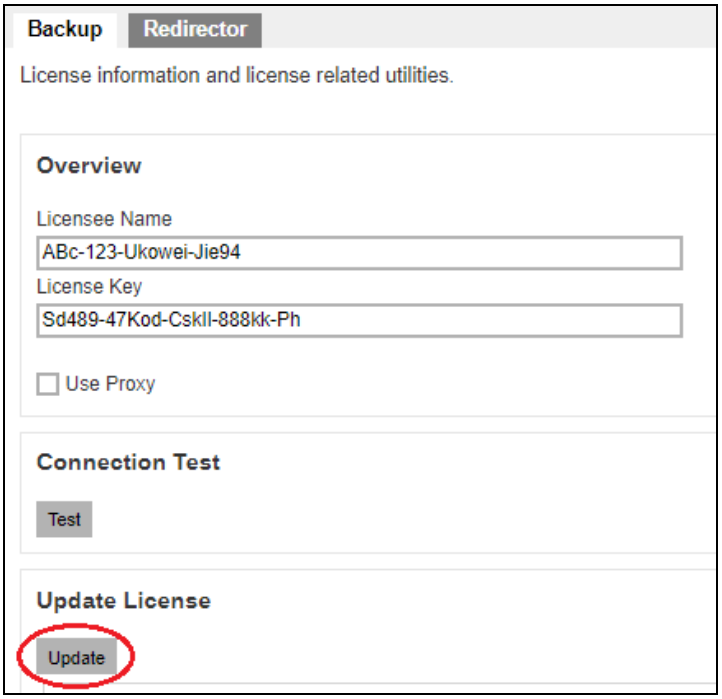
- If you are evaluating the AhsayCBS, you can use the evaluation license key provided on the page by default and click the **Update** button.
- If you have purchased a Backup license, click on the Backup tab then copy and paste the licensee name, license key into the relevant field. Then click the **Update** button.



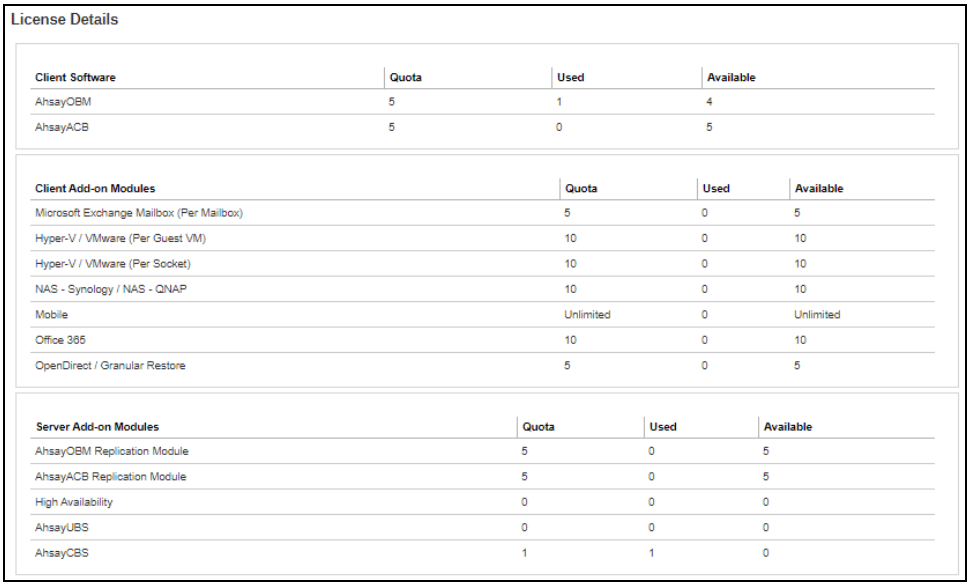
- If you have purchased a Redirector license, go to the Redirector tab, do the same by copying and pasting the licensee name and license key to the relevant field then click the **Update** button.



- For the Replication Server, an additional AhsayCBS license module is needed. Go to the Backup tab then copy and paste the licensee name, license key into the relevant field. Then click the **Update** button.



Make sure that you have sufficient Replication module license in your backup server. You can check it in the License Details section.



License Details

Client Software	Quota	Used	Available
AhsayOBM	5	1	4
AhsayACB	5	0	5

Client Add-on Modules	Quota	Used	Available
Microsoft Exchange Mailbox (Per Mailbox)	5	0	5
Hyper-V / VMware (Per Guest VM)	10	0	10
Hyper-V / VMware (Per Socket)	10	0	10
NAS - Synology / NAS - QNAP	10	0	10
Mobile	Unlimited	0	Unlimited
Office 365	10	0	10
OpenDirect / Granular Restore	5	0	5

Server Add-on Modules	Quota	Used	Available
AhsayOBM Replication Module	5	0	5
AhsayACB Replication Module	5	0	5
High Availability	0	0	0
AhsayUBS	0	0	0
AhsayCBS	1	1	0

6. Click  at the bottom right corner of the page to save the settings.

NOTE

The evaluation key can only be applied if it has not been activated before in the machine. If you are using the evaluation license key, you will be able to evaluate the AhsayCBS for 60 days. After which the AhsayCBS service will automatically stop working. Although the service is still active, the AhsayOBM and AhsayACB clients will not be able to connect to perform any backups or restores. If you would like to continue to use AhsayCBS, please contact the Sales team at Ahsay by email at sales-kb@ahsay.com or call our International Sales Hotline +852 3580 8091.

Two types of license: OEM and Meter Key

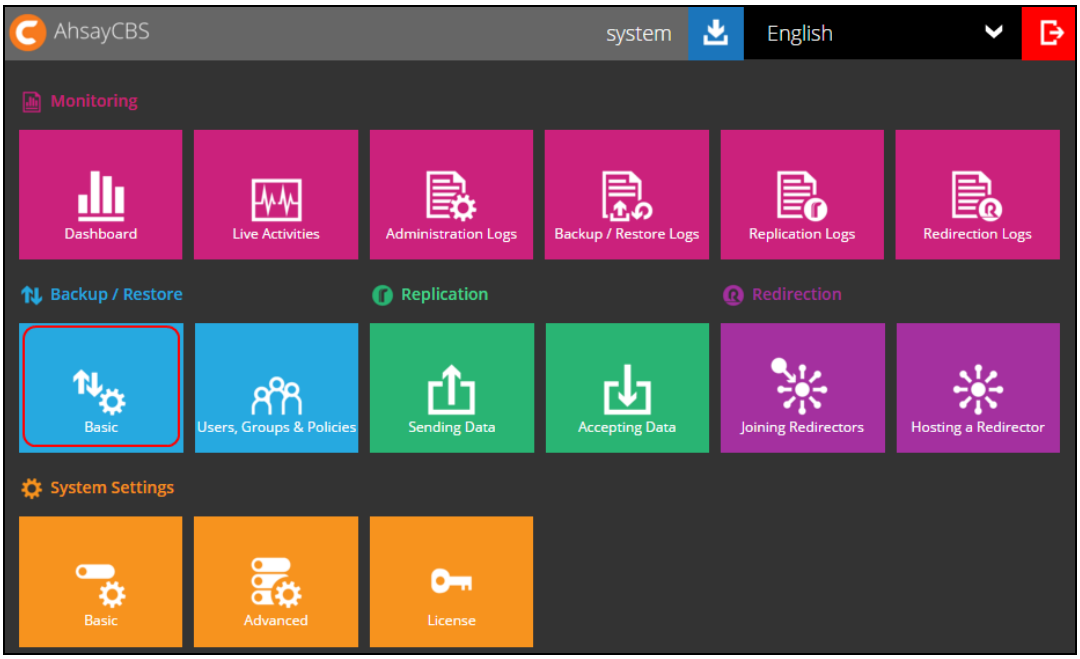
- One type of license is the OEM Key where you purchase the license key and included in the purchase price is the first-year maintenance. This will be enrolled in the Standard Support plan wherein you are entitled to hotfixes and releases. The maintenance will start upon activation of the license key in the AhsayCBS server. For example if you purchased an OEM Key and it was activated on January 1, then you will be entitled to a Standard Support plan for one year from date of activation. So the Standard Support plan will end on December 31. Afterwhich, you need to renew a valid support maintenance if you want to continue getting support. To know more about the different support maintenance please check the page Get Served by Our Support Engineers.

- Another type of license is the Meter Key where you only pay for what you use monthly. With this license you only need to pay an initial meter deposit which is valid for eighteen (18) months. Your monthly usage will be automatically deducted from the initial meter deposit. Once the meter deposit is depleted, you have the option of topping up the meter deposit or pay your invoices on a monthly basis. In this type of license, there is no need to pay for support maintenance since it is already included in the monthly meter rate. Check out the latest price for the Meter Key by checking this page Pricing for Meter License.

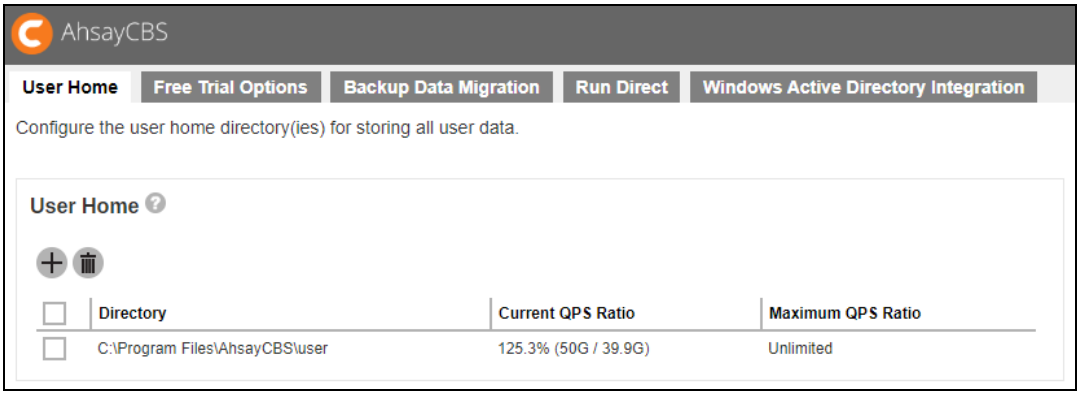
6.2 Setting up User Home

Set up a user home in your AhsayCBS to store the user's information and back up files in your local or network drive.

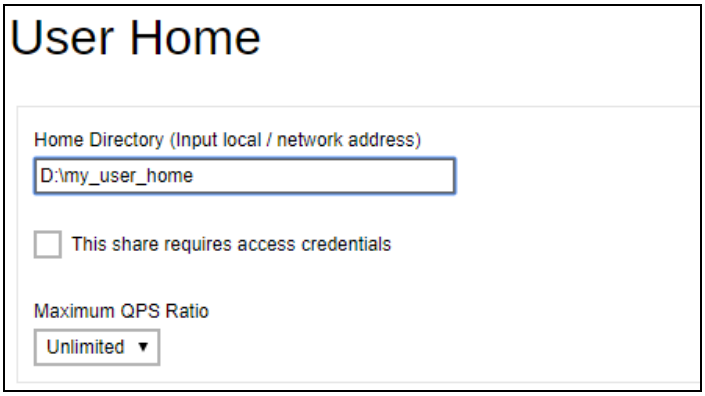
1. Click the blue **Basic** icon on the AhsayCBS main page.



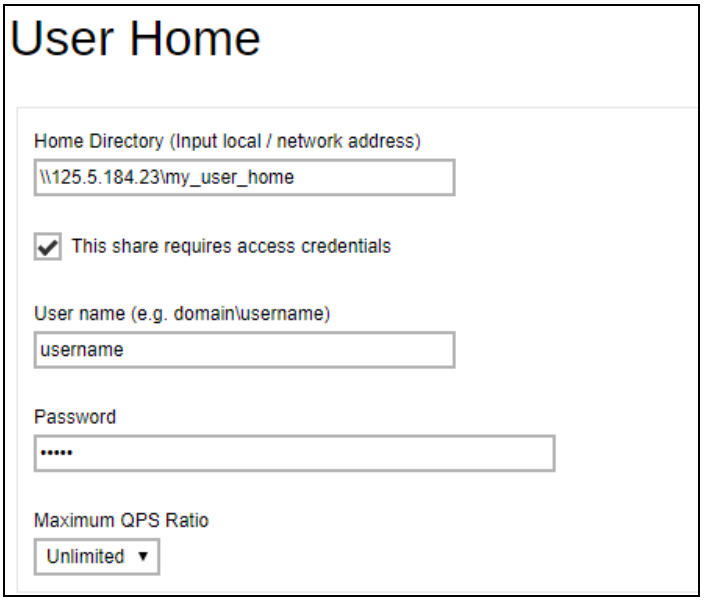
2. In the **User Home** tab, click  .



3. Enter the directory path in the **Home Directory** field (e.g. **D:\my_user_home**) and click when done.



It may also be set up in a network drive. Enter the network address in the **Home Directory** field. If access credentials are required to connect to the network drive, check the box beside **This share requires access credentials**. Enter the **User name** and **Password**. Click when done.



NOTE

It is NOT suggested to store your user home in your system partition, e.g. **C:**.

4. Click at the bottom right corner to save the new user home settings.

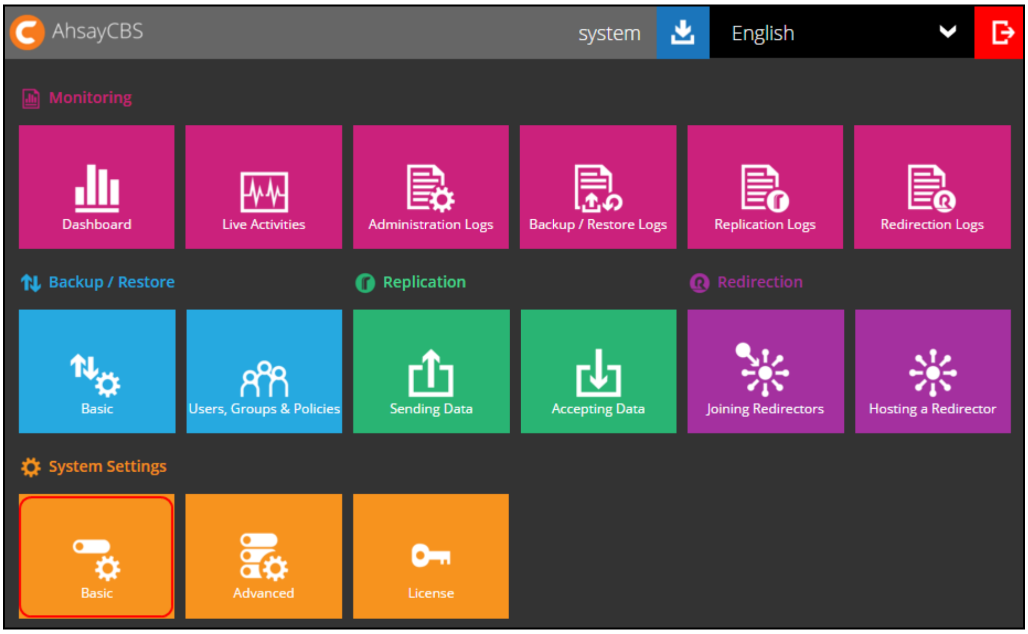
NOTE

For cloud setup, please refer to AhsayCBS v8 Administrator's Guide.

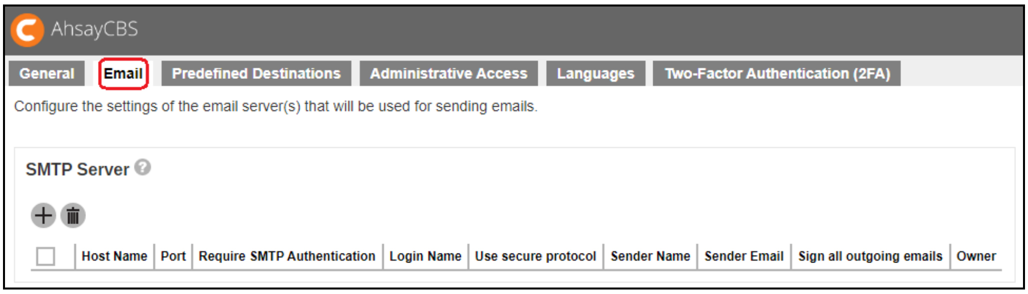
6.3 Setting up SMTP

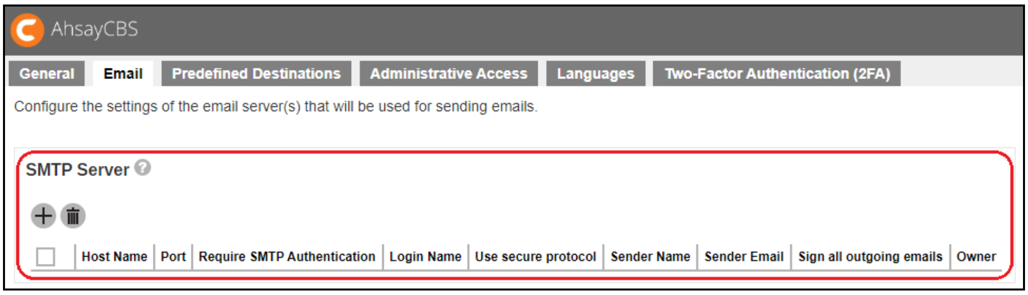
Configure the SMTP so that you can receive reports from the AhsayCBS.

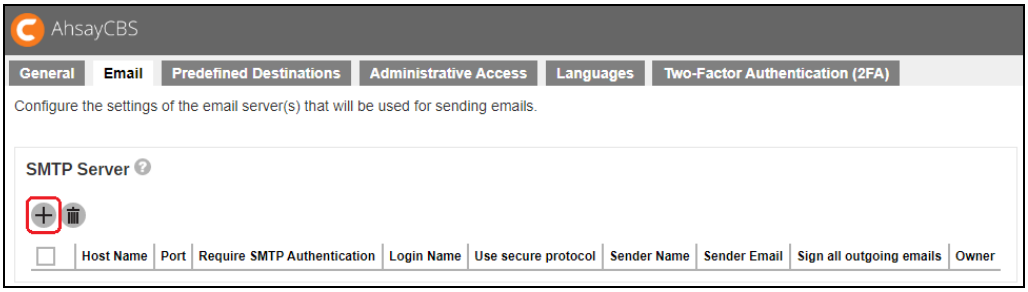
1. Click the orange **Basic** icon under **System Settings** section on AhsayCBS main page.



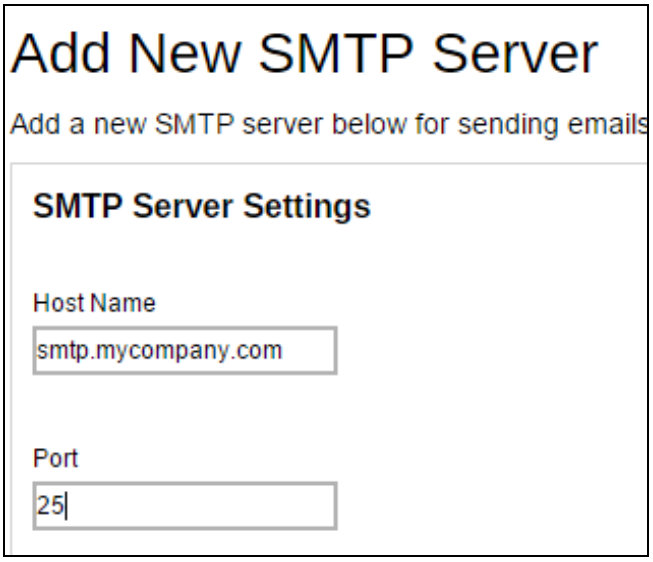
2. In the **Email** tab, locate the **SMTP Server** section. Then, click +.



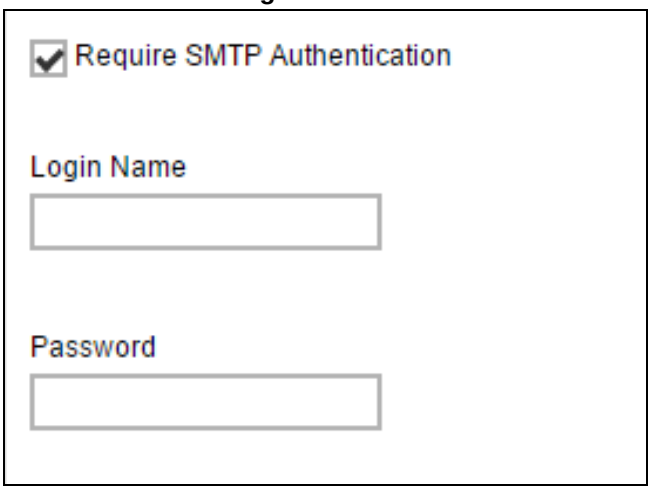




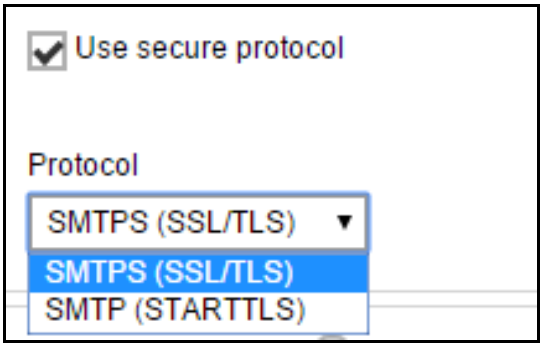
3. Enter the SMTP mail server settings in the Host Name and Port fields.



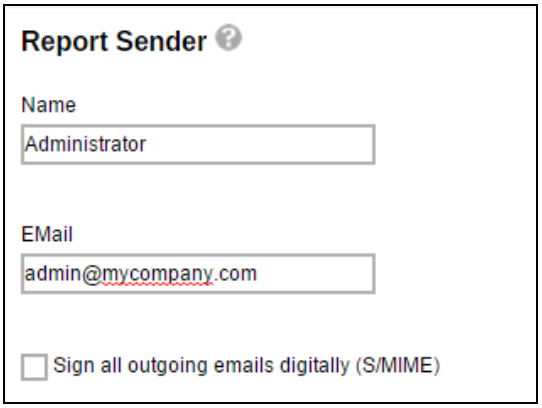
4. If authentication is required, click the checkbox next to Require SMTP Authentication and then enter the **Login Name** and **Password**.



Optional: Click the checkbox **Use secure protocol** if required. Select the type of **Protocol** from the drop-down box.



5. Enter the report sender's name and email address.



6. Click  at the bottom right corner to save the SMTP settings.

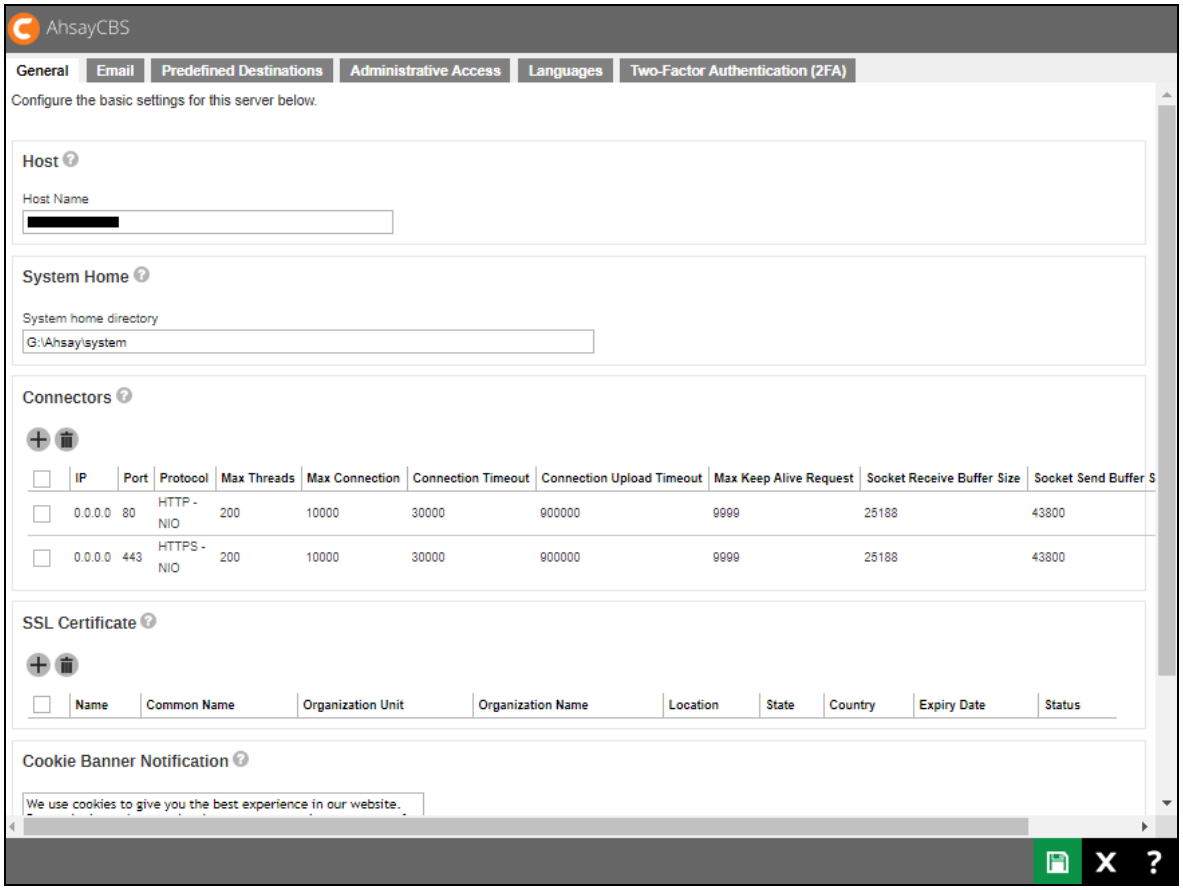
7. Click  at the bottom right corner to save the settings.

