Ahsay Backup

Ahsay Cloud Backup Suite v7

Administrator's Guide

Ahsay Systems Corporation Limited

31 July 2019

A wholly owned subsidiary of
Ahsay Backup Software Development Company Limited
HKEx Stock Code: 8290

www.ahsay.com

Copyright Notice

© 2019 Ahsay Systems Corporation Limited. All rights reserved.

The use and copying of this product is subject to a license agreement. Any other use is prohibited. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without prior written consent of Ahsay Systems Corporation Limited. Information in this manual is subject to change without notice and does not represent a commitment on the part of the vendor, Ahsay Systems Corporation Limited does not warrant that this document is error free. If you find any errors in this document, please report to Ahsay Systems Corporation Limited in writing.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Trademarks

Ahsay, Ahsay Cloud Backup Suite, Ahsay Online Backup Suite, Ahsay Offsite Backup Server, Ahsay Online Backup Manager, Ahsay A-Click Backup, Ahsay Replication Server, Ahsay BackupBox Firmware, Ahsay Universal Backup System, Ahsay NAS Client Utility are trademarks of Ahsay Systems Corporation Limited.

Amazon S3 is registered trademark of Amazon Web Services, Inc. or its affiliates.

Apple and Mac OS X are registered trademarks of Apple Computer, Inc.

Dropbox is registered trademark of Dropbox Inc.

Google Cloud Storage and Google Drive are registered trademarks of Google Inc.

Lotus, Domino, Notes are registered trademark of IBM Corporation.

Microsoft, Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, One Drive and One Drive for Business are registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle, Oracle 10g, Oracle 11g and MySQL are registered trademarks of Oracle Corporation.

Rackspace and OpenStack are registered trademarks of Rackspace US, Inc.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. www.redhat.com in the U.S. and other countries. Linux is a registered trademark of Linus Torvalds.

ShadowProtect is registered trademark of StorageCraft Technology Corporation.

VMware, ESX, ESXi, vCenter are registered trademarks of VMware, Inc.

All other product names are registered trademarks of their respective owners.

Disclaimer

Ahsay Systems Corporation Limited will not have or accept any liability, obligation or responsibility whatsoever for any loss, destruction or damage (including without limitation consequential loss, destruction or damage) however arising from or in respect of any use or misuse of reliance on this document. By reading and following the instructions in this document, you agree to accept unconditionally the terms of this Disclaimer and as they may be revised and/or amended from time to time by Ahsay Systems Corporation Limited without prior notice to you.

Revision History

Date	Descriptions	Type of modification
26 January 2018	Added icon description for toast.ico for Appendix F	New
22 March 2018	Added information and updated screenshot for Auto Save for Ch.5.2.1; Modified %USER_HOME% for Ch.7.1.3; Added suggestion, assumption and steps for Move/ Import/ Export Users for Ch.6.2.1.7; Update the screenshot for Move/ Import/ Export Users for Ch.6.2.1.7	New/ Modification
28 May 2018	Update the screen shot for Ch.5, 6; Update the steps for Ch.6; Added Destination for Backup User Settings for Ch.5.1.4.3 Managing System User; Modified shared quota for Ch.6.4.5.2; Added User Quota for Ch.6.4.5.2; Added new quota management explanation for Ch.6.2.2.1; Updated email report screen shot for Ch.6.4.5.2	New/ Modification
11 June 2018	Added screen shot comparison for quota management between pre-v7.15.6.0 and post-v7.15.6.0 ; Add GDPR compliance for Ch.3.1; Add Cookie Banner Notification for Ch.5.1.1.9; Update screen shot for Ch.3.1, 3.3, 3.4	New/ Modification
7 August 2018	Added clarification for hostname setting for Ch.5.1.1.1 Host	New
15 August 2018	Added instruction for customization for OneDrive for Business in Ch.10.	New
14 September 2018	Added Progressive DIC for Ch.6.1.6; Updated screenshot for Ch.6.1; Added Suggestion on antivirus exclusion for Ch.1.3; Assed note and table for system sub admin for Ch.5.1.4.3 ; Added note for manage license key for Ch.4.2; Added note for license summary and requirement for Ch.4.3; Added Upgrade from pre-v7.17.0.0 to v7.17.0.0 and above for Ch.4.3	New/ Modification
31 July 2019	Added Email me Consolidated Report in Ch. 5.1.2	Modification

Table of Contents

1 Overview 1

What is this software? 1

System Architecture 1

Recommendation on Antivirus Exclusion 2

AhsayCBS System Components 2

Client Components 2

Server Components 6

Agentless Backup / Restore 7

Why should I use AhsayCBS to manage my backup users and system? 8

2 About this Document 11

What is the purpose of this document? 11

What should I expect from this document? 11

Who should read this document? 11

3 Log in to AhsayCBS Server 12

Log in to AhsayCBS Web Management Console 12

Download Client Backup Agents 14

Change the Language 17

Invoke Online Help 18

4 Managing License 20

Verify License Connectivity 20

Manage License Key 23

License Summary and Requirements 27

Automatic License Renewal 32

License Evaluation Expiry 32

Offline License Activation 32

License Management Portal 33

Active Pool Key 34

5 System Settings 35

Basic Backup Server Configuration 35

General 35

Host 36

System Home 37

Listening to non-standard TCP/IP Port 37

Listening to a single IP address 37

Restricting access to system page by IP address 38

Installation a trusted SSL certificate 38

Renew a trusted SSL certificate 42

Wild card SSL certificate with redirector setup 43
Cookie Banner Notification 47
Email 48
Predefined Destinations Tab 50
Set up predefined destination on cloud storage 51
Administrative Access Tab 54
Add a new system user 54
Sending a broadcast message 56
Managing System User 57
Export/Import System Users 69
Languages 70
Advanced Backup Server Configuration 71
Auto Save 71
Proxy 77
Logging 78
File Explorer 80
Runtime Options Tab 81

6 Managing Backup/Restore 82

Backup / Restore Basic Configuration 82
User Home 83
Free Trial Options 84
Backup Data Migration 86
Suggestion and Requirement 86
How to Perform the Data Migration 87
To add the exclusion of a v6 backup set from the data migration: 88
To delete an existing exclusion of a v6 backup set: 88
Run Direct 89
Windows Active Directory Integration 90
To enable Windows Active Directory Integration 90
Progressive Data Integrity Check 91
To enable Progressive Data Integrity Check 92
Manage Backup Users 94
Backup User Tab 94
Create a New Backup User 95
Delete Backup User 101
Auto Update 101
Broadcast 102
Backup User 103
Export Users' Usage Statistics to CSV File 103
Move/ Import/ Export Users 104
Rebuild Storage Statistics 110

Rescan all user home directories 111
Managing Backup Users 114
User Profile 116
Backup Set 125
Settings 132
Report 133
Statistics 134
Effective Policy 137
Manage User Groups 140
The default user group 140
To add backup user to a user group 141
To add a new policy group to a user group 141
Manage Policy Groups 142
To create a new policy group 143
To modify a policy group 144
To delete a policy group 144
To duplicate a policy group 145
To configure a policy group 147
General 147
User Settings 148
Backup Set Settings 171
GUI Settings 176
Default Values 179
Preempted Values 201
Preempted Backup Sets 219
Mobile Settings 225

7 Replication 229

Overview 229
Differences between v6 and v7 on Replication 230
How does Replication Work 231
Replication Scope 232
Coexistence of v6 and v7 Formats Backup Data 234
Transaction Log Location 236
Replication Order 237
Benefits of using Replication? 238
Multiple Threads Replication 238
Improved System Logs Monitoring 240
Replication Close to Real-Time 240
Replication of Individual Backup Set Only 241
Retention Policy for Replicated Data 241
Flexible Deployment Options 241

Quick Recovery of Backup Sever 241
Replication of v6 backup sets on AhsayCBS v7 242
Requirements 243
Limitations 243
Before Getting Started 244
Requirements and Best Practices 244
License Information 244
Version / Platform Compatibility 244
Replication Server Storage Requirement 244
Location of the Replication Server 245
AhsayCBS Replication Partitioning 246
Replication Performance Tuning 246
AhsayCBS Java Heap Size Setting 246
Firewall Settings 247
Don’t Deploy the Backup and Replication Servers on a Single Machine 247
Dedicated Restore Drive on Replication Server 247
Storage Requirement on Replication Server 247
Replication Server with Multiple Receivers 247
Replication Using Cross Over Cable 248
Deployment Options and Comparison 249
Deployment Method 249
Comparison between Deployment on AhsayCBS and Cloud Storage 253
Deployment Combinations of Backup and Replication Servers 255
Deployment 256
Major Steps to Deploy a Replication Service 256
Configuration on the Replication Receiving End 257
Create a Replication User Account 257
Editing Replication Receiver 260
Configuration on the Replication Sending End 261
AhsayCBS v7 Backup Server to AhsayCBS v7 Receiver 261
AhsayOBS v6 Backup Server to AhsayCBS v7 Receiver 264
AhsayCBS v7 Backup Server to a Predefined Destination 265
Other Replication Settings 267
Traffic Limit 267
Replicate Individual Backup Sets 268
Setting the Number of Backup Sets to Replicate Concurrently 270
Cyclic Redundancy Check (CRC) Checking 270
Recovery Process Overview 272
Recovery Methods 274
Method 1 - Rebuild AhsayCBS from Replication 274
Method 2 - Rebuild from Auto Save 276
Method 3 - Startup Replication Server as Backup Server 280

Extract Data from Replication Destination 285
Getting Started 285
To check replication logs on the Backup Server: 285
To check the replication logs on the Replication Server: 286
Extract from AhsayCBS Replication Server 287
Extract from a Predefined Destination - Cloud storage 291
Extract from the FTP/SFTP 293
Extract from the Local/Mapped Drive/Removable Drive 295
Extract from v6 Replication 296
Extract Snapshot from Retention Area 300
Restore Replication Data 303
Restore Replication Data to the Backup Server 303
Restore Raw Data Using AhsayOBM / AhsayACB 306

8 Configuring Redirector 308

Hosting a Redirector 310
Joining Redirector 311
Advanced Setup 312
Setup Wild Card Certificate 312
Setup Replication in Redirector Server Group 312
Multiple Redirector Setup 312

9 Monitoring Activities 315

Set up a Read-only Admin Account for Operators 315
Dashboard 317
To Dos 317
Viewing options 318
Missed Backups 319
Failed Backups 320
System Errors 321
Replication Errors 321
API Errors 322
Email Errors 323
Overview 324
CPU 325
Memory 326
Storage 327
Live Threads 328
Live Activities 329
Backup Status 329
Restore Status 330
Replication 332

Receiver 332
Redirection 333
Administration Logs 334
SNMP Log 334
Message History 334
Activities Log 335
Audit Trails 335
Backup / Restore Logs 336
Backup Jobs 336
Restored Jobs 336
Backup Errors 337
Backup Set Log 337
Activities Log 337
Replication Log 338
Sent to Receiver 338
Received from Other Backup Servers 338
Activities Log 339
Redirection Logs 340
Enable Third Party Monitoring Tools 340

10 Branding the AhsayCBS 341

Prerequisite 341
Before Getting Started 341
Prepare Branding for AhsayCBS Interface 342
Prepare Branding for AhsayOBM/AhsayACB 348
Brand the AhsayCBS Interface and AhsayOBM/AhsayACB Installers for your Resellers 364
Customize Application Name on Cloud Storages 366
Request for Permission Pages 366
Customize the Folder/Bucket name in Standard Destination 377
Customize the Storage in Predefined Destination 378

11 API 379

12 Contacting Ahsay 380

Technical Assistance 380
Documentation 380

Appendix 381

Appendix A Supported Language Code 381
Appendix B Supported Time Zone 382
Appendix C Error Code 1011 and 1012 387
Appendix D Differences between AhsayOBS v6 vs AhsayCBS v7 388

Appendix E Setting up Cloud Storage 389
Appendix F Image Specifications 414
Appendix G Comparison on Different Replication Setup Environments 458
Appendix H System Job 459
Appendix I Daily User Report 461
Appendix J System Files for Continuous Backup Exclusion 474
Appendix K Comparison Screen Shot for Quota Management between Pre-v7.15.6.0 and Post- v7.15.6.0 475

1 Overview

What is this software?

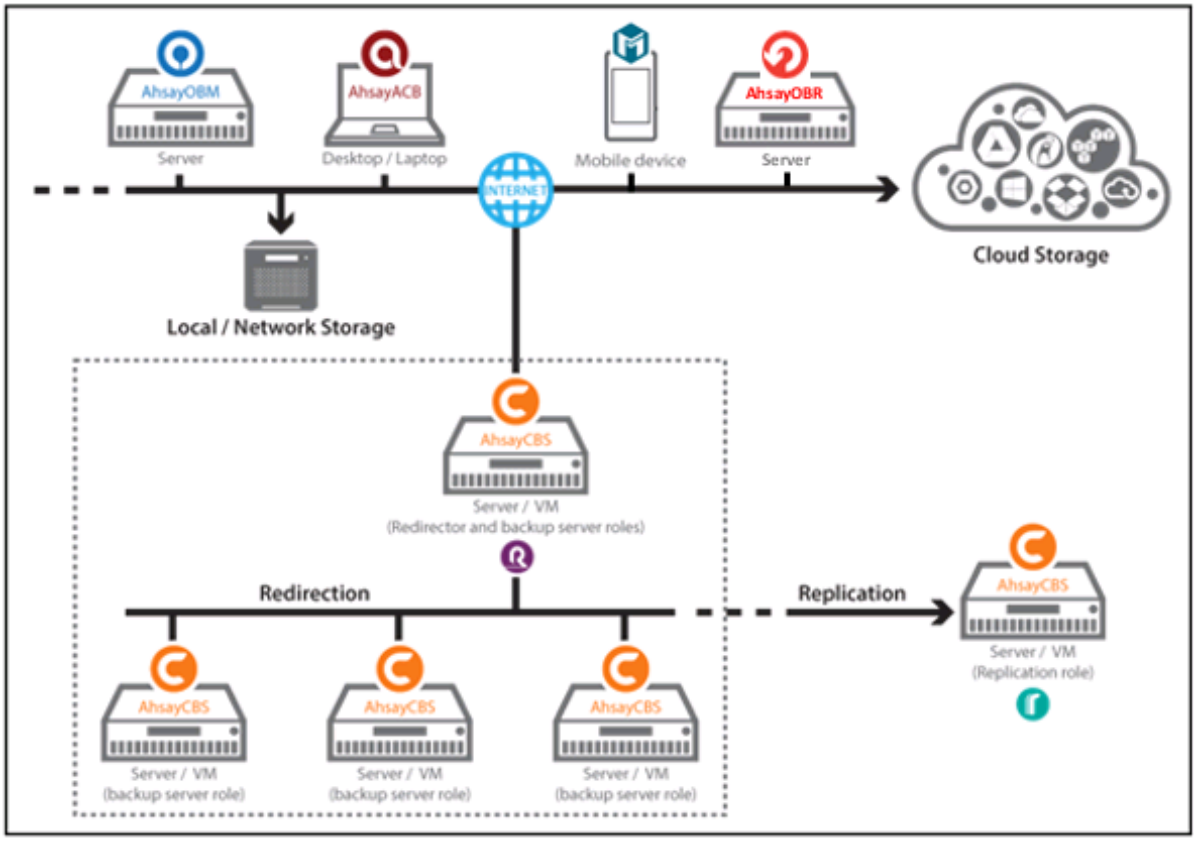
AhsayCBS is a web-based centralized management console for backup service administrators or users to manage backup and restore, and to monitor backup, restore, replication and redirection activities. Administrators can create backup user accounts, manage group policies, and keep track of system performance and health.

Administrators can create sub-admin or reseller accounts so that they can manage the backup users by themselves. In addition, non-admin operator accounts with read only permission can be created to help backup service administrator to monitor daily backup and restore jobs, as well as system activities.

To further safeguard the data hosted on the Backup Server, AhsayCBS comes with replication feature to replicate the backup data offsite to a Replication Server hosted in another site or to commercial cloud storages such as network storage, FTP/SFTP and common cloud storages (Google Drive, Dropbox, OneDrive, Amazon Drive, Box, etc.)

System Architecture

Below is a diagram illustrating the relationship among the AhsayCBS, client components and server components.



Recommendation on Antivirus Exclusion

To optimize performance of AhsayCBS on Windows, and to avoid conflict with your antivirus software, refer to the following KB article the list of processes and directory paths that should be added to all antivirus software white list / exclusion list:

FAQ: Suggestion on antivirus exclusions to improve performance of Ahsay software on Windows

NOTE

For AhsayCBS version 7.17 or above, the cbssvcX64.exe or cbssvcX86.exe processes are automatically added to Windows Defender exclusion list for Windows 10 and 2016, during installation / upgrade via installer.

AhsayCBS System Components

Client Components

Below is a brief introduction of the **three** client backup agents.

AhsayOBM is a versatile backup application that backup databases, applications and virtual machines to local and offsite destinations, e.g. local storage, on premise Backup Server or Backup Server located in datacenters, and common cloud storages (Google Drive, Dropbox, OneDrive, Amazon Drive, Box, etc.)

All the backup data are compressed and encrypted before uploading to the Backup Server, while the restore process would require downloading the compressed and encrypted data onto the client computer for decryption and un-compression.

AhsayOBM allows the creation of multiple backup sets, and backup file, 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/Notes, MySQL, Office365 Exchange Online, Cloud File, and Windows Bare Metal** with our dedicated backup modules.

Refer to the URL below to obtain the Quick Start Guide of AhsayOBM for instructions on installing the software, running a backup job and restoring backed up data.

Windows	Click to obtain the v7 Quick Start Guide
Mac	Click to obtain the v7 Quick Start Guide
Linux (CLI)	Click to obtain the v7 Quick Start Guide
Linux (GUI)	Click to obtain the v7 Quick Start Guide
Synology	Click to obtain the v7 Quick Start Guide

AhsayACB is an advanced yet easy-to-use desktop and laptop backup software for backing up files, Cloud files, Windows System backup and IBM Lotus Notes to local and offsite destinations, e.g. local storage, on premise Backup Servers or Backup Servers located in datacenters, and common cloud storages (Google Drive, Dropbox, OneDrive, Amazon Drive, Box, etc.)

All the backup data are compressed and encrypted before uploading to the Backup Server, while the restore process would require downloading the compressed and encrypted data onto the client computer for encryption and un-compression.

Refer to the URL below to obtain the Quick Start Guide of AhsayACB for instructions on installing the software, running a backup job and restoring backed up data.

Windows	Click to obtain the v7 Quick Start Guide
Mac	Click to obtain the v7 Quick Start Guide

AhsayMOB

As a comprehensive backup solution to Android and iOS mobile devices, AhsayMOB's user-friendly interface allows users to quickly configure backup settings and easily back up important data on their smartphones, such as photos, videos and contacts.

You can choose to enable or disable the backup data encryption feature according to your preference. If you choose to disable the encryption feature, some backup data (e.g. photos or videos) backed up to the cloud storage can be viewed directly from there.

Below is a table showing the supported Cloud Backup Destinations and supported Backup Data Type on both platforms.

Supported Cloud Backup Destinations		
	iOS	**Android**
AhsayCBS Storage	✔	✔
Google Drive	✔	✔
Dropbox	✔	✔
OneDrive	✔	✔
Supported Backup Data Types		
	iOS	**Android**
Photo	✔	✔
Video	✔	✔
Contact	✔	✔
Voice File	X	✔
Message (SMS)	X	✔
WhatsApp	X	✔

Refer to the URL below to obtain the User Guide of AhsayMOB for instructions on installing the software, running a backup job and restoring backed up data.

iOS	Click to obtain the User Guide
Android	Click to obtain the User Guide

Below is a brief introduction of the client restore agents.

AhsayOBR supports the restore of multiple backup sets; file, 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/Notes, MySQL, Windows System, Windows System State, ShadowProtect, Synology NAS Devices, Office365 Exchange Online, Cloud File** with our dedicated restore modules.

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 purposes. 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**	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	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
	Client Backup Agent		

		first. OpenDirect restore gives you the flexibility to restore selective file(s) quickly, so it saves you time and effort to achieve your restore goal.	take these factors in consideration when selecting this restore option.
Granular Restore	**AhsayOBR**	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 make 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.
	Client Backup Agent		
Cross platform usage	**AhsayOBR**	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.	
	Client Backup Agent		
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.

Refer to the URL below to obtain the User Guide of AhsayOBR for instructions on installing the software, running a backup job and restoring backed up data.

Windows	Click to obtain the v7 User Guide
Mac	Click to obtain the v7 User Guide
Linux (GUI)	Click to obtain the v7 User Guide

Server Components

There are **three** server components: Backup Server, Replication Server, and Redirector. You can manage these components by logging to AhsayCBS with an admin role account. The following screen shows the AhsayCBS server components.

Backup Server

The Backup Server is a platform for backup clients to perform backup to its local hard disk, network storage, FTP/SFTP and common cloud storages such as Google Drive, Dropbox, OneDrive, Amazon Cloud Drive, Amazon S3, MS Azure, Google Cloud Storage etc.

All the backup jobs, with the exception of File, VMware, and Hyper-V backup sets with either Run Direct and or Open Direct / Granular feature enabled, are compressed and encrypted before uploading to the Backup Server, while the restore process would require downloading the compressed and encrypted data onto the client computer for decryption and un-compression.

Replication Server

Replication Server offers close to real time replication of the Backup Server (backup server configuration files, user profiles & backup set settings, and backup data hosted on the backup server). So that when your production Backup Server is out of service, you can switch the Replication Server into Backup Server within a short period to reduce potential downtime of your backup service.

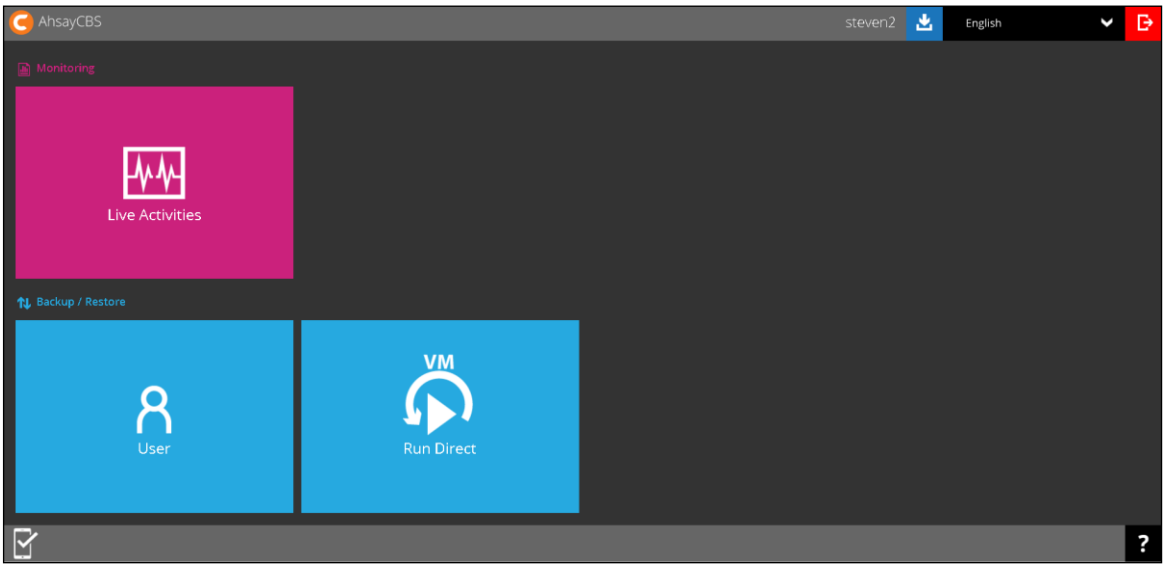
Redirector

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.

Agentless Backup / Restore

AhsayCBS v7.9.0.0 or above supports agentless backup and restore for Cloud File and Office 365 Exchange mailbox backup sets, which does not require any AhsayOBM/AhsayACB backup agents to be installed on the client machine. Instead, Cloud File and Office 365 Exchange mailbox backup or restore jobs are performed directly by the AhsayCBS server itself. For VMware ESXi/vCenter backup sets backed up to AhsayCBS, the guest VMs can be recovered using the agentless restore feature, which supports both Run Direct and Non Run Direct restores.

Below is the main user interface of the AhsayCBS (user role), also known as AhsayCBS User Web Console, where your clients login to manage their backup sets, perform the agentless backup/restore (Office 365 Exchange Online Mailbox and Cloud File backup sets), Run Direct restore for VMware ESXi/vCentre backup sets.



There are three backup sets that support agentless backup and restore in AhsayCBS v7.9.0.0 or above:

- **Cloud File Backup and Restore**

  You can now back up your data stored on Cloud storage (Google Drive, OneDrive, Dropbox, Amazon Cloud Drive, MS Azure, Google Cloud Storage, Amazon S3 etc) to the AhsayCBS or other cloud backup destination.

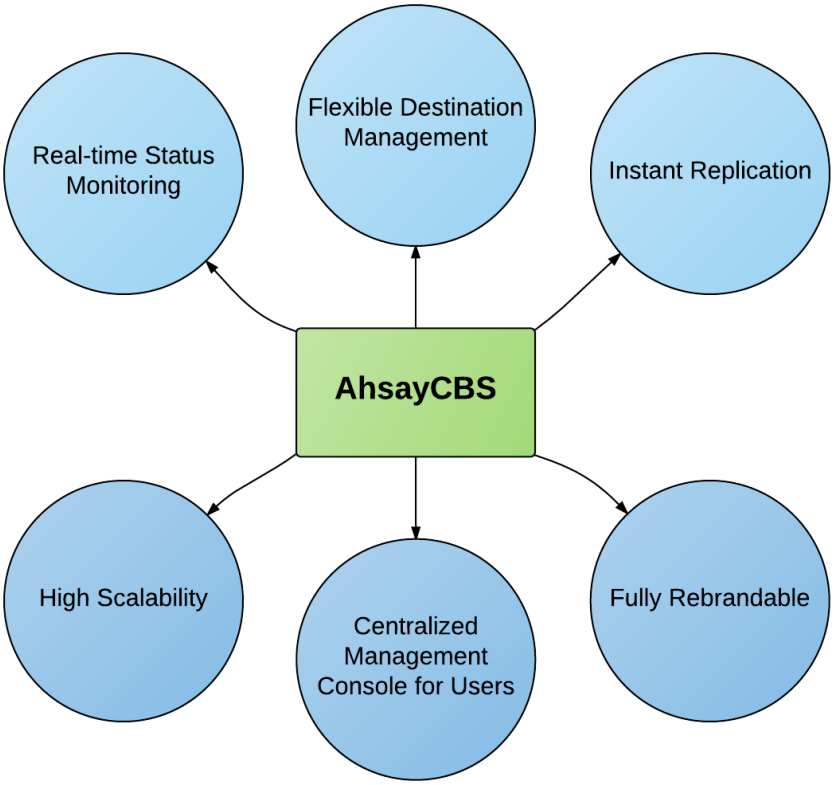
- **Exchange Online Mailbox Backup and Restore for Office 365**

  You can now back up mail objects from your Office 365 mailbox, and then restore them to your original account or another user under the same Office 365 Exchange Online account, all on the AhsayCBS without having to install a client backup agent first.

- **Run Direct of VMware vCenter/ESXi VM from AhsayCBS server**

  You can now perform a Run Direct restore of the VMware vCenter/ESXi VM directly using the AhsayCBS without the presence of a client backup agent (AhsayOBM/AhsayACB/ AhsayOBR).

Why should I use AhsayCBS to manage my backup users and system?



Real-time Status Monitoring

Monitor System Health and Backup/Restore Status, Anytime Anywhere – the AhsayCBS user interface (UI) has been designed to provide you with a user-friendly and informative view of various kinds of information you need. Highlighted features including:

- A dashboard to view the system usage and performance
- Live Activities panel to view real-time status of backup, restore, replication, redirection, etc.
- Panels to view all log files of backup, restore, replication and redirection

Flexible Destination Management

Wide range of backup destination options – to offer you with the greatest flexibility of backup destination, AhsayCBS now supports local drive, mapped network drive, FTP / SFTP server, and public cloud object storage as the backup destination for storing the backup data.

Below is a full list of the supported cloud storage:

Aliyun (阿里云) *	CTYun (中国电信天翼云)*	Amazon S3	Amazon Cloud Drive
Google Cloud Storage	Google Drive	OneDrive	Microsoft OneDrive / OneDrive for Business
Rackspace	OpenStack	Microsoft Azure	Dropbox

FTP	SFTP	AWS S3 Compatible Cloud Storage	

* Available on computers with China or Hong Kong local settings

Cloud backup gives you **two major advantages**:

- ***Multi-destination Backup for Extra Protection*** – you can now back up your database, files or data to both local drive and cloud destination. While local destination backup gives you the convenience of faster backup and restore as a result of the local infrastructure, you can take a further step to utilize the cloud backup to give you an extra layer of protection in the event of a local drive corruption, where you will still be able to retrieve data from the cloud destination.
- ***Eliminate Hardware Investment*** – with the increasingly affordable cloud storage cost, you can deploy on cloud platform and utilize cloud storage as your centralized data repository, or simply expand your cloud storage as a backup destination without having to invest on hardware.

Instant Replication

Extra layer of data protection – the replication server provides an additional layer of data protection by providing an offsite backup store for backing up data from either a single or multiple AhsayCBS servers. The Ahsay replication process is close to real-time and hence this will reduce the probability of significant data loss in the event of an AhsayCBS outage. The synchronization process does not require stopping or interrupting any backup operations. As the replication module will be replicating the backup data using four modes, pending, resync, replay, and sleep mode.

Furthermore, you have flexibility to select specific user's backup set from the backup server to replicate instead of replicating all users and backup sets. The replication speed has been enhanced by utilizing the multiple thread replication technology.

Refer to the Replication section for further details.

High Scalability

Easy system expansion for your business growth – as your business continues to grow, you need greater storage and backup capabilities to keep all your data safe and protected. With AhsayCBS, you can always scale up your backup service. With the program's built-in redirection module, you can redirect the extra user traffic to other AhsayCBS servers to manage your growing volume of data easily.

We understand that expanding backup service could be a difficult situation when you have to deal with multiple domain servers, a high scalable backup system should make this kind of transition as seamless as possible to users. Our Redirector is designed to facilitated easy expansion of your backup service.

Refer to the Configuring Redirector section for further details.

Fully Rebrandable

Rebrand and customize to best cater your clients' needs – All graphics and wordings in AhsayCBS are rebrandable and customizable for MSPs. Thus, you can use a rebranded AhsayCBS to build your branded backup appliance for customers who preferred on-site backup solution.

Centralized Management Console for Users

Monitor and Manage Backup without Client Backup Agent – our enriched features on the centralized web console offers users a one-stop location for running and configuring backup jobs, monitoring backup and restoring activities, and initiating a Run Direct restore.

For further instructions on using the User Web Console, refer to the Ahsay CBS User Guide.

2 About this Document

What is the purpose of this document?

This document aims at providing all necessary information for you to work with the AhsayCBS server at the administrator level to manage backup and restore jobs.

What should I expect from this document?

After reading through this documentation, you can expect to have sufficient knowledge to perform all administrative tasks and manage your AhsayCBS server effectively.

Who should read this document?

This documentation is intended for IT professionals who need to work with AhsayCBS server at the administrator level.

Where can I get information about System Requirements and Settings for installing the AhsayCBS?

Before you read through this Administrator's Guide for information on managing all administrative tasks on AhsayCBS, you should have the AhsayCBS installed first. Refer to the Ahsay Cloud Backup Suite Quick Start Guide for instructions on software installation, system requirements, network, and firewall settings.

3 Log in to AhsayCBS Server

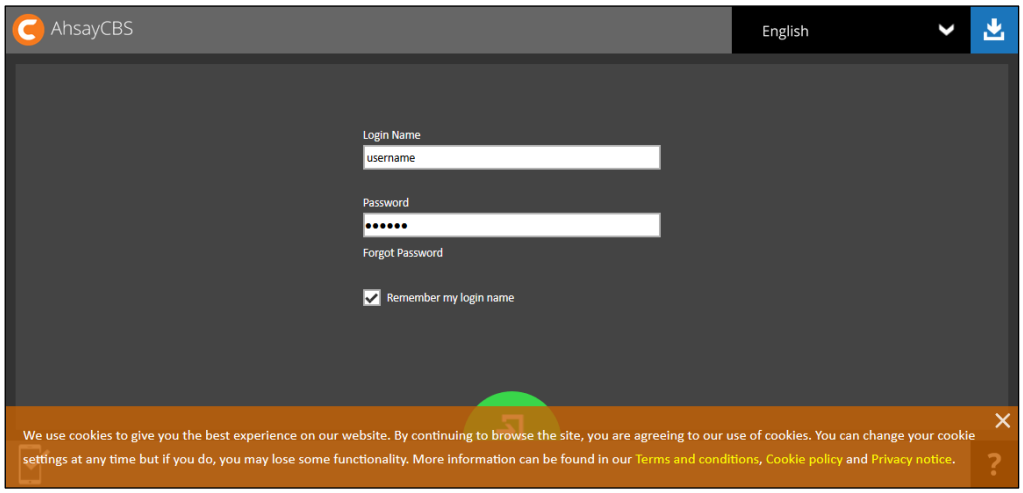
Log in to AhsayCBS Web Management Console

1. Enter the IP address or domain name on a web browser.
   https://<IP_Address:port_number/>

2. Enter the system **login name** and **password.** The default login credential are:

   Login Name: system

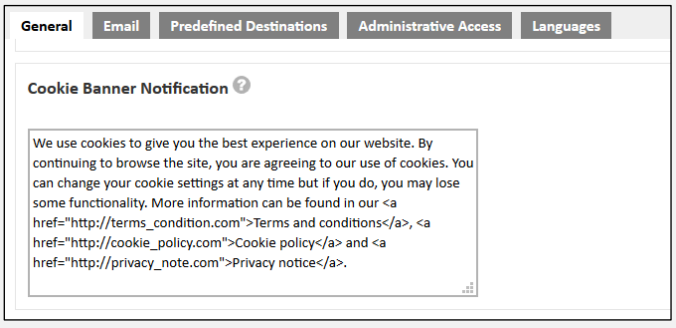
   Password: system



NOTE

Please kindly note that to comply with the new General Data Protection Regulation (GDPR) requirements, there will display a banner stating the organizations cookie policy when processing to login AhsayCBS server. This will also apply to the AhsayCBS web console.

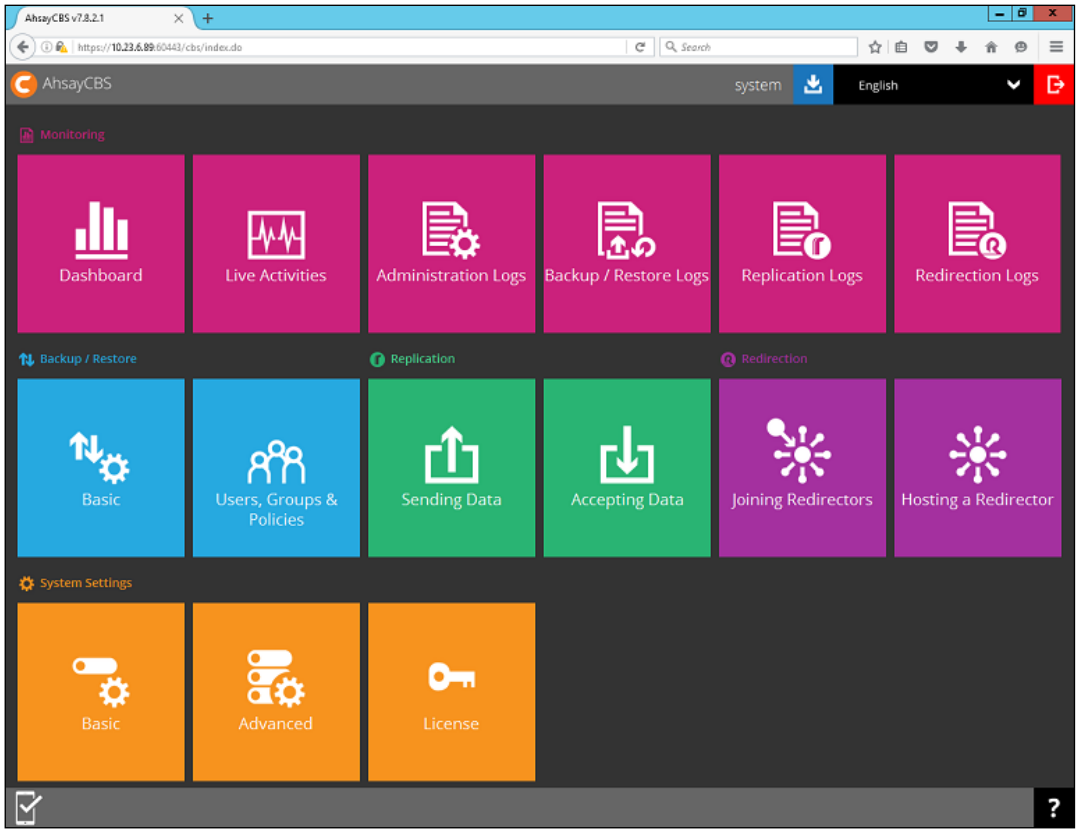
From AhsayCBS version 7.15.6.0 onwards, administrator can configure a notification banner to be displayed on the AhsayCBS web console (displayed at the login interface), and the contents of the banner can be configured on the AhsayCBS web console at “System Settings > Basic > General > Cookie Banner Notification”.



HTML codes can be used for content of the banner.

3. Click the green **Login** button to login.

4. The following screen appears with five sections: **Monitoring**, **Backup / Restore**, **Replication**, **Redirection**, and **System Settings**. Each of these sections are described in detail in later chapters.



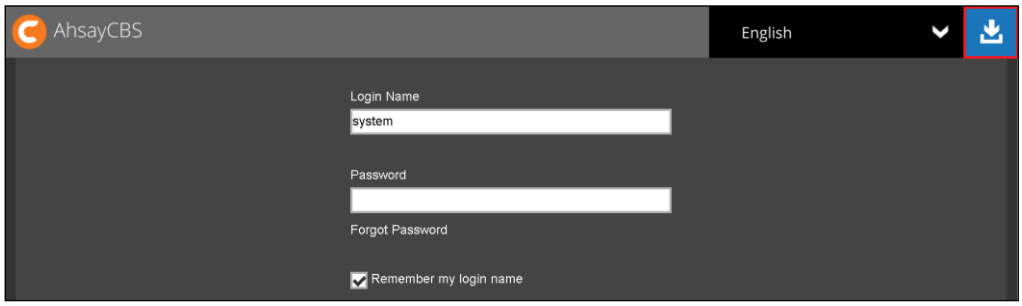
Forgot your Password?

If you have forgotten your system or administrator password, please refer to the following KB article for instructions. **FAQ: How to recover AhsayCBS system account password? (5122)**

Download Client Backup Agents

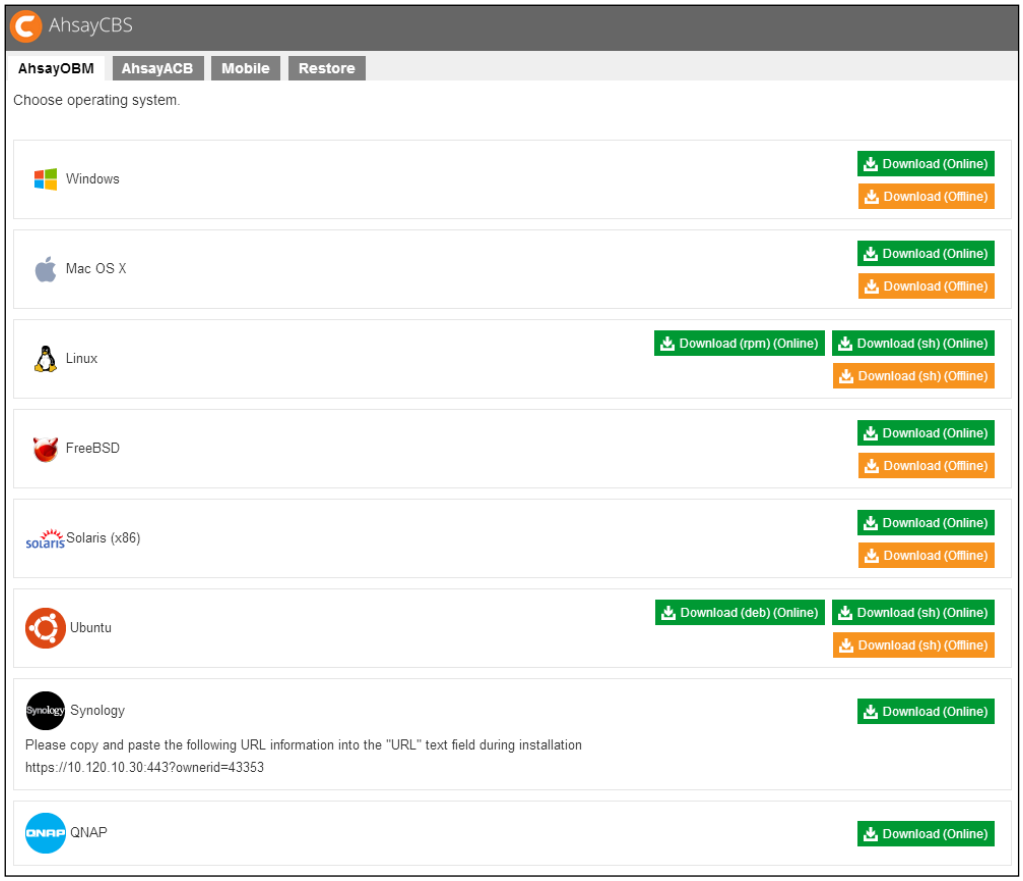
You can choose the client software you wish to download as follows.

1. On the AhsayCBS Logon page, click the download arrow on the top right hand corner.

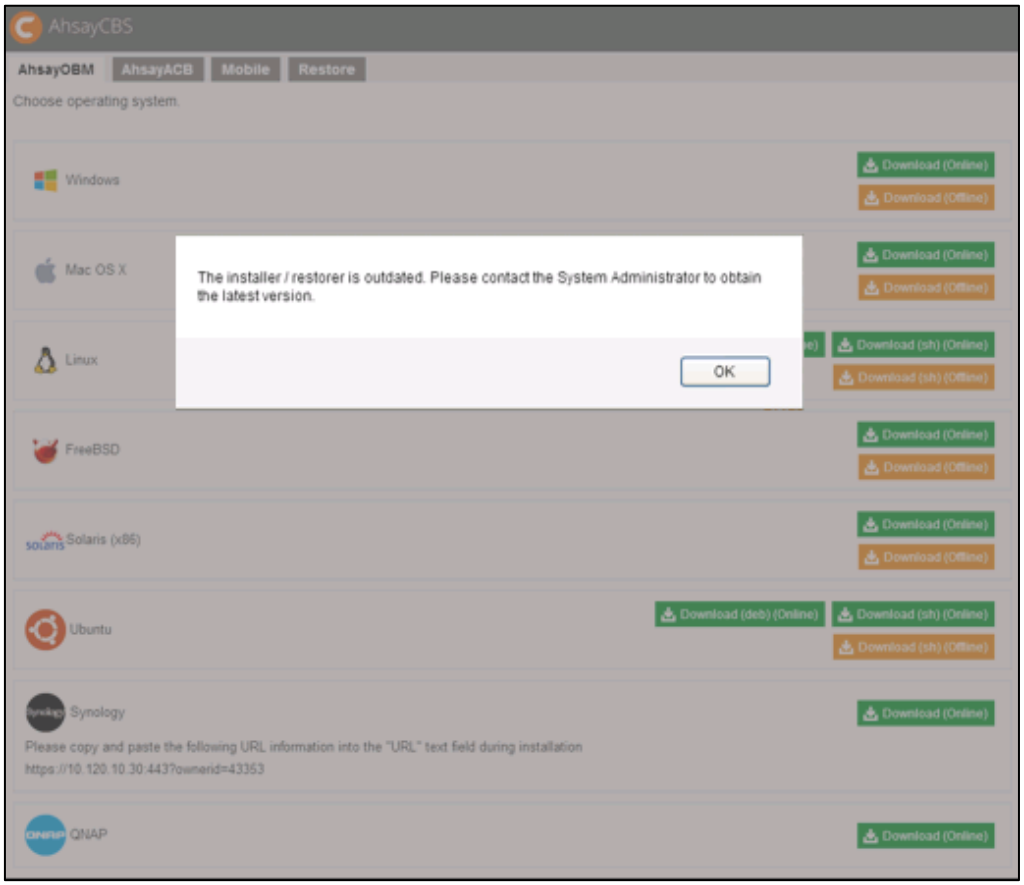


2. Click on the tab with the name of the client backup agent you wish to download.

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



Please kindly note that each time after upgrading AhsayCBS version, it is required to rebuild the installers. Otherwise, you cannot download the installer and following warning will prompt.



From v7.15.0.0 onwards AhsayCBS support two installation modes, online and offline installation (except for Linux (rpm), Ubuntu (deb) and AhsayMOB which supports online installation only). User can download and run either one of the installers.

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.	➢ Once the offline installer is downloaded, the client does not require an

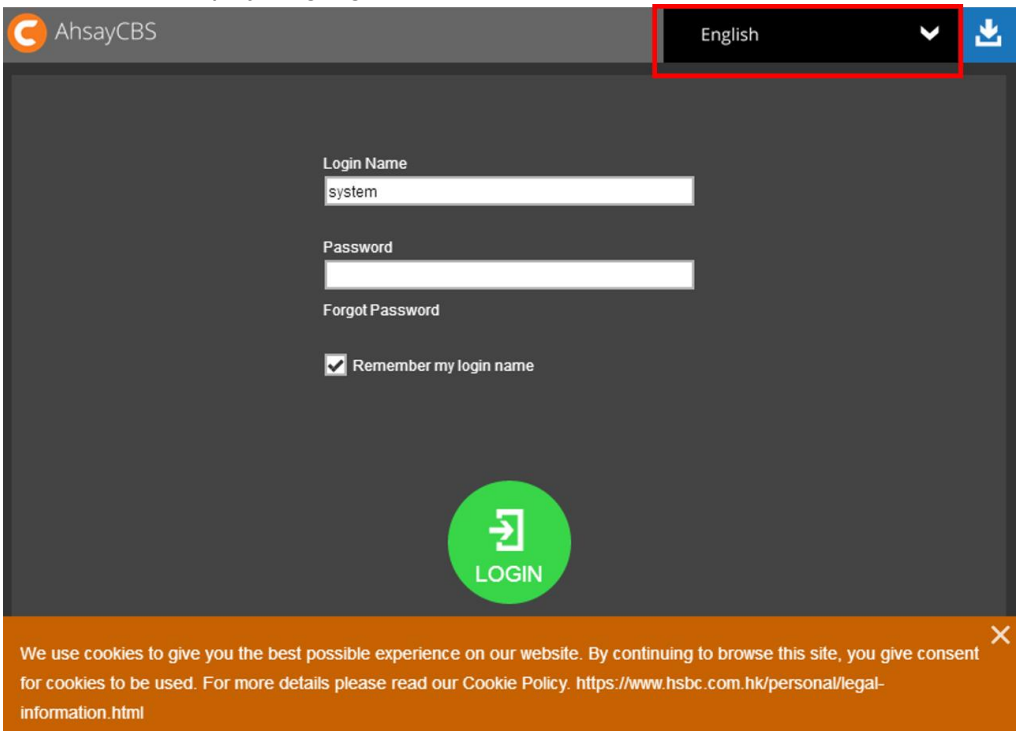
	➢ Clients need to have an internet connection each time an installation is run. ➢ If the client internet connection is interrupted or is not stable the installation may be unsuccessful. ➢ Online installer size is 6KB to 3.5MB depending on operating system as it contains only the initial installation package files.	internet connection each time an installation is run. ➢ The offline installer size is 80MB to 140MB depending on operating system as it contains all 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 component files are already available in the offline installer.
Version Control	Online installation 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.

For instructions regarding installation of the client backup agent, refer to the Client Components section for the URL to obtain the Quick Start Guide.

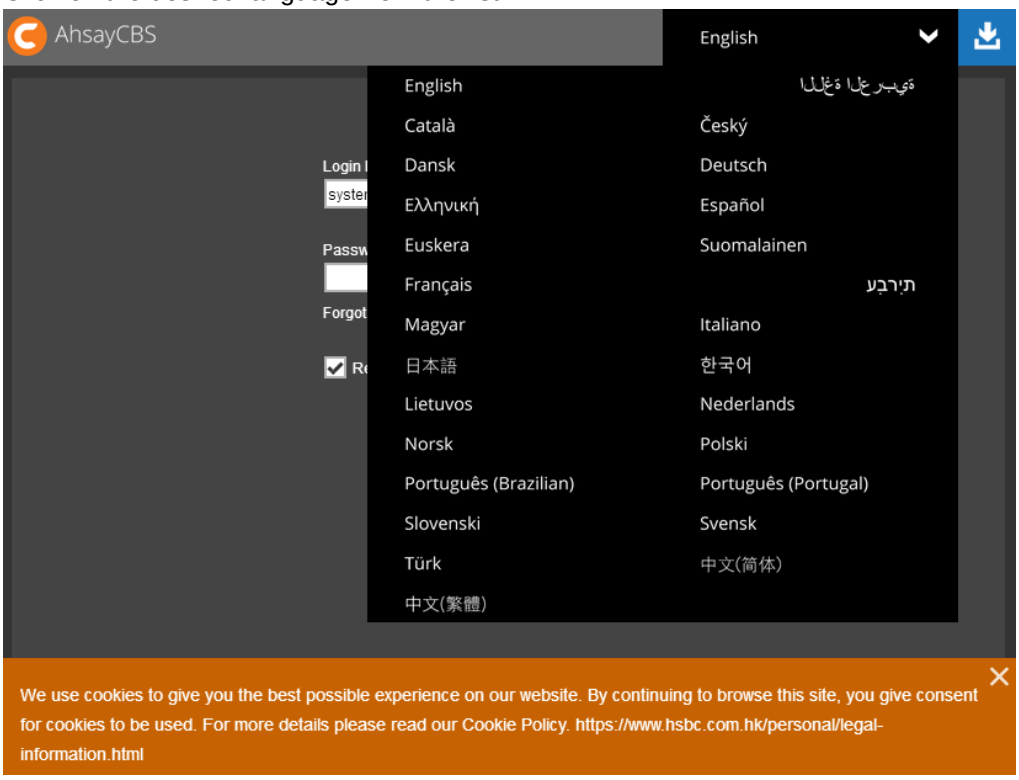
Change the Language

You can change the language shown on AhsayCBS web console

1. To change the display language, click on the dropdown box on the top right of the screen to select another display language.



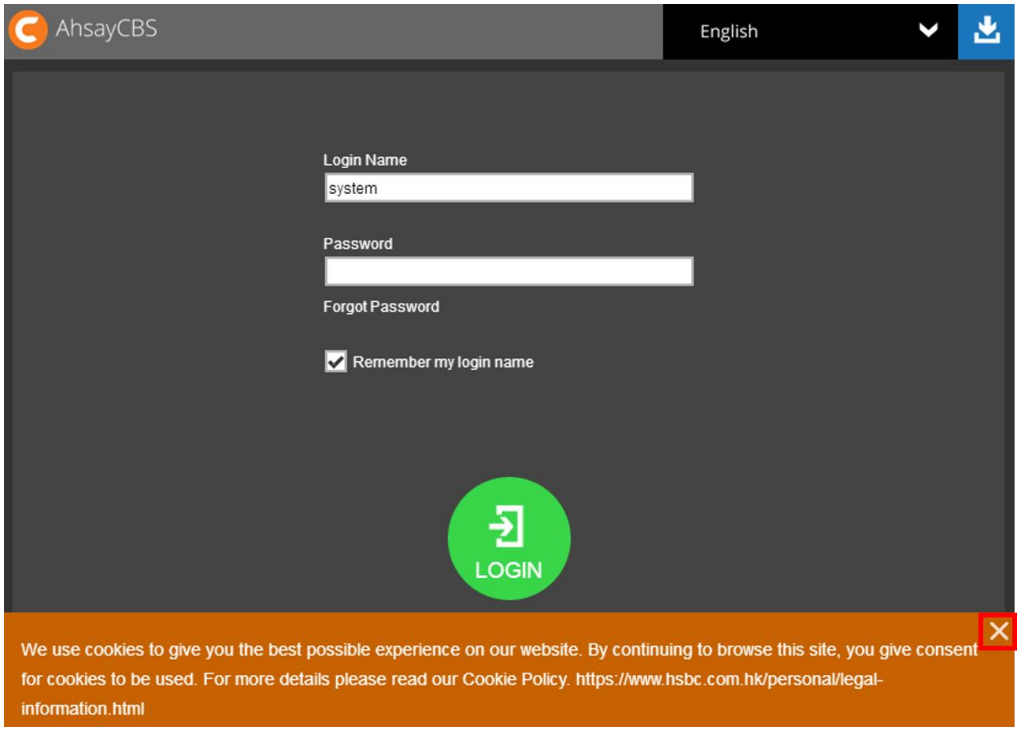
2. Click on the desired language from the list.



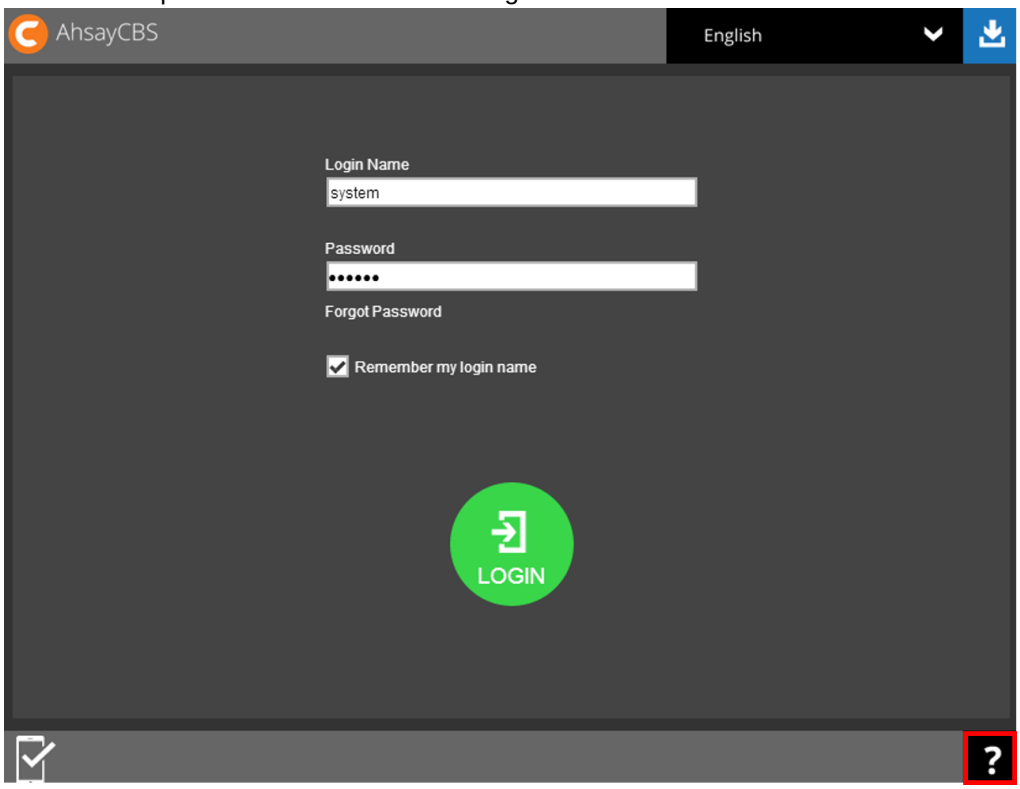
Invoke Online Help

You can invoke the online help on most of the pages while navigating the AhsayCBS. The online help aims at providing instructions on operation on the corresponding page.

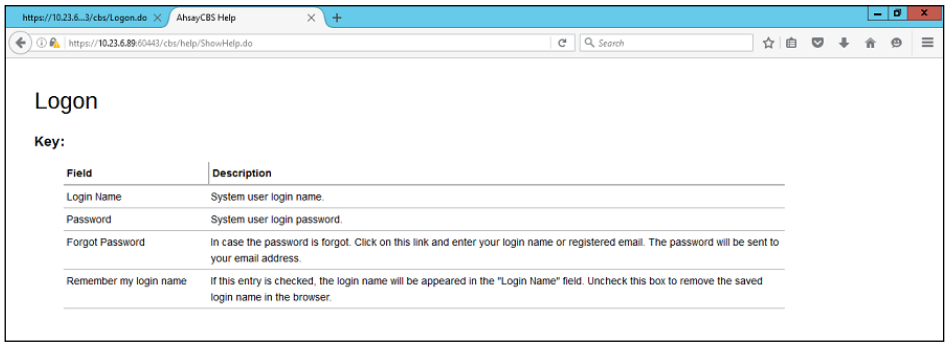
1. Click **X** to shut down the banner.



2. Click on the question mark at the bottom right corner.



3. The corresponding online help page shows.



4. You can print the online help by clicking the print button at the bottom right corner. To exit, click **X**.

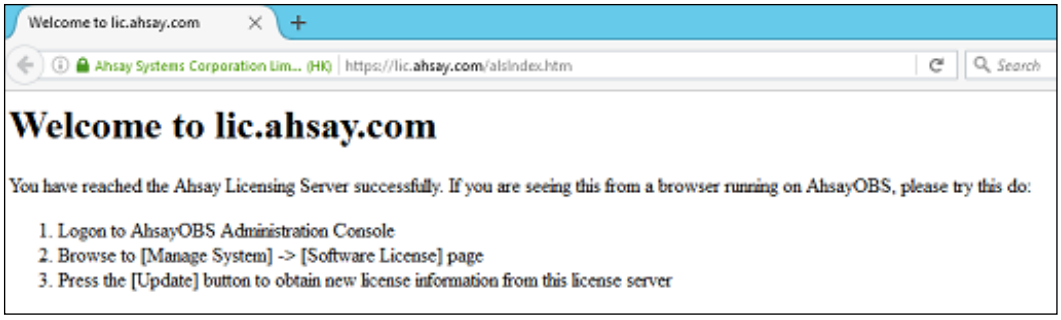
4 Managing License

Verify License Connectivity

The AhsayCBS server is required to access the Internet and to connect to the Ahsay License Server (lic.ahsay.com) using https protocol for license activation, daily license checks, and license CAL updates. Make sure your firewall settings are configured to allow outbound connections to lic.ahsay.com via port 443 using TLSv1.

To verify Ahsay license connectivity you can either:

- Open a web browser on your AhsayCBS and enter the following URL https://lic.ahsay.com the following message is displayed when the connection is successful.



-OR-

- Use the **telnet** command to check the connection on your AhsayCBS server.

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

Use the **openssl s_client** command to check whether TLSv1 is enabled.

```
# openssl s_client -connect lic.ahsay.com:443 -tls1
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, ST = Hong Kong, L =
Kowloon, 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/ST=Hong
Kong/L=Kowloon/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-----
MIIIATCCBumgAwIBAgIJAPwOHyVgUxkXMA0GCSqGSIb3DQEBCwUAMIG0MQswCQYD
VQQGEwJVUzEQMA4GA1UECBMHQXJpem9uYTETMBEGA1UEBxMKU2NvdHRzZGFsZTEa
MBgGA1UEChMRR29EYWRkeS5jb20sIEluYy4xLTArBgNVBAsTJGh0dHA6Ly9jZXJ0
cy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5LzEzMDEGA1UEAxMqR28gRGFkZHkgU2Vj
dXJlIENlcnRpZmljYXRlIEF1dGhvcml0eSAtIEcyMB4XDTE2MDQyMjAzMDAzOFoX
DTE4MDQxNTAzMjMzOFowgbkxEzARBgsrBgEEAYI3PAIBAxMCSEsxHTAbBgNVBA8T
FFByaXZhdGUgT3JnYW5pemF0aW9uMRAwDgYDVQQFEwcwNDk4ODI1MQswCQYDVQQG
EwJISzESMBAGA1UECBMJSG9uZyBLb25nMRAwDgYDVQQHEwdLb3dsb29uMSowKAYD
VQQKEyFBaHNheSBTeXN0ZW1zIENvcnBvcmF0aW9uIExpbWl0ZWQxEjAQBgNVBAMT
CWFoc2F5LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1cvjg+
GpaWn18IjmBCkIpDRWzL7tocrB7+reoN619nQTq7W6AlsD/UWTldoOMeQyEWY+3b
kdsI4QGNB2hNwzd36+k5yxST8IPuyGE7eLHe6L7RyQxNT3BLos48i9pOl0cXKEWo
08wDFw0y2bMiTbkTTErrGk1VqR8oYKV5Pg9RYDoNg2j6I7mCz1v05KJWxTL49PAQ
TmKmK3EX1esvkss9Pz3mfhm/fpJFQfhT+KSTA8b/75RbW2pCQyKW7a9NVX4Iyx6o
dIDDAU568bAV6y74b9hh4ty6+0zSW+x3+CQLPXEd8NJJCtXAitb78qJENkDSxGMH
sW4vuEDKX6UF3f8CAwEAAaOCBA0wggQJMAwGA1UdEwEB/wQCMAAwHQYDVR0lBBYw
FAYIKwYBBQUHAwEGCCsGAQUFBwMCMA4GA1UdDwEB/wQEAwIFoDA1BgNVHR8ELjAs
MCqgKKAmhiRodHRwOi8vY3JsLmdvZGFkZHkuY29tL2dkaWcyczMtNC5jcmwwXAYD
VR0gBFUwUzBIBgtghkgBhv1tAQcXAzA5MDcGCCsGAQUFBwIBFitodHRwOi8vY2Vy
dGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMAcGBWeBDAEBMHYGCCsG
AQUFBwEBBGowaDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20v
MEAGCCsGAQUFBzAChjRodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3Jl
cG9zaXRvcnkvZ2RpZzIuY3J0MB8GA1UdIwQYMBaAFEDCvSeOzDSDMKIz1/tss/C0
LIDOMIH5BgNVHREEgfEwge6CCWFoc2F5LmNvbYINd3d3LmFoc2F5LmNvbYIOc2hv
cC5haHNheS5jb22CEHd3dy51ay5haHNheS5jb22CFXBhcnRuZXJzLmFoc2F5LmNv
bS5jboINbG1wLmFoc2F5LmNvbYIVcGFydG5lcnMtdXMuYWhzYXkuY29tgg1wY3Au
YWhzYXkuY29tghVwYXJ0bmVycy11ay5haHNheS5jb22CDWlkcC5haHNheS5jb22C
DGtiLmFoc2F5LmNvbYIQd3d3LmFoc2F5LmNvbS5jboIPZm9ydW0uYWhzYXkuY29t
gg1saWMuYWhzYXkuY29tMB0GA1UdDgQWBBQU/GniKbSMjgEmaqndKdtzS0DqlDCC
AX8GCisGAQQB1nkCBAIEggFvBIIBawFpAHcAVhQGmi/XwuzT9eG9RLI+x0Z2ubyZ
EVzA75SYVdaJ0N0AAAFUO+sXggAABAMASDBGAiEA3hPo2F1QZZX75QIRGFlMbspW
n8MlmeM8k1TCYmHDie8CIQC0Eg8Z9duyg6RvYBT7ahtQ8eojA/7GsOpBoZKXDoK1
NAB1AGj2mPgfZIK+OozuuSgdTPxxUV1nk9RE0QpnrLtPT/vEAAABVDvrGT0AAAQD
AEYwRAIgbj3ZWvwZL75Zx1Vd1sC4ZSZhAN1TfaIlecBS9Ie4K3ICICKTx2OTGWHO
spDVowj59LSWHDG5Z9c1B/bs9sRl5nUcAHcApLkJkLQYWBSHuxOizGdwCjw1mAT5
G9+443fNDsgN3BAAAAFUO+scaAAABAMASDBGAiEA5MdV9o+iN4ecJnjCgA0qxhno
Mm5+9s5JUX+oKknk5pkCIQDwDkuAEcjEM4vouxZzAtqcozWikMJoTFn++vIFbrEZ
SzANBgkqhkiG9w0BAQsFAAOCAQEAcKpSovHqtpyAx5bKyXQRRh8Fyo/WTA0eBMc1
5KpgII49V6/ww1e6rmbMa3xVKqNEnjH4GaqGY2AZAx9iVr+NN+VFNroPUGqzpJ0B
ih9tLl/VCV/lvy67Chs7NHv3D1AEsrKJYUqpl0sQy/QhSIRAAa3bY8i7+MOfEYJt
ADa+254k6G19s99PvmBniepxuUy8x/9h7h7K4m+OIgXQaLXE6lr4LG50p/GOKx/I
```

```
1feC6RUCx8gW9qBoTTl7M6o8Jb/SXUN6/mAVsronEG+yyqNXCcUQwNpaKJK5hMkz
0EbBq1tS/VyTtW9z0g4vA1PQrgaqCLG/ZJIvBESf8wvsgfZNpA==
-----END CERTIFICATE-----
subject=/1.3.6.1.4.1.311.60.2.1.3=HK/businessCategory=Private
Organization/serialNumber=0498825/C=HK/ST=Hong
Kong/L=Kowloon/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 6160 bytes and written 289 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : ECDHE-RSA-AES256-SHA
    Session-ID:
6914212983C0321AB9520FFC6E7515845D8836D7B185EF1D2363D3C7EAA85D48
    Session-ID-ctx:
    Master-Key:
79BECEF9E2C3088F4928229047A21BE9E9239C32D2F79B4DB4FC7CF66098423D0
EF0D64741E3075AEA62E9222D6DD4B2
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - 8c 55 8e c3 19 9a 34 14-63 67 66 aa 49 7b c9
41    .U....4.cgf.I{.A
    0010 - 3f 03 db c1 ec f9 db e1-b6 eb 4f 51 0c 3a 83
9b    ?.........OQ.:..
    0020 - 73 20 93 c1 41 6e 5a ac-f5 65 92 4f b8 92 fb ef
s ..AnZ..e.O....
    0030 - 2b 3d f7 f3 03 c8 3a b5-1b 52 9a 5a 43 ba 0a 7d
+=....:..R.ZC..}
    0040 - 47 e8 6a 22 72 85 9d d2-f1 dd 9d 6d b5 65 8a 0a
G.j"r......m.e..
    0050 - 30 26 1b d9 55 8c 25 65-71 0b a5 1f 57 38 2b 71
0&..U.%eq...W8+q
    0060 - 81 f1 c0 4e bd 51 d3 43-b5 41 40 8f 71 3c 72
8d    ...N.Q.C.A@.q<r.
    0070 - 5a c8 70 72 38 47 a0 b0-4a cd 8b e3 10 48 0c 2e
Z.pr8G..J....H..

    0080 - 44 a9 48 9e df 56 7a 9f-e5 00 f4 37 f2 59 ee 2f
D.H..Vz....7.Y./
    0090 - eb 3a 33 7b 1e 26 09 d9-cd a4 d8 2e 30 51 80
1a    .:3{.&......0Q..
    00a0 - 72 78 ae 0a a8 48 bd 0a-ca 16 23 8a e9 44 db ce
rx...H....#..D..

    Start Time: 1503557290
```

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

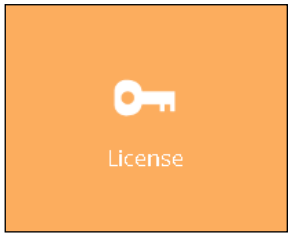
NOTE

A single license key can only be used on one machine once it has been activated. If you use the same license key to activate another installation of AhsayCBS, you will get an error message. You would be able to run this copy of AhsayCBS for another 14 days. After the 14-day grace period has expired, the AhsayCBS service will stop working completely. Please contact Ahsay Support for further assistance.

Manage License Key

To manage your AhsayCBS backup server and redirector license keys, do the following:

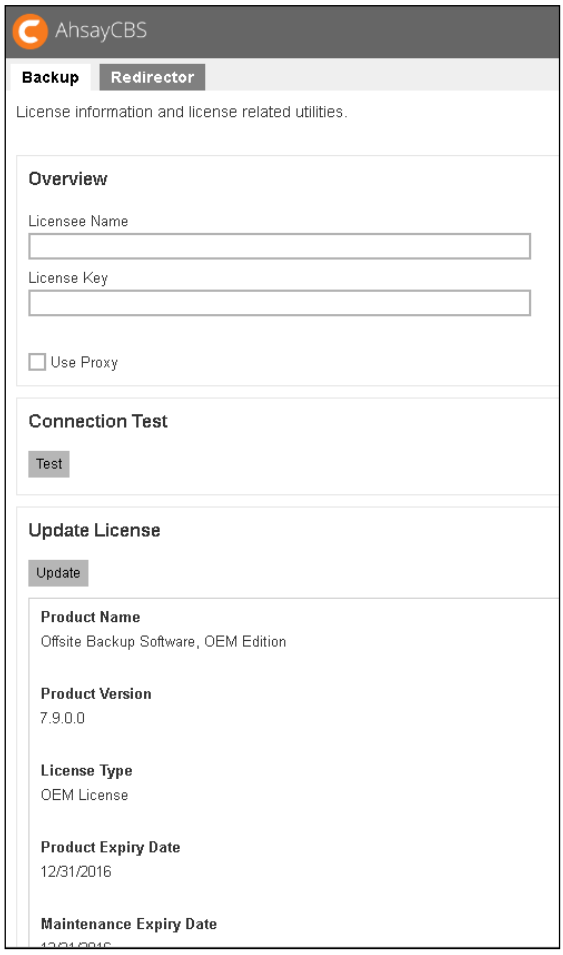
1. Click the **License** icon under **System Settings** from your AhsayCBS web management console.



2. There are two tabs on the license page. The **Backup** tab is for backup server license, while the **Redirector** tab is for redirector license. You can activate the software on these tabs.

   Please make sure that the AhsayCBS license key is applied on the **Backup** tab. If you have purchased a Redirector license key, you need to enter the key in the **Redirector**

tab. Do NOT enter the AhsayCBS license key on the **Redirector** tab or vice versa.

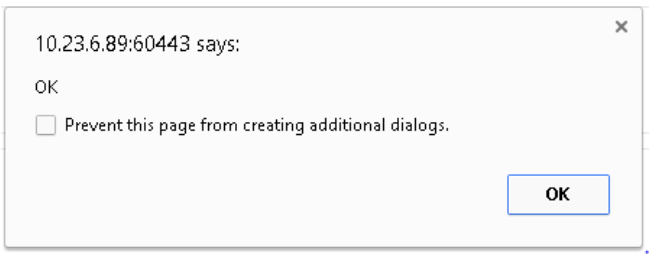


3. Enter your **Licensee Name** and **License Key** on the Backup server license page. Both fields are case sensitive. Please enter them exactly as stated in your software receipt.

   - If you are using the evaluation license, you will be able to evaluate the AhsayCBS for 60 days. Just accept the default **Licensee Name** and **License Key** on the page to activate the license.
   - If you have already purchased a license, copy and paste the licensee name and license key into the relevant fields to activate the license.

4. If a proxy server is required to access the Internet from AhsayCBS, check the **Use Proxy** checkbox. Refer to the Proxy Tab section for information on how to set up the proxy server.

5. Press the **Test** button under **Connection Test** section to test the connection with the license server. You get a dialog box with the testing result. Click **OK**.

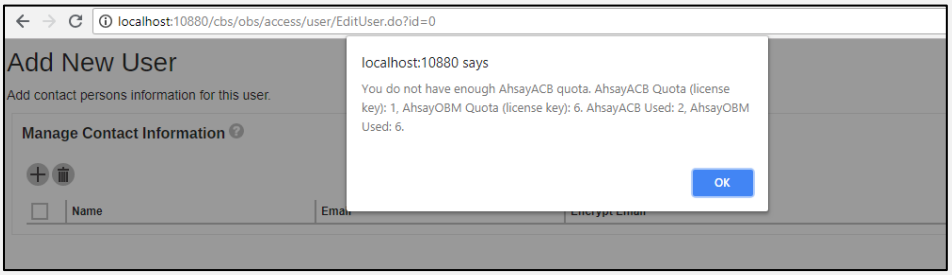


NOTE

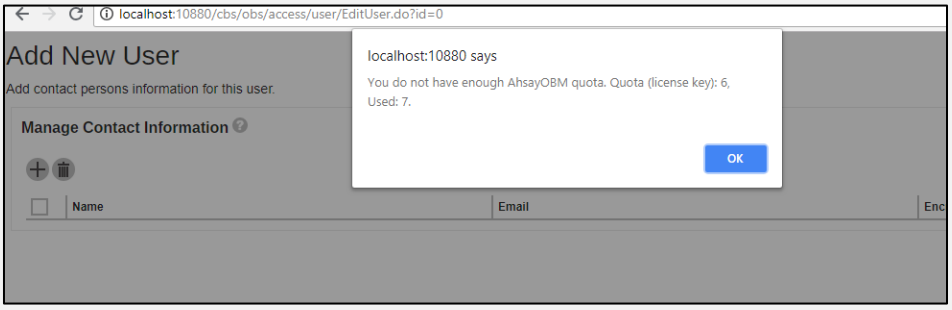
After upgrading AhsayCBS to v7.17.0.0. and above, any actions that may lead to quota exceeded will be blocked, i.e. generate a new backup user, creating a new backup set from AhsayCBS or v6/ v7 AhsayOBM/ AhsayACB, importing users in AhsayCBS, updating licnese in AhsayCBS, update user, and so on. If there is any license error, there will be email to alert about the license error.

Below screenshot shows about blocked actions:

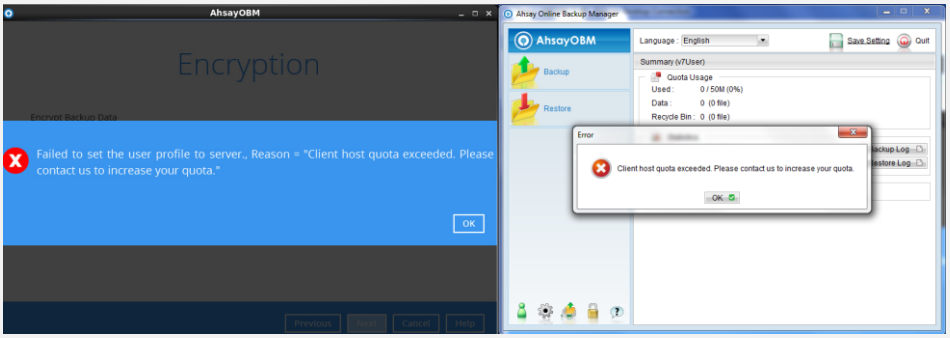
- Generate a new AhsayOBM user.



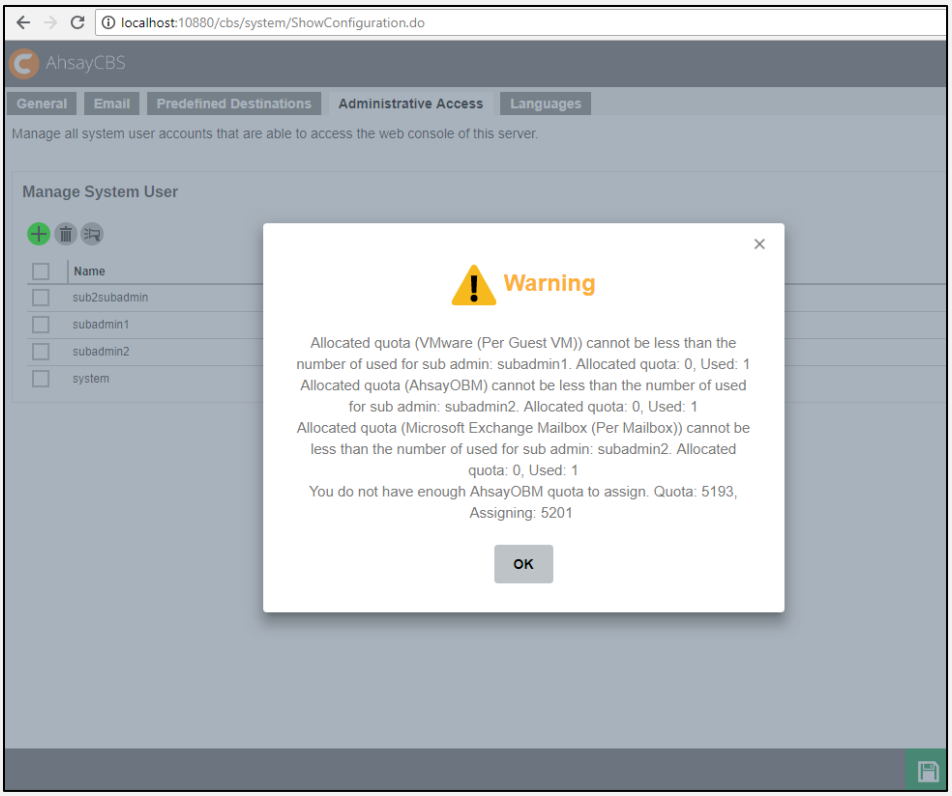
- Gnerate a new AhsayACB user.



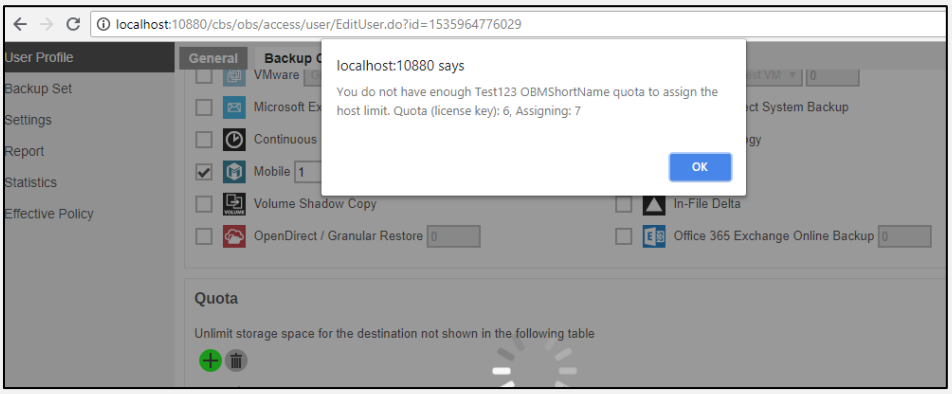
- Create a new backup set from AhsayCBS or v6/ v7 AhsayOBM/ AhsayACB.



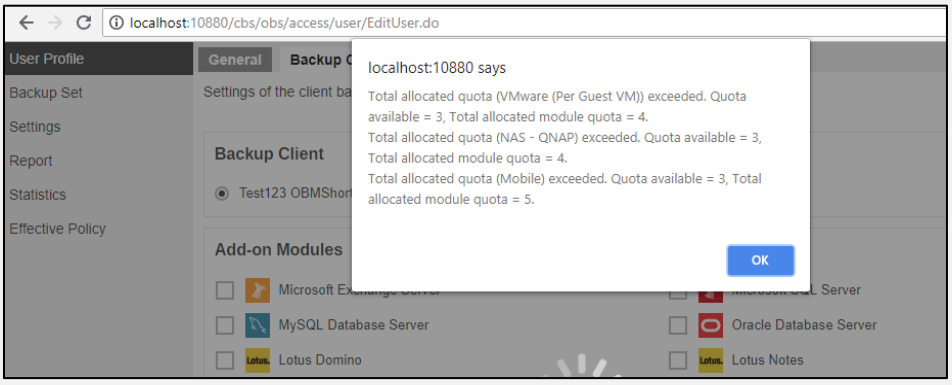
- AhsayCBS license quota assigned for each sub admin user beyond the range between sub admin user's current usage and license quota limit.



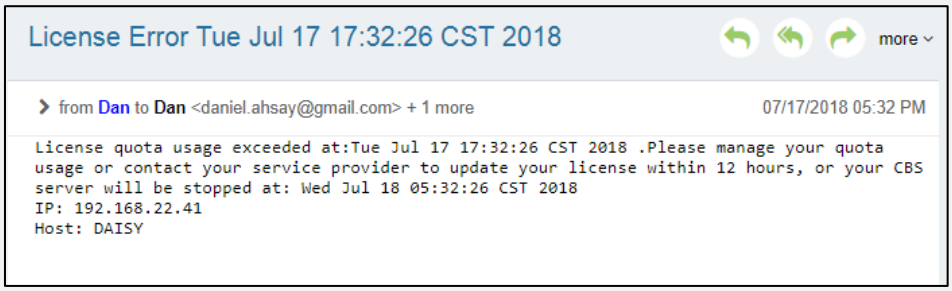
- Update user with max host limit beyond license quota.



- Update user with module quota exceeded.

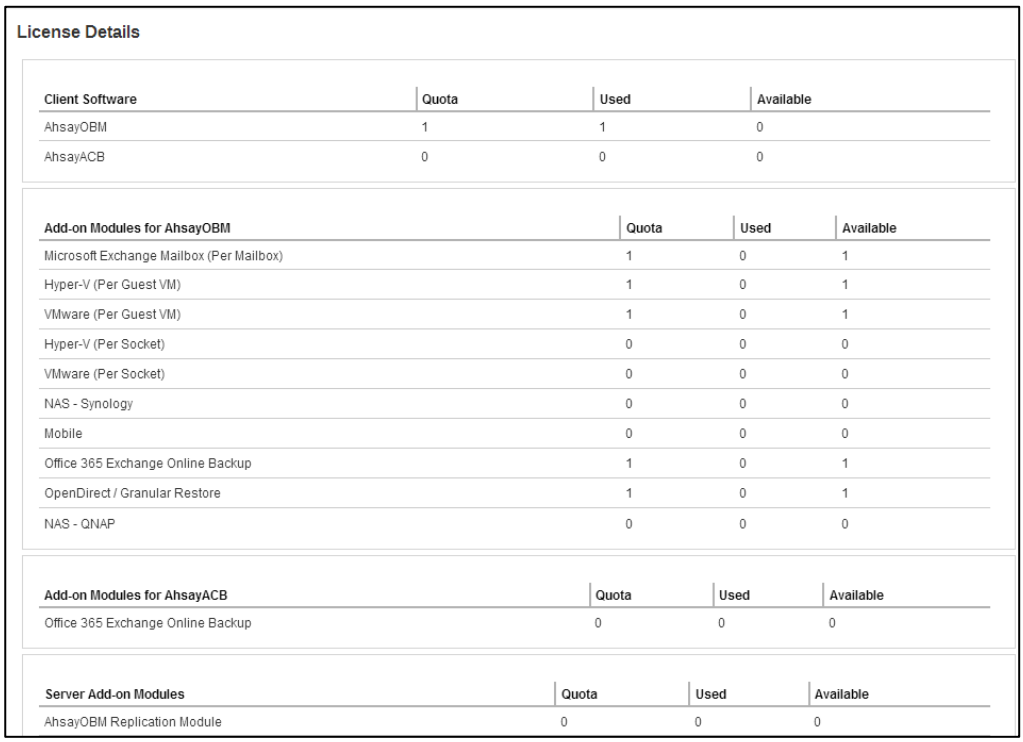


Below screenshot shows about email alert:



License Summary and Requirements

The **License Details** section on the Backup Server license page shows a summary of the quota used and licenses available for each of the modules you have subscribed.



License Details

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

Add-on Modules for AhsayOBM	Quota	Used	Available
Microsoft Exchange Mailbox (Per Mailbox)	1	0	1
Hyper-V (Per Guest VM)	1	0	1
VMware (Per Guest VM)	1	0	1
Hyper-V (Per Socket)	0	0	0
VMware (Per Socket)	0	0	0
NAS - Synology	0	0	0
Mobile	0	0	0
Office 365 Exchange Online Backup	1	0	1
OpenDirect / Granular Restore	1	0	1
NAS - QNAP	0	0	0

Add-on Modules for AhsayACB	Quota	Used	Available
Office 365 Exchange Online Backup	0	0	0

Server Add-on Modules	Quota	Used	Available
AhsayOBM Replication Module	0	0	0

Client Software	License quota and availability for client backup agents (AhsayOBM & AhsayACB)
Add-on Modules for AhsayOBM	License quota and availability for add-on modules for AhsayOBM Click here to view a list of all available add-on modules
Add-on Modules for AhsayACB	License quota and availability for add-on modules for AhsayACB Click here to view a list of all available add-on modules
Server Add-on Modules	License quota and availability for server add-on modules, e.g. Replication module, AhsayUBS, AhsayCBS, etc.

VMware Backup Module	Per Guest VM to back up or Per CPU socket
Hyper-V Backup Module	Per Guest VM to back up or Per CPU socket
Support Languages	Supported languages for UI display. The availability of support languages is subject to your license key. For license related inquiries, please contact the Sales team at Ahsay by email at sales-kb@ahsay.com or call our International Sales Hotline +852 3580 8091.

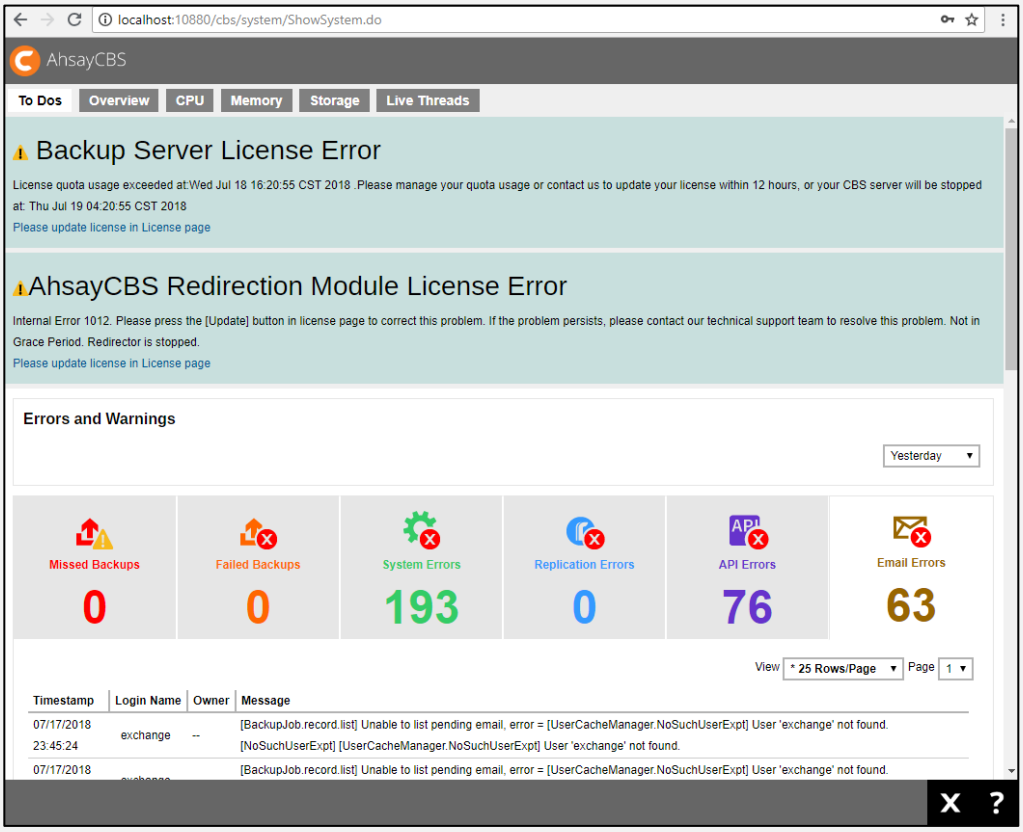
Upgrade from v6 to v7

Since the AhsayCBS license module is introduced in version 7, if you are upgrading from v6, you need to purchase one extra AhsayCBS license module for each of your existing v6 backup server license. Make sure you have valid maintenance before you perform the upgrade/migration.

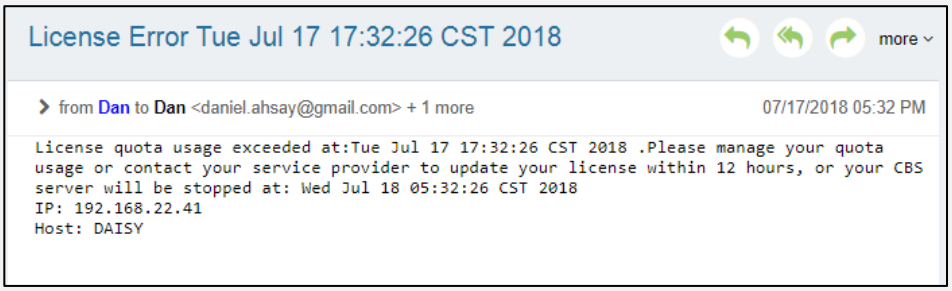
NOTE

If upgrade AhsayCBS from v6 to v7 without purchasing AhsayCBS module and the quota exceeded, then there will be a grace period of 60 days to allow sufficient time to resolve the license related problems.

If upgrade AhsayCBS from v6 to v7 with purchasing AhsayCBS module and the quota exceeded, then there will be a grave period of 12 hours for you to manage the quota usage. If quota usage issue was not solved within grace period, the server will be stopped after the grace period. After login AhsayCBS system console, the web console will redirect to [To Do] page and the license error will be shown on the top.

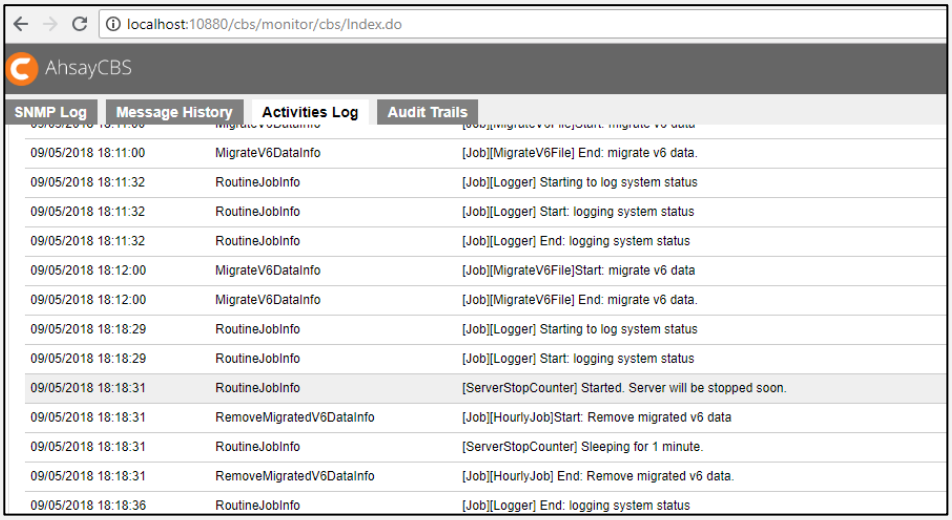


If there is any license error, there will be email to alert about the license error.

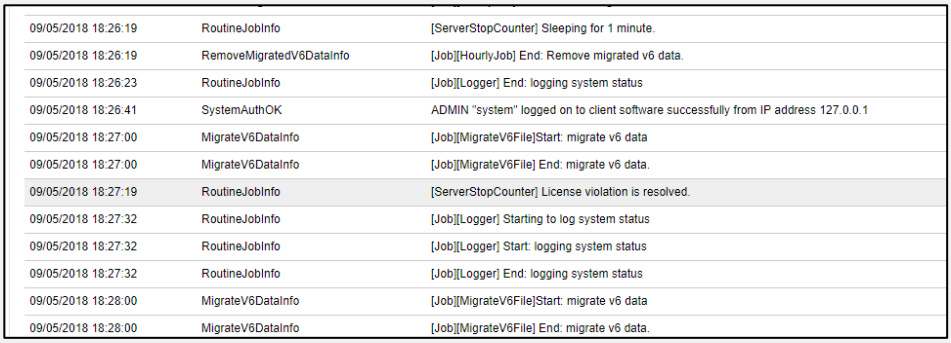


The server stop counter will start in the last hour of grace period. There will be log showing the process of server stop.

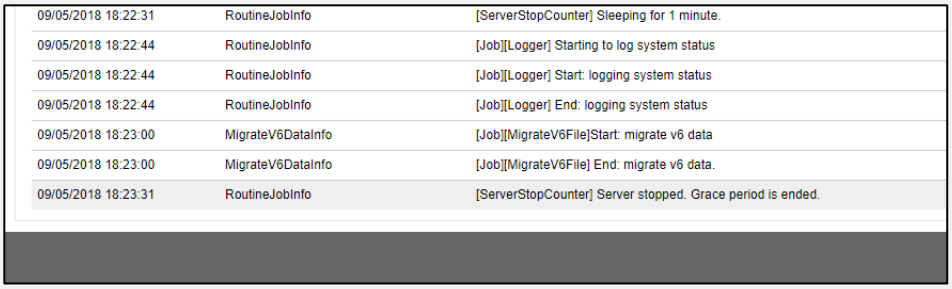
- Server stop counter starts.



- Quota usage issue solved and the server stop counter stopped.



- Quota issue not solved within grace period and server stopped.



If you utilize only one AhsayOBM across multiple physical/virtual devices in previous v6 version, you will need to purchase supplement AhsayOBM when you upgrade to v7.

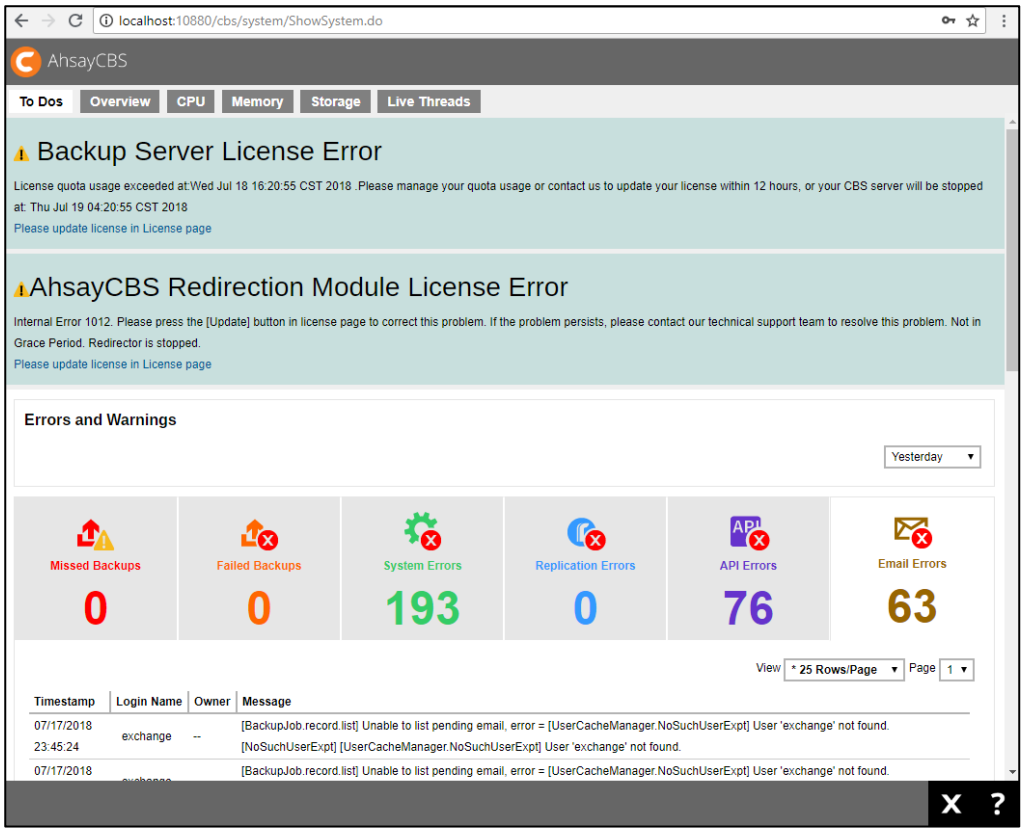
The **VMware** and **Hyper-V** license modules are charged per guest VM. Since version 7.7, there are new options for **VMware** and **Hyper-V** license module to be charged per CPU socket. Existing backup set that are charged per guest VM will not be affected.

NOTE

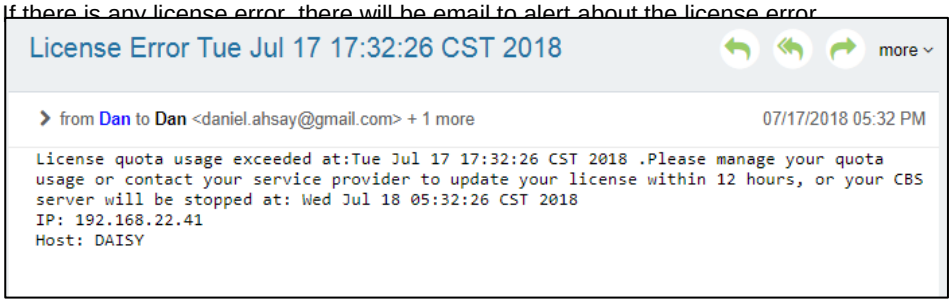
For license to charge by socket, the AhsayOBM has to be in v7.7 or above to work.

Upgrade from pre-v7.17.0.0 to v7.17.0.0 and Above

If upgrade AhsayCBS from pre-v7.17.0.0 to v7.17.0.0 and above with purchasing AhsayCBS module and the quota exceeded, then there will be a grave period of 12 hours for you to manage the quota usage. If quota usage issue was not solved within grace period, the server will be stopped after the grace period. After login AhsayCBS system console, the web console will redirect to [To Do] page and the license error will be shown on the top.



If there is any license error, there will be email to alert about the license error.



Extra License for Replication Server

If you are going to replicate the Backup Server to another Replication Server, you need to purchase additional AhsayCBS license module for the replication server.

License for Standalone Redirector

Since the AhsayCBS Redirector license does not come with an AhsayCBS module, for a standalone AhsayCBS Redirector, you will need to purchase one extra AhsayCBS license module with a Backup Server license.

License Requirements for Software and Modules

Software	
AhsayCBS	Per running instance
AhsayOBM	Per device to back up
AhsayMOB	Per AhsayOBM/AhsayACB account that needs to back up mobile device
AhsayACB	Per device to back up
AhsayUBS	Per installation
Module	
VMware Backup Module	Per Guest VM to back up & Per CPU socket
Hyper-V Backup Module	Per Guest VM to back up & Per CPU socket
Office 365 Exchange Online Individual Mailbox Backup Module New in v7.9	Per mailbox to back up
MS Exchange Individual Mailbox Backup Module	Per mailbox to back up
OpenDirect / Granular Restore	Per backup set
NAS Backup Module	Per AhsayOBM account that needs to back up NAS device
Replication Module for AhsayOBM	Per device to replicate
Replication Module for AhsayACB	Per device to replicate
Redirection module	Per device to redirect

For more information about License pricing or license requirements for different software and modules, refer to the Pricing Details page. To purchase license directly, visit the Ahsay Shopping Centre site.

Automatic License Renewal

If the AhsayCBS is under a monthly leasing plan (meter key), the license key will have an expiry date of 30 days from the current date, the license key is renewed automatically.

In the event of any problems during the license renewal process, i.e. AhsayCBS is not able to connect to the Ahsay License server, the expired license key will have a grace period of 14 days. AhsayCBS can still function normally using the expired license for an extra 14 days before the service is automatically shut down. The 14-day grace period is to allow sufficient time to resolve any license related problems.

For meter key inquiries please contact the Sales team at Ahsay by email at sales-kb@ahsay.com or call our International Sales Hotline +852 3580 8091.

License Evaluation Expiry

After the evaluation period expires (60 days after activation), 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.

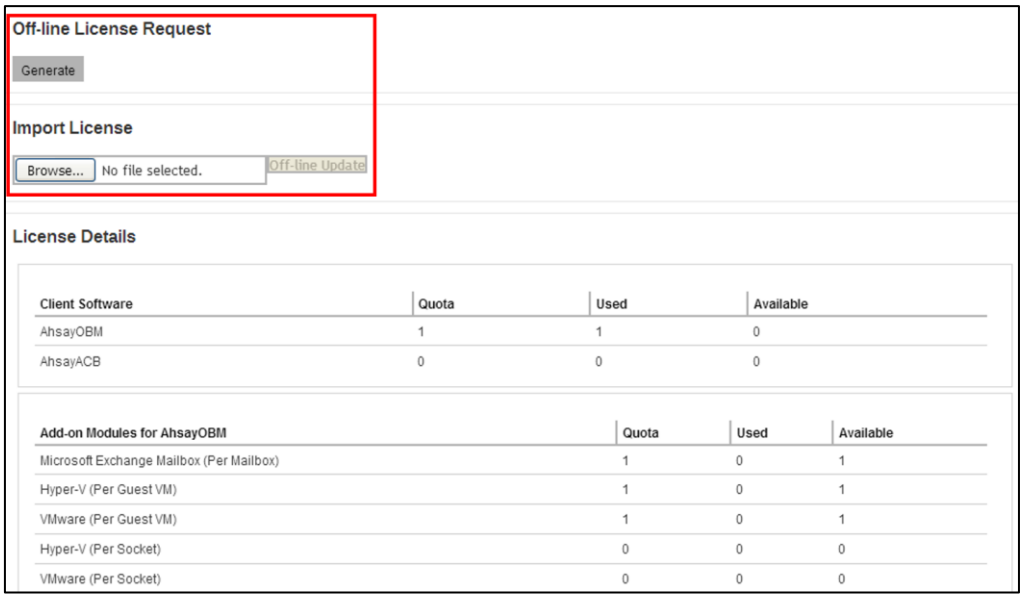
If you would like to continue to use AhsayCBS, please contact the Sales team at Ahsay by email at sales-kb@ahsay.com or call our International Sales Hotline +852 3580 8091.

Offline License Activation

Offline License Activation is used to activate the license keys on AhsayCBS servers that do not have an Internet connection.

Offline license activation is only applicable for OEM license type.

1. Open the License page of AhsayCBS. The two relevant sections are: **Offline License Request** and **Import License**.



2. Click the **Generate** button to generate an offline license request file, **req.olr**.

3. The **req.olr** file is an encrypted file that contains all the information required for the activation process, for example, MAC address and local IP address. The system will prompt for the location to save the offline license request file.

4. When the offline license request file is ready, please send it to Ahsay Support team. An offline license file, **license.olr**, will be generated and sent back to you. This file is used to offline activate the license key your AhsayCBS server.

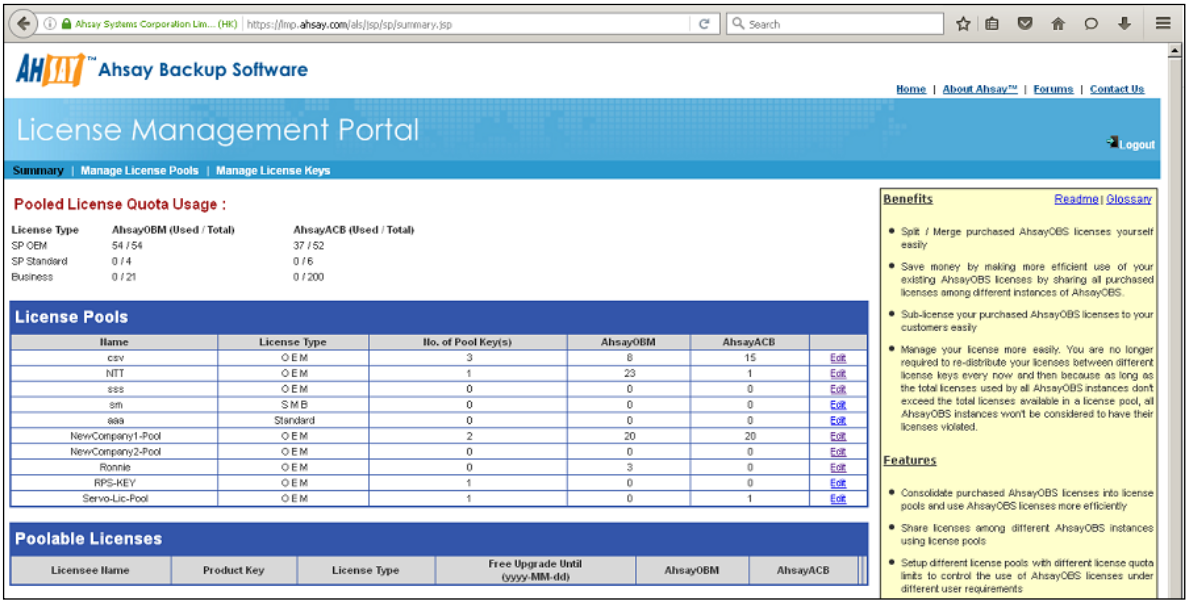
5. After you have received the offline license file, you would need to import it to the AhsayCBS server to complete the offline activation process.

6. Click the **Choose File** button under the **Import License** section to select the offline license file (**license.olr**) from AhsayCBS system home. Click the Off-line Update button to complete the license activation process.

License Management Portal

The Ahsay License Management Portal is for partners to:

- Consolidate purchased Backup Server licenses into License Pool(s).
- Flexibly generate and update Backup Server license(s) as requirements change.
- Improve efficiency on use of Backup Server licenses by sharing CALs (Client Access License) in license pool among multiple Backup Server instances.



With the Ahsay License Management Portal, partners can place purchased Backup Server licenses (Poolable License) into a pool to be shared among multiple Backup Server instances. This process is called converting Poolable License into Pooled License.

Example:

If you have the following 2 licenses:

- LICENSE001 - 50 ACB and 80 OBM
- LICENSE002 - 20 ACB and 30 OBM

You can put these 2 licenses into a single license pool so that you can generate a new license with a maximum of 70 ACB and 110 OBM license CALs or any number of new licenses within these available license CALs.

For more information about the Ahsay License Management Portal, please refer to the following forum articles:

- FAQ: Ahsay License Management Portal Overview
- FAQ: How to create a Pool Key from a License Pool

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.

Active Pool Key

After you applied a pool key on your AhsayCBS server, please make sure your AhsayCBS server has an Internet connection and is able to connect the Ahsay License Server at (https://lic.ahsay.com). **If AhsayCBS service cannot connect to the Ahsay License Server after 14 days, the license key will be deactivated and the AhsayCBS service will be automatically stopped.**

5 System Settings

Basic Backup Server Configuration

To manage your AhsayCBS basic backup server configurations, simply click the **Basic** icon under **System Settings** from your AhsayCBS environment.

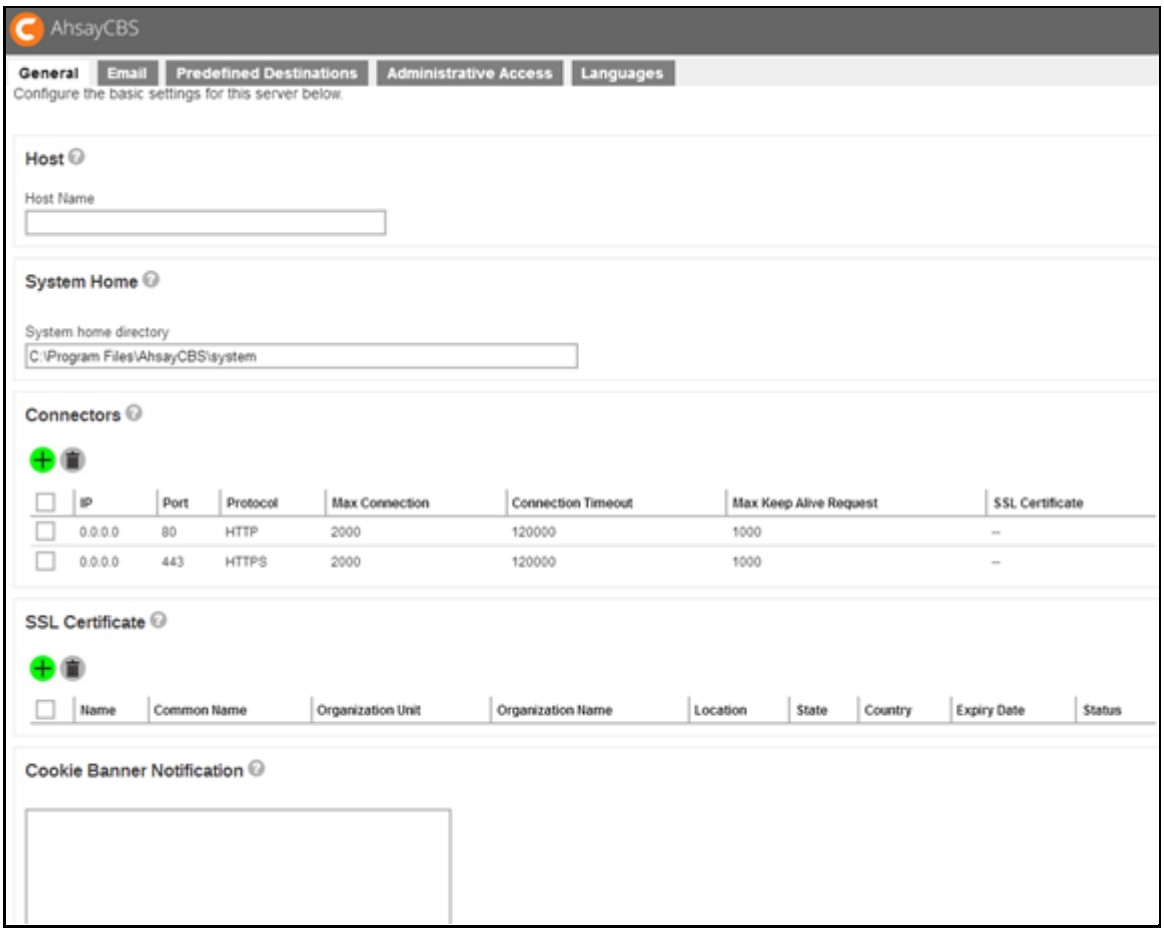
You can perform the following basic configurations on your Backup Server:

- Manage general setup for AhsayCBS
- Manage email settings and general email reports
- Define destinations to store backup or replication data
- Manage Administrator accounts for the MSPs (Managed Service Providers)
- Customize languages available to users on AhsayCBS and User Web Console

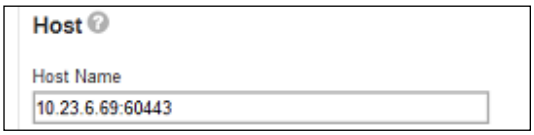
There are 5 tabs under basic server configurations, each of which is described below.

General

The following shows the **General** tab under **System Settings > Basic**. It is used for general setup of AhsayCBS. There are several groups of settings under the **General** tab, and they are described below.



Host



This is the host name of your AhsayCBS. You can enter the domain name of your AhsayCBS in the format:

<www.mybackup.com:port_number>

-OR-

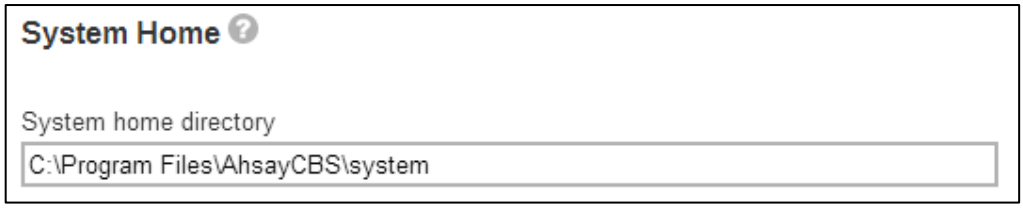
<IP:port_number>

IMPORTANT

- The "port_number" is only needed for non-conventional ports and can be omitted for the usual ports, such as 80 and 443.
- The host name will be the access link for your users to get access to the AhsayCBS. 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 password, users applying Run Direct restore feature, it is important that you ensure the host name is accessible by users from external network environment.

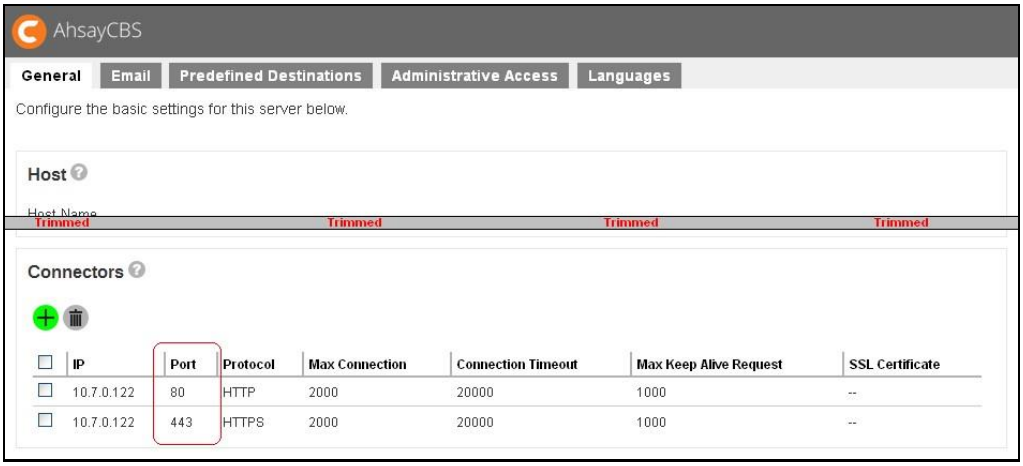
System Home

This is the system home location of your AhsayCBS. This path is set to your installation home by default.



Listening to non-standard TCP/IP Port

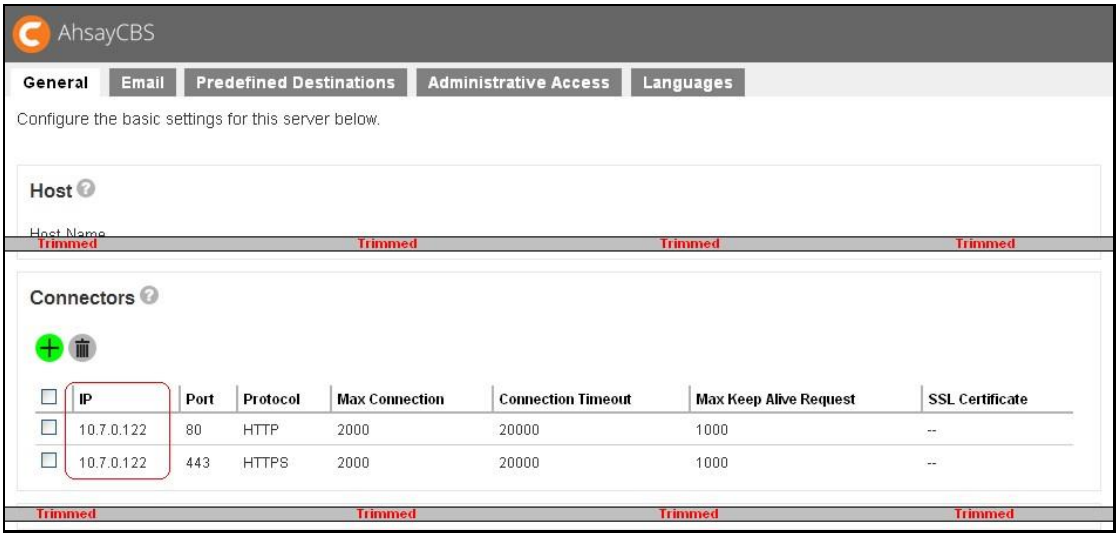
If you like to run your own web server, or some other services using port 80 and 443. On your AhsayCBS server, you can change the listening TCP/IP port of AhsayCBS from port 80 and 443 to some other port numbers such as port 8080 and 8443, you can modify the connector settings from the AhsayCBS management console -> **System Settings** -> **Basic** -> **General** -> **Connectors**, and modify your new port in the connector settings.



Listening to a single IP address

If the backup server has more than one network interface installed or has more than one IP address bind to a single network interface, you can configure AhsayCBS to use only a single IP address for backup services (by default the TCP port of all IP addresses available within the system are used and open). This has the benefits of sparing other IP addresses for other applications, e.g. Apache Web Server or Microsoft Internet Information Server (IIS). You can modify the connector setting from the AhsayCBS management console -> **System Settings** ->

Basic -> **General** -> **Connectors**, and modify the IP address in the connector settings.

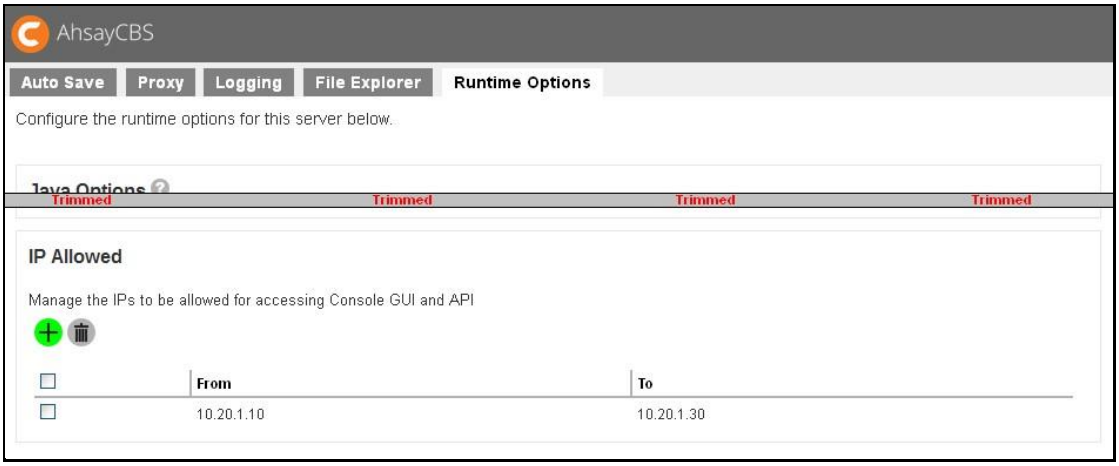


WARNING

Do not remove the last HTTPS connector in the AhsayCBS. If you remove the last HTTPS connector, you will not be able to login AhsayCBS again.

Restricting access to system page by IP address

For better security, you can restrict access to the AhsayCBS management console by IP addresses. To do so, please add IP restriction in your AhsayCBS management console -> **System Settings** -> **Advanced** -> **Runtime Options** -> **IP Restriction**. You can enter a range of IPs or a specific IP in the restrict IP settings.



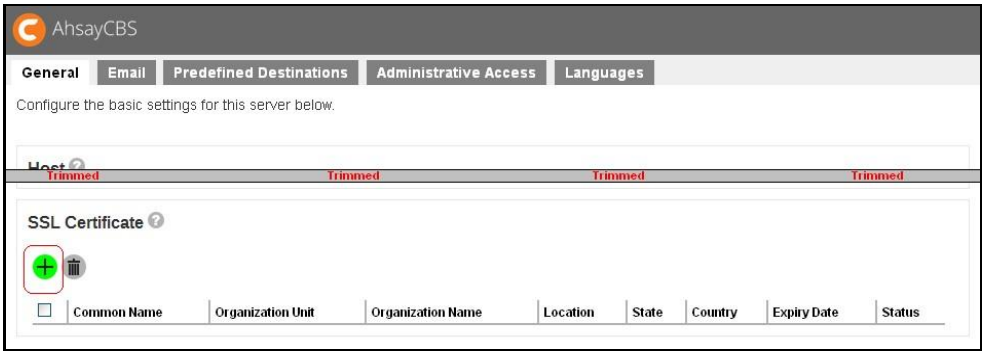
Installation of a trusted SSL certificate

Default installation of AhsayCBS enables SSL (Secure Socket Layer) support using a dummy certificate. For your own security, you are advised to replace the pre-installed dummy SSL certificate with a secure SSL certificate from a trusted CA (Certificate Authority). To replace the non-secure dummy SSL certificate with a secure SSL certificate, you need to generate a CSR (Certificate Signing Request) and submit the CSR to your CA. Please perform the following in your AhsayCBS.

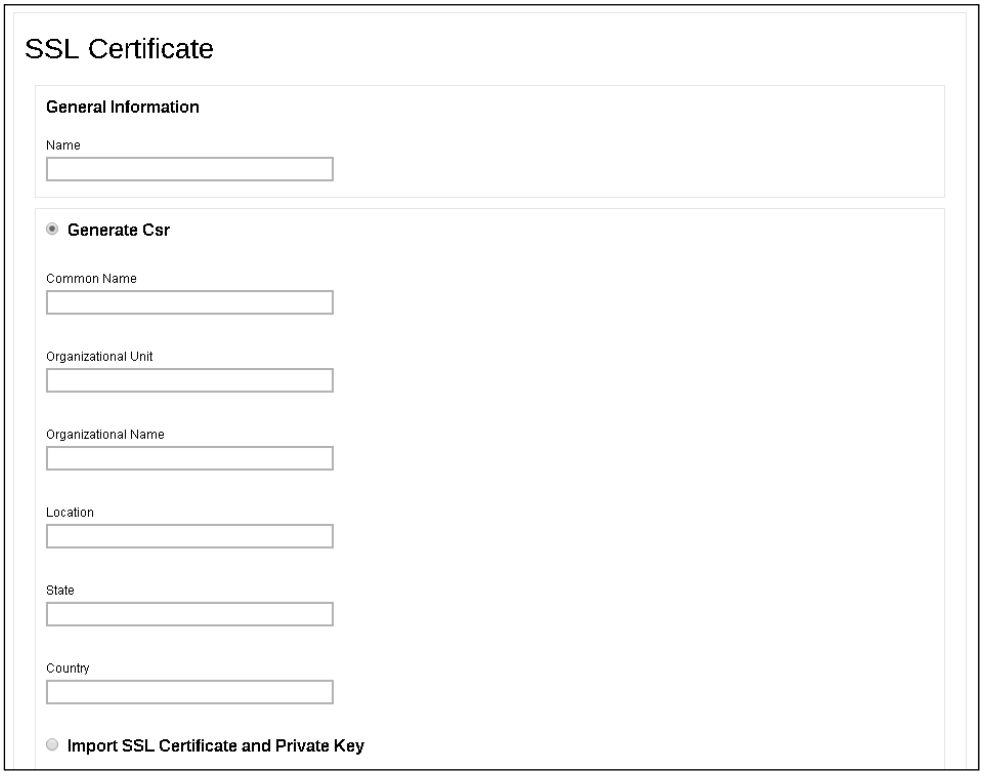
SSL Certificate Installation Service

Let our professional customer service team help you with the SSL certificate purchase and installation. Click here to visit the Ahsay Shopping Centre for subscription.

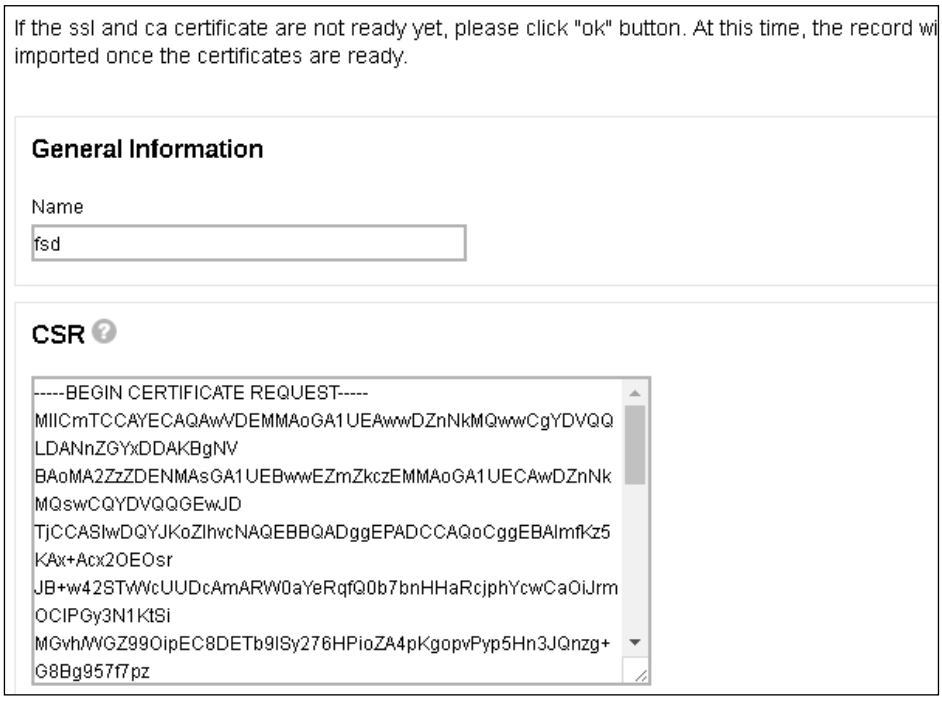
1. Navigate to **System Settings** -> **Basic** -> **General** -> **SSL certificate**, click on .



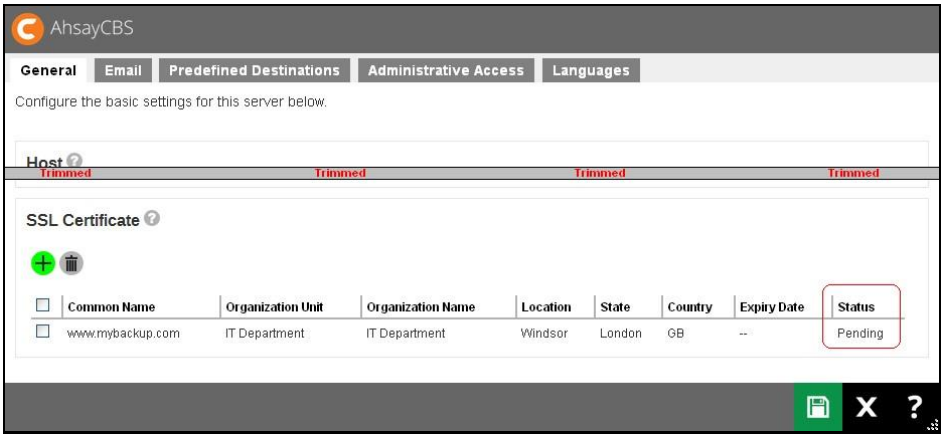
2. Enter the CSR details, then click the Next button to proceed.



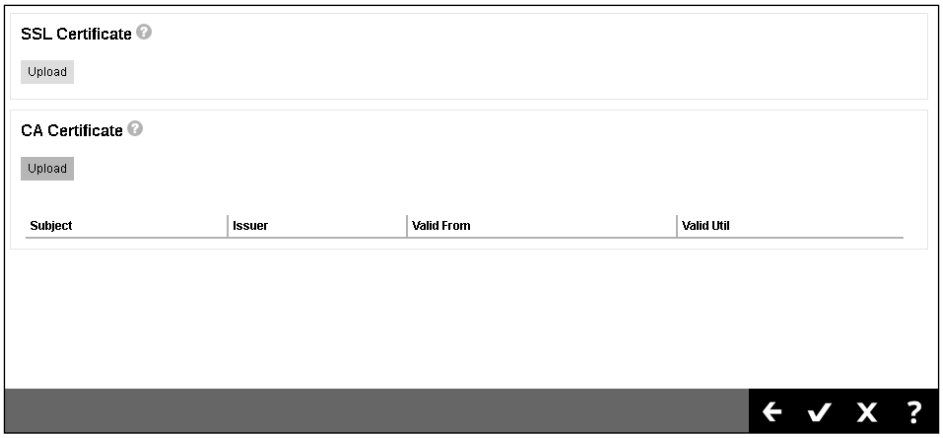
3. Generate a CSR to apply the SSL certificate from your trusted CA.



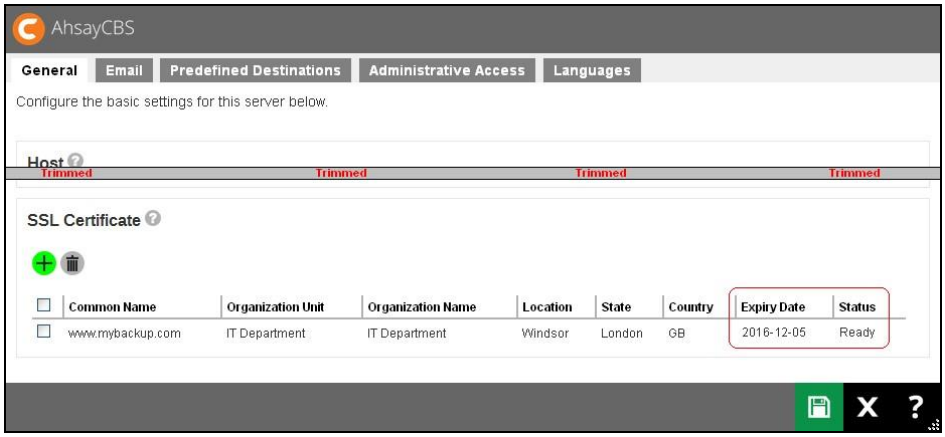
4. You will see a **Pending** status in the SSL Certificate page.



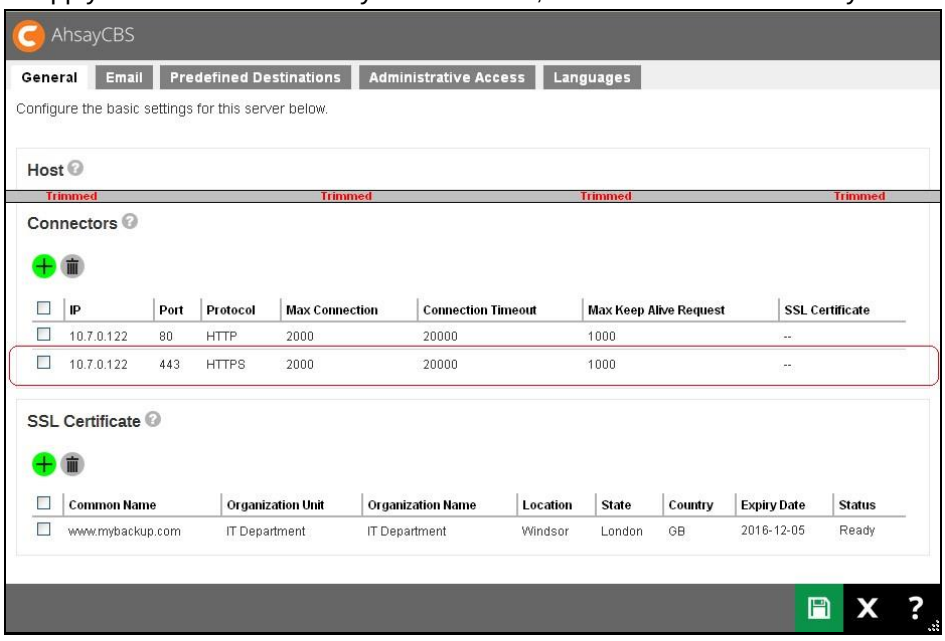
5. When the SSL certificate is ready, click into the certificate entry and import the SSL certificate and CA certificate.



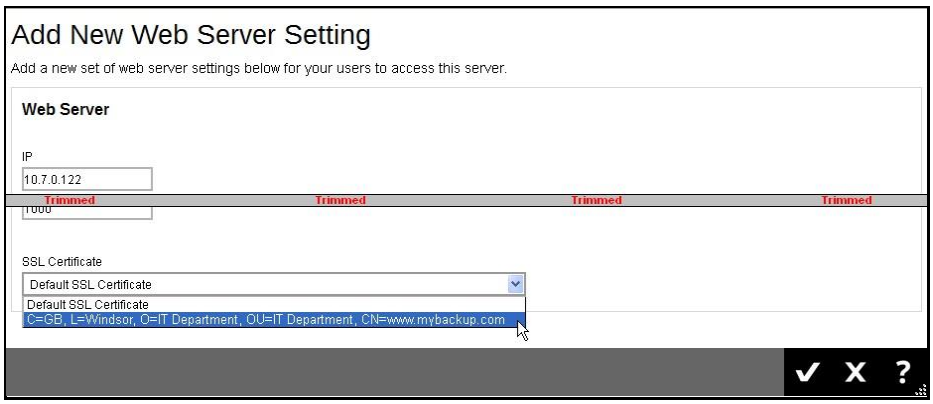
6. You will be able to see the status of the certificate as **Ready** and a valid **Expiry Date**.



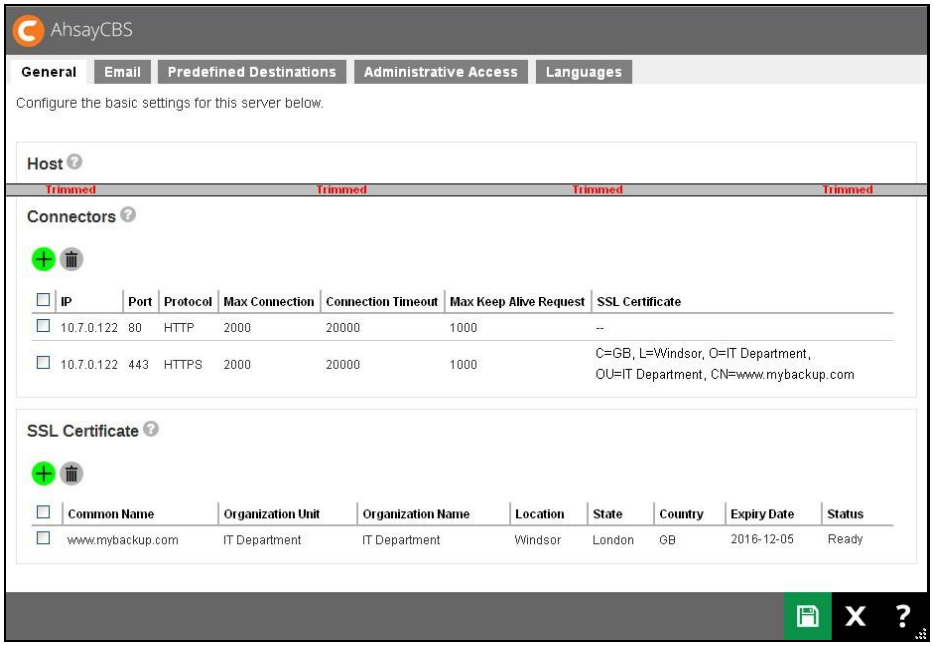
7. To apply the SSL certificate to your connector, click into the HTTPS entry.



8. Add the **SSL certificate** to this connector as shown below.



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



Renew a trusted SSL certificate

When your SSL certificate is due to expire, you can renew your SSL cert via your CA's website. Your CA may ask you to use the existing CSR that you submitted previously or submit a new CSR.

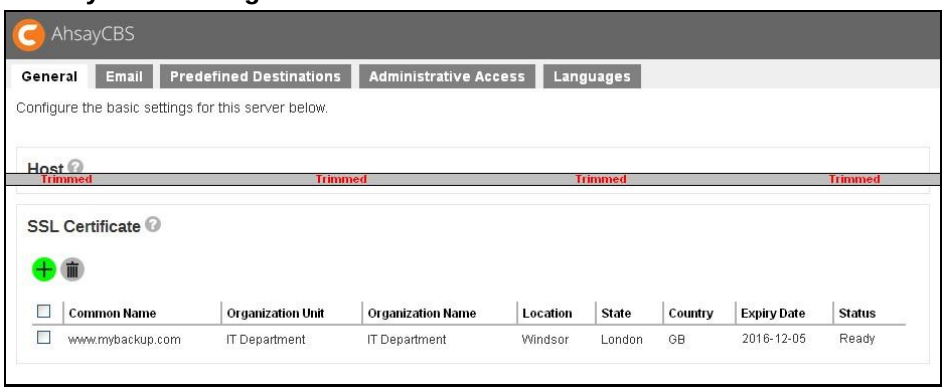
- If you decided to use a new CSR, most likely the information on the old CSR is not up-to-date. Most CA will not consider this as a renew process and you need to start from the beginning of a certificate process described in previous section.
- If you purchase a renew SSL certificate with the existing CSR, wait for your CA to sign the renew SSL certificate.

NOTE

The renewal process may be different for different CA. You need to follow your CA's instruction on the renewal process.

The import step of a renewed SSL certificate is similar to the installation of a SSL certificate. Please perform the following in your AhsayCBS.

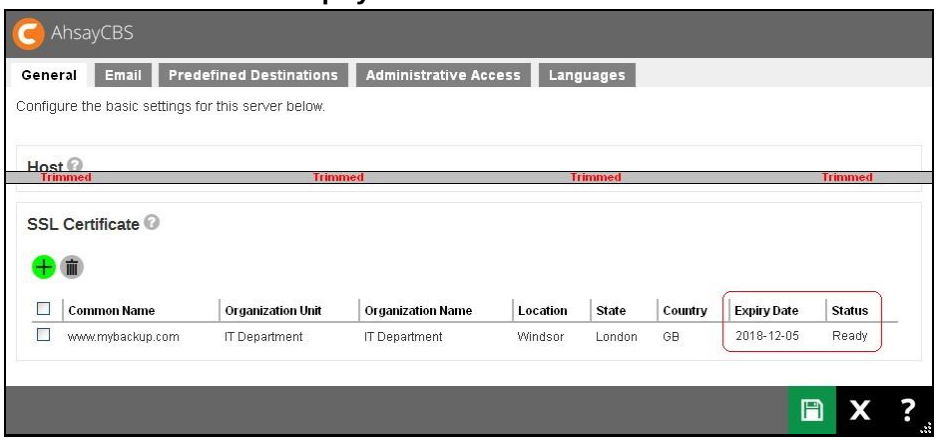
1. Enter **System Settings** -> **Basic** -> **General** -> **SSL certificate**.



2. Click into the certificate entry.

3. Import the SSL certificate and CA certificate.

4. You will see the date of "**Expiry Date**" is extended.

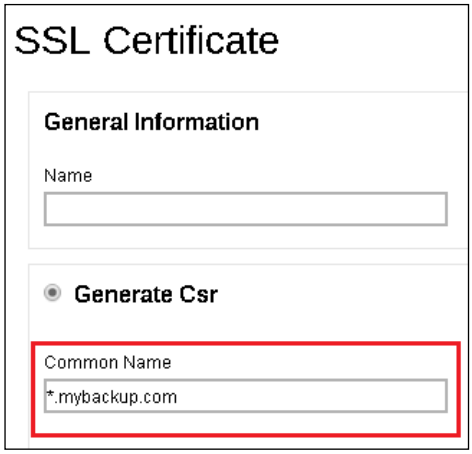


Wild card SSL certificate with redirector setup

In the Redirector with a number of Backup Servers setup scenario, you need to apply a wild card certificate for all your AhsayCBS servers. The application of the wild card certificate is the same as a normal certificate except the common name needs to enter *.backup.com instead. To apply a wild card certificate for all your AhsayCBS servers, please perform the following:

1. In the AhsayCBS with the Redirector role, enter **System Settings** -> **Basic** -> **General** -> **SSL certificate**.

2. Generate a CSR with the common name set to, for example ***.mybackup.com**, and apply the SSL certificate from your trusted CA.



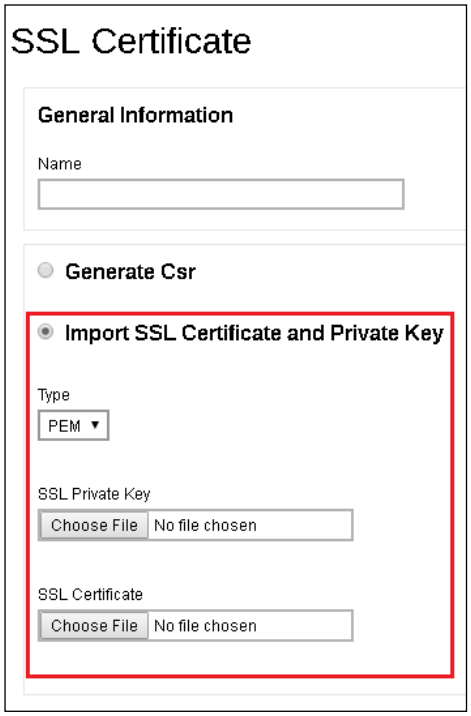
3. When the SSL certificate is ready, import the SSL certificate.

4. Copy the SSL certificate, private key and the CA certificate file from your AhsayCBS_HOME/conf/cert folder and transfer to your AhsayCBS with Backup Server role. They are named similar as the following:

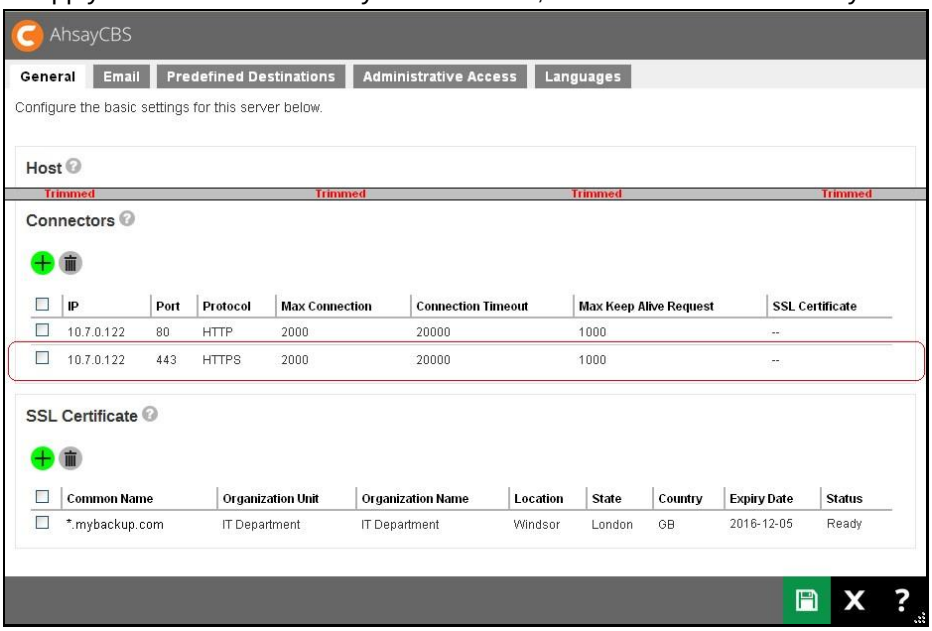
   E.g.:
   1449049185371.crt
   1449049185371.key
   1449049185371.ca

5. Import these 3 certificate files in one of your AhsayCBS (Backup Server role) in the **System Settings** -> **Basic** -> **General** -> **SSL certificate**, click on the **+** button.

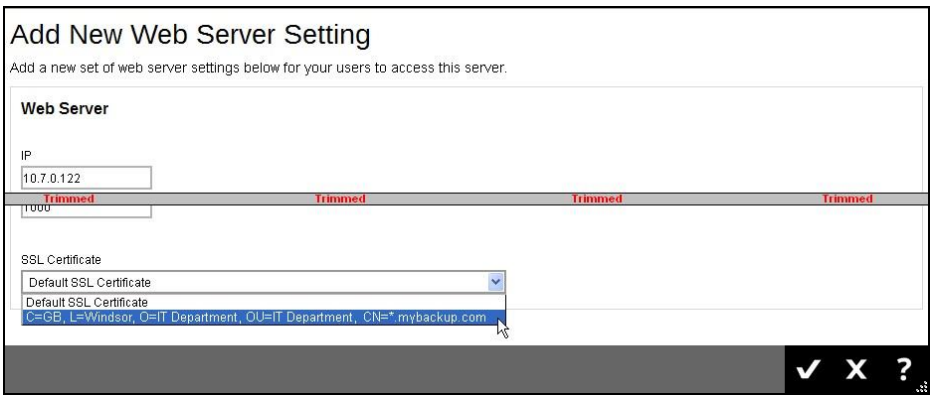
6. Select the **Import SSL Certificate and Private Key** radio button. Select the **Type** and then import the SSL Private Key, SSL certificate and the CA certificate.



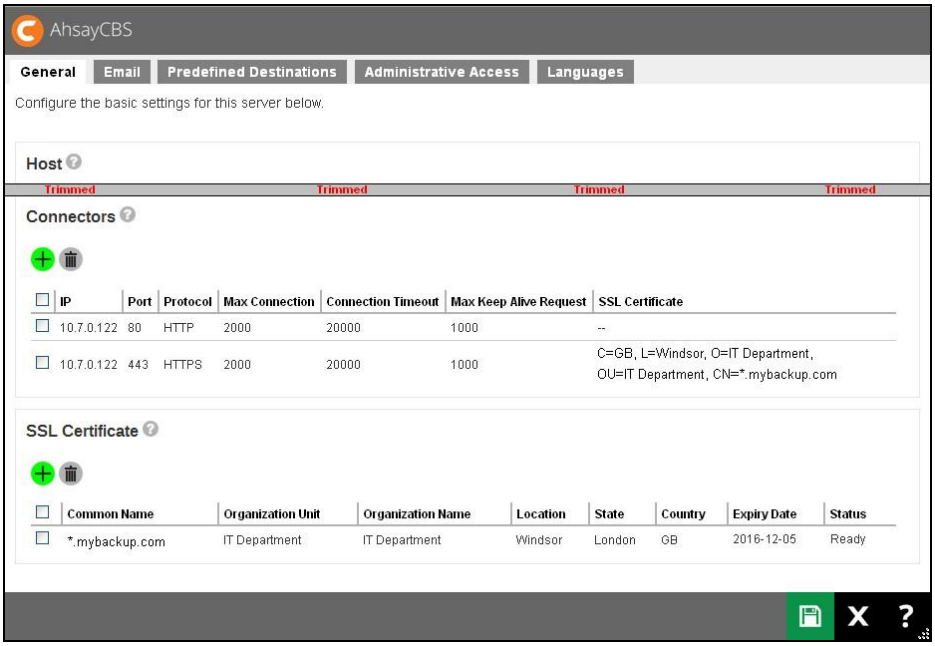
7. To apply the SSL certificate to your connector, click into the HTTPS entry.