NOTE

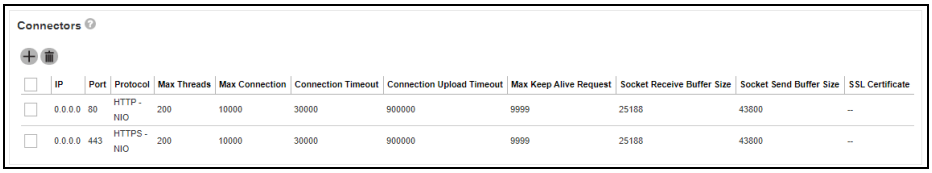
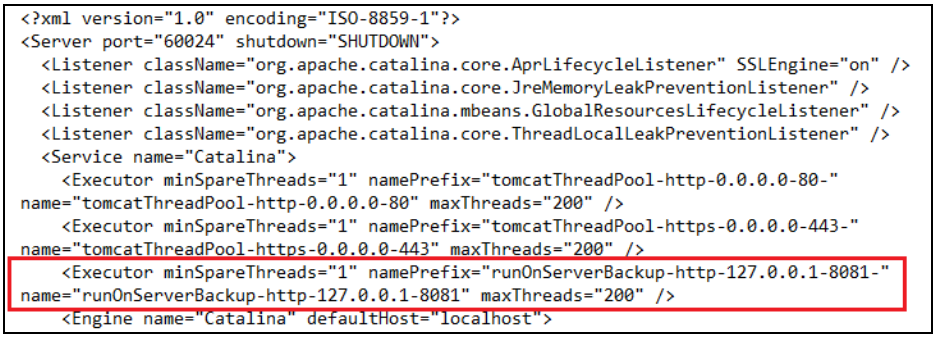
- If you don't have a SMTP server, you can consider using a free SMTP such as Gmail.
- AhsayCBS supports SMTP servers which use either TLS v1.0, v1.1 or v1.2.

6.4 Setting up Hostname & System Home

Configure the AhsayCBS hostname and system home path.



Section	Description
Host	This is the host name of your AhsayCBS. You can enter the domain name of your AhsayCBS in the formats of "IP Address:port_number" or "www.mybackup.com:port_number" **Note**: The **Host Name** will be the access link for your users to get access to the AhsayCBS. It needs a fully qualified domain name (FQDN) and must be resolvable. Since the host name will be used in various locations, such as inside welcome email as a reference point for the users to access the AhsayCBS, inside email as a reference link for the users to recover the password, users applying Run Direct restore feature, it is important to ensure the host name is accessible by users from external network environment.
System Home	This is the system home location of your AhsayCBS where the system logs and group policy files are located. This path is set to your installation home by default. For production systems the system home should not be setup on the O/S partition, as the logs could fill up the drive and result in system instability.

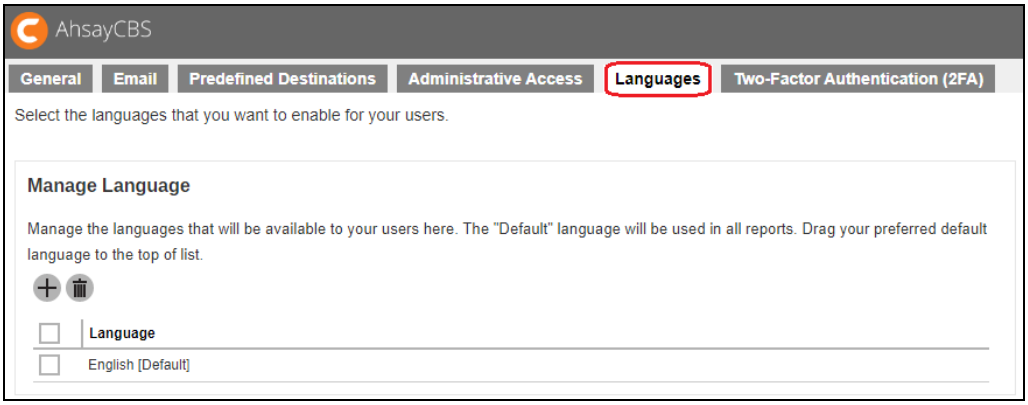
Connectors	This is the web server settings used to access the AhsayCBS web console. There are three connectors that are automatically setup by AhsayCBS upon installation. Two of them are the Apache Tomcat connectors which can be readily checked from the AhsayCBS web console.  While the third connector is used for Run on Server (Agentless) Office 365 and Cloud File backups, this is not visible from the AhsayCBS web console. The settings can be checked from the server.xml file which is located in the $Application_Home\conf folder. 


```
<?xml version="1.0" encoding="ISO-8859-1"?>
<Server port="60024" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
  <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />
  <Service name="Catalina">
    <Executor minSpareThreads="1" namePrefix="tomcatThreadPool-http-0.0.0.0-80-"
name="tomcatThreadPool-http-0.0.0.0-80" maxThreads="200" />
    <Executor minSpareThreads="1" namePrefix="tomcatThreadPool-https-0.0.0.0-443-"
name="tomcatThreadPool-https-0.0.0.0-443" maxThreads="200" />
    <Executor minSpareThreads="1" namePrefix="runOnServerBackup-http-127.0.0.1-8081-"
name="runOnServerBackup-http-127.0.0.1-8081" maxThreads="200" />
    <Engine name="Catalina" defaultHost="localhost">
```

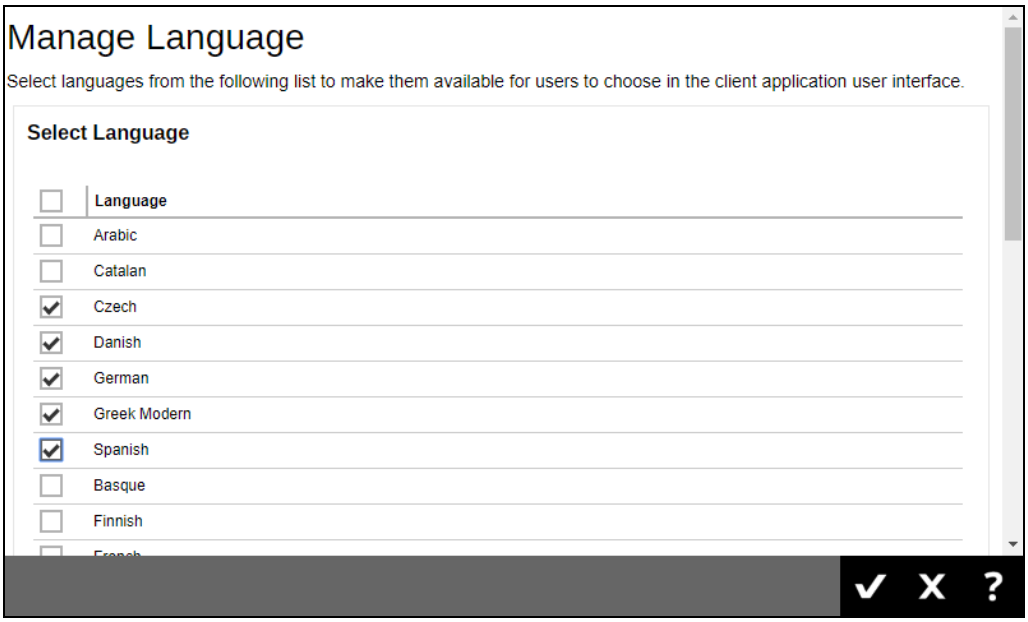
6.5 Setting up Languages

Upon installation, only English will be available for the languages. You need to set it up so that your preferred language will be included in the choice for languages.

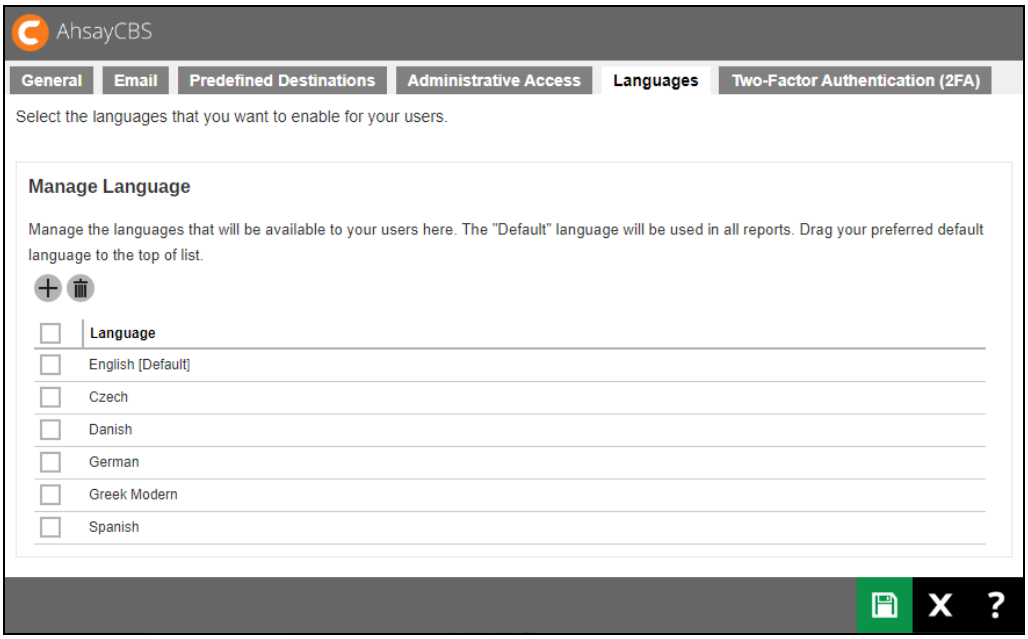
1. In the Languages tab click  to add a language.



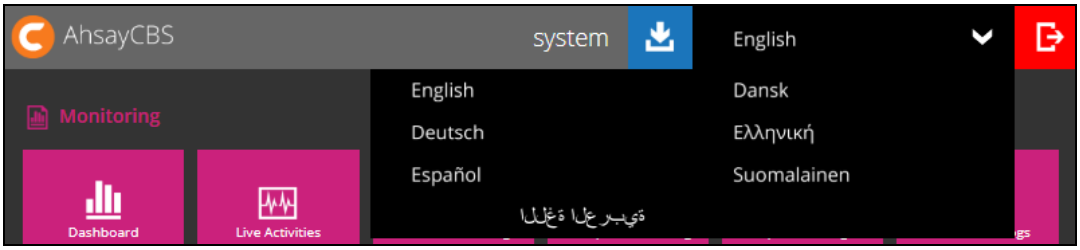
2. Click the checkbox beside your preferred language and click  at the bottom right corner to continue.



3. Click  at the bottom right corner to save the settings.



4. The languages you saved will now be included in the choice for languages.



6.6 Setting up Two-Factor Authentication (2FA)

This feature will give additional security to your account. User can only successfully login after entering the password and the passcode or accepting the notification request that will be sent to the Ahsay Mobile app, which needs to be installed on an Android or iOS mobile device.

Mobile Authentication is the new two-factor authentication feature introduced in AhsayCBS v8.5.0.0. Upon login, aside from providing the username and password of the user account, an additional step is needed to complete the login.

Users have two options once this feature is enabled to complete the login:

- If using Ahsay Mobile, user must either accept the notification request or enter the time-based one-time password code generated in the app.
- If using a third-party TOTP authenticator, user must enter the time-based one-time password code generated in the app. Examples of third-party TOTP authenticator apps are Google Authenticator, Microsoft Authenticator, LastPass Authenticator etc.

Requirements for AhsayCBS:

- AhsayCBS v8.5.0.0 or onwards must be installed.
- To use Two-Factor Authentication with https protocol, a valid SSL certificate from a trusted CA must be installed on AhsayCBS. Otherwise, you will have to use http instead which means all AhsayOBM/AhsayACB users with Two-Factor Authentication enabled will need to connect using http as well.
- The firewall on the AhsayCBS machine must be configured to allow outbound connections to pns.ahsay.com via port 80 or 443. Failure to do so will prevent you from logging in to AhsayCBS, AhsayOBM and AhsayACB using Push Notification feature.

Requirements for Ahsay Mobile:

- A mobile device with the latest version of Ahsay Mobile and/or a TOTP Authenticator such as Google or Microsoft Authenticator installed is available for Two-Factor Authentication.

  NOTE

  Although only one authenticator app is needed for Two-Factor Authentication , several authenticator apps may be used. For example, AhsayOBM/AhsayACB can register and use both Ahsay Mobile and Google Authenticator.

- Ahsay Mobile must be installed on a supported Android or iOS mobile device.
  - For android device, android version must be Android 8 or above.
  - For apple device, iOS version must be 12.0 or above.
- Ensure that Ahsay Mobile is connected to the same local WIFI network as the AhsayOBM/AhsayACB machine. Failure to do so will prevent Ahsay Mobile from performing mobile backup/restore.

- Ahsay Mobile or third-party TOTP authenticator must be registered with AhsayOBM and AhsayACB.
- AhsayOBM and AhsayACB must be connected to the internet.
- The mobile device must have a valid mobile service and be able to receive SMS notifications.
- The mobile device must have a functioning camera for scanning QR code to register 2FA.
- To use push notification for Two-Factor Authentication with Ahsay Mobile, the mobile device must have an internet connection.
- Ensure to allow Notification on Ahsay Mobile for your mobile devices.

Limitations:

- Not supported for AhsayCBS API type accounts.
- For Replication, both sending and receiving are not covered.
- For Redirector, both hosting and joining are not covered.
- 2FA will not work in AhsayOBM and AhsayACB earlier than v8.5.0.0.
- Not supported in AhsayOBR.
- Not supported in AhsayOBM running on Synology and QNAP NAS.
- Not supported in Linux CLI and FreeBSD CLI.

Supported Applications / Modules	
AhsayCBS	✔
➢ Replication (Accepting Data and Sending Data)	✘
➢ Redirection (Joining Redirectors and Hosting a Redirector)	✘
AhsayOBM	✔
AhsayACB	✔
AhsayOBR	✘

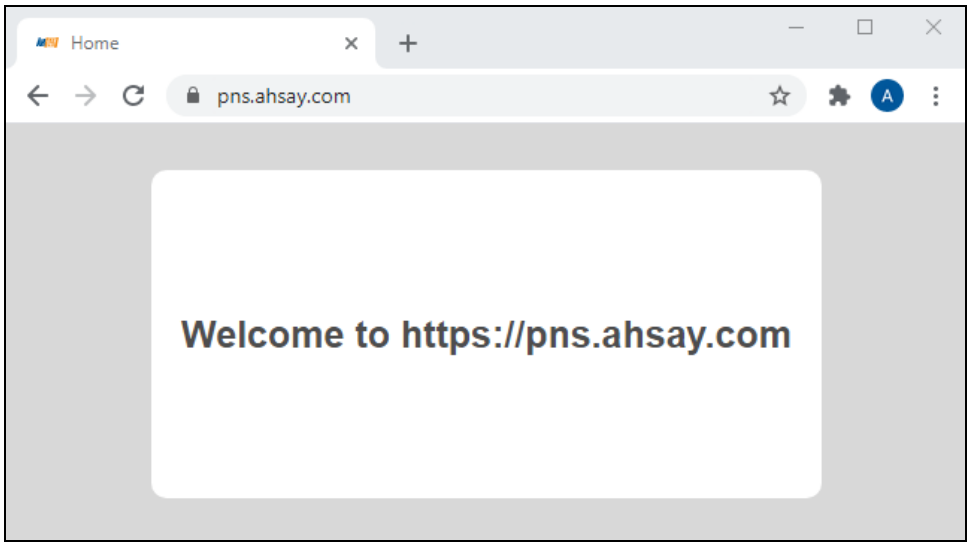
Supported System Users	
Admin	✔
Sub-Admin	✔
Read-only Admin	✔
API	✘

Supported Backup Users	
AhsayOBM/AhsayACB User (Paid)	✅
AhsayOBM/AhsayACB User (Trial)	✅

Supported Operating System	
Windows	✅
Mac	✅
Linux GUI	✅
Linux CLI	❌
FreeBSD CLI	❌
Synology DSM	❌
QNAP QTS	❌

Before setting up your 2FA, ensure that you can receive push notification by checking first if you can connect to pns.ahsay.com.

In Windows, open a web browser and enter https://pns.ahsay.com. You should get this result.



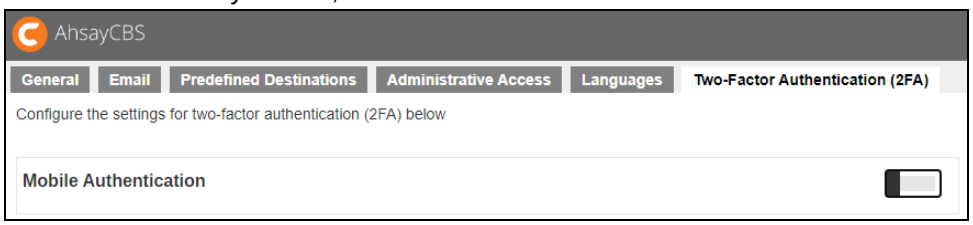
In Linux and FreeBSD, use the telnet command to check if you can connect to pns.ahsay.com. You should get this result.

```
# telnet pns.ahsay.com 443
Trying 52.168.142.119...
Connected to pns.ahsay.com.
Escape character is '^]'.
```

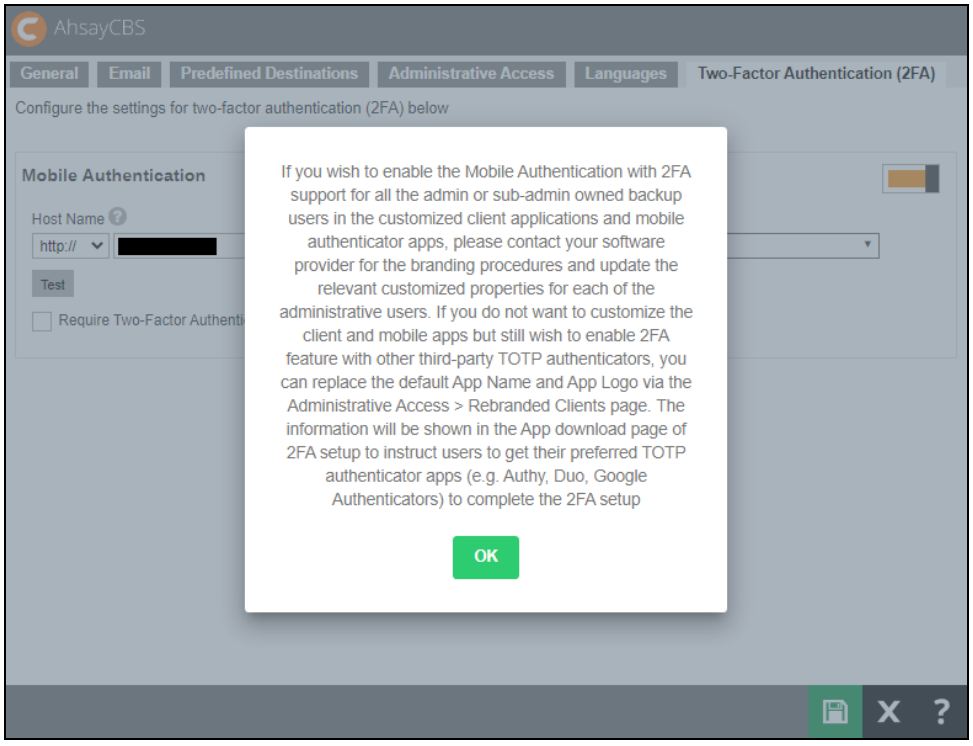
Once done, there are two steps in setting up your 2FA, first you need to set up Mobile Authentication then you need to enable it for the user.

6.6.1 Set up Mobile Authentication:

1. In the Two-Factor Authentication (2FA) tab, make sure to switch on **Mobile Authentication**. By default, this is switched off.



2. Once switched on this pop up message will appear. Click OK to continue.



3. Register AhsayCBS Host Name details for 2FA:

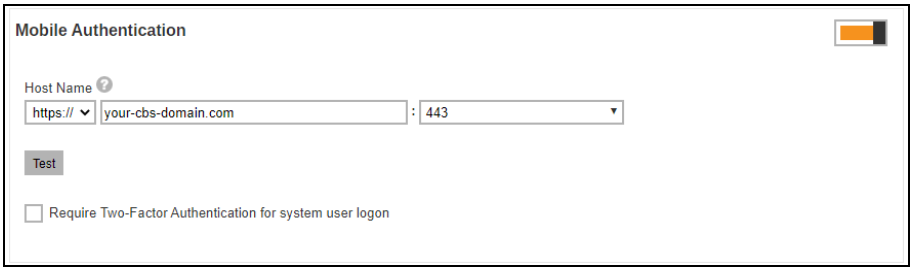
   i. Select the type of protocol, whether http or https.

   ii. Enter the **Host Name or external IP address of your AhsayCBS server**.

> **NOTE**
>
> The host name must be a FQDN (Fully Qualified Domain Name) which consists of the host name and domain name or an external IP address.

   iii. Select the port used by AhsayCBS, for example 80 for http or 443 for https.

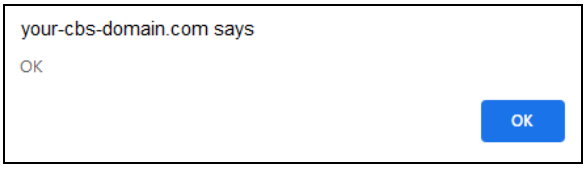
Example: https://your-cbs-domain.com



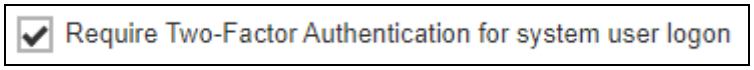
NOTE

To use Two-Factor Authentication with https protocol, a valid SSL certificate from a trusted CA must be installed on AhsayCBS. Otherwise, you will have to use http instead which means all AhsayOBM/AhsayACB users with Two-Factor Authentication enabled will need to connect using http as well.

4. Click on Test to verify. A confirmation message will be displayed once the verification is done.



5. **Optional**: Check the box if it is mandatory for system users to login using two-factor authentication.



6. Click to save.

NOTE

Although the 2FA setting has been setup on the AhsayCBS server, you have to enable 2FA for each AhsayOBM/AhsayACB user account before they can use it. For more information please refer to Chapter 6.6.2 Enable two-factor authentication of users.

6.6.2 Enable two-factor authentication of users:

There are three ways to enable two-factor authentication of AhsayOBM/AhsayACB users:

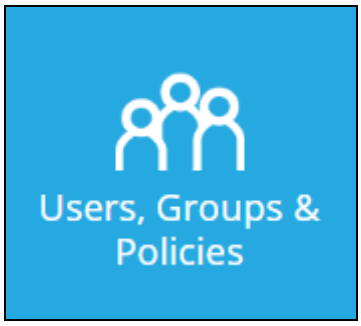
- The two-factor authentication can be enabled for individual AhsayOBM/AhsayACB user account,
- Be enabled for several AhsayOBM/AhsayACB user accounts at once,

  or

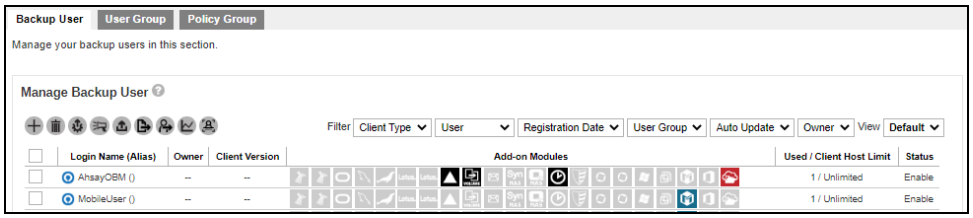
- Be enabled for all AhsayOBM/AhsayACB user accounts.

For individual AhsayOBM/AhsayACB users:

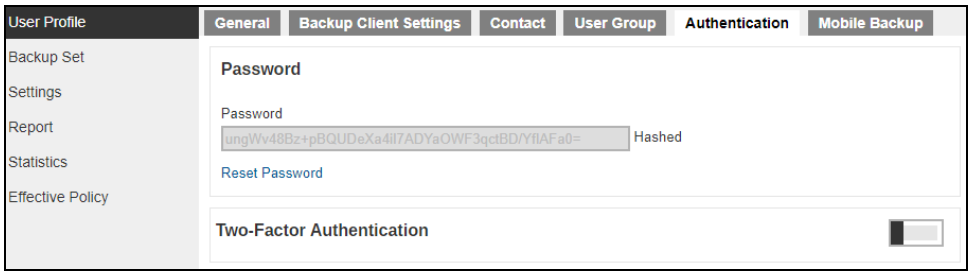
1. Go to **Backup / Restore** > **Users, Groups & Policies**.



2. Select the backup user.



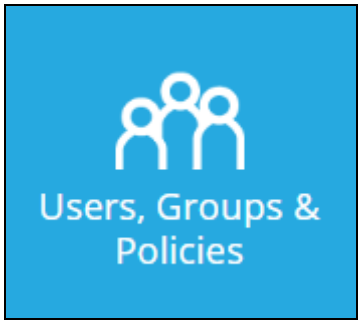
3. Go to the **Authentication** tab and switch on **Two-Factor Authentication**.



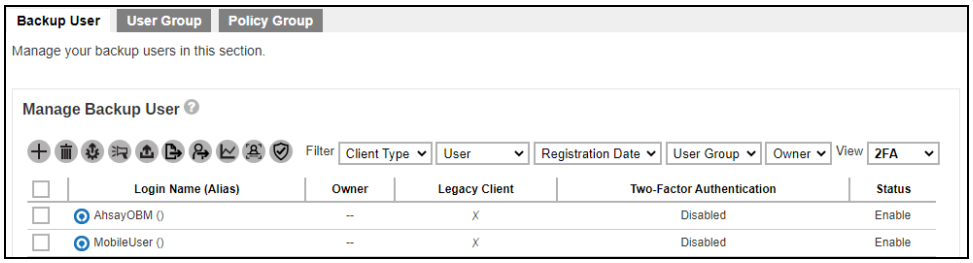
4. Click  to save.

For several AhsayOBM/AhsayACB users at once:

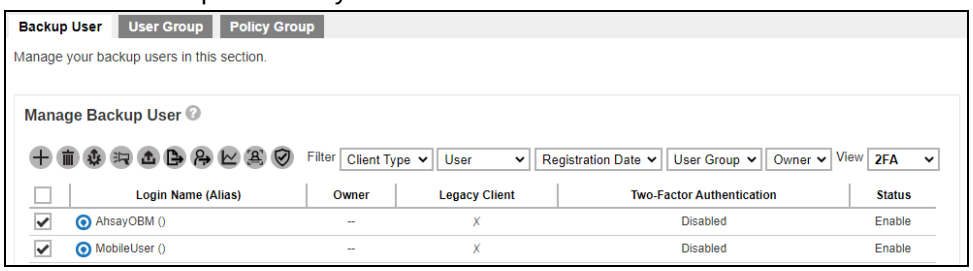
1. Go to **Backup / Restore** > **Users, Groups & Policies**.



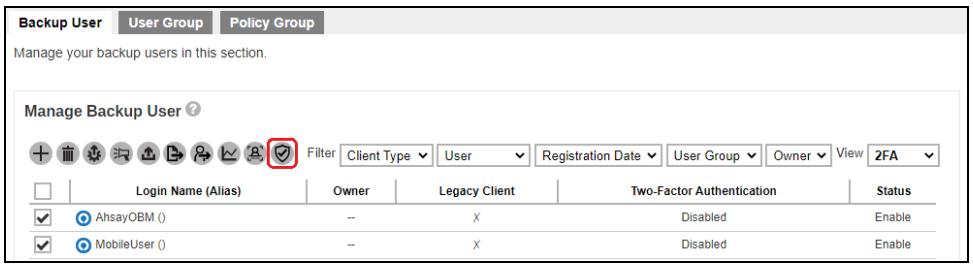
2. Filter the View by selecting **2FA**.



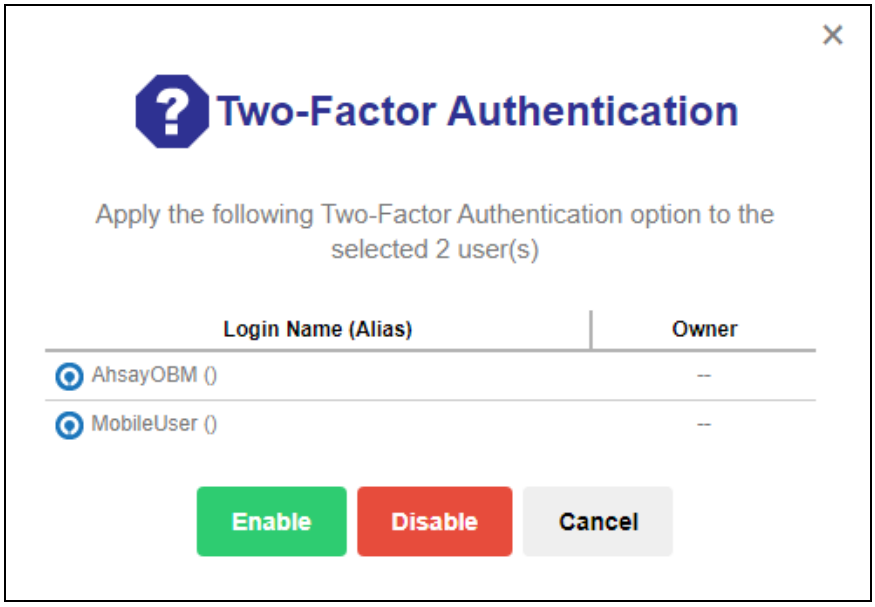
3. Select the backup user that you want to enable/disable the 2FA.



4. Click the **Enable / Disable Two-Factor Authentication** button.

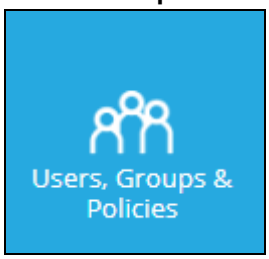


5. Select if you want to enable or disable the 2FA for the selected account.

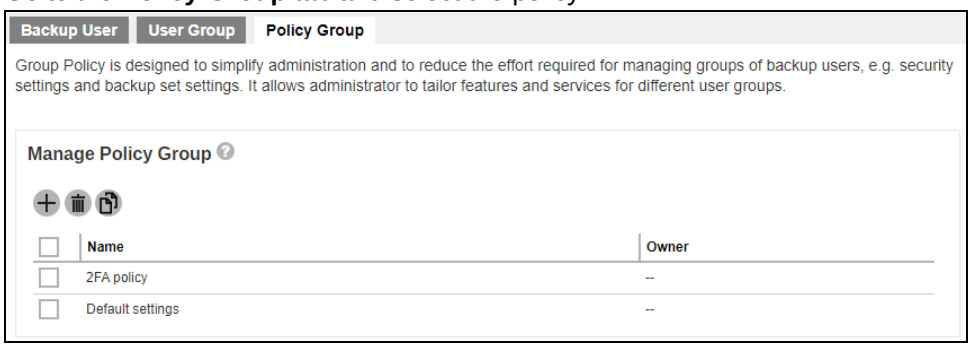


For all AhsayOBM/AhsayACB users:

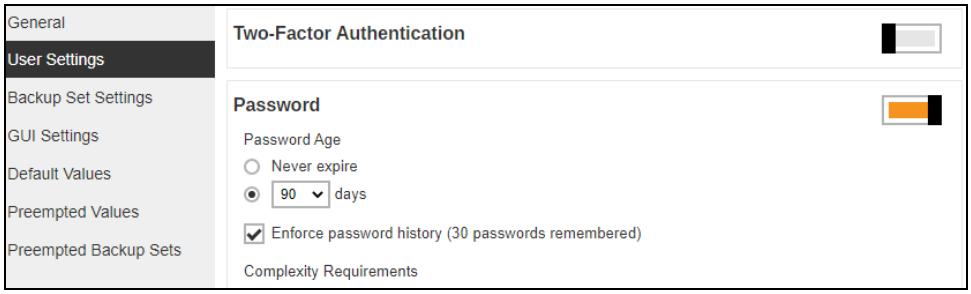
1. Go to **Backup / Restore** > **Users, Groups & Policies**.



2. Go to the **Policy Group** tab and select the policy.



3. Go to **User Settings**, switch on **Two-Factor Authentication**.



4. Enable **Require Two-Factor Authentication for user logon**.

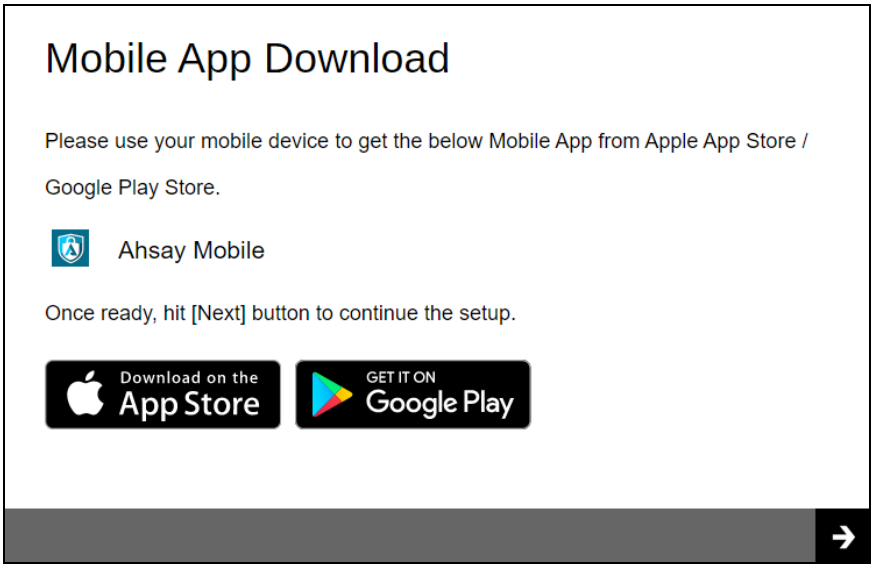
5. Click  to save.

Once enabled, on the next login for all AhsayOBM/AhsayACB v8.5.0.0 or above users which support Mobile Authentication 2FA or AhsayCBS web console user login, users will be required to register a mobile device for the new Mobile Authentication 2FA. Otherwise, they will not be allowed to proceed with the login.

Here are examples of the next login in AhsayCBS web console once two-factor authentication has been enabled.

Depending on the App Download Page Settings, the screen that will be displayed may be either of the two:

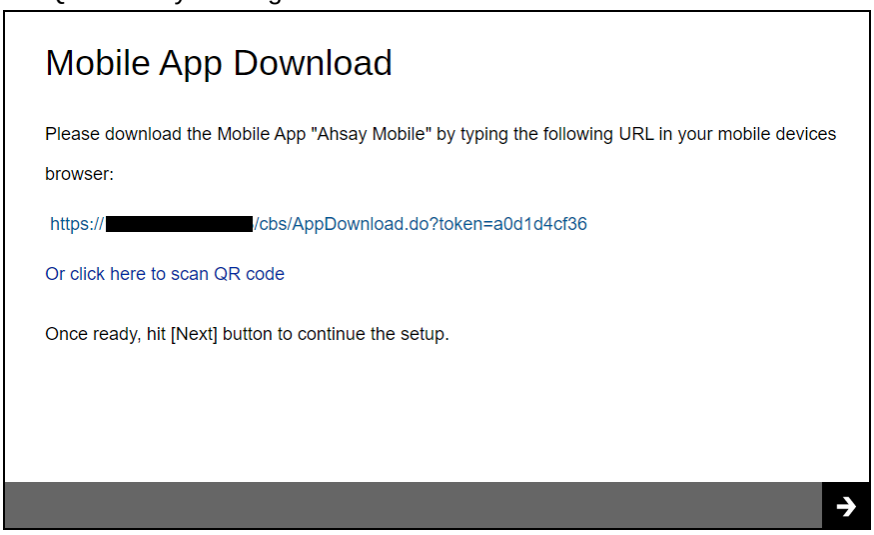
This is the default screen which has instructions to download Ahsay Mobile from the Apple App Store / Google Play Store.



Of

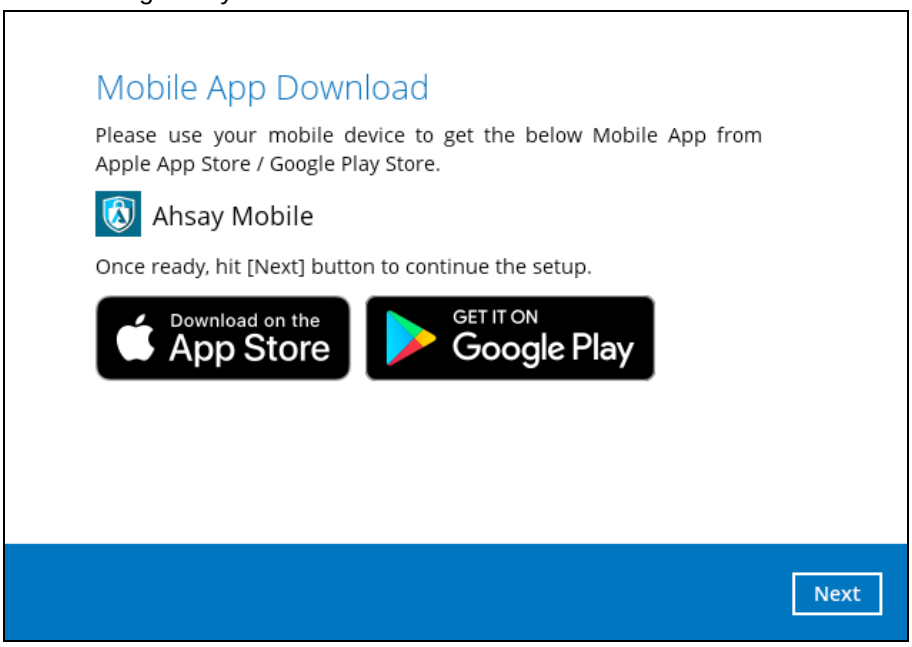
For branded application, this will be the screen, which has instructions to download the mobile app by entering the URL provided in your device's browser or you can also scan

the QR code by clicking Or click here to scan QR code link.



While these are the examples for AhsayOBM/AhsayACB.

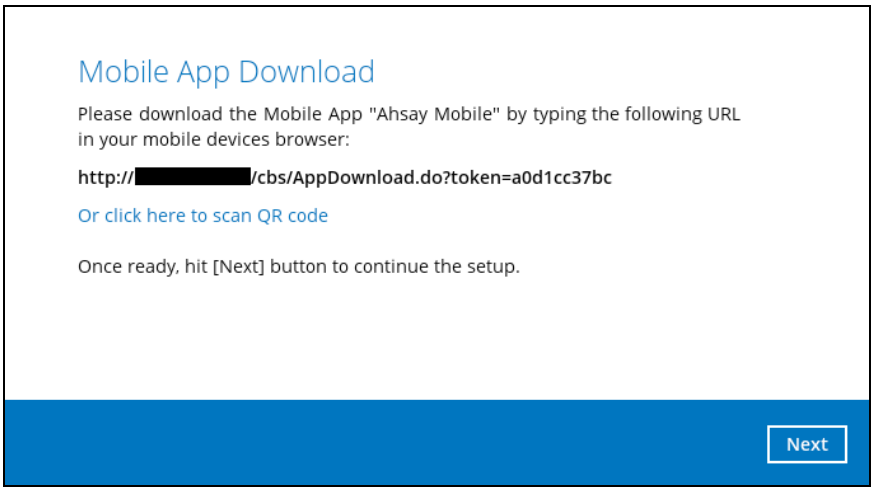
The default screen which has instructions to download Ahsay Mobile from the Apple App Store / Google Play Store.



Or

The branded application screen, which has instructions to download the mobile app by entering the URL provided in your device's browser or you can also scan the QR code by

clicking Or click here to scan QR code link.

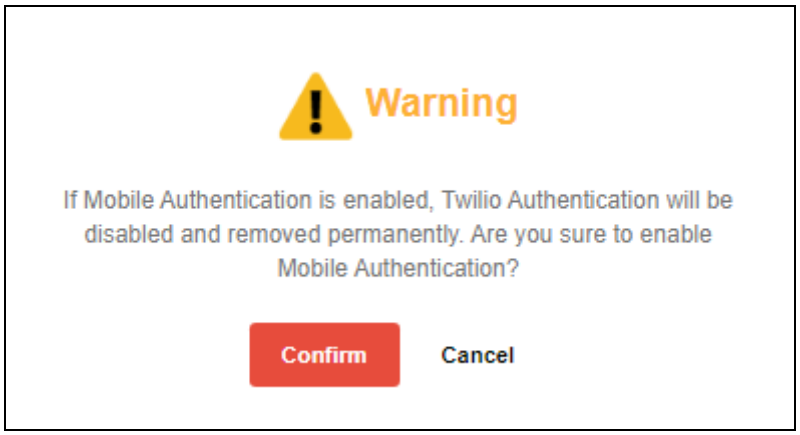


6.6.3 Migrate Users from Twilio to Mobile Authentication:

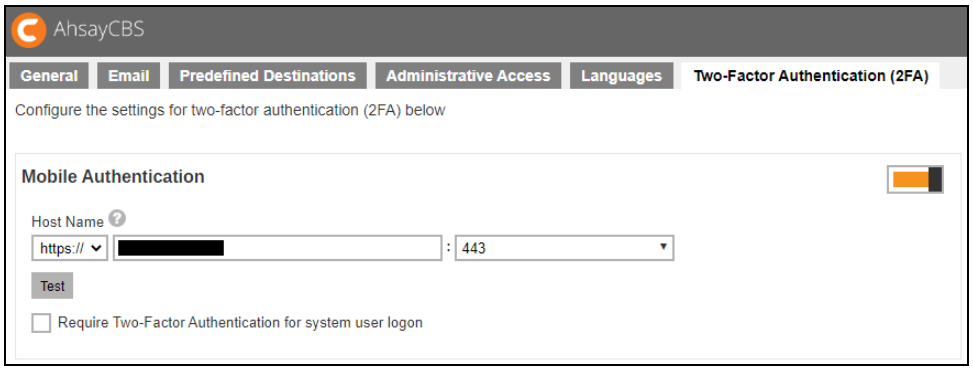
For users with Twilio Credentials Verification set up prior to upgrading to AhsayCBS v8.5.0.0 or above, since only one two-factor authentication may be used, if you have decided to use Mobile Authentication instead of Twilio please follow the instructions below on how to migrate your users from Twilio to Mobile Authentication.

1. Switch on **Mobile Authentication**.

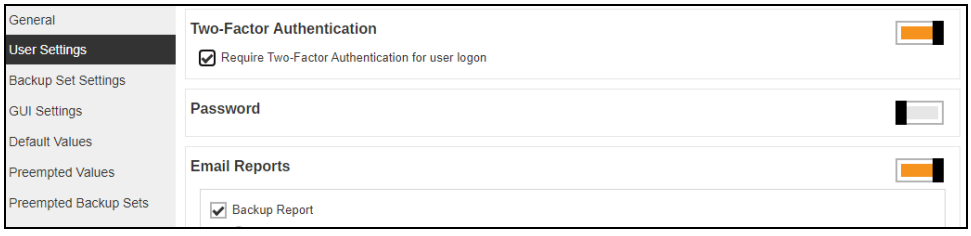
2. Click **Confirm**.



3. Twilio Credentials Verification is now deleted. Set up mobile authentication and click  to save.

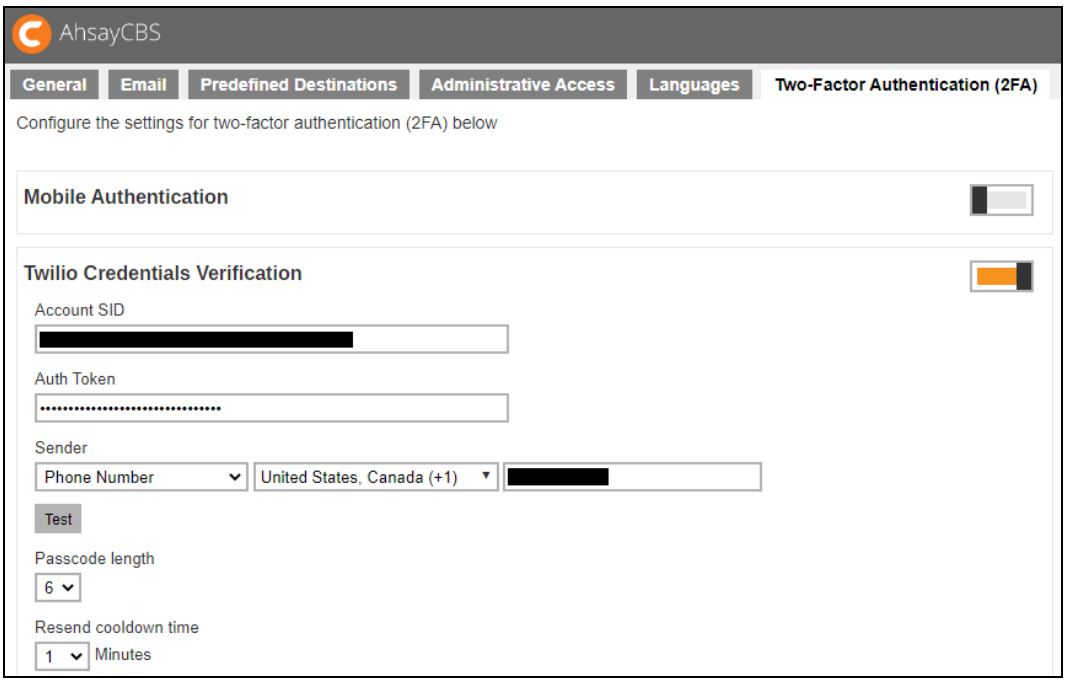


4. Enable for your users by enabling the **Require Two-Factor Authentication for user logon** setting.



6.6.4 Modify Twilio Credentials Verification:

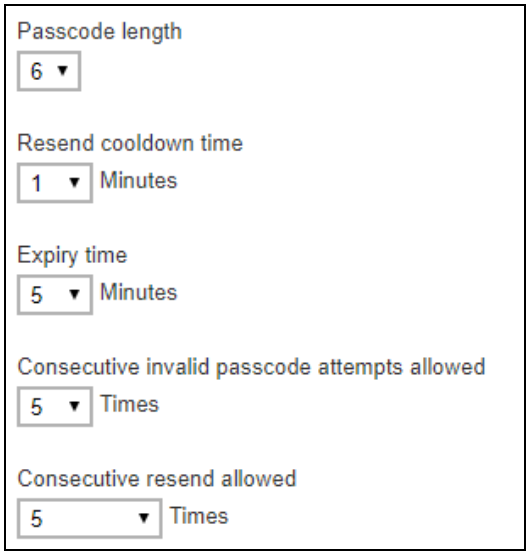
Users on AhsayCBS v8.3.0.30 until v8.3.6.x using Twilio Credentials Verification may continue using it for your two-factor authentication since it will be automatically migrated after upgrading to AhsayCBS v8.5.0.0 or above. However, if it has not been setup in the previous AhsayCBS version, setup of Twilio Credentials Verification is desupported in AhsayCBS v8.5.0.0 or above. Only modification of existing Twilio Credentials Verification setting is allowed.



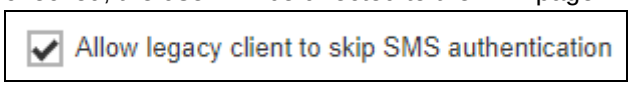
1. Update the **Account SID**, **Auth Token** and **Sender** details, if needed.

2. Click on Test to verify.

3. Update the following: **Passcode length**, **Resend cooldown time**, **Expiry time**, **Consecutive invalid passcode attempts allowed** and **Consecutive resend allowed**, if needed.



4. Check the box if you will allow legacy clients to skip SMS authentication. Legacy clients are AhsayOBM users who has an old version of AhsayOBM installed who upgraded to the latest version but has not run any backup yet. If this box is not checked, the user will be directed to the 2FA page.



5. Click  to save.

NOTE

Also do not forget to check the **Allow legacy client to skip SMS authentication** box if you are using an older version of AhsayOBM v8.3.0.30 or else your users will not be able to login and your scheduled and continuous backups will not run. All functions requiring access and authentication to AhsayCBS will not work. Like starting a manual backup from the System Tray in AhsayOBM/AhsayACB in Windows. Running AhsayOBM/AhsayACB batch files in Windows. Running AhsayOBM scripts in Linux/FreeBSD. Running AhsayOBM/AhsayACB scripts in MacOS. AhsayCBS server initiated backups on AhsayOBM/AhsayACB. And Auto Upgrade (AUA) on AhsayOBM/AhsayACB. For more details please refer to the AhsayOBM Quick Start Guide for Windows and AhsayOBM Quick Start Guide for Linux (CLI).

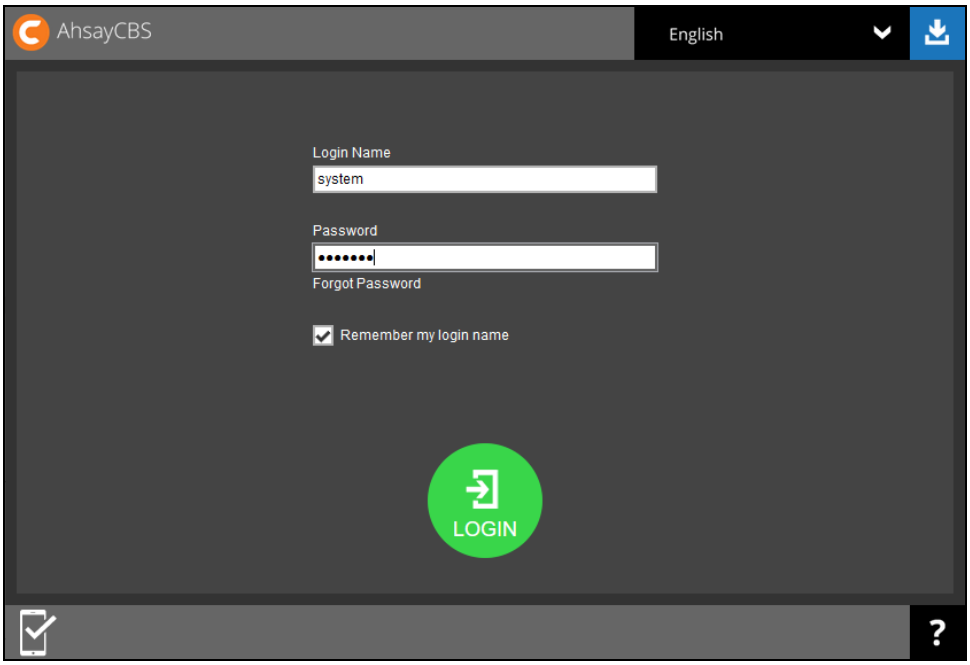
6.6.5 Log in to AhsayCBS Web Console with Two-Factor Authentication (2FA) enabled:

Here are the two scenarios upon logging in to AhsayCBS with 2FA enabled:

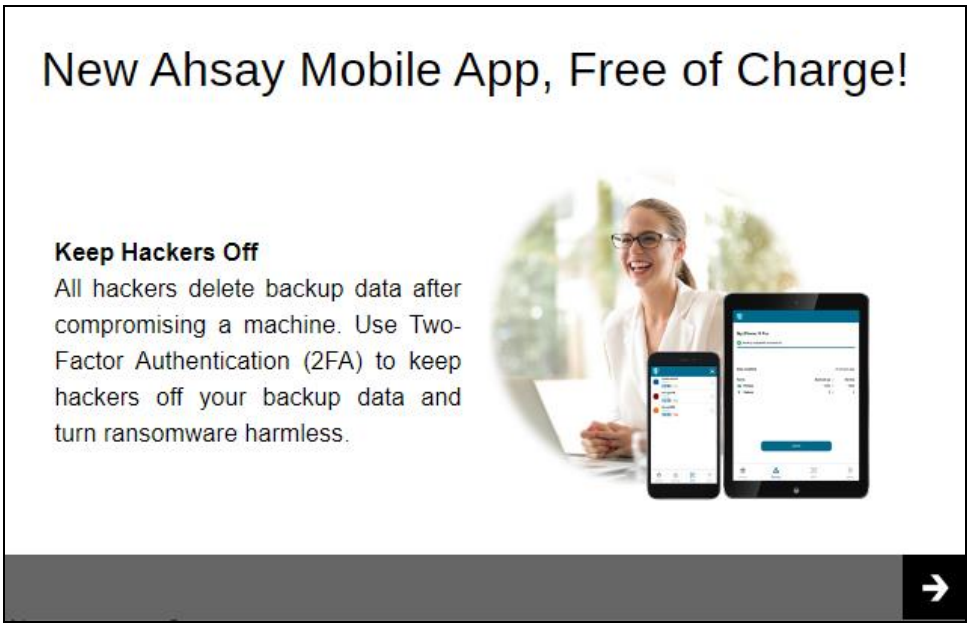
- Initial log in – user will log in to AhsayCBS for the first time.
- Subsequent log in – user has already set up 2FA.