8. Add the SSL certificate to this connector.

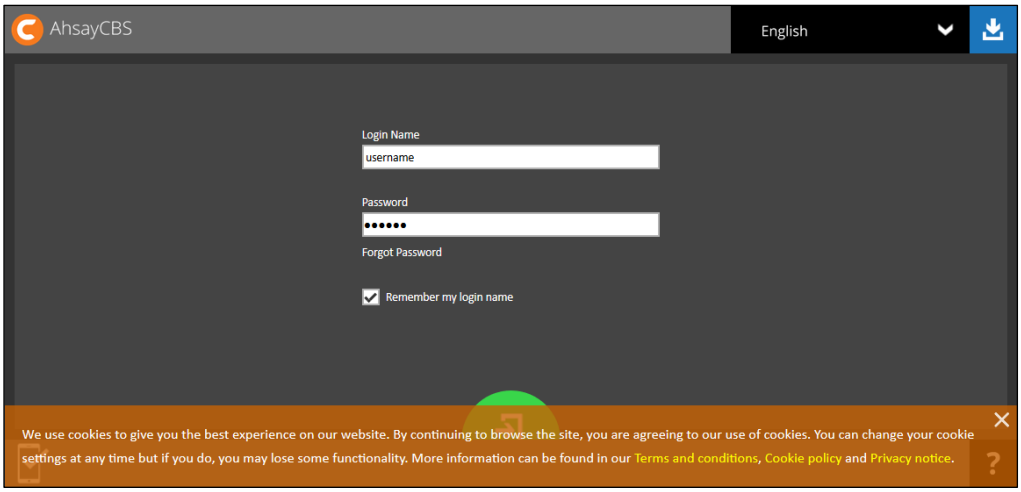


9. Click at the bottom right corner to save the settings.

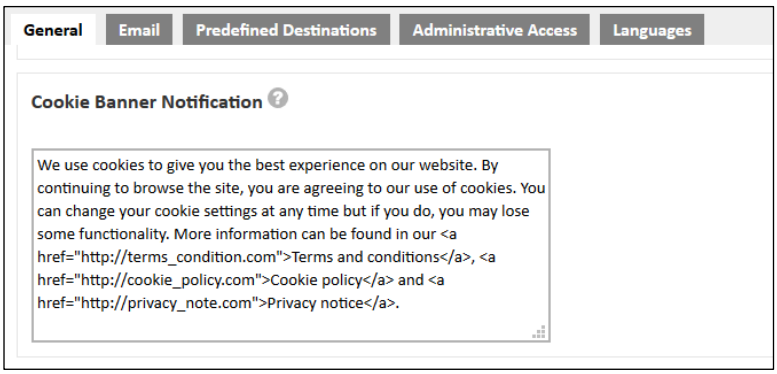


Cookie Banner Notification

To comply with the new General Data Protection Regulation (GDPR) requirements, there will display a banner stating the organizations cookie policy when processing to login AhsayCBS server. This will also apply to the AhsayCBS web console.



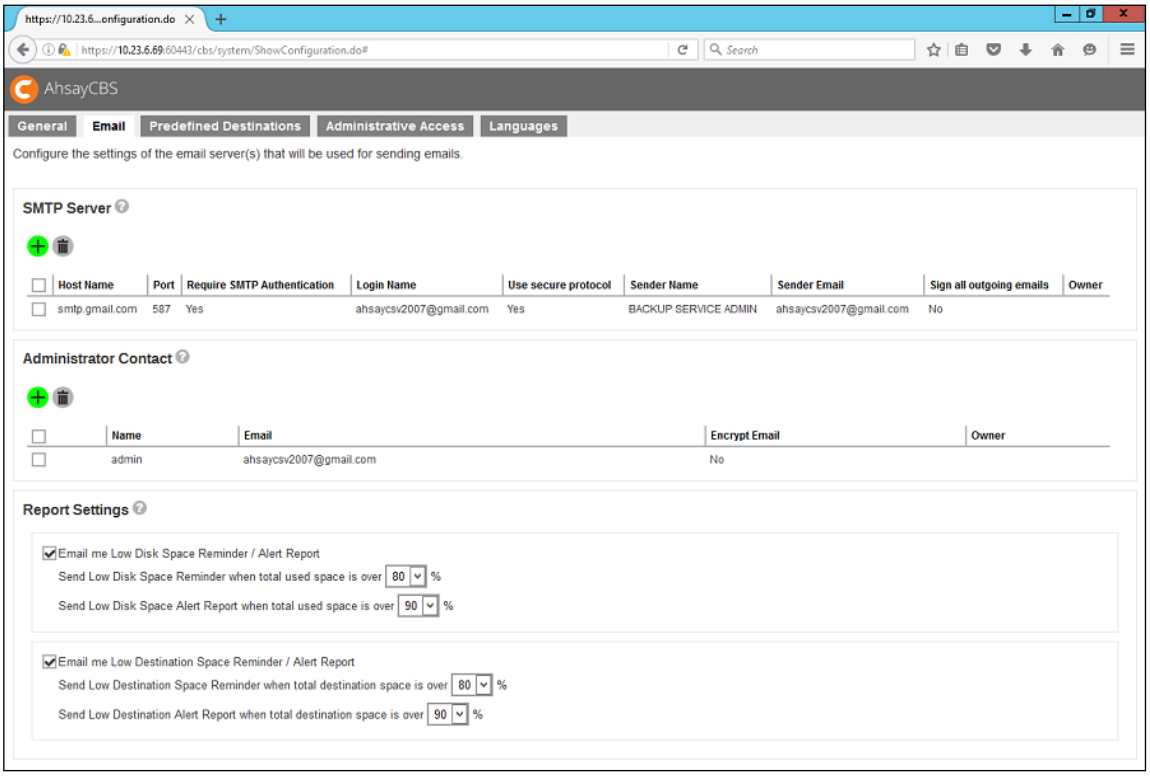
From AhsayCBS version 7.15.6.0 onwards, administrator can configure a notification banner to be displayed on the AhsayCBS web console (displayed at the login interface), and the contents of the banner can be configured on the AhsayCBS web console. Also the HTML codes can be used for content of the banner.



.

Email

The following shows the **Email** tab under **System Settings > Basic**. This is used for defining the various email settings that AhsayCBS uses to generate email reports to backup system administrator and backup users.



There are several groups of settings under the **Email** tab, and they are listed below.

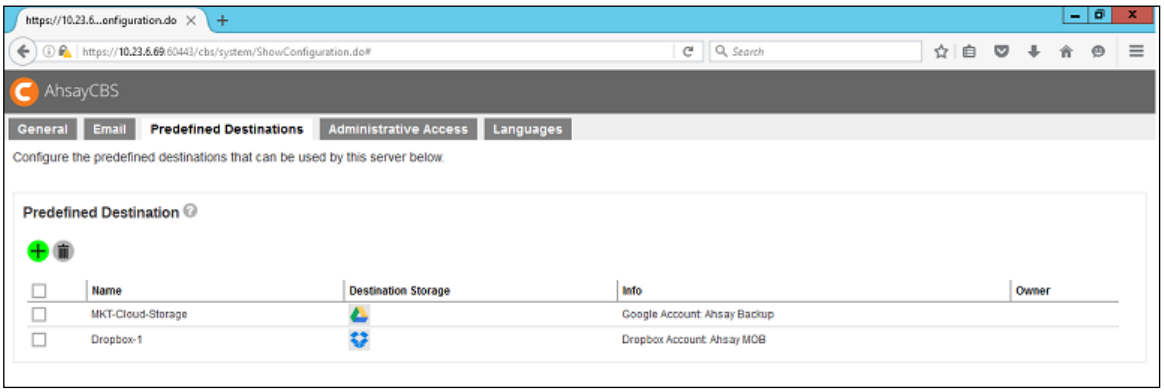
Section	Description
SMTP Server	Multiple SMTP servers can be setup for AhsayCBS. If the first SMTP server is unavailable, the next SMTP server will be used. To avoid your report emails being filtered by the SMTP server or mail client, you need to enter a valid report sender in the email settings. **Note**: If you don't have an SMTP server, you can consider using a free SMTP such as Gmail.
Administrator Contact	This entry defines the administrative contact of AhsayCBS. AhsayCBS will send usage, error and all critical system alerts to all email addresses defined here.
Report Settings	This setting allows the AhsayCBS administrator to define the threshold for email reminder / alert low disk space on AhsayCBS and backup destinations. The default settings are 80% and 90% respectively: ➢ Low Disk Space Reminder / Alert Report for AhsayCBS user home and system home drives: Send Low Disk Space Reminder when total used space is over 80%.

	Send Low Disk Space Alert Report when total used space is over 90%. A Low Disk Space Reminder email is sent to the administrator 15 minutes when the disk usage has exceeded the preset threshold. A Low Disk Space Alert email is sent to the administrator every 15 minutes when the disk usage has exceeded the preset threshold. ➢ Low Destination Space Reminder / Alert Report for OneDrive and Google Drive destinations only: Send Low Destination Space Reminder when total destination space is over 80% Send Low Destination Alert Report when total destination space is over 90% A Low Destination Space Reminder email is sent to the administrator at 6:00 AM daily when the destination disk usage has exceeded the preset threshold. A Low Destination Alert email is sent to the administrator at 6:00 AM daily when the destination disk usage has exceeded the preset threshold. ➢ Email me Consolidated Report: A consolidated report is sent daily at the time defined by the administrator. The report contains four types of information: problems, issues, activities and statistics. For more information please refer to the discussion regarding the Daily User Report.

Predefined Destinations Tab

The following shows the **Predefined Destinations** tab under **System Settings > Basic**. Predefined destination defines a list of local destinations, FTP or cloud storages in which the AhsayCBS server, users and sub admin can be used to store backup data. Predefined destination makes it easily to add extra cloud storage for current or new client and also makes the backup destination redundancy in cloud storage to double the stability. Predefined Destination can also be used to customize frequently used backup destination as visible optional destination choice for backup sets.

Predefined destination can also be used to replicate the AhsayCBS database and backup data to cloud destination which ensures single failure of AhsayCBS database won't influence the subsequent backup and restore jobs.



You can set predefined destination on the following destination storage:

- Local / Mapped Drive / Removable Drive
- Amazon Cloud Drive
- AWS S3 Compatible Cloud Storage
- Google Drive
- OneDrive
- Rackspace
- Dropbox
- SFTP
- AhsayCBS Receiver
- CTYun
- Amazon S3
- Google Cloud Storage
- Microsoft Azure
- OneDrive for Business
- Open Stack
- FTP
- AhsayCBS
- 阿里云

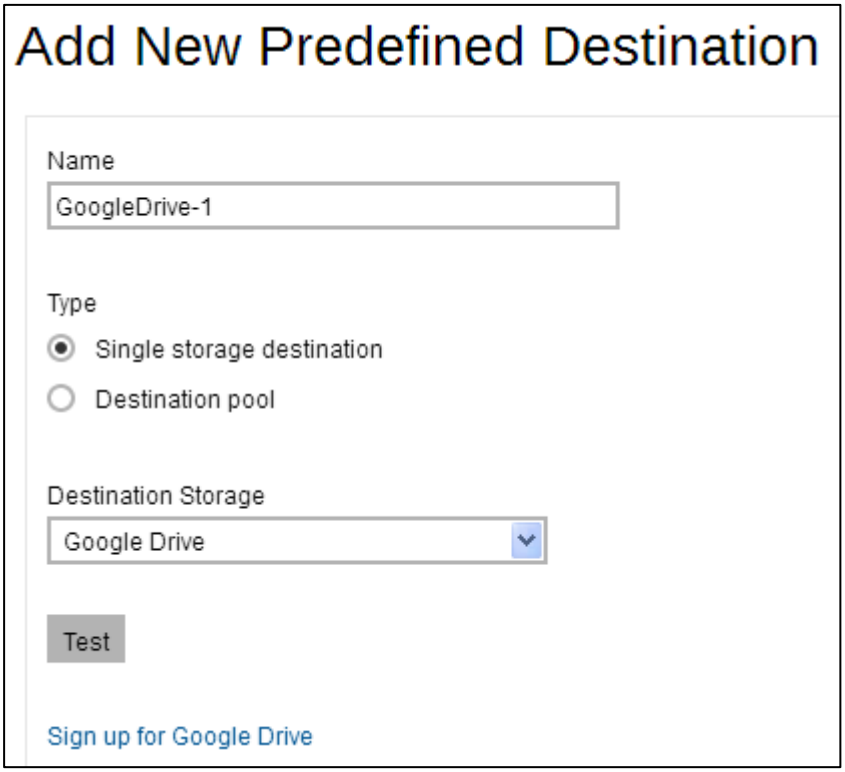
NOTE

From version 7.15.6.0 onwards, Admin user can determine the predefined destination available to each Sub Admin type user. You can refer to the section on Manage System User (System Settings > Basic > Administrative Access > %system user%> Backup User Settings > Destination) for details.

Set up predefined destination on cloud storage

AhsayCBS allows setting a backup destination on some common cloud storage, local hard disk and FTP servers. The setup method is similar on different cloud storage. In the following example, we show you how to set up a predefined destination for **Google drive**. The steps for other destination storages are similar.

1. Click to add a predefined destination. The following screen appears:



2. Enter the name of the backup destination. In our example, the name is **GoogleDrive-1**.

3. Select **Single storage destination** as the type of predefined destination.

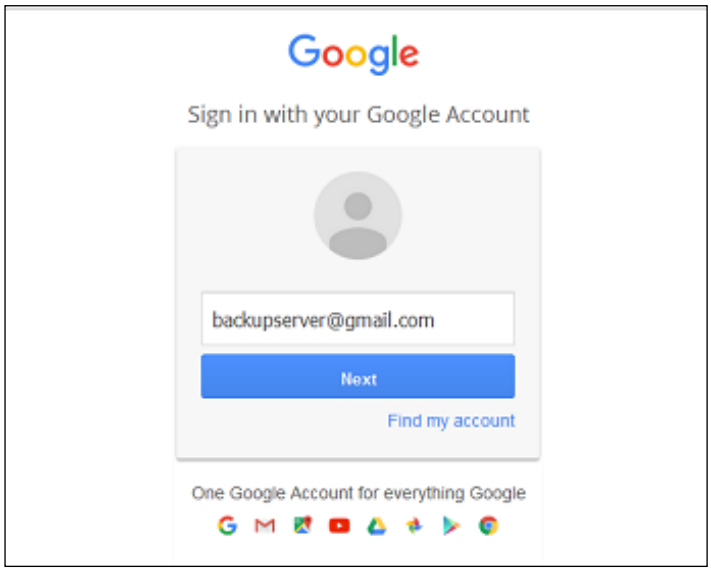
> **NOTE**
>
> The option Destination pool is defined from a number of single storage destination.

4. Select **Google Drive** from the **Destination Storage** dropdown box.

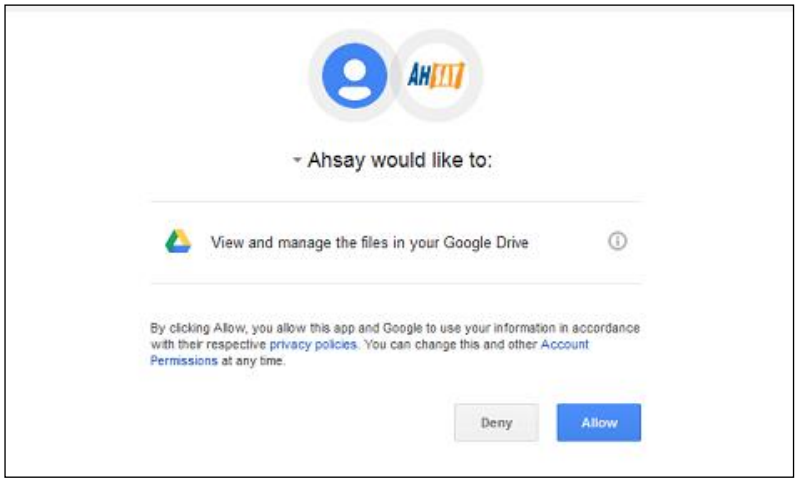
5. If you do not have Google Drive, please click the link **Sign up for Google Drive** to create a Google account.

6. Click “Test” to continue. AhsayCBS will forward to Google Drive page.

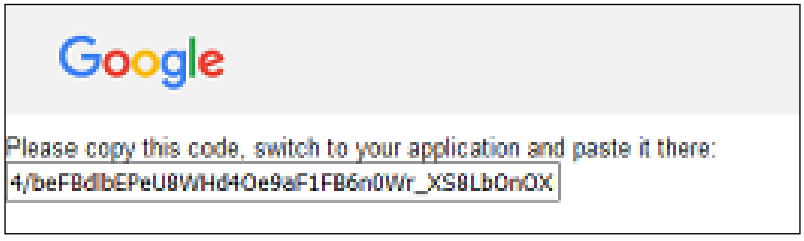
7. Enter your login credential for Google Drive.



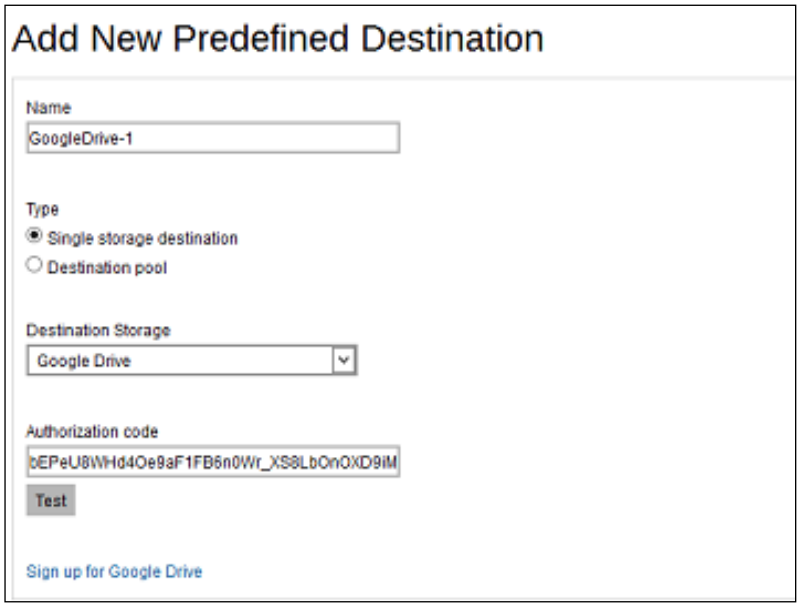
8. A browser pops up and Google asks for your permission to access the storage. Click **Allow**.



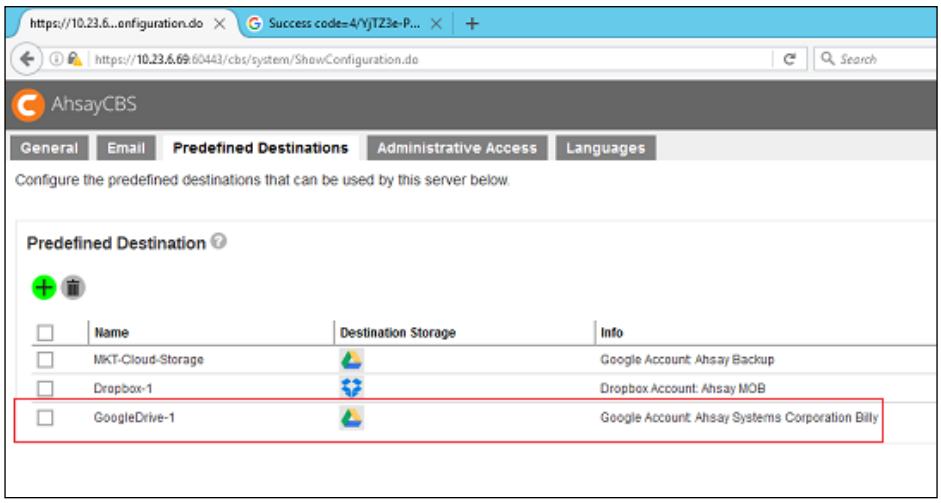
9. On the browser, a code is displayed. Copy this code, then switch to AhsayCBS to paste the code.



10. Paste the code to the **Authorization code** field on the **Add New Predefined Destination** page in AhsayCBS. Click to continue.



11. You can see the newly created predefined storage **GoogleDrive-1** appears under the **Predefined Destination** page.

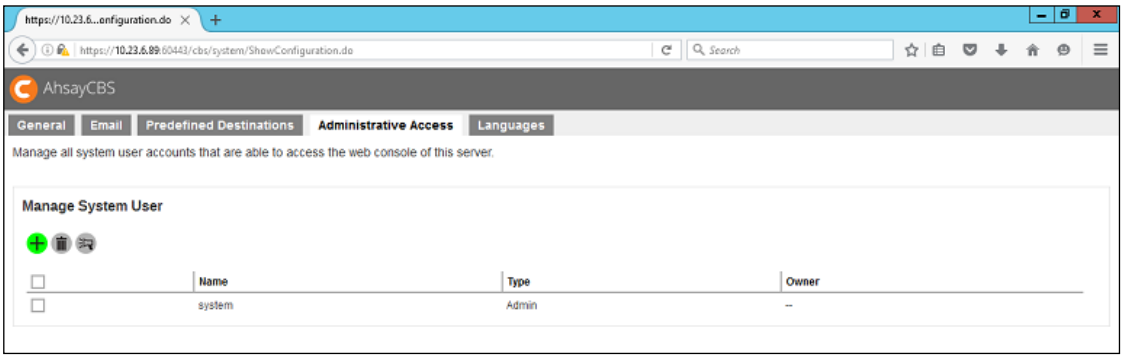


12. Click to confirm. When you create a backup set for a user, you will be able to see the new predefined destination.

For more examples on setting up other cloud storages, refer to Appendix E Setting up Cloud Storage.

Administrative Access Tab

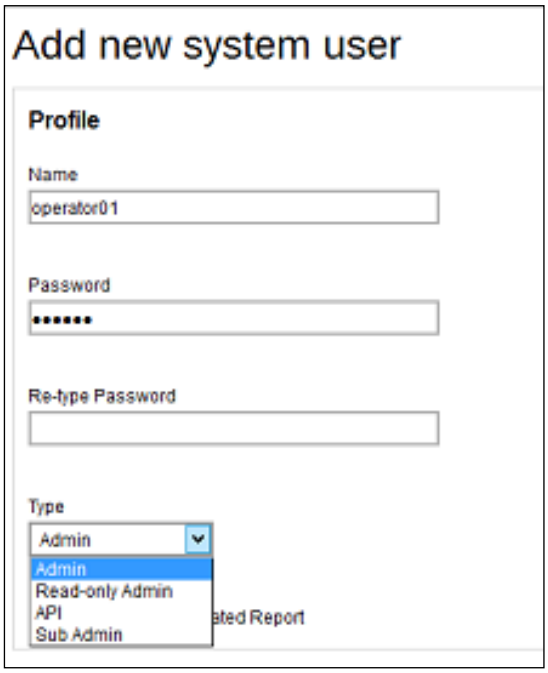
The following screen shot shows the **Administrative Access** tab under **System Settings > Basic**. You can manage your system user accounts on this page.



On daily operation, you may need to assign your operators or administrators to work on your AhsayCBS. You may have programmers to write API for your applications with the AhsayCBS. You may also want to hire some resellers so that you can expand your business. You will need to setup different system users with different role/privileges to work on the AhsayCBS.

Add a new system user

1. Click in the middle of the page to add a new system user. The following screen appears:



2. Enter the **Name** of the system user.

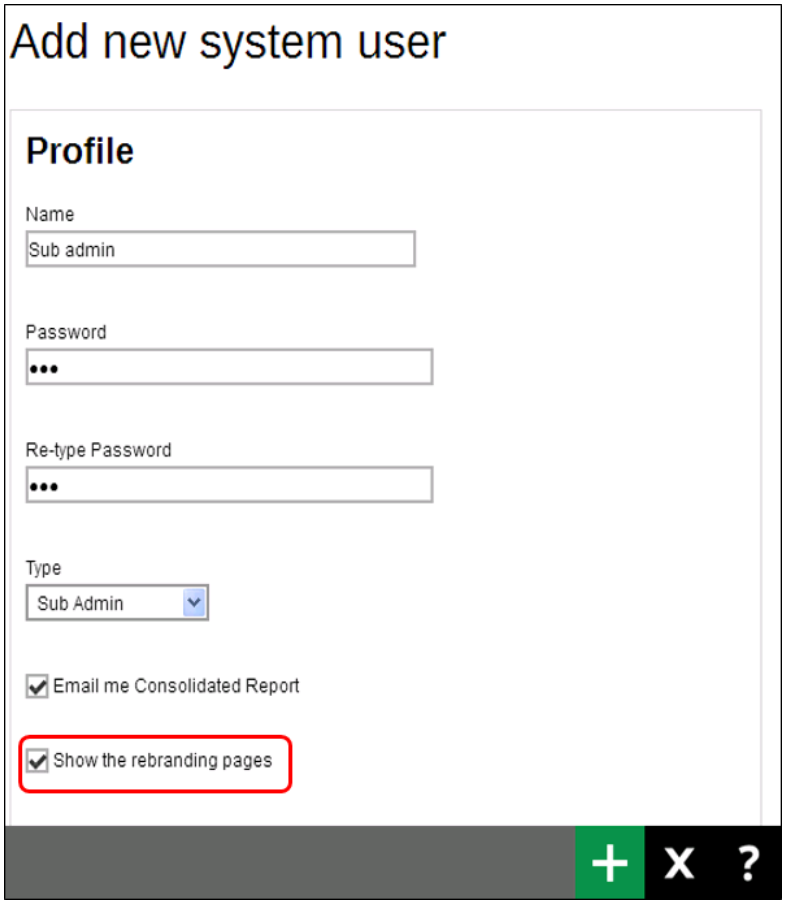
3. Enter the **Password** of the system user. Enter the same password again at the **Re-type Password** field.

4. Select the system user type from the **Type** dropdown Box. There are four types of system users:

- **Admin**

  The Admin role has the same privilege as the build-in **system** account. For example, you can assign this account for your administrator(s) to configure or administer the AhsayCBS for you.

  From v7.15.0.0 onwards, AhsayCBS allow Admin role user account to independently disable or enable Sub Admin user account access right to the branding pages.



- **Read-only Admin**

  The Read-only Admin role shares similar accessibility as its creator with Admin role, except with read permission only.

- **API**

  The API role has full access right to the system; it has the same privilege as the build-in **system** account. This account is created for external application developers who can use this for API login authentication purposes.

- **Sub Admin**

  The Sub Admin role has the full access right to the users that was created under this sub admin and has the right to manage the backup and restore jobs or activities similar as the system administrator with less admin options.

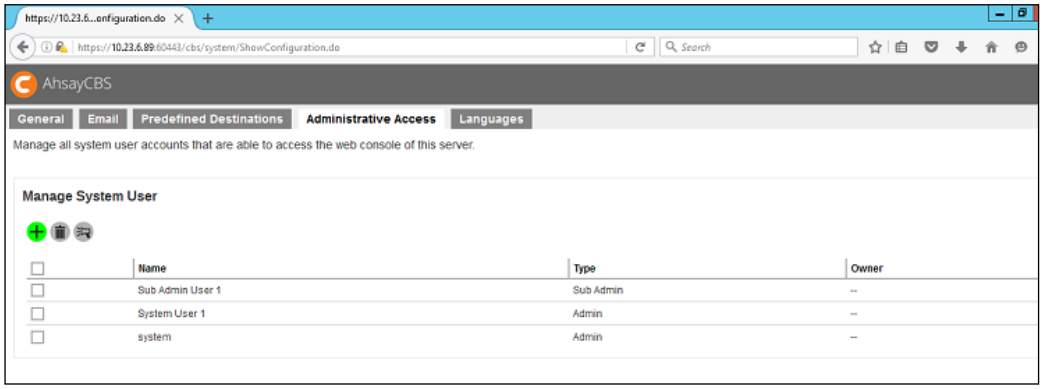
The following table provides a summary of the permissions of different system users in AhsayCBS.

Permission	Admin	Read-only Admin	API	Sub Admin
Read permission	✔	✔	✔*	✔
Write permission	✔	✘	✔*	✔
Login AhsayCBS	✔	✔	✘	✔
Create new system users	✔	✘	✔*	✔
Profile page	✔	✔	✘	✔
Backup User Settings page	✔	✘	✘	✔**
Rebrand Web Console page	✔	✘	✘	✔
Rebrand Client page	✔	✘	✘	✔
Export/Import profile	✔	✘	✘	✔

* API role has full access to the AhsayCBS which is similar as the Admin role through the API call, except login to the AhsayCBS interface.

** Sub Admin role has full access to the settings (except the Backup User Settings page) and users under this sub admin user only.

5. Click to add. The newly-created system user, **System User 1**, appears on the page.

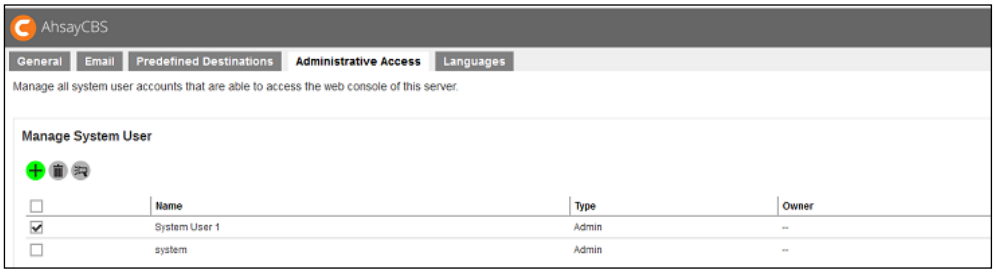


6. Click to confirm.

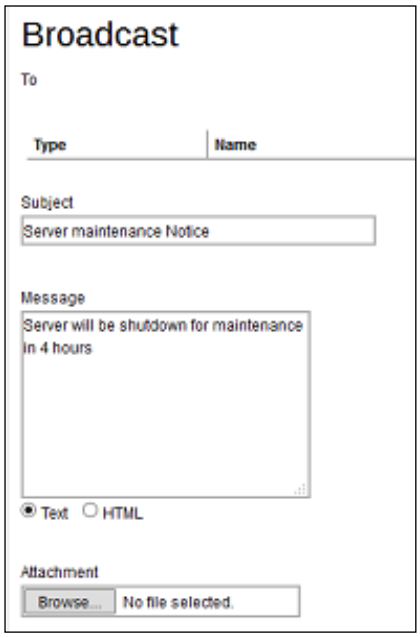
Sending a broadcast message

If you want to send broadcast message to other Sub Admin or Read-only Admin, do the following:

1. Select the system users to whom you need to send the broadcast message. In our example, **System User 1** is selected.



2. Click the **Broadcast** icon in the middle of the page. The following appears:



3. Enter the **Subject** and **Message** for the broadcast message.

   - You can select **Text** or **HTML** for the message body.
   - If you want to include an attachment, click **Choose File** and browse to the desired location to select the file you want.

   Click the **Send** button at the bottom right hand corner of the page to send the broadcast message. Click **X** to exit.

Managing System User

You can modify the setting of your system user by clicking into the system user's name. You will see 4 tabs:

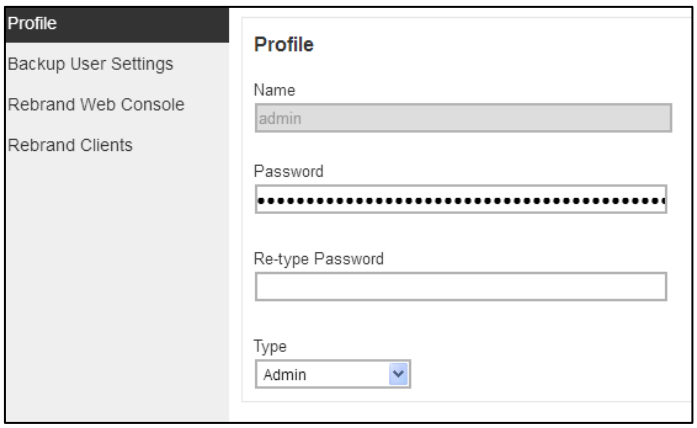
Profile	**Backup User Settings**
Rebrand Web Console	**Rebrand Clients**

Each of these 4 tabs are described in detail below.

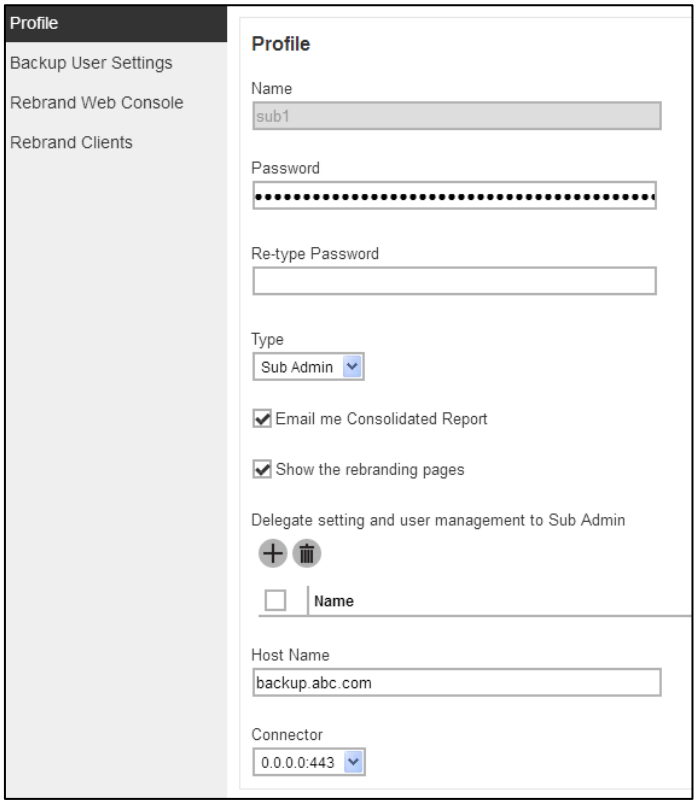
- **Profile Tab**

The profile tab is available to all Admin, Read-Only Admin, and Sub Admin users after they login.

The following screen shows the Profile tab of the user used. In our example, **System User 1**, the type of the user is **Admin**. You can change the **Password** and **Type** of the user on this page.



For **Sub Admin** users, the Profile page contains more settings.

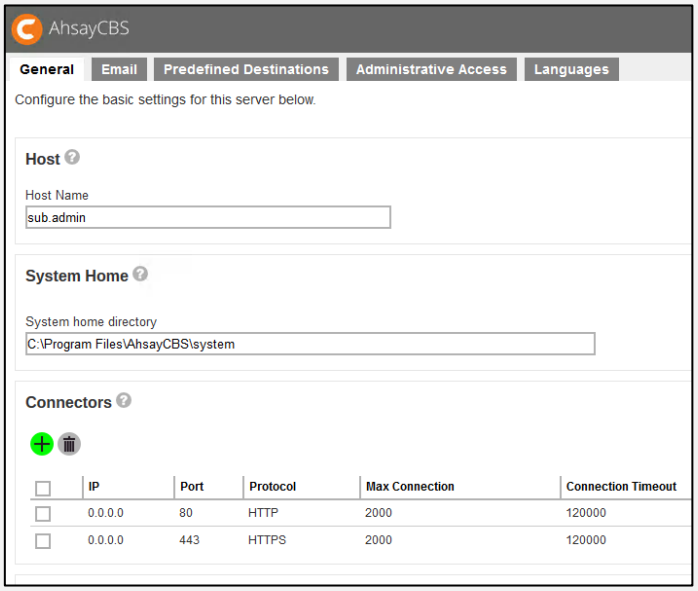


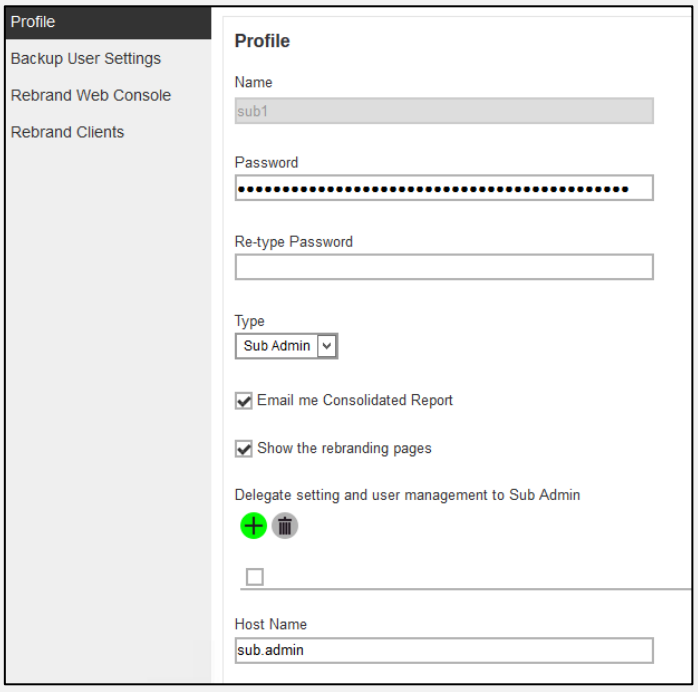
The Sub Admin profile page is different from the Admin profile page in the following 3 ways:

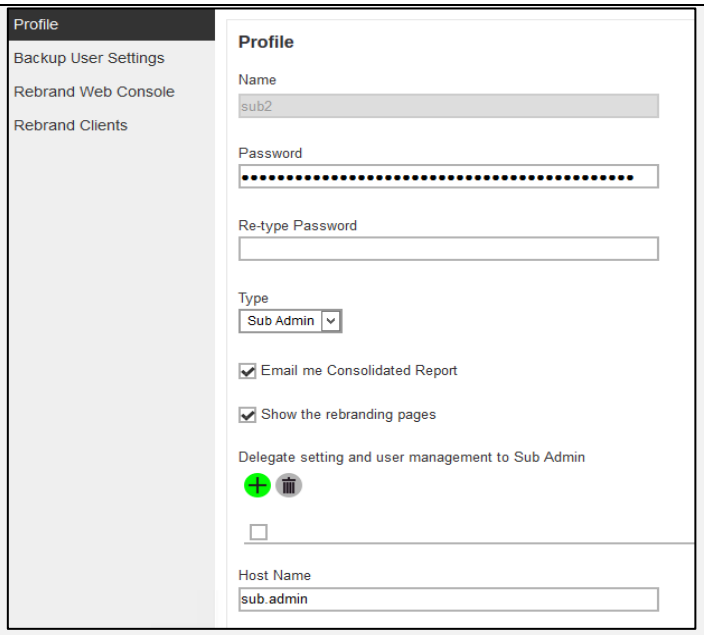
- Another Sub Admin is possible to be delegated for a Sub Admin user through the interface.
- The Host Name for the Sub Admin user can be modified.

NOTE

- From v7.15.0.0 onwards AhsayCBS Sub Admin users (resellers) can share the same hostname as the system admin user. In our example, the host name for system admin is “sub.admin”, and so is for the Sub Admin users “sub1” and “sub2”.



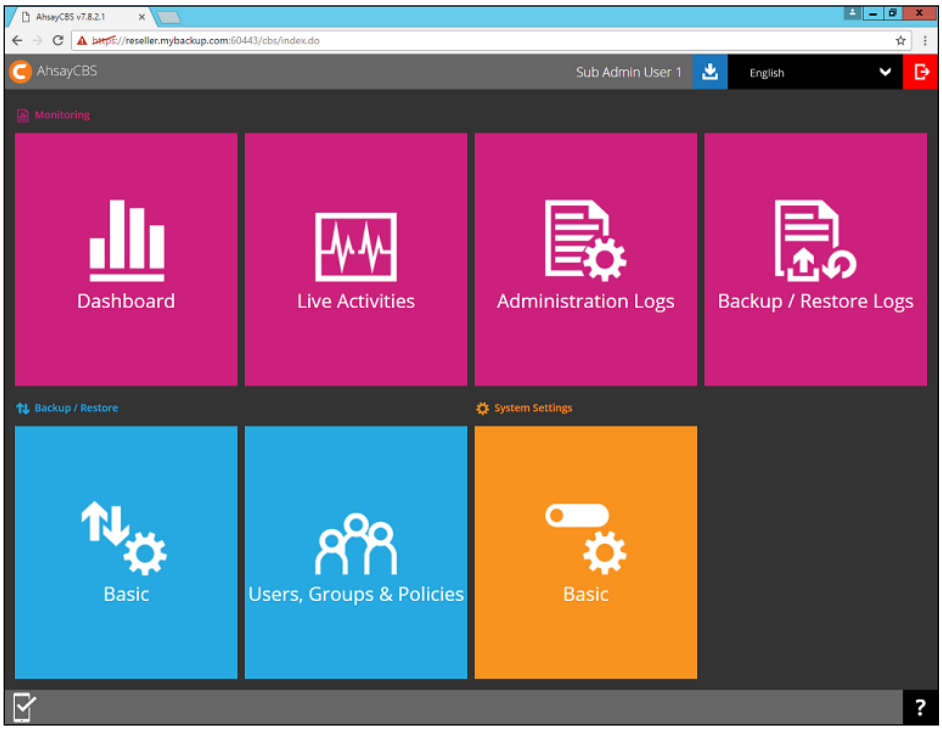




➢ The hostname setup for a Sub Admin user is important, as AhsayCBS uses connecting hostname to determine which branding should be applied on the interface.

- A different connector can be applied for the Sub Admin users.

The Sub Admin user has fewer privileges as the full Admin user. In our example, the Sub Admin User 1 account shows a subset of the functions available when the Sub Admin user logs onto AhsayCBS and even within each subset a sub admin user has only access to certain functions:



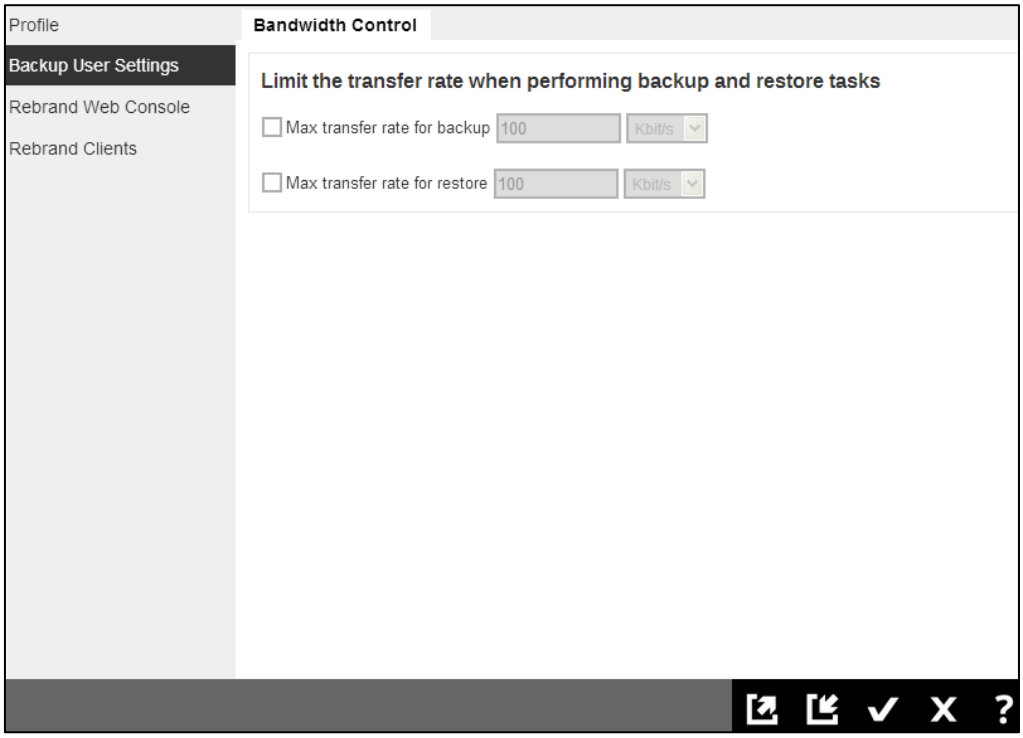
Available functions for Sub Admin users.

Monitoring	
Dashboard	➢ To Dos ➢ CPU ➢ Memory ➢ Storage
Live Activities	➢ Backup Status ➢ Restore Status
Administration Logs	➢ Audit Trails
Backup / Restore Logs	➢ Backup Jobs ➢ Restored Jobs ➢ Backup Errors ➢ Backup Set Log ➢ Activities Log
Backup / Restore	
Basic	➢ Free Trial Options
Users, Groups, & Policies	➢ Backup User ➢ User Group ➢ Policy Group
System Settings	
Basic	➢ Email ➢ Predefined Destinations ➢ Administrative Access

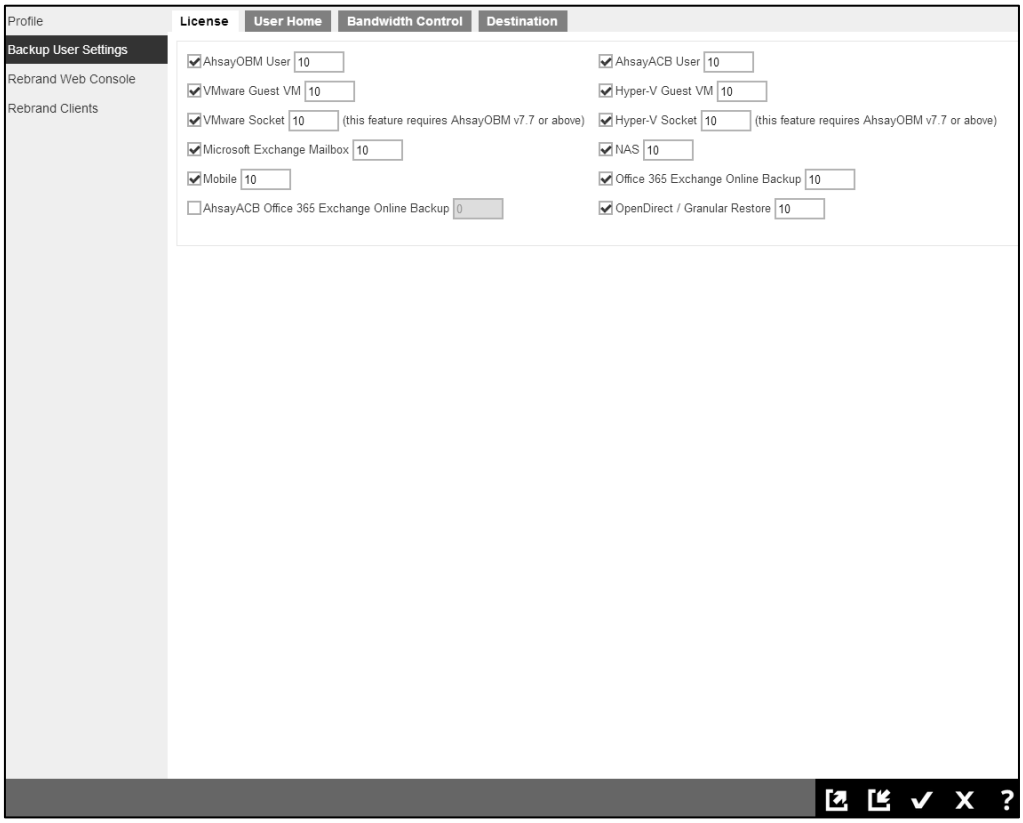
Backup User Settings Tab

The Backup User Settings tab is available to admin and sub admin users after they login, although for sub admin user they have read-only access.

The following screen shot shows the Backup User Settings tab of the user used in our example, **admin**, whose type is **Admin**.



The following screenshot shows the Backup User Settings tab of the user used in our example, **Sub Admin User 1**, whose type is **Sub Admin**.



NOTE

Please kindly note that:

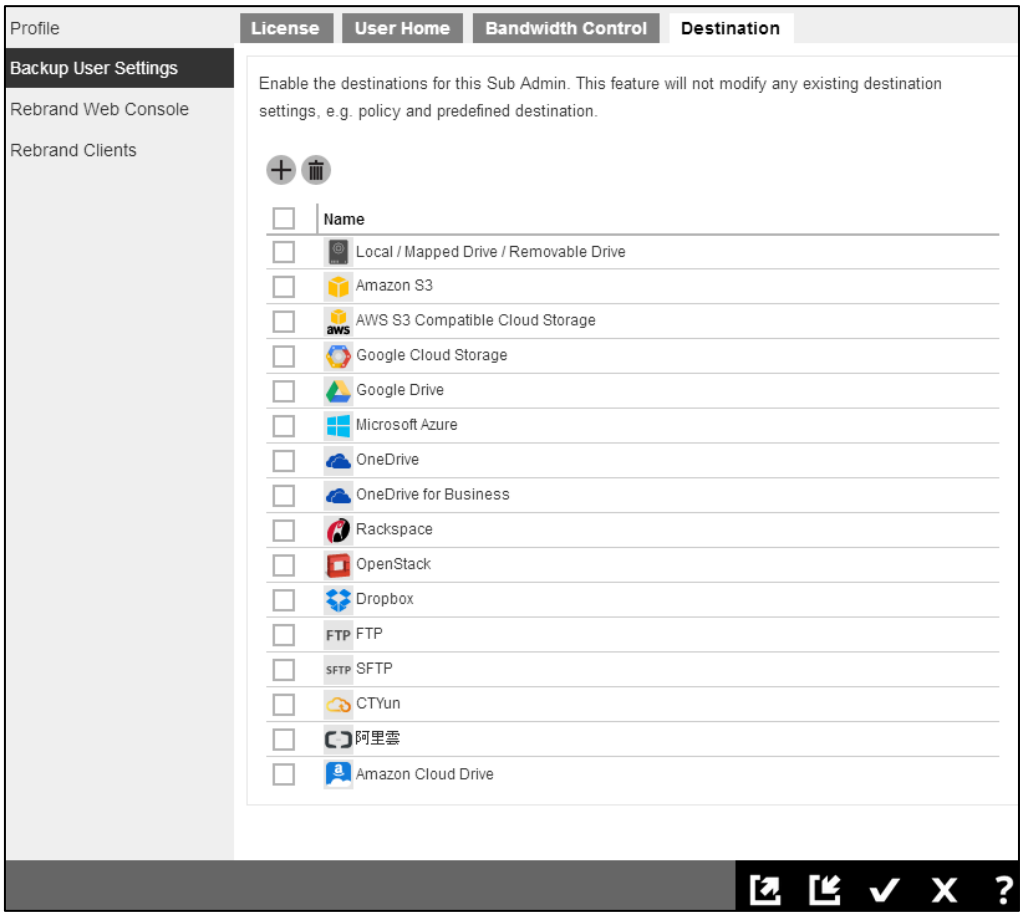
- If uncheck the box, there is no limit for license quota assigned to the module.
- If check the according box and the assigned value for license is less than the used ones, there will be error message prompted to block the update. For example, if check the box and assign 10 quota of VMware Guest VM to sub admin, but it already has 20 quota used, then there will be error message prompted to block the update.

The administrator can assign the number of AhsayOBM/ AhsayACB CALs and add-on modules to each sub admin user.

Field	Description
AhsayOBM User	License quota for AhsayOBM users.
AhsayACB User	License quota for AhsayACB users.
VMware Guest VM	License quota for backing up VMware Guest VMs.
Hyper-V Guest VM	License quota for backing up Hyper-V Guest VMs.

VMware Socket (this feature requires AhsayOBM v7.7 or above)	License quota for VMware Socket.
Hyper-V Socket (this feature requires AhsayOBM v7.7 or above)	License quota for Hyper-V Socket.
Microsoft Exchange Mailbox	License quota for backing up Microsoft Exchange Mailboxes.
Mobile	License quota for backing up Mobile devices.
NAS - Synology	License quota for backing up Synology NAS devices.
NAS - QNAP	License quota for backing up QNAP NAS devices.
AhsayACB Office 365 Exchange Online Backup	License quota for backing up AhsayACB Office 365 Exchange Online user mailboxes.
Office 365 Exchange Online Backup	License quota for backing up Office 365 Exchange Online user mailboxes.
OpenDirect / Granular Restore	License quota for file-level restore from guest VM or compressed/image files. Applicable only to File / Hyper-V / VMware backup sets on Windows platform.

Administrator can determine the destination category(both predefined and standard destination) for the sub admin user, but the configuration will not modify any existing destination settings, e.g. policy and predefined destination.



The administrator can enable/ disable the destination by adding/ deleting the according destination. If the administrator disable the destination option, the according destination will not show in the sub admin user login interface during adding the new predefined destination or standard destination.

NOTE

Please kindly note that:

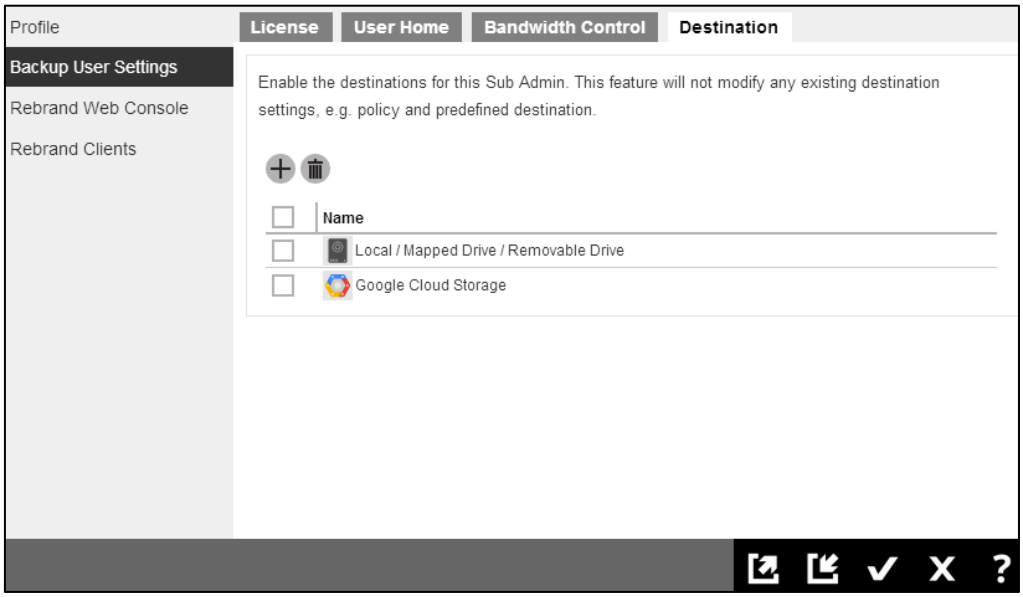
- The Destination settings can be overridden by the setting under "Users, Groups & Policies > Policy Group > Backup Set Settings > Destination Visible to Users".

  For example, if "OneDrive" is hidden from a user group (Group-1). Even if it is enabled for the sub admin (Sub-1), backup users under that sub admin (Sub-1) and user group (Group-1) will not be able to use OneDrive as backup destination.

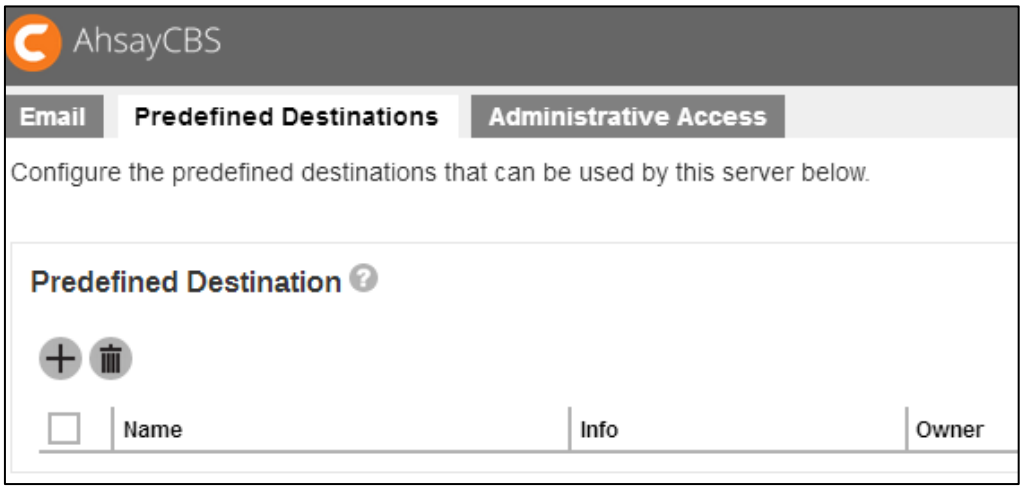
- Destination feature will not affect existing backup sets created before the upgrade.

- All the standard destination will be displayed but only the Predefined destination visible to users configured in "Users, Groups & Policies > Policy Group > Backup Set Settings > Destination Visible to Users" can be displayed here.

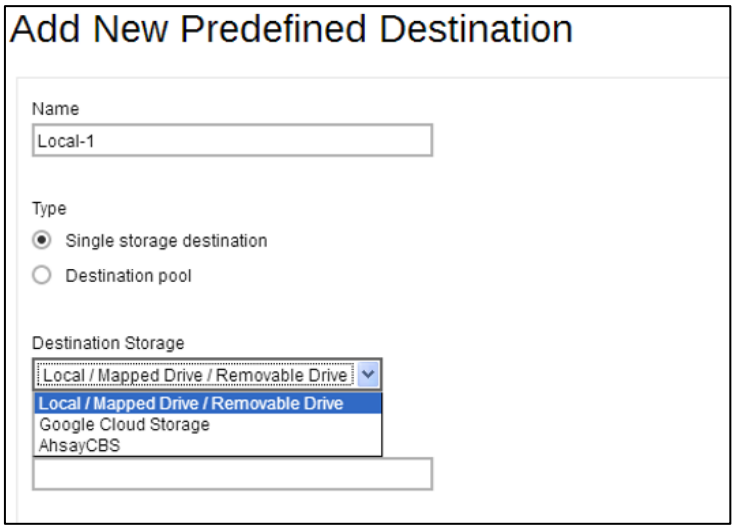
For example: If only enable “Local/ Mapped Drive/ Removable Drive” and “Google Cloud Storage” for the **Sub Admin User 1** whose type is Sub Admin.



Login AhsayCBS with **Sub Admin User 1**, go to System Settings > Basic > Predefined Destinations.



Click under Predefined Destination to add the new predefined destination. For the destination storage category, you can find that besides AhsayCBS, there are only “Local/ Mapped Drive/ Removable Drive” and “Google Cloud Storage” option available which are enabled by administrator.

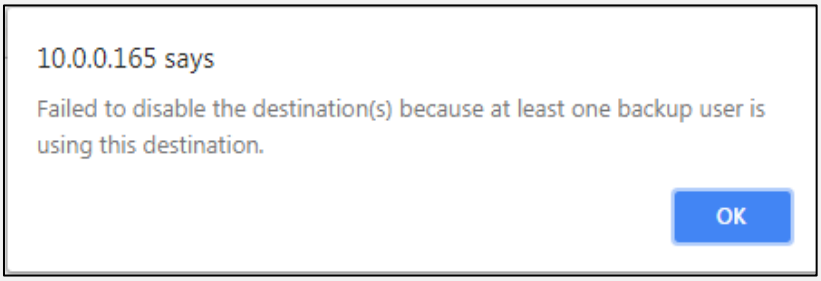


NOTE

- Sub admin user has NO authority to modify the Destination option, and the Backup User Settings tab is hidden in System Settings > Basic > Administrative Access > %System User% > Backup User Settings after login AhsayCBS with sub admin user.

- Destination setting determines the Standard Destination of “Users, Groups & Policies > Policy Group > Backup Set Settings > Destination Visible to Users” for Sub admin user, but will not influence the Cloud File Backup Source Visible to Users of “Users, Groups & Policies > Policy Group > Backup Set Settings” for Sub admin user.

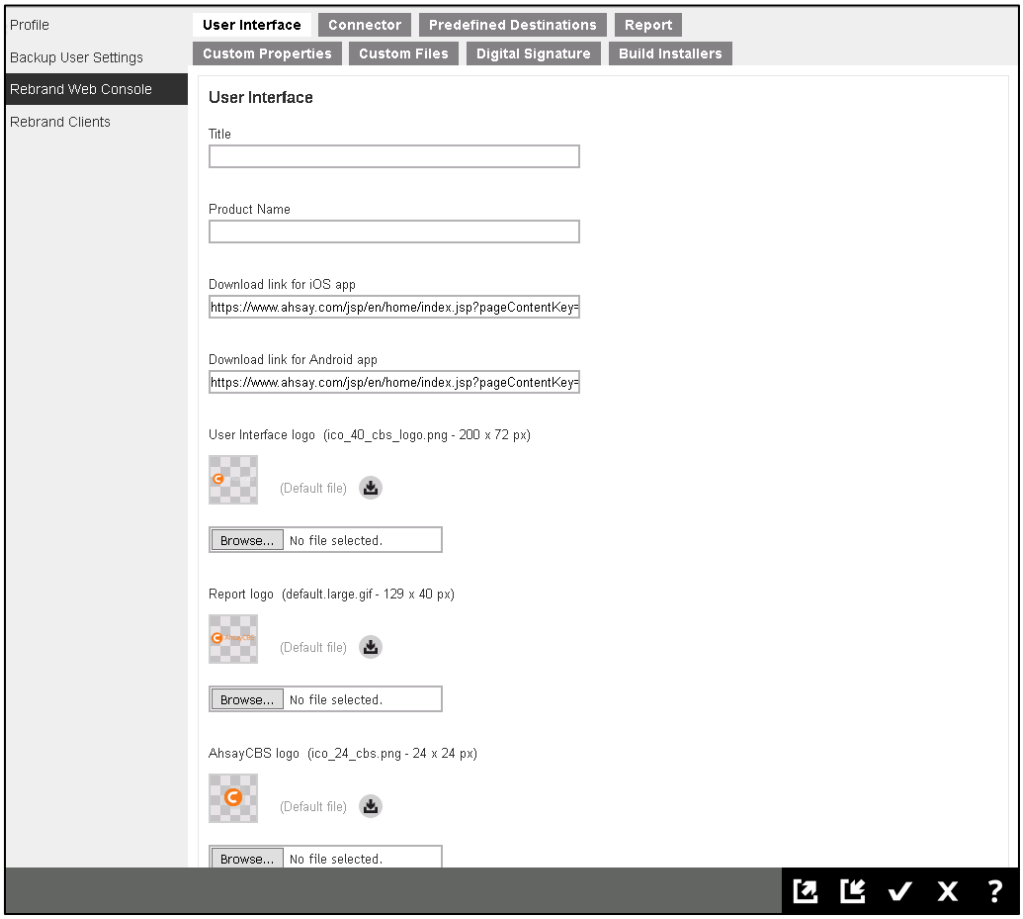
- If sub admin type user account has created backup user using the existing allowed destination, the according destination category cannot be disabled afterwards. The following screen shot shows the error prompted if trying to delete the destination category.



- **Rebrand Web Console Tab**

The Rebrand Web Console tab is available to admin and sub admin users after they login. Both admin and sub admin user can use this feature to rebrand the images on the AhsayCBS web console when accessed by the sub admins hostname.

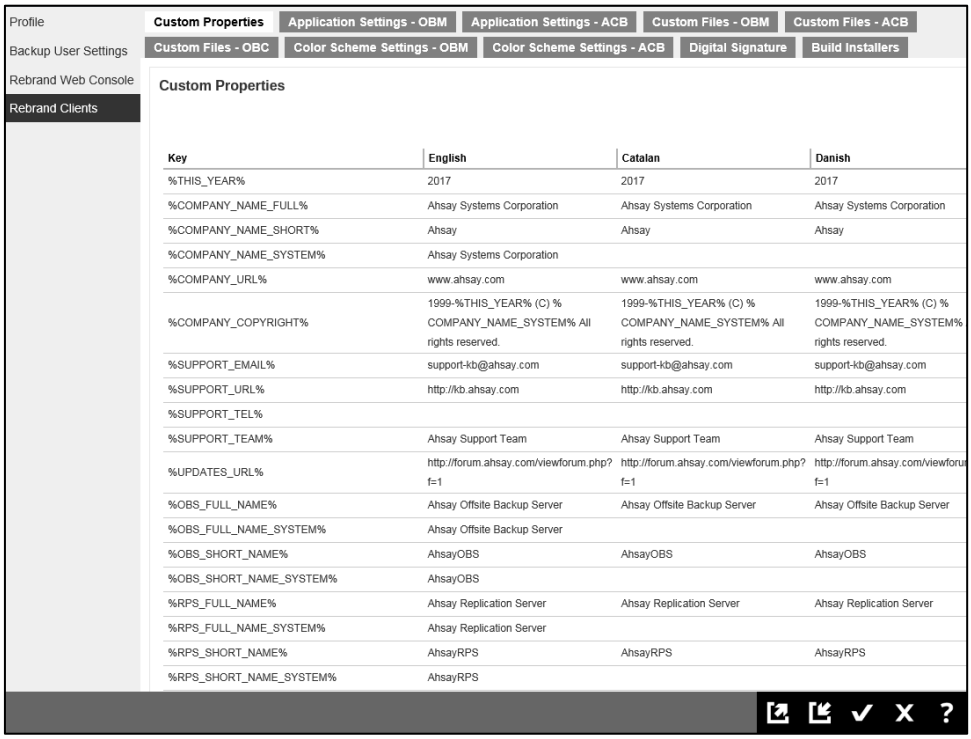
The following screen shows the Rebrand Web Console tab of the user used in our example, **Sub Admin User 1**, the type of the user is **Sub Admin**.



Rebrand Clients Tab

The Rebrand Clients tab is available to admin and sub admin users after they login.

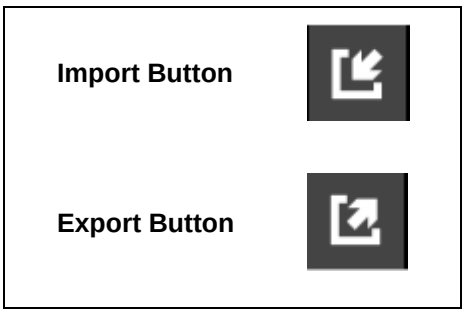
The following screen shows the Rebrand Clients tab of the user used in our example, **Sub Admin User 1**, the type of the user is **Sub Admin**.



Export/Import System Users

The export function can export the branded images, and branded properties that is set in the **Rebrand Web Console** and **Rebrand Clients** into a JSON format file. If you need to apply the branding to other sub admin users, you may import the branded JSON file back to the user.

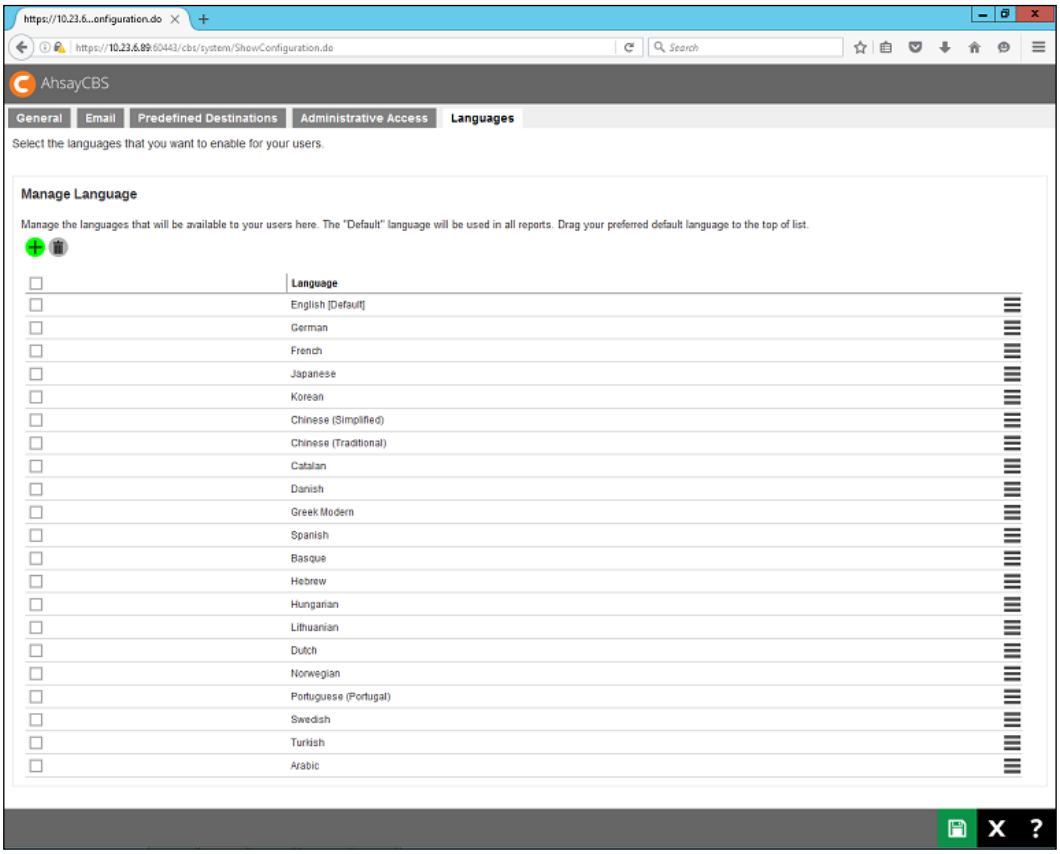
The **Import** and **Export** buttons are available to Admin and Sub Admin users only. They are found at the bottom right corner of the screen.



Languages

The following shows the **Languages** tab under **System Settings > Basic**. You can select the language(s) available to your users.

To change the default language settings for the AhsayCBS web console, simply drag your preferred default language to the top of the list.



To select the language you want to make available to your users, simply click check the box next to that language.

The available languages are:

- English (default)
- German
- French
- Japanese
- Korean
- Chinese (Simplified)
- Chinese (Traditional)
- Catalan
- Danish
- Greek Modern
- Spanish
- Basque
- Hebrew
- Hungarian
- Lithuanian
- Dutch
- Norwegian
- Portuguese (Portugal)
- Swedish
- Turkish
- Arabic
- Italian
- Portuguese (Brazil)
- Slovenian
- Polish
- Finnish
- Czech

Advanced Backup Server Configuration

To manage your AhsayCBS advanced backup server configurations, simply click the **Advanced** icon under **System Settings** from your AhsayCBS environment.

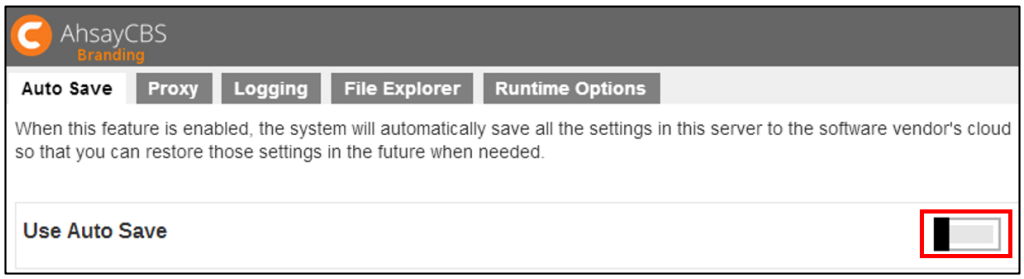
You can perform the following advanced configurations on your Backup Server:

- Restore data that has been automatically saved to Ahsay License Server.
- Configure settings for proxy connection
- Publish system and error messages to third party monitoring tools
- Retrieve system files for troubleshooting
- Configure run time options such as Java heap size, thread stack, etc.

There are 5 tabs under the **Advanced** system settings section, each of which is described below.

Auto Save

The following shows the **Auto Save** tab under **System Settings > Advanced**. Default setting of Auto Save feature is disabled, you can slide the switch to right to enable it.



When this feature is enabled, the system will automatically save all the settings in this server to the Ahsay License Server daily at 6:00AM, so you can restore those settings in the future when needed.

NOTE

Please kindly note that:

- The Auto Save feature is **NOT** supported for either Evaluation license keys or the expired license keys. If the license is expired, neither backup nor restore will be supported, and there will be "**LicenseError**" in "Monitoring > Backup / Restore Logs > Activities Log" showing "[disableConfArchival] License maintenance and support period has expired".

- Maximum of 30 snapshots will be created and saved in the Ahsay License Server. When over 30, the 31st snapshot will overwrite the 1st one. The size limit for each snapshot uploaded to Ahsay License

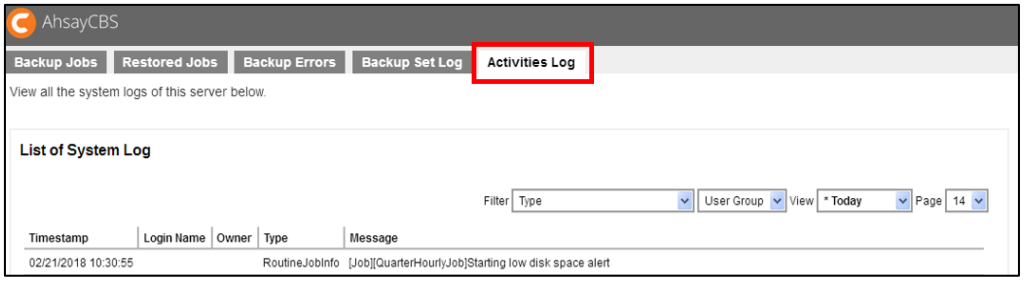
Server is 50MB, there will be "**RoutineJobError**" of "The size of "filename" is larger than 50MB." when the snapshot exceeds the size limit.

- The created snapshot will also be stored in the local drive with directory of "**%AhsayCBS_INSTALL%\AhsayCBS\conf\Backup\dr-YYYY-MM-DD.zip**". Maximum of 25 snapshots can be saved in the local drive, so when over 25, the 26th snapshot will overwrite the 1st one. You can check whether there is automatically delete process by searching the sentences of "[ConfigurationArchival.removeLocalBkp] Removed configuration backup file(s) [filename.zip] locally." in the AhsayCBS web console > Monitoring > Backup/ Restore Logs > Activities Log.