Initial log in with 2FA enabled:

1. Enter the **Login Name** and **Password** and click **LOGIN.**

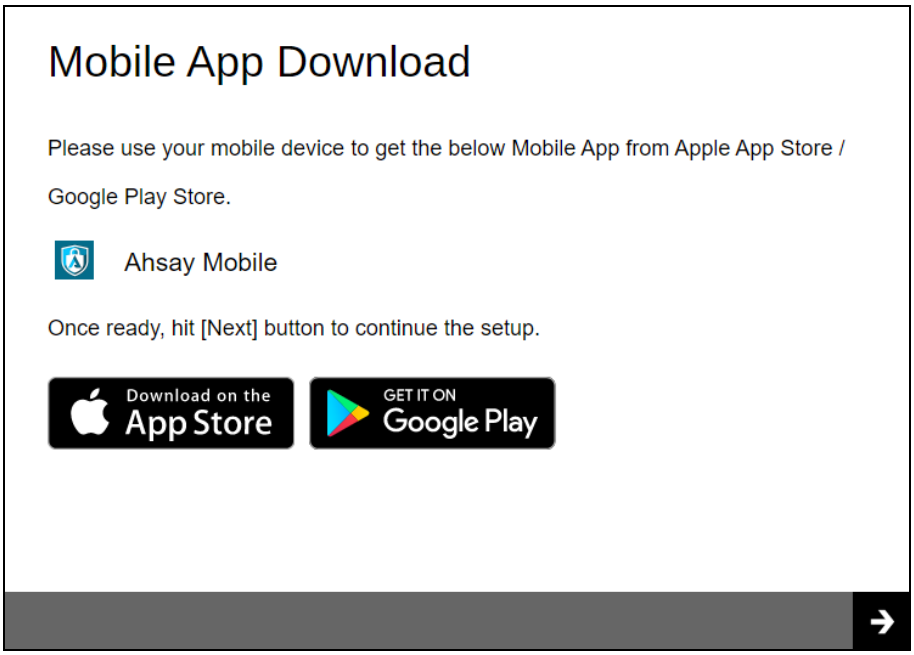


2. Click → to proceed with setting up 2FA.

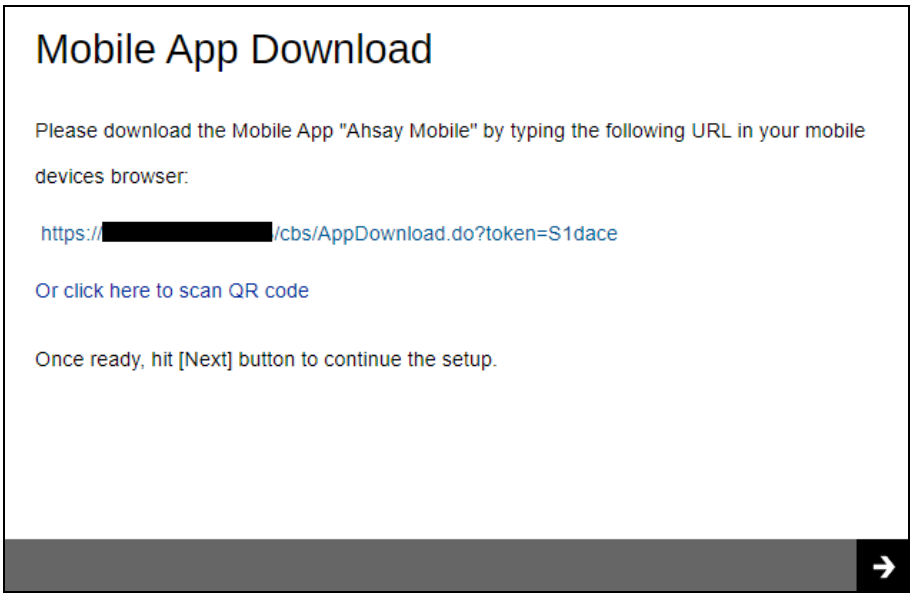


3. The screen displayed next will depend on the App Download Page Settings. Either of the two screens below will be displayed:

   - This is the default screen that will be displayed, with instructions to download the Ahsay Mobile from the Apple App Store / Google Play Store.

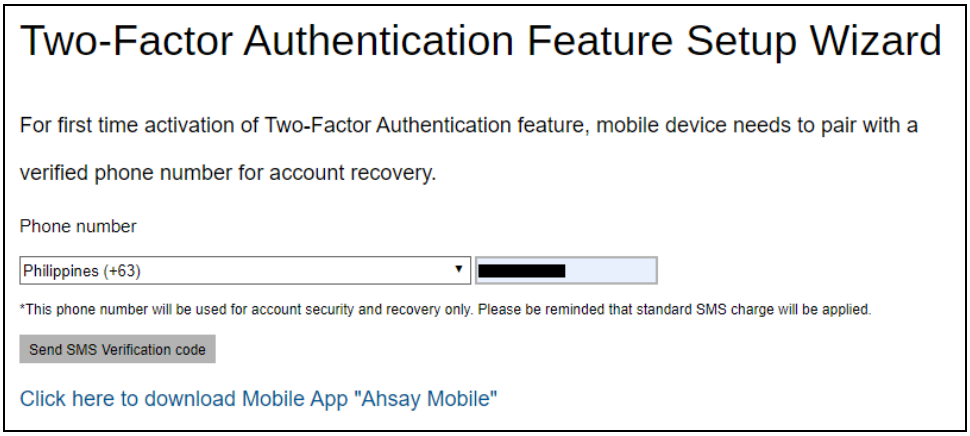


   - While this is the screen that will be displayed for branded application, with instructions to download the mobile app by entering the URL provided in your device's browser or you can also scan the QR code by clicking Or click here to scan QR code link.

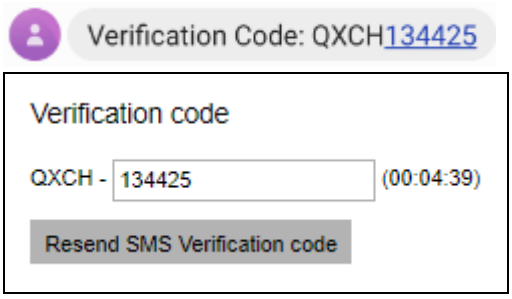


Click → to proceed.

4. Select the country code and enter your phone number. Click Send SMS Verification code.

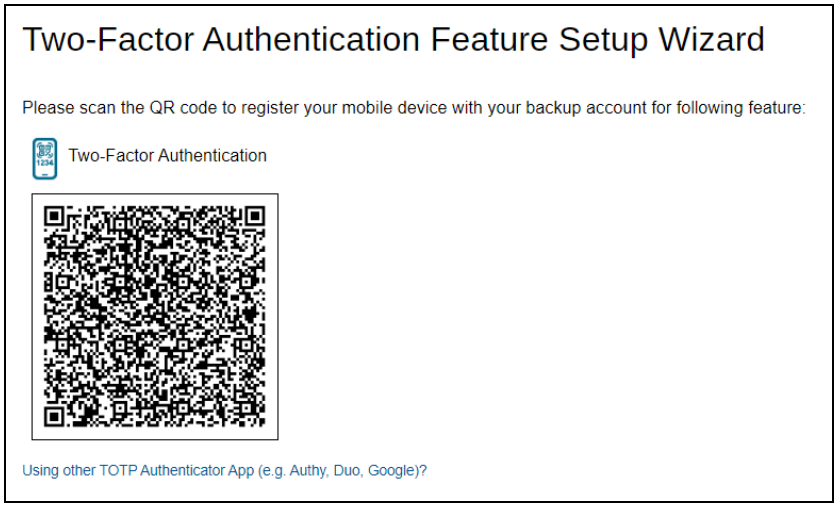


5. Enter the verification code and click →.



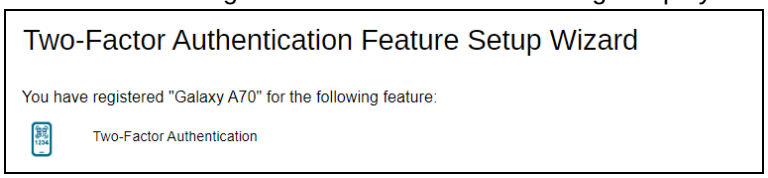
6. Pair the device with the user account. There are two ways to do this:
   - Using Ahsay Mobile
   - Using third-party TOTP Authenticator App
     - Ahsay Mobile can be configured to support two 2FA modes:
       - Push Notification and TOTP (default mode)
       - TOTP only

For Push Notification and TOTP, scan the QR code.

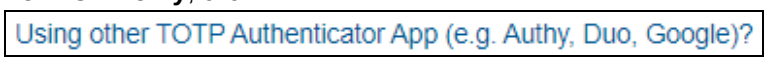


This is a sample of the Ahsay Mobile app installed on a mobile device named “Galaxy A70”.

After successful registration this will be the message displayed.



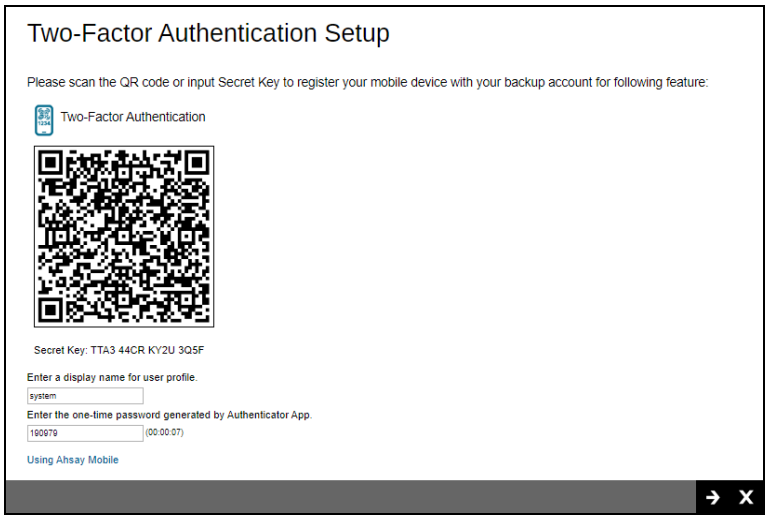
For TOTP only, click



link.

Scan the QR code. After doing so, the one-time password will be generated in the Ahsay Mobile. Enter a name and the one-time password code generated in Ahsay Mobile here and click  .

This is a sample of the one-time password code generated in Ahsay Mobile.



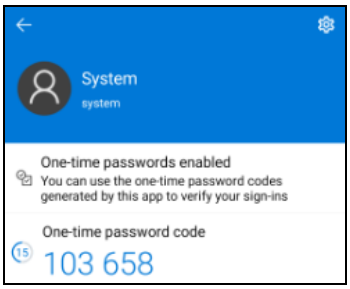
After successful registration, this will be the message displayed.

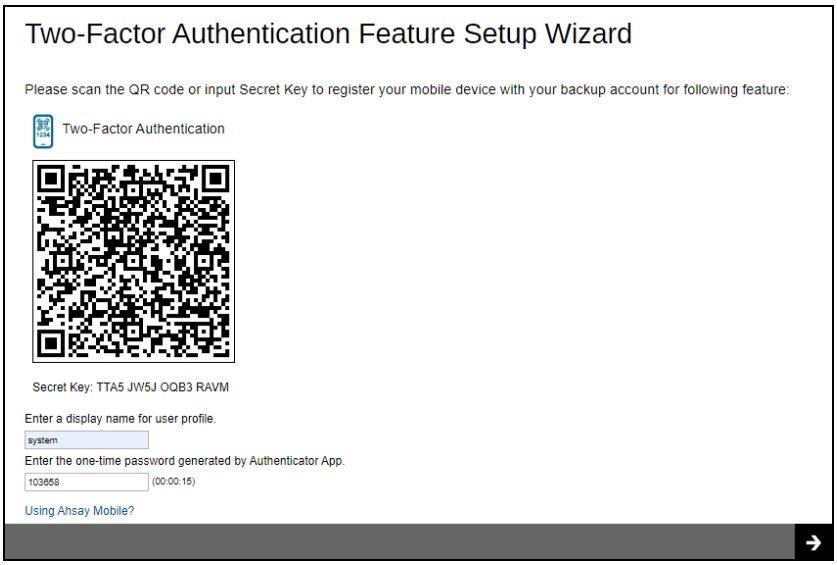
Or

- By using a third-party TOTP Authenticator App, click Using other TOTP Authenticator App (e.g. Authy, Duo, Google)? link.

  Either scan the QR code using the third-party authenticator app or enter the Secret Key in the third-party authenticator app. After doing so, the one-time password will be generated in the authenticator app. Enter a name and the one-time password code generated in the third-party authenticator app here and click →.

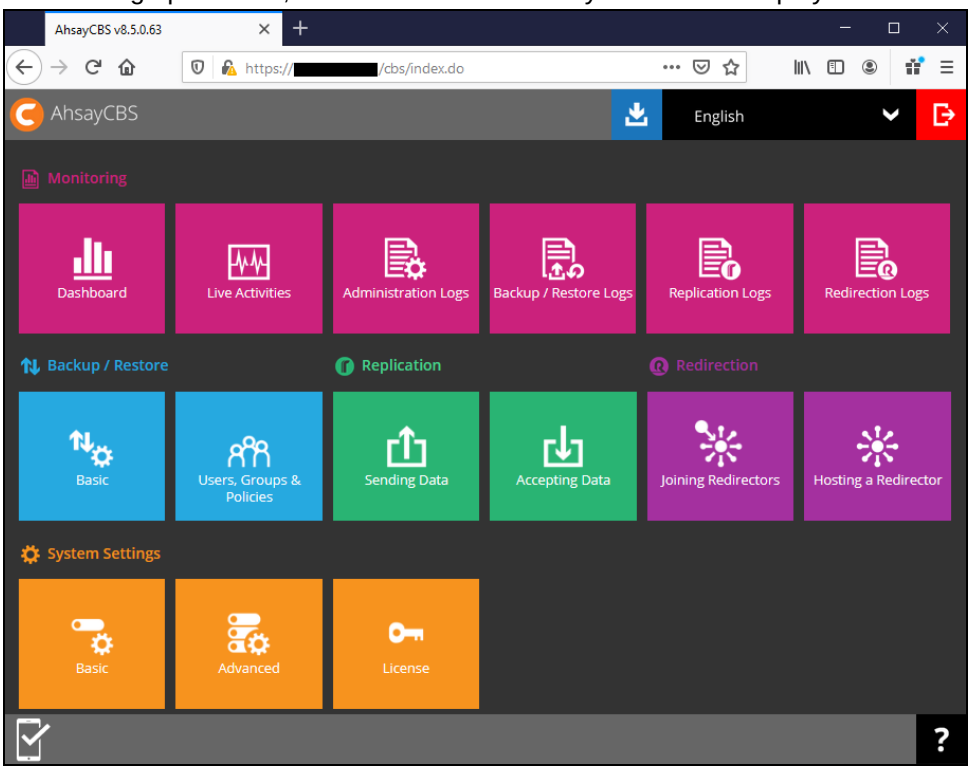
  This is a sample of the one-time password code generated using Microsoft Authenticator.





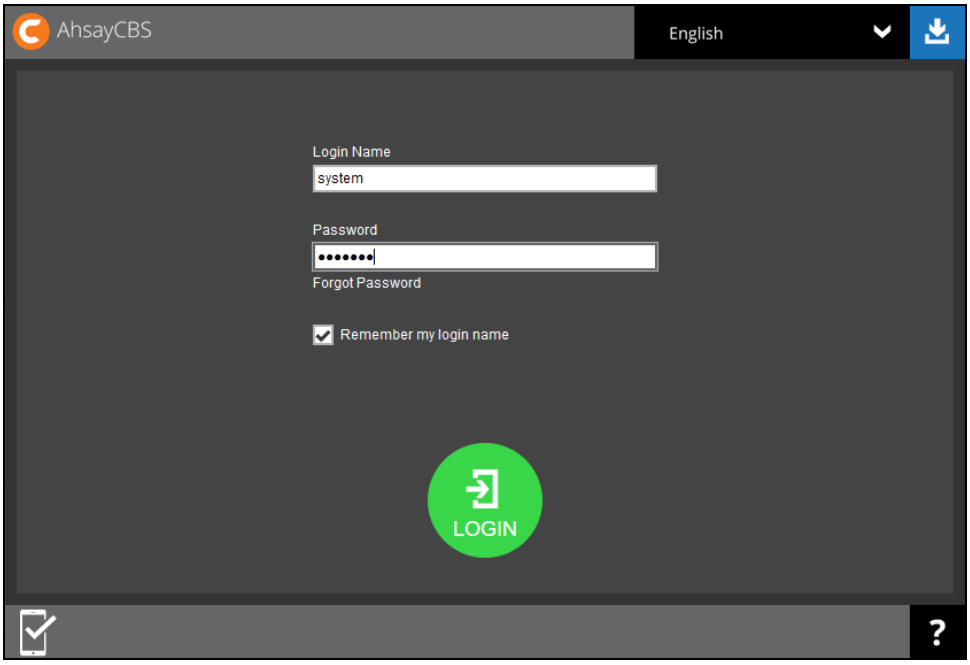
7. Click ☑ to finish setup.

8. After setting up the 2FA, the main screen of AhsayCBS will be displayed.



Subsequent log in with 2FA enabled:

1. Enter the **Login Name** and **Password** and click **LOGIN**.



2. Select the authentication method to continue with the login.

   There are two authentication method to choose from it is possible to use both methods on the same AhsayOBM/AhsayACB user account:

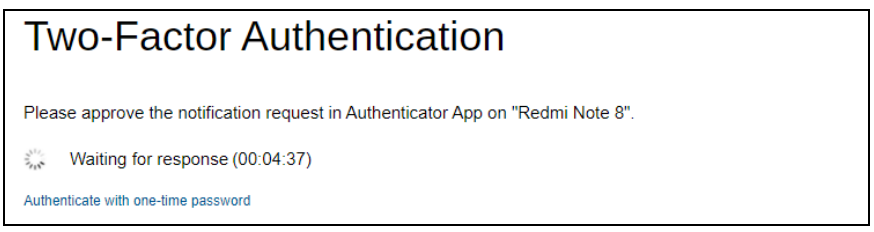
   - Ahsay Mobile app
     - Supports two types of authentication:
       - Push Notification
       - TOTP
     - Can be configured to support two 2FA modes:
       - Push Notification and TOTP (default mode) or,
       - TOTP only
   - Third-party TOTP Authenticator App

     (e.g. Authy, Duo, Google)

If **Ahsay Mobile app** will be used as authenticator, there are two 2FA modes that can be selected:

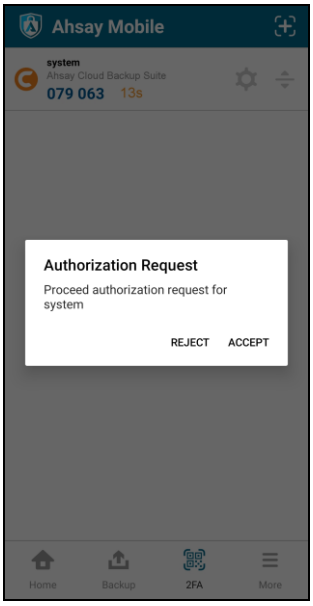
- **Push Notification and TOTP (default mode)**

  Example of the 2FA alert screen on AhsayCBS after login with correct username and password.

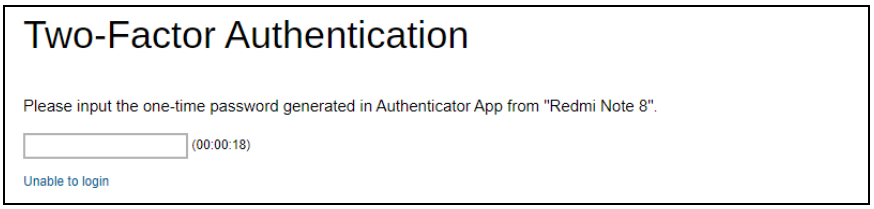


Push notification is the default 2FA mode. Accept the login request on Ahsay Mobile to complete the login.

Example of the login request sent to the Ahsay Mobile app.

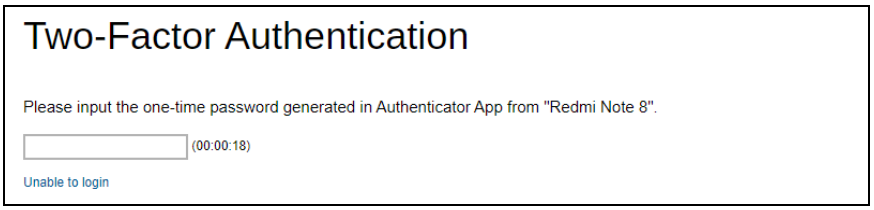


However, if push notification is not working or you prefer to use one-time password, click the “Authenticate with one-time password” link, then input the one-time password generated from Ahsay Mobile to complete the login.

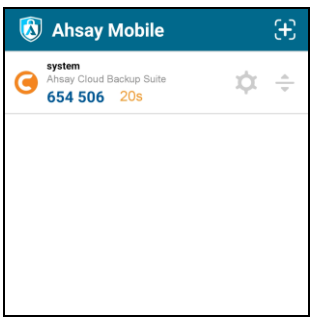


- **TOTP only**

Example of the 2FA alert screen on AhsayCBS after login with correct username and password.

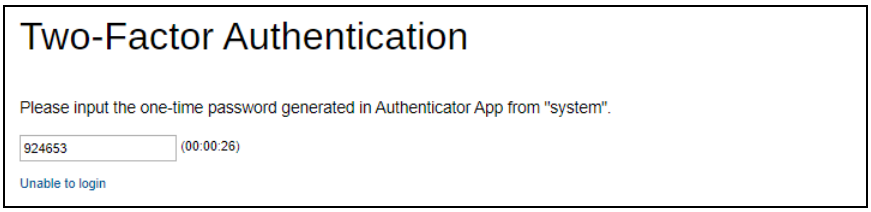


Example of the one-time password generated from Ahsay Mobile to complete the login.

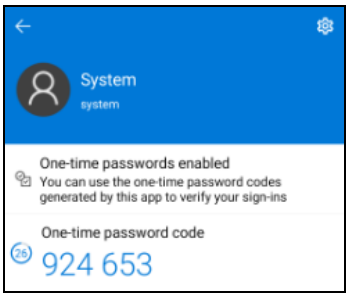


If a third-party **TOTP Authenticator App** will be used instead, follow the steps below to login.

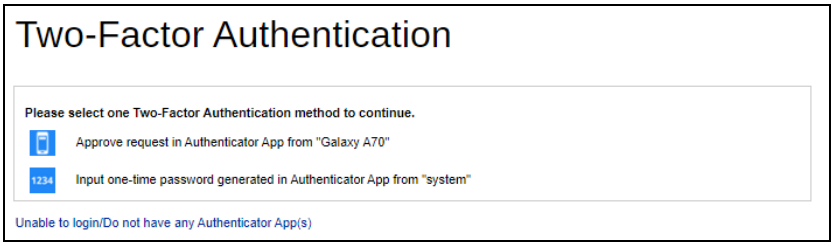
i. Enter the one-time password that is generated by the authenticator app and click **Next**.



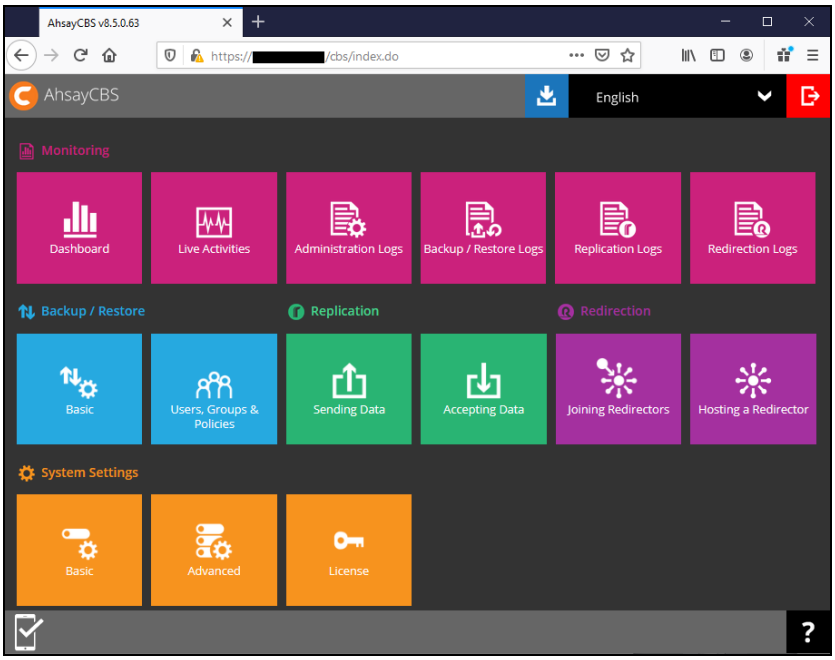
ii. Example of the one-time password generated in the third-party Authenticator App Microsoft Authenticator.



In the following example, both Ahsay Mobile and a third-party TOTP Authenticator App has been setup for 2FA, select your preferred 2FA method from the options available to complete the login.



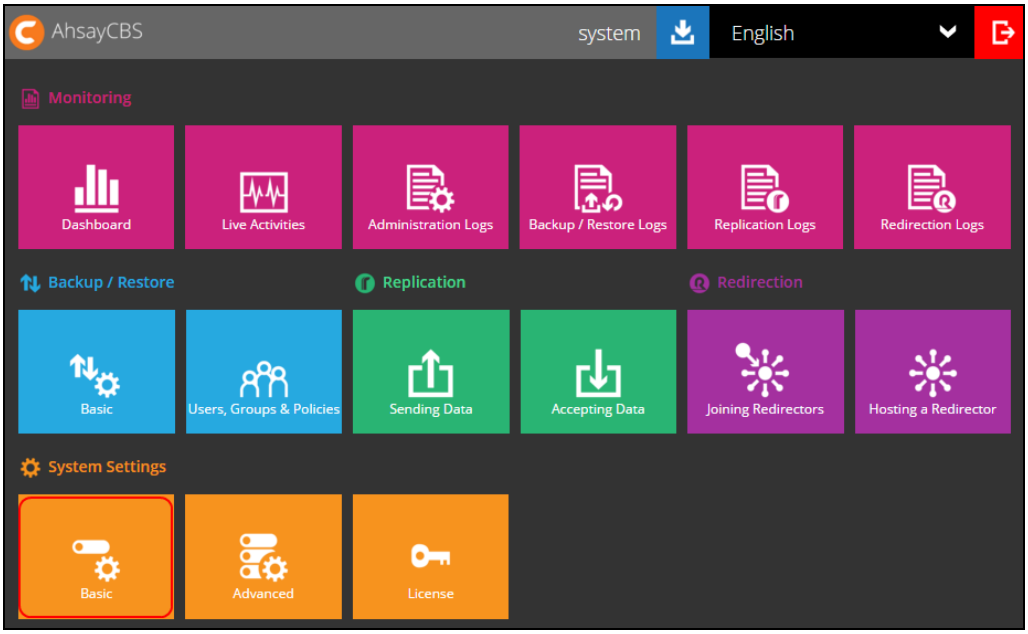
3. After successful login, the following screen will appear.



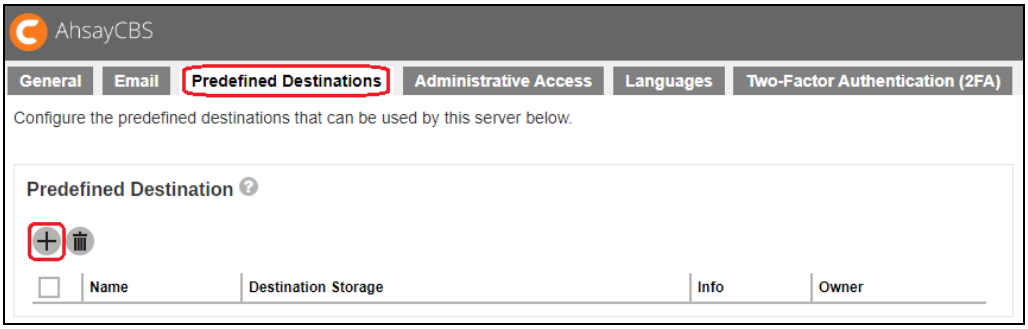
6.7 Setting up Predefined Destination

Setup the predefined destination, which allows your customers backup data to be saved onto centralized cloud storage, i.e. Amazon S3, Microsoft Azure, OneDrive for Business, Dropbox, Google Cloud Storage, Backblaze, Wasabi etc.

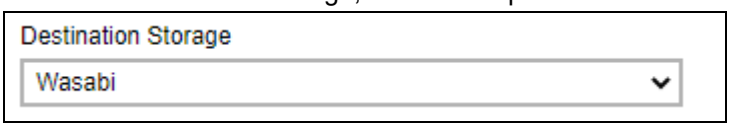
1. Click the orange **Basic** icon under **System Settings** section on AhsayCBS main page.



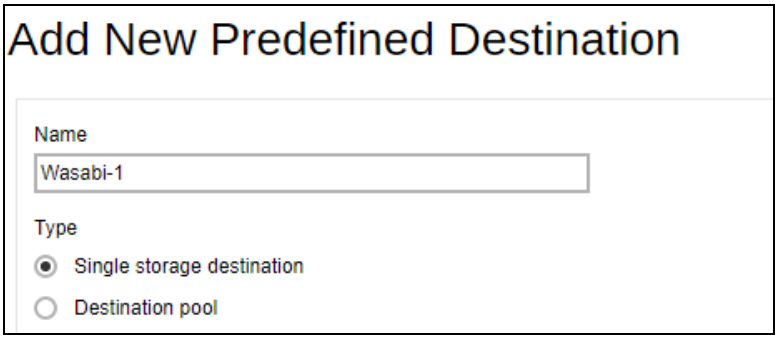
2. In the **Predefined Destinations** tab, click  .



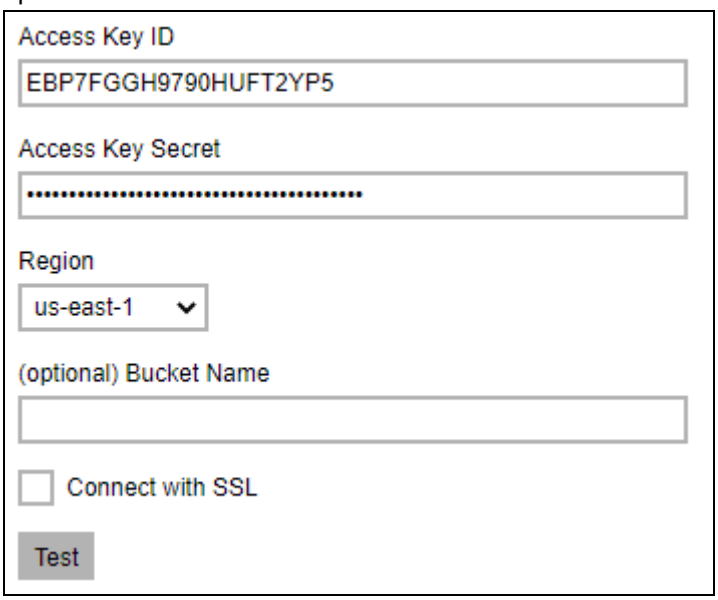
3. Select the destination storage, in our example we will use 'Wasabi'.



4. Enter the destination name and select the type which is 'Single storage destination'.



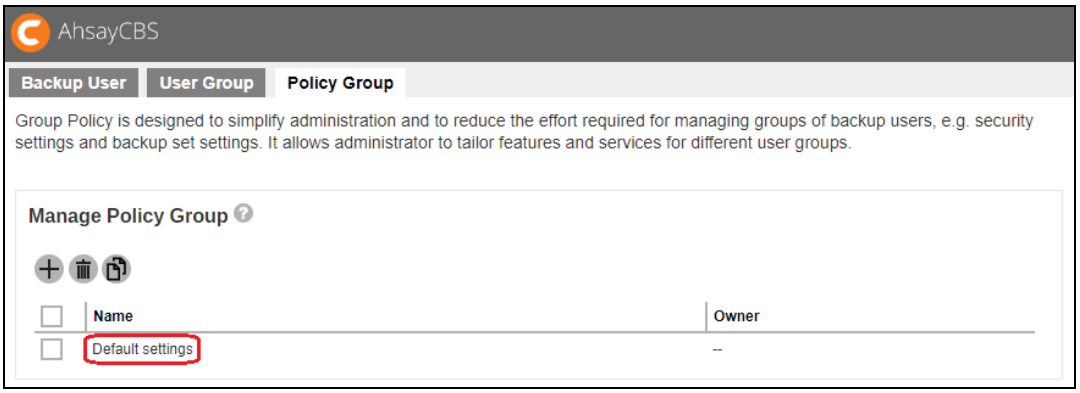
5. Enter the Access Key ID, Access Key Secret. Select the region and it is optional to enter the bucket name. Check the "Connect with SSL" checkbox if needed. It is also optional to click the Test button to check the connection.



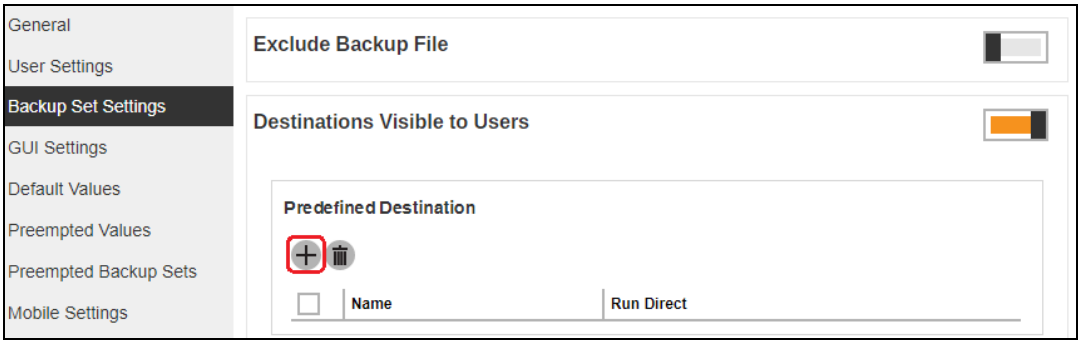
6. Click + at the bottom right corner to add the predefined destination.

7. Click the save icon at the bottom right corner to save the settings.

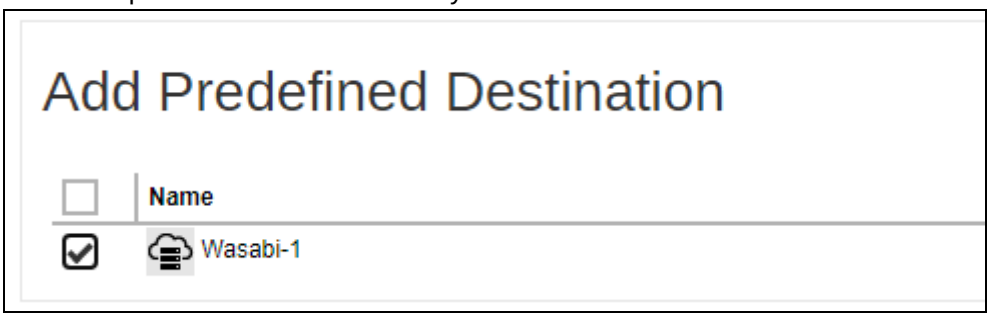
8. After saving the predefined destination, you must make it visible for the users. Go to **Backup/Restore > Users, Groups & Policies > Policy Group > Manage Policy Group**. Click on the 'Default settings'.



9. Go to **Backup Set Settings > Destinations Visible to Users > Predefined Destination** and click  .

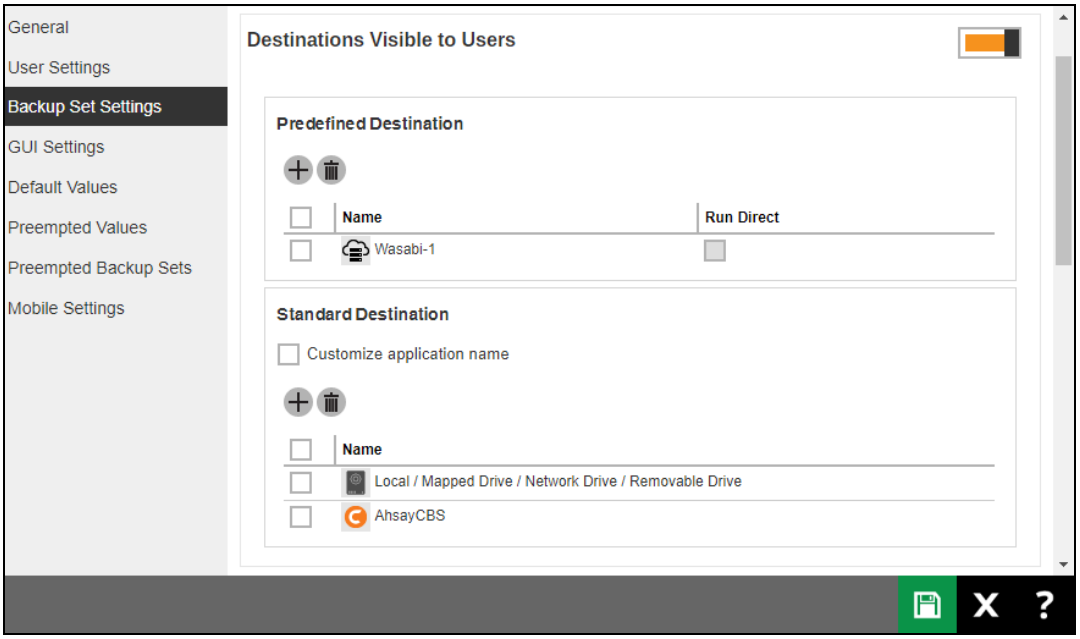


10. Select the predefined destination that you saved.



11. Click  at the bottom right corner to add the predefined destination.

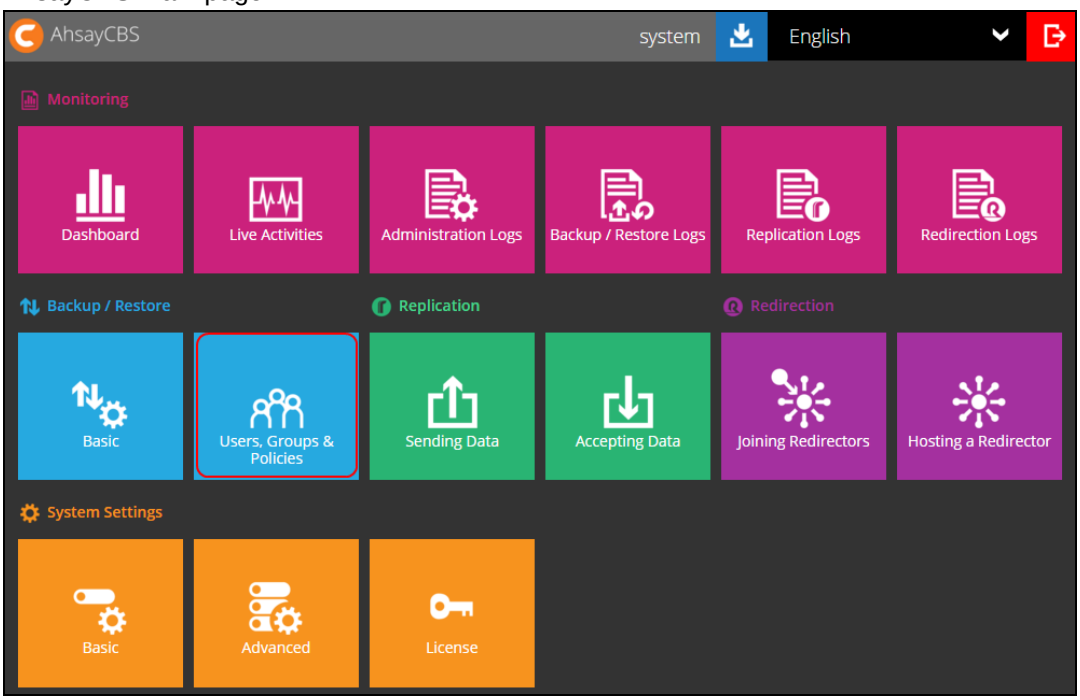
12. Click  at the bottom right corner to save the settings. The predefined destination you created will now be visible to the users.



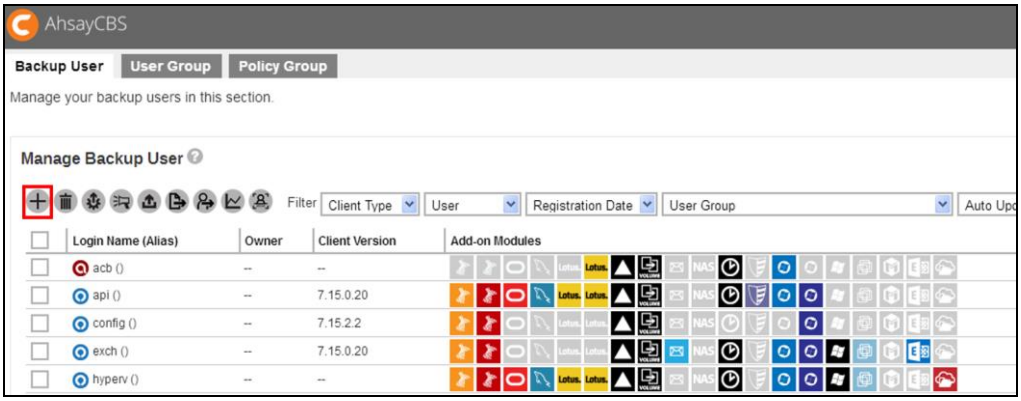
6.8 Creating User Account

Create a user account for the backup machine.

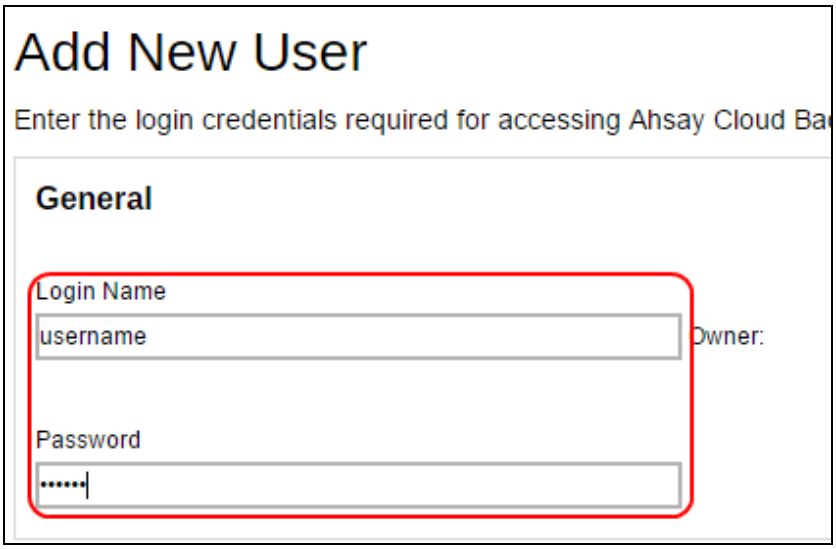
1. Click the **Users, Groups & Policies** icon under the **Backup / Restore** section on the AhsayCBS main page.



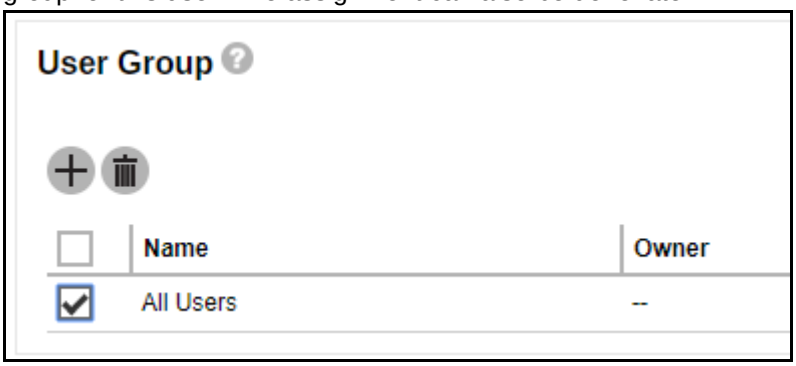
2. Click  to create a new user account.



3. Enter the Login Name and Password in the relevant fields. The password should be at least 6 alphanumeric characters.



Optional: Click the check box in front of the user group if you need to assign a user group for this user. The assignment can also be done later.

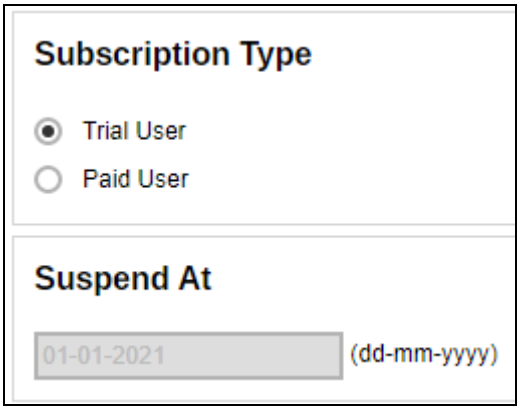


4. Click  at the bottom right corner to continue.

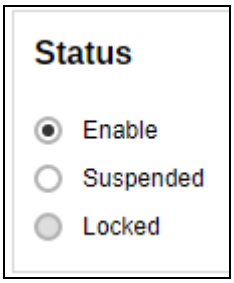
5. If you need to assign a dedicated storage location for the backup account, select Manually assigned and choose the storage location under the Home Directory section. If you select Auto assigned, you can skip this step.

Optional: Alias can be left empty if you do not know or do not want to enter the details at this stage.

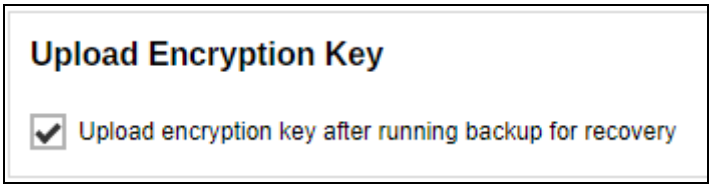
6. Set the desired Subscription Type. Select Paid User if you are creating an account for a user with no expiration period or service will be suspended for this user on the date you specified under the Suspend At drop-down menu. If you select Trial User, service will be suspended after one month.



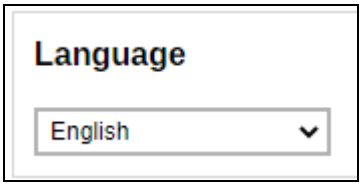
7. Select the status for this user account.



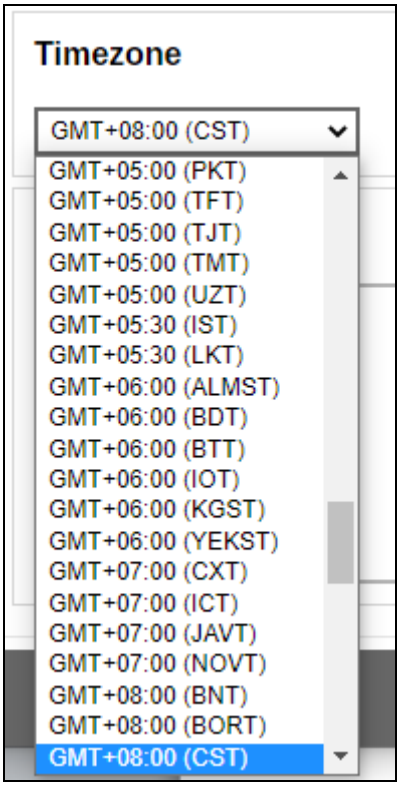
8. By default, the **Upload Encryption Key** option is enabled. This is one of the three settings that requires to be turned on to fulfill the recovery purpose for the encryption key which will be sent to the backup server. This is useful when backup users have lost their key and Ahsay can recover the encryption key for them. For more details, refer to the **Recovering Encryption Key via AhsayCBS Web Console** section in the AhsayCBS v8 Administrator's Guide.



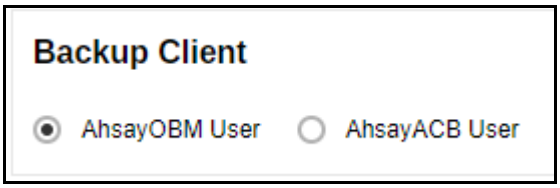
9. Select the language for this user.



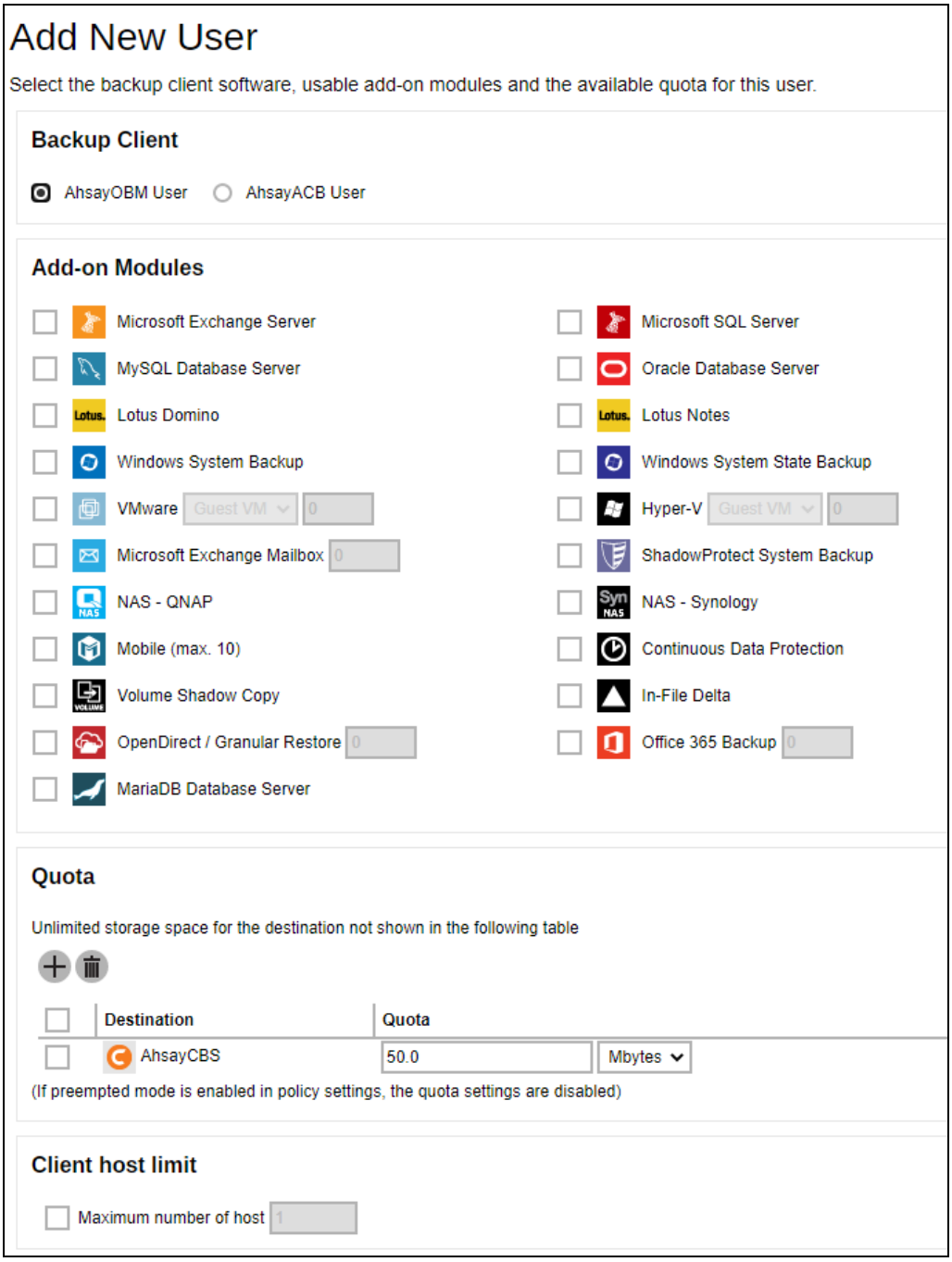
10. Select time zone for this user and then click  at the bottom right corner to continue.