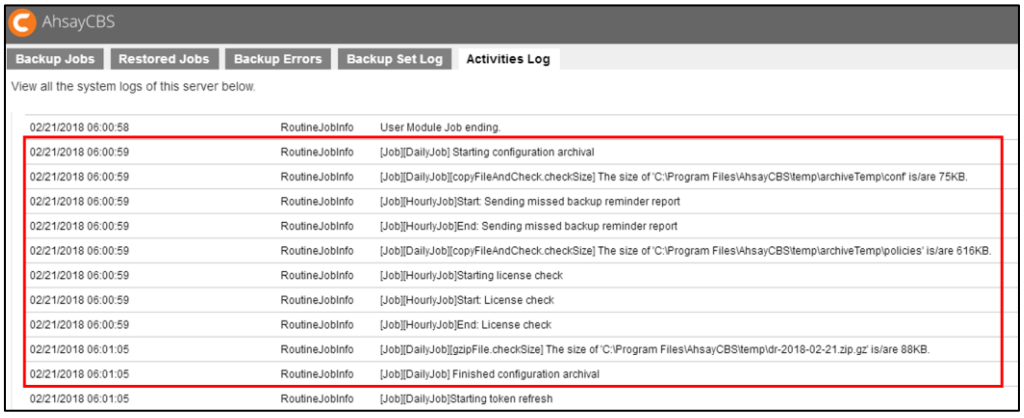
You can check the Auto Save daily job status by the following steps:

1. Click the **Backup/ Restore Logs** under **Monitoring** from your AhsayCBS environment.

2. Click **Activities Log** to find the according system log.



3. Search the log message of "**[Job][DailyJob] Starting configuration archival**" and "**[Job][DailyJob] Finished configuration archival**" with timestamp being around 06:00:00.

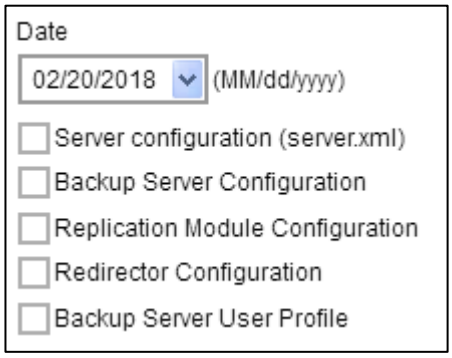


4. If the job is finished with no "**RoutineJobError**", the Auto Save job is finished successfully.

The following system configuration files will be saved on the cloud daily by the auto save system job.

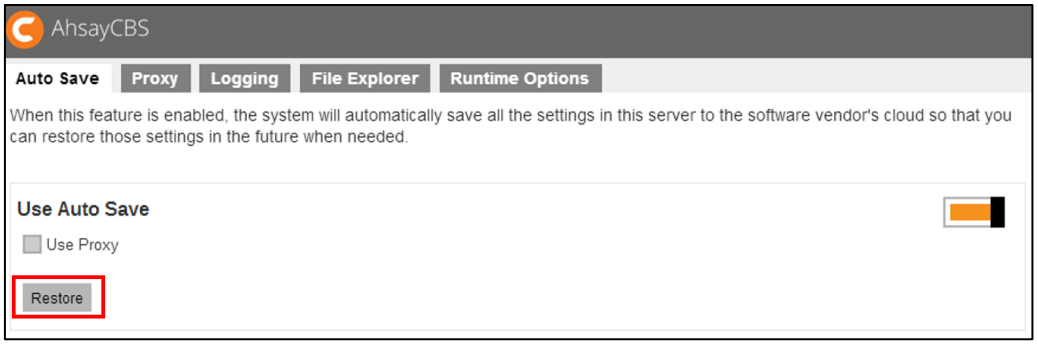
Server Configuration	
Description	**Path**
Connector setting file	/conf/server.xml
CBS option files	/conf/afc.opt /conf/cbs.opt
Runtime setting file	/conf/cbssvc.ini
Default certificate files	/conf/ca.crt /conf/ssl.crt /conf/ssl.key
CBS setting files	/conf/cbs.json
Redirector configuration files	/conf/lfsConfig.xml
OBS Configuration	
Description	**Path**
Backup Server setting files	/conf/obs.json
License files	/conf/lic.json /conf/license.xml
CBS/OBS option files	/conf/cbs.opt
Autoupdate index	/conf/autoUpdate.bdb
Replication configuration files	/conf/rpsSend.xml
RPS Configuration	
Description	**Path**
Replication configuration files	/conf/rps.xml /conf/rpsRecv.xml /conf/rps-recv.json
RDR Configuration	
Description	**Path**
Redirector configuration files	/conf/rdr.xml /conf/rdr.json
License files	/conf/rdr-lic.json /conf/rdr-license.xml
OBS User Profile	
Description	**Path**
Users' profile	/conf/users.xml
Others	
Description	**Path**
Branding directory	/conf/Branding/*.*
User group definition	/system/obs/policies/userGroup.xml
Policy group definition	/system/obs/policies/policyList.xml

Please note that there are no options to restore the **Others** category, however it will be restored automatically every time when you need to restore the auto save files.

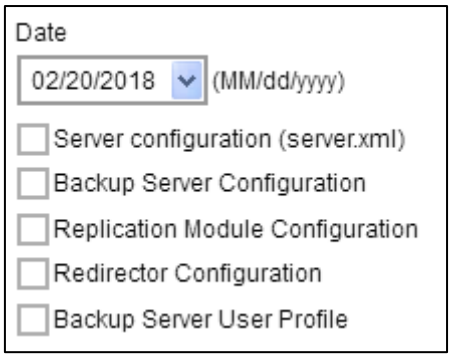


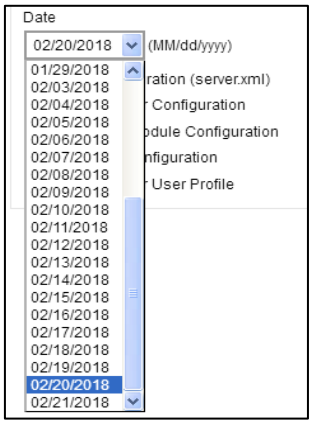
The restore process is as followed:

1. Click on the **[Restore]** button.

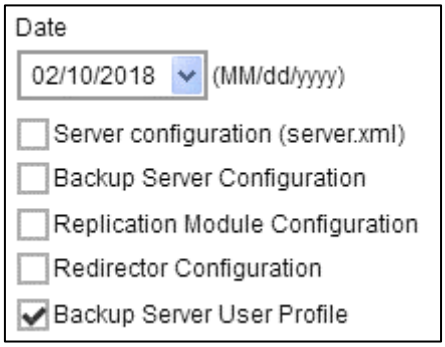


2. Select the date of the system settings backup from the drop down list.



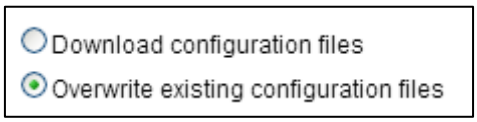


3. Select the type of configuration that you want to restore.



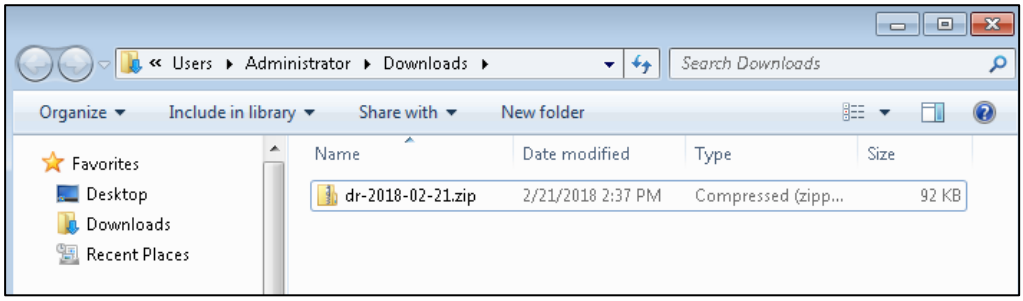
Click on to continue.

4. Choose which operation you want to make.

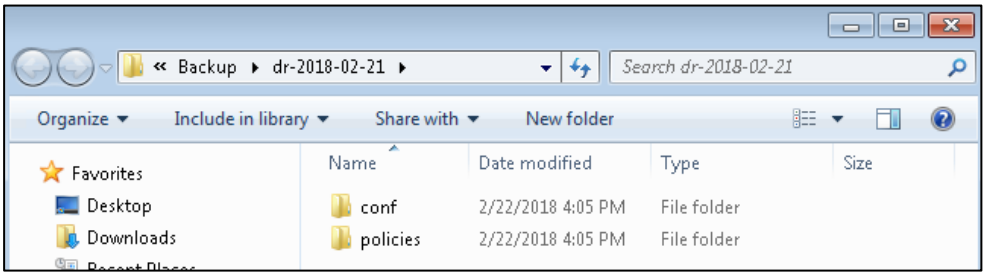


Click to start restore.

i. If click on "**Download configuration files**", the according configuration file "dr-YYYY-MM-DD.zip" will be downloaded and you can manually restore the configuration file.



- Extract the .zip configuration file.



- Copy the contents of "conf" folder to "%AhsayCBS_INSTALL%\AhsayCBS\conf".
- Copy the contents of "policies" folder to "%AhsayCBS_INSTALL%\AhsayCBS\system\obs\policies".
- Restart the AhsayCBS service.

Refer to the KB article [FAQ: How to recover my users.xml file from a previous backup on AhsayCBS v7.9.0.0 or above? (5198)] for further details on this feature.

ii. If click on "**Overwrite existing configuration files**", the backed up configuration file will overwrite the existing configuration file.

> **WARNING**
>
> Please kindly note that if choose **Overwrite existing configuration files** option, the backed up configuration file will automatically overwrite the existing configuration file and the process cannot be canceled.

- After restore process, the interface will skip back to the previous page. Click and to save and exit.
- Click **Administration Logs** under **Monitoring**.

- Click **Activities Log** to find the according system log.
- Search the log message of "**Starting configuration recovery**" and "**Finished configuration recovery**" with timestamp being starting restore operation time, which means the restore process is finished successfully.

02/21/2018 14:12:11	AutoSaveConfigInfo	Starting configuration recovery
02/21/2018 14:12:11	AutoSaveConfigInfo	Finished configuration recovery

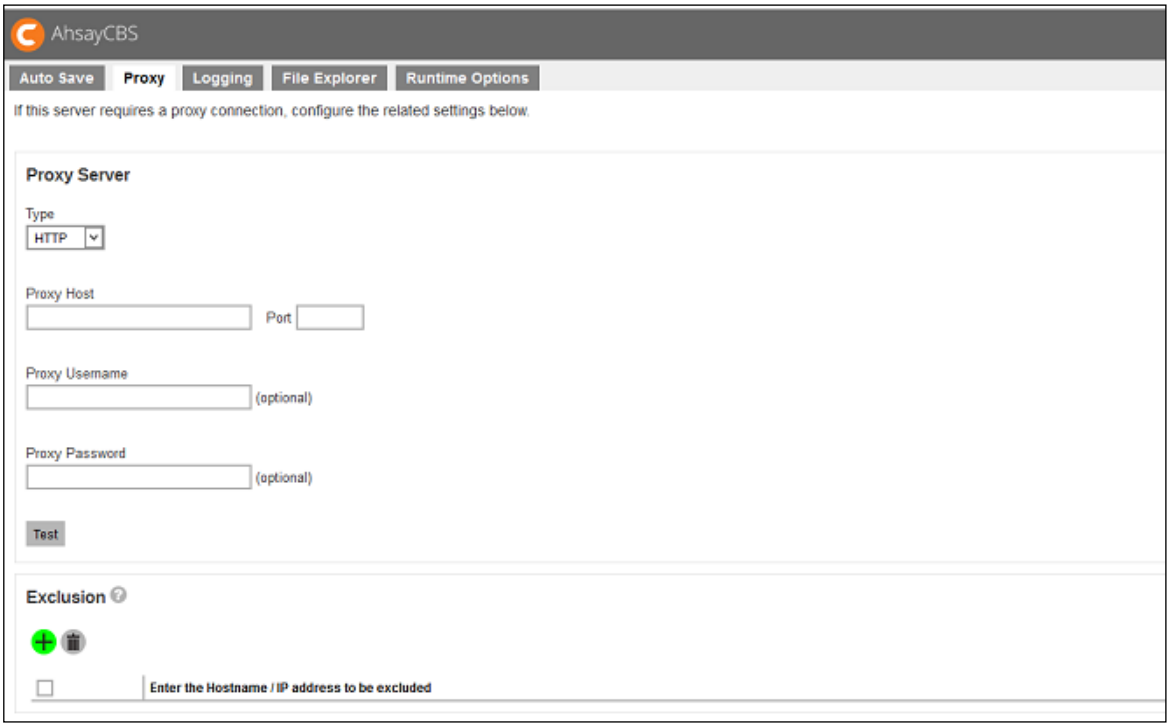
- Restart the AhsayCBS service.

Proxy

The following shows the **Proxy** tab under **System Settings > Advanced**. It is used for defining whether AhsayCBS should use a proxy to gain access to the Internet.

Two types of proxy, **HTTP/HTTPS** and **SOCKS 4/5**, are supported. You can use the **Proxy Host** and **Port** entries to define the location of your proxy server.

If the proxy server you are using requires user authentication, please use the **Proxy Username** and **Proxy Password** entries to set the username/password for your proxy server.



If you need to exclude some hostnames and IP address for proxy connection, you can add those excluded hostname and IP address at the bottom of the page.

NOTE

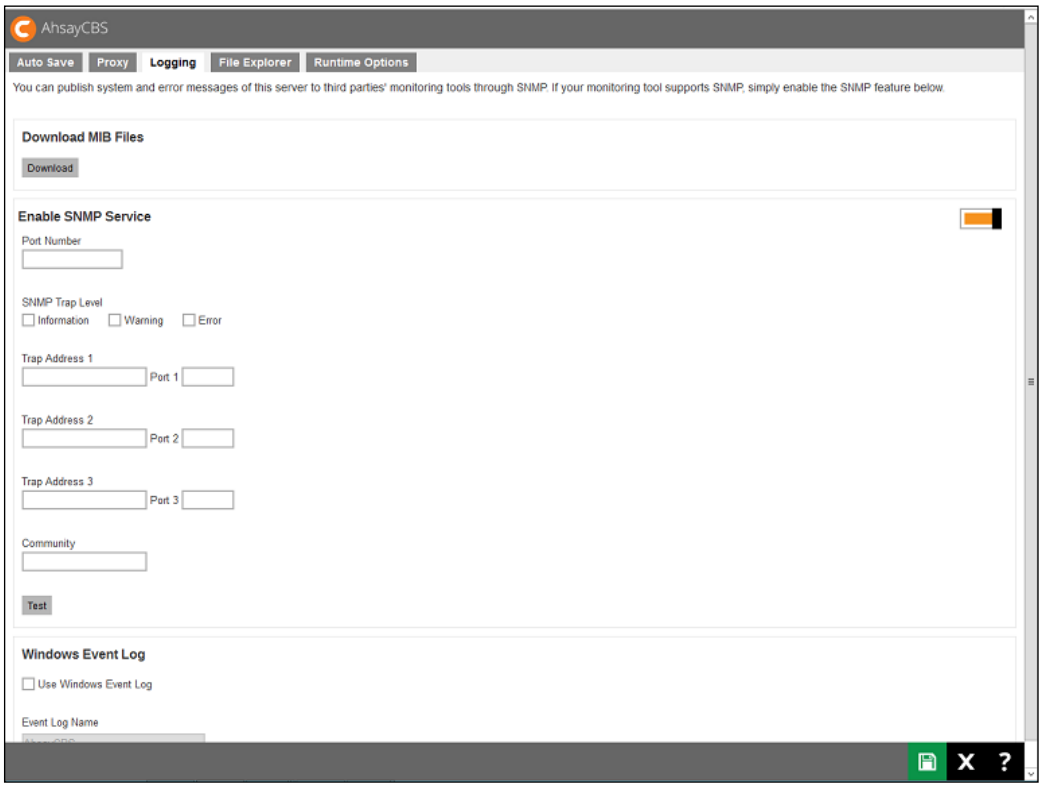
Please make sure there are no traffic restrictions on the proxy server, which could affect backup/restore performance.

Logging

The following shows the **Logging** tab under **System Settings > Advanced**. There are two types of third party monitoring support, SNMP and Windows Event Log.

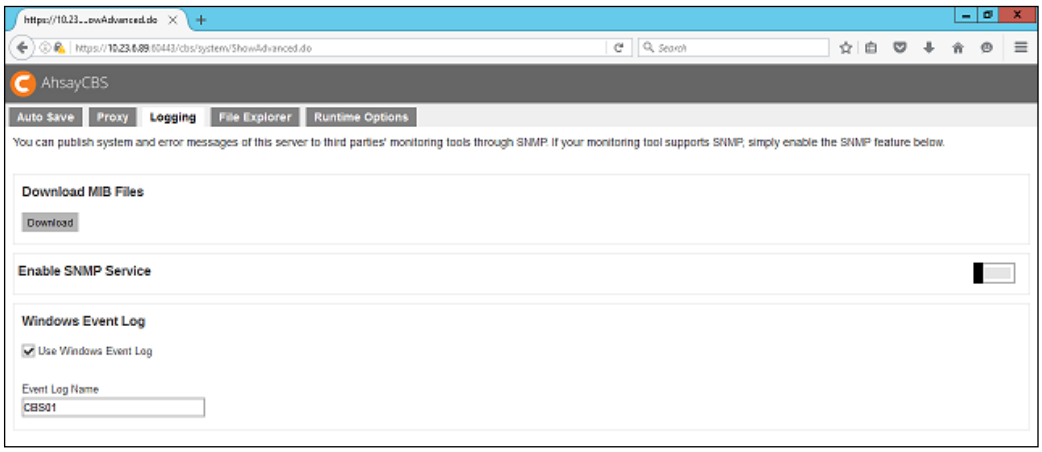
- **SNMP**

  For the SNMP, you can download the MIB definition file and import to your SNMP application by clicking the **Download** button under **Download MIB Files**.

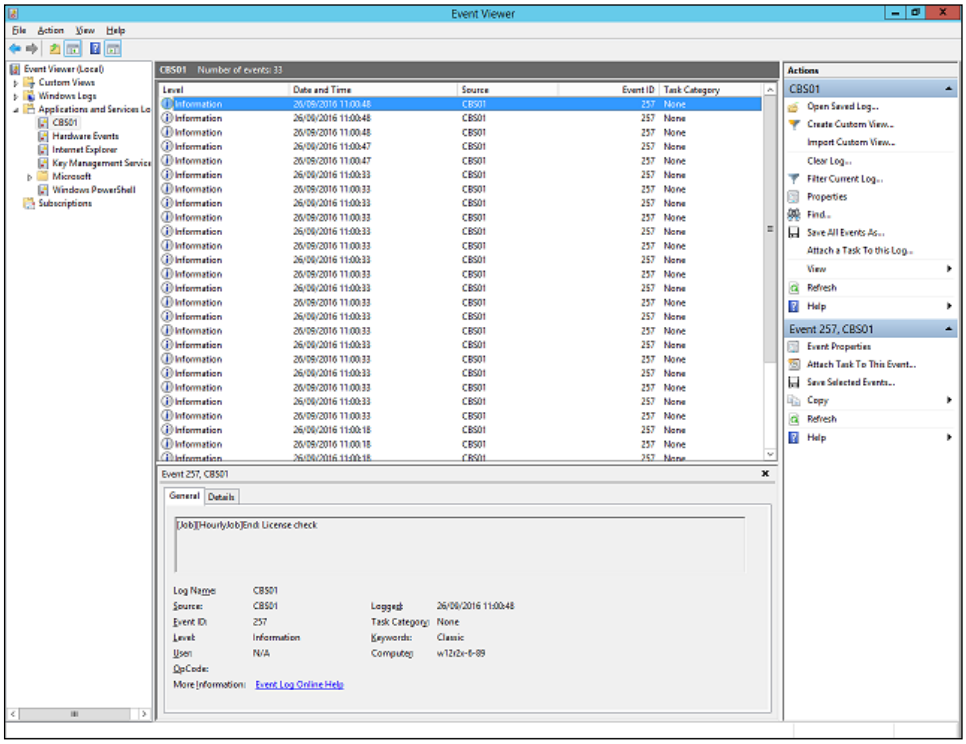


- **Windows Event Log**

  This feature is supported for AhsayCBS installations on Microsoft Windows platforms where the **Windows Event Log** service enabled. All AhsayCBS system log information such as errors, warnings, and information message types will also be written to the Windows event logs. The event log name is limited to eight characters.



The backup server's administrator can view the logs entries using the Windows event viewer.

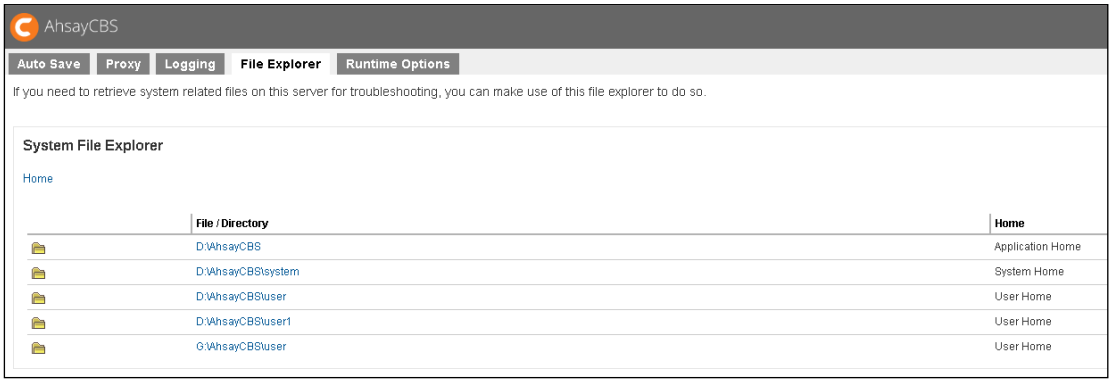


File Explorer

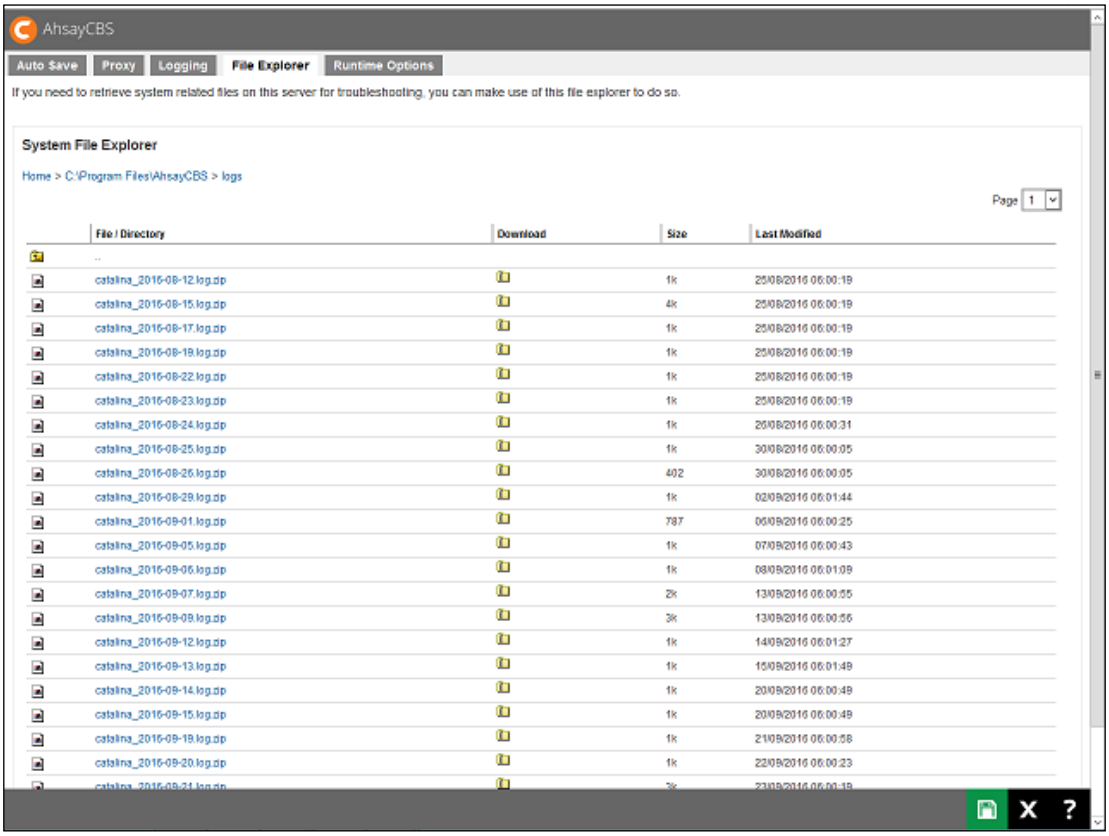
The following shows the **File Explorer** tab under **System Settings > Advanced**. If administrator or support staff needs to retrieve system related files on the AhsayCBS server for troubleshooting, they can make use of the **File Explorer** feature to download log or configuration files from the server without having to login remotely using RDP or SSH.

The **File Explorer** feature is limited to access files/folder related to AhsayCBS:

- AhsayCBS Application Home.
- AhsayCBS System Home.
- AhsayCBS User Home(s).



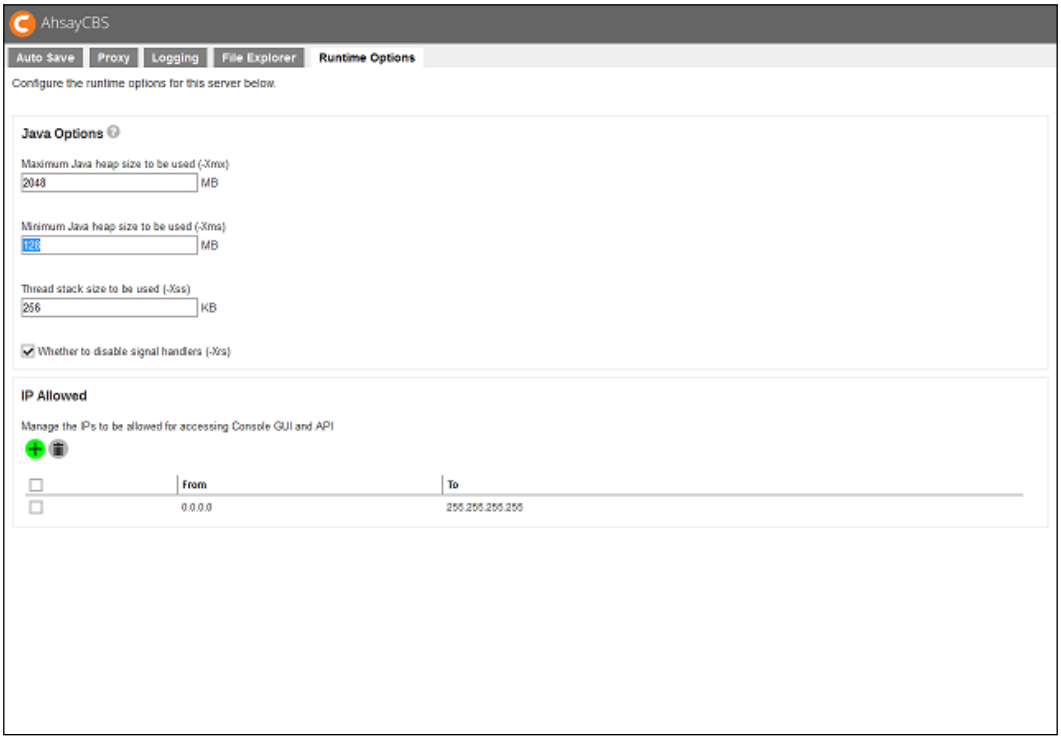
All files download via the AhsayCBS **File Explorer** tab are compressed by default.



Runtime Options Tab

The following shows the **Runtime Options** tab under **System Settings > Advanced**. It allows administrators to modify Java options such as Java heap size (maximum and minimum), thread stack size and IP allowed to access the AhsayCBS management console.

By default the maximum Java heap size is 1024MB and there are no restrictions on IP address access to AhsayCBS web console.



IMPORTANT

When editing the maximum heap size for AhsayCBS, ensure that there is sufficient memory reserved for the operating system.

It is not recommended to set excessively high values for the maximum Java heap size, as this could result in AhsayCBS performance issues during internal Java VM garbage collection or memory recycling routines.

For changes in Java heap size setting the AhsayCBS service needs to be restarted before it becomes effective.

6 Managing Backup/Restore

Backup / Restore Basic Configuration

To manage your AhsayCBS backup/restore basic configurations, simply click the **Basic** icon under **Backup / Restore** from your AhsayCBS environment.

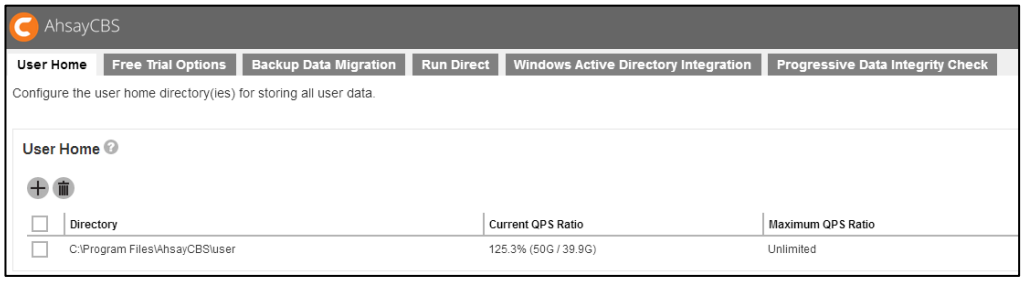
You can perform the following configurations for Backup/Restore:

- Configure user home directories.
- Configure free trial settings.
- Configure backup data migration settings.
- Define maximum number of concurrent VMs permitted to be started using Run Direct on AhsayCBS.
- Configure Windows active directory integration settings.
- Configure Progressive Data Integrity Check

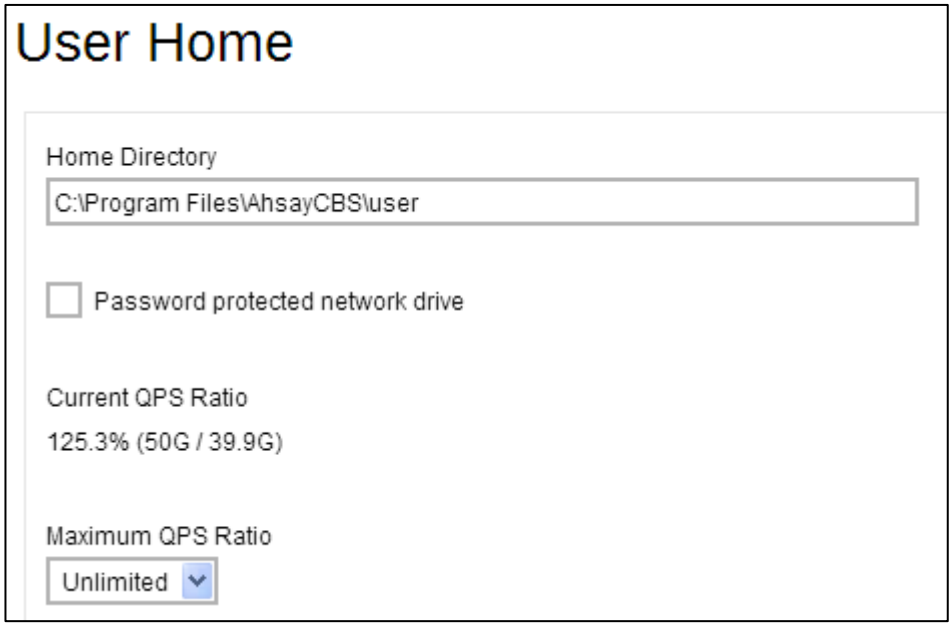
There are 6 tabs under basic backup/restore configurations, each of which is described below.

User Home

The following shows the **User Home** tab under **Backup / Restore > Basic**. It is used for configuring the user home directories for storing all the user data.



If you want to modify the existing user home, click on the user home directory and the following screen shot will appear:



Enter the **Home Directory** path and check the box next to **Password protected network drive** if your user home drive is on a network drive.

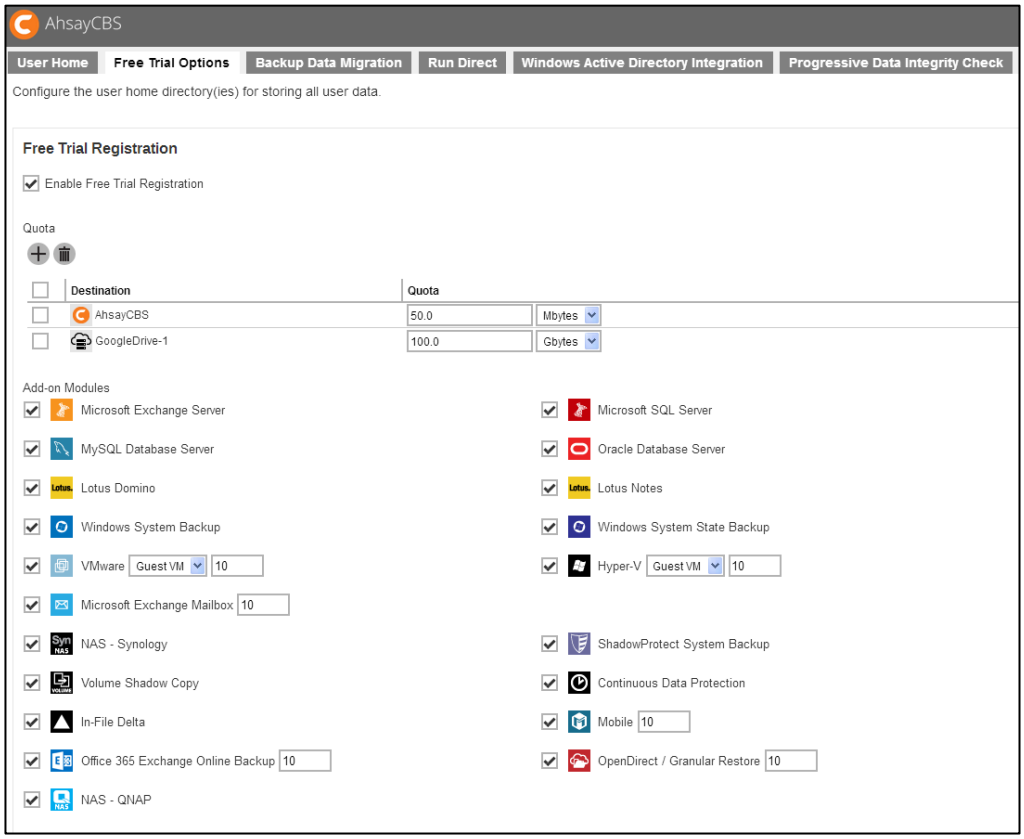
QPS Ratio (Quota - Partition Size Ratio) is the ratio (in percentage) of the sum of all user quotas within a user home divided by the total size of the partition of the user home. You can see the Current QPS Ratio displayed in the form of a percentage. You can select the Maximum QPS Ratio from the dropdown list.

If the QPS ratio of a user home exceeds the Maximum QPS ratio after adding a user, the user will be added to the next available user home. **Unlimited** means that the QPS ratio is not checked and new users can be added to that user home. **Not Used** means that new users are never added to that user home.

After you have modified the desired information, click to exit the Home Directory details page. Then click at the user home page to save your changes.

Free Trial Options

The following shows the **Free Trial Options** tab under **Backup / Restore > Basic**. It defines various free trial settings available in AhsayCBS.



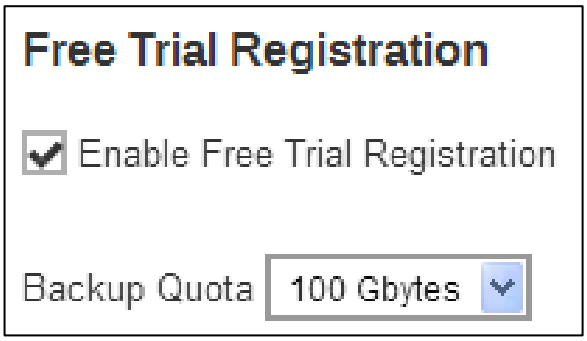
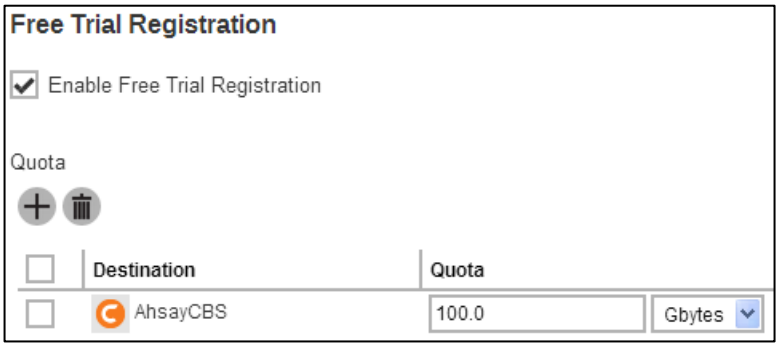
Trial users do not count towards the maximum number of users allowed within AhsayCBS under the paid software license, therefore it is possible to have an unlimited number of trial users within AhsayCBS. However, each trial user is limited to the quota storage settings for a period of maximum 90 days.

- To allow users to create a trial backup account from AhsayOBM or AhsayACB, please enable the **Enable Free Trial Registration** option at the top of the page. If this feature is unchecked, the option to register for a trial account will not be available to end users.

- From v7.15.6.0, the **Destination** and **Quota** defines the backup destination and quota for per destination of trial backup accounts upon registration. Destination includes predefined and standard destination, and the quota settings for free trial user account is independent of the quota settings in Group Policy. For the backup destinations which are not listed under Quota tab, the quota storage assigned for the destination is unlimited.

  The following screen shot shows the comparison for quota management between pre-v7.15.6.0 and post-v7.15.6.0.

Pre-v7.15.6.0	The Backup Quota defines the maximum backup quota of trial backup accounts upon registration.

	Situation: Define the backup quota to be 100GB. 
Post-v7.15.6.0	After migration, there will display AhsayCBS with quota setting being 100GB. You can configure the quota setting for AhsayCBS and click ⊕ to add predefined destination as required. 

- The **Add-on Modules** option defines whether you want to allow trial users to have different add-on modules.

- The **User will be suspended after <xx> days** option under **Settings for existing free trial users** defines the number of days after which the trial users will be suspended. In our example, the period is **30** days, and the maximum value is **90** days.
- The **Remove User <xx> days after registration** option under **Settings for existing free trial users** defines whether you want to remove trial backup users for certain number of days after registration. In our example, you can use this option to tell AhsayCBS to remove trial backup users from the system automatically after backup users have registered for **60** days, and the maximum value is **180** days.

Backup Data Migration

The data migration is designed to migrate backup sets that were created in v6 backup server to v7 backup set blocks format to take advantage of the backup/restore performance enhancement delivered by the new file storage format.

In v6 backup set, all the backup files are stored as individual files in the user home, whereas in v7 files will be handled in the following ways.

Small files (16MB or smaller)	Merge into one 16MB data block
Large files (32MB or above)	Split into multiple 32MB data blocks
NAS server	Merge/split into 8MB data black(s)
Mobile device	Remain in native format

The data migration process converts the v6 backup files into v7 backup set format, it will read small files that were stored in v6 backup set, and write a number of small files into a new data blocks. For larger files, the process will read a fixed amount of data which equals to a data block size from the selected large files, and rewrite the data block into a new 32MB data block file. The process will continue until the large file has completed to write the data into multiple new data blocks.

IMPORTANT

As the data migration process is **NOT** reversible. If you downgrade your backup server to v6, the migrated data in v7 will not be usable. All historical backup are lost and you need to start over the backup again in v6. Please communicate with your clients and check if they are comfortable with the upgrade and data migration.

Suggestion and Requirement

The data migration process will perform the backup set migration one by one. To avoid heavy I/O on the disk/CPU utilization on your backup server, we suggest you to perform the data migration in a small batch of users to test the performance on your environment. This would minimize any possible impact on the I/O usage or affect your current backup operation.

The data migration will be carried out if the following criteria are met:

1. Both AhsayCBS and AhsayOBM/AhsayACB are upgraded to v7.7 or later version.
2. More than 100GB of free space in each user home on your backup server is available.
3. For large backup sets that are more than 100GB of total size, please reserve more than 150% of the free space on the user home for the data migration. This is because the migration process will read the v6 backup data and write the v7 format to new location. After the migration, the reserved space will be recovered.

   Free Space = Largest v6 backup set on the user home X 150%

   For example: If your largest backup set is 150GB backup set, please reserve at least 225GB of free space for the migration.

If these requirements are not met, the data migration will not be started. You may find the following entry in the [**Activities Log**] available in your AhsayCBS, [**Monitoring**] -> [**Administration Logs**]

E.g. MigrateV6DataError [Thread][Job][MigrateV6File]Error Migrating v6 data of user ... is too big to be migrated to ...

By selecting the filter "MigrateV6DataError" from the filter drop down box, you can collect the errors related to the data migration.

REMINDERS

1. If data replication has been turned on, after the v6 data migrated to the v7 format, the replication will start to replicate new v7 format backup set to the replication server or to a predefined destination
2. You may notice that the storage of that user will be doubled for a short period of time. For example: the replicated v6 backup set is 10GB, after the data migration, another 10GB will be used for replicating the new v7 format backup set. After the synchronization is completed, there is a mechanism to clean up the old migrated v6 data automatically.

How to Perform the Data Migration

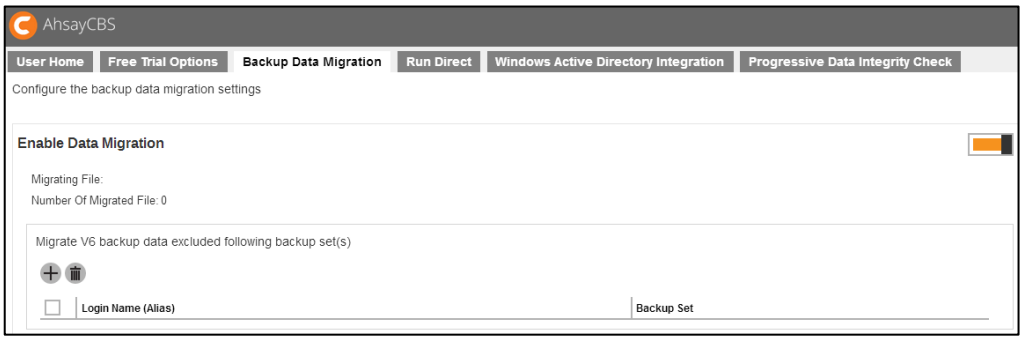
IMPORTANT

While a backup set is undergoing the data migration process, the following activities pertaining to that particular backup set **CANNOT** be performed.

Data Integrity Check	**Space Freeing Up**
Delete Data	**Delete Backup Set**

That being the case, update of the backup set, such as backup schedule, backup source, destination, etc., is still possible during the data migration process.

1. Upgrade both AhsayCBS and AhsayOBM/AhsayACB to version 7.7 or above.
2. Administrator needs to check if any backup set should be excluded in this data migration operation. For example, when we need to limit the number of migration in a small batch of backup sets, we can exclude some of the backup sets from the interface. Click the “+” icon under the Enable Data Migration section to add the user(s) you wish to exclude from the migration.



3. Click at the bottom right corner to start the migration when you are ready.

4. Once the backup runs on the client machine, the index migration starts on the client machine. When the index migration finished, the AhsayCBS will arrange the data migration on the backend.

5. Administrator can check the migration activity through the **Monitoring** > **Administration Logs** > **Activities Log**.

   By selecting the filter "MigrateV6DataInfo" or "MigrateV6DataError" from the filter drop down box, you can collect the logs related to the data migration.

6. When the data migration completed on a client's backup set. You will see the following in the activities log.

   ```
   MigrateV6DataInfo [Thread][Job][MigrateV6File] End: migrate v6 data.
   ```

7. On the next backup, that client will use the new index and new migrated data for the backup operation. This will also trigger the backup server to remove old v6 backup data.

NOTE

In case the index migration stops for any reason, on the next backup, the index migration can resume from the last recorded progress.

For backup sets such as Exchange DAG, when one of the node triggered the index migration when backup runs, all other nodes will wait for the first node to complete the index migration, and all other nodes will reload the new index file.

During the old v6 backup data removal, the performance on the user home which stores the v6 backup data could be slow down.

To add the exclusion of a v6 backup set from the data migration:

1. Click on under the **Migrating File** section.

2. Select the login name and backup set that that you wish to exclude from the data migration.

3. Click to continue.

To delete an existing exclusion of a v6 backup set:

1. Click on the check box next to the entries you wish to delete.

2. Click on the icon in this section.

3. Click to confirm.

4. Click at the bottom right corner to confirm again.

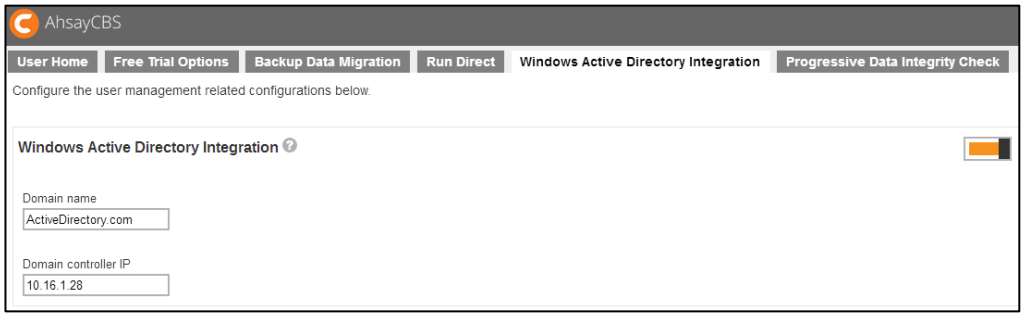
Run Direct

The following shows the **Run Direct** tab under **Backup / Restore > Basic**. It defines the maximum number of virtual machines started by Run Direct on AhsayCBS. Simply enter the number of virtual machine and click to save your changes.

For more information on Run Direct on AhsayCBS, please refer to the Ahsay Cloud Backup Suite v7 User's Guide.

Windows Active Directory Integration

The following shows the **Windows Active Directory Integration** tab under **Backup / Restore** > **Users, Groups & Policies**.



When this feature is enabled and AhsayCBS fails to authenticate a user logon using its own records, a user authentication will be dispatched to Windows Active Directory automatically. This means that if an AD is presented in the network, it is only required to create a user account once in the Windows Active Directory. The same user account can also be used on the AhsayCBS server. This is because AhsayCBS will create this user account automatically after authenticating this logon using AD. The user account created will be of the type **Paid** and of backup client **AhsayACB** (unless the user logon using AhsayOBM).

To enable Windows Active Directory Integration

1. Click the switch on the right to turn on this feature.
2. Enter the Domain name and Domain controller IP of the machine where the active directory is hosted.
3. Click the button at the bottom of the page to confirm.

Progressive Data Integrity Check

The progressive data integrity check feature is introduced since AhsayCBS v7.17.0.0.

The Progressive Data Integrity Check tab can be accessed under **Backup / Restore** > **Users, Groups & Policies**.

Note: The feature is enabled by default after installation / upgrade to AhsayCBS version 7.17.0.0 or above.

Below is the features of progressive data integrity check (DIC):

- **Automatic Apply**: When the progressive data integrity check (DIC) feature is enabled, a progressive data integrity check (DIC) job will be performed automatically before the start of each backup job to ensure that the integrity of the backup data are correct.
- **Regularly Apply**: The progressive data integrity check (DIC) will perform check for backup data regularly based on the value configured for the progressive DIC interval.
- **Centralized Control**: The progressive data integrity check (DIC)feature centralized the control of progressive DIC for all backup users and backup sets.
- **Fast**: The progressive data integrity check (DIC)feature will only perform check for backup files in the current data area and the latest index, so therefore, the progressive DIC process can be completed quickly.
- **Efficient**: The progressive data integrity check (DIC) feature will only check for backup files outside of the progressive DIC interval.

Below is the table of comparison between Progressive DIC and Manual DIC.

	Progressive DIC	Manual DIC
Speed & Performance	➢ Regular progressive DIC will be applied automatically to ensure the integrity of data. ➢ Backup time will be longer as the progressive DIC process needs to be completed before each backup job is started. ➢ Progressive DIC is faster than manual DIC, as it only performs check for backup files in current data area and the latest index, that are outside of the progress DIC interval.	➢ DIC must be applied manually. ➢ Manual DIC will not influence the backup process time. ➢ Manual DIC takes longer to complete, as it performs check for all backup data in both the current and retention area, along with all indexes.

Checked Data & Index	➢ Current data area. ➢ The latest index.	➢ Current & retention data area. ➢ All indexes.
Run on Server **or** **Run on Client**	Support both Run on Server and Run on Client backup set.	Only Cloud File backup set and Office 365 Exchange Online backup set can support both Run on Server and Run on Client. Others backup types can only support Run on Client.
DIC Log	Only sentences for the start and end of the progressive DIC job and progressive DIC interval but no detailed logs.	Detailed logs about which files were checked and the whole DIC process will be shown in the manual DIC log page.
Removal Action	➢ If a backup file does not exist physically at the backup destination, the process will automatically remove record of the corresponding backup file from the index file. ➢ If a backup file exists, but the index file does not contain record of the backup file, no removal action will be executed.	For both cases where a backup file does not exist physically at the backup destination, or the index file does not contain record of a backup file, the user will need to manually click to start and confirm on the data removal of the backup file, or record from the index file.
Trigger Replication	No as progressive DIC will not delete or modify any backup files.	Yes if manual DIC delete any corrupted file.
Deployments	Suitable for administrator who wants to perform regular simple data integrity check for all users automatically to ensure that the integrity of all data are correct.	Suitable for end user who wants to perform a full data integrity check manually to locate any mismatch between the backup data and index, that may cause backup failure.

To enable Progressive Data Integrity Check

1. Click the switch on the right to turn on this feature.

2. Enter the progressive data integrity check interval that you want to configured, in the textbox under “Progressive Data Integrity Check (DIC) is executed before running backup”.

   The progress data integrity check job will only perform check for backup files that have not been checked within the specified interval.

Precisely, this means that there will be a last DIC check time marked for each backup file, and the progressive data integrity check (DIC) will perform check for file if its last data integrity check (DIC) time exceeded the progressive data integrity check (DIC) interval.

Note: The default value is set to 60 days.

NOTE

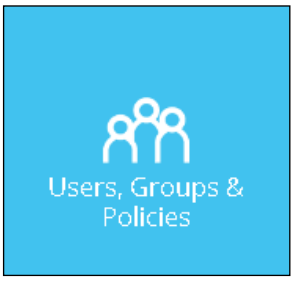
Please kindly note that:

- The progressive data integrity check job will only perform check for backup files that have not been checked within the PDIC interval configured, but a manual DIC job will perform check for all backup files, in both the current and retention area, even if the file are within the progressive DIC interval.
- The minimum value that you can configure for the PDIC interval is 1 day, there is no limit to the maximum value that you can configure.
- If the Progressive DIC interval is set to a small value, the time for each backup job to complete will be longer, as data file would be checked more often (due to the small Progressive DIC interval). However, setting the Progressive DIC interval to a small value can further minimize the possibility of data corruption (e.g. backup files and index mismatch).
- On the other hand, if the PDIC interval is set to a large value, the time for each backup job to complete will be shorter (compared to if the interval is set to a small value), as data file would be checked less often (due to the larger PDIC interval). However, setting the PDIC interval to a large value may increase the possibility of data corruption (e.g. backup files and index mismatch).

3. Click the button at the bottom of the page to confirm.

Manage Backup Users

To manage your AhsayCBS users, groups, and policies, simply click the **Users, Groups & Policies** icon under **Backup / Restore** from your AhsayCBS environment.

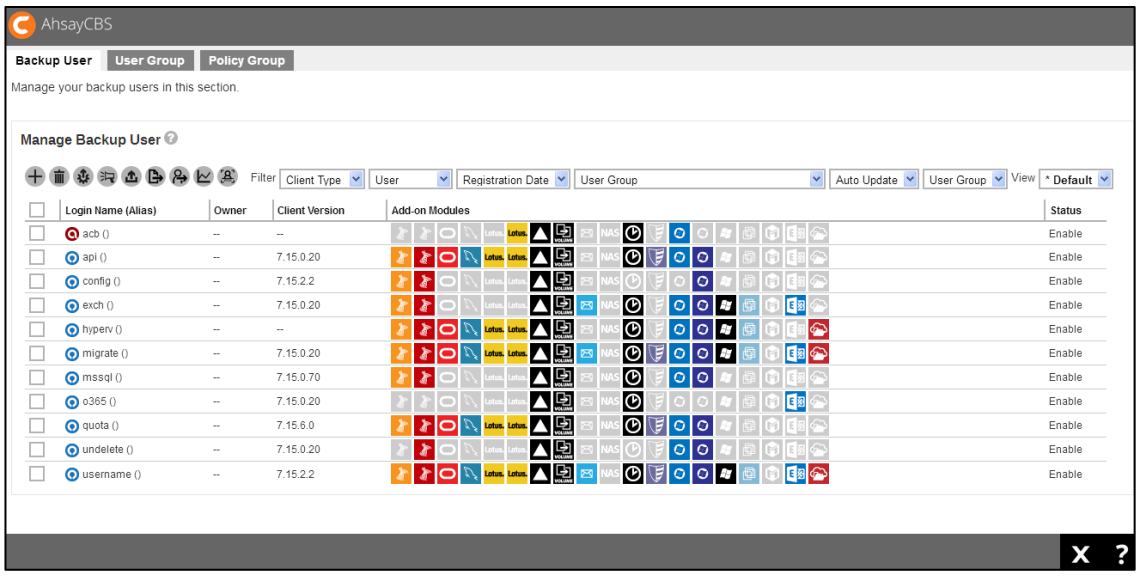


There are 3 tabs under managing users, groups, and policies, each of which is described below.

Backup User Tab

A backup account contains user's account information, client type, backup modules and backup set settings, etc. A backup user account can be created by administrator or registered via the backup client application by the end user as a trial account (if this option is enabled).

The following screen shows the **Backup User** tab under **Backup / Restore > Users, Groups & Policies**. You can create a new user account on this tab.



If AhsayCBS is deployed for internal use, as a system administrator, you need to determine the following when you create a backup account:

- Backup client type, whether it is **AhsayOBM** or **AhsayACB**
- Backup destination

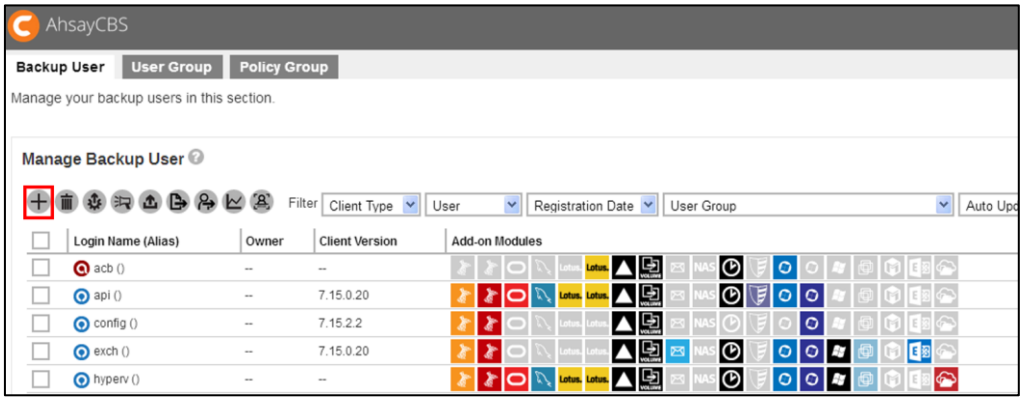
If you are a Managed Service Provider (MSP) or reseller you may require to take into consideration the following items when you create a backup user account:

- Types of users, whether it is **Paid** or **Trial**
- Backup client type, whether it is **AhsayOBM** or **AhsayACB**. Also the modules subscribed by the client.
- The backup destination and the subscribed quota

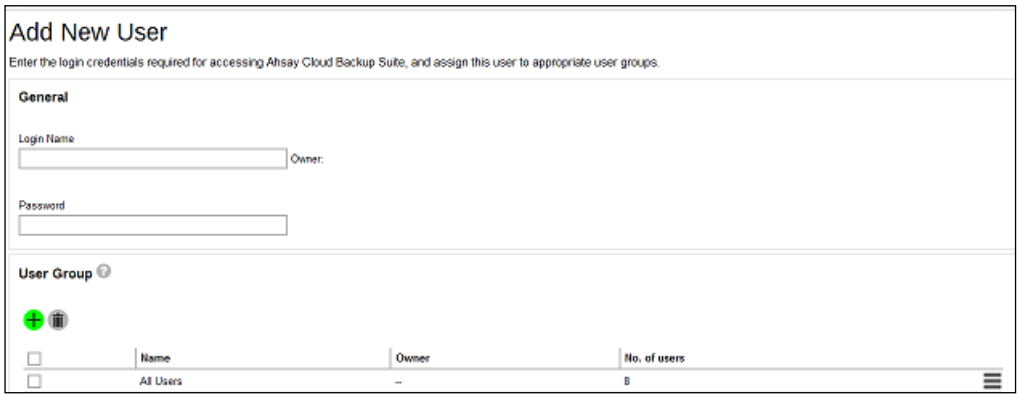
Create a New Backup User

To create a new backup user, do the following:

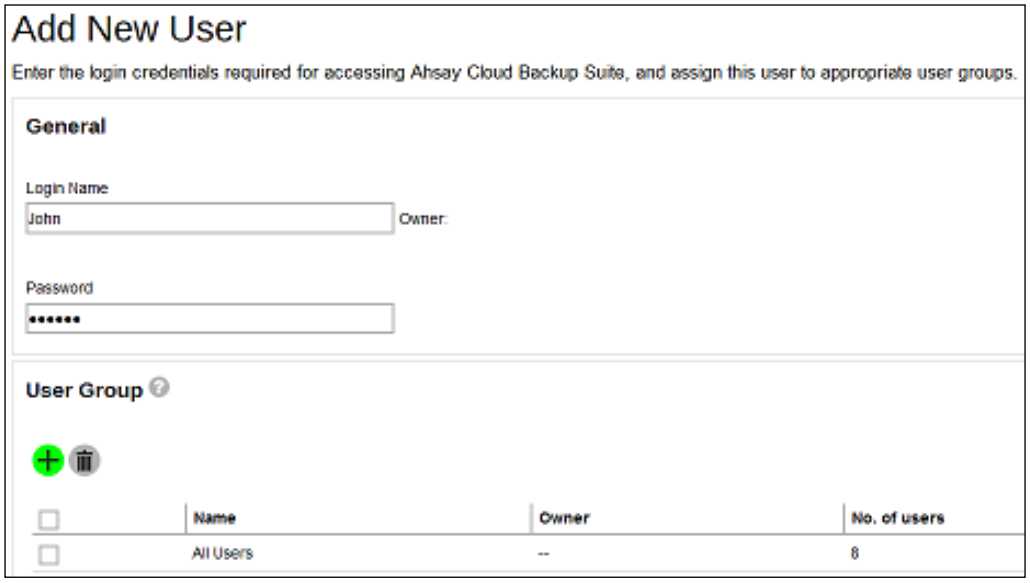
1. Click as highlighted below.



2. The **Add New User** page appears.



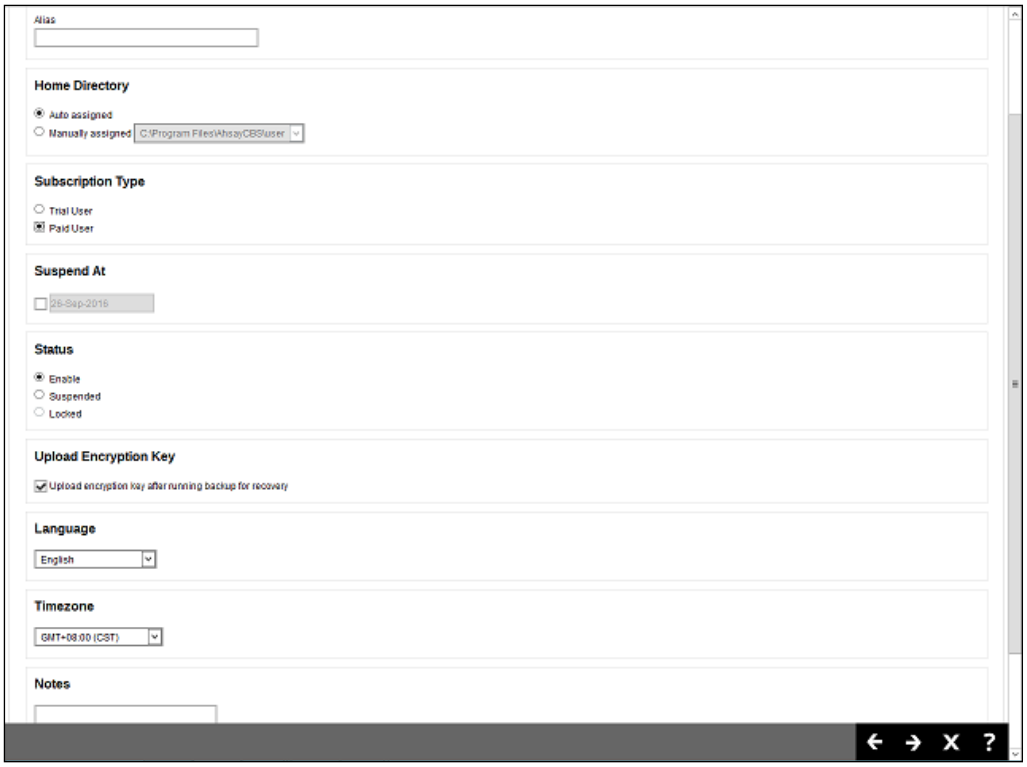
3. Enter the **Login Name**, **Password**, and select the **User Group** by checking the desired user group. Click → to proceed.



4. Enter the following information that appears on this page.

Field	Description
Alias	Another name of the backup user.
Home Directory	You can select **Auto assigned** or **Manually assigned** user home path. The user backup data will be stored here.
Subscription Type	There are 2 subscription types: **Trial User** and **Paid User**. Trial users are subject to automatic removal as defined by the **Free Trial Options** tab under **Backup / Restore** > **Basic**. The automatic removal option can be disabled.
Suspend At	A scheduled date to suspend this user. For trial users, the suspension date is based on the settings in the **Free Trial Options** tab under **Backup / Restore** > **Basic**.
Status	There are 3 types of status for a user account: **Enable**, **Suspended**, and **Locked**. Under normal circumstances, administrator may change the **Enable** or **Suspended** status of a user. The **Locked** status is referring to account lockout rules that are set inside the policy group, refer to the Managing Policy Groups section for more details. For example, if a user has 3 consecutive unsuccessful login attempts in 30 minutes, the user account will be locked out.
Upload Encryption Key	Once you enabled the encryption recovery option, the encryption key file is uploaded to the backup server. In case the user forgot the encryption key, you can still contact us to have it recovered. The recovered encryption key will be sent directly to the email address registered on the user account. Refer to the Encryption key section for further details.

Language	Preferred language for all email reports of the backup user.
Timezone	Time zone of the backup user. Since AhsayCBS v7.15.0.8, timezone information will be automatically updated when user login client backup agent, such as AhsayOBM and AhsayACB, or perform backup job to avoid the false alarm of missed backup job.
Notes	A field for administrators to add notes for the backup user.



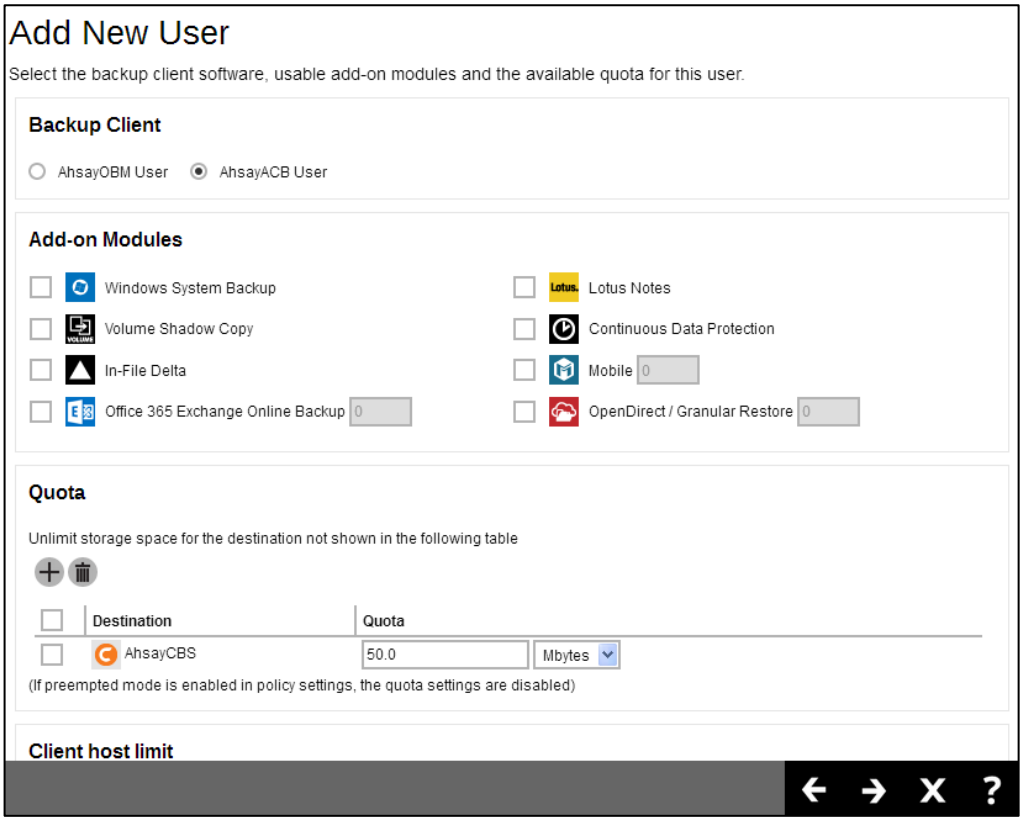
Click to proceed when you are done with the settings.

5. Enter the following information that appears on this page.

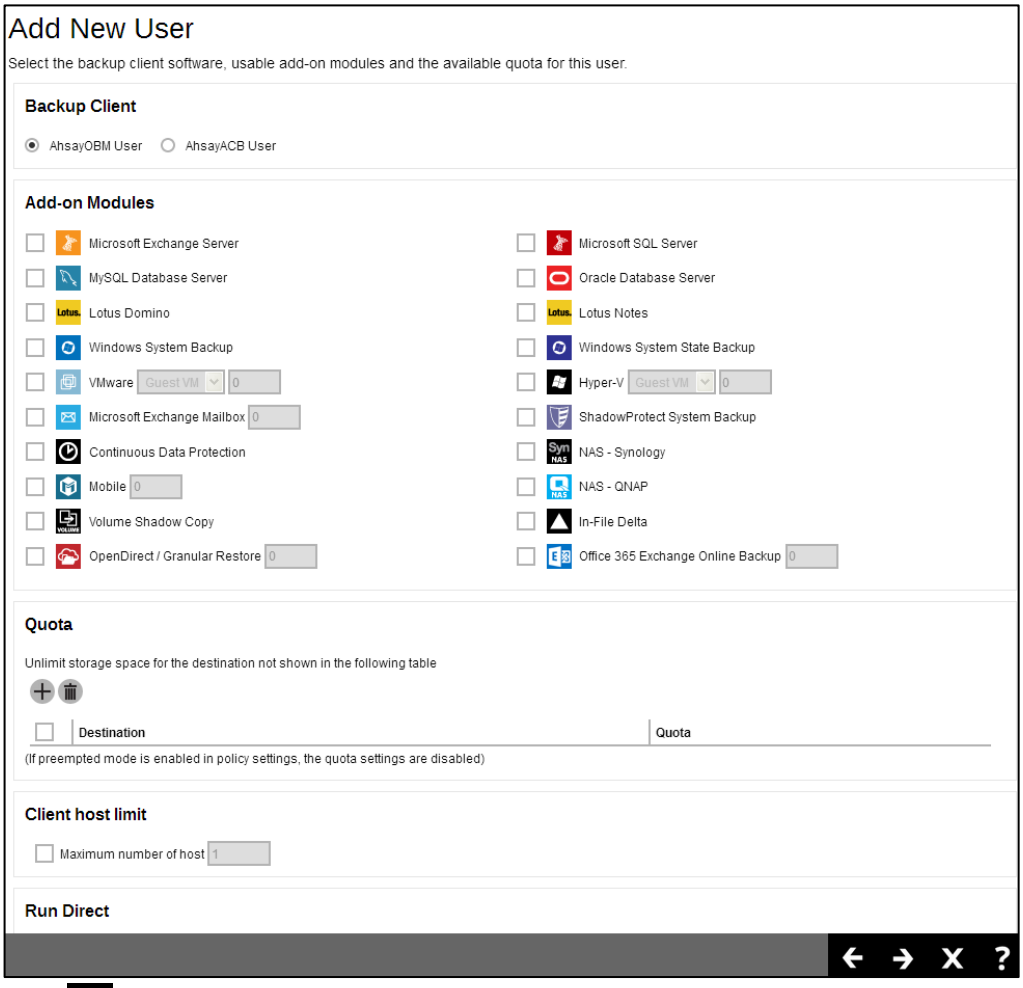
Field	Description
Backup Client	If the backup client machine requires to backup files only, such as a desktop computer or a notebook, then you can simply create an **AhsayACB** backup account. Otherwise, you will need to setup **AhsayOBM**, because it comes with backup modules to perform Windows system backup, database backup and virtual machine backup. By default **AhsayACB** backup account is selected.
Add-on Modules	You can select which add-on module to enable for the backup user. Some add-on modules has a text field after its name. For example, the number after **Microsoft Exchange Mailbox** defines the number of Exchange mailboxes that are allowed to be backed up under this user account.

Quota	Backup **Quota** of each destinations for the user account. Refer to the User Settings Tab section for details. **Note:** Quota management for individual predefined destination is only available for AhsayCBS version 7.15.6.0 or above.
Client host limit	This is to limit the maximum number of hosts allowed in a client's backup account, i.e. the number of devices that they can install AhsayOBM/AhsayACB on. Refer to the User Settings Tab section for details.
Run Direct (For AhsayOBM only)	Set the maximum number of VMs for VM Run Direct restore on AhsayCBS for this user. Refer to the Run Direct section for details.

AhsayACB User Account

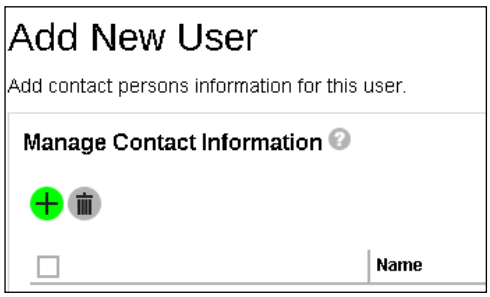


AhsayOBM User Account

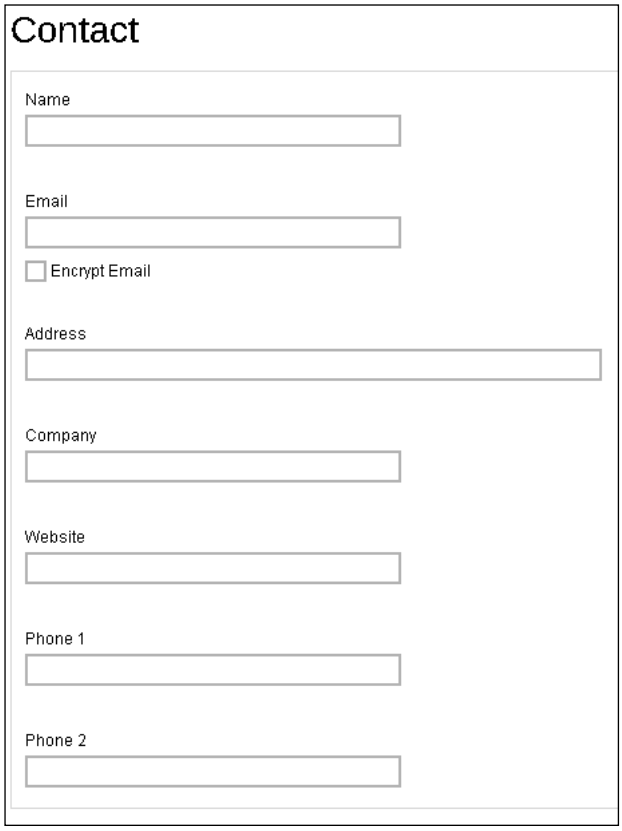


Click at the bottom of the page to proceed when you are done with the settings.

6. This page allows you to add contact person information for this user. Click to add new contact information.



7. Enter the contact information such as **Name**, **Email**, **Address**, etc. In our example, the name of the contact is **john**.



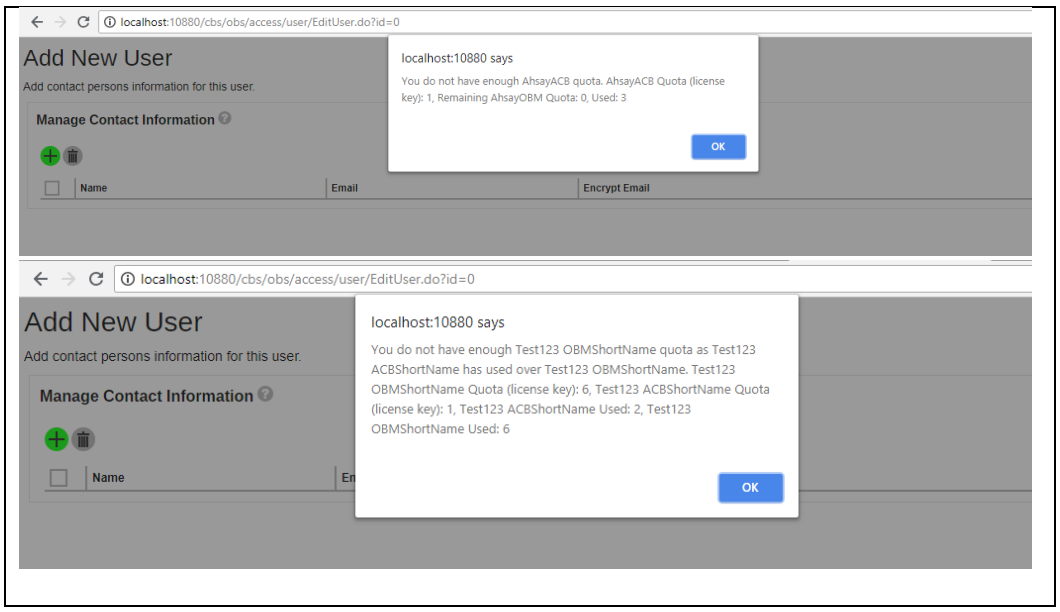
Click at the bottom right hand corner of the page to proceed when you are done with the settings.

8. A new contact called **john** is added.

9. Click at the bottom right corner of the page to confirm. The newly added user appears on the **Backup User** tab.

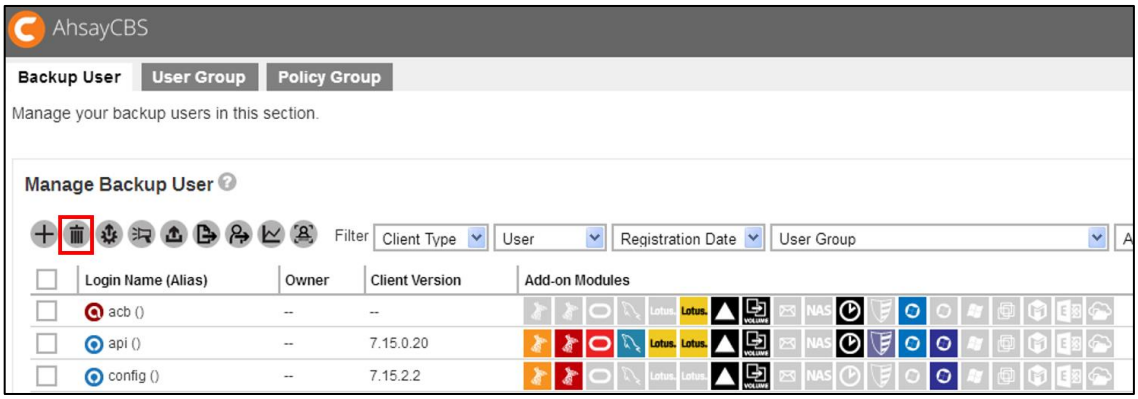
NOTE

Please kindly note that since AhsayCBS v7.17.0.0, if the license quota for backup user(AhsyaOBM/ AhsayACB) has already been fully used, adding another new backup user will be blocked.



Delete Backup User

To delete an existing user, select the user you want to delete, then click the **Delete** button as shown below. You will be prompted to confirm deleting the selected user, click **OK** to confirm.



WARNING

When you remove a backup user account, all the backup sets and backup data on CBS or predefined destinations, as well as the backup user profile on the AhsayCBS will be removed.

For the backup data residing on local destinations on the AhsayOBM/AhsayACB machine or on customers personal cloud storage accounts, SFTP/FTP servers will not be deleted.

Auto Update

The automatic upgrading of AhsayOBM/ AhsayACB clients to the latest version is performed using the Auto Update function. To perform a successful auto upgrade of the AhsayOBM/ AhsayACB clients need to connect to the AhsayCBS backup server.

The AhsayOBM/ AhsayACB client backup machine:

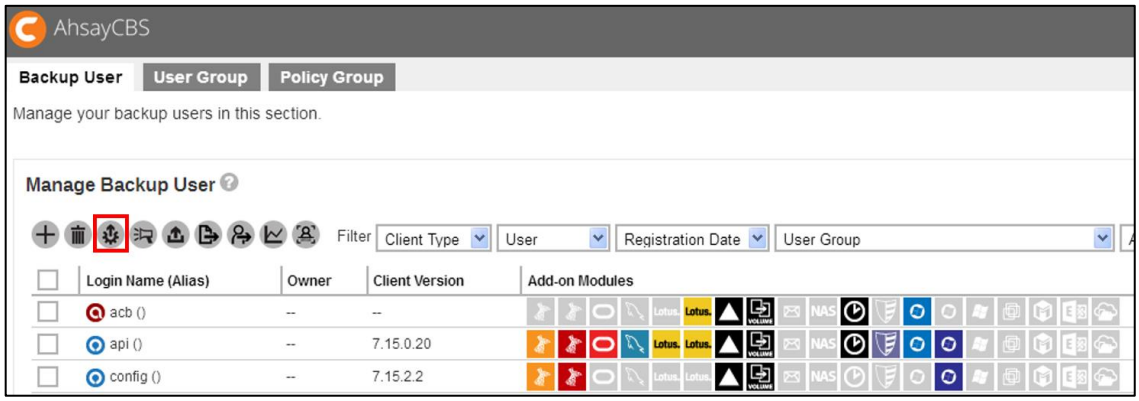
- Must be powered on.
- Must be connected to the internet.
- The AhsayOBM/ AhsayACB scheduler services must be running.
- The AhsayOBM/ AhsayACB client is connecting to AhsayCBS server using the latest login credentials.
- The AhsayOBM/ AhsayACB application GUI must be closed.

For every 720 minutes or whenever the backup client service restarts (v7) or the auto update agent service restarts (v6), AhsayOBM/ AhsayACB will check with your AhsayCBS for any available updates. If any auto update instructions were found on the AhsayCBS, the update progress will be started.

NOTE

AhsayOBM on Synology NAS does not support Auto Update feature.

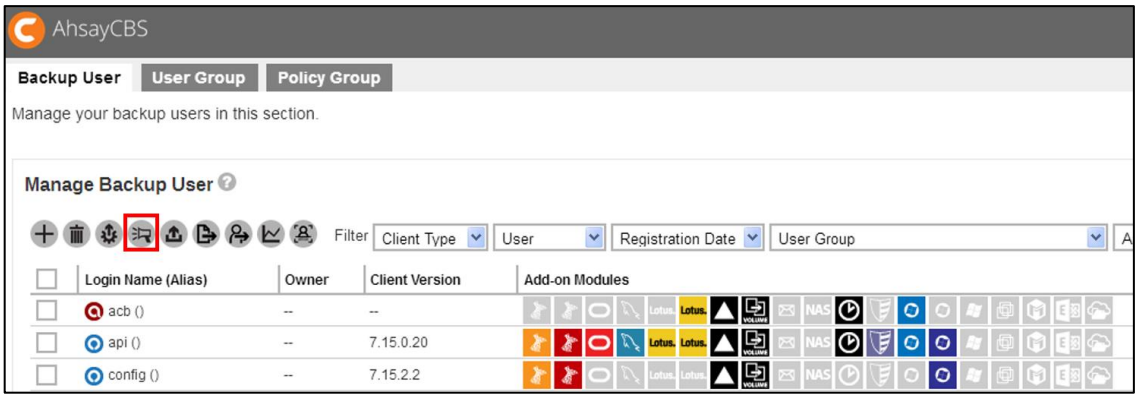
To perform an auto update, select the desired user then click **Auto Update** as shown below.



Broadcast

After you selected a list of users for broadcast, you will be able to send broadcast message to the selected users. This is useful when you need to send announcement such as server maintenance, applied latest patch or some promotion offers to your users.

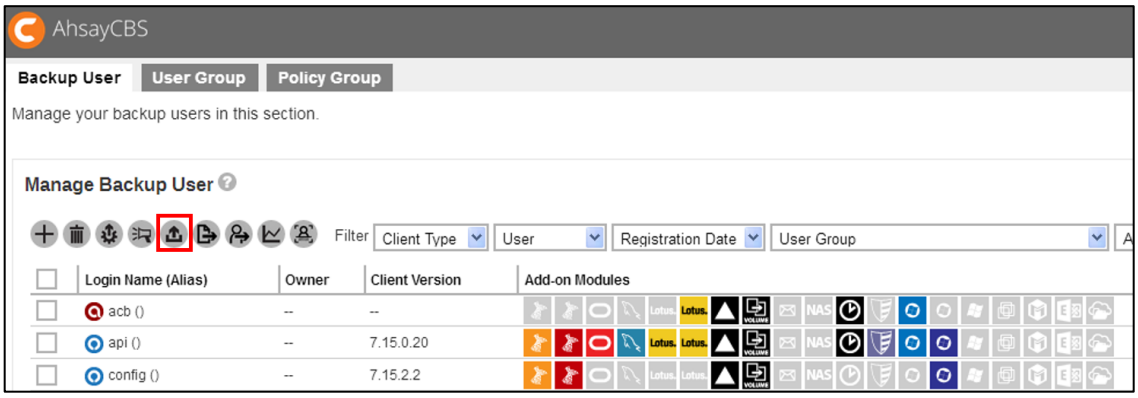
To broadcast a message to users, select the desired users then click the **Broadcast** button as shown below. Edit the broadcast message then click the **Send** button at the bottom right corner to send the message.



Backup User

You can select user(s) and trigger their backup machines to run the backup set(s). Select the desired backup user then click the **Backup User** button as shown below. Select the backup set you would like to start a backup on, and then click the **Run Backup** button at the bottom right corner to trigger a backup.

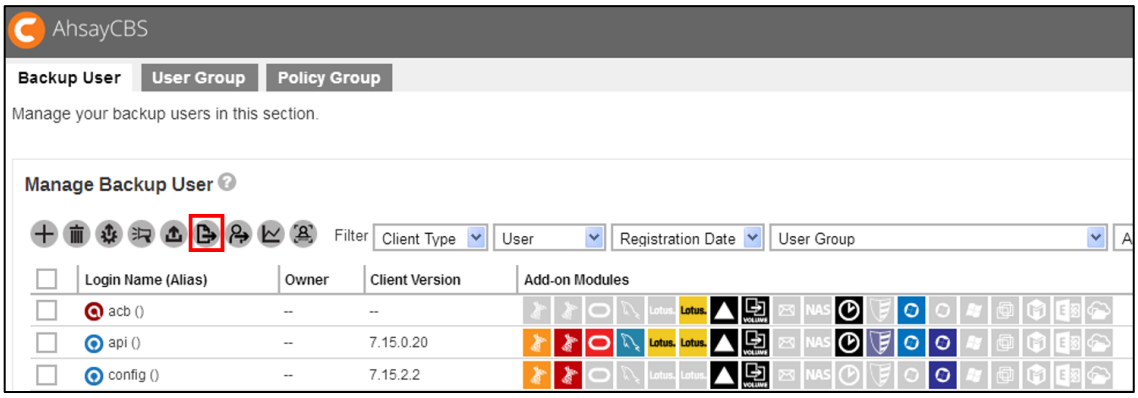
The backup will start shortly and you can monitor the progress using the **Live Activities** feature. Refer to Backup Status for further details.



Export Users' Usage Statistics to CSV File

You can export the usage of your selected user(s) to a CSV (Comma Separated Value) file. This format can be imported into spreadsheets or other program/database for further analysis or billing purpose.

To export usage of users to CSV, select the desired user then click the **Export Users' Usage Statistics to CSV** button as shown below. You will see a .csv file being downloaded.

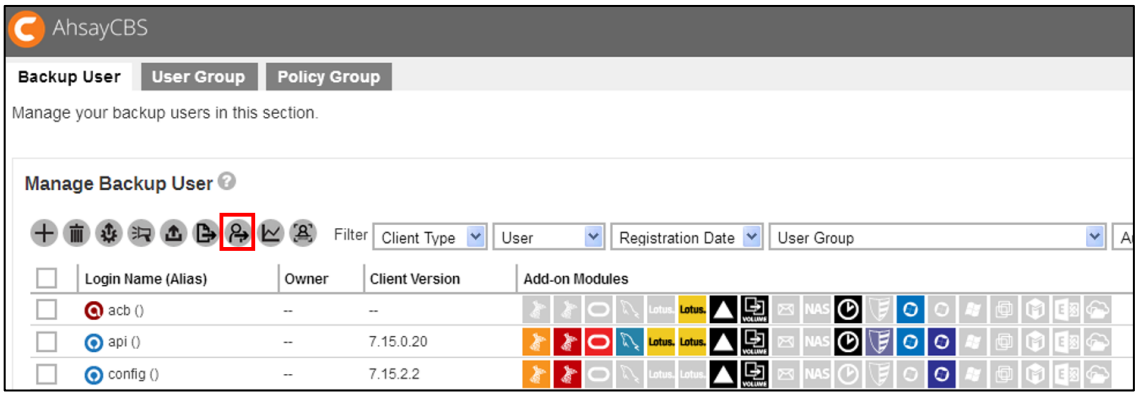


Move/ Import/ Export Users

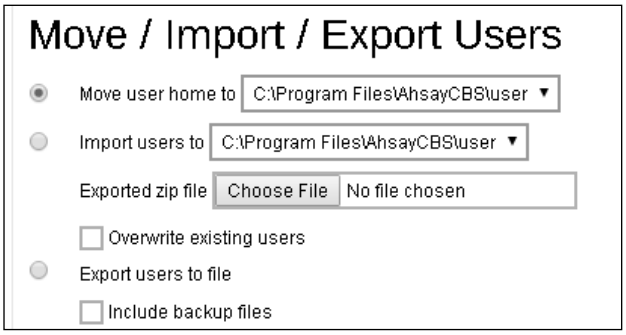
This function can be used to export users to a zip file, and import users from a zip file.

You can also use this function to migrate backup users from one AhsayCBS server to another AhsayCBS server, or to migrate users from their current user home to another user home on the same server. This function is limited to system user with admin role.

Select the desired user, and then click the **Move/ Import/ Export Users** button as shown below.



The following screen appears:



- **Move user home to** – Export user from a user home to another user home on the same AhsayCBS server .
- **Import users to** – Import a previously exported user to the selected user home.
- **Export users to file** – Export user profile and backup files to a zip file format.

NOTE

- Please schedule a time with the backup user before migrating a user to another user home / to another AhsayCBS. Ensure that the AhsayOBM / ACB client interface is closed, and that no backup / restore job is performed during the migration.
- It is highly recommended to temporarily suspend the backup user during the export / import procedure.
- It is not supported to import users belong to the AhsayCBS v7.15.6.0 or above to the old version of AhsayCBS server.

Since the migration of a backup user to another user home / AhsayCBS may involve export of the user profile and backup data, for user with a large amount of backup data, the time required for the export may take a while. During the export, please do not restart the AhsayCBS service or the server. In case of power failure or server shutdown, the export of the user will fail.

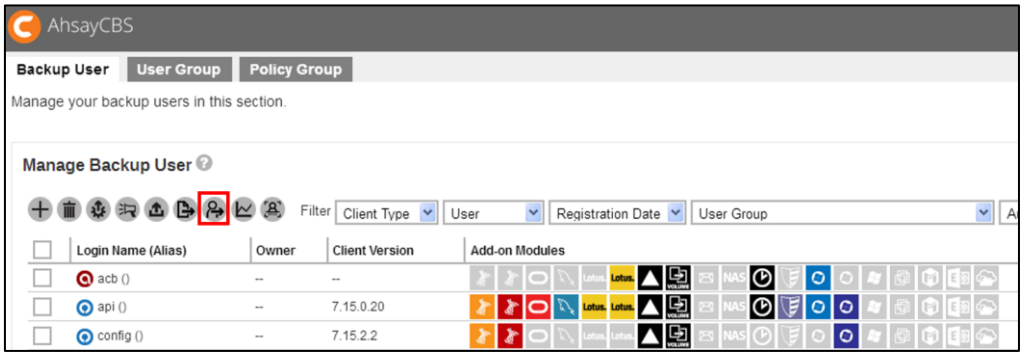
Example: Case 1 -- Migrate users from one user home in D: drive to another user home in F: drive within the same AhsayCBS

Assumptions:

- The backup users to be moved only have small amount of backup files.
- These users are located in **D:\u001** to be moved to **F:\u001**.

Steps:

1. Login to the AhsayCBS and go to **Backup/Restore > Users, Groups & Policies**.
2. Select the user(s) to be migrated.



3. Click the **Move/ Import/ Export Users** button.

4. Make sure the radio button of **Move user home to** is turned on and select the dropdown box next to it. Choose the **F:\u001.**

5. Click ✔ to proceed.

Example: Case 2 -- Export a user (including data) from one AhsayCBS and import to another AhsayCBS

Suggestions:

- Perform the export and import procedure for one user at a time.
- Suspend the user during the export and import procedures to ensure that no backup / restore job is performed during the migration.
- If the exported “users.zip” file is not saved to a local destination, ensure that the network between the AhsayCBS server and the save destination remain stable throughout the export process.
- For best result (performance and stability wise), it is recommended that:
  - The export and import operation of the backup user is performed directly on the corresponding AhsayCBS server, or in the same LAN environment.
  - The exported “users.zip” files are copied directly onto the destination AhsayCBS server, or a network drive in the same LAN environment.
- For backup user with large amount of data, please
  - Perform the user data export at a time when the resource usage is low on the AhsayCBS server.

Assumptions:

- The user to be exported is located on AhsayCBS1, to be moved to AhsayCBS2.
- Before importing the user to AhsayCBS2, make sure that there is no backup user with the same username on AhsayCBS2.

- Backup data are stored on the AhsayCBS server. Data on cloud storage or pre-defined destination is not supported.
- The user should be removed on the original server (e.g. AhsayCBS1) after exporting the user to the new AhsayCBS server. This is especially important if these AhsayCBS servers are under the same Redirector setup.

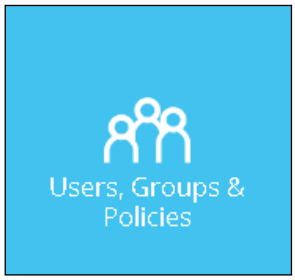
NOTE

Please kindly note that the default size limit for the users.zip file (including Users.xml and backup data) to be imported to the different AhsayCBS server is 50G. If you want to change the size limit, you need to change the number of "50" in the line of "<controller maxFileSize="50G"/>" in "$CBS_HOME/webapps/cbs/WEB-INF/struts-config.xml" to be other value.

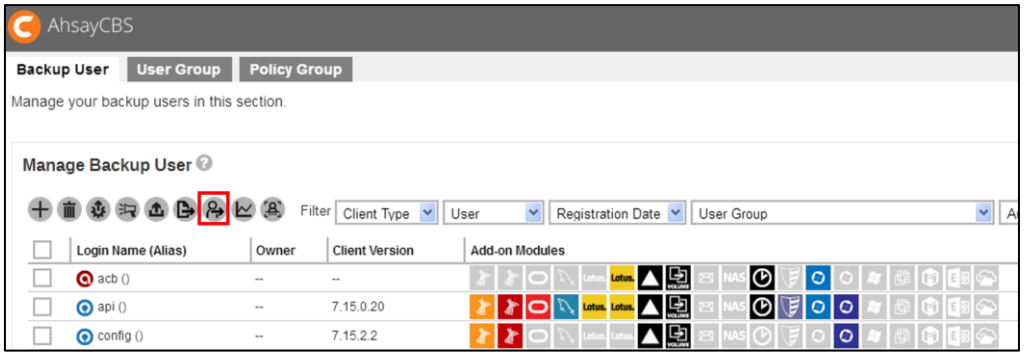
Please refer to the following article for further details about how migration of users between different AhsayCBS under the same Rediector setup:
http://wiki.ahsay.com/doku.php?id=public:5303_how_to_move_user_in_same_ahsayrdr_setup

Steps:

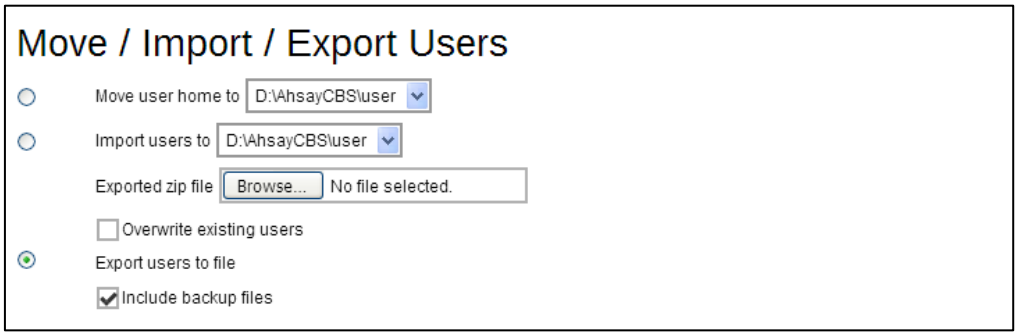
1. Login to the AhsayCBS1 and go to **Backup/Restore > Users, Groups & Policies**.



2. Select the user you need to export and click the **Move/ Import/ Export Users** button.



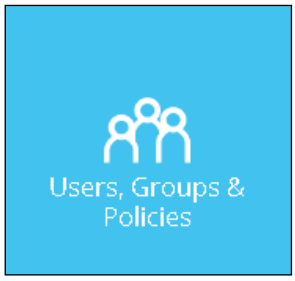
3. Click on the **Export users to file** radio button and click on the **Include backup files** check box to export the backup user data.



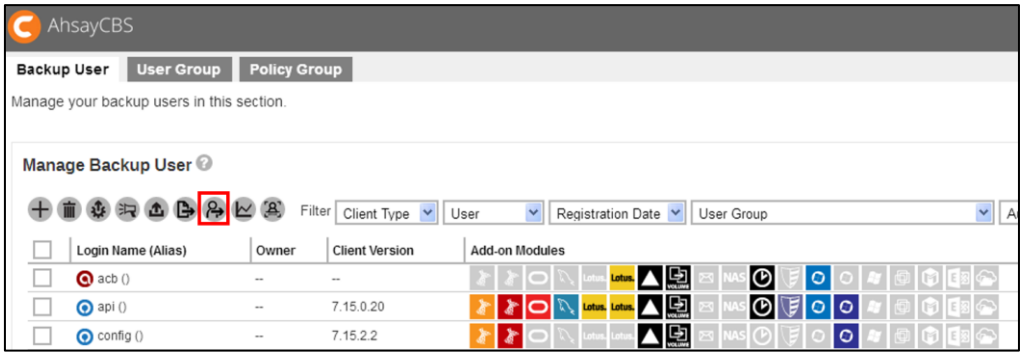
4. Click on to proceed. The system will prompt you to save the file (users.zip) in your local machine. You need to have enough disk space to save the zip file. If the user account has large backup sets, it is expected to wait for a long time.

5. After exporting process, click to skip to the **Backup User Tab** page. Click afterward to save the change.

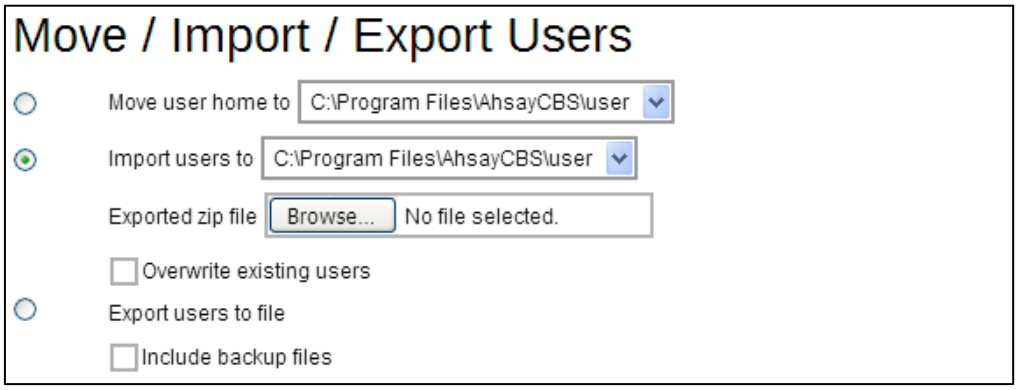
6. Login to the AhsayCBS2 and go to **Backup/Restore > Users, Groups & Policies**.



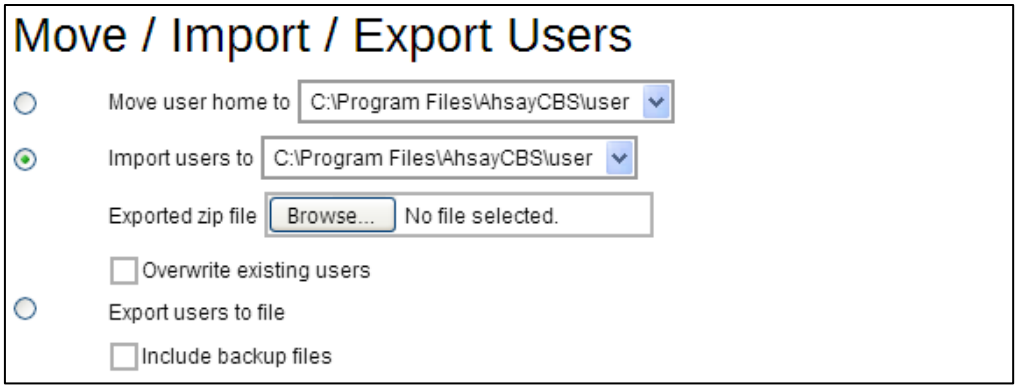
7. Click the **Move/ Import/ Export Users** button.



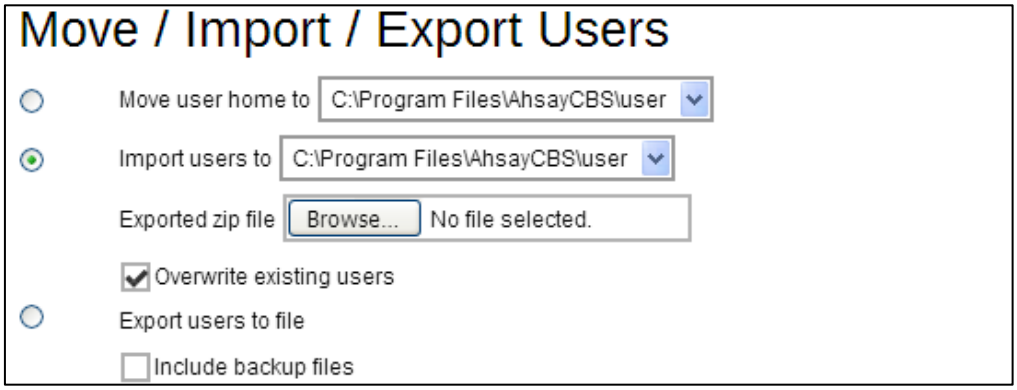
8. Click on the **Import users to** radio button and select the destination user home on the AhsayCBS2 from the drop down list.



9. Click on the **Browse** button under the **Import users to** radio button. Select your previous exported zip file.

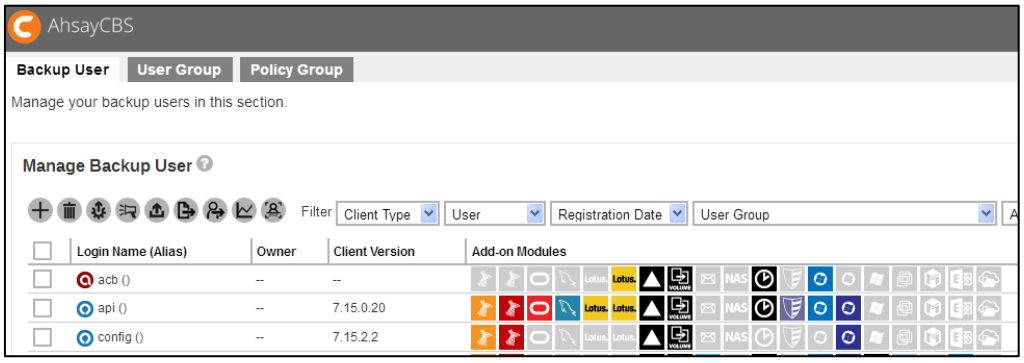


10. If the overwrite option is selected, the user account on the AhsayCBS2 which has the same user name in the users.zip will be overwritten.



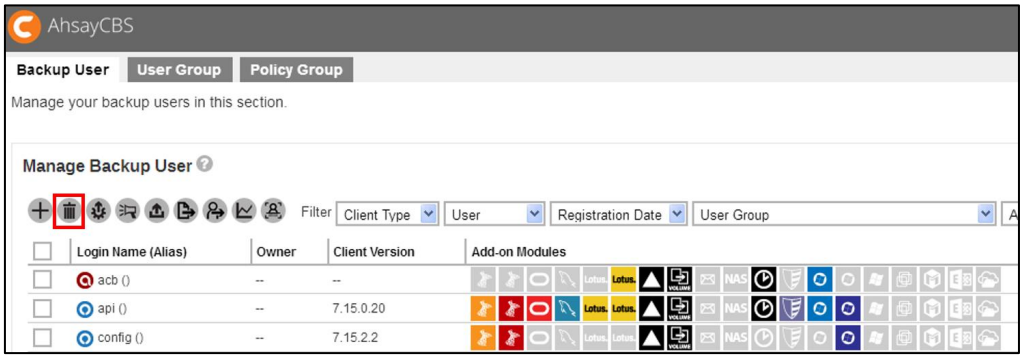
11. Click on to proceed.

12. Restart the AhsayCBS service and login to AhsayCBS2 to check the newly imported user in the **Backup User** page.



Please refer to the following article for further details about how migration of users between different AhsayCBS under the same Rediector setup: http://wiki.ahsay.com/doku.php?id=public:5303_how_to_move_user_in_same_ahsayrdr_setup

13. After the entire migration process is completed, delete the original backup account on AhsayCBS1. On the AhsayCBS web console of AhsayCBS1, under **Backup User** tab, select the migrated user account and click on the **Delete** button to delete it.



Rebuild Storage Statistics

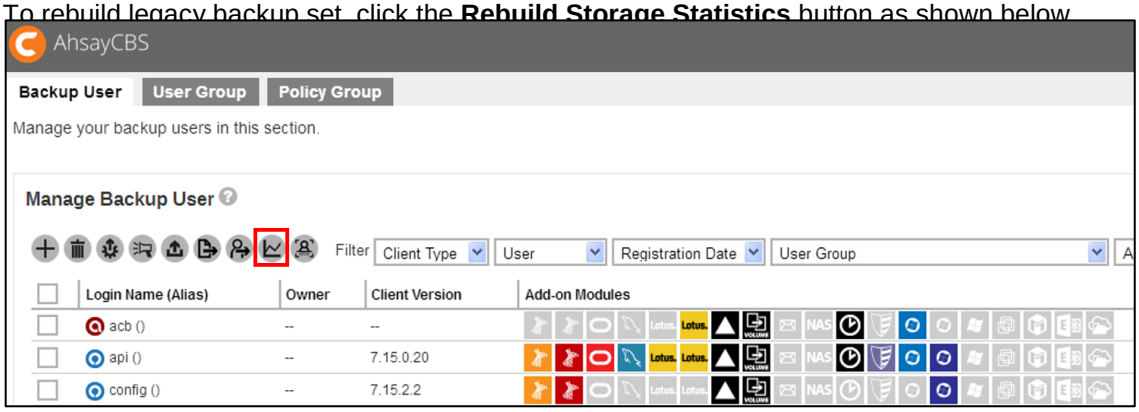
This option can only rebuild legacy backup sets created in version 6, which have not been migrated to v7 block storage format. The option is used to enhance the accuracy of storage statistics for the backup set created in version 6.

The time taken to complete a rebuild depends on a number of factors such as the number of files / folders in the backup set(s), the number of backup sets, the hardware specifications of your AhsayCBS server such as the disk I/O and CPU performance, and if there are other resource intensive jobs running.

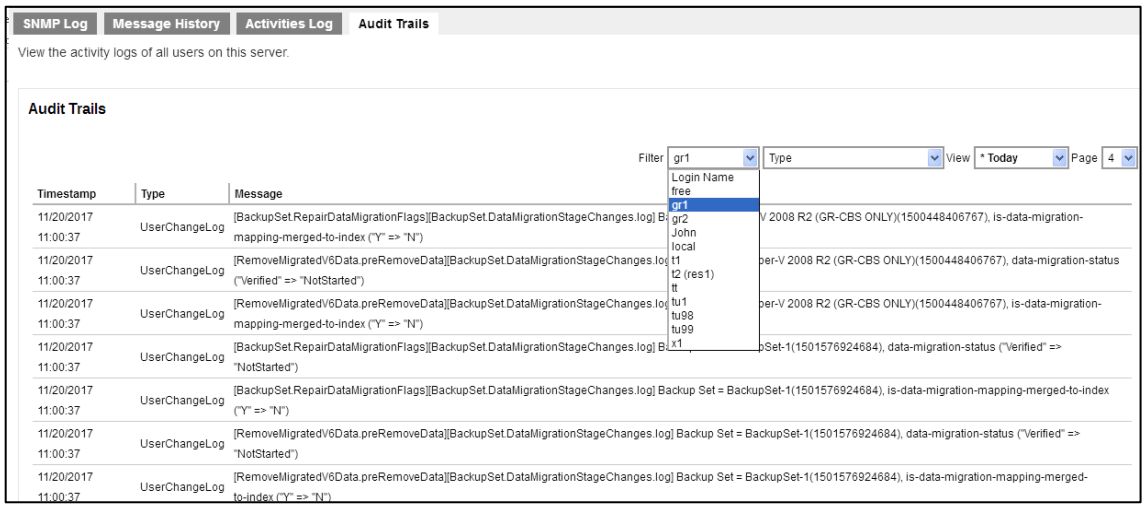
NOTE

Note that a backup set rebuild can only be started when there is no backup job running (of the corresponding backup set), and vice versa.

To rebuild legacy backup set, click the **Rebuild Storage Statistics** button as shown below.

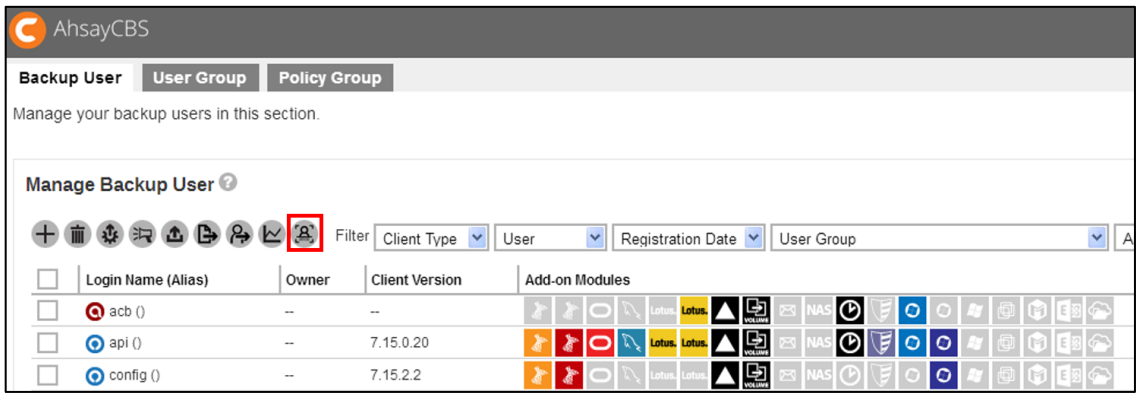


To check the progress or status of the Rebuild Storage Statistics job, go to [Monitoring]> [Administration Logs]>[Audit Trails], use the Filter "login Name" and select the backup user.



Rescan all user home directories

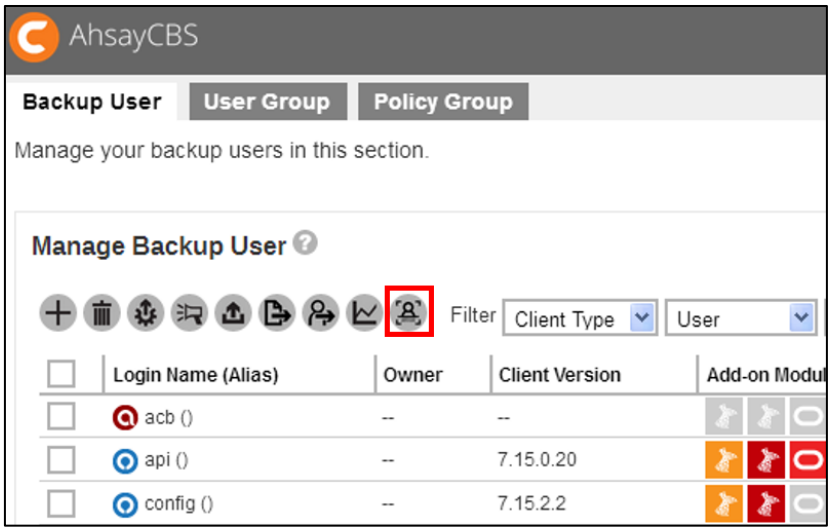
Since version 7.15.0.20, AhsayCBS added the feature of rescanning all user home directories. The feature ensures the status of all user home is updated so that the backup sets under available user home should be shown in the selecting list for Admin user account to exclude while the backup sets under unavailable user home should not be listed during backup data migration. And also if the user home is offline, the backup and restore job cannot be run properly, so the feature helps confirm applying backup and restore job.



The feature will be applied in the following 3 conditions:

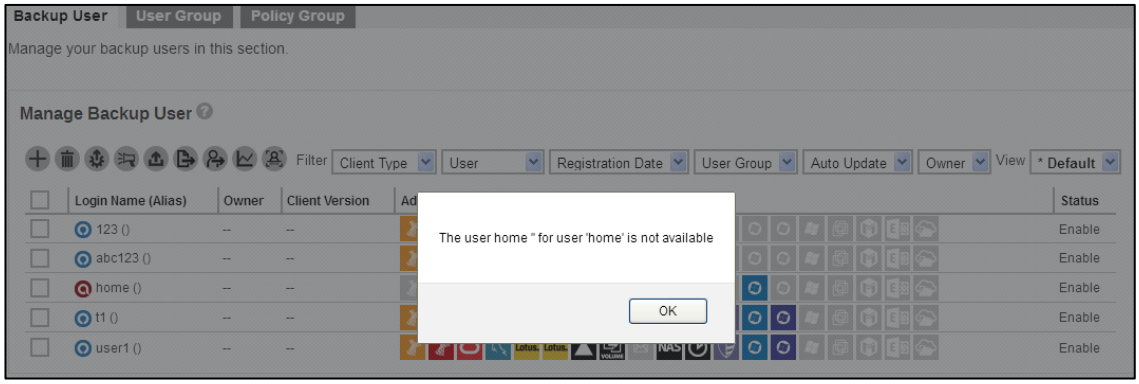
1. Startup AhsayCBS service.

2. Click on the **Rescan all user home directories** button, as shown in screen shot.

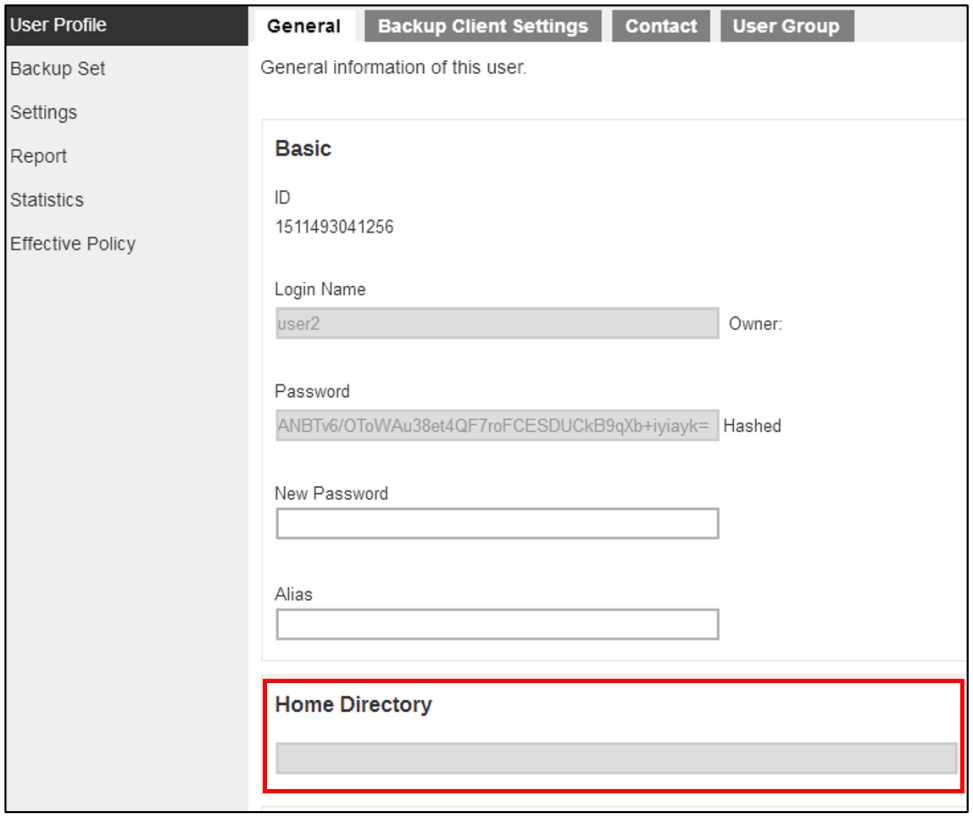


3. Run routine job (HourlyJob)

If there is user home offline, which may be caused by disk temporary unavailable, user home directory rename, network drive disconnected or disk corrupted, a message will pop up as shown in the following screen shot.



After clicking into the according user account, **Home Directory** will be blank.



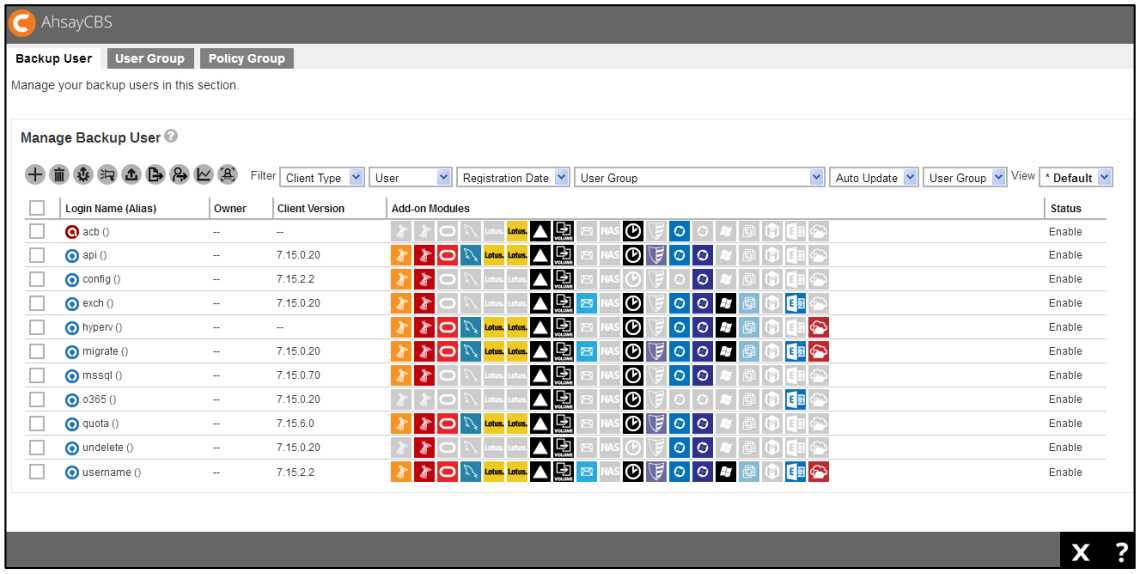
Managing Backup Users

After you have created a backup user in previous section, you can perform the following operation for your users such as:

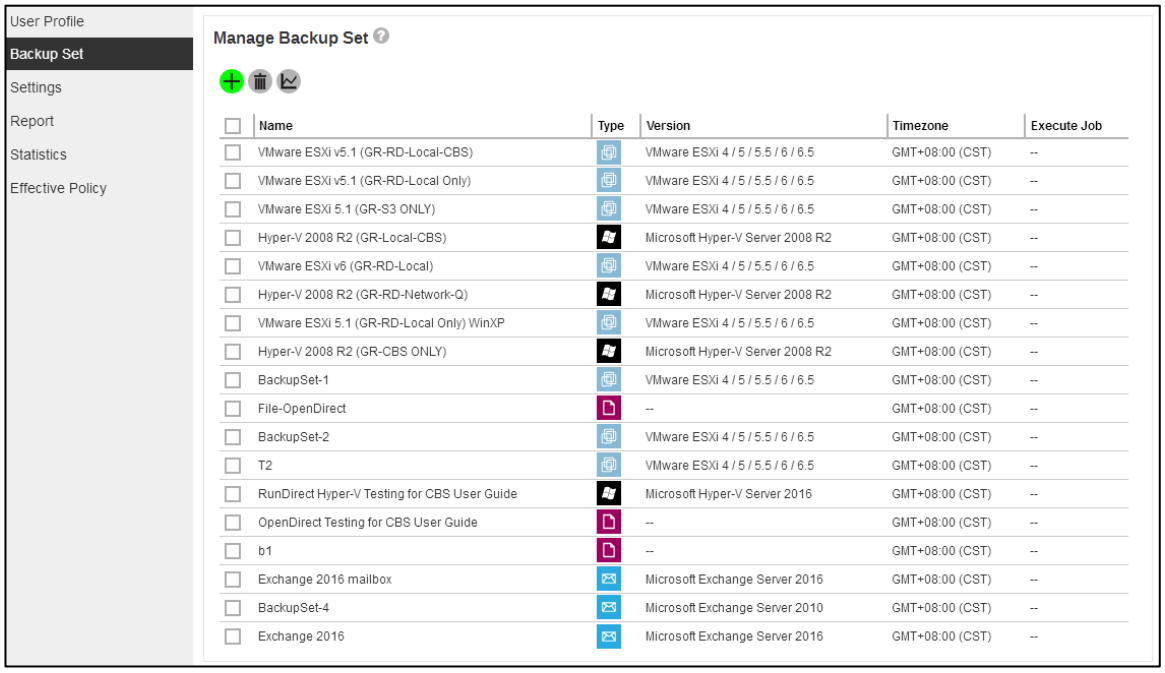
- Customize backup users profile settings
- Customize subscribed modules
- Create backup sets
- View backup/restore reports
- View usage statistics
- Manage the policies applied to a user
- Update client software via the auto update agent
- Send broadcast message to users
- Export usage to a CSV file
- Export users
- Rebuild storage statistic

Accessing the Backup User

Click the login name of the backup user account you want to manage from the **Backup User** tab.



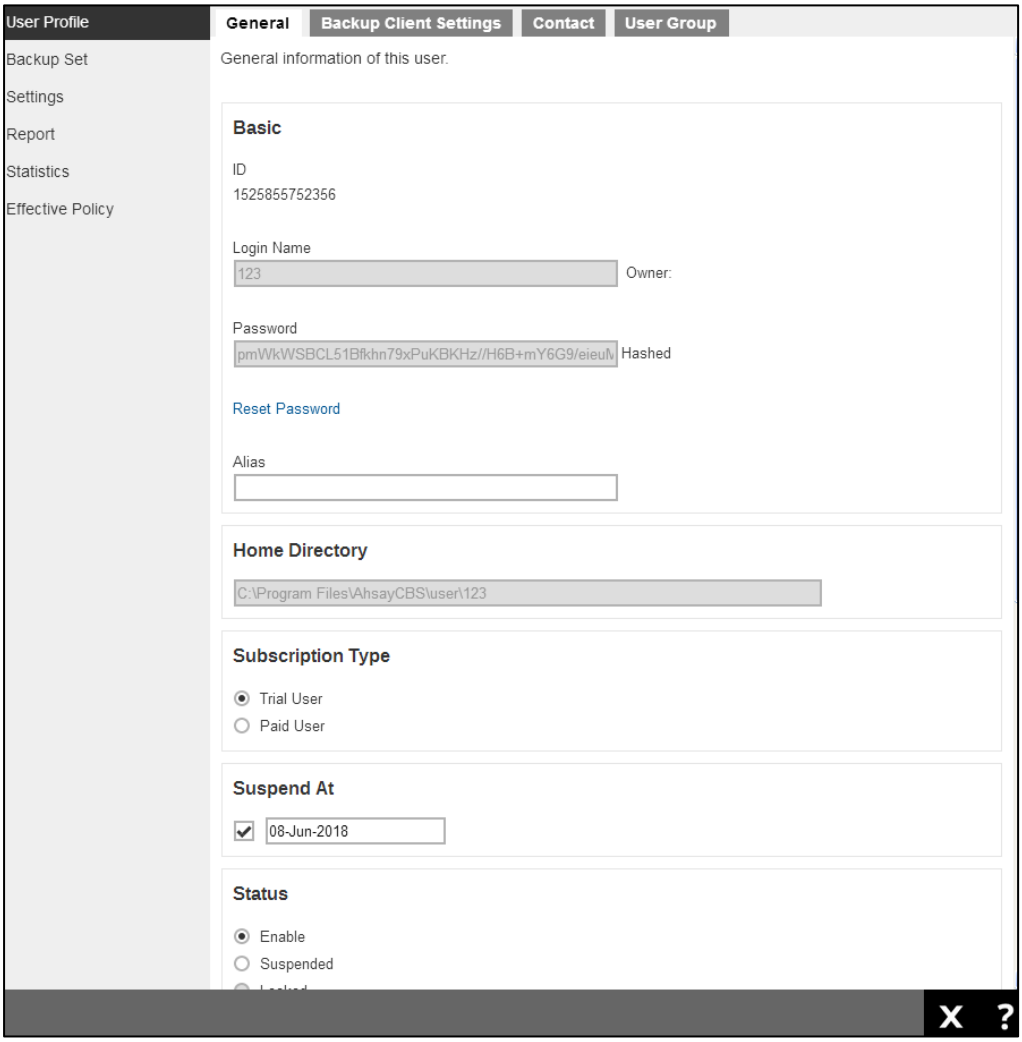
The backup user account opens. You will see 6 tabs (**User Profile**, **Backup Set**, **Settings**, **Report**, **Statistics**, **Effective Policy**), each of which is described in detail below.



User Profile

The User Profile tab contains user backup account settings information, subscribed modules, backup quota, subscription type, contact information and user group information. It is located under **Users, Groups & Policies > Backup User**. It is sub divided into four tabs, as described below.

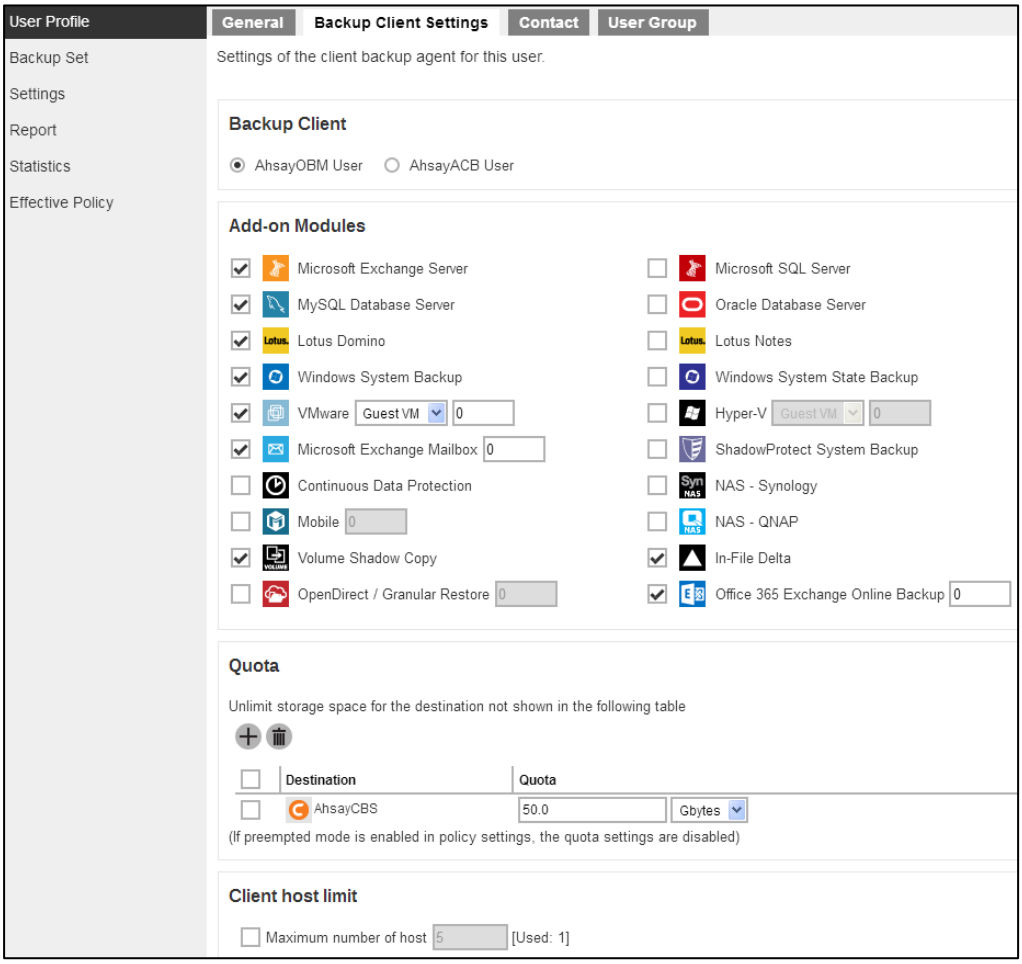
➢ General Tab



- **Reset Password** – Click to change or reset the password for this user, in case if they forgot the current password.
- **Alias** – Update the alias for this user.
- **Subscription Type** – Change the type from Trial User to a Paid User, for example after a user subscribes to backup service after a trial.
- **Suspend At** – Scheduled date to suspend this user's account.
- **Status** – Suspend or enable locked accounts
- **Upload Encryption Key** – Enable or disable the "Upload Encryption Key" feature.
- **Language** - Preferred language for all email reports of the backup user.

- **Timezone** – Update the time zone of the backup user.
- **Notes** – Add or update notes about this user.

➢ Backup Client Settings Tab



- **Backup Client** - Type of backup user account, AhsayOBM or AhsayACB. In case you need to change the backup client type, it is better to check if there are existing backup sets in the backup account. For example, if you have an AhsayOBM user account with Exchange backup set and you change the account type to AhsayACB, the Exchange backup set will not be run due to the backup client type does not match.
- **Add-on Modules** – Below is a short summary of the add-on modules available for both AhsayOBM and AhsayACB

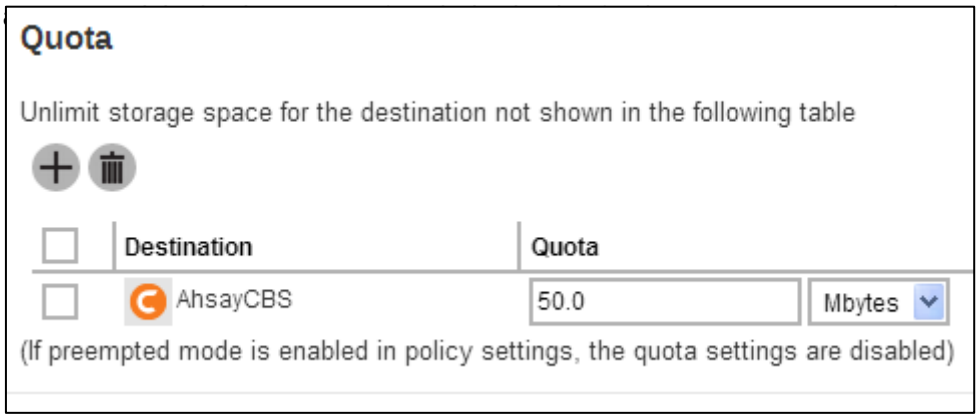
Add-on Module	Reference	AhsayOBM	AhsayACB
Microsoft Exchange Server	Backup and restore of Microsoft Exchange Server. Refer to the following link for how to use Microsoft Exchange Database Server with AhsayOBM client:	✔	✘

	Ahsay Online Backup Manager v7 Microsoft Exchange Database Backup and Restore Guide		
Microsoft SQL Server	Backup and restore of Microsoft SQL Server. Refer to the following link for how to use Microsoft SQL Server with AhsayOBM client: Ahsay Online Backup Manager v7 Microsoft SQL Server Backup and Restore Guide	✔	✘
MySQL Database Server	Backup and restore of MySQL Database Server. Refer to the following link for how to use MySQL Database for the Windows platform with AhsayOBM client: Ahsay Online Backup Manager v7 MySQL Database Backup and Restore for Windows Refer to the following link for how to use MySQL Database for the Linux platform with AhsayOBM client: Ahsay Online Backup Manager v7 MySQL Database Backup and Restore for Linux (CLI)	✔	✘
Oracle Database Server	Backup and restore of Oracle Database Server on Windows and Linux platforms.	✔	✘
Lotus Domino	Backup and restore of Lotus Domino.	✔	✘
Lotus Notes	Backup and restore of Lotus Notes.	✔	✔
Windows System Backup	Backup and restore of Windows System Backup. Refer to the following link for how to use Windows System Backup with AhsayOBM and AhsayACB clients: Ahsay Online Backup Manager v7 Microsoft System Backup and Restore Guide	✔	✔
Windows System State Backup	Backup and restore of Windows System State Backup. Refer to the following link for how to use Windows System State Backup with AhsayOBM client: Ahsay Online Backup Manager v7 Microsoft System State Backup and Restore Guide	✔	✘
VMware	Backup and restore of VMware guest VMs.	✔	✘

	Refer to the following link for how to use VMware VCenter/ESXi with AhsayOBM client: Ahsay Online Backup Manager v7VMware vCenter/ESXi Backup and Restore Guide		
Hyper-V	Backup and restore of Hyper-V guest VMs. Refer to the following link for how to use Microsoft Hyper-V with AhsayOBM client: Ahsay Online Backup Manager v7 Microsoft Hyper-V Backup and Restore Guide	✔	✘
Microsoft Exchange Mailbox	Backup and restore of Microsoft Exchange Mailboxes. Refer to the following links for how to use Microsoft Exchange Mailbox with AhsayOBM client: Ahsay Online Backup Manager v7 Microsoft Exchange 2007/2010/2013 Mail Level Backup and Restore Guide Ahsay Online Backup Manager v7 Microsoft Exchange 2016 Mail Level Backup and Restore Guide	✔	✘
NAS - Synology	Backup and restore of file on Synology NAS devices. Refer to the following link for how to use the Synology NAS with AhsayOBM client: Ahsay Online Backup Manager v7 Quick Start Guide for Synology NAS Refer to the following link for a list of Synology hardware compatible with AhsayOBM: FAQ: Ahsay Hardware Compatibility List (HRL) for AhsayOBM on Synology NAS (5058)	✔	✘
NAS - QNAP	Backup and restore of file on QNAP NAS devices. Refer to the following link for how to use the QNAP NAS with AhsayOBM client: Ahsay Online Backup Manager v7 Quick Start Guide for QNAP NAS Refer to the following article for the list of QNAP NAS models and supported list: FAQ: Ahsay Hardware Compatibility List (HRL) for AhsayOBM on QNAP NAS	✔	✘

Shadow Protect System Backup	Backup and restore of Shadow Protect System image (requires Shadow Protect)	✔	✘
Volume Shadow Copy	Volume Shadow Copy to support open file backups on Windows platform.	✔	✔
Continuous Data Protection	A backup will be made whenever this is a change (between 1 min to 12 hour intervals) for Windows platform only.	✔	✔
In-File Delta	When enabled only the changes since the last backup job is backed up.	✔	✔
Mobile	Backup and restore of Mobile (iOS and Android) Refer to the following links for instructions on using the AhsayMOB for Android and iOS platforms. - AhsayMOB v7 User Guide – Android - AhsayMOB v7 User Guide - iOS	✔	✔
Office 365 Exchange Online	Backup and restore of Office 365 Exchange mailboxes. Refer to the following link for instructions on using the Office 365 Exchange Online with AhsayOBM. - AhsayOBM v7 User Guide - Office365 Exchange Online Backup & Restore for Windows - AhsayOBM v7 User Guide - Office365 Exchange Online Backup & Restore for Mac	✔	✔
OpenDirect / Granular Restore	For OpenDirect and Granular Restore. Refer to the following link for instructions on using OpenDirect / Granular Restore. - Ahsay Online Backup Manager v7 Quick Start Guide for Windows - Ahsay A-Click Backup v7 Quick Start Guide for Windows - Ahsay Online Backup Manager v7 Microsoft Hyper-V Backup and Restore Guide - Ahsay Online Backup Manager v7 VMware vCenter/ESXi Backup and Restore Guide	✔	✘

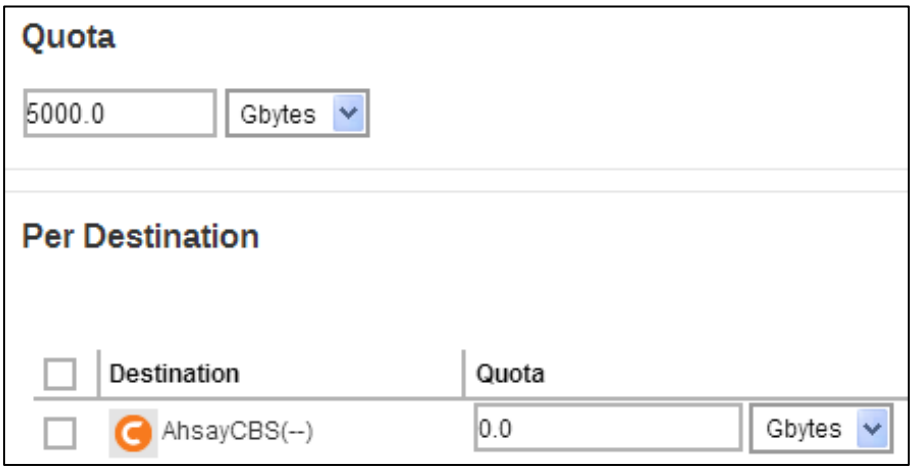
- **Quota** – list all the predefined destinations and AhsayCBS associated with the user



NOTE

Please kindly note that the local destination will not be included.

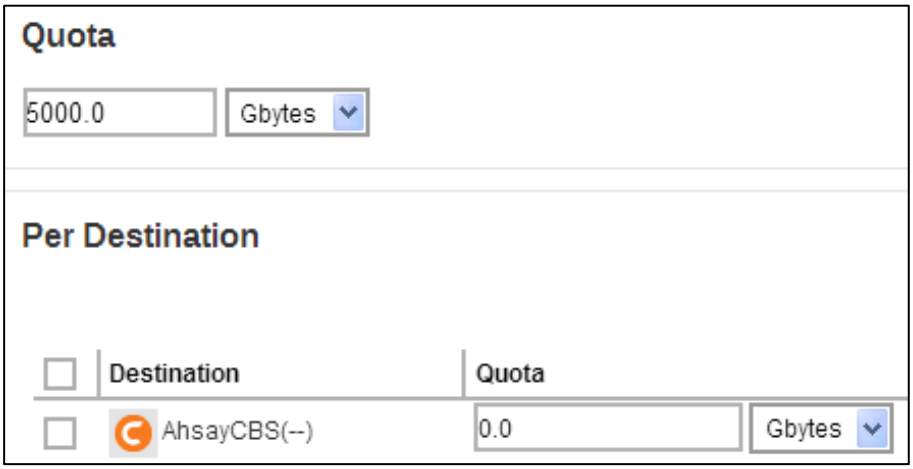
- Quota management for individual predefined destination is only available for AhsayCBS version 7.15.6.0 or above. For previous version before version 7.15.6.0, only a total quota storage can be set and you cannot configure individual quota for predefined destination, which is shown as following.



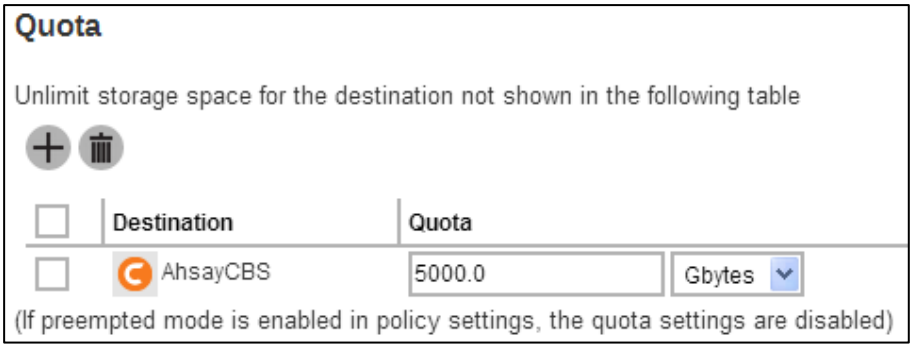
If your AhsayCBS was upgraded from a previous version to 7.15.6.0 or above, for users with pre-existing predefined destinations and AhsayCBS, the quota settings for each predefined destination and AhsayCBS will be set according to different situation.

For example

Situation-1: the previous total quota setting is 5000Gbytes, and the quota storage setting for AhsayCBS was default setting.

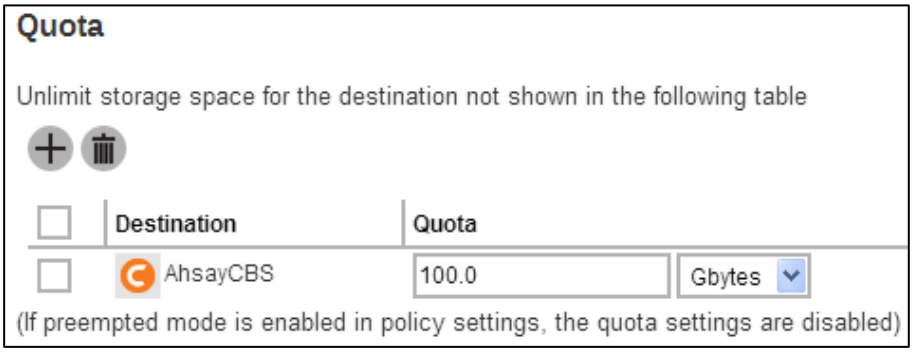


After the upgrade, the new quota setting for AhsayCBS will be 5000Gbytes.



Situation-2: the previous total quota setting is 5000Gbytes, and the quota storage setting for AhsayCBS was 100Gbytes.

After the upgrade, the quota setting for AhsayCBS will maintain to be 100Gbytes.

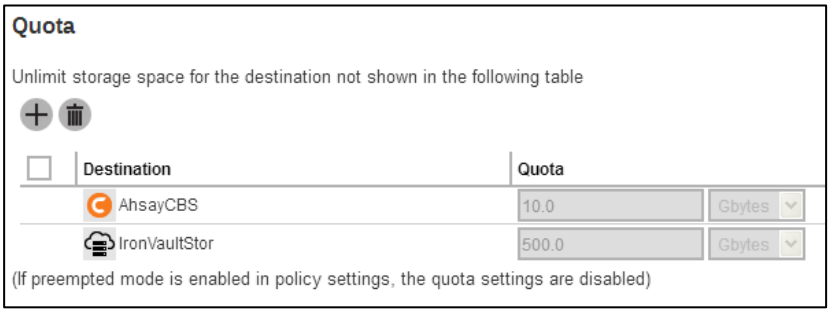


- For the destination not shown in the Quota table, the storage space is unlimited. If you want to limit storage space to according destination, please ensure to add the destination here and assign the quota appropriately.

NOTE

Please kindly note that only the destinations already defined by the backup sets can be shown and added to be the backup destination for the backup user.

- If preempted mode is enabled in Backup/ Restore > Users, Groups & Policies > Policy Group > %policygroup% > User Settings > User Quota, the quota settings here will be disabled and cannot be modified.

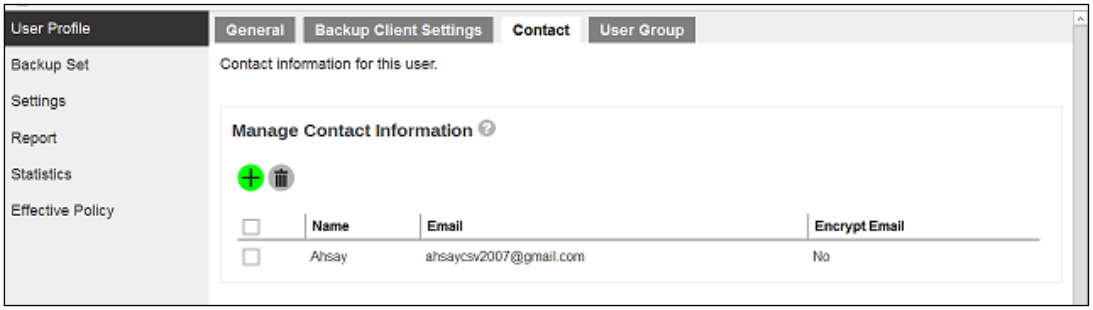


NOTE

The backup quota of a VMware VDDK backup set should be set to a value that is higher than the provision size. Even if the backup only upload the actual usage, if the quota is smaller than the provision size, the backup would fail with quota exceed.

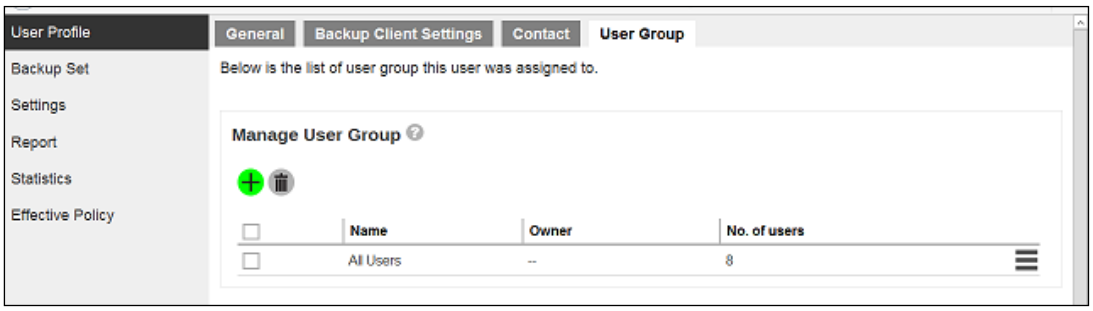
- **Client Host Limit** - Set the maximum number of host machine or devices the backup user can install AhsayOBM/AhsayACB on.
- **Run Direct** – Set the maximum number of VMs for VM Run Direct restore on AhsayCBS for this user.

- **Contact Tab**



You can configure the client contact here for them to receive backup or restore reports.

- **User Group Tab**

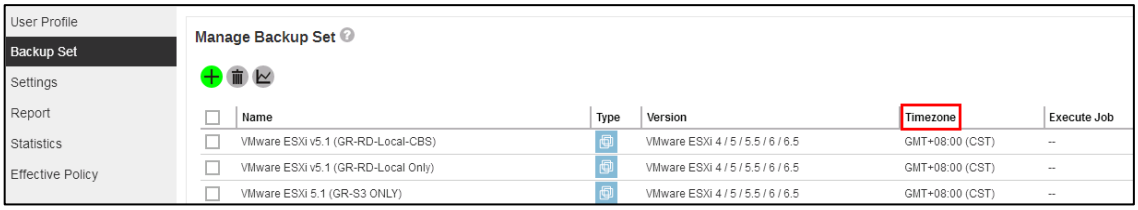


You can assign the user to an existing/assigned user group. When you drag the user group with the side button, it will affect the sequence of the policy rules that will apply to the user.

Backup Set

This function is used to create backup sets for this user account. In some cases, you may need to create backup sets first before you install a backup client on the client machine, or it may be an alternative option for administrator to create/modify a backup set for Linux users with no graphical interface, or there may be access restrictions for administrator to access the backup machine again after the backup client installed.

The following shows the Backup Set tab under **Users, Groups & Policies** > **Backup User**.

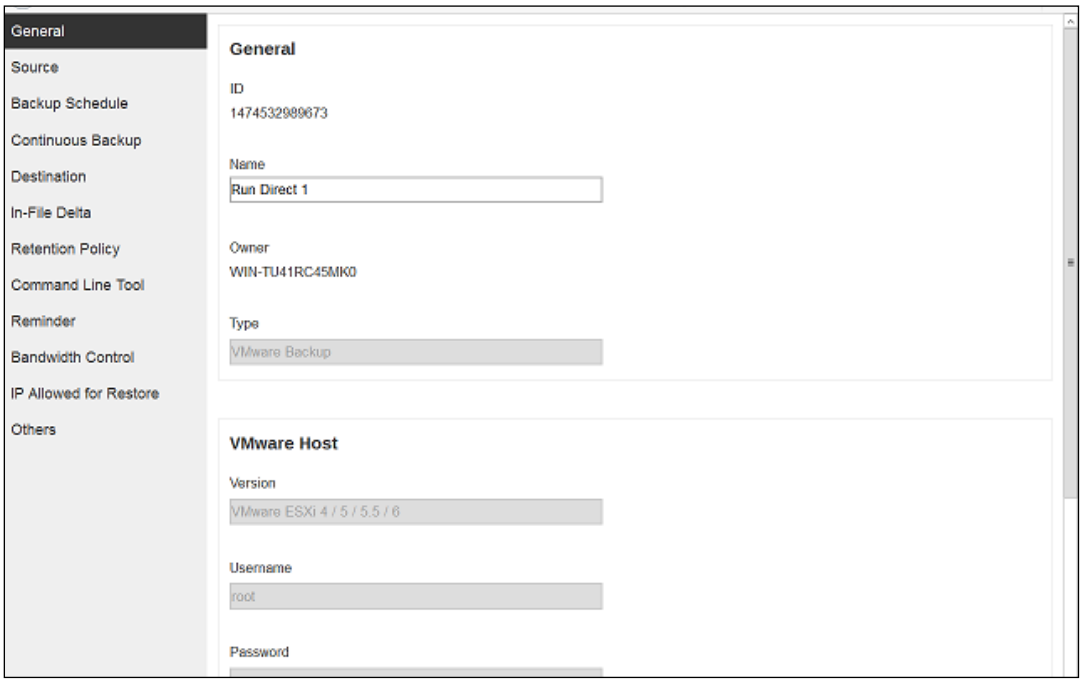


Timezone feature is introduced for the backup set since AhsayCBS v7.15.0.8. Timezone information will be automatically updated when user login client backup agent, such as AhsayOBM and AhsayACB, or perform backup job to avoid the false alarm of missed backup job.