11. Select the backup user type under the Backup Client section. If the backup client machine requires to backup files only, such as a desktop computer or a notebook, then you can simply create an AhsayACB backup account. Otherwise, you will need to set up AhsayOBM, because it comes with backup modules to perform Windows system backup, database backup and virtual machine backup.



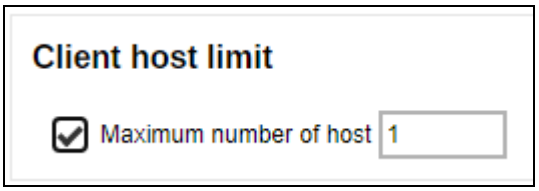
12. Click the checkbox(es) to select the Add-on Modules for this backup user.



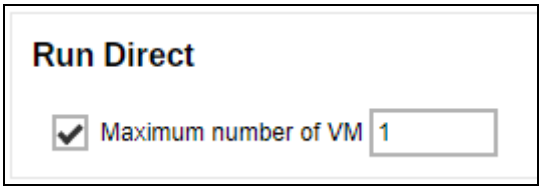
13. You can click  to add backup destination for the backup user account. The destination can be both predefined and standard destination and you can assign backup quota for each destination for the user account.

For details about quota management, please refer to AhsayCBS v8 Administrator's Guide.

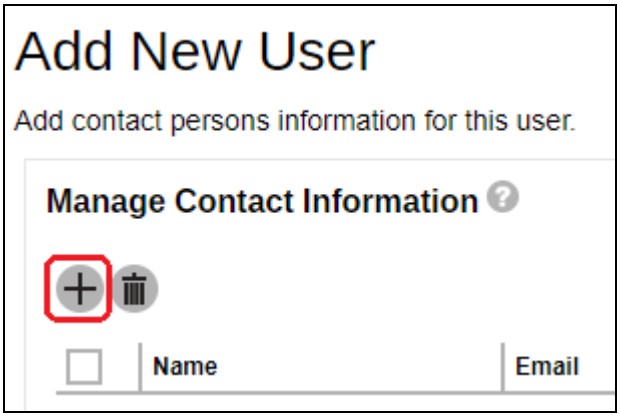
14. By default the Client host limit is non-selected. You can check the checkbox and enter the client host limit value as needed.



15. By default the Run Direct is non-selected. You can check the checkbox and enter the value of maximum number of VM as needed. Click  at the bottom right corner to continue.



16. Click  to add user's contact information.



17. Fill in the contact details and then click  at the bottom right corner to return to the previous Add New User page.

18. Click  at the bottom right corner to save the new user account information.

6.9 Setting up memory for Run on Server (Agentless) Backups

By default, the maximum Java heap size of each Run on Server backup process is set to 2GB. While the minimum Java heap size is set to 128MB. This can be modified by appending the options "`com.ahsay.obs.core.job.ServerRunBackup.Xmx=%value%`" and "`com.ahsay.obs.core.job.ServerRunBackup.Xms=%value%`" in the cbs.opt file.

To configure follow the steps below:

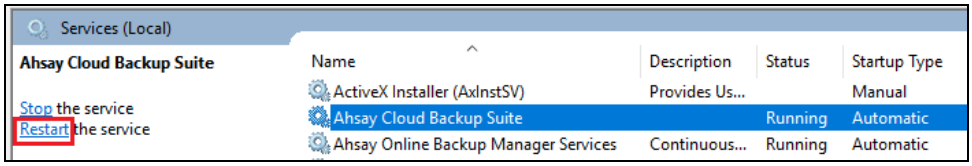
In Windows:

1. Locate the cbs.opt file in the `$APPLICATION_HOME\conf` folder.

2. Open the file, add the options "`com.ahsay.obs.core.job.ServerRunBackup.Xmx=%value%`" and

"com.ahsay.obs.core.job.ServerRunBackup.Xms=%value%" then save.

3. Restart the AhsayCBS service.



In Linux/FreeBSD:

1. Locate the cbs.opt file in the /usr/local/cbs/conf folder.

```
# cd /usr/local/cbs/conf
# ls -la
total 896
drwxr-xr-x.  3 root root   4096 Jul  3 17:45 .
drwxr-xr-x. 22 root root   4096 Jul  3 11:59 ..
-rwxr-xr-x.  1 root root    316 Oct 16  2014 acb-config.xml
-rwxr-xr-x.  1 root root   4961 Jun 28  2017 afc.opt
-rwxr-xr-x.  1 root root     70 May 23  2008 autoDiscovery.xml
-rwxr-xr-x.  1 root root   1152 Jul  3 12:46 autoUpdate.bdb
-rwxr-xr-x.  1 root root   1952 Apr  4  2014 ca.crt
-rwxr-xr-x.  1 root root      0 Feb 23  2015 Catalina
-rwxr-xr-x.  1 root root  12505 May 19  2014 catalina.policy
-rwxr-xr-x.  1 root root  12839 Jun 16 16:03 catalina.properties
-rwxr-xr-x.  1 root root  19366 Jul  3 15:15 cbs.json
-rwxr-xr-x.  1 root root  19371 Jul  3 15:15 cbs.json.1
-rwxr-xr-x.  1 root root  19649 Jul  3 12:27 cbs.json.10
-rwxr-xr-x.  1 root root  19649 Jul  3 12:27 cbs.json.11
-rwxr-xr-x.  1 root root  19371 Jul  3 14:25 cbs.json.2
-rwxr-xr-x.  1 root root  19375 Jul  3 14:25 cbs.json.3
-rwxr-xr-x.  1 root root  19375 Jul  3 14:21 cbs.json.4
-rwxr-xr-x.  1 root root  19374 Jul  3 14:21 cbs.json.5
-rwxr-xr-x.  1 root root  19657 Jul  3 13:58 cbs.json.6
-rwxr-xr-x.  1 root root  19653 Jul  3 13:58 cbs.json.7
-rwxr-xr-x.  1 root root  19653 Jul  3 13:50 cbs.json.8
-rwxr-xr-x.  1 root root  19649 Jul  3 13:50 cbs.json.9
-rwxr-xr-x.  1 root root   9667 Jul  3 14:17 cbs.opt
```

2. Open the file, using a text editor add the options "com.ahsay.obs.core.job.ServerRunBackup.Xmx=%value%" and "com.ahsay.obs.core.job.ServerRunBackup.Xms=%value%" then save.

```
com.ahsay.obs.core.job.ServerRunBackup.Xmx=4096
com.ahsay.obs.core.job.ServerRunBackup.Xms=256
```

3. Restart the AhsayCBS service

```
# cd /usr/local/cbs/bin
# sh restart.sh
```

In AhsayUBS:

1. Locate the cbs.opt file in the `/ubs/mnt/eslsfw/obsr/conf` folder.

```
# cd /ubs/mnt/eslsfw/obsr/conf
# ls -la
 total 925
 drwxr-xr-x   3 root  wheel     142 Jul  9 02:15 .
 drwxr-xr-x  13 root  wheel      13 Jul  8 08:25 ..
 -rwxr-xr-x   1 root  wheel     316 Nov 19  2018 acb-config.xml
 -rwxr-xr-x   1 root  wheel    4966 Jul  8 08:35 afc.opt
 -rwxr-xr-x   1 root  wheel      70 Nov 19  2018
 autoDiscovery.xml
 -rwxr-xr-x   1 root  wheel    1152 Jul  8 08:48 autoUpdate.bdb
 -rwxr-xr-x   1 root  wheel    1952 Nov 19  2018 ca.crt
 -rwxr-xr-x   1 root  wheel       0 Nov 19  2018 Catalina
 -rwxr-xr-x   1 root  wheel   12505 Nov 19  2018 catalina.policy
 -rwxr-xr-x   1 root  wheel    8008 Nov 19  2018
 catalina.properties
 -rwxr-xr-x   1 root  wheel   19671 Jul  8 10:25 cbs.json
 -rwxr-xr-x   1 root  wheel   19672 Jul  8 10:25 cbs.json.1
 -rwxr-xr-x   1 root  wheel   18755 Jul  8 08:43 cbs.json.10
 -rwxr-xr-x   1 root  wheel   19028 Jul  8 08:28 cbs.json.11
 -rwxr-xr-x   1 root  wheel   19672 Jul  8 09:09 cbs.json.2
 -rwxr-xr-x   1 root  wheel   19672 Jul  8 09:09 cbs.json.3
 -rwxr-xr-x   1 root  wheel   19373 Jul  8 08:46 cbs.json.4
 -rwxr-xr-x   1 root  wheel   19169 Jul  8 08:46 cbs.json.5
 -rwxr-xr-x   1 root  wheel   19169 Jul  8 08:44 cbs.json.6
 -rwxr-xr-x   1 root  wheel   19208 Jul  8 08:44 cbs.json.7
 -rwxr-xr-x   1 root  wheel   19208 Jul  8 08:43 cbs.json.8
 -rwxr-xr-x   1 root  wheel   18958 Jul  8 08:43 cbs.json.9
 -rwxr-xr-x   1 root  wheel    9666 Jul  8 08:54 cbs.opt
```

2. Open the file, using a text editor add the option "`com.ahsay.obs.core.job.ServerRunBackup.Xmx=%value%`" and "`com.ahsay.obs.core.job.ServerRunBackup.Xms=%value%`" then save.

```
com.ahsay.obs.core.job.ServerRunBackup.Xmx=4096
com.ahsay.obs.core.job.ServerRunBackup.Xms=256
```

3. Restart the AhsayCBS service

```
# cd /ubs/mnt/esfmfw/obsr/system/obsr/bin
# sh restart.sh
```

NOTE

In the example, 4096 and 256 are the maximum and minimum Java heap size. The size of the Java memory that you will set for each backup job depends on the number of Office 365 user selected in your backup sets and how much RAM your system has.

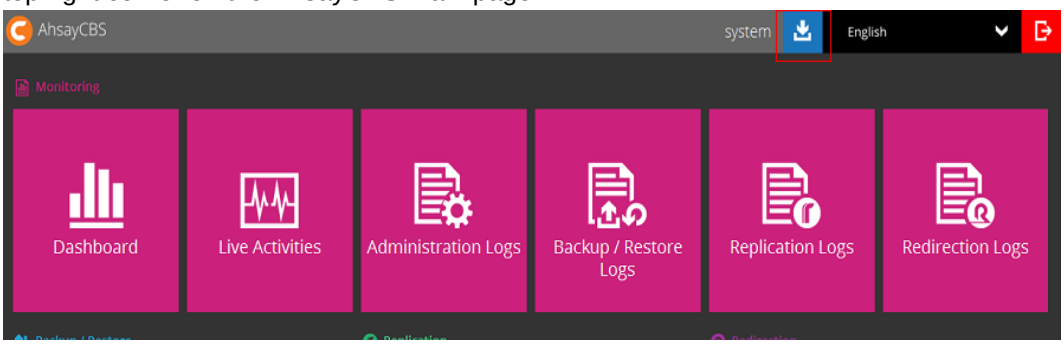
7 Download Backup / Restore Client

There are four backup / restore clients for you to choose from:

- AhsayOBM and AhsayACB for computer users to backup and restore
- AhsayOBR for computer users to restore only
- Ahsay Mobile for mobile device users to backup and restore

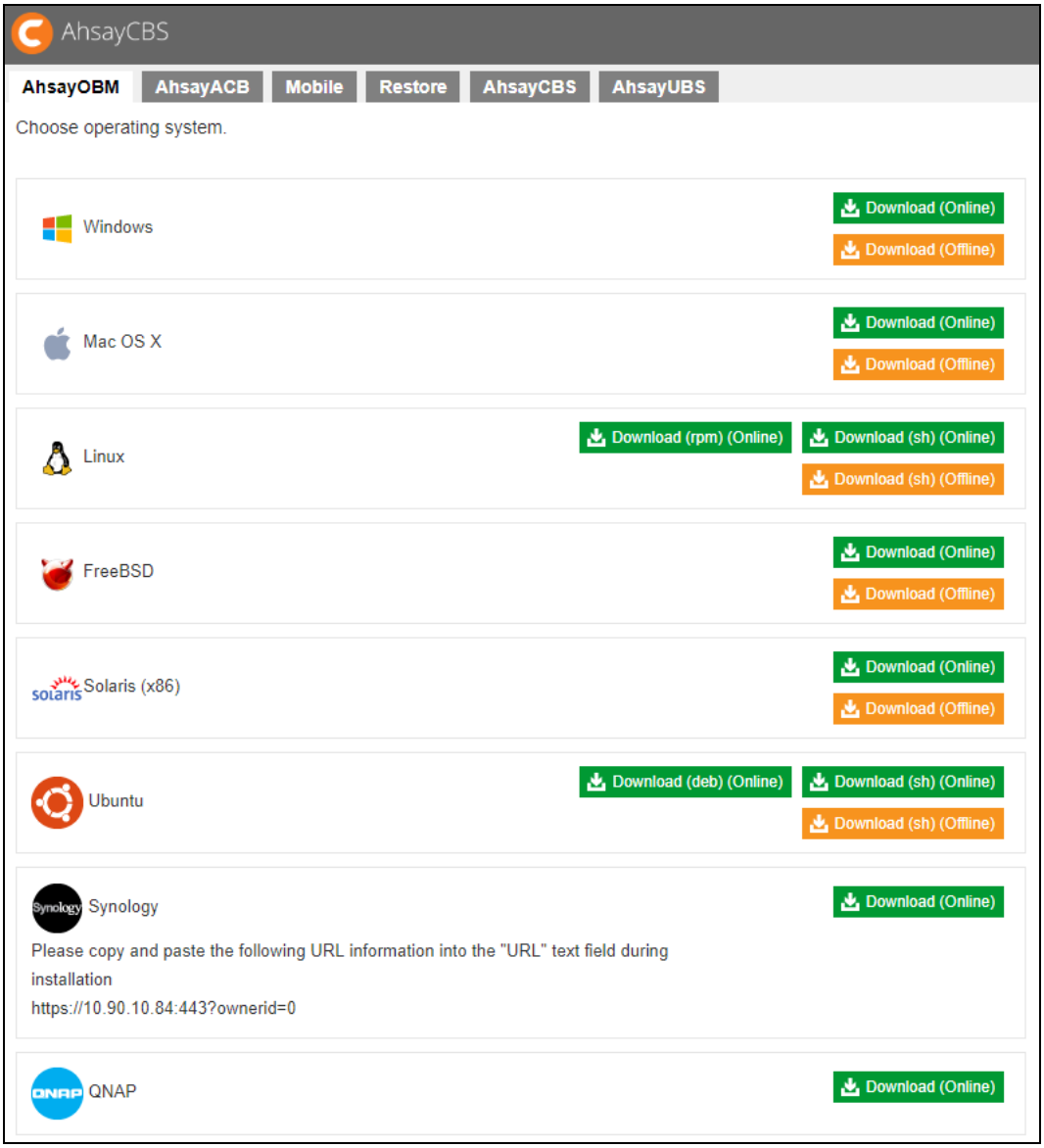
7.1 Download AhsayACB / AhsayOBM / AhsayOBR on Computer

1. In a browser, download the backup clients by clicking the blue **Download** icon at the top right corner on the AhsayCBS main page.



2. Click on the tab with the name of the client backup/ restore agent you wish to download, AhsayOBM tab, AhsayACB tab or Restore tab (AhsayOBR).

3. Click on the Download (Online) or Download (Offline) button of the platform on which you wish to install the client backup/ restore agent.



AhsayCBS support two installation modes, online and offline installation (except for Linux (rpm), Ubuntu (deb), Synology NAS and QNAP which supports online installation only). User can apply either of the installation modes.

Below is the table of comparison between online installation and offline installation.

	Online Installation	Offline Installation
Internet	➢ It cannot be started without an internet connection. ➢ Clients need to have an internet connection each time an installation is run. ➢ If the client internet connection is interrupted or is not stable the installation may be unsuccessful.	➢ Once the offline installer is downloaded, the client does not require an internet connection each time an installation is run. ➢ The offline installer size is 80MB to 140MB depending on operating system as it contains all

	➢ Online installer size is 6KB to 3.5MB depending on operating system as it contains only the initial installation package files.	the necessary binary and component files.
Backup Server Availability	The online installer requires the backup server to be online in order to run and complete the installation.	An offline installation can be performed independently of the backup server availability.
Installation Time	➢ Takes more time as it needs to download the binary and component files (80MB to 140MB depending on operating system) each time the installation is run. ➢ A slow internet connection on the client machine will also result in longer installation time.	Takes less time as all the necessary binary and components files are already available in the offline installer.
Version Control	Ensures the latest version of the product is installed.	May need to update the product version after installation if an older offline installer is used.
Administrative Support	Need more time on the support for the installation as network factor might lead to unsuccessful installation.	Need less time as independent of network factor influence.
Deployments	➢ Suitable for single or small amount of device installations. ➢ Suitable for client sites with fast and stable internet connection.	➢ Suitable for multiple or mass device installations. ➢ Suitable for client sites with metered internet connections.

7.2 Download Ahsay Mobile on a Mobile Device

7.2.1 Android Device

The latest version of Ahsay Mobile is available from Google Play.

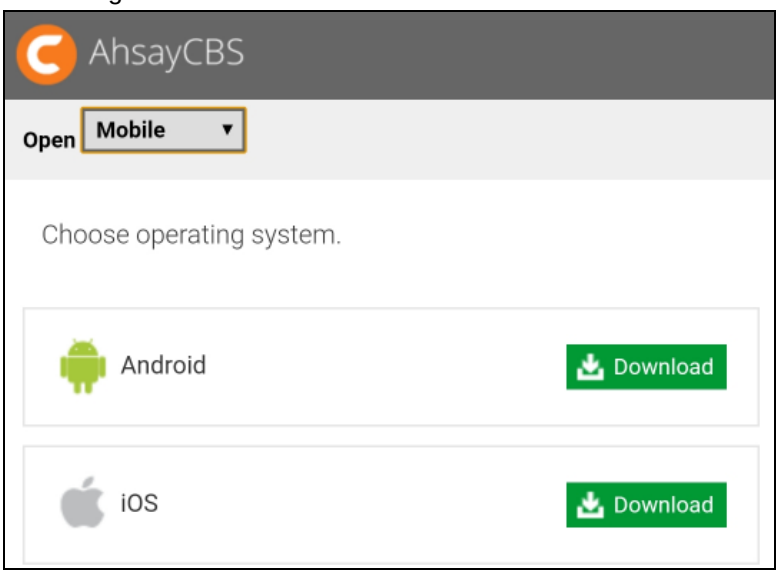
7.2.2 iOS Device

The latest version of Ahsay Mobile is available from Apple App Store.

7.3 Download Ahsay Mobile using a web browser

Ahsay Mobile can also be downloaded using the following links from the Mobile tab of the AhsayCBS web console. Make sure to use an Android or iOS mobile device when clicking on the respective download links on the AhsayCBS web console, so you are automatically redirected to either Google Play or the App Store.

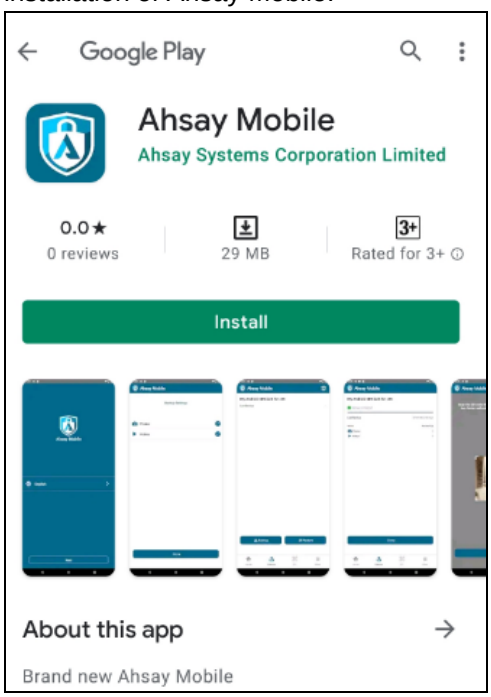
1. Tap the Download button of the platform on which you wish to install the client backup/ restore agent.

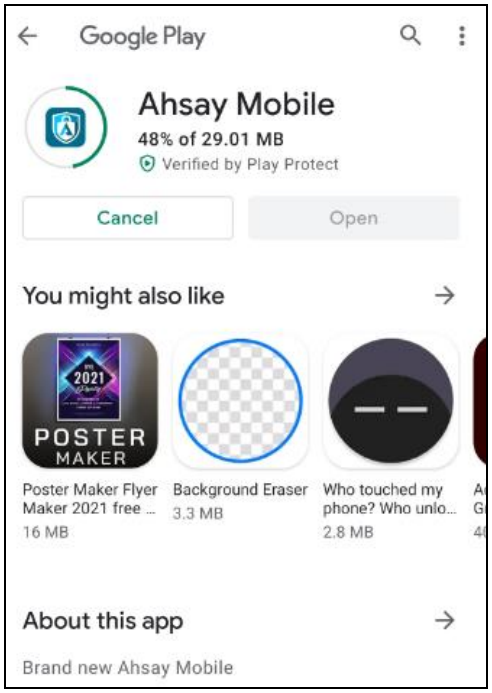


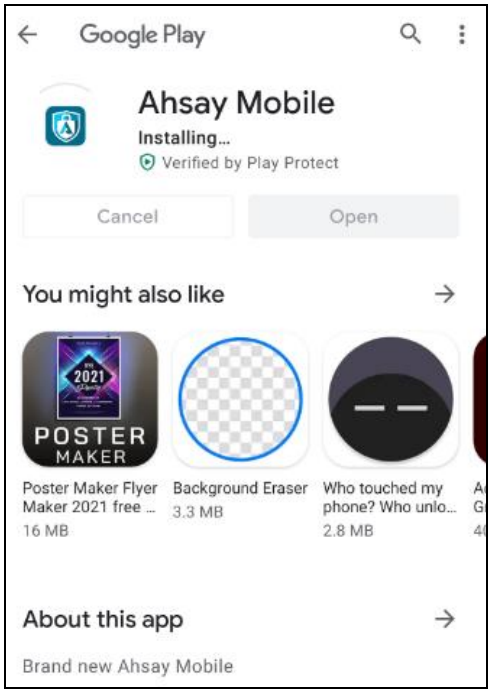
2. The following page would be displayed depending on the platform you chose:

   - Android
   - iOS

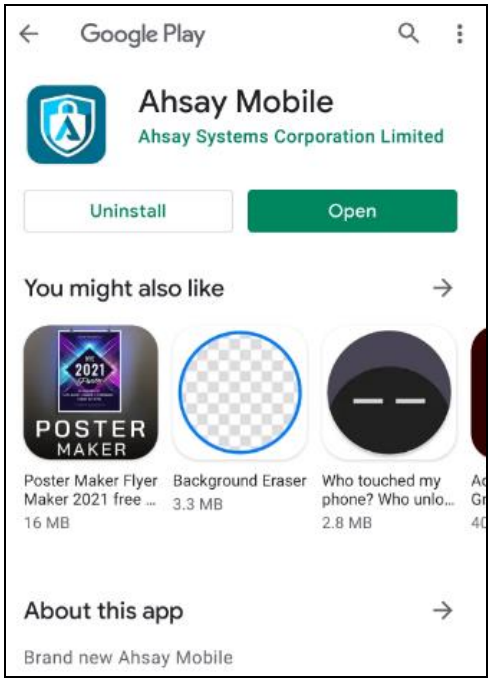
   For Android, user will be redirected to Google Play. Tap **Install** to begin installation of Ahsay Mobile.