Accessing the Backup Set

Click the backup set name of the user account you want to manage from the **Backup Set** tab. It is sub divided into the following tabs:

- General
- Continuous Backup
- Retention Policy
- Bandwidth Control
- Source
- Destination
- Command Line Tool
- IP Allowed for Restore
- Backup Schedule
- In-File Delta
- Reminder
- Others



Recovering Encryption Key via AhsayCBS Web Console

From AhsayCBS v7.9.2.0 onwards, it is possible to engage the **AhsayCBS v7 Encryption Key Recovery Service** via the AhsayCBS web console under the **Others** menu of this section. Click here for details on the scope of this professional service.

Required Permission

Only system user with **Admin** role has the right to access the Recover Encryption Key feature via AhsayCBS web console.

Required Settings

Encryption key is recoverable only if the following three settings are **ENABLED**:

- The **Upload Encryption Key** feature in the **Encryption Key** section under the **Users, Group & Policies > Policy Group > %Policy Group Name % > User Settings** menu which applies to the corresponding backup set.
- The **Encryption Recovery** feature under the **Profile > Encryption Recovery** menu in your AhsayOBM or AhsayACB.
- The **Upload Encryption Key** feature under the **Users, Group & Policies > Backup User > %User Name % > User Profile** of the backup user requesting for key recovery.

With these three features on, encryption keys will be uploaded to the backup server during the backup process, so as to make recovery possible.

Preparation before Getting Started

Make sure the following items are valid before getting started with the encryption key recovery process.

- Valid login credentials to log on to the Ahsay Shopping Centre.
- Valid maintenance. For inquiries about maintenance, please contact our Sales Team at partners-kb@ahsay.com.

Encryption Key Recovery for Branded AhsayCBS

Background

If your AhsayCBS is branded, the Recover Encryption Key feature is HIDDEN by default. This measure is enforced to prevent backup users from accessing the Ahsay Shopping Centre directly after clicking the Recover Encryption Key button under a branding environment.

What is a branded AhsayCBS

Your AhsayCBS is considered “branded” when the following criteria are met:

Under the **System Settings > Basic > Administrative Access > %system user% > Rebrand Web Console > User Interface** page in the web management console, if any one of the following parameters is not empty or not holding default image:

Title	Product Name	User Interface logo	Report logo
AhsayCBS logo	AhsayOBM logo	AhsayACB logo	

Force enable the Recover Encryption Key feature

The Recover Encryption Key button can be forced to show by enabling the debug option as shown below in the **cbs.opt** file under the **%CBS_INSTALL%\conf** folder. This debug option will make the Recover Encryption Key button visible to backup users even if the AhsayCBS is branded.

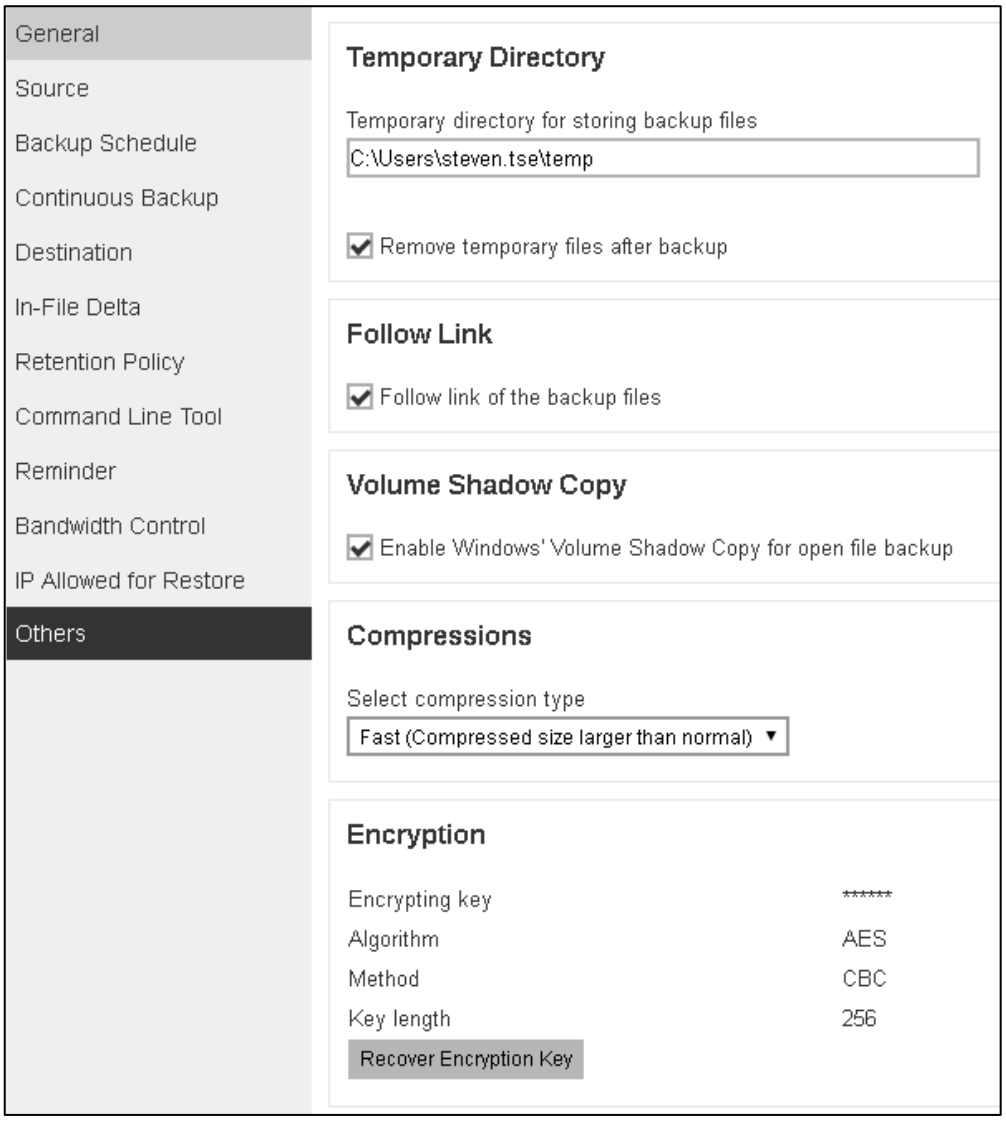
com.ahsay.cbs.system.config.accounts.editSysUserBean.ShowRecoveryEncryptionKeyBtn.debug=true

Recovery Steps

Follow the steps below to submit an encryption key recovery request.

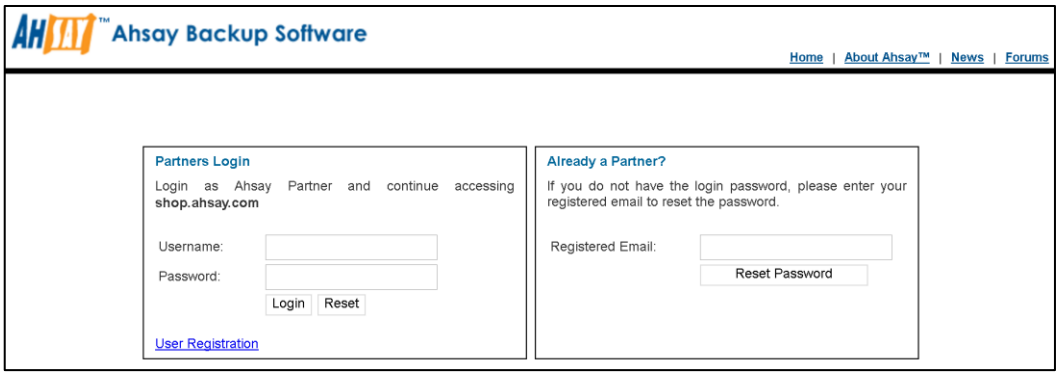
1. Click on the backup set, which you wish to recover the encryption key for, under the Manage Backup Set section.

2. Navigate to the **Others** tab.

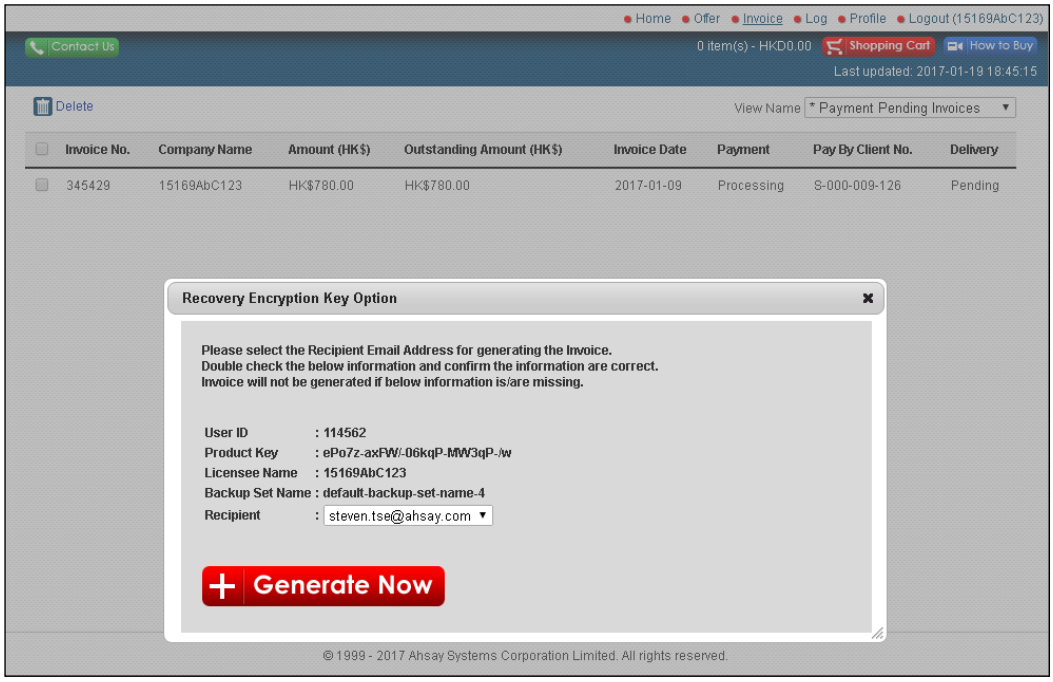


3. Look for the **Encryption** sub-section on this page and click on the **Recover Encryption Key** button.

4. You will be prompted to log in to the Ahsay Shopping Centre as shown below, if you have not done so yet.

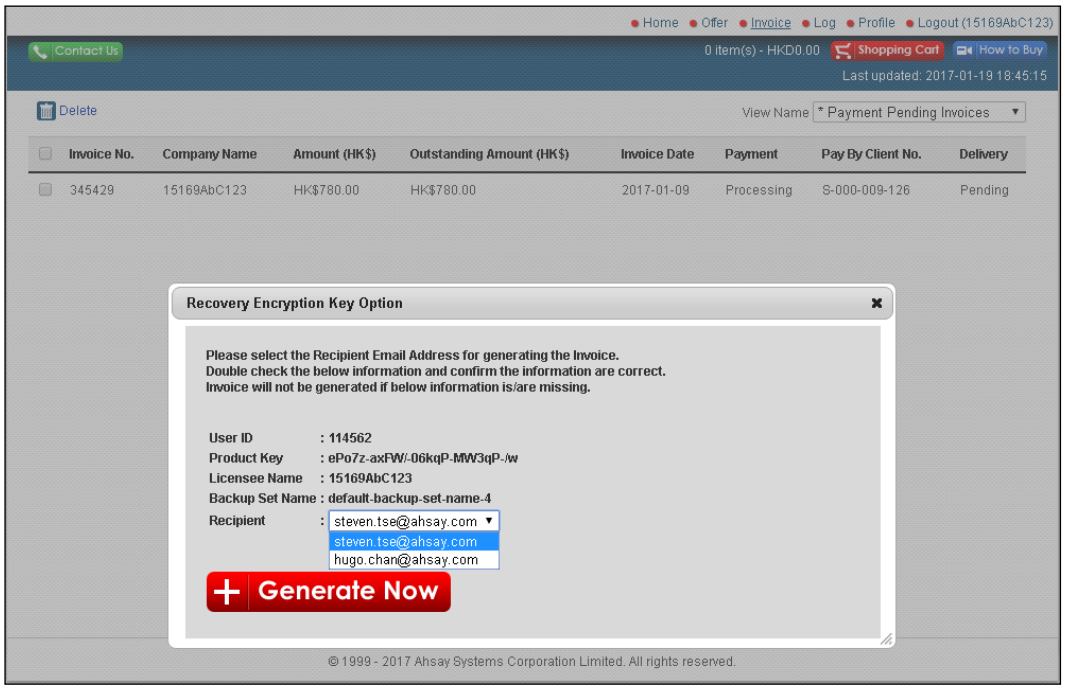


5. Upon successful login, you will be re-directed to the Ahsay Shopping Centre to proceed with the encryption key recovery process. You will see a page with your User ID, license information and backup set name listed as shown.

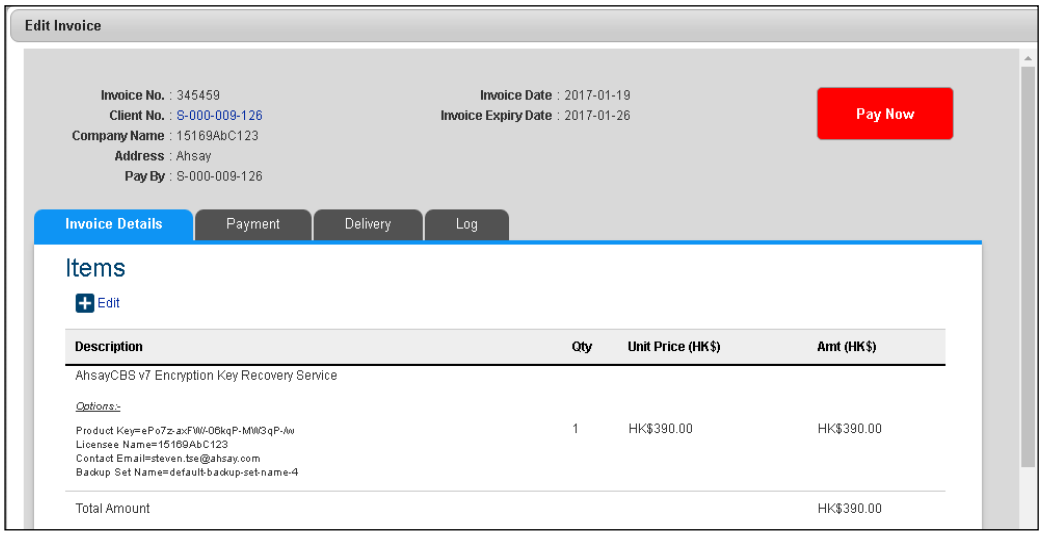


6. In the **Recipient** drop-down menu, the backup user's email will be selected as the primary recipient of the decrypted key by default, provided that the backup user has provided an email in his/her user profile. Otherwise, the decrypted key will be sent to you instead, where you can choose to deliver to either your Primary or Alternative Email registered under your account.

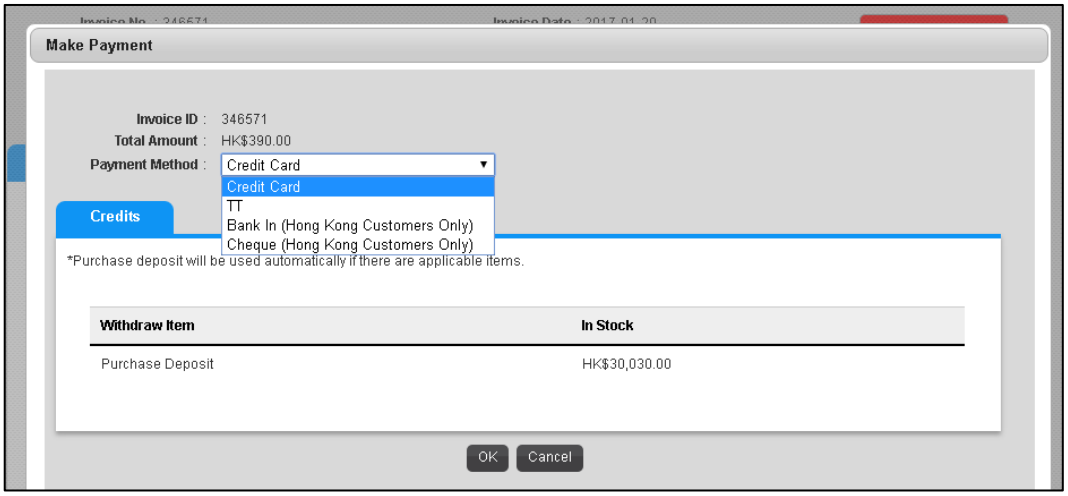
   Click **Generate Now** when you are ready to proceed.



7. You will then be taken to the Invoice page where you can confirm the details of the Encryption Key Recovery Service and the service price. Click the **Pay Now** button when you are ready to proceed with payment.



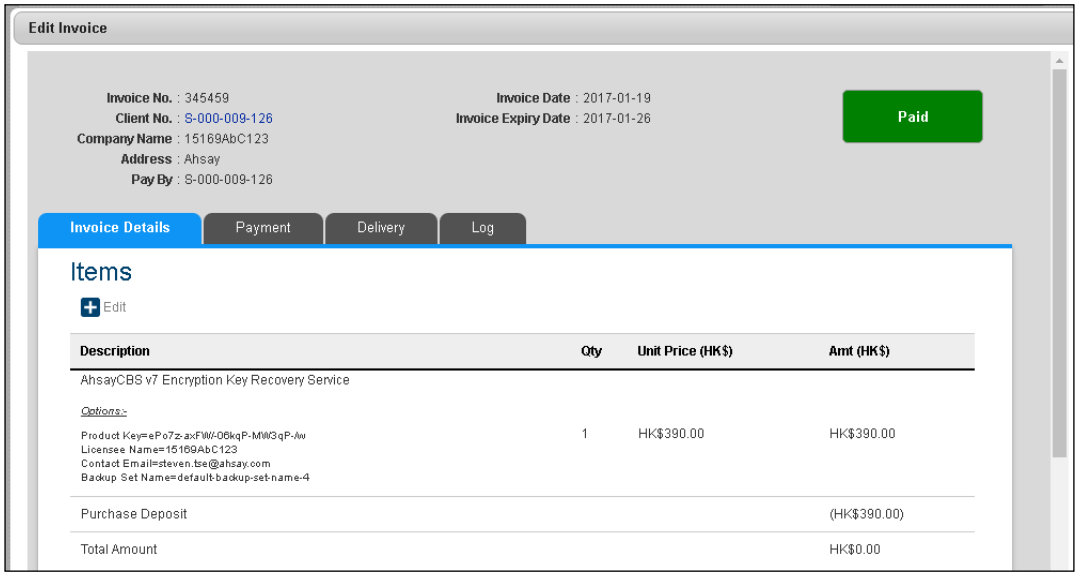
8. Select the desired payment method on this page. You are strongly recommended to pay by Credit Card so that the payment can be confirmed immediately in order to expedite the recovery process. Click **OK** when you are ready to proceed.



9. Depending on the payment method you have selected, you will be taken to the corresponding page to process your payment. Follow the relevant on-screen instructions to confirm the payment.

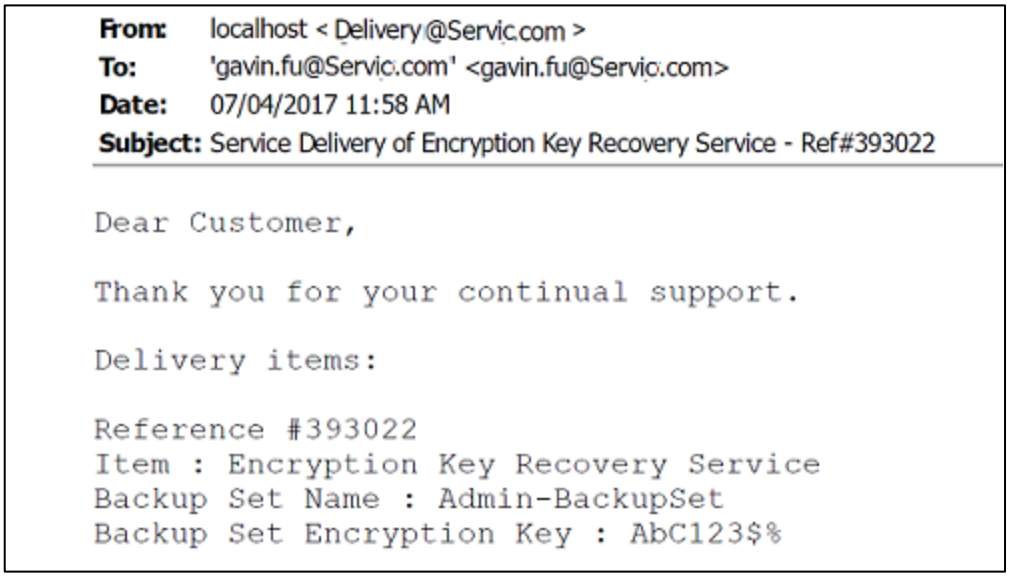
10. When the payment is processed successfully, you will be re-directed to the Invoice page again with the green icon labeled **Paid** as shown.

The Encryption Key Recovery request process is now completed.



11. The decrypted key will be delivered to the selected email within 15 minutes after the payment has been confirmed.

12. Below is a sample of the email with the decrypted key delivered.



From: localhost < Delivery@Servic.com >
To: 'gavin.fu@Servic.com' <gavin.fu@Servic.com>
Date: 07/04/2017 11:58 AM
Subject: Service Delivery of Encryption Key Recovery Service - Ref#393022

Dear Customer,

Thank you for your continual support.

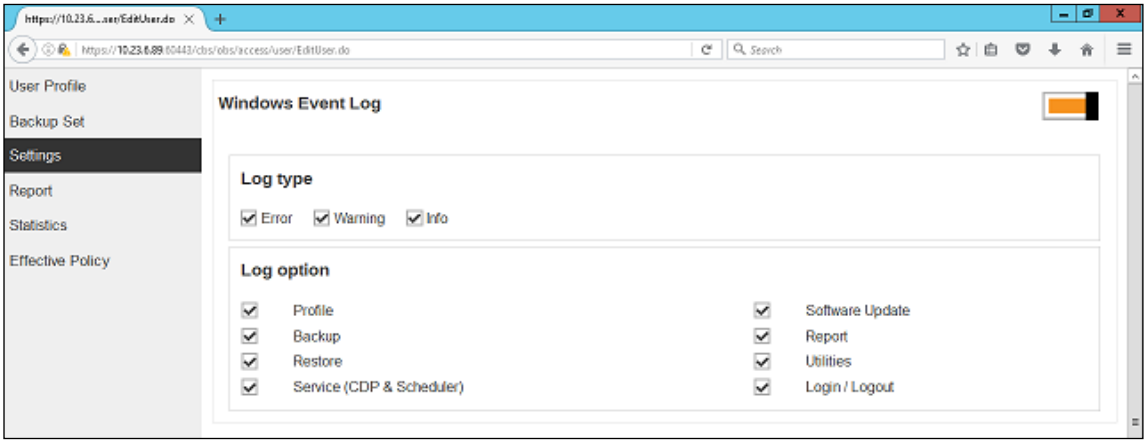
Delivery items:

Reference #393022
Item : Encryption Key Recovery Service
Backup Set Name : Admin-BackupSet
Backup Set Encryption Key : AbC123$%

Settings

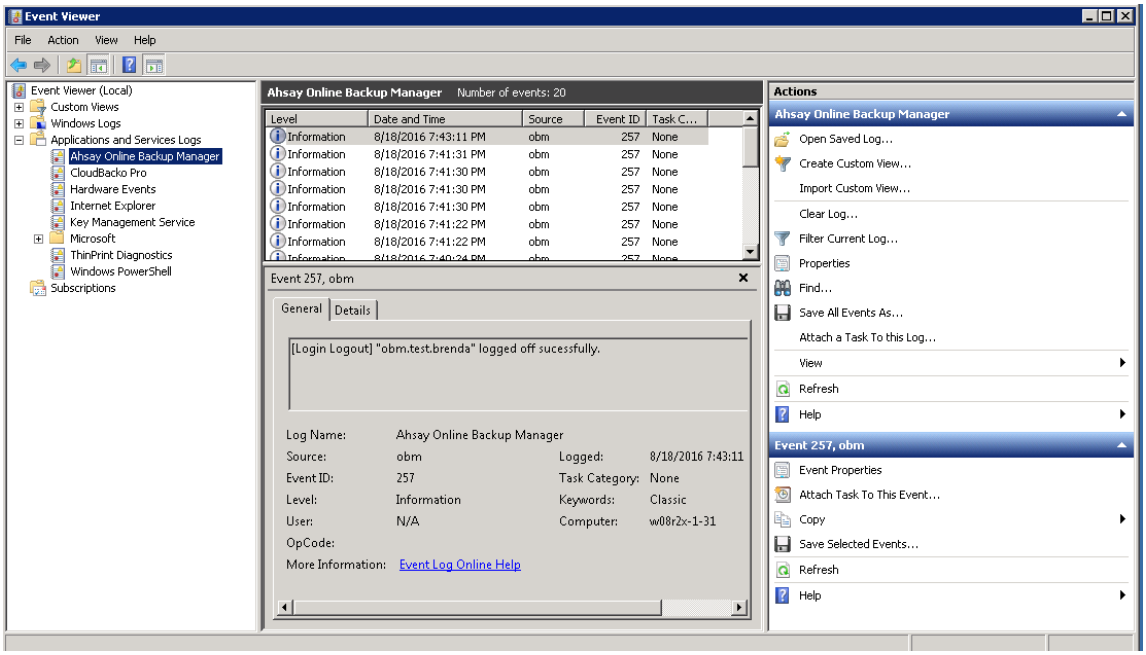
The **Settings** tab allows user to backup client to log the optional events, besides AhsayOBM/ AhsayACB logs, to the Windows event log. This feature is supported on AhsayOBM/AhsayACB clients installed on Windows platform only.

Windows event log



- **Log type** – There are 3 log types: **Error**, **Warning** and **Info**. Select any of the 3 log types, they will be logged in the Windows event log.
- **Log option** - Select the desired log option to be captured in the Windows event log. Currently there are 8 different log options: **Profile**, **Backup**, **Restore**, **Service (CDP & Scheduler)**, **Software Update**, **Report**, **Utilities**, **Login/ Logout**.

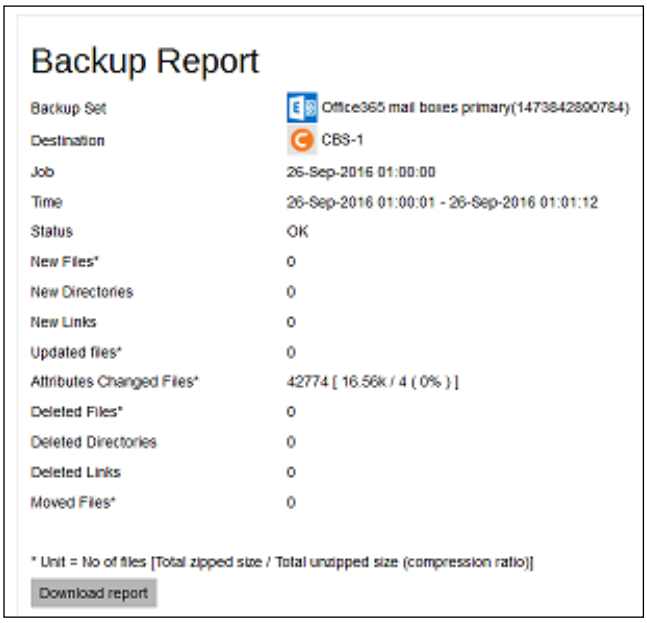
The events are logged in the Windows event log and can be view from the Windows Event Viewer:



Report

The **Report** tab allows you to check the backup report and restore report for the backup user.

Click the report to see the details. Below is an example of a backup report.



Click the **Download report** button at the bottom of the **Backup Report** page to download the complete report in PDF format. The report contains the following information in details.

- Backup Job Summary
- Backup Set Settings
- Backup Logs
- Backup Files

NOTE

The **Download report** button should be visible around 20 minutes after the backup job has completed.

OpenDirect restore of file backup sets or granular restore of files from VMware and Hyper-V backup sets performed using Windows File Explorer will NOT generate any restore reports on AhsayCBS. Restore reports are only available when the restore is performed directly through AhsayOBM/ AhsayACB/ AhsayOBR or AhsayCBS User Web Console.

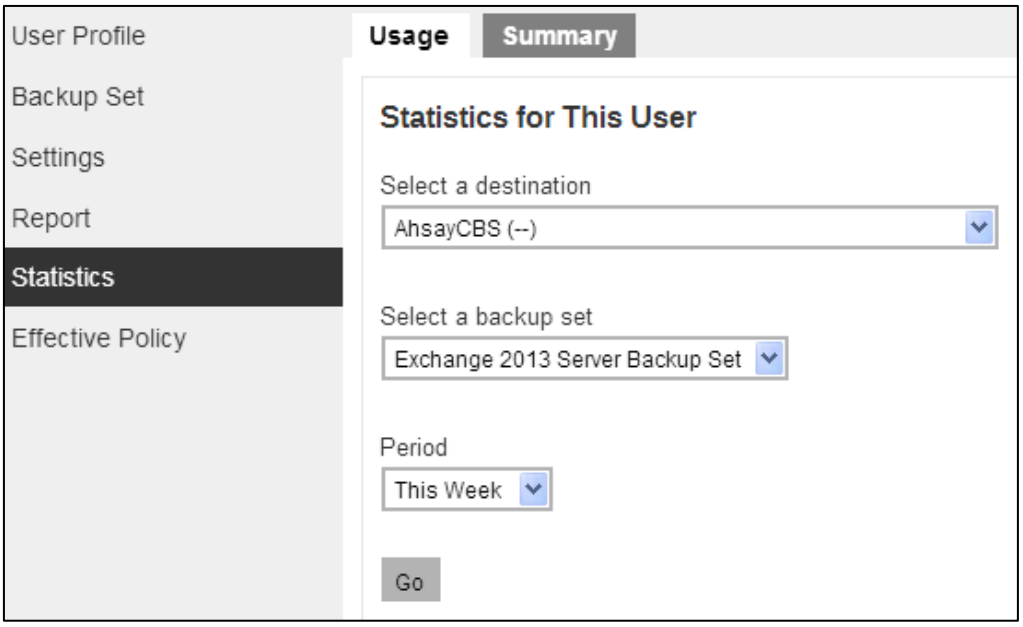
Statistics

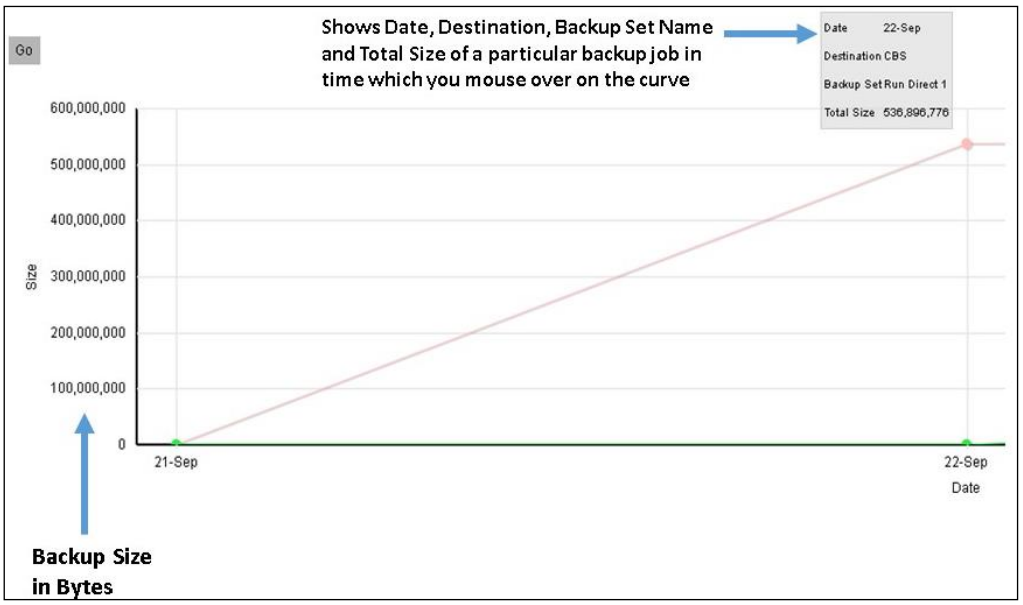
The Statistics tab allows you to generate a graph of storage statistics for the user by modifying a few factors such as the backup destination, backup set and the period of the backup. The statistics shows the storage capacity of different backup sets on different dates.

Usage

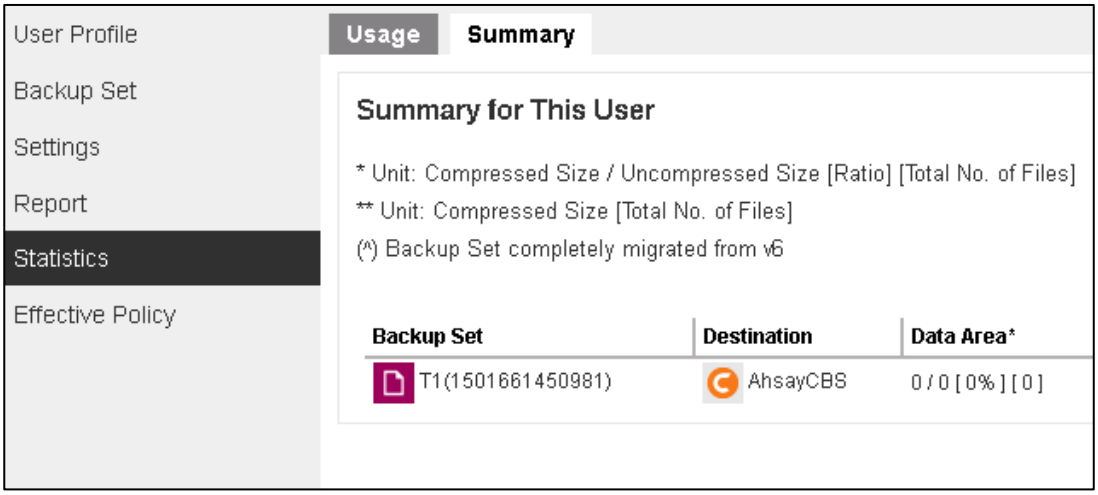
The following options are configurable for generating statistics in your desirable view.

- **Select a destination** – select the backup destination of your choice
- **Select a backup set** – you can choose a specific backup set or all backup sets
- **Period** – select the period of time during which backups were performed





Summary Tab



There are four columns showing the following information of each backup set.

Data Area

Data Area**
0 / 0 [0%] [0]
1.18G / 1.17G [0%] [149]
3.98M / 4.98M [20%] [12]
181.01M / 1.24G [86%] [703]

Format:
[Compressed Size] / [Uncompressed Size] [Compression Ratio in %] [Number of files]

Example: 3.98M / 4.98M [20%] [12]
The data interpreted as the backup set has 12 files in the data area; the files compressed and uncompressed sizes are 3.98M and 4.98M respectively; the compression ratio is 20%.

Retention Area

Retention Area**
0 / 0 [0%] [0]
4.12M / 4.12M [0%] [12]
0 / 0 [0%] [0]
0 / 0 [0%] [0]
0 / 0 [0%] [0]
34.12M / 234.07M [86%] [239]

Format:
[Compressed Size] / [Uncompressed Size] [Compression Ratio in %] [Total number of files]

Example: 34.12M / 234.07M [86%] [239]

The data interpreted as the backup set has 239 files in the retention area; the files compressed and uncompressed sizes are 34.12M and 234.07M respectively; the compression ratio is 86%.

Total Upload

Total Upload*
0 [0]
1.19G [183]
4M [20]
181.02M [706]
21.06M [78]
789.86M [683]

Format:
[Compressed Size] [Total number of files]

Example: 4M [20]
There are a total of 20 files sized of 4M uploaded for this backup set.

Total Restore

Total Restore*
0 [0]
612.2M [92]
0 [0]
0 [0]
25.12M [36]
4.48G [1044]

Format:
[Compressed Size] [Total number of files]

Example: 612.2M [92]
There are a total of 92 files sized of 612.2M restored from this backup set.

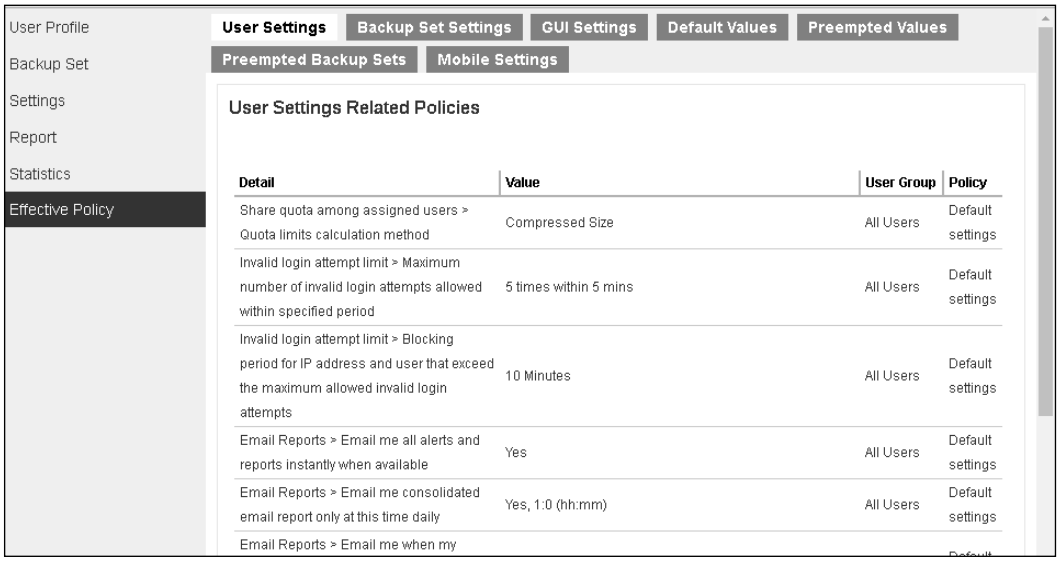
Effective Policy

The Effective Policy tab shows the details of all policies and settings which applies to the backup user account. The **Effective Policy** tab is located under **Users, Groups & Policies > Backup User**. It can be hidden by unchecking the box of **View** for **Effective Policy** under **Users, Groups & Policies > Policy Group > Default settings > GUI Settings.**

It is subdivided into 7 tabs, each of which is described below.

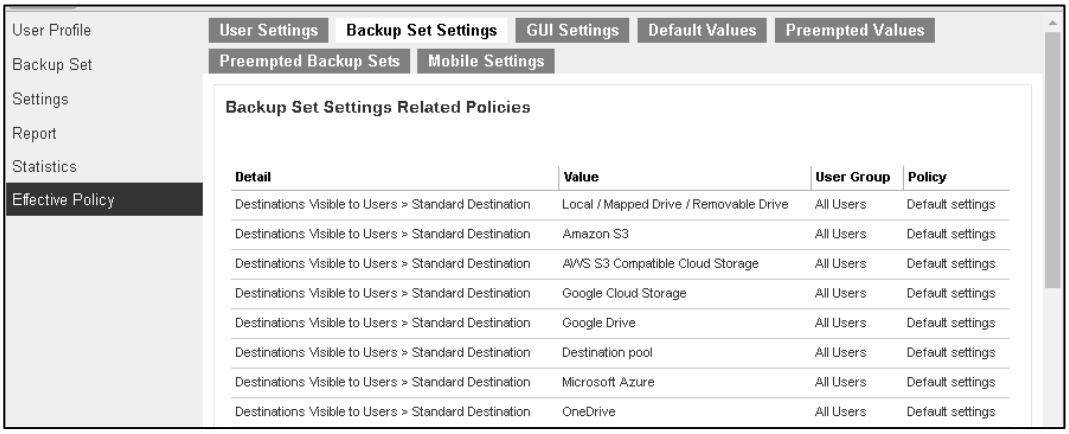
User Settings Tab

You can see the effective policy on user settings for this user on the **User Settings** tab.



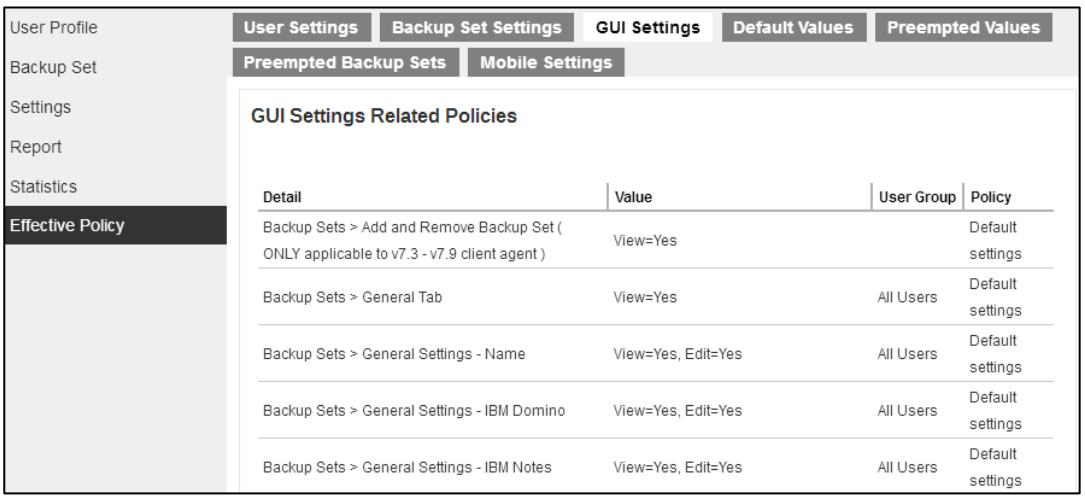
Backup Set Settings Tab

You can see the effective policy on backup set settings for this user on the **Backup Set Settings** tab.



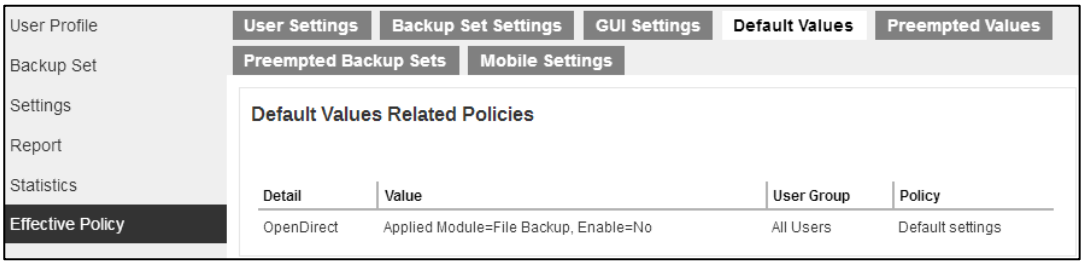
GUI Settings Tab

You can see the effective policy on AhsayOBM or AhsayACB GUI settings for this user on the **GUI Settings** tab.



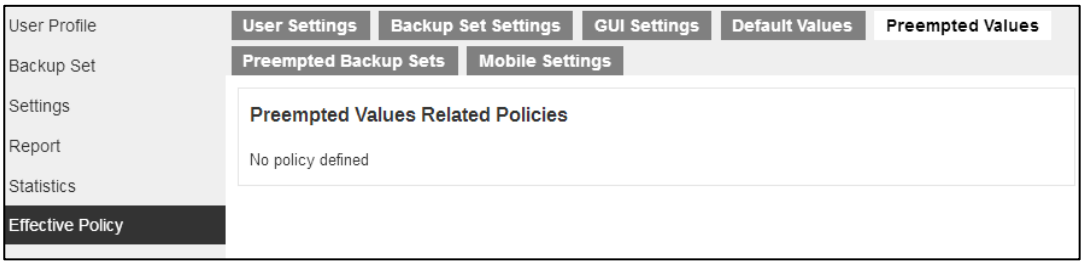
Default Values Tab

You can see the effective policy on default values for this user on the **Default Values** tab.



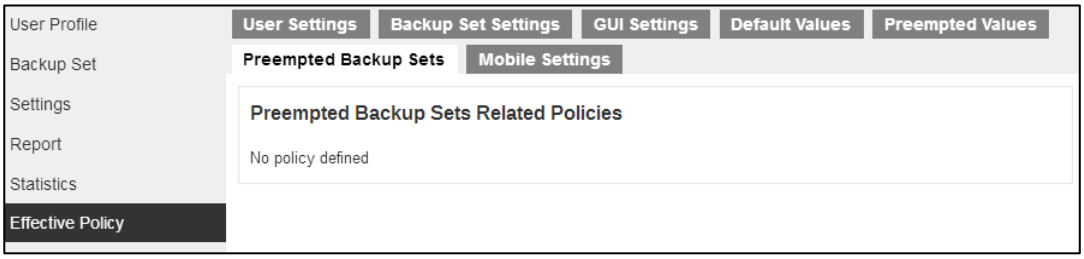
Preempted Values Tab

You can see the effective policy on preempted values for this user on the **Preempted Values** tab.



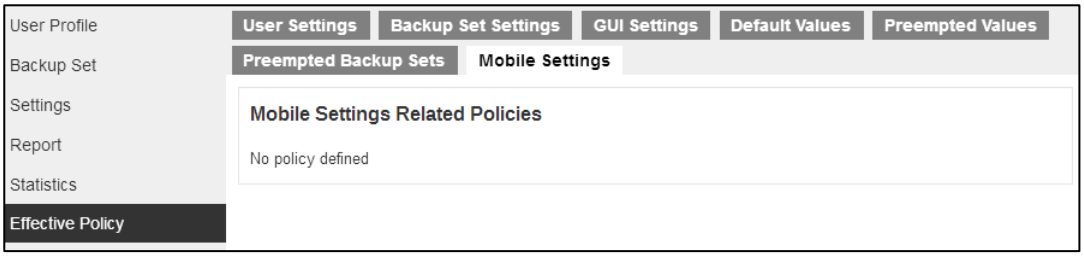
Preempted Backup Sets Tab

You can see the effective policy on preempted backup sets for this user on the **Preempted Backup Sets** tab.



Mobile Settings Tab

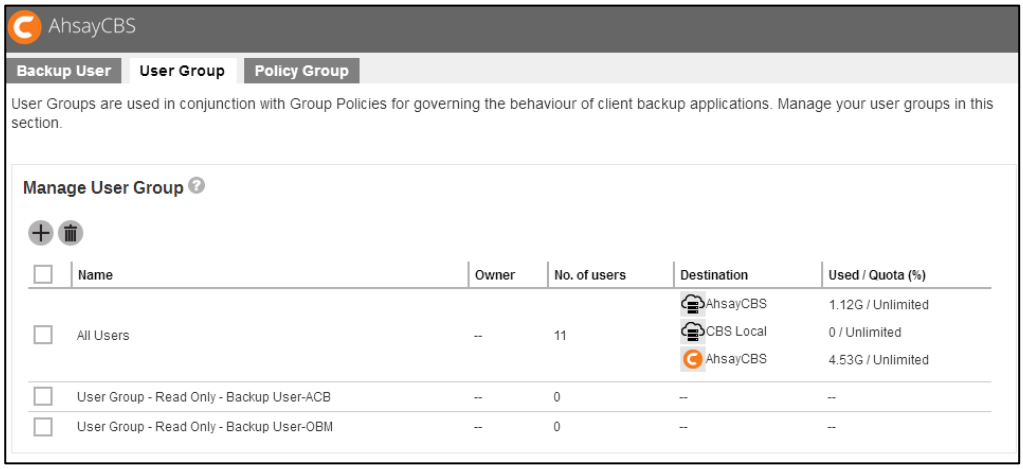
You can see the effective policy on mobile settings for this user on the **Mobile Settings** tab.



Manage User Groups

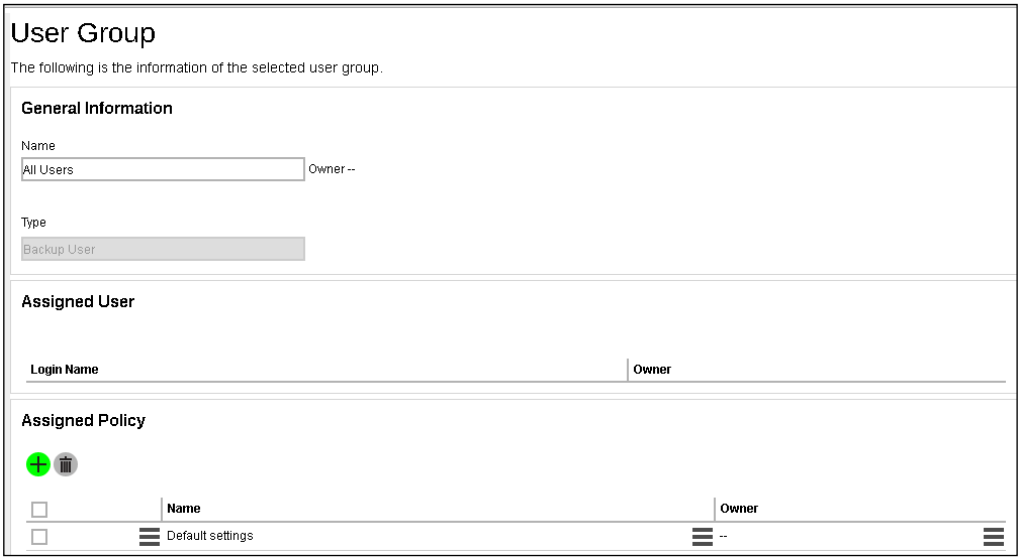
User Group is used in conjunction with Group Policies (see the next chapter Manage Policy Groups for details) for governing the behavior of client backup agent and the AhsayCBS.

The following shows the User Group tab under **Backup / Restore** > **Users, Groups & Policies**.



The default user group

By default, the user group named All Users has been created. All backup users will be put under the **All Users** user group by default after the user account has been created. When you click on one of the user groups, you will be able to see the followings:



- **General Information** – It shows the information of the user group, ownership, etc.
- **Assigned User** – A list of users assigned to the group.
- **Assigned Policy** – It shows a list of assigned polices to the user group. As the order of the policy would affect the actual applied to the user group, i.e. the policy on the top would probably overwrite the policy at the bottom of the list. If you want to arrange the order of the policies, you can simply drag the policy up and down.

For the **All Users** user group, it has a predefined policy called **Default settings**.

To add backup user to a user group

Backup user cannot be added to a user group in this menu. To do so, you can either:

- Add a user to a user group when you first create the user account, refer to Create a New Backup User for further instructions.

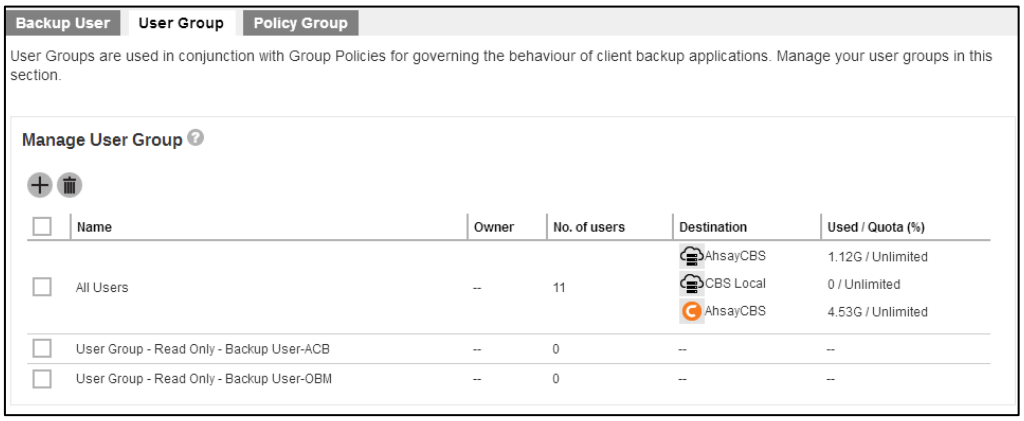
  -OR-

- You can add user a to a user group after the account has been created, refer to User Profile for further instructions.

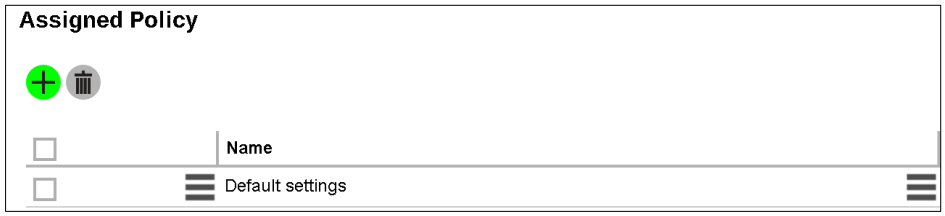
To add a new policy group to a user group

Follow the steps below to either add an additional policy group to the default user group (All Users) **OR** add a policy group to a newly created user group.

1. Click the user group which you wish to add a policy group to.



2. Click the button under the **Assigned Policy** section.

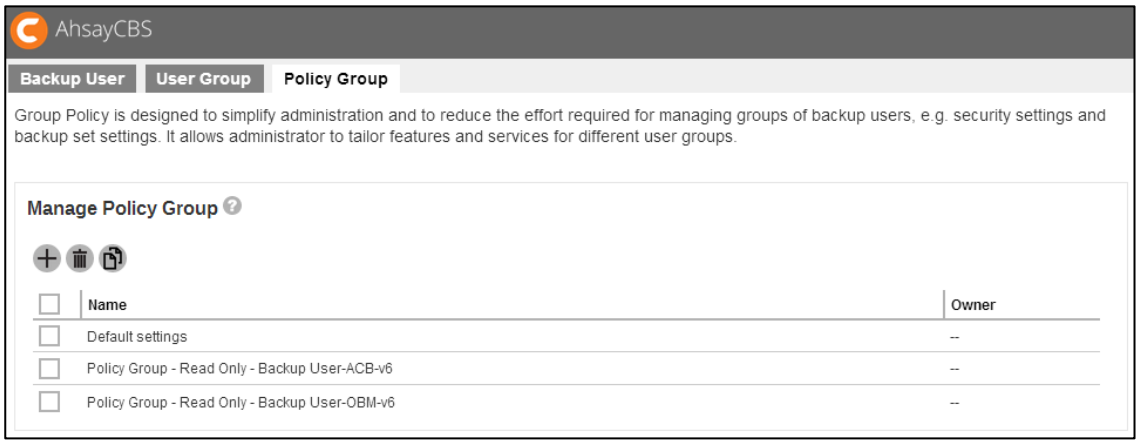


3. You will see a list of policy groups available for selection.

4. Select the desired policy group by checking the box in of the policies, then click to add, and then click to confirm.

Manage Policy Groups

The following shows the **Policy Group** tab under **Backup / Restore** > **Users, Groups & Policies**.



Policy Group is designed to simplify administration and to reduce the effort required for managing groups of backup users, e.g. security settings and backup set settings. It allows administrator to tailor features and services for different user groups. On a fresh AhsayCBS installation, there is a **Default settings** policy group and it is assigned to the **All users** user group.

WARNING

As all the default settings are stored inside “Default settings” policy group, if you change the settings in this policy group, it would affect all users in your AhsayCBS.

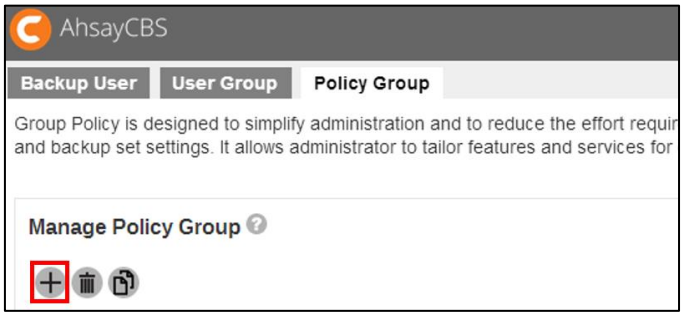
In case you need to work on the policy settings for a group of user base on the default policy group settings, you can consider the followings:

- Duplicate the **Default settings** policy group. Refer to the steps in To duplicate a policy group for details.
- Create a user group for your selected users and apply the duplicated policy group to this new user group. Refer to the steps in To create a new policy group for details.

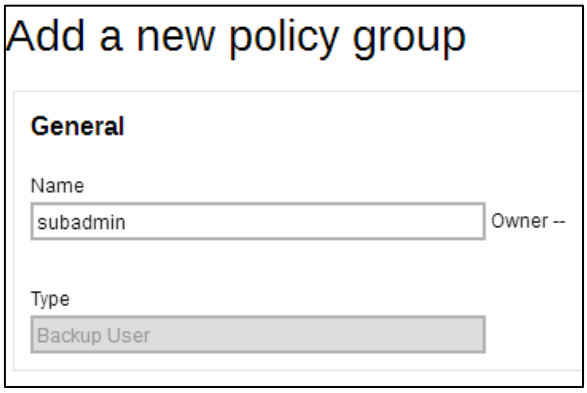
To create a new policy group

Follow the steps below to create a new policy group.

1. Click the button under the **Manage Policy Group** section.

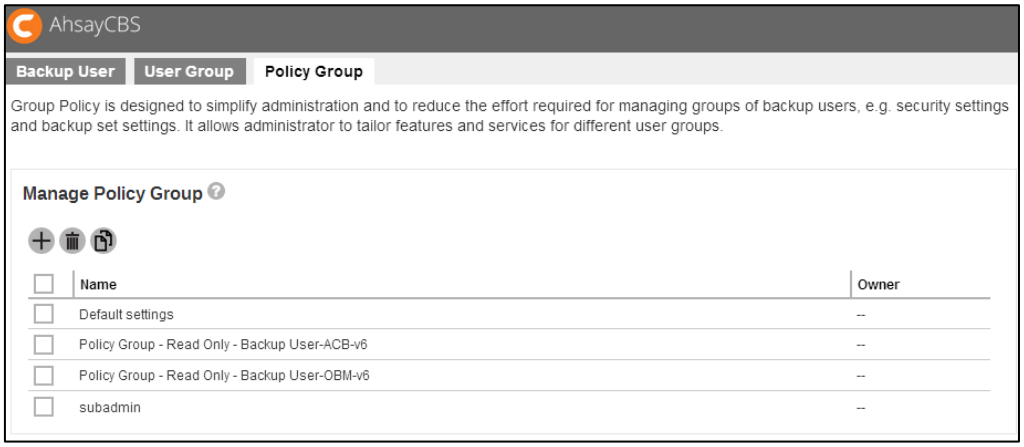


2. Enter a name for the policy group.



3. Click to confirm.

4. Go back to the **Policy Group** tab under **Backup / Restore** > **Users, Groups & Policies,** and you should be able to see the policy group name you have just created.

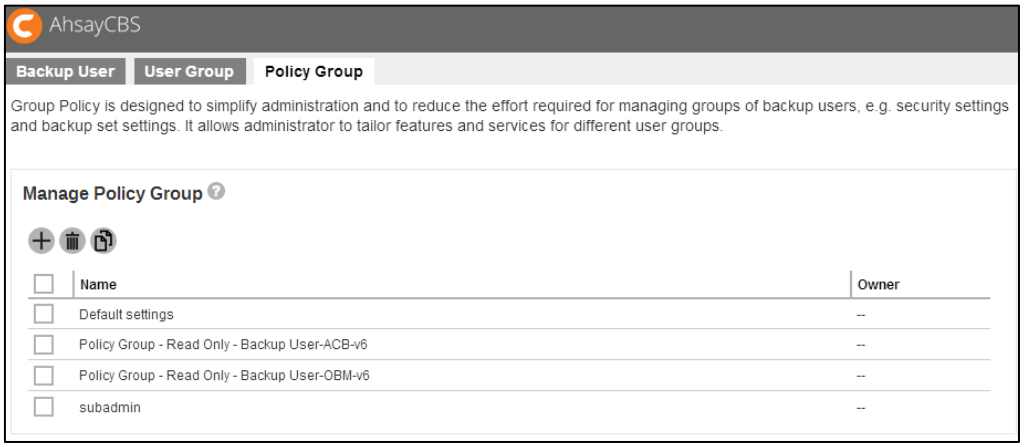


5. Click on the policy group for configuration. The configuration items are subdivided into 8 sections, each of which is described in the To configure a policy group section below.

To modify a policy group

After a policy group has been created, you can modify its settings by following the steps below.

1. Navigate to the **Policy Group** tab under **Backup / Restore** > **Users, Groups & Policies.**

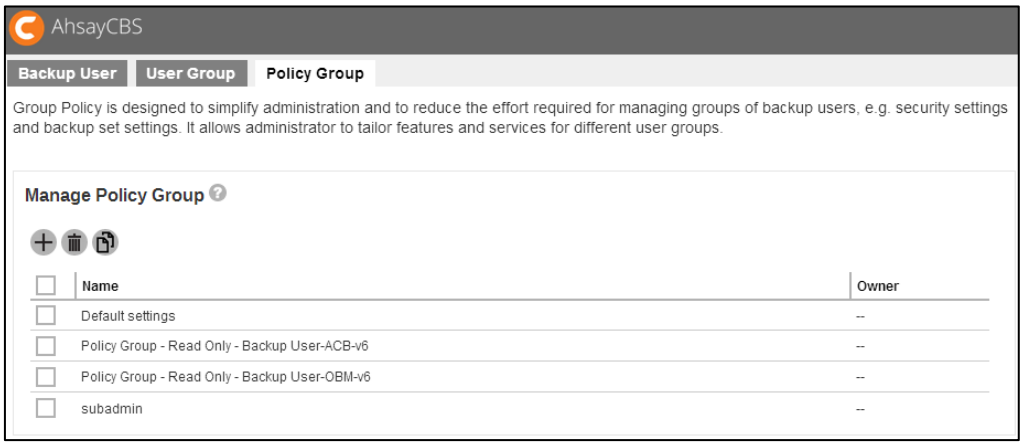


2. Click on the policy group you wish to modify, then follow the steps in the To configure a policy group section below for further instructions on modifying the configurations.

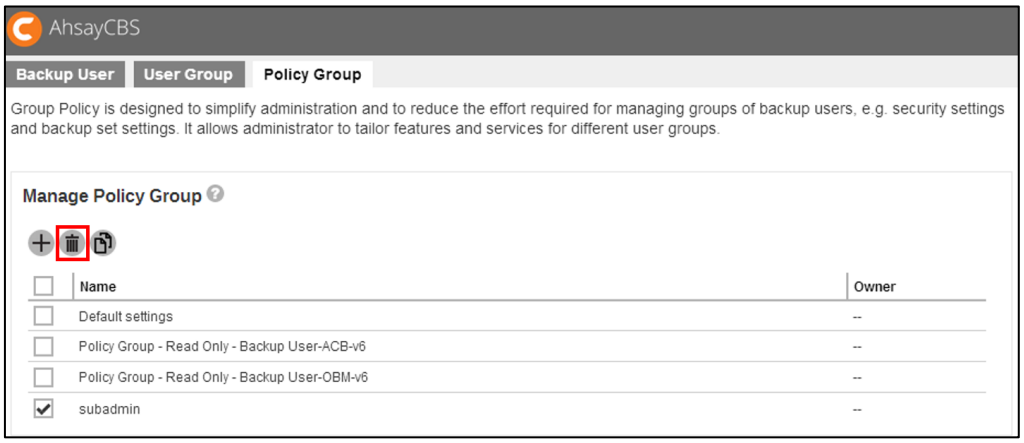
To delete a policy group

Follow the steps below to delete a policy group.

1. Navigate to the **Policy Group** tab under **Backup / Restore** > **Users, Groups & Policies.**



2. Check the box of the policy group you wish to delete, then click on the button as highlighted in the screen shot below.

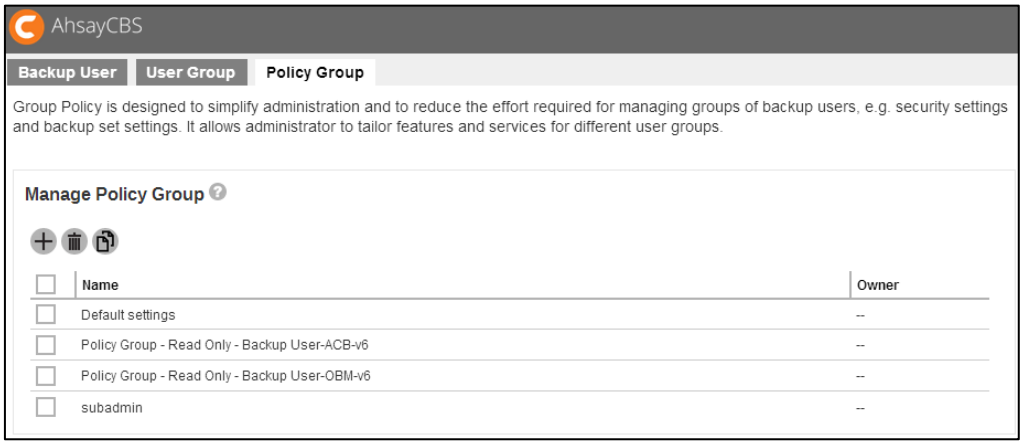


3. Click “OK” to confirm.

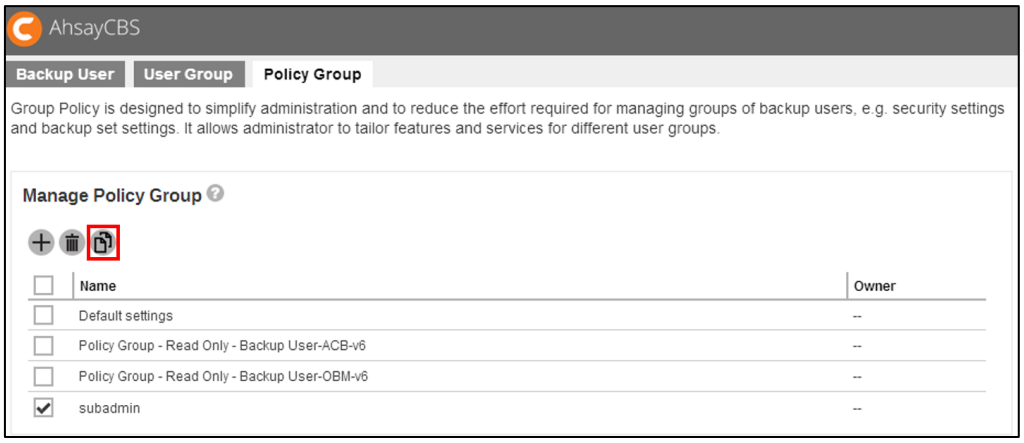
To duplicate a policy group

Follow the steps below to duplicate an existing policy group. This is useful when you wish to apply the same configurations from a policy group to a group of users.

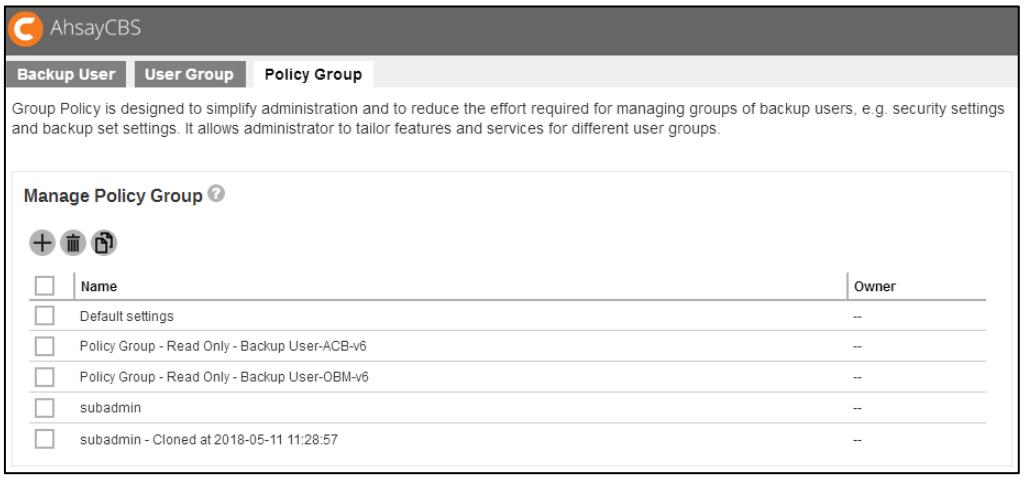
1. Navigate to the **Policy Group** tab under **Backup / Restore** > **Users, Groups & Policies.**



2. Check the box of the policy group you wish to duplicate, then click on the button as highlighted in the screen shot below.



3. You will immediately see the policy group is being duplicated, with the suffix "**Clone at YYYY-MM-DD HH:MM:SS**" in the duplicated group policy's name.

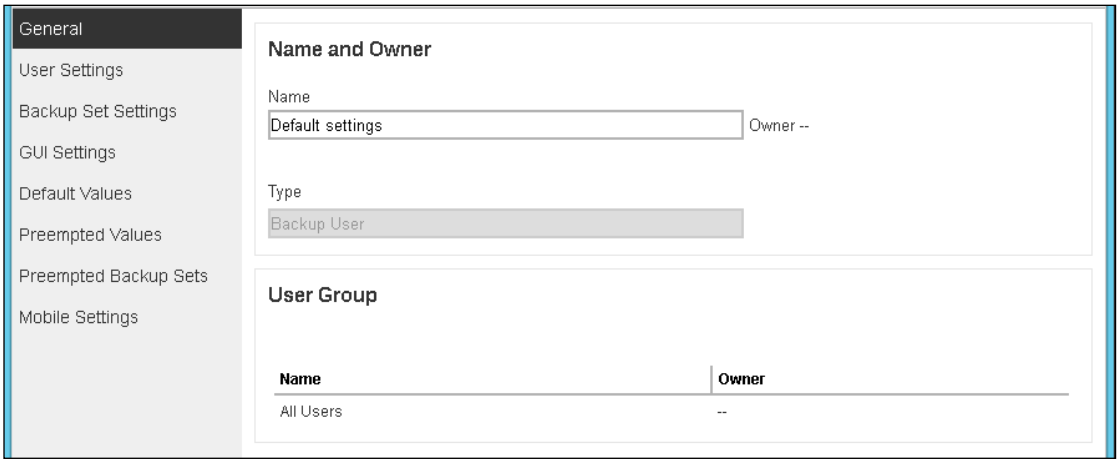


4. If you need to configure the duplicated policy group, follow the steps in the To configure a policy group section below for details.

To configure a policy group

General

This is the general settings of the policy group page, and the user group is a list of user group which is a list of user groups which has applied this policy.



- **Name** – the name of the policy group. The name is configurable.
- **Type** – predefined as Backup User
- **User Group** – displays the user group(s) with this policy group applied.

If you have changed the policy group name, click to confirm.

➢ **To add backup user to a policy group**

Backup users cannot be added to a policy group directly in this setting menu. To do so, you have to:

Step 1: Add the user to a user group first by following the steps in either case below:

➢ Add a user to a user group when you first create the user account, refer to Create a New Backup User for further instructions.

-OR-

➢ You can add user a to a user group after the account has been created, refer to User Profile for further instructions.

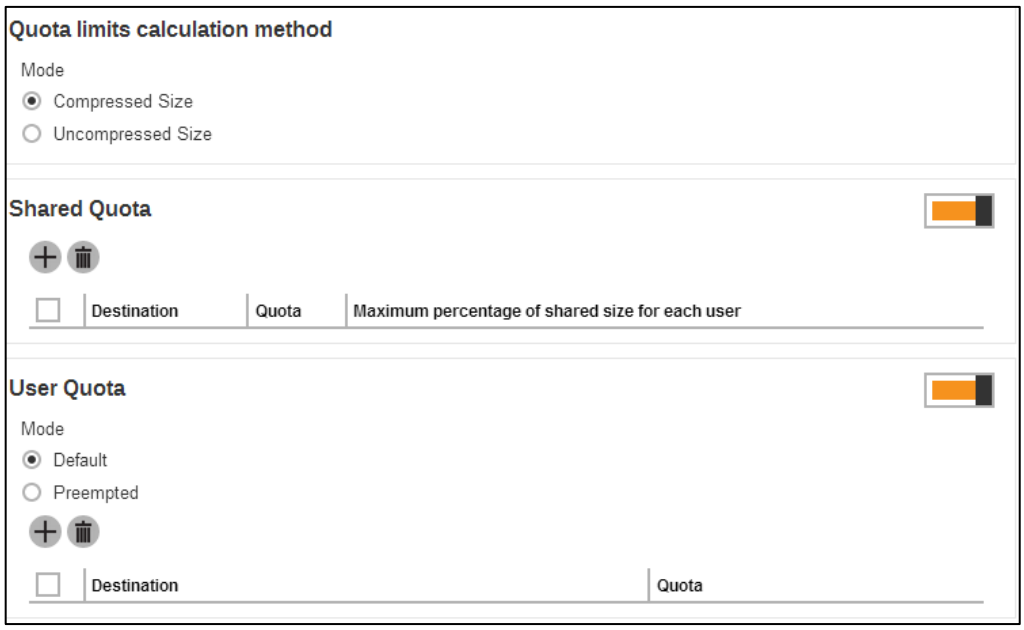
Step 2: Assign the desired policy group to the user group by following the steps in To add a new policy group to a user group.