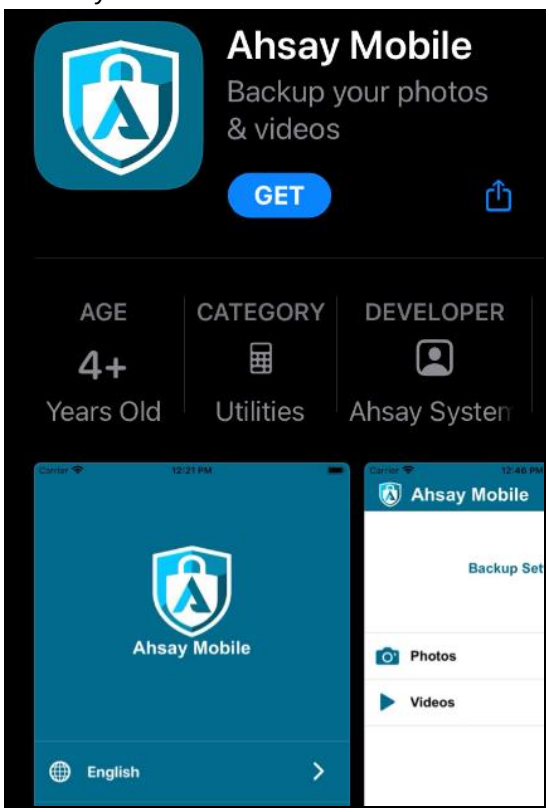




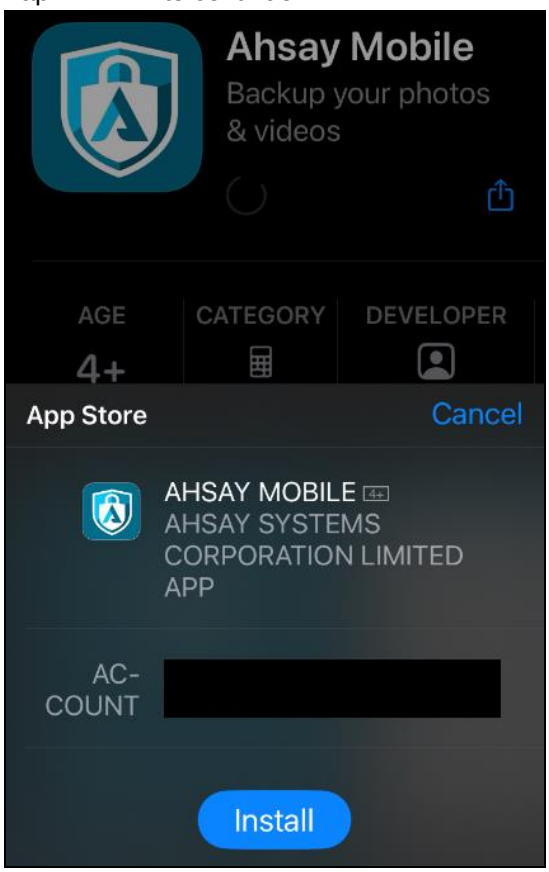
Once done installing, tap **Open** to start using Ahsay Mobile.



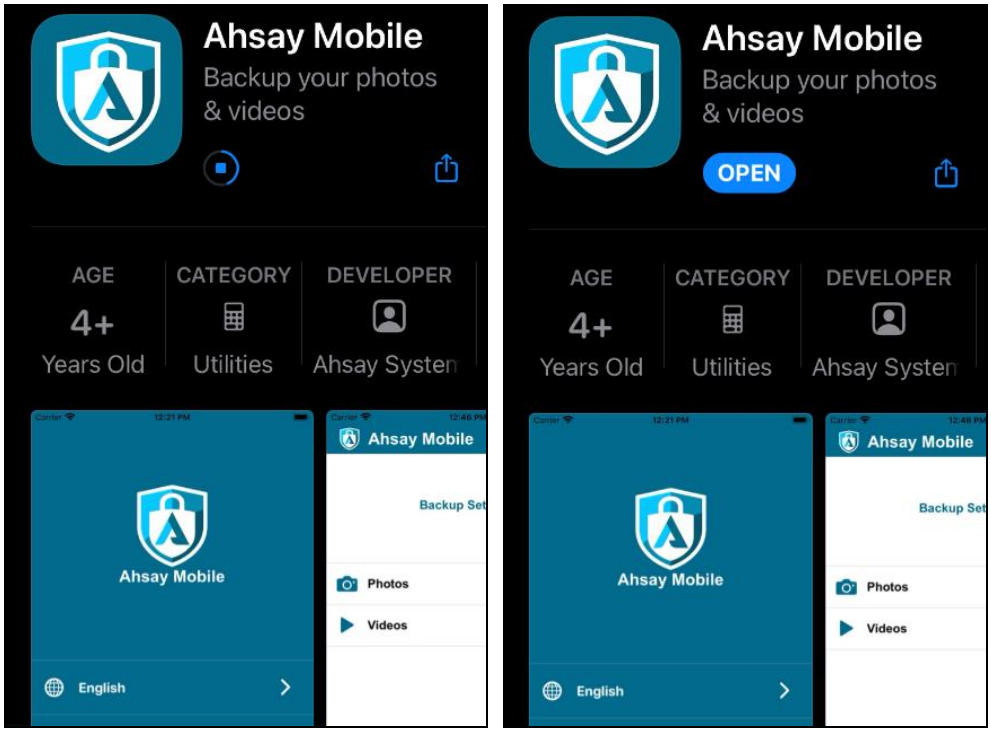
For iOS, user will be redirected to the App Store. Tap **GET** to start the installation of Ahsay Mobile.



Tap **Install** to continue.



Once done installing, tap OPEN to start using Ahsay Mobile.



7.4 Instruction Regarding Installation of Client Backup Agent

For information about the installation of AhsayACB, AhsayOBM, AhsayOBR and Ahsay Mobile, creating backup sets and restoration, please refer to the User Guides/Quick Start Guides via the respective URL below.

AhsayACB

Windows	https://www.ahsay.com/download/download_document_v8_acb-quickstart-windows.jsp
Mac OS X	https://www.ahsay.com/download/download_document_v8_acb-quickstart-mac.jsp

AhsayOBM

Windows	https://www.ahsay.com/download/download_document_v8_obm-quickstart-windows.jsp
Mac OS X	https://www.ahsay.com/download/download_document_v8_obm-quickstart-mac.jsp
Linux (CLI)	https://www.ahsay.com/download/download_document_v8_obm-quickstart-linux.jsp

Linux (GUI)	https://www.ahsay.com/download/download_document_v8_obm-quickstart-linux-gui.jsp
FreeBSD	https://www.ahsay.com/download/download_document_v8_obm-user-guide-freebsd.jsp
Synology NAS	https://www.ahsay.com/download/download_document_v8_obm-quickstart-synology.jsp
QNAP NAS	https://www.ahsay.com/download/download_document_v8_obm-user-guide-qnap-nas.jsp

Windows	https://www.ahsay.com/download/download_document_v8_obr-user-guide-win.jsp
Mac OS X	https://www.ahsay.com/download/download_document_v8_obr-user-guide-mac.jsp
Linux (GUI)	https://www.ahsay.com/download/download_document_v8_obr-user-guide-linux-gui.jsp

Android / iOS	https://download.ahsay.com/support/document/v8/guide_ahsay_app_user_v8.pdf

8 Contacting Ahsay

8.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the Partner Portal:
https://www.ahsay.com/partners/

Also use the Ahsay Wikipedia for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:
https://wiki.ahsay.com

8.2 Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_downloads_documentation_guides

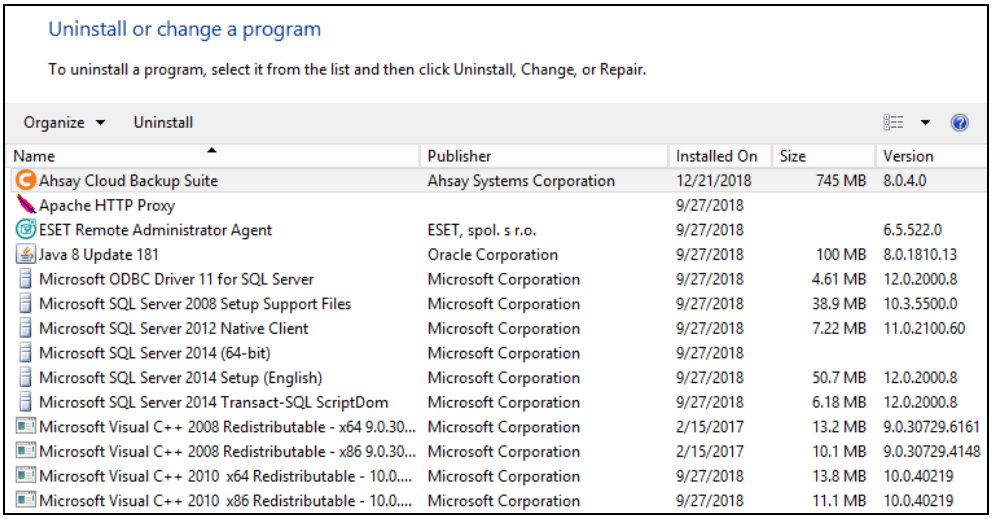
You can send us suggestions for improvements or report on issues in the documentation, by contacting us at:
https://www.ahsay.com/partners/

Please specify the specific document title as well as the change required/suggestion when contacting us.

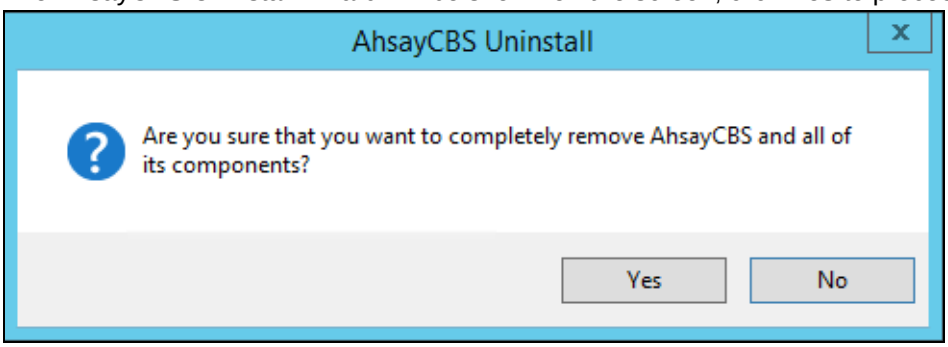
Appendix

Uninstall AhsayCBS on Windows

1. Go to **Control Panel** > **Programs and Features** > **Uninstall a program**, then look for **Ahsay Cloud Backup Suite**. Then click **Uninstall**.

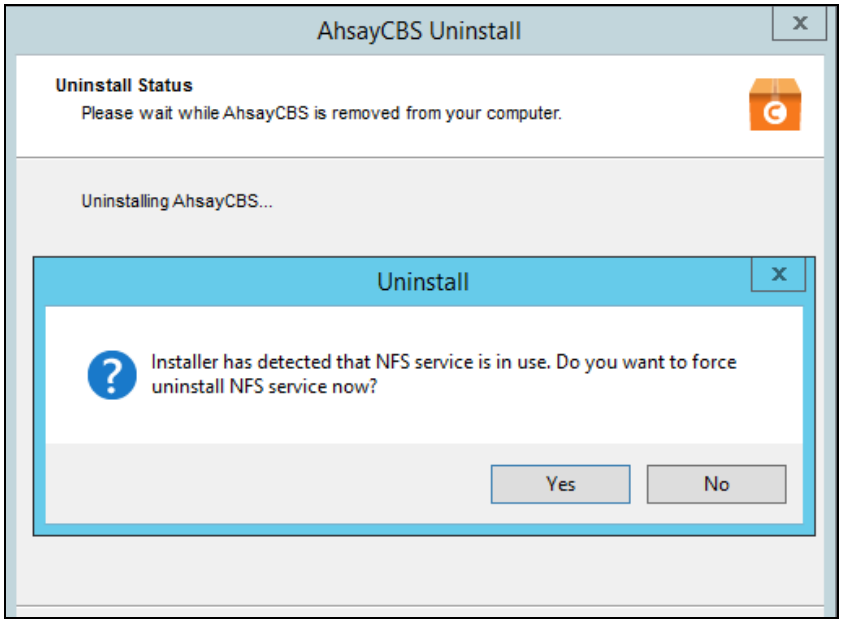


2. The AhsayCBS Uninstall wizard will be shown on the screen, click **Yes** to proceed.

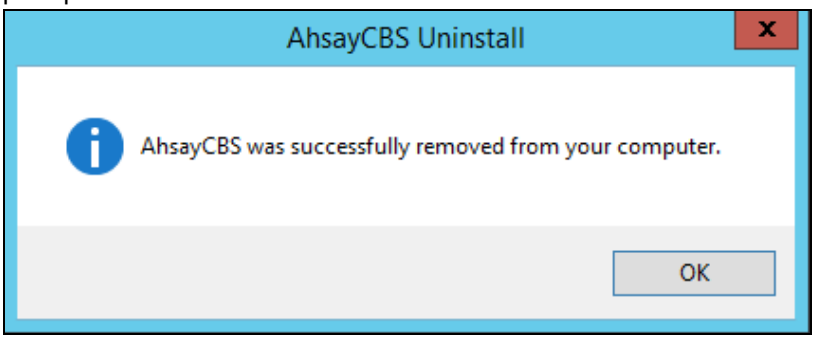


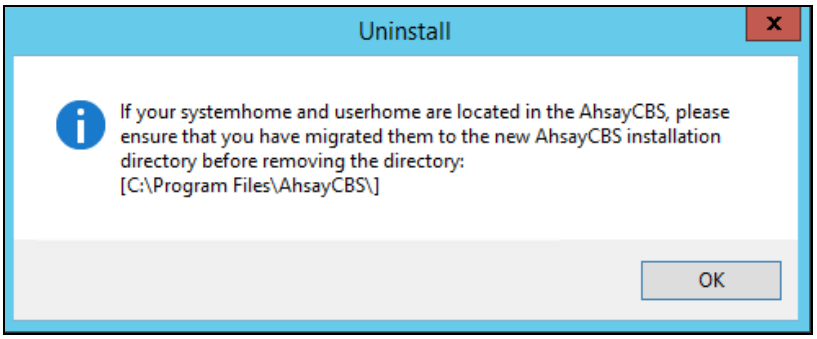
3. If there is a Run Direct restore running at the time of the AhsayCBS uninstallation, the following screen prompts to alert you the NFS service is in use.

   - Select **No** if you do not wish to force uninstall the NFS service. AhsayCBS will be uninstalled without affecting the NFS service, where the Run Direct restore will not be interrupted.
   - Select **Yes** to force uninstall the NFS service. Both AhsayCBS and NFS service will be uninstalled from the machine. The VM running Run Direct restore session and the datastore are both unmounted from the VMware server.



4. The following screens prompt when the uninstallation is completed. Click **OK** to exit the prompts.





5. The system will automatically open a file folder directing to the installation path, so that the USER_HOME, SYSTEM_HOME and POLICY_HOME can be copied/backed up easily if required.

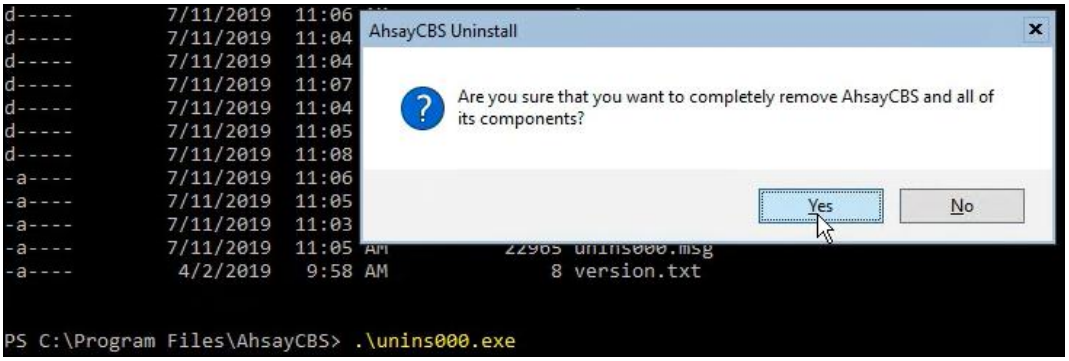
Uninstall AhsayCBS on Windows Server Core

1. Change the directory to the installation directory.

```
> cd 'C:\Program Files\AhsayCBS\'
```

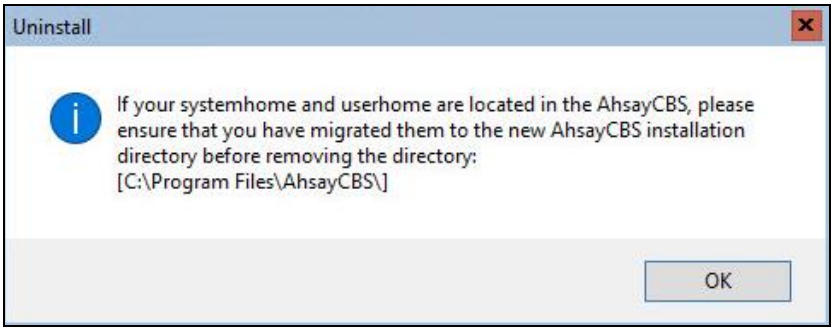
2. Execute **unins000.**exe and click Yes.

```
> .\unins000.exe
```



3. The following screen prompts when the uninstallation is completed. Click **OK** to continue.

4. Click **OK** to continue.



5. Make a backup of your existing SYSTEM_HOME, USER_HOME and POLICY_HOME directory if necessary before removing the AhsayCBS directory.

6. Remove the AhsayCBS directory from the system. Once done, AhsayCBS will now be removed from the system.

```
PS C:\Program Files> rm .\AhsayCBS\
```

```
PS C:\Program Files> rm .\AhsayCBS\

Confirm
The item at C:\Program Files\AhsayCBS\ has children and the Recurse parameter was not specified. If
you continue, all children will be removed with the item. Are you sure you want to continue?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

Uninstall AhsayCBS on Linux/FreeBSD

To uninstall AhsayCBS from a Linux or FreeBSD system, please follow the steps below.

1. Login as root to the Linux/FreeBSD machine.

2. Go to the `/usr/local/cbs/bin` directory.

```
# cd /usr/local/cbs/bin
```

3. Uninstall AhsayCBS using the sh command.

```
# sh uninstall.sh
```

4. After successful uninstallation, AhsayCBS and NFS service will no longer be available because removal of the startup scripts will stop the services from starting at bootup.

   For Linux:

```
Log Time: Thu Apr  4 15:29:29 HKT 2019

Verifying current user privilege ...
Current user has enough privilege to "uninstall".

Using CBS_HOME: /usr/local/cbs
Using JAVA_HOME: /usr/local/cbs/java
Try to shutdown [ Ahsay Cloud Backup Suite ]
--------------------------------------------------------------------------
You may set SYSTEM_DEBUG=0 to disable the debug message
--------------------------------------------------------------------------
Current User Name   : root
Using SYSTEM_TYPE   : linux
Using SYSTEM_ARCH   : x86_64
--------------------------------------------------------------------------
Using CBS_HOME      : /usr/local/cbs
Using JAVA_HOME     : /usr/local/cbs/java
Using CATALINA_HOME : /usr/local/cbs/tomcat
Using JAVA_OPTS     : -Djava.library.path=/usr/local/cbs/lib/LinX64 -
DCATALINA_PID=/var/run/obsr.pid -Dsun.net.inetaddr.ttl=3600 -
Dnetworkaddress.cache.ttl=3600 -Dsun.net.inetaddr.negative.ttl=300 -
Dnetworkaddress.cache.negative.ttl=300 -
Dsun.nio.PageAlignDirectMemory=true -Djava.net.preferIPv4Stack=true -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -
Djava.util.logging.config.file=conf/logging.properties -
Dtc.work.path=work -Dtc.log.path=logs -
Djavax.servlet.context.tempdir=work
Using CATALINA_OPTS :
Using CATALINA_PID  : /var/run/obsr.pid
--------------------------------------------------------------------------
Stopping AhsayCBS service
Wait 5 seconds before [ Ahsay Cloud Backup Suite ] is down
Remove [ Ahsay Cloud Backup Suite ] (cbs) from service
Uninstall Service for NIX type OS
Using init script path /etc/init.d
Using run level script path /etc
Removing symbolic link from run levels
Removing script file cbs from /etc/init.d
[ Ahsay Cloud Backup Suite ] uninstall service is complete!
Try to shutdown [ NFS Service (Ahsay Systems Corporation) ]
Stopping NFS Service (Ahsay Systems Corporation)
Wait 5 seconds before [ NFS Service (Ahsay Systems Corporation) ] is
down
Remove [ NFS Service (Ahsay Systems Corporation) ] (cbsnfs) from service
```

```
Uninstall Service for NIX type OS
Using init script path /etc/init.d
Using run level script path /etc
Removing symbolic link from run levels
Removing script file cbsnfs from /etc/init.d
[ NFS Service (Ahsay Systems Corporation) ] uninstall service is
complete!
It is now safe to remove files from /usr/local/cbs
```

For FreeBSD:

```
Log Time: Thu Apr  4 14:55:31 HKT 2019
Verifying current user privilege ...
Current user has enough privilege to "uninstall".
Using CBS_HOME: /usr/local/cbs
Using JAVA_HOME: /usr/local/cbs/java
Try to shutdown [ Ahsay Cloud Backup Suite ]
--------------------------------------------------------------------------
You may set SYSTEM_DEBUG=0 to disable the debug message
--------------------------------------------------------------------------
Current User Name   : root
Using SYSTEM_TYPE   : bsd
Using SYSTEM_ARCH   : amd64
--------------------------------------------------------------------------
Using CBS_HOME      : /usr/local/cbs
Using JAVA_HOME     : /usr/local/cbs/java
Using CATALINA_HOME : /usr/local/cbs/tomcat
Using JAVA_OPTS     : -Djava.library.path=/usr/local/cbs/lib/LinX64 -
DCATALINA_PID=/var/run/obsr.pid -Dsun.net.inetaddr.ttl=3600 -
Dnetworkaddress.cache.ttl=3600 -Dsun.net.inetaddr.negative.ttl=300 -
Dnetworkaddress.cache.negative.ttl=300 -
Dsun.nio.PageAlignDirectMemory=true -Djava.net.preferIPv4Stack=true -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -
Djava.util.logging.config.file=conf/logging.properties -
Dtc.work.path=work -Dtc.log.path=logs -
Djavax.servlet.context.tempdir=work
Using CATALINA_OPTS :
Using CATALINA_PID  : /var/run/obsr.pid
--------------------------------------------------------------------------
Stopping AhsayCBS service
Wait 5 seconds before [ Ahsay Cloud Backup Suite ] is down
Remove [ Ahsay Cloud Backup Suite ] (cbs) from service
Uninstall Service for BSD type OS
Remove script cbs from /usr/local/etc/rc.d
[ Ahsay Cloud Backup Suite ] uninstall service is complete!
Try to shutdown [ NFS Service (Ahsay Systems Corporation) ]
Stopping NFS Service (Ahsay Systems Corporation)
Wait 5 seconds before [ NFS Service (Ahsay Systems Corporation) ] is
down
Remove [ NFS Service (Ahsay Systems Corporation) ] (cbsnfs) from service
Uninstall Service for BSD type OS
Remove script cbsnfs from /usr/local/etc/rc.d
[ NFS Service (Ahsay Systems Corporation) ] uninstall service is
complete!
It is now safe to remove files from /usr/local/cbs
```

5. Make a backup of your existing $SYSTEM_HOME, $USER_HOME and $POLICY_HOME directories to another computer if necessary.

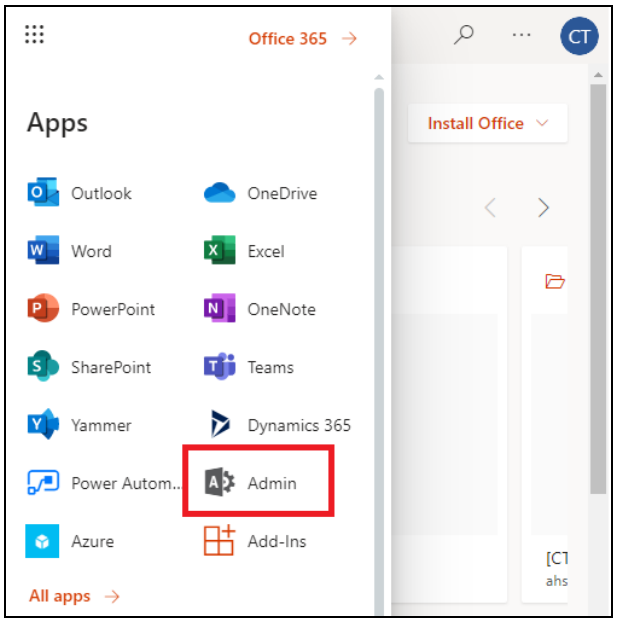
6. **For FreeBSD only**, ensure that cbs and nfs service are disabled by removing the cbs_enable="YES" and cbsnfs_enable="YES" lines from /etc/rc.conf by using a text editor like vi.

7. Remove the $CBS_HOME directory from the system. Once done, AhsayCBS will now be removed from your system.

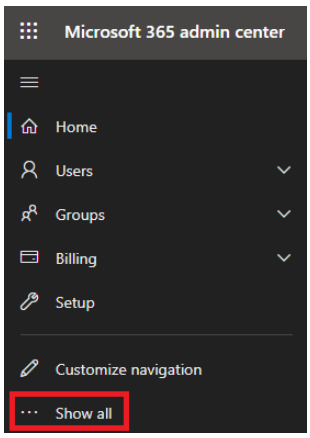
How to view item count and storage used in Microsoft 365 Admin Center

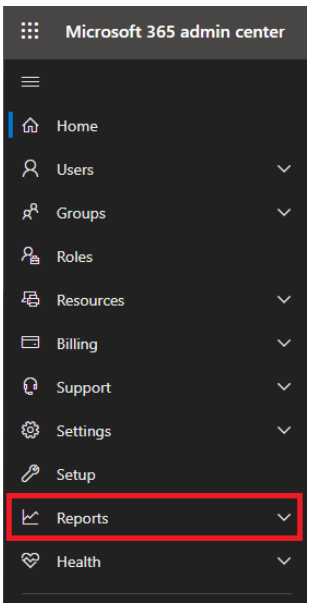
To view the item count and storage size of Office 365 user account based on the usage of Exchange (Outlook), OneDrive and SharePoint, follow the instructions below:

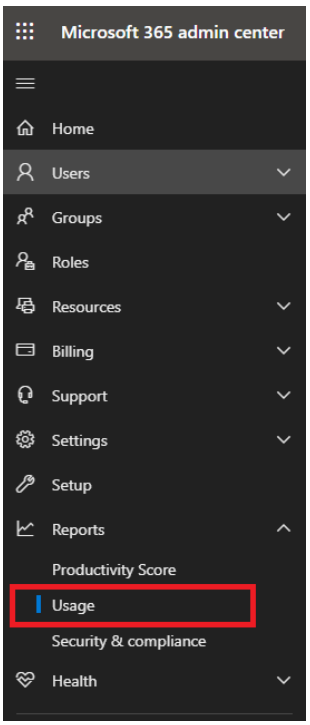
1. Login to Office 365 (https://login.microsoft.com).
2. Go to Microsoft 365 admin center.



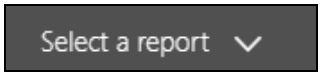
3. In the Microsoft 365 admin center, click **Show all** then click the dropdown arrow for the **Reports** and select **Usage**.

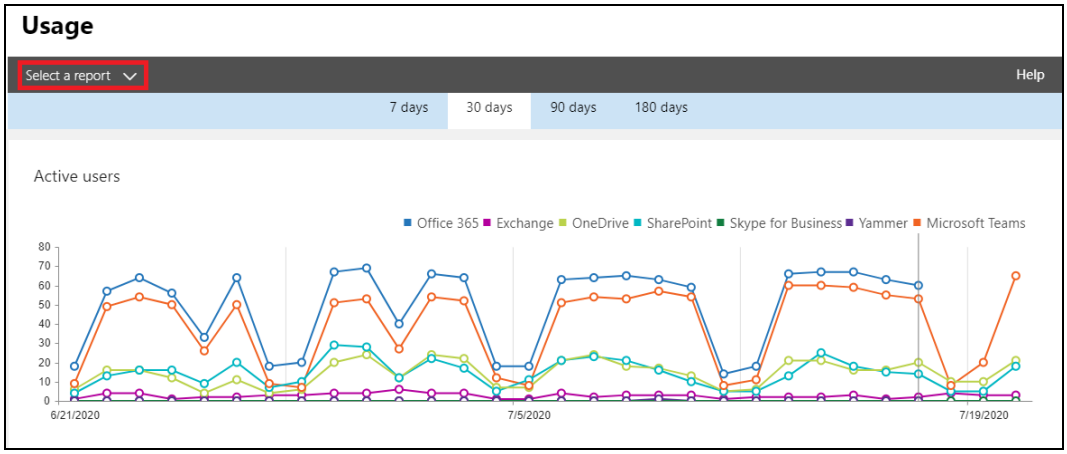


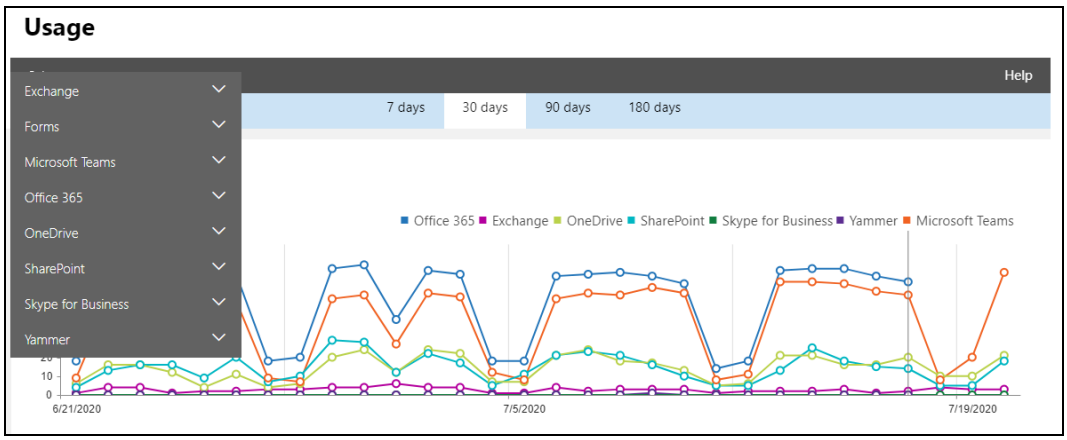




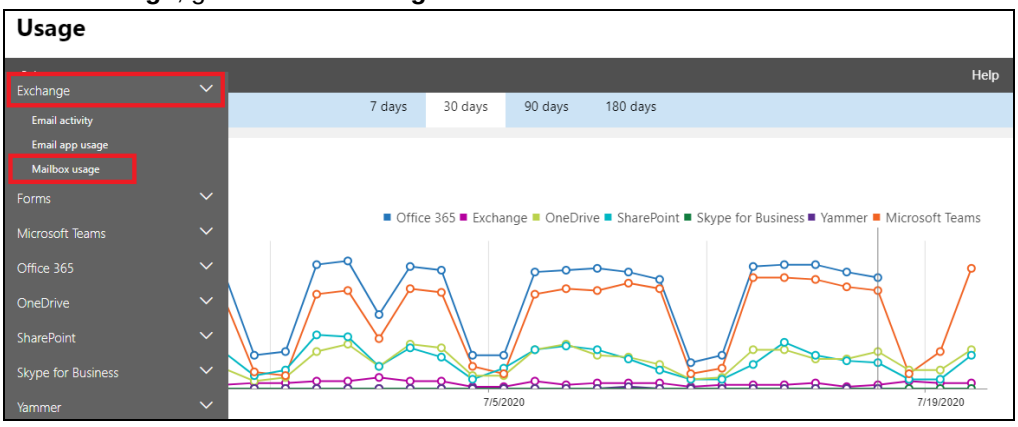
4. In the **Usage** screen, select a report you want to view.

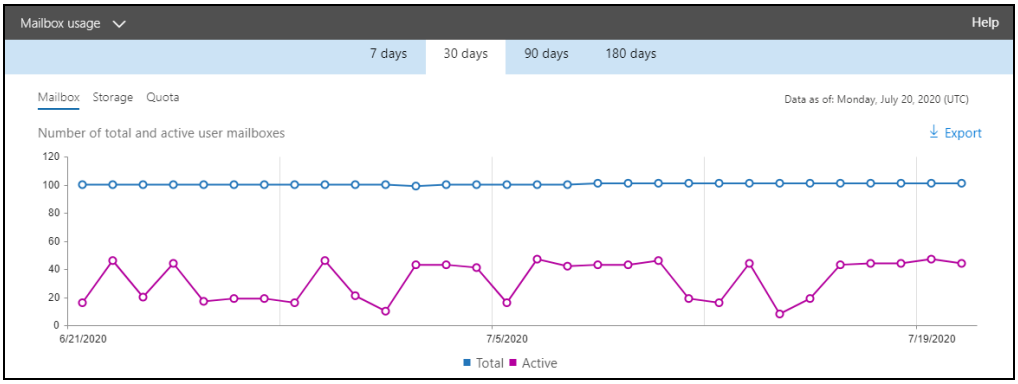






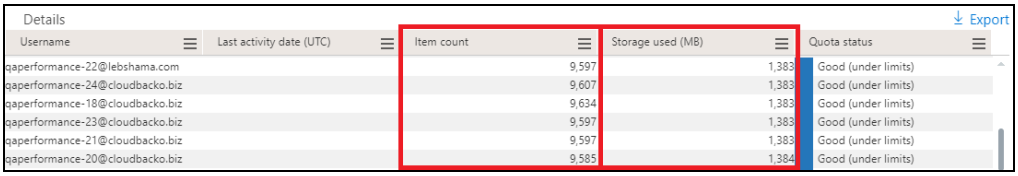
- For **Exchange**, go to **Mailbox usage**.



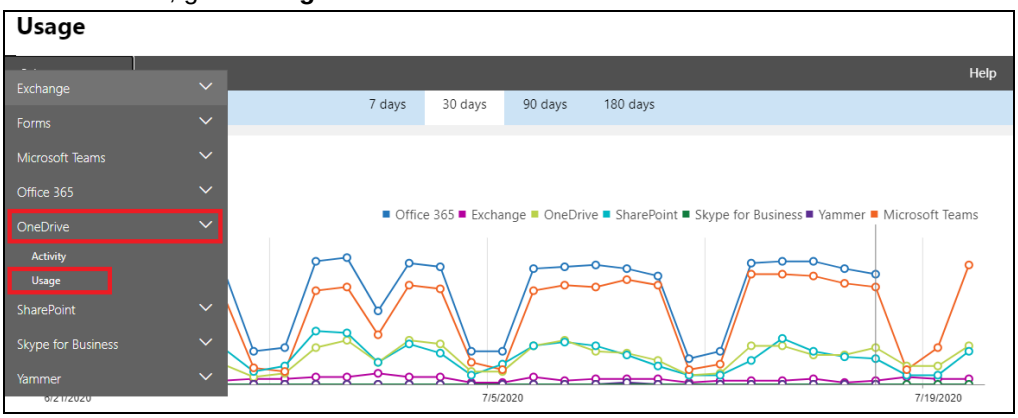


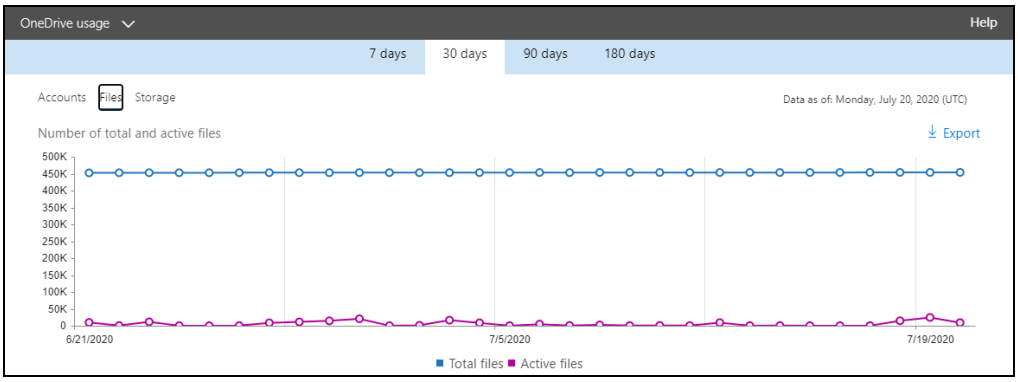
Highlighted columns are Item count and Storage used (MB).

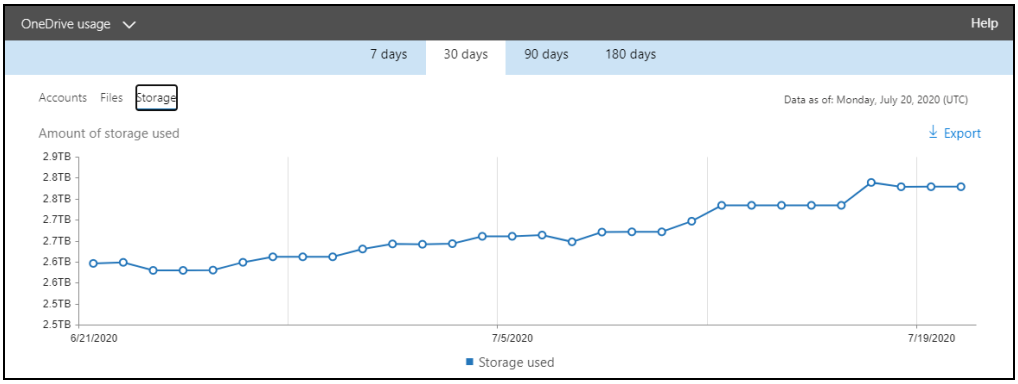
- **Item count** – number of mailbox items in Outlook per Office 365 user account
- **Storage used (MB)** – storage used in MB size per Office 365 user account



- For **OneDrive**, go to **Usage**

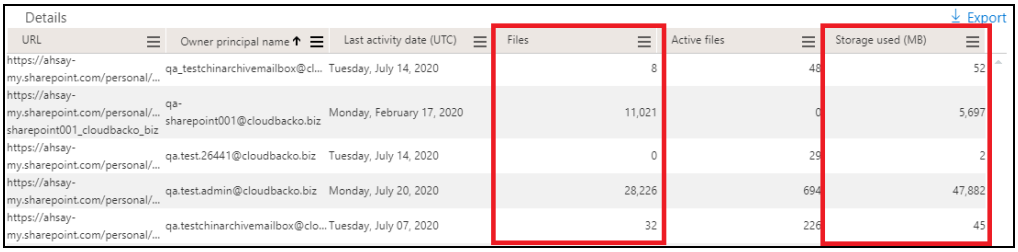




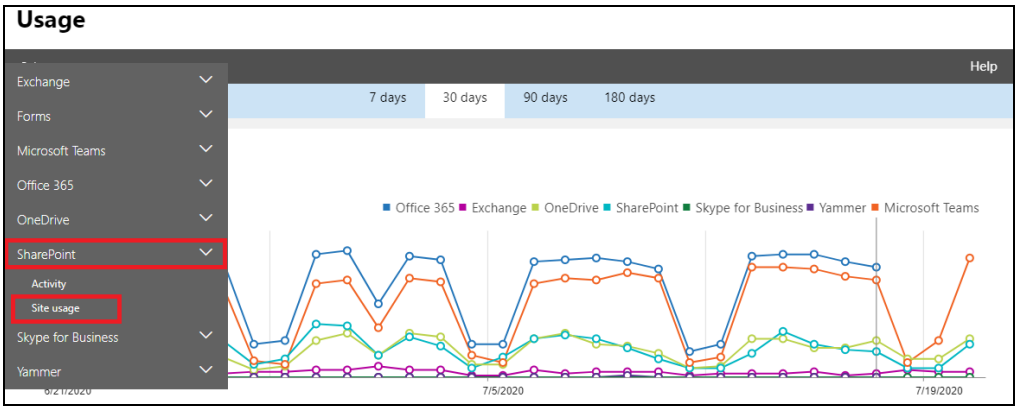


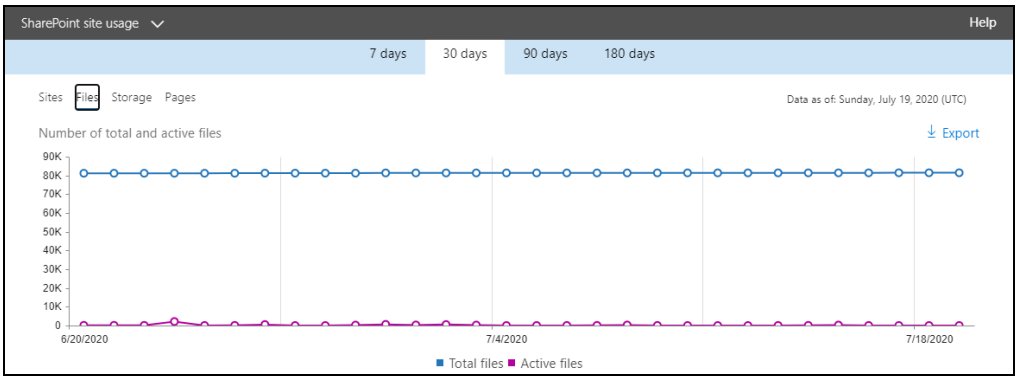
Highlighted columns are Files and Storage used (MB).

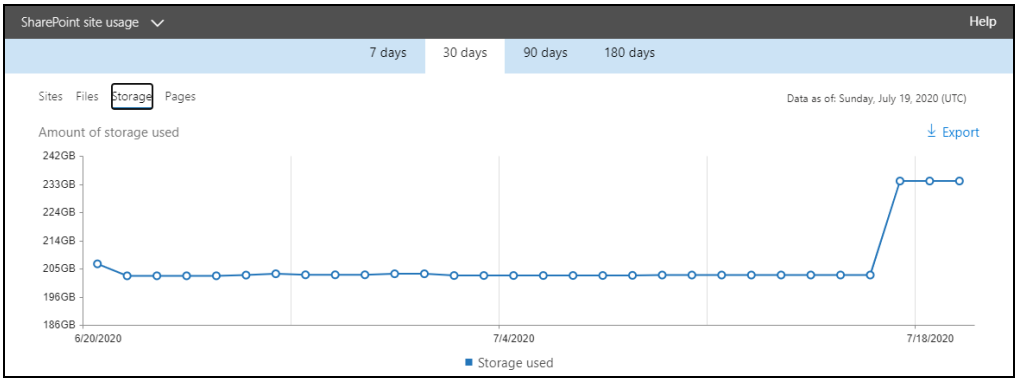
- **Files** – number of files in OneDrive per Office 365 user account
- **Storage used (MB)** – storage used in MB size per Office 365 user account



- For **SharePoint**, go to **Site usage**.

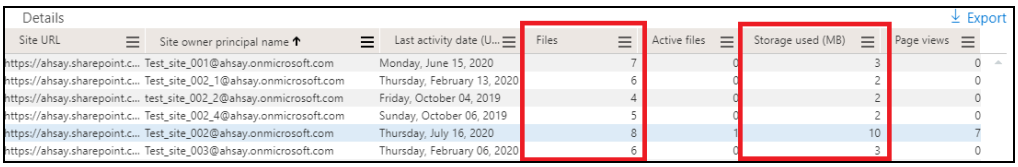






Highlighted columns are Files and Storage used (MB).

- **Files** – number of files in SharePoint per Office 365 user account
- **Storage used (MB)** – storage used in MB size per Office 365 user account



Office 365 agentless backup set for a large number of Office 365 users

To split the Office 365 users into several Office 365 agentless backup sets, we will use 10,000 Office 365 users that needs to be backed up as an example. Since the maximum number of Office 365 user per Office 365 agentless backup set is 2,000, there are many options available but this will involve a large number of backup sets and maintenance of these backup sets will not be practical so we will show you only two options below.

- Option 1 - 5 Backup Sets, each has 2,000 Office 365 Users
- Option 2 - 10 Backup Sets, each has 1,000 Office 365 Users

Option 1 – 5 Backup Sets, each has 2,000 Office 365 Users

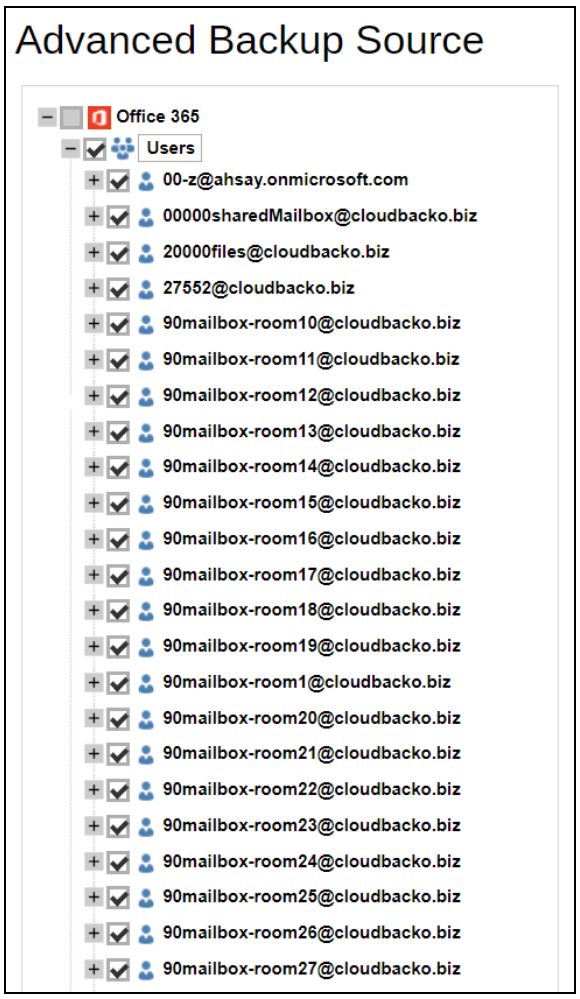
Backup Set Name	User Number
Backup -Set-1	No.1 – 2000
Backup -Set-2	No.2001 – 4000
Backup -Set-3	No. 4001 – 6000
Backup -Set-4	No. 6001 – 8000
Backup -Set-5	No. 8001 – 10000

Option 2 – 10 Backup Sets, each has 1,000 Office 365 Users

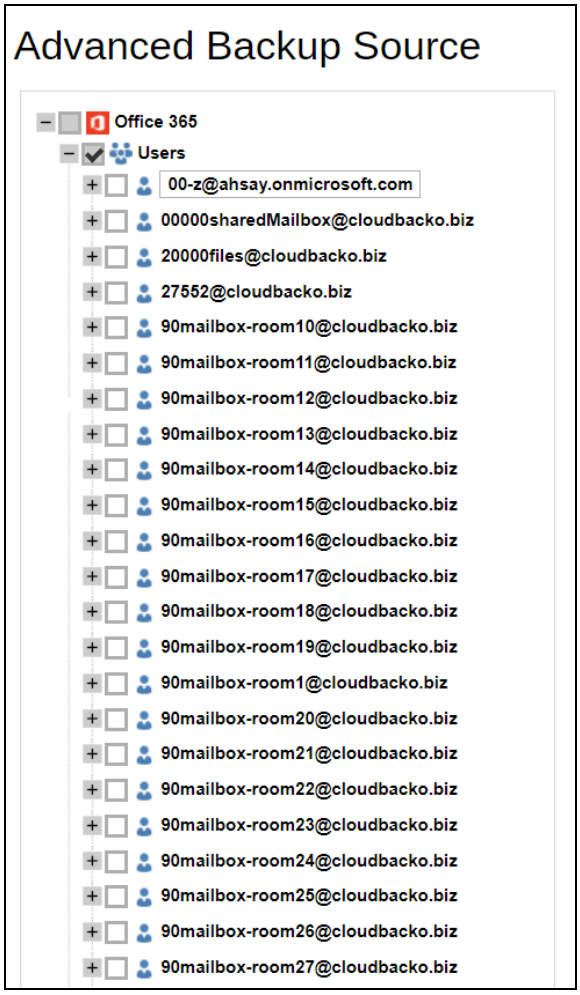
Backup Set Name	User Number
Backup -Set-1	No.1 – 1000
Backup -Set-2	No.1001 – 2000
Backup -Set-3	No. 2001 – 3000
Backup -Set-4	No. 3001 – 4000
Backup -Set-5	No. 4001 – 5000
Backup -Set-6	No. 5001 – 6000
Backup -Set-7	No. 6001 – 7000
Backup -Set-8	No. 7001 – 8000
Backup -Set-9	No. 8001 – 9000
Backup -Set-10	No. 9001 – 10000

If Option 2 was selected, for the last backup set, Backup -Set-10, follow the instructions on how to select the Office 365 users. Doing these steps will ensure that additional Office 365 users will automatically be included in the backup set.

1. On the backup source, tick the checkbox for the root selection. This will select all the Office 365 users.



2. De-select the first 9000 Office 365 users.

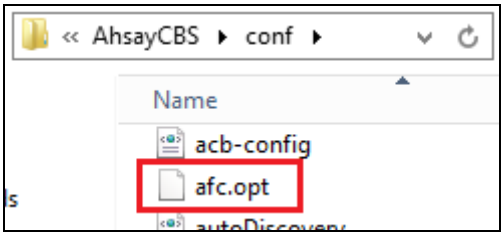


How to configure backup threads on AhsayCBS

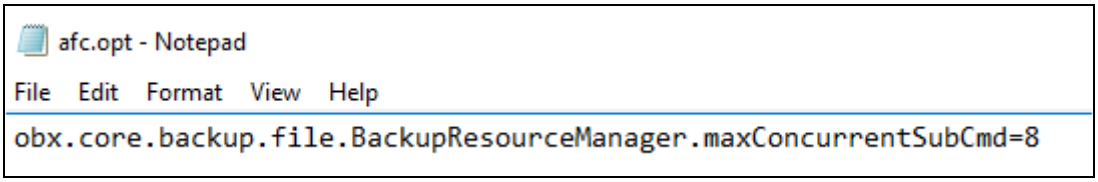
To configure the number of backup threads on AhsayCBS, follow the instructions below:

In Windows:

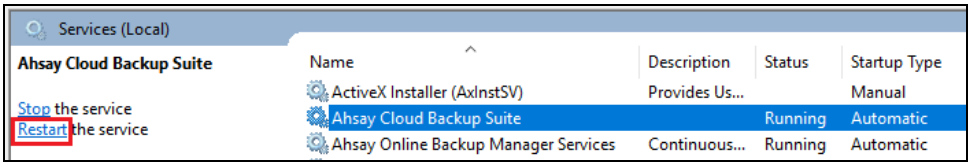
1. Locate the afc.opt file in the %APPLICATION_HOME%\conf folder.



2. Open the file, add the parameter "`obx.core.backup.file.BackupResourceManager.maxConcurrentSubCmd`" with the preferred number of backup threads and save. In our example, we are using 8 as the preferred number of backup threads.



3. Restart the AhsayCBS service.



In Linux/FreeBSD:

1. Locate the afc.opt file in `/usr/local/cbs/conf` folder.

```
# cd /usr/local/cbs/conf
# ls -la
total 996
drwxr-xr-x.  4 root root   4096 Jul 24 13:15 .
drwxr-xr-x. 22 root root   4096 Jul  9 23:49 ..
-rwxr-xr-x.  1 root root    316 Oct 16  2014 acb-config.xml
-rwxr-xr-x.  1 root root   4961 Jun 28  2017 afc.opt
```

2. Open the file, using a text editor add the parameter "`obx.core.backup.file.BackupResourceManager.maxConcurrentSubCmd`" with the preferred number of backup threads and save. In our example, we are using 8 as the preferred number of backup threads.

```
obx.core.backup.file.BackupResourceManager.maxConcurrentSubCmd=8
```

3. Restart the AhsayCBS service

```
# cd /usr/local/cbs/bin
# sh restart.sh
```

In AhsayUBS:

1. Locate the afc.opt file in `/ubs/mnt/eslsfw/obsr/conf` folder.

```
# cd /ubs/mnt/eslsfw/obsr/conf
# ls -la
total 933
drwxr-xr-x   4 root  wheel     144 Jul 24 04:30 .
drwxr-xr-x  13 root  wheel      13 Jul  8 08:25 ..
-rwxr-xr-x   1 root  wheel     316 Nov 19  2018 acb-config.xml
-rwxr-xr-x   1 root  wheel    4966 Jul  8 08:35 afc.opt
```

2. Open the file, using a text editor add the parameter "`obx.core.backup.file.BackupResourceManager.maxConcurrentSubCmd`" with the preferred number of backup threads and save. In our example, we are using 8 as the preferred number of backup threads.

```
obx.core.backup.file.BackupResourceManager.maxConcurrentSubCmd=8
```

3. Restart the AhsayCBS service.

```
# cd /ubs/mnt/esfmfw/obsr/system/obsr/bin
# sh restart.sh
```