User Settings

This section allows you to manage user settings such as Quota, Invalid Login Attempt Limit, Password, Email Reports, Encryption Key, Client Host limit, Run Direct VM Limit and Advertisement.

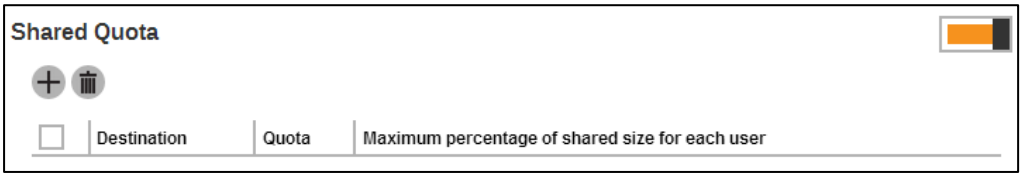
➢ **Quota**

Administrators can set a group storage quota to a user group.



The following items can be set:

- **Quota limits calculation method** - this defines if the quota limit is calculated by Compressed Size or Uncompressed Size.
- **Shared quota**



NOTE

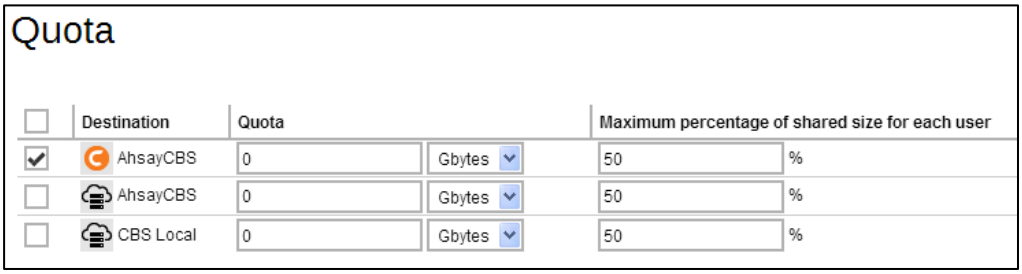
Please kindly note that:

➢ For fresh installation user, Shared Quota default setting is disabled.

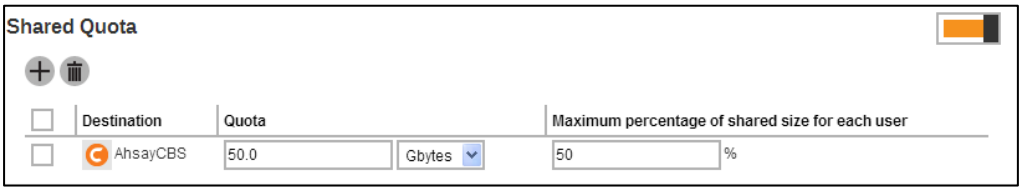
➢ For the user migrated from pre-v7.15.6.0, Shared Quota will be same with the previous setting.

When this feature is enabled by turning on the switch to the right, you can click to add the shared quota option, and the destination storage quota will be shared by all

users within the user group.



After adding the shared destination, you can configure the following two settings.



- **Quota** – this defines the storage quota allowed for the user group.
- **Maximum percentage of shared size for each user** - defines the maximum percentage of shared storage allowed for each user. For example, setting 50% means all users in the user group can occupy up to 50% of the assigned storage quota. If 100GB is the assigned storage, each user can store up to 50GB of the assigned storage quota. If the value is set to 100%, all users can fully utilize the storage until the assigned storage quota is full.

IMPORTANT

The shared storage quota is allocated to users on a first-come-first-serve basis. If the shared storage quota remains unchanged when the number of backup user grows or there is a change on the maximum percentage of shared size for each user, it may cause issue like the one mentioned below.

Example

Settings: The shared storage quota is 100GB shared by 2 users with a maximum percentage of 50% of each user. In other words, each user is entitled to a maximum of 50GB of storage.

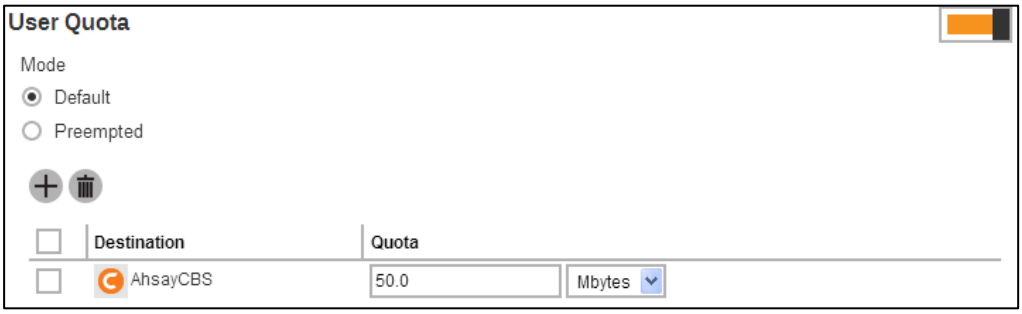
Current usage: Now, one of the users has used up 45GB of capacity

New setting: The maximum percentage of shared size for each user has adjusted to 30%.

Impact: In that case, that backup user has exceeded the new maximum percentage allowed for each user, which is 30GB. The backed up data will remain on the backup destination but that user will no longer be allowed to perform any new backup.

Best Practice: System administrator should consider upgrading the shared storage quota as the number of backup users in the user group grows or there is a change on the maximum percentage of shared size for each user.

- **User Quota –** the feature is used to define the destination and quota storage for the newly-added backup user.



NOTE

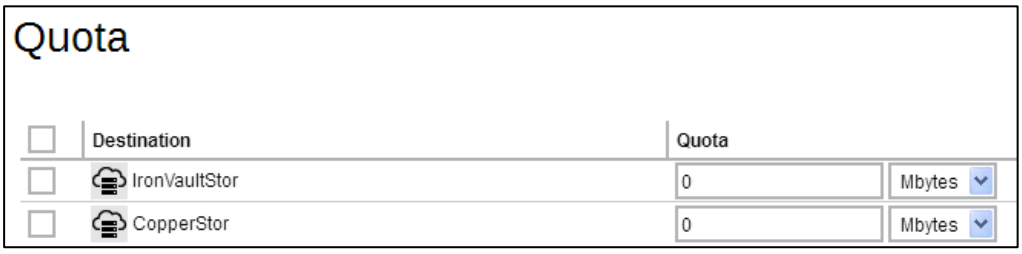
Please kindly note that:

- For fresh installation user, User Quota will be Default mode and Destination contains AhsayCBS with default quota setting, 50MB.
- For the user migrated from pre-v7.15.6.0, User Quota will be Default mode and Destination contains AhsayCBS with default setting, 50MB. If the policy group enable quota setting, the predefined destination will also be displayed.

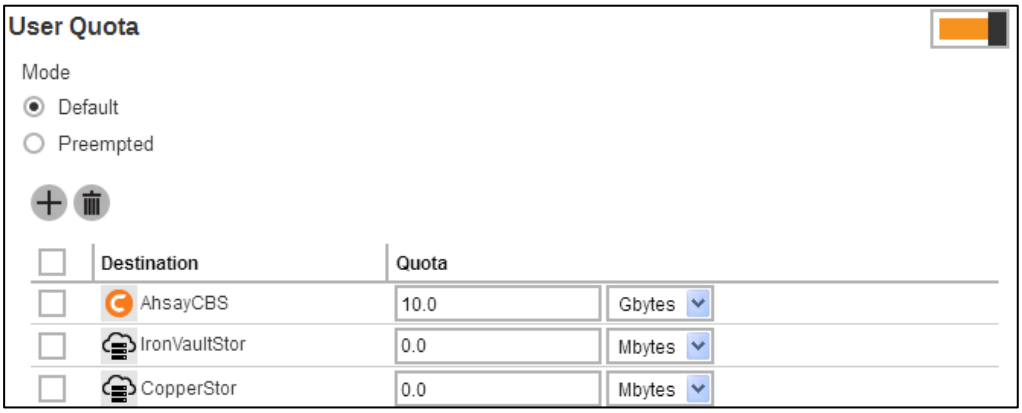
If the feature is disabled by turning the switch to the left, the backup user quota for newly-added user will be default quota setting, AhsayCBS with 50MB, but you can configure the quota setting as required.

When this feature is enabled, this defined if the user quota mode is Default or Preempted. If you choose Preempted mode, you cannot configure the quota settings in Backup/ Restore > Users, Groups & Policies > Backup User > %backup user% > User Profile > Backup Client Settings.

You can click to add predefined destination for the user as backup destination.

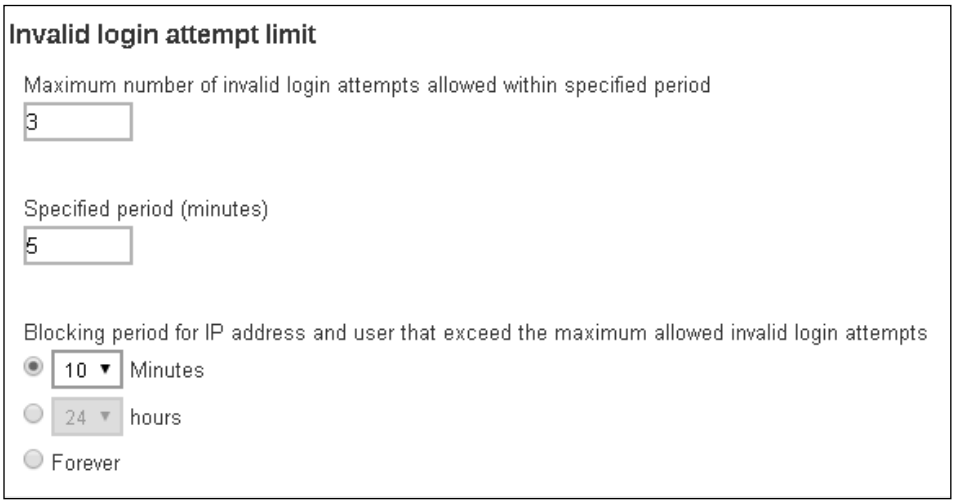


After adding the backup destination, you can configure the quota storage setting for per destination.



➢ Invalid Login Attempt Limit

This setting allows administrator to apply conditions for the number of invalid login attempt allowed to the user group. The following conditions can be set after you turned on the switch on the right.



- **Maximum number of invalid login attempts allowed within specified period** – this defines the maximum number of attempt allowed for invalid login within the set period time. The backup user account will be blocked after the set number of invalid login attempts have been reached.
- **Specified period (minutes)** – this defines the period of time during which the set maximum number of invalid login attempt is allowed before the invalid login counter resets.
- **Blocking period for IP address and user that exceed the maximum allowed invalid login attempts** – this defines the period of time during when the IP address and user that has exceeded the invalid login attempts will be blocked from logging in again.

Example:

If the following settings are applied:

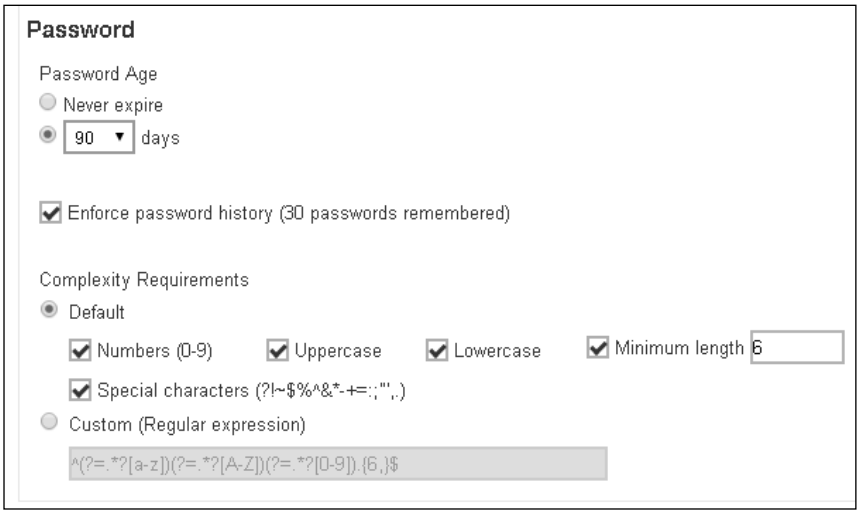
- **Maximum number of invalid login attempts allowed** - 3
- **Specific period** – 5 minutes

- **Blocking period for IP address and user that exceed the maximum allowed invalid login attempts** – 10 minutes

That means backup user can only enter a maximum of 3 times of invalid login within 5 minutes since the first attempt. If invalid login is made for the 4th time within that 5 minutes duration, the user account will be blocked for 10 minutes.

Password

This setting allows administrator to set up the password policy. The following items can be set after you turned on the switch on the right.



- **Password Age** – defines the period of time when the login password of a backup user account expires. When the set period of time is reached, backup users will have to change their passwords before they can continue using the CBS.
- **Enforce password history (30 passwords remembered)** – when this feature is enabled, the last 30 login passwords of each user are recorded and cannot be used again when users are changing a new password.
- **Complexity Requirements** – you can customize the complexity requirements for the password to provide better protection for the users. Under the **Default** option, the selected item(s) will be the mandatory element(s) when backup users create their passwords.

Email Reports

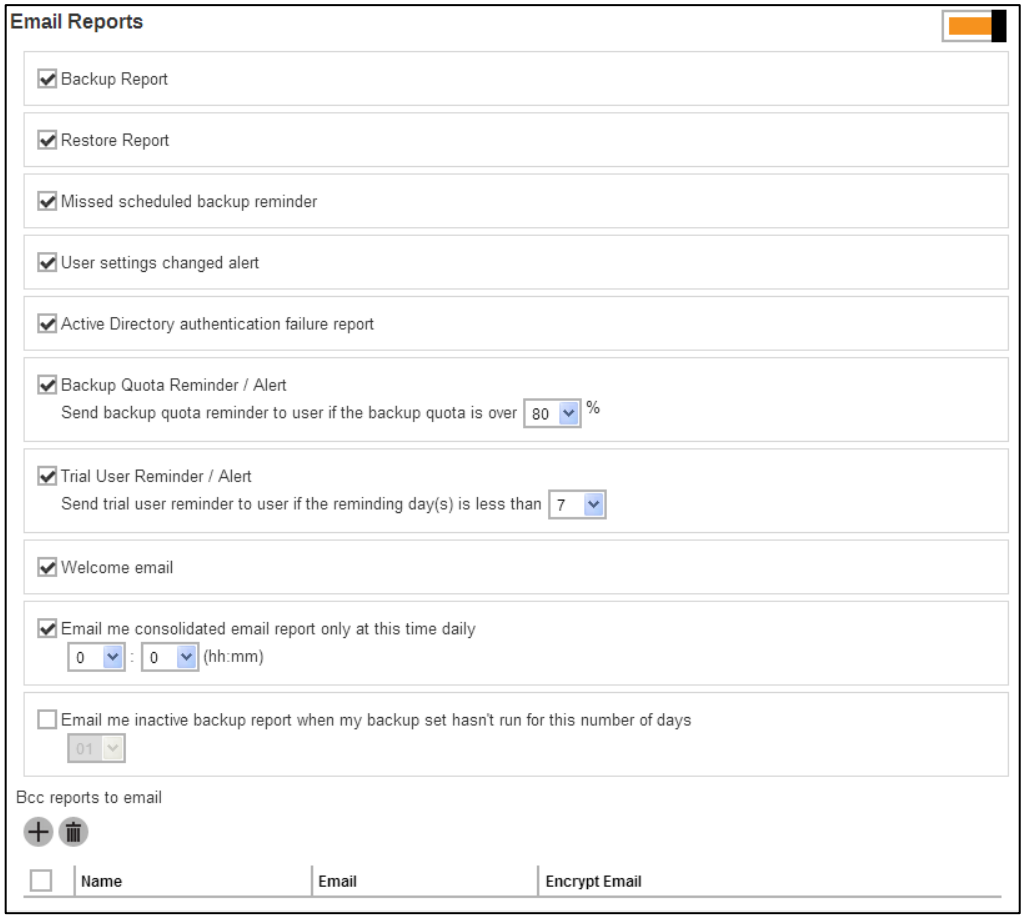
This menu allows administrator to select what email reports to be sent to the users of a user group. Turn on the switch on the right then select the desired email report(s) to send. By default, no email report is selected after you turned on this feature.

The table below lists out all types of email reports, together with explanation on what the email report is about, when it will be sent, what action backup user should take, and sample screen shot of the email and report. You can also add email recipients in the **Bcc reports to email** section so that the email reports will be sent to them as well.

NOTE

If the PDF report is too large to be sent through email (>20MB), the PDF attached in the email will only contains the first 100 pages of original backup report, with the 101st page showing "**Report truncated because it is too big to be sent in email**". Truncating the attached large report can avoid blocking from some SMTP server caused by email too big size and help save the capacity of client email box.

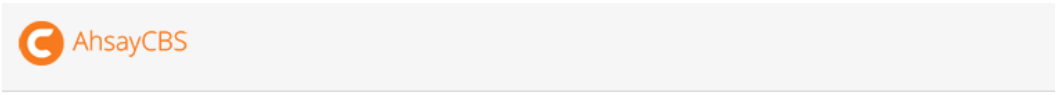
If the attached PDF report is truncated, the email will contain the links which point to the full PDF report download page.



Backup Report	
What is this email about?	**When will you receive it?**
A full backup report in PDF format, showing the Backup Job Summary (backup size, backup source and destination, etc.), Backup Logs, Backup Set Settings, Backup Files, etc.)	Backup Report is generated and sent to backup user every 15 mins (every :00, :15, :30 and :45 of an hour) *Depending on the backup size and backup finish time, the actual report sending time may be longer than 15 mins.

What action should you take?
Download the backup report as attached with the email
Email / Report Sample

Email sample:



Dear steven.tse@ahsay.com,

Please download the attachment "DailyUserReport.html" to view your consolidated Daily User Report for 11/24/2016. **58 error(s)** and **83 issue(s)** were found by the system. Please review and fix them as soon as possible.

Backup Job

User	Backup Set	Backup Job	Report
steven	K Drive Backup (1479792751514)	2016-11-24-10-24-33	Download
steven	K Drive Backup (1479792751514)	2016-11-24-12-45-00	Download
steven	K Drive Backup (1479792751514)	2016-11-24-18-15-00	Download

Report sample:

AhsayCBS

Full Backup report

Backup Job Summary

User	steven
Backup Set	K Drive Backup (1479792751514)
Data Size	940.28M
RetentionSize	68.26M
Backup Job	2016-11-24-10-24-33
Destination	GoogleDrive-1 (Google Drive)
Job Status	OK
Start - End	11/24/2016 10:24:33 - 11/24/2016 10:25:46
IP Address	192.168.7.105
New Files *	3 (11.3M)
New Directories	0
New Links	0
Updated Files *	3 (12.2M)
Attributes Changed Files *	0 (0)
Deleted Files *	0 (0)
Deleted Directories	0
Deleted Links	0
Moved Files *	0 (0)

* No. of files (size)

Backup Set Settings

Field	Value
Backup Source	[\\LAUREL\Departments\Customer Services\Common\KMT\Steven]
Backup Schedule	[Computer Name: STEVEN-TSE][Daily Schedule: [Name: Daily-1, Time: 18:15, Type: , Duration: -1, Run Retention Policy: false]][Weekly Schedule: [Name: Weekly-1, Time: 12:45, Sun: false, Mon: true, Tue: true, Wed: true, Thu: true, Fri: true, Sat: false, Type: , Duration: -1, Run Retention Policy: , false]][Monthly Schedules][Custom Schedules]
Continuous Data Protection	[Enabled: false]
In-File Delta	[Enabled: true, Default Type: I, Block Size: -1, Minimum delta file size = 26214400, Maximum number of delta = 100, Maximum delta ratio = 50, Weekly variations: [], Monthly Variations: [, Day: 0, Criteria: Friday, Occurrence: First]
Retention Policy	[Type: SIMPLE, Period: 7, Unit: DAYS]
Command Line Tool	
Reminder	Log Off Reminder Computer Name: STEVEN-TSE, Offline Backup Reminder Computer Name: , Tolerance period: 1 Days 0 hours
Bandwidth Control	[Enabled: false, Mode: independent, Bandwidth Control:]
Others	Remove Temporary Files: true, Follow Link: true, Volume Shadow Copy: true, File Permissions: true, Compression Type: GzipBestSpeedCompression

Backup Logs

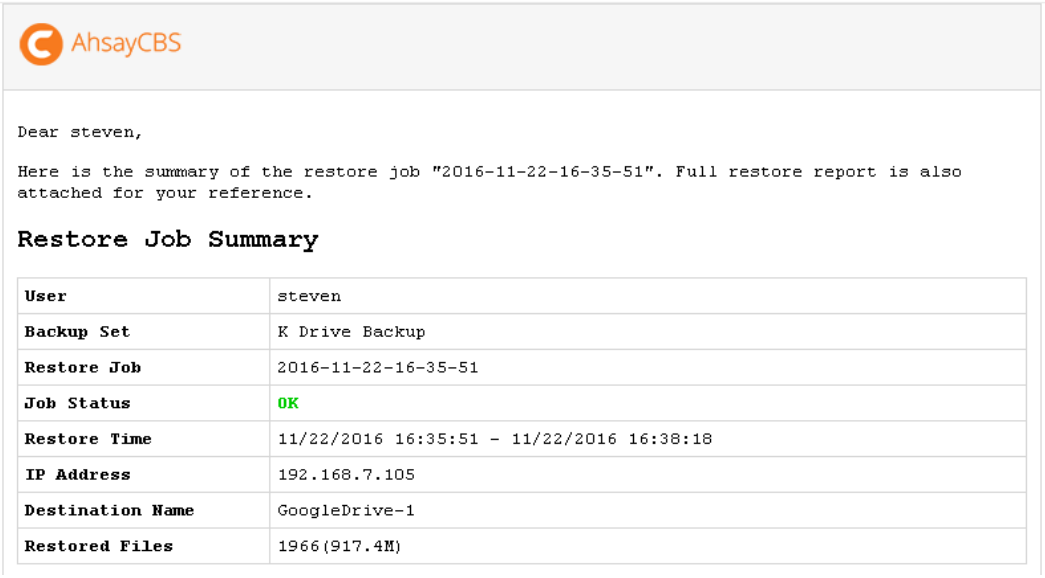
No.	Type	Timestamp	Log
1	start	2016/11/24 10:24:33	Start [Windows 7 (STEVEN-TSE), AhsayOBM v7.9.0.0]
2	info	2016/11/24 10:24:33	Saving encrypted backup set encryption keys to server...
3	info	2016/11/24 10:24:33	Using Temporary Directory C:\Users\steven.tse\temp\1479792751514\GDrive81479792876141
4	info	2016/11/24 10:24:33	Start running pre-commands
5	info	2016/11/24 10:24:33	Finished running pre-commands
6	info	2016/11/24 10:25:45	Start running post-commands
7	info	2016/11/24 10:25:45	Finished running post-commands

Backup Files

No.	Type	Dirs/Files	Size	Last Modified
1	new	\\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayCBS\AhsayCBS Administrator's Guide v7 \screen shot\User settting - Run Direct VM Limit.PNG	2k / 2k (14%)	11/23/2016 18:18
2	upd	\\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayCBS\AhsayCBS Administrator's Guide v7 \~$ide_ebs_admin_20161123.doc	106 / 162 (34%)	11/24/2016 09:19
3	new	\\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayCBS\AhsayCBS Administrator's Guide v7 \~$ide_ebs_admin_20161124.doc	106 / 162 (34%)	11/24/2016 09:49
4	upd	\\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayCBS\AhsayCBS Administrator's Guide v7 \guide_ebs_admin_20161123.doc	11.31M / 13.75M (17%)	11/23/2016 19:11
5	upd	\\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayCBS\AhsayCBS Administrator's Guide v7 \screen shot\Thumbs.db	907k / 1.02M (12%)	11/23/2016 18:18
6	new	\\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayCBS\AhsayCBS Administrator's Guide v7 \guide_ebs_admin_20161124.doc	11.31M / 13.76M (17%)	11/24/2016 09:53

Restore Report	
What is this email about?	**When will you receive it?**
A full report in PDF format, showing the Restore Job Summary, Restore Logs and Restore Files	Restore Report is generated and sent to backup user every 15 mins (every :00, :15, :30 and :45 of an hour) *Depending on the restore size and restore finish time, the actual report sending time may be longer than 15 mins.
What action should you take?	
Download the restore report as attached with the email	
Email / Report Sample	

Email sample:



AhsayCBS

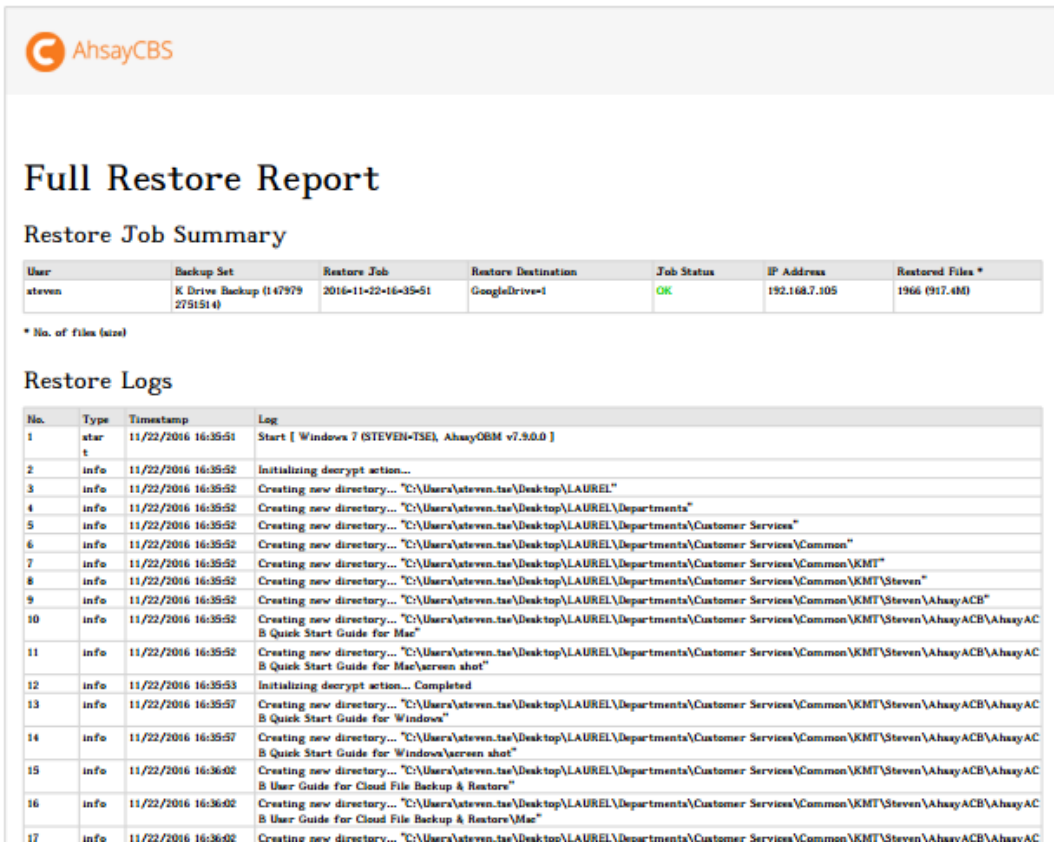
Dear steven,

Here is the summary of the restore job "2016-11-22-16-35-51". Full restore report is also attached for your reference.

Restore Job Summary

User	steven
Backup Set	K Drive Backup
Restore Job	2016-11-22-16-35-51
Job Status	OK
Restore Time	11/22/2016 16:35:51 - 11/22/2016 16:38:18
IP Address	192.168.7.105
Destination Name	GoogleDrive-1
Restored Files	1966(917.4M)

Report sample:



AhsayCBS

Full Restore Report

Restore Job Summary

User	Backup Set	Restore Job	Restore Destination	Job Status	IP Address	Restored Files *
steven	K Drive Backup (1479792751514)	2016-11-22-16-35-51	GoogleDrive-1	OK	192.168.7.105	1966 (917.4M)

* No. of files (size)

Restore Logs

No.	Type	Timestamp	Log
1	start	11/22/2016 16:35:51	Start [Windows 7 (STEVEN-TSE), AhsayOBM v7.9.0.0]
2	info	11/22/2016 16:35:52	Initializing decrypt action...
3	info	11/22/2016 16:35:52	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL"
4	info	11/22/2016 16:35:52	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments"
5	info	11/22/2016 16:35:52	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services"
6	info	11/22/2016 16:35:52	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services\Common"
7	info	11/22/2016 16:35:52	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services\Common\KMT"
8	info	11/22/2016 16:35:52	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services\Common\KMT\Steven"
9	info	11/22/2016 16:35:52	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayACB"
10	info	11/22/2016 16:35:52	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayACB\AhsayACB Quick Start Guide for Mac"
11	info	11/22/2016 16:35:52	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayACB\AhsayACB Quick Start Guide for Mac\screen shot"
12	info	11/22/2016 16:35:53	Initializing decrypt action... Completed
13	info	11/22/2016 16:35:57	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayACB\AhsayACB Quick Start Guide for Windows"
14	info	11/22/2016 16:35:57	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayACB\AhsayACB Quick Start Guide for Windows\screen shot"
15	info	11/22/2016 16:36:02	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayACB\AhsayACB User Guide for Cloud File Backup & Restore"
16	info	11/22/2016 16:36:02	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayACB\AhsayACB User Guide for Cloud File Backup & Restore\Mac"
17	info	11/22/2016 16:36:02	Creating new directory... "C:\Users\steven.tse\Desktop\LAUREL\Departments\Customer Services\Common\KMT\Steven\AhsayACB\AhsayAC

Missed scheduled backup reminder	
What is this email about?	**When will you receive it?**
A reminder to alert the backup user about a scheduled backup failure. Any backups that are failed to start 6 hours after the scheduled backup time will be considered as missed schedule backup.	The report is generated and sent to backup users at the next :00 after it's classified as missed scheduled backup (6 hours after backup failure)

Common causes for missed scheduled backups

The following table highlights some of the common reasons causing missed scheduled backups or scheduled backups not running according to schedule. The cause of missed backups can be related to either server side issues (AhsayCBS or Redirector) or client side issues (AhsayOBM/AhsayACB client machine setup).

Server Side Issues
The AhsayCBS service is unresponsive ➢ License error ➢ Out of Java memory / threads ➢ Out of space on AhsayCBS user home drive ➢ AhsayCBS service is not started ➢ AhsayCBS server is powered down ➢ SSL certificate expired
The Redirector service is unresponsive (if applicable) ➢ License error ➢ Out of Java memory / threads ➢ AhsayCBS system password is not updated on Redirection settings ➢ AhsayCBS service is not started on the redirector machine ➢ AhsayCBS server is powered down on the redirector machine ➢ SSL certificate expired
The time zone on the AhsayOBM/AhsayACB account user profile on AhsayCBS is set incorrectly. This will cause the scheduled backup time to run either later or earlier than the actual scheduled time but will trigger a missed backup notification.
There is no backup schedule configured for the affected backup set(s) or the schedule date and/or time is incorrect.
Client Side Issues
The AhsayOBM/AhsayACB client machine was switched off, hanged or running in power saving mode.
The date/time, time zone, or locale on AhsayOBM/AhsayACB client machine is set incorrectly.

A backup set and backup schedule was created on AhsayCBS but AhsayOBM/AhsayACB client was not installed on the client machine or was uninstalled.
If the AhsayOBM/AhsayACB runs on Windows machine, ensure the login credentials in the Windows User Authentication is correct or is kept updated.

What action should you take?

You may have to check for the causes for the missed scheduled backup. That could be caused by, for example, incorrect login credentials of the client backup application, Internet connection problem, time zone settings, etc.

Email / Report Sample

Email sample:

AhsayCBS

Dear PaidUser,
Your backup job for "default-backup-set-name" was missed. Please check the client software configuration to see if everything is running correctly. Below is the detail of backup set.

User	PaidUser	
Backup Set	default-backup-set-name	
Backup Statistics	**Data Area***	5[928]
	Retention Area*	1[48]
	* Unit = No. of file[Total file size]	
Last Backup Time(Days Without Backup)	2018-05-08-17-30-00(5)	
Missed backup job	2018-05-13-20-00-00	

You are suggested to perform a backup manually for this backup set to avoid undesired data loss.backup activity of this backup set.
Sincerely
Ahsay Support Team

User settings changed alert

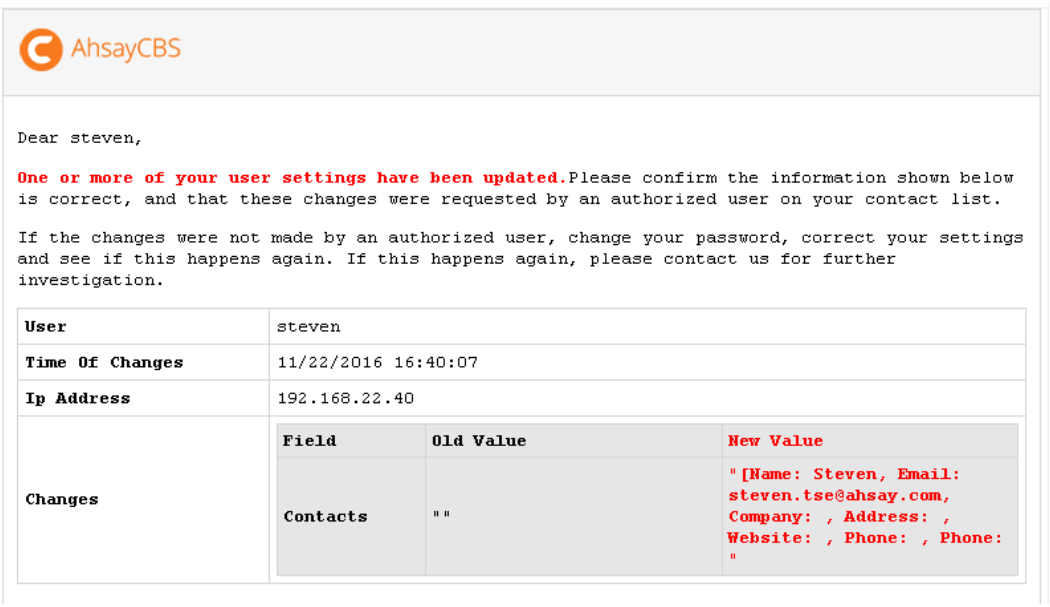
What is this email about?	When will you receive it?
A summary report showing the user settings that have been changed in details, with the old values and new values of the changed settings shown.	User Settings Changed Alert Report is generated and sent to backup user every 15 mins (every :00, :15, :30 and :45 of an hour)

What action should you take?

The purpose of this email is to allow user to confirm the changes that have made, and alert user for unauthorized access if they have not made those changes. In the latter case, user should change their login password and correct the settings as soon as possible.

Email / Report Sample

Email sample:



AhsayCBS

Dear steven,

One or more of your user settings have been updated. Please confirm the information shown below is correct, and that these changes were requested by an authorized user on your contact list.

If the changes were not made by an authorized user, change your password, correct your settings and see if this happens again. If this happens again, please contact us for further investigation.

User	steven
Time Of Changes	11/22/2016 16:40:07
Ip Address	192.168.22.40
Changes	

Field	Old Value	New Value
Contacts	""	"[Name: Steven, Email: steven.tse@ahsay.com, Company: , Address: , Website: , Phone: , Phone: "

Active Directory authentication failure report	
What is this email about?	**When will you receive it?**
A reminder to alert the backup user about a backup failure due to the incorrect Active Directory authentication.	Shortly after the active directory authentication failure occurred

What action should you take?

Check if the active directory authentication is properly set. If you have changed the login credentials of the machine running the client backup application, you have to alter the authentication details as well for the backup to perform. To do so, follow the steps below.

i) Log in to AhsayOBM/AhsayACB.

ii) Click on the **Backup Sets** icon.

iii) Click on the backup set you would like to alter the authentication details.

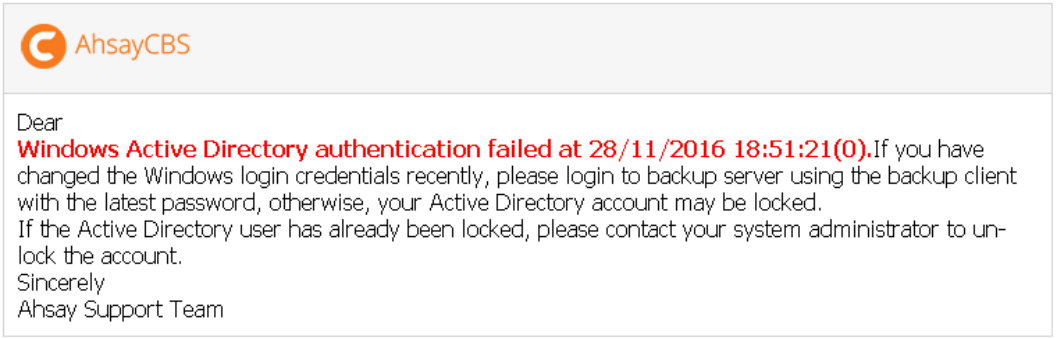
iv) Click on the **General** section.

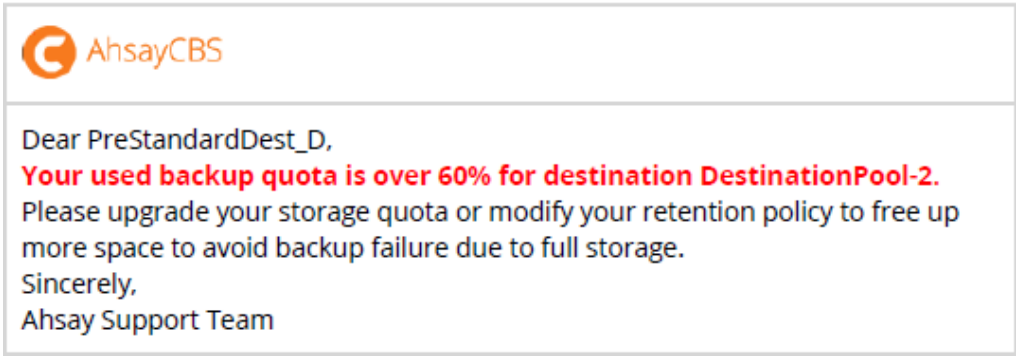
v) Modify the Password under the **Windows User Authentication** section.

vi) Click to confirm the change.

Email / Report Sample

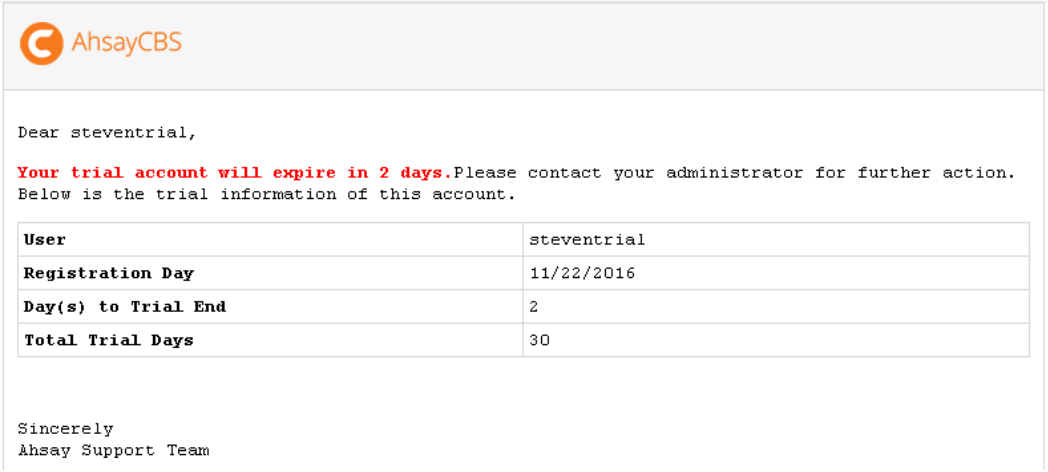
Email sample:



Backup Quota Reminder / Alert	
What is this email about?	**When will you receive it?**
A reminder to alert backup users about the backup quota has exceeded the set percentage. User can configure the percentage where the reminder/alert email is triggered when it is reached. By default, this percentage is preset as 80% when this feature is enabled.	The backup quota reminder / alert email is generated and sent to backup user at 6:00am daily.
What action should you take?	
The backup quota is going to exceed its storage quota. Contact your backup service provider to increase the capacity. Alternatively, consider cleaning up the existing backup sets that you are no longer using, or reviewing the retention policy.	
Email / Report Sample	
Email example:  	

Trial User Reminder / Alert	
What is this email about?	**When will you receive it?**
A reminder to alert trial backup users their account is about to expire in the set number of days. Be default, the preset value of this setting is 7 when this feature is enabled.	The trial user reminder / alert email is generated and sent to backup user at 6:00am daily.
What action should you take?	
In order to continue using your account for backup and restore, contact your backup service provider to subscribe to the paid backup service.	
Email / Report Sample	

Email sample:



AhsayCBS

Dear steventrial,

Your trial account will expire in 2 days. Please contact your administrator for further action.
Below is the trial information of this account.

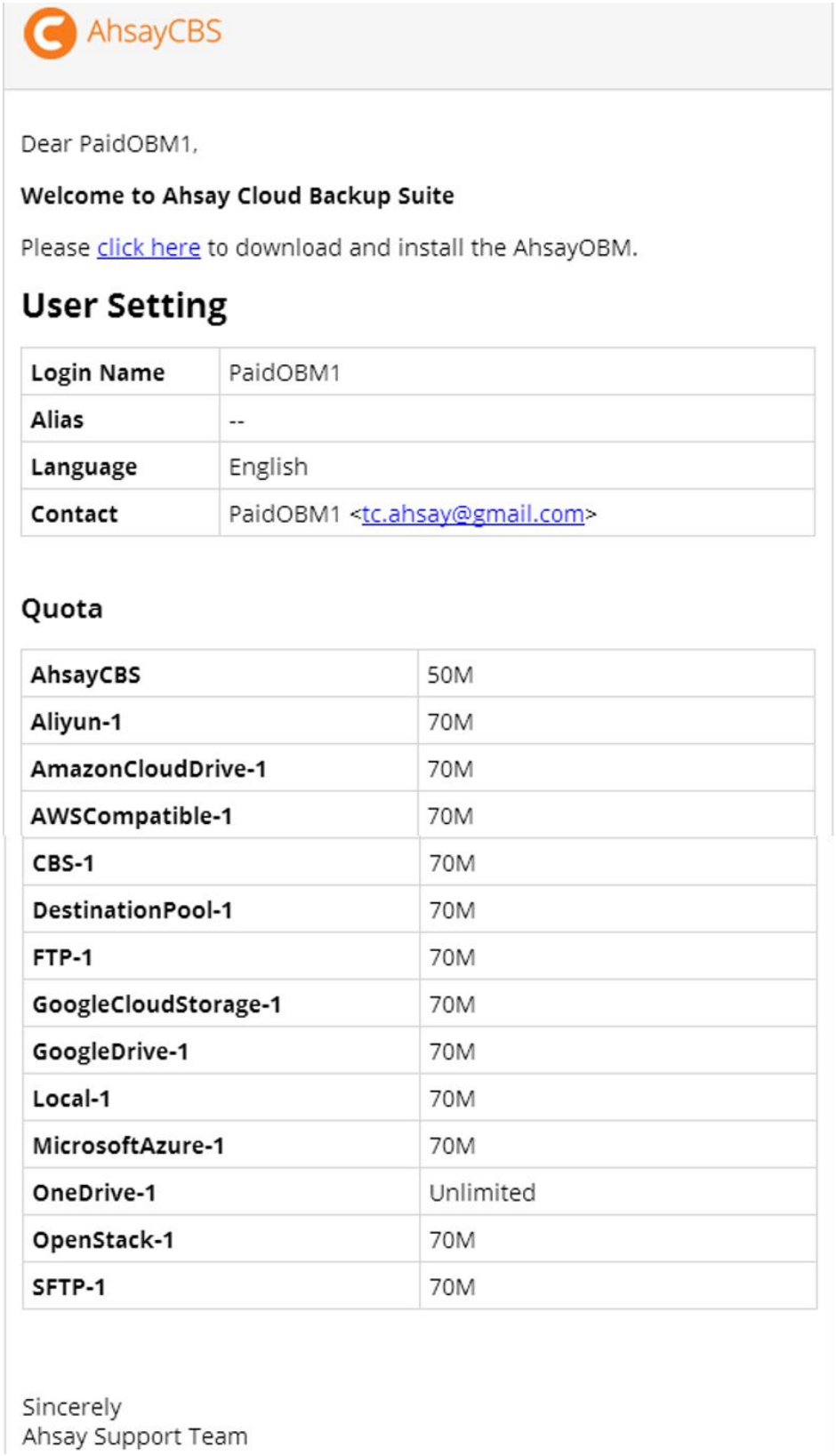
User	steventrial
Registration Day	11/22/2016
Day(s) to Trial End	2
Total Trial Days	30

Sincerely
Ahsay Support Team

Welcome Email	
What is this email about?	**When will you receive it?**
A welcome message generated by the AhsayCBS to confirm a backup account has been created	Shortly after a Backup User account has been created
What action should you take?	
You can click on the link in the email to download the client backup application if you have not done so.	

Email / Report Sample

Email sample:



AhsayCBS

Dear PaidOBM1,

Welcome to Ahsay Cloud Backup Suite

Please click here to download and install the AhsayOBM.

User Setting

Login Name	PaidOBM1
Alias	--
Language	English
Contact	PaidOBM1 <tc.ahsay@gmail.com>

Quota

AhsayCBS	50M
Aliyun-1	70M
AmazonCloudDrive-1	70M
AWSCompatible-1	70M
CBS-1	70M
DestinationPool-1	70M
FTP-1	70M
GoogleCloudStorage-1	70M
GoogleDrive-1	70M
Local-1	70M
MicrosoftAzure-1	70M
OneDrive-1	Unlimited
OpenStack-1	70M
SFTP-1	70M

Sincerely
Ahsay Support Team

Daily User Report
(Appears as: Email me consolidated email report only at this time daily)

What is this email about?	When will you receive it?
A consolidated report in PDF format, showing the following categories of information: • **PROBLEMS** – errors for System / Backup / Restore / Replication / Redirection • **ISSUES** – potential issues that may cause problems on System/Security, Users or Backup Sets • **ACTIVITIES** – all Backup Jobs / Restore Jobs / Setting Changes performed • **STATISTICS –** statistics on User Account / Data Transfer / Disk Storage Usage	The daily user report is generated and sent to backup user at the time defined by the system administrator in this menu

What action should you take?

Click on the attachment in the email to get re-directed to the consolidated report page. The report is in interactive format which allows you click on different tabs/sections for the corresponding report data. Refer to Appendix I for further explanation of the daily user report.

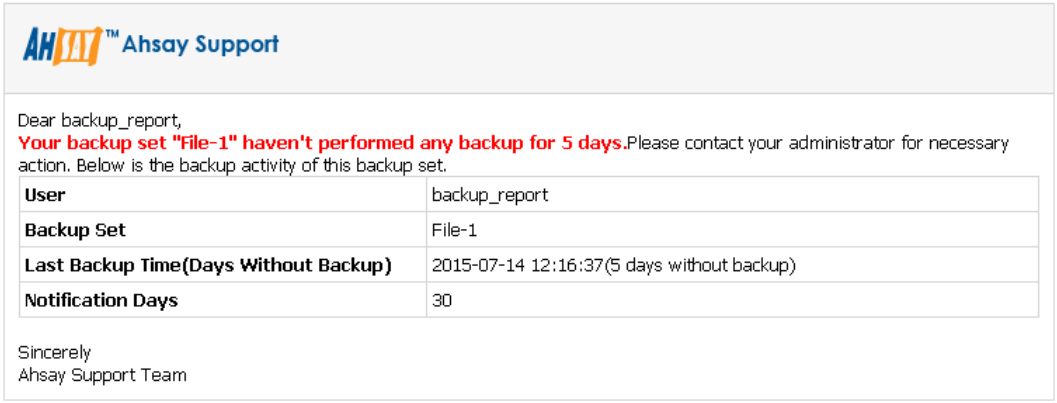
Email / Report Sample

Email sample:

Report sample:

Inactive Backup Report **(Appears as: Email me inactive backup report when my backup set hasn't run for this number of days)**	
What is this email about?	**When will you receive it?**
A report showing all backup sets under this backup user account that have not been run in the set number of day.	Inactive Backup Report is generated and sent to backup user every 15 mins (every :00, :15, :30 and :45 of an hour)
What action should you take?	
You may have to check for the causes for the backup sets, especially scheduled backup sets that are not running. That could be caused by, for example, incorrect login credentials of the client backup application, Internet connection problem, etc.	
Email / Report Sample	

Email sample:



AhsayTM Ahsay Support

Dear backup_report,
Your backup set "File-1" haven't performed any backup for 5 days. Please contact your administrator for necessary action. Below is the backup activity of this backup set.

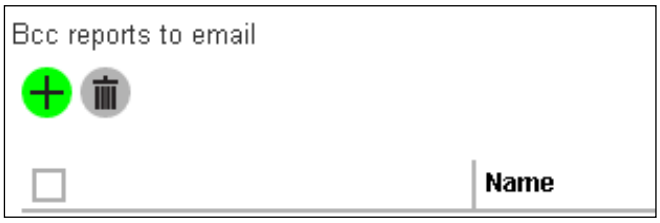
User	backup_report
Backup Set	File-1
Last Backup Time(Days Without Backup)	2015-07-14 12:16:37(5 days without backup)
Notification Days	30

Sincerely
Ahsay Support Team

Bcc reports to email

You can add email recipients in this section so that they will receive a blind carbon copy (bcc) of the email reports as well.

1. Click the button under the **Bcc reports to email** section.



2. Enter the name of the recipient, email address and other details if necessary.

- If you wish to encrypt the email, check the Encrypt Email box. You will be re-directed to another page to upload the **Digital Certificate**. Click the Choose File button to upload the digital certificate, then click the tick button at the bottom of the page to confirm.

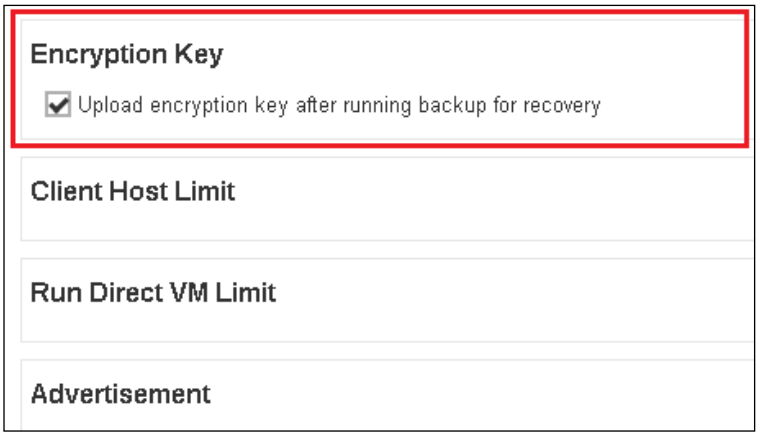
3. Click when you are done with the settings.

4. Click to confirm the setting.

➢ Encryption Key

Once you enabled the encryption recovery option. The encryption key file will be uploaded to the Backup Server. In case user has forgotten the encryption key, you can still contact us to recover the key.

Turn on the switch on the right and then make sure the check box **Uploaded encryption key after running backup for recovery** is checked for this feature to work.

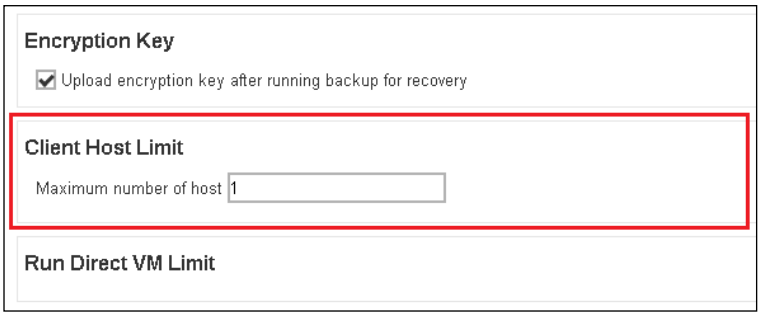


From AhsayCBS v7.9.2.0 onwards, it is possible to submit an encryption key recovery request via the AhsayCBS web console. Refer to the Recovering Encryption Key via AhsayCBS Web Console section for detailed instructions.

➢ Client Host Limit

Since version 7.7, administrator is able to set the maximum number of host machine for a backup users account.

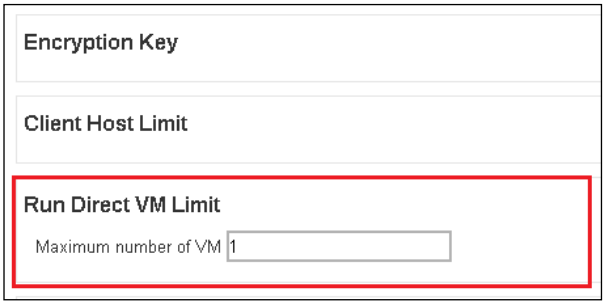
Turn on the switch on the right and then enter the **Maximum number of host** as shown below.



➢ Run Direct VM Limit

Since version 7.9, administrator is able to set the maximum number of VM for Run Direct restore.

Turn on the switch on the right and then enter the **Run Direct VM Limit** as shown below.



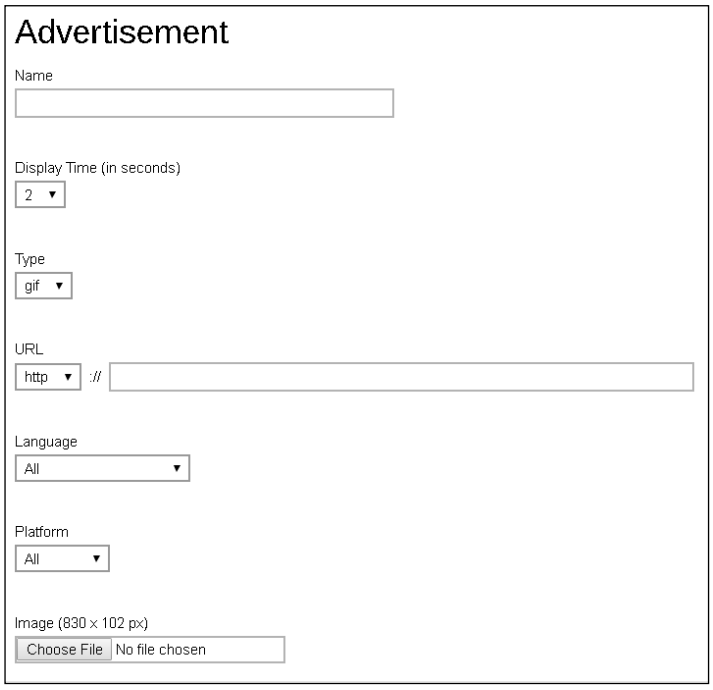
➢ Advertisement

Since version 7.7, administrator is able to customize the advertising banner on the AhsayOBM/AhsayACB interface. CBS supports both GIF and SWF formats at the size of (830 x 102 px).

1. Turn on the switch on the right to turn on this feature.

2. Press to add the advertisement.

3. Enter details in the following fields below.



- **Name** – name of the advertisement banner.
- **Display Time (in seconds)** – period of time for the advertisement to be shown before it rotates to the next one.
- **Type** – format of the banner, whether it is in **gif** or **swf** format.
- **URL** - the click through URL of the gif type banner. For flash banner, the click through URL should be coded inside the flash banner.
- **Language** – select in which language setting in AhsayOBM/AhsayACB will the banner be shown. If **All** is selected, the banner shows no matter what language is selected in the AhsayOBM/AhsayACB.
- **Platform** – select on which platform (Windows, Mac & Linux) AhsayOBM/AhsayACB is used for the banner to show. If **All** is selected, the banner shows no matter what platform the AhsayOBM/AhsayACB is running on.
- **Image (830 x 102 px)** – click **Choose File** to upload the banner.

4. Click when you are done with the settings.

5. Click to confirm the setting.

Backup Set Settings

This section allows administrator to set up backup exclusion and backup destination visible to users. It has 3 sub-sections.

➢ Exclude Backup File

This menu allows you to set filter to exclude files from performing backup job. This feature is disabled by default.

- **Files on mapped drive** – files from mapped drive will be excluded from backup (applicable only to UNC path on Windows platform). Typical UNC path is in the format of \\drive or IP address\folder name (e.g. \\10.1.0.10\My Documents).
- **Files larger than** – files larger than the defined size will be excluded from backup
- **File older than** – files created the set period of time ago or before a specific set date will be excluded from backup

➢ Destinations Visible to Users

There are two kinds of destinations backup users can choose from when creating a backup set, they are the Predefined Destination and Standard Destination. Only the destinations selected in this menu will be available for backup users to choose from when they are creating a backup set. This feature is disabled by default. You can enable the feature by turning on the switch to the right.

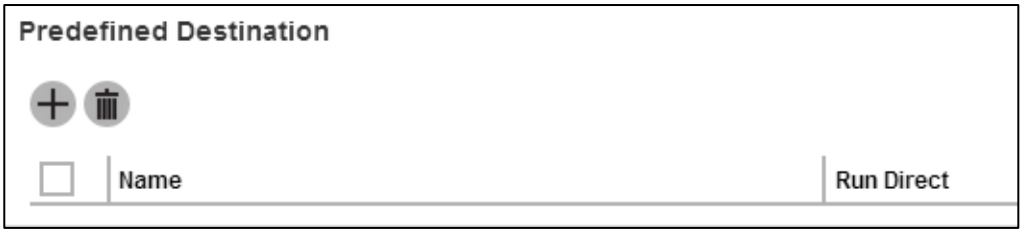
Below is a brief explanation on the differences between the Predefined Destination and Standard Destination.

Predefined Destination vs Standard Destination

- **Predefined Destination** - The predefined destination can be a single storage destination on the local drive where CBS is installed, mapped drive, cloud storage or FTP server, or a destination pool with a mix of storage options mentioned above. Before you can select a predefined destination in this menu, it must first be configured under the **System Settings** > **Backup** > **Predefined Destinations**. Refer to Predefined Destinations Tab and Backup User Settings Tab for details on configuration.
- **Standard Destination** - Except for the AhsayCBS storage option, all other storage options under the Standard Destination belong to the backup users, whether it could be a single storage destination on the mapped drive, cloud storage or FTP server, or a destination pool with a mix of storage options mentioned above.

To configure the Predefined Destination

1. Turn on the switch on the right under the **Destinations Visible to Users** section.
2. Click on under the **Predefined Destination** section.



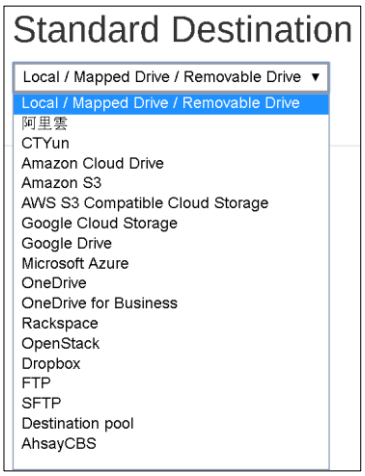
3. Select the desired destination option, which has been defined in the **System Settings** > **Backup** > **Predefined Destinations** menu, by checking the box on the desired destination item.

4. Click to confirm adding the predefined destination.
5. If you have multiple predefined destinations to add, repeat steps 3 -4 until all desired destinations have been selected.
6. Click to confirm.

To configure the Standard Destination

1. Turn on the switch on the right under the **Destinations Visible to Users** section.
2. Click on under the **Standard Destination** section.

3. Select the desired storage option from the drop-down menu as shown below.

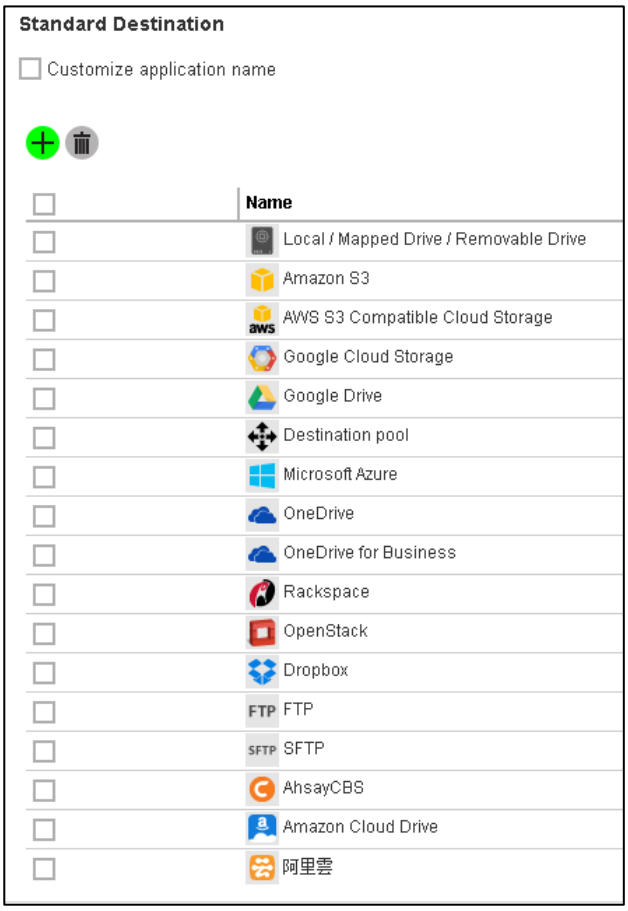


4. Click to add the selected standard destination storage.

5. If you have multiple destination storages to add, repeat steps 3 – 4 until all desired storages have been selected.

6. Click to confirm.

7. You will see the newly added destination shown on the list as shown.

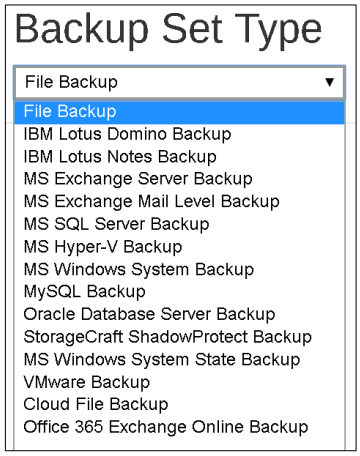


➢ Backup Set Types Visible to Users

The AhsayCBS supports a wide range of backup set types for backup and restore. This menu allows the administrator to select the backup set types to be displayed for backup users to choose from when they are creating a backup set on AhsayCBS, AhsayOBM or AhsayACB. This feature is disabled by default.

1. Turn on the switch on the right under the **Backup Set Types Visible to Users** section.
2. Click on .

3. Select the **Backup Set Type** you wish to add from the drop-down menu as shown below.



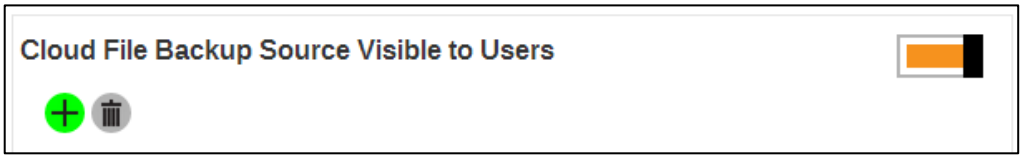
4. Click to add the selected backup set type.
5. If you have multiple backup set types to add, repeat steps 3 - 4 until all options have been selected.
6. Click to confirm.

➢ Cloud File Backup Source Visible to Users

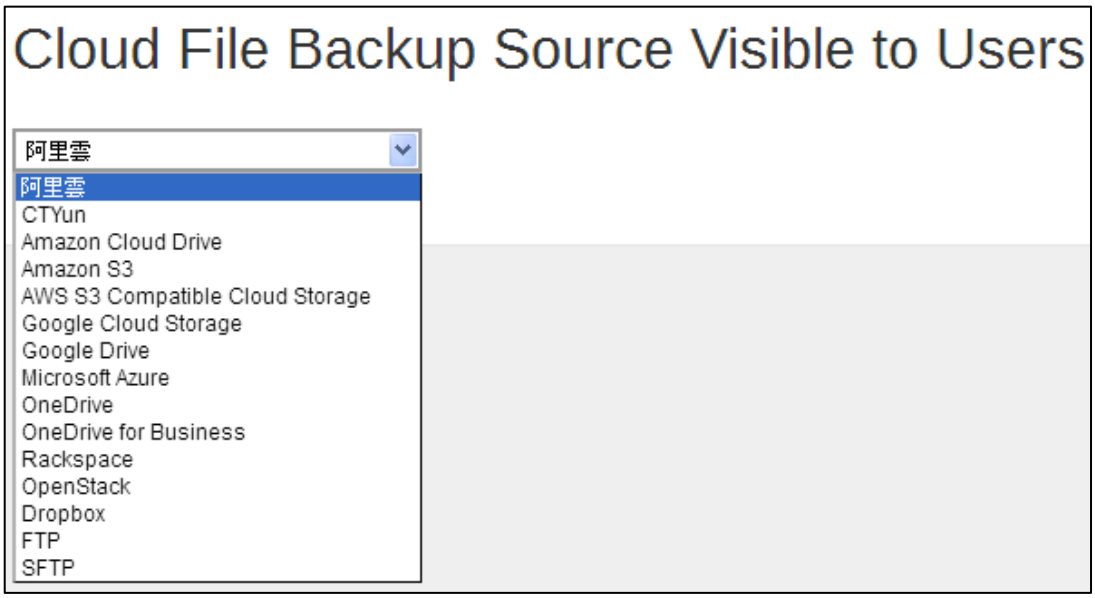
This menu allows the administrator to select specific cloud file backup source(s) to be visible to backup users when they are creating a Cloud File Backup Set. By default, this feature is on with all cloud file backup sources pre-selected.

1. Turn on the switch on the right under the **Cloud File Backup Source Visible to Users** section.

2. Click on .



3. Select the **Cloud File Backup Source Visible to Users** you wish to add from the dropdown menu as shown below.



4. Click to add the selected cloud file backup source.

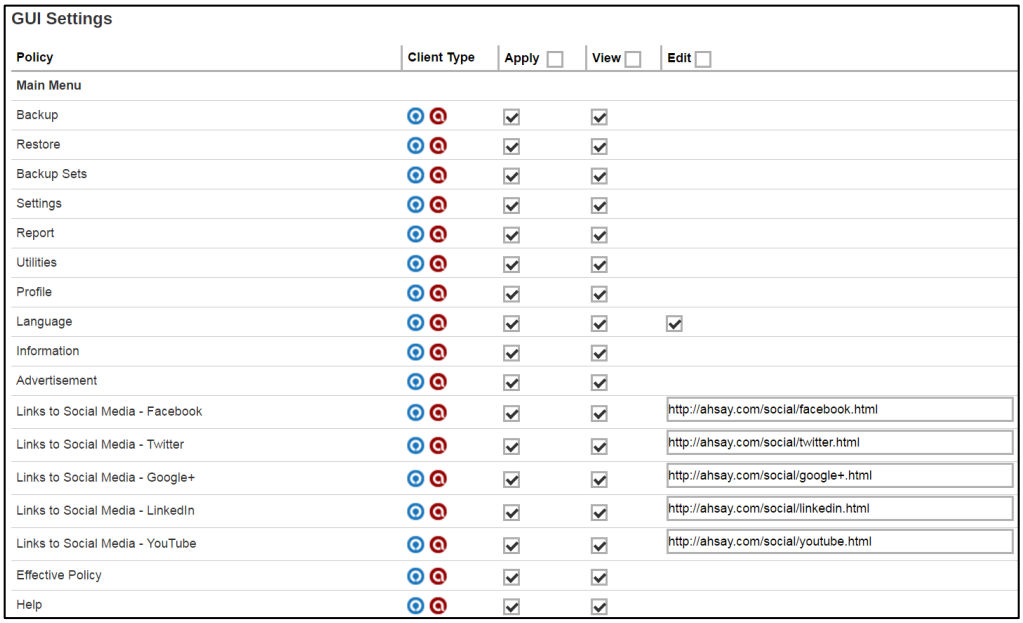
5. If you have multiple cloud file backup source to add, repeat step 3 - 4 until all options have been added.

6. Click to confirm.

GUI Settings

In this menu, administrator can configure the GUI elements to be shown on the client backup agent (AhsayOBM or AhsayACB) interface for backup users. The **View** checkbox allows administrator to decide whether to display the GUI item, and for some items, the **Edit** checkbox is available to enable backup users for changing or accessing the GUI item(s).

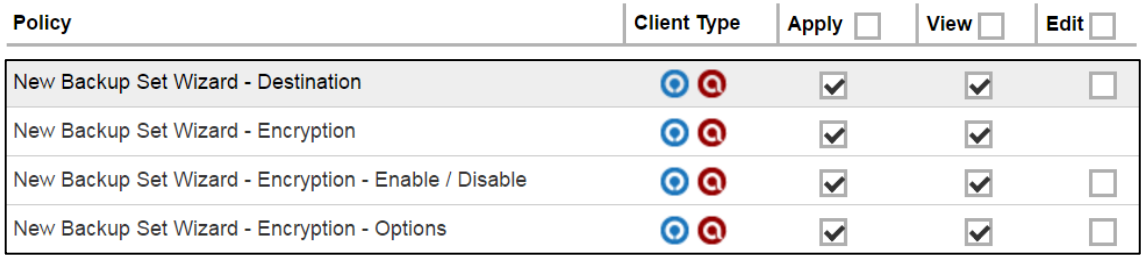
Policy	The GUI element on AhsayOBM/AhsayACB
Client Type	The Client Backup Type (AhsayOBM or AhsayACB)
Apply	Check this box if you wish to configure the "**View**" and "**Edit**" option for the GUI item. If this box is not checked, the GUI item will be shown on AhsayOBM/AhsayACB by default.
View	Enable or disable backup user to view the item
Edit	Enable or disable backup user to edit the item



Since AhsayCBS v7.11.0.0, we have added additional items under the GUI settings to give you greater flexibility for customizing the GUI elements on the client backup agent (AhsayOBM & AhsayACB). Refer to the information below for further details.

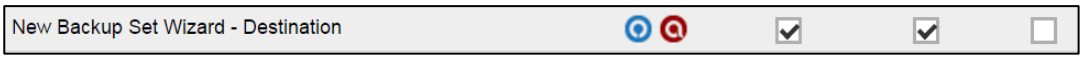
➢ New Backup Set Wizard

There are four setting items under this new setting category to enable or disable the Destination and Encryption Key settings when creating a new backup set using the client backup agent.



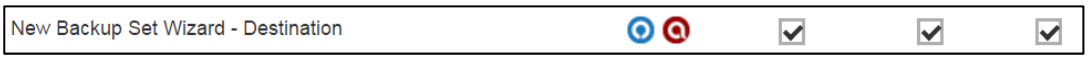
New Backup Set Wizard – Destination

You can set to restrict backup users from using the default destination where they can only view the default destination but cannot change it **OR** to allow them to choose the desired backup destination on their own.



To restrict the backup destination WITHOUT letting backup user to change it, check the **View** box and left the **Edit** box unchecked. With this configuration, backup users can only view the backup destination that is predefined under the **Users, Group & Policies > Policy Group > Default Values > Destination** page, but cannot alter the backup destination when creating a new backup set using the client backup agent.

Note: If there is no destination defined in the **Default Values** menu as mentioned above, you will not be allowed to configure this setting.



By checking both the **View** and **Edit** checkboxes, backup users can choose their desired backup destination from the choices defined under the **Users, Group & Policies > Policy Group > Backup Set Settings > Standard Destination.**

New Backup Set Wizard – Encryption

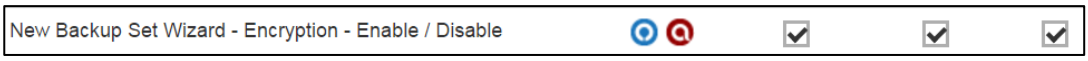
This setting is used in conjunction with the **New Backup Set Wizard – Enable/Disable** and **New Backup Set Wizard – Options** settings.

When the **View** checkbox is checked for this option, the encryption key setting page will be shown when creating a new backup set with a client backup agent, otherwise, the relevant page will be skipped.

New Backup Set Wizard – Enable / Disable

In order for this setting to work, the View option for **New Backup Set Wizard – Encryption** setting must be turned on.

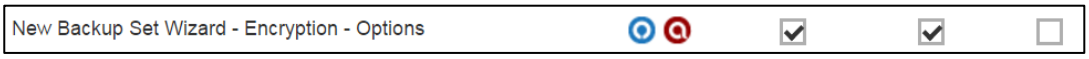
When you set the View option on and the Edit option off for this setting, the Encryption Key feature will be turned on by default.



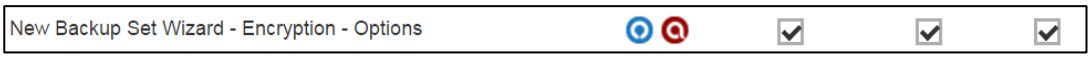
When you set both the **View** and **Edit** options on, backup users will be able to enable or disable this feature on their own.

- **New Backup Set Wizard – Options**

  This setting allows backup users to choose the Encryption Type among **Default**, **User Password** or **Custom**.



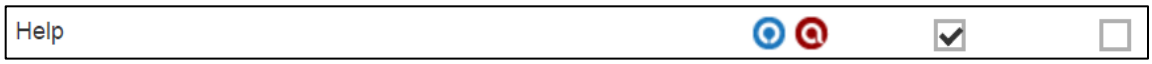
When you set the View option on and the Edit option off for this setting, the encryption type will not be configurable and will use the default value defined in **Users, Group & Policies > Policy Group > Default Values > Others > Encryption.**



When you set both the **View** and **Edit** options on, backup users will be able to choose their desired encryption type.

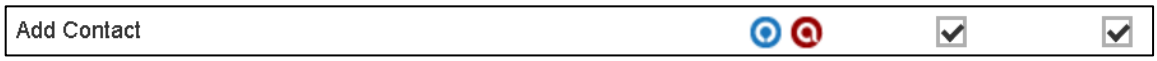
➢ **Help Page**

This option allows you to configure whether to show the Help button on the UI of the client backup agent. The Help button takes you to a set of online help instructions that correspond to the relevant page in the client backup agent.



➢ **Add Contact**

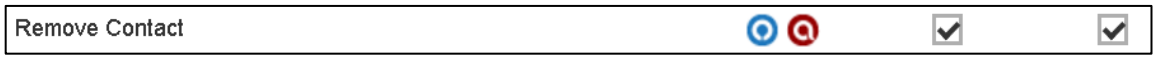
This option allows backup users to add Contact information, such as name, email, address, etc. under the **Profile > Contacts** page in the client backup agent.



By checking the View checkbox for this option, backup users can configure contact information on their own.

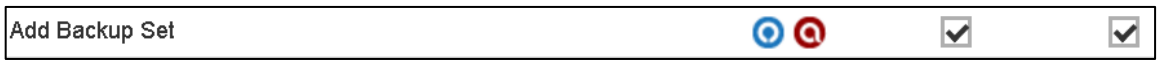
➢ **Remove Contact**

This option allows backup users to remove contact information under the **Profile > Contacts** page in the client backup agent.



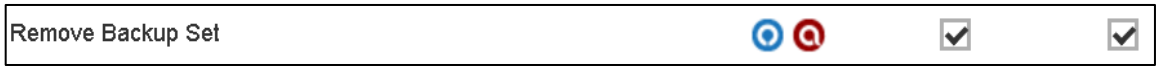
By checking the View checkbox for this option, backup users can remove contact information on their own in the client backup agent.

➢ **Add Backup Set**



By enabling the View checkbox of this option, backup users are able to add backup set using the client backup agent.

➢ Remove Backup Set

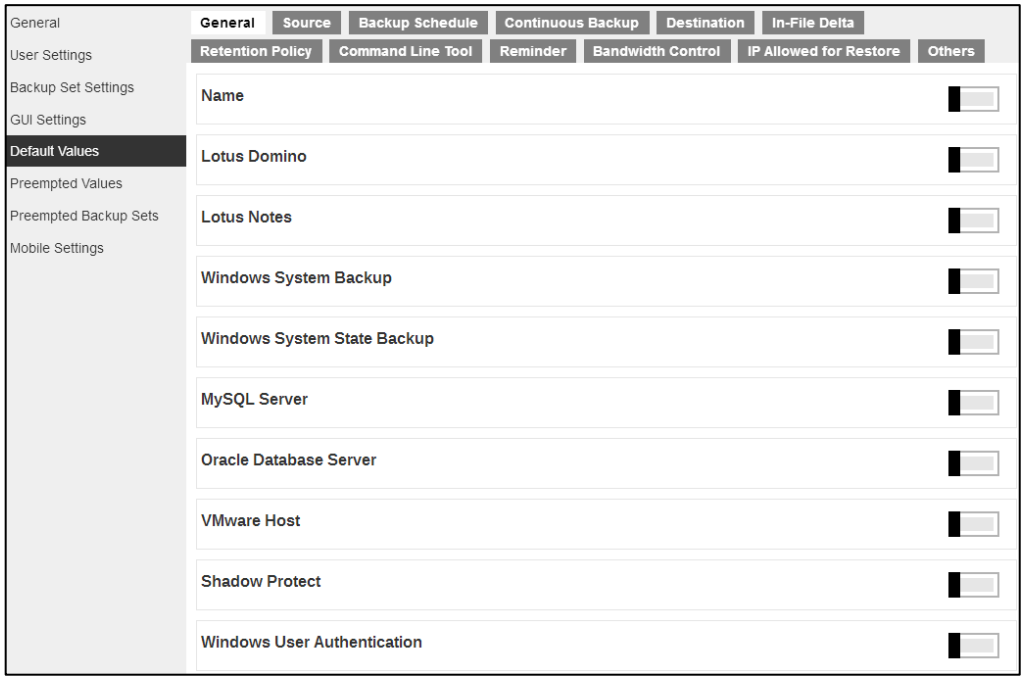


By enabling the View checkbox of this option, backup users are able to remove backup set using the client backup agent.

Default Values

This section allows administrator to define the default values for numerous setting items. The default values set under this setting menu will be applied to the backup sets directly. However, users can still override the default values during new backup set creation. As opposed to Preempted Values, which will be introduced later in this chapter, is a set of predefined values by the system administrator where backup users have no right to override the settings.

All setting items under the Default Values tab are disabled by default. Click the switch on the right of each setting item and then follow the steps below for configuration.



➢ General

This section defines the default values of some general configuration items. The following table explains each setting item under the **General** tab, with a brief description of what the setting is about and all the configurable items.

Name	
What is this setting about?	Defines the default backup set name when backup users create a backup set. Multiple settings can be created in this menu if you wish to define different default backup set names for different backup modules.

What are the configurable items?	➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Backup Set Name** – default backup set name to be displayed when a backup set is created for the selected module(s).
Lotus Domino	
What is this setting about?	Defines the path to **notes.ini**. Please exercise extra caution when changing this setting because an accidental or incorrect change of this path may cause unpredictable impact on running the Lotus Domino. Refer to the URL below for further information on this setting. http://www.ibm.com/support/knowledgecenter/SSKTMJ_9.0.1/admin/conf_editingthenotesinifile_c.html
What are the configurable items?	➢ **Name** – name of this setting item ➢ **Path to notes.ini** – path name of the **Path to notes.ini**

Lotus Notes	
What is this setting about?	Defines the path to **notes.ini** . Please exercise extra caution when changing this setting because an accidental or incorrect change of this path may cause unpredictable impact on running the Lotus Notes. Refer to the URL below for further information on this setting. http://www.ibm.com/support/knowledgecenter/SSKTMJ_9.0.1/admin/conf_editingthenotesinifile_c.html
What are the configurable items?	➢ **Name** – name of this setting item ➢ **Path to notes.ini** – path name of the **Path to notes.ini**

Windows System Backup	
What is this setting about?	Defines the default location where you wish to store the system backup for MS Windows System Backup module
What are the configurable items?	➢ **Name** – name of this setting item ➢ **Specify the location where you want to store the system backup** – location path where you wish the system backup be stored

Windows System State Backup

What is this setting about?	Defines the default location where you wish to store the system backup for MS Windows System State Backup module.
What are the configurable items?	➢ **Name** – name of this setting item ➢ **Specify the location where you want to store the system backup** – location path where you wish the system state backup be stored
MySQL Server	
What is this setting about?	Defines the default Login ID, Host name, Port and Path to mysqldump for MySQL server backup module
What are the configurable items?	➢ **Name** – name of this setting item ➢ **Login ID –** login ID for accessing the MySQL server ➢ **Host –** host name of the MySQL server ➢ **Port –** port number ➢ **Path to mysqldump –** path name to the mysqldump utility

Oracle Database Server	
What is this setting about?	Defines the default Login ID, Host name, Port and SID for Oracle Database Server module
What are the configurable items?	➢ **Name** – name of this setting item ➢ **Login ID –** login ID for accessing the Oracle Database server ➢ **Host –** host name of the Oracle server ➢ **Port –** port number ➢ **SID –** the unique identifier to the database instance

VMware Host	
What is this setting about?	Defines the default VMware version, host name, port number and SSH port for VMware backup module
What are the configurable items?	➢ **Name** – name of this setting item ➢ **Version –** VMware version ➢ **Host –** host name of the VMware host

	➢ **Port –** port number ➢ **SSH Port –** SSH port number

Shadow Protect	
What is this setting about?	Defines the default path to install the Shadow Protect and whether to encrypt the image file in temporary directory.
What are the configurable items?	➢ **Name** – name of this setting item ➢ **Path to StorageCraft ShadowProtect** – the path where you installed the ShadowProtect ➢ **Encrypt the image file in temporary directory** – to enable or disable encryption for image file in the temporary directory where the ShadowProtect image is stored.

Windows User Authentication	
What is this setting about?	Defines the default domain name/host name and user name for backup users to enter the Windows User Authentication details. Multiple settings can be created in this menu if you wish to define different default domain name/host name and user name for different modules.
What are the configurable items?	➢ **Name** – name of this setting item ➢ **Applied Modules** – modules you wish to apply this default setting to ➢ **Domain Name (e.g. ahsay.com) / Host Name** – domain name or host name of the Windows login ➢ **User name** – user name to log in to the backup user's Windows for backup

➢ Source

This section defines the default backup source values. The following table explains each setting item under the **Source** tab, with a brief description of what the setting is about and all the configurable items.

Common Folders for Windows	
What is this setting about?	Defines the default common files and folders to be selected when user are creating a backup set for File Backup.

What are the configurable items?	➢ **Name** – name of the setting item ➢ **Common Files and Folders** – a list of common files or folders to choose from as default backup source when creating a file backup set.

Filter	
What is this setting about?	Defines the default filters which used to include/exclude files in the backup source from performing backup. This filter applies only to File Backup on Windows platform. Creating multiple filter settings is possible.
What are the configurable items?	➢ **Name** – name of the filter setting ➢ **Matching pattern -** defines the pattern of the file selection, e.g., *.doc, *.png. ➢ **For each of the matched files/folders under top directory** – define to include or exclude all the files/folder matching the filtering criteria under the top directory ➢ **Exclusion / Inclusion** – to include (if you have chosen to exclude the matched files) or exclude (if you have chosen to include the matched files) those unmatched files/folder in the backup ➢ **Match file/folder names by** – you can set the following filtering rules: **[Simple comparison starts with]** Include/Exclude all files/directories with name starting with a certain pattern. ***Example:*** *You can use B* to match all file with name starting with a B character.* **[Simple comparison ends with]** Include / Exclude all files / directories with name ending with a certain pattern. ***Example:*** *You can use *.doc to match all files with name ending with .doc (all Word Documents)* **[Simple comparison contain]** Include/Exclude all files/directories with name containing a certain pattern. ***Example:*** *You can use *B* to match all files with name containing with a B character.* **[Regular Expression (UNIX-style)]** Include/Exclude all files/directories with name matching a regular expression. ***Notes:*** ➢ The pattern of a backup filter is case sensitive.

<table>
<tr><td></td><td>

If multiple patterns are required, please add the pattern one by one e.g.: *.doc and then *.xls

How to Apply This Filter – you can choose to apply this filter on “All hard disk drivers” or a selected folder of your choice.

Apply to - apply the filter to the File and/or Folder level

</td></tr>
<tr><td>Use Cases</td><td>
<u>Example 1</u>
If you want to backup only Word, Excel and PowerPoint documents in your document directory (e.g. C:\My Documents), you should setup your backup filter as follows.

Matching pattern = *.doc, *.xls, *.ppt
For each of the matched files/folders under top directory = Include them
Exclusion = Check
Match file/folder names by = Simple comparison end with
How to Apply This Filter = This folder only C:\My Documents
Apply to = File

<u>Example 2</u>
If you want to backup all files, excluding all *.exe, *.dll and *.tmp, in C:\Application, you should setup your backup filter as follows.

Matching pattern = *.exe, *.dll, *.tmp
For each of the matched files/folders under top directory = Exclude them
Inclusion = Check
Match file/folder names by = Simple comparison end with
How to Apply This Filter = This folder only C:\Applicaitons
Apply to = File

<u>Example 3</u>
If you have already chosen files (all under C:\) from the backup source setting but you want to exclude all images (e.g. *.jpg and *.gif) from your selection, you should setup your backup filter as follows.

Matching pattern = *.jpg, *.gif
For each of the matched files/folders under top directory = Exclude them
Inclusion = uncheck
Match file/folder names by = Simple comparison end with
How to Apply This Filter = This folder only C:\
Apply to = File

Please note that the Inclusion setting should not be checked because you have already chosen the desired files to back up and do not want to include all other files (NOT *.jpg, *.gif) under C:\ into the backup set.

<u>Example 4</u>
If you want to include everything, except the “log" directory, under
</td></tr>
</table>

	C:\Applications into a backup set, you should setup your backup filter as follows. **Matching pattern** = ^log$ **For each of the matched files/folders under top directory** = Exclude them **Inclusion** = check **Match file/folder names by** = Regular Expression (UNIX-style) **How to Apply This Filter** = C:\Applications **Apply to** = Folder **Example 5** If you want to include all directories named “log" from the backup set files with file name starting with “B" and ending with “*.doc" under C:\My Documents into the backup set, you can use a regular expression of “^B.*\.doc$" to do your selection. The filter backup can then be setup as follows. **Matching pattern** = ^B.*\.doc$ **For each of the matched files/folders under top directory** = Include them **Exclusion** = check **Match file/folder names by** = Regular Expression (UNIX-style) **How to Apply This Filter** = C:\My Documents **Apply to** = File

Advanced	
What is this setting about?	Defines the default advanced settings, including the platform of the user’s machine, the backup module, selected or deselected source for backup.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Platform –** select the platform to apply this advanced filter ➢ **Applied Modules** – modules you wish to apply this default setting to ➢ **Other Selected Source** – define the path of the source, e.g. Windows: C:\My folder; Linux: /home/my folder, to include in the backup set ➢ **Deselected Source** - define the path of the source, e.g. Windows: C:\My folder; Linux: /home/my folder, to exclude in the backup set

➢ Backup Schedule

Setting up the backup schedule allows backup sets to run automatically at the specified time. This section allows administrator to define the default backup schedule. The following table explains each setting item under the **Backup Schedule** tab, with a brief description of what the setting is about and all the configurable items.

Schedule	
What is this setting about?	Defines the default backup schedule when backup users create a backup set. Multiple settings can be created in this menu if you wish to define different default backup schedule for different backup modules. Within a backup schedule setting, multiple schedules can be added.
What are the configurable items?	**Backup Schedule** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Run scheduled backup for this backup set –** to enable or disable the scheduled backup settings you set in this menu **Manage Schedule** ➢ **Name** – name of the scheduler ➢ **Type** – frequency of running the scheduled backup **Daily** – to run the scheduled backup everyday **Weekly** – to run the scheduled backup on the selected days of a week **Monthly** – to run the scheduled backup on a specific day in a month, or on a specific day in a specific week. **Custom** – to run the scheduled backup on a specific day of your selection ➢ **Start backup at** – specify a specific time to run the scheduled backup based on the frequency set in the Type menu above. ➢ **Stop** – set the scheduled backup to stop either - Full backup is completed regardless of how much time it takes **OR** - After the backup has started for the set time (1-24 hr) regardless if the backup is done ➢ **Run Retention Policy after backup** – enable this feature if you wish the modified or deleted data after backup remains in the backup server for the set number of retention day

➢ Continuous Backup

When the Continuous Backup feature is enabled, a backup job will be triggered whenever a change is made in the backup source. This section allows administrator to define the default continuous backup settings. The following table explains each setting item under the **Continuous Backup** tab, with a brief description of the available settings and all the configurable items. **Continuous Backup is only available on Windows platform.**

IMPORTANT

When setting up the Continuous Backup feature for a backup set, you must run a manual or scheduled backup job first so that the initial files are uploaded your designated backup destination.

Continuous Backup	
What is this setting about?	Defines whether to enable this feature, whether to exclude system files, frequency of running backup when changes are detected, configure the maximum file size allowed for backup and configure filters to exclude files from backup.
What are the configurable items?	**Continuous Backup** ➢ **Name** – name of the setting item ➢ **Backup whenever a change is made** – enable or disable the continuous backup feature. ➢ **Exclude system files** – enable this feature if you do not want to back up system files. Refer to Appendix J for a full list of system files excluded from the backup set. ➢ **How often should the backup run** – set the frequency of running backup when changes are detected. ➢ **Only apply to files smaller than** – file size that is larger than the set value will not be backed up. ➢ **Run CDP on computers named** – define the name of the computer on which continuous backup will be run. **Exclude Filter** ➢ **Name** - name of the filter setting item ➢ **Match file/folder names by** – you can set the following filtering rules: **[Simple comparison starts with]** Include/Exclude all files/directories with name starting with a certain pattern. ***Example:***

	You can use B to match all file with name starting with a B character.* **[Simple comparison ends with]** Include / Exclude all files / directories with name ending with a certain pattern. ***Example:*** *You can use *.doc to match all files with name ending with .doc (all Word Documents)* **[Simple comparison contain]** Include/Exclude all files/directories with name containing a certain pattern. ***Example:*** *You can use *B* to match all files with name containing with a B character.* **[Regular Expression (UNIX-style)]** Include/Exclude all files/directories with name matching a regular expression. ***Notes:*** - The pattern of a backup filter is case sensitive. - If multiple patterns are required, please add the pattern one by one e.g.: *.doc and then *.xls ➢ **Matching pattern** - defines the pattern of the file selection, e.g., *.doc, *.png. ➢ **Apply This Filter to all files/folders in** – you can choose to apply this filter on "**All selected sources**" or a selected folder of your choice ➢ **Apply to** - apply the filter to the File and/or Folder level
Use Cases	**Example 1** If you want to back up all files, except all Word, Excel and PowerPoint documents, in your document directory (e.g. C:\My Documents), you should setup your backup filter as follows. **Match file/folder names by** = Simple comparison end with **Matching pattern** = *.doc, *.xls, *.ppt **Apply this filter to all files/folders in** = This folder only C:\My Documents **Apply to** = File **Example 2** If you want to include everything, except the "log" directory, under C:\Applications into a backup set, you should setup your backup filter as follows. **Match file/folder names by** = Regular Expression (UNIX-style) **Matching pattern** = ^log$

	Apply this filter to all files/folders in = C:\Applications **Apply to** = Folder **Example 3** If you want to exclude all directories named “log" from the backup set files with file name starting with “B" and ending with “*.doc" under C:\My Documents into the backup set, you can use a regular expression of “^B.*\.doc$" to do your selection. The filter backup can then be setup as follows. **Match file/folder names by** = Regular Expression (UNIX-style) **Matching pattern** = ^B.*\.doc$ **Apply this filter to all files/folders in** = C:\My Documents **Apply to** = File

➢ Destination

This section allows administrator to define the default backup destination for backup set. The following table explains each setting item under the **Destination** tab, with a brief description of what the setting is about and all the configurable items.

Destination	
What is this setting about?	Defines the default backup destination when backup users create a backup set. Multiple settings can be created in this menu if you wish to define different default destinations for different backup modules.
What are the configurable items?	**Destination** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Backup Mode –** select the files transfer method during backup **Sequential –** backup files are sent to the backup destination one by one, one after another. **Concurrent –** multiple files are sent to the backup destination at the same time ➢ **Maximum concurrent backup destinations (only if you have selected Concurrent as the Backup Mode) –** select the maximum number of files allowed for uploading to the backup destination ➢ **Predefined Destination** – select the predefined destination you have configured in the Predefined Destinations Tab section.

➢ In-File Delta

In-file delta technology is an advanced data block matching algorithm with the intelligence to pick up changes (delta) of file content between two files.

Using this algorithm, daily backup of large files over low-speed internet connection is made possible because it requires only the changes of information since the last backup to be sent over (assuming that the full backup of the file has been saved on the backup server already).

This section allows administrator to define the default In-File Delta type for backup set. The following table explains each setting item under the **In-File Delta** tab, with a brief description of what the setting is about and all the configurable items.

In-File Delta	
What is this setting about?	Defines the default in-file delta setting for backup set. Multiple settings can be created in this menu if you wish to define different default in-file delta settings for different backup modules.
What kind of in-file delta type are there?	**Incremental In-file delta** Incremental Delta will facilitate ease of backup. The delta is generated by comparing with the last uploaded full or delta file. Delta generated with this method is smaller and uses the least bandwidth. However, for restoration, the full file and all deltas up to the required point-in-time are required to be restored and merged. **Differential In-file delta** Differential Delta will facilitate ease of restore. The delta is generated by comparing with the last uploaded full file only. Delta generated with this method will grow daily and uses more bandwidth. However, for restoration, the full file and a single delta is required to be restored and merged.
What are the configurable items?	**Destination** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Default Type –** type of backup method (Incremental or Differential) **Advanced settings** ➢ **In-File Delta block size** – defines the size of delta block used when detecting changes between last full or delta file and the file to be backed up. **In-file delta backup with small block size** - Produce a smaller delta file due to a more precise comparison - Require more processing power on the client machine - Comparison may take longer to complete - Require more Java memory

In-file delta backup with large block size:

- Produce a larger delta file due to a less precise comparison
- Require less processing power on the client machine
- Comparison will complete faster
- Require less Java memory

For most cases, the default setting **Auto** will select the optimal block size for each file (depending on the size of the file).

File size	Block size
Smaller than 2GB	4KB
2GB – 8GB	8KB
Larger than 8GB	16KB

- **Only apply In-File Delta to files larger than –** defines the minimum file size a file to apply the in-file delta setting. If the size of a file to be backed up is smaller than the set value, the in-file delta setting will not apply and the whole file will be uploaded to the backup server.

  It is not necessary to perform In-file delta backup on small files because backing up the whole file does not take long. Backing up the whole file instead reduces the time required to restore the file.

- **Upload full file when either of these conditions is met** – a backup of the full file will be perform if the following condition is met:
  - **Number of deltas is over** – when the number of delta file exceeds the set value
  - **Delta ratio (delta file size / full file size) is over** – this setting is to ensure that a full file backup is performed for file with significant changes, as it is preferable to upload a full file instead to reduce the time required to restore the file

- **Weekly variations for overriding default type** – override the default in-file delta setting in the **Default Type** field on selected day(s) of a week

- **Yearly variations for overriding default type and weekly variations** – override the default in-file delta setting in the **Default Type** field as well as the setting in the "**Weekly variations for overriding default type**" section on a selected day in a week based on either of the following selection
  - **Day of selected months in yearly variations -** select a specific day in a month. On this specified day in the month defined above will the in-file delta variation setting override the default value.

➢ Retention Policy

Retention policy defines the policies of persistent data management for meeting business data archival requirements. When a backup job is performed, for data that are modified or deleted on the client computer, their existing versions on the backup server (backup records) will be moved into retention area, while newly backed up files will be placed in the current data area.

Specifically, retention policy setting defines how long are the backup records kept in the retention area before they are deleted permanently from the backup server.

This section allows administrator to define the default Retention Policy for backup set. The following table explains each setting item under the **Retention Policy** tab, with a brief description of what the setting is about and all the configurable items.

<table>
<tr><th colspan="3">Retention Policy</th></tr>
<tr><td>What is this setting about?</td><td colspan="2">Defines the default retention policy for backup sets when they are created. Multiple settings can be created in this menu if you wish to define different default retention policy for different backup modules.</td></tr>
<tr><td>What are the configurable items?</td><td colspan="2">
Destination
➢ Name – name of the setting item
➢ Applied Modules – modules to apply this setting to
➢ How to retain the files in the backup set, which have been deleted in the backup source – choose between Simple and Advanced setting, which is explained in details below.
- Simple – enter a specific number of day or backup job number. The retained data will be removed from the backup destination permanently after the set number of day or set number of job is met.
- Advanced – manage advanced retention policies by applying advanced settings
<table>
<tr><td rowspan="2">Daily</td><td>The past number of days on which different versions of your files are retained</td></tr>
<tr><td>Set the number of day(s) on which the old version of data will be stored</td></tr>
<tr><td rowspan="4">Weekly</td><td>The days within a week on which different versions of your files are retained</td></tr>
<tr><td>Select the day(s) in a week (Monday – Sunday) on which the old version of data will be stored</td></tr>
<tr><td>The number of weeks to repeat the above selection</td></tr>
<tr><td>Enter the number of week(s) for the above setting to repeat</td></tr>
<tr><td>Monthly</td><td>The days within a month on which different versions of your files are retained</td></tr>
</table>
</td></tr>
</table>

			Select a day in a month on which the old version of data will be stored. You can either set: - An exact day (1-31) **or** - The (First/Second/Third/Forth/Last) of (Monday - Sunday)
			The number of months to repeat the above selection
			Enter the number of month(s) for the above setting to repeat
		Quarterly	**The day within a quarter on which different versions of your files are retained**
			Select a day within a quarter on which the old version of data will be stored. You can either set: - An exact day (1-31) **or** - The (First/Second/Third/Forth/Last) of (Monday - Sunday)
			Months of quarter
			Select the desired combination of months of quarter - (January, April, July, October) - (February, May, August, November) - (March, June, September, December)
			The number of quarters to repeat the above selection
			Enter the number of quarter(s) for the above setting to repeat
		Yearly	**The day within a year on which different versions of your files are retained**
			Select a day within a year on which the old version of data will be stored. You can set the day by using one of the following methods: - Select an exact day (1 – 31) in an exact month (January – December) - Select the (First/Second/Third/Forth/Last) of (Monday/Tuesday/Wednesday/Thursday/ Friday/Saturday/Sunday/Weekday/Weekend) in an exact month (January – December) - Select a day in a week (Monday – Sunday) in an exact week of a year (Week 1 - 53)
			The number of years to repeat the above selection
			Enter the number of year(s) for the above setting to repeat

		Custom	**A specific day on which different versions of your files are retained**
			Select a day on which the old version of data will be stored. You can set the day by using one of the following methods: - Select an exact day (1 – 31) in an exact month (January – December) - Select the (First/Second/Third/Forth/Last) of (Monday/Tuesday/Wednesday/Thursday/ Friday/Saturday/Sunday/Weekday/Weekend) in an exact month (January – December) - Select a day in a week (Monday – Sunday) in an exact week of a year (Week 1 - 53)
			Year
			Enter a specific year for the day set above to execute the retention policy

➢ Command Line Tool

This section allows administrator to configure a Pre-Backup or Post-Backup command. Command such as batch file to stop and start an application before and after a backup job is completed, or other command such as to shut down the computer when a backup job is completed can be configured.

The following table explains each setting item under the **Retention Policy** tab, with a brief description of what the setting is about and all the configurable items.

Command Line Tool	
What is this setting about?	Defines the default command line to execute before or after a backup is performed. Multiple settings can be created in this menu if you wish to define different default command line for different backup modules.
What are the configurable items?	**Destination** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Pre-Backup Command Line Tool –** configure the pre-backup command line - **Name –** name of this command line setting. - **Working Directory –** directory which the pre-backup command will run at.

	- **Command –** Enter the pre-backup command to be run ➢ **Post-Backup Command Line Tool –** configure the post-backup command line - **Name –** name of this command line setting. - **Working Directory –** directory which the post-backup command will run at. - **Command –** enter the post-backup command to be run

➢ Reminder

This section allows administrator to enable the backup reminder feature where users will be reminded to run a backup job when they log off or shut down their computers. The reminder feature is only available on Windows platform.

The following table explains each setting item under the **Reminder** tab, with a brief description of what the setting is about and all the configurable items.

Reminder	
What is this setting about?	Defines whether the backup reminder is on for backup users when they log off or shut down their computers. Multiple settings can be created in this menu if you wish to define different settings for different backup modules.
What are the configurable items?	**Destination** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Remind me to backup during Windows log off or shut down –** turn on or off this feature - **Computer name –** you can specify the computer's name for this reminder to apply on

➢ Bandwidth Control

This section allows administrator to limit the data transfer rate when performing backup and restore jobs.

NOTE

➢ The actual value will be around +/- 5% of the limit value when the bandwidth control set to below 32Mb/s. When the bandwidth control set to above 64Mb/s, the gap between actual value and limit value might be over 5%.

- Network stability might influence the transfer rate fluctuation accuracy.

The following table explains each setting item under the **Bandwidth Control** tab, with a brief description of what the setting is about and all the configurable items.

<table>
<tr><th colspan="2">Bandwidth Control</th></tr>
<tr><td>What is this setting about?</td><td>Defines the default settings on limiting the data transfer rate when performing backup and restore jobs. Multiple settings can be created in this menu if you wish to define different settings for different backup modules.</td></tr>
<tr><td>What are the configurable items?</td><td>
Destination
➢ Name – name of the setting item
➢ Applied Modules – modules to apply this setting to
➢ Limit the transfer rate when performing backup and restore tasks – click to turn on or off this feature
- Mode
<table>
<tr><td>Independent</td><td>Each backup and restore job has its assigned bandwidth</td></tr>
<tr><td>Share</td><td>All backup and restore jobs are sharing the same assigned bandwidth
Note: Share mode does not support performing backup job on multiple destinations concurrently.</td></tr>
</table>
- Existing bandwidth controls – configure the bandwidth control details
<table>
<tr><td>Name</td><td>Name of the bandwidth control setting item</td></tr>
<tr><td>Type</td><td>Always – apply the bandwidth control settings at all times
Only within this period – configure a specific start time and end time on a day of a week for this bandwidth control setting to take place</td></tr>
<tr><td>Maximum transfer rate</td><td>Enter the maximum transfer rate allowed, in the unit of Kbit/s, Mbit/s or Gbit/s.</td></tr>
</table>
</td></tr>
</table>

➢ IP Allowed for Restore

This section allows administrator to IP ranges that are allowed to perform restore. The following table explains each setting item under the **IP Allowed for Restore** tab, with a brief description of what the setting is about and all the configurable items.

IP Allowed for Restore	
What is this setting about?	Defines the default settings on IP allowed for restore. Multiple settings can be created in this menu if you wish to define different settings for different backup modules.
What are the configurable items?	**Destination** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **IP Allowed for Restore–** configure the IP ranges allowed for restore - **From** – restore allowed from this IP value - **To** - restore allowed up to this IP value

➢ **Others**

This section allows administrator to configure other default settings. The following table explains each setting item under the **Others** tab, with a brief description of what the setting is about and all the configurable items.

Temporary Directory	
What is this setting about?	The temporary directory is used for various purposes, such as storage of temporary spooled file, remote file list, local file list, temporary delta file and other files of temporary nature. Administrator can define the default location of the temporary directory. Multiple settings can be created in this menu if you wish to define different temporary directory locations for different backup modules.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Platform** – the platform on which this setting will apply on ➢ **Applied Modules** – modules to apply this setting to ➢ **Temporary directory for storing backup files –** location of the temporary directory you wish to set. ➢ **Remove temporary files after backup –** the temporary files after backup if this option is selected

Follow Link

What is this setting about?	Administrator can define whether to turn on the Follow Link feature by default. When this feature is on, not only the symbolic link or junction point will be restored, the directories and files that the symbolic link or junction point links to will also be restored. This feature is only applicable to File Backup module.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Follow link of the backup files** – check the box to enable this feature

Volume Shadow Copy	
What is this setting about?	Enabling the Volume Shadow Copy option will allow backup of local files that are exclusively opened during the backup process (e.g. Outlook PST file). Some requirements of the Volume Shadow Copy option include: - Volume Shadow Copy can only be applied for local drive; exclusively opened file on network shared drive cannot be backed up even with the Volume Shadow Copy option enabled. - Volume Shadow Copy is only available on Windows platforms (e.g. Vista / 2008 / 2008 R2 / 7 / 2012 / 2012 R2 / 8 /10). - The user using the backup application must have administrative privileges to access the Volume Shadow Copy service on a computer. - At least one of the partitions on the machine must be in NTFS format. For more technical information on Volume Shadow Copy, please refer to the following page from Microsoft for details: http://technet.microsoft.com/en-us/library/cc785914(WS.10).aspx Administrator can define whether to turn on the Volume Shadow Copy feature by default .This feature is only applicable to File Backup module.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Enable Windows' Volume Shadow Copy for open file backup** – check or uncheck to enable or disable this feature

File Permissions

What is this setting about?	By enabling this option, file permissions of the operating system files will be backed up. File permission defines, for example, the right to view or change a file by the system owner/group/individual. Administrator can define whether to turn on the backup of File Permissions by default .This feature is only applicable to File Backup module.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Backup files' permissions** – check the box to enable this feature

Archived Log Deletion	
What is this setting about?	Administrator can define whether the archived log files will be deleted after backup by default .This feature is only applicable to Oracle Database Server Backup module.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Delete the archived logs after backup** – turn on or off this feature - **Delete archived logs that are older than the following days** – set the number of day(s) that the archived logs will be deleted when exceeding this number

OpenDirect	
What is this setting about?	Administrator can enable the OpenDirect setting for Windows File backup sets on AhsayOBM and AhsayCB, to support restore of selected files/folder within a compressed or images file without the need to restore the compressed of image file first.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **OpenDirect** – enable or disable this feature

Granular Restore	
What is this setting about?	Administrator can enable the Granular Restore setting for VMware ESXi/vCenter and Hyper-V guest VM backup sets, to support restore of selected files/folder within a virtual disk of a guest VM without the need to restore the guest VM file first.

What are the configurable items?	➢ **Name** – name of the setting item ➢ **Granular Restore** – enable or disable this feature

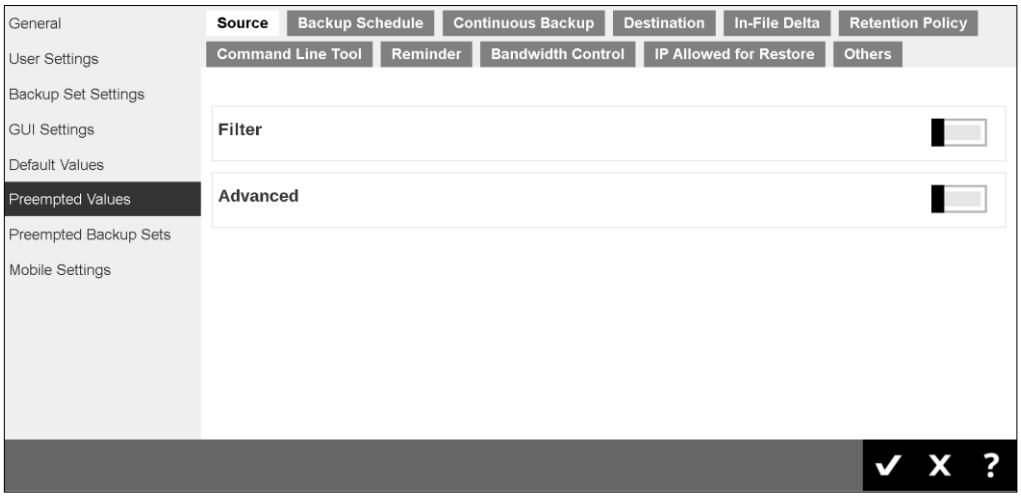
Compressions	
What is this setting about?	Compressing data before they are backed up brings faster backup and restore time and save storage space on the backup destination. Compression does not apply on Run direct backup sets for Hyper-V and VMware even this feature is on. Administrator can define the default compression type for backup set. Multiple settings can be created in this menu if you wish to define different default compression types for different backup modules.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Select compression type** – select the desired compression type among **No Compression**, **Normal** and **Fast** (Compressed size larger than normal)

Encryption	
What is this setting about?	For better security reason, backup users can choose to encrypt their backup data with an algorithm, mode and key of their choice. Encryption does not apply on Run direct backup sets for Hyper-V and VMware even this feature is on. Administrator can define the default encryption setting for backup set. Multiple settings can be created in this menu if you wish to define different default encryption settings for different backup modules.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Encrypt Backup Data** – enable or disable this feature - **Default (Machine Generated Random)** – the system will randomly generate an encryption key - **Custom –** define your own algorithm, encryption key, method and key length.

Preempted Values

This section allows administrator to define the predefined values for backup users' backup sets. The preempted values set under this setting menu will be applied to the backup sets directly. Backup users can add additional values on top of the preempted values when creating a backup set but **CANNOT** remove the preempted values preset by the system administrator.

All setting items under the Preempted Values tab are disabled by default. Click the switch on the right of each setting item and then follow the steps below for configuration.



Mode

In all the setting items in the Preempted Values section, there is a **Mode** setting item that contains 3 options on how this preempted values are applied to user defined settings.

- **Prepend** – the preempted values will be applied as the first user defined settings
- **Append** – the preempted values will be applied as the last user defined settings
- **Override** – override all user defined settings

NOTE

In some preempted value settings, "Override" mode is set as default and cannot be modified, e.g. Reminder, as administrator should take full control of the policy settings. However, prepend and append mode are available for some non-administrator related features, such as backup schedule, where users defined settings can also be considered.

➢ Source

This section defines the preempted backup source values. The following table explains each setting item under the **Source** tab, with a brief description of what the setting is about and all the configurable items.

Filter	
What is this setting about?	Defines the default filter mode, filters which used to include/exclude files in the backup source from performing backup. This filter applies only to File Backup on Windows platform. Creating multiple filter settings is possible.
What are the configurable items?	➢ **Name** – name of the filter setting ➢ **Apply filters to the backup source** – turn this on to configure the filters ➢ **Matching pattern -** defines the pattern of the file selection, e.g., *.doc, *.png. ➢ **For each of the matched files/folders under top directory** – define to include or exclude all the files/folder matching the filtering criteria under the top directory ➢ **Exclusion / Inclusion** – to include (if you have chosen to exclude the matched files) or exclude (if you have chosen to include the matched files) those unmatched files/folder in the backup ➢ **Match file/folder names by** – you can set the following filtering rules: **[Simple comparison starts with]** Include/Exclude all files/directories with name starting with a certain pattern. ***Example:*** *You can use B* to match all file with name starting with a B character.* **[Simple comparison ends with]** Include / Exclude all files / directories with name ending with a certain pattern. ***Example:*** *You can use *.doc to match all files with name ending with .doc (all Word Documents)* **[Simple comparison contain]** Include/Exclude all files/directories with name containing a certain pattern. ***Example:*** *You can use *B* to match all files with name containing with a B character.* **[Regular Expression (UNIX-style)]** Include/Exclude all files/directories with name matching a regular expression.

<table>
<tr><td></td><td>

Notes:

- The pattern of a backup filter is case sensitive.
- If multiple patterns are required, please add the pattern one by one e.g.: *.doc and then *.xls

- **How to Apply This Filter** – you can choose to apply this filter on "**All hard disk drivers**" or a selected folder of your choice.

- **Apply to** - apply the filter to the File and/or Folder level

</td></tr>
<tr><td>Use Cases</td><td>

Example 1

If you want to backup only Word, Excel and PowerPoint documents in your document directory (e.g. C:\My Documents), you should setup your backup filter as follows.

Matching pattern = *.doc, *.xls, *.ppt
For each of the matched files/folders under top directory = Include them
Exclusion = Check
Match file/folder names by = Simple comparison end with
How to Apply This Filter = This folder only C:\My Documents
Apply to = File

Example 2

If you want to backup all files, excluding all *.exe, *.dll and *.tmp, in C:\Application, you should setup your backup filter as follows.

Matching pattern = *.exe, *.dll, *.tmp
For each of the matched files/folders under top directory = Exclude them
Inclusion = Check
Match file/folder names by = Simple comparison end with
How to Apply This Filter = This folder only C:\Applicaitons
Apply to = File

Example 3

If you have already chosen files (all under C:\) from the backup source setting but you want to exclude all images (e.g. *.jpg and *.gif) from your selection, you should setup your backup filter as follows.

Matching pattern = *.jpg, *.gif
For each of the matched files/folders under top directory = Exclude them
Inclusion = uncheck
Match file/folder names by = Simple comparison end with
How to Apply This Filter = This folder only C:\
Apply to = File

*Please note that the **Inclusion** setting should not be checked because you have already chosen the desired files to back up and do not want to include all other files (NOT *.jpg, *.gif) under C:\ into the backup set.*

</td></tr>
</table>

	Example 4 If you want to include everything, except the “log" directory, under C:\Applications into a backup set, you should setup your backup filter as follows. **Matching pattern** = ^log$ **For each of the matched files/folders under top directory** = Exclude them **Inclusion** = check **Match file/folder names by** = Regular Expression (UNIX-style) **How to Apply This Filter** = C:\Applications **Apply to** = Folder **Example 5** If you want to include all directories named “log" from the backup set files with file name starting with “B" and ending with “*.doc" under C:\My Documents into the backup set, you can use a regular expression of “^B.*\.doc$" to do your selection. The filter backup can then be setup as follows. **Matching pattern** = ^B.*\.doc$ **For each of the matched files/folders under top directory** = Include them **Exclusion** = check **Match file/folder names by** = Regular Expression (UNIX-style) **How to Apply This Filter** = C:\My Documents **Apply to** = File

Advanced	
What is this setting about?	Defines the default advanced settings for backup source, including backup mode, other selected source and deselected source.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Applied Module** – module you wish to apply this default setting to ➢ **Other Selected Source** – define the path of the source, e.g. Windows: C:\My folder; Linux: /home/my folder, to include in the backup set ➢ **Deselected Source** - define the path of the source, e.g. Windows: C:\My folder; Linux: /home/my folder, to exclude in the backup set.

➢ Backup Schedule

Setting up backup schedule allows backup sets to run automatically at the specified time. This section allows administrator to pre-define default backup schedule(s) for backup users. The following table explains each setting item under the **Backup Schedule** tab, with a brief description of what the setting is about and all the configurable items.

Schedule	
What is this setting about?	Predefine backup schedule(s) for backup sets. Multiple settings can be created in this menu if you wish to pre-define different backup schedules for different backup modules. Within a backup schedule setting, multiple scheduled times can be added.
What are the configurable items?	**Backup Schedule** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Run scheduled backup for this backup set –** to enable or disable the scheduled backup settings you set in this menu **Manage Schedule** ➢ **Name** – name of the scheduler ➢ **Type** – frequency of running the scheduled backup - **Daily** – to run the scheduled backup everyday - **Weekly** – to run the scheduled backup on the selected days of a week - **Monthly** – to run the scheduled backup on a specific day in a month, or on a specific day in a specific week. - **Custom** – to run the scheduled backup on a specific day of your selection ➢ **Start backup at** – specify a specific time to run the scheduled backup based on the frequency set in the Type menu above. ➢ **Stop** – set the scheduled backup to stop either - Full backup is completed regardless of how much time it takes **OR** - After the backup has started for the set time (1-24 hr) regardless if the backup is done ➢ **Run Retention Policy after backup** – enable this feature if you wish the modified or deleted data after backup remains in the backup server for the set number of retention day

➢ Continuous Backup

When the Continuous Backup feature is enabled, a backup job will be triggered whenever a change is made in the backup source. This section allows administrator to define the default continuous backup settings. The following table explains each setting item under the **Continuous Backup** tab, with a brief description of the available settings and all the configurable items. **Continuous Backup is only available on Windows platform.**

IMPORTANT
When setting up the Continuous Backup feature for a backup set, you must run a manual or scheduled backup job first so that the initial files are uploaded your designated backup destination.

Continuous Backup	
What is this setting about?	Predefine the settings and filters to trigger continuous backup, including to exclude system files, frequency of running backup when changes are detected, configure the maximum file size allowed for backup and configure filters to exclude files from backup.
What are the configurable items?	**Continuous Backup** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Backup whenever a change is made** – enable or disable the continuous backup feature ➢ **Exclude system files** – enable this feature if you do not want to back up system files. Refer to Appendix J for a full list of system files excluded from the backup set. ➢ **How often should the backup run** – set the frequency of running backup when changes are detected. ➢ **Only apply to files smaller than** – file size that is larger than the set value will not be backed up **Exclude Filter** ➢ **Name** - name of the filter setting item ➢ **Match file/folder names by** – you can set the following filtering rules: **[Simple comparison starts with]** Include/Exclude all files/directories with name starting with a certain pattern. ***Example:*** *You can use B* to match all file with name starting with a B*

	character. **[Simple comparison ends with]** Include / Exclude all files / directories with name ending with a certain pattern. ***Example:*** *You can use *.doc to match all files with name ending with .doc (all Word Documents)* **[Simple comparison contain]** Include/Exclude all files/directories with name containing a certain pattern. ***Example:*** *You can use *B* to match all files with name containing with a B character.* **[Regular Expression (UNIX-style)]** Include/Exclude all files/directories with name matching a regular expression. ***Notes:*** - The pattern of a backup filter is case sensitive. - If multiple patterns are required, please add the pattern one by one e.g.: *.doc and then *.xls ➢ **Matching pattern** - defines the pattern of the file selection, e.g., *.doc, *.png. ➢ **Apply This Filter to all files/folders in** – you can choose to apply this filter on "**All selected sources**" or a selected folder of your choice ➢ **Apply to** - apply the filter to the File and/or Folder level
Use Cases	**<u>Example 1</u>** If you want to back up all files, except all Word, Excel and PowerPoint documents, in your document directory (e.g. C:\My Documents), you should setup your backup filter as follows. **Match file/folder names by** = Simple comparison end with **Matching pattern** = *.doc, *.xls, *.ppt **Apply this filter to all files/folders in** = This folder only C:\My Documents **Apply to** = File **<u>Example 2</u>** If you want to include everything, except the "log" directory, under C:\Applications into a backup set, you should setup your backup filter as follows. **Match file/folder names by** = Regular Expression (UNIX-style) **Matching pattern** = ^log$

	Apply this filter to all files/folders in = This folder only C:\Applications **Apply to** = Folder **Example 3** If you want to exclude all directories named “log" from the backup set files with file name starting with “B" and ending with “*.doc" under C:\My Documents into the backup set, you can use a regular expression of “^B.*\.doc$" to do your selection. The filter backup can then be setup as follows. **Match file/folder names by** = Regular Expression (UNIX-style) **Matching pattern** = ^B.*\.doc$ **Apply this filter to all files/folders in** = This folder only C:\My Documents **Apply to** = File
Use Cases	**Example 1** If you want to back up all files, except all Word, Excel and PowerPoint documents, in your document directory (e.g. C:\My Documents), you should setup your backup filter as follows. **Match file/folder names by** = Simple comparison end with **Matching pattern** = *.doc, *.xls, *.ppt **Apply this filter to all files/folders in** = This folder only C:\My Documents **Apply to** = File **Example 2** If you want to include everything, except the “log" directory, under C:\Applications into a backup set, you should setup your backup filter as follows. **Match file/folder names by** = Regular Expression (UNIX-style) **Matching pattern** = ^log$ **Apply this filter to all files/folders in** = This folder only C:\Applications **Apply to** = Folder **Example 3** If you want to exclude all directories named “log" from the backup set files with file name starting with “B" and ending with “*.doc" under C:\My Documents into the backup set, you can use a regular expression of “^B.*\.doc$" to do your selection. The filter backup can then be setup as follows. **Match file/folder names by** = Regular Expression (UNIX-style) **Matching pattern** = ^B.*\.doc$ **Apply this filter to all files/folders in** = This folder only C:\My Documents **Apply to** = File

➢ Destination

This section allows administrator to predefine backup destination for backup sets. The following table explains each setting item under the **Destination** tab, with a brief description of what the setting is about and all the configurable items.

Destination	
What is this setting about?	Pre-define backup destination when backup users create a backup set. Multiple settings can be created in this menu if you wish to define different default destinations for different backup modules.
What are the configurable items?	**Destination** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Backup Mode –** select the files transfer method during backup - **Sequential –** backup files are sent to the backup destination one by one, one after another - **Concurrent –** multiple files are sent to the backup destination at the same time ➢ **Maximum concurrent backup destinations (only if you have selected Concurrent as the Backup Mode) –** select the maximum number of files allowed for uploading to the backup destination ➢ **Predefined Destination** – select the predefined destination you have configured in the Predefined Destinations Tab section.

➢ In-File Delta

In-file delta technology is an advanced data block matching algorithm with the intelligence to pick up changes (delta) of file content between two files.

Using this algorithm, daily backup of large files over low-speed internet connection is made possible because it requires only the changes of information since the last backup to be sent over (assuming that the full backup of the file has been saved on the backup server already).

This section allows administrator to predefine the In-File Delta settings for backup set. The following table explains each setting item under the **In-File Delta** tab, with a brief description of what the setting is about and all the configurable items.

In-File Delta

<table>
<tr><td>What is this setting about?</td><td>Predefine In-File delta setting for backup set. Multiple settings can be created in this menu if you wish to pre-define different in-file delta settings for different backup modules.</td></tr>
<tr><td>What kind of in-file delta type are there?</td><td><u>Incremental In-file delta</u>

Incremental Delta will facilitate ease of backup. The delta is generated by comparing with the last uploaded full or delta file. Delta generated with this method is smaller and uses the least bandwidth. However, for restoration, the full file and all deltas up to the required point-in-time are required to be restored and merged.

<u>Differential In-file delta</u>

Differential Delta will facilitate ease of restore. The delta is generated by comparing with the last uploaded full file only. Delta generated with this method will grow daily and uses more bandwidth. However, for restoration, the full file and a single delta is required to be restored and merged.</td></tr>
<tr><td>What are the configurable items?</td><td><u>Destination</u>
➢ Name – name of the setting item
➢ Applied Modules – modules to apply this setting to
➢ Default Type – type of backup method (Incremental or Differential)

<u>Advanced settings</u>
➢ In-File Delta block size – defines the size of block used when detecting changes between last full or delta file and the file to be backed up.

<u>In-file delta backup with small block size</u>
- Produce a smaller delta file due to a more precise comparison
- Require more processing power on the client machine
- Comparison may take longer to complete
- Require more Java memory

<u>In-file delta backup with large block size:</u>
- Produce a larger delta file due to a less precise comparison
- Require less processing power on the client machine
- Comparison will complete faster
- Require less Java memory

For most cases, the default setting Auto will select the optimal block size for each file (depending on the size of the file). The Auto setting will set the block size according the following criteria:
<table><tr><th>File size</th><th>Block size</th></tr><tr><td>Smaller than 2GB</td><td>4KB</td></tr></table></td></tr>
</table>

2GB – 8GB	8KB
Larger than 8GB	16KB

- **Only apply In-File Delta to files larger than –** defines the minimum file size a file to apply the in-file delta setting. If the size of a file to be backed up is smaller than the set value, the in-file delta setting will not apply and the whole file will be uploaded to the backup server.

  It is not necessary to perform In-file delta backup on small files because backing up the whole file does not take long. Backing up the whole file instead reduces the time required to restore the file.

- **Upload full file when either of these conditions is met** – a backup of the full file will be perform if the following condition is met:
  - **Number of deltas is over** – when the number of delta file exceeds the set value
  - **Delta ratio (delta file size / full file size) is over** – this setting is to ensure that a full file backup is performed for file with significant changes, as it is preferable to upload a full file instead to reduce the time required to restore the file

- **Weekly variations for overriding default type** – override the default in-file delta setting in the **Default Type** field on selected day(s) of a week

- **Yearly variations for overriding default type and weekly variations** – override the default in-file delta setting in the **Default Type** field as well as the setting in the "**Weekly variations for overriding default type**" section on a selected day in a week based on either of the following selection
  - **Day of selected months in yearly variations -** select a specific day in a month. On this specified day in the month defined above will the in-file delta variation setting override the default value.

➢ Retention Policy

Retention policy defines the policies of persistent data management for meeting business data archival requirements. When a backup job is performed, for data that are modified or deleted on the client computer, their existing versions on the backup server (backup records) will be moved into retention area, while newly backed up files will be placed in the current data area.

Specifically, retention policy setting defines how long are the backup records kept in the retention area before they are deleted permanently from the backup server.

This section allows administrator to pre-define the Retention Policy for backup set. The following table explains each setting item under the **Retention Policy** tab, with a brief description of what the setting is about and all the configurable items.

<table>
<tr><th colspan="3">Retention Policy</th></tr>
<tr><td>What is this setting about?</td><td colspan="2">Pre-define the retention policy for backup sets when they are created. Multiple settings can be created in this menu if you wish to define different default retention policy for different backup modules.</td></tr>
<tr><td>What are the configurable items?</td><td colspan="2">
Destination
➢ Name – name of the setting item
➢ Applied Modules – modules to apply this setting to
➢ How to retain the files in the backup set, which have been deleted in the backup source – choose between Simple and Advanced setting, which is explained in details below.
- Simple – enter a specific number of day or backup job number. The retained data will be removed from the storage destination permanently after the set number of day or set number of job is met.
- Advanced – manage advanced retention policies by applying advanced configurations
<table>
<tr><td rowspan="2">Daily</td><td>The past number of days on which different versions of your files are retained</td></tr>
<tr><td>Set the number of day(s) on which the old version of data will be stored</td></tr>
<tr><td rowspan="4">Weekly</td><td>The days within a week on which different versions of your files are retained</td></tr>
<tr><td>Select the day(s) in a week (Monday – Sunday) on which the old version of data will be stored</td></tr>
<tr><td>The number of weeks to repeat the above selection</td></tr>
<tr><td>Enter the number of week(s) for the above setting to repeat</td></tr>
<tr><td rowspan="4">Monthly</td><td>The days within a month on which different versions of your files are retained</td></tr>
<tr><td>Select a day in a month on which the old version of data will be stored. You can either set:
- An exact day (1-31) or
- The (First/Second/Third/Forth/Last) of (Monday -Sunday)</td></tr>
<tr><td>The number of months to repeat the above selection</td></tr>
<tr><td>Enter the number of month(s) for the above setting to repeat</td></tr>
</table>
</td></tr>
</table>

		Quarterly	**The day within a quarter on which different versions of your files are retained**
			Select a day within a quarter on which the old version of data will be stored. You can either set: - An exact day (1-31) **or** - The (First/Second/Third/Forth/Last) of (Monday -Sunday)
			Months of quarter
			Select the desired combination of months of quarter - (January, April, July, October) - (February, May, August, November) - (March, June, September, December)
			The number of quarters to repeat the above selection
			Enter the number of quarter(s) for the above setting to repeat
		Yearly	**The day within a year on which different versions of your files are retained**
			Select a day within a year on which the old version of data will be stored. You can set the day by using one of the following methods: - Select an exact day (1 – 31) in an exact month (January – December) - Select the (First/Second/Third/Forth/Last) of (Monday/Tuesday/Wednesday/Thursday/ Friday/Saturday/Sunday/Weekday/Weekend) in an exact month (January – December) - Select a day in a week (Monday – Sunday) in an exact week of a year (Week 1 - 53)
			The number of years to repeat the above selection
			Enter the number of year(s) for the above setting to repeat
		Custom	**A specific day on which different versions of your files are retained**
			Select a day on which the old version of data will be stored. You can set the day by using one of the following methods: - Select an exact day (1 – 31) in an exact month (January – December)

			- Select the (First/Second/Third/Forth/Last) of (Monday/Tuesday/Wednesday/Thursday/ Friday/Saturday/Sunday/Weekday/Weekend) in an exact month (January – December) - Select a day in a week (Monday – Sunday) in an exact week of a year (Week 1 - 53)
			Year
			Enter a specific year for the day set above to execute the retention policy

➢ Command Line Tool

This section allows administrator to configure a Pre-Backup or Post-Backup command. Command such as batch file to stop and start an application before and after a backup job is completed, or other command such as to shut down the computer when a backup job is completed can be configured.

The following table explains each setting item under the **Retention Policy** tab, with a brief description of what the setting is about and all the configurable items.

Command Line Tool	
What is this setting about?	Predefine command line to execute before or after a backup is performed. Multiple settings can be created in this menu if you wish to pre-define different command line for different backup modules.
What are the configurable items?	**Destination** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Pre-Backup Command Line Tool –** configure the pre-backup command line - **Name –** name of this command line setting. - **Working Directory –** directory which the pre-backup command will run at. - **Command –** Enter the pre-backup command to be run ➢ **Post-Backup Command Line Tool –** configure the post-backup command line - **Name –** name of this command line setting. - **Working Directory –** directory which the post-backup command will run at.

	- **Command –** enter the post-backup command to be run

➢ Reminder

This section allows administrator to enable the backup reminder feature where users will be reminded to run a backup job when they log off or shut down their computers. Reminder feature is only available on Windows platform.

The following table explains each setting item under the **Reminder** tab, with a brief description of what the setting is about and all the configurable items.

Reminder	
What is this setting about?	Pre-define to turn on the reminder so that backup users will be reminded to perform backup when they log off or shut down their computers. Multiple settings can be created in this menu if you wish to define different settings for different backup modules.
What are the configurable items?	**Destination** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Remind me to backup during Windows log off or shut down –** turn on or off this feature - **Computer name –** you can specify the computer's name for this reminder to enable on

➢ Bandwidth Control

This section allows administrator to pre-define the limit for data transfer when performing backup and restore jobs.

NOTE

➢ The actual value will be around +/- 5% of the limit value when the bandwidth control set to below 32Mb/s. When the bandwidth control set to above 64Mb/s, the gap between actual value and limit value might be over 5%.

➢ Network stability might influence the transfer rate fluctuation accuracy.

The following table explains each setting item under the **Bandwidth Control** tab, with a brief description of what the setting is about and all the configurable items.

Bandwidth Control

<table>
<tr><td>What is this setting about?</td><td>Pre-define the settings on limiting the data transfer rate when performing backup and restore jobs. Multiple settings can be created in this menu if you wish to pre-define different settings for different backup modules.</td></tr>
<tr><td>What are the configurable items?</td><td>
Destination

Name – name of the setting item
Applied Modules – modules to apply this setting to
Limit the transfer rate when performing backup and restore tasks – click to turn on or off this feature

- Mode
<table>
<tr><td>Independent</td><td>Each backup and restore job has its assigned bandwidth</td></tr>
<tr><td>Share</td><td>All backup and restore jobs are sharing the same assigned bandwidth
Note: Share mode does not support performing backup job on multiple destinations concurrently.</td></tr>
</table>
- Existing bandwidth controls – configure the bandwidth control details
<table>
<tr><td>Name</td><td>Name of the bandwidth control setting item</td></tr>
<tr><td>Type</td><td>Always – apply the bandwidth control settings at all times
Only within this period – configure a specific start time and end time in a day of a week for this bandwidth control setting to take place</td></tr>
<tr><td>Maximum transfer rate</td><td>Enter the maximum transfer rate allowed, in the unit of Kbit/s, Mbit/s or Gbit/s.</td></tr>
</table>
</td></tr>
</table>

➢ IP Allowed for Restore

This section allows administrator to predefine IP ranges that are allowed to perform restore. The following table explains each setting item under the **IP Allowed for Restore** tab, with a brief description of what the setting is about and all the configurable items.

IP Allowed for Restore

What is this setting about?	Pre-define the IP allowed for restore. Multiple settings can be created in this menu if you wish to pre-define different settings for different backup modules.
What are the configurable items?	**Destination** ➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **IP Allowed for Restore–** configure the IP ranges allowed for restore - **From** – restore allowed from this IP value - **To** - restore allowed up to this IP value

➢ Others

This section allows administrator to pre-define other configurations for backup sets. The following table explains each setting item under the **Others** tab, with a brief description of what the setting is about and all the configurable items.

Follow Link	
What is this setting about?	Administrator can pre-define whether to turn on the Follow Link feature. When this feature is on, not only the symbolic link or junction point will be restored, the directories and files that the symbolic link or junction point links to will also be restored. This feature is only applicable to File Backup module.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Follow link of the backup files** – check the box to enable this feature

Volume Shadow Copy	
What is this setting about?	Enabling the Volume Shadow Copy option will allow backup of local files that are exclusively opened during the backup process (e.g. Outlook PST file). Some requirements of the Volume Shadow Copy option include: - Volume Shadow Copy can only be applied for local drive; exclusively opened file on network shared drive cannot be backed up even with the Volume Shadow Copy option enabled. - Volume Shadow Copy is available on Windows platforms (e.g. Vista / 2008 / 2008 R2 / 2012 / 2012 R2 / 7 / 8 / 10).

	- The user using the backup application must have administrative privileges to access the Volume Shadow Copy service on a computer. - At least one of the partitions on the machine must be in NTFS format. For more technical information on Volume Shadow Copy, please refer to the following page from Microsoft for details: http://technet.microsoft.com/en-us/library/cc785914(WS.10).aspx Administrator can pre-define whether to turn on the Volume Shadow Copy feature by default .This feature is only applicable to File Backup module.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Enable Windows' Volume Shadow Copy for open file backup** – check or uncheck to enable or disable this feature
File Permissions	
What is this setting about?	By enabling this option, file permissions of the operating system files will be backed up. File permission defines, for example, the right to view or change a file by the system owner/group/individual. Administrator can pre-define whether to turn on the backup of File Permissions by default .This feature is only applicable to File Backup module.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Backup files' permissions** – check or uncheck to enable or disable this feature

Archived Log Deletion	
What is this setting about?	Administrator can pre-define whether the archived log files will be deleted after backup by default .This feature is only applicable to Oracle Database Server Backup module.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Delete the archived logs after backup** – turn on or off this feature - **Delete archived logs that are older than the following days** – set the number of day(s) that the archived logs will be deleted when exceeding this number

Compressions

What is this setting about?	Compressing data before they are backed up brings faster backup and restore time and save storage space on the backup destination. Compression does not apply on Run direct backup sets for Hyper-V and VMware even this feature is on. Administrator can pre-define the default compression type for backup set. Multiple settings can be created in this menu if you wish to define different default compression types for different backup modules.
What are the configurable items?	➢ **Name** – name of the setting item ➢ **Applied Modules** – modules to apply this setting to ➢ **Select compression type** – select the desired compression type among **No Compression**, **Normal** and **Fast** (Compressed size larger than normal)

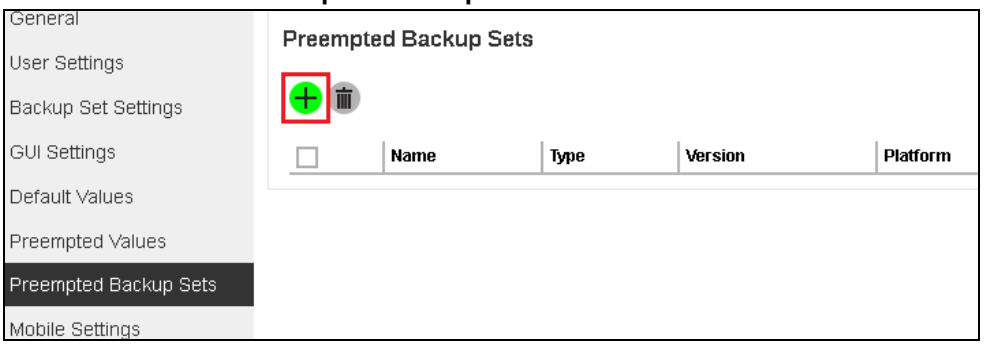
Preempted Backup Sets

This section allows you predefine a backup set that will be run a default backup set for backup user with this policy group setting. Backup user **CANNOT** remove this preempted backup set from their backup job once it is preset by the system administrator.

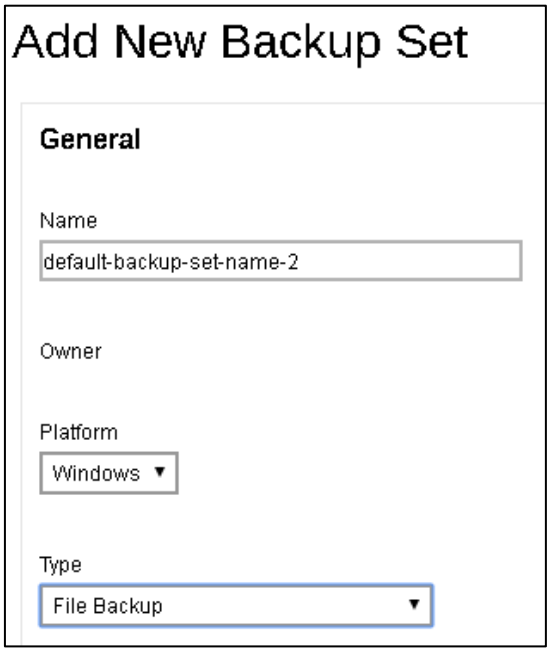
Create a preempted backup set

Follow the steps below to create a preempted backup set

1. Click ⊕ under the **Preempted Backup Sets** section.



2. Enter the **Name** of the new backup set, the **Platform** on which the backup set will run on, and select the backup set type from the **Type** dropdown box. |



The choices for Platform

- Windows
- Mac
- Linux

The choices for backup set types

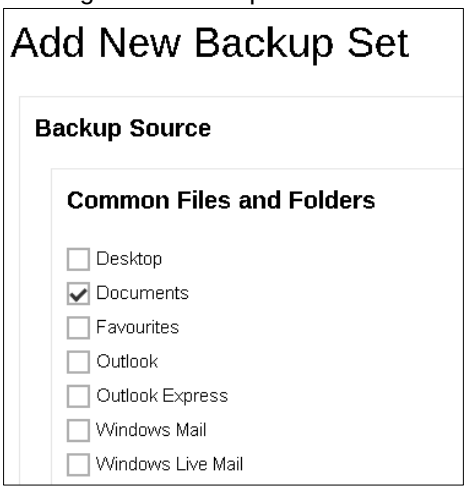
- File Backup
- IBM Lotus Notes Backup
- MS Exchange Mail Level Backup
- MS Hyper-V Backup
- MySQL Backup
- Storage Craft ShadowProtect Backup
- VMware Backup
- IBM Lotus Domino Backup
- MS Exchange Server Backup
- MS SQL Server Backup
- MS Windows System Backup
- Oracle Database Server Backup
- MS Windows System State Backup

In our example, the new backup set is called **default-backup-set-name-2** which is a File Backup type that will be run on Windows.

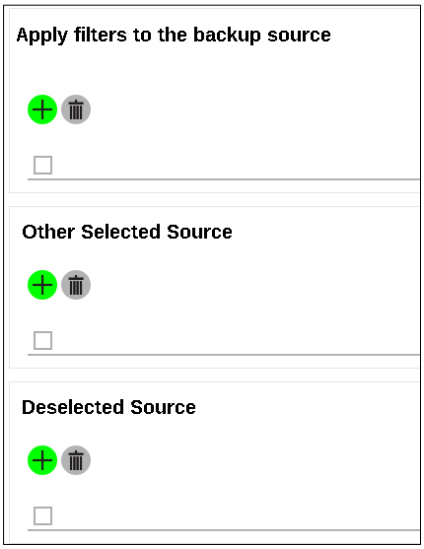
Click to continue.

3. Specify the backup source for the new backup set. The selection items of this page varies depending on the backup set type you have chosen. Below is an example of

creating a File Backup set.

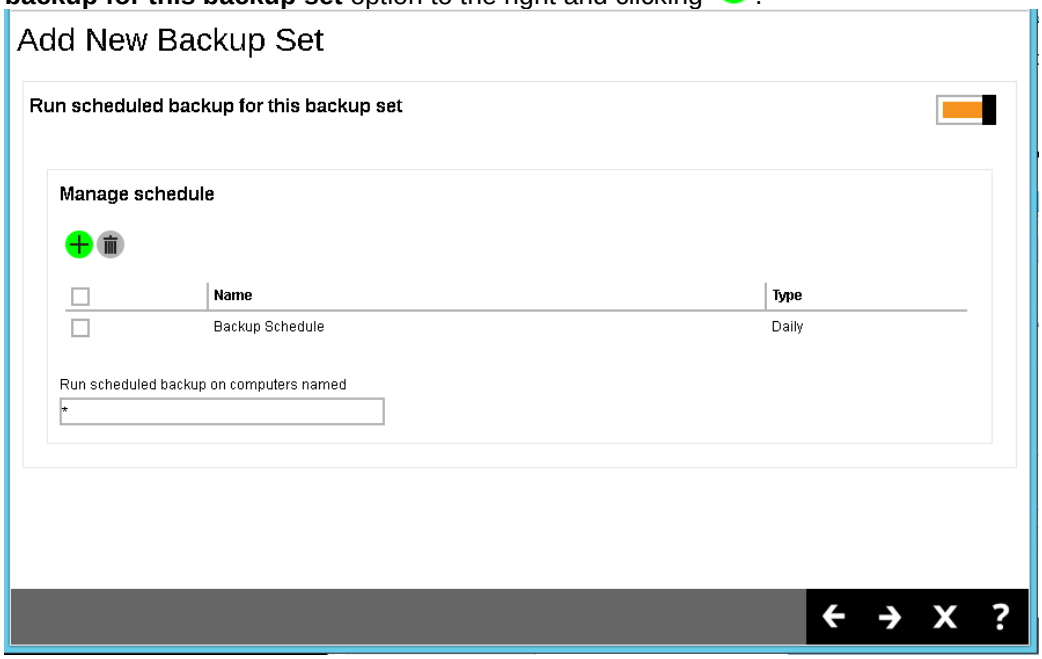


4. You can apply filters to the backup source, select other backup source or deselect backup source. Click to get redirected to the relevant section in the previous chapter for configurations details.

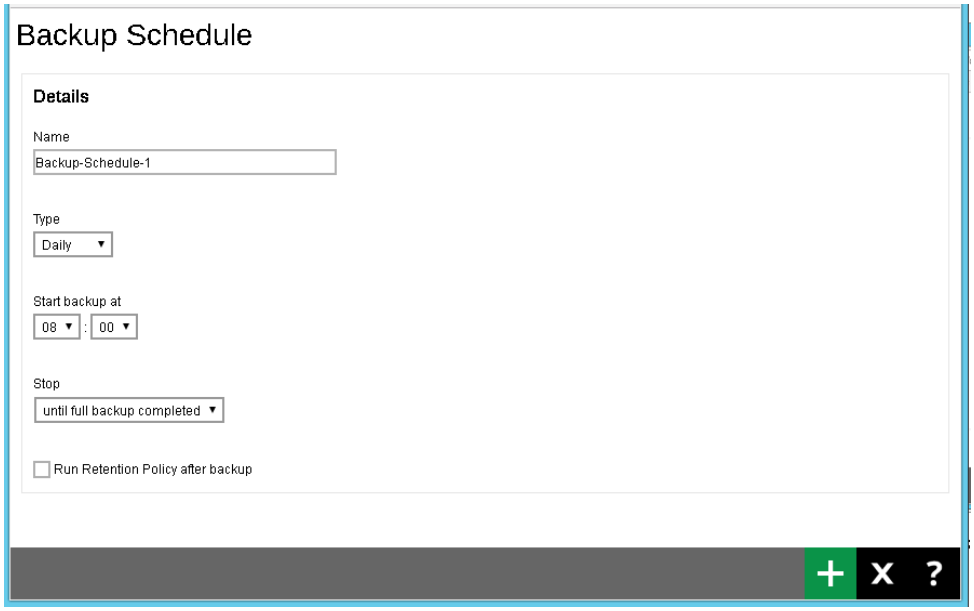


5. Click to continue.

6. If necessary, add a Backup Schedule for this backup set by sliding the **Run scheduled backup for this backup set** option to the right and clicking .

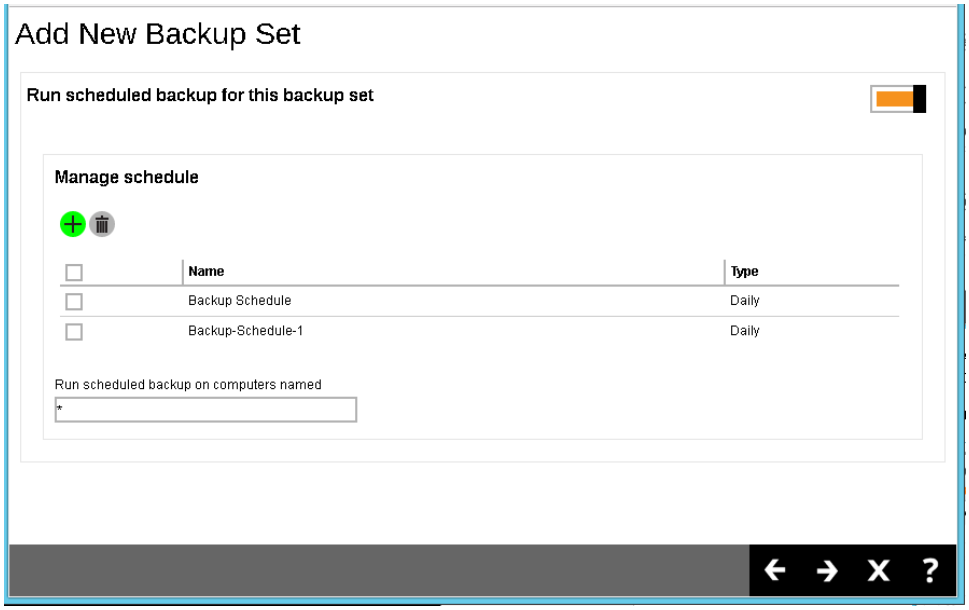


- Enter the information of the new backup schedule you want to add. Click to continue.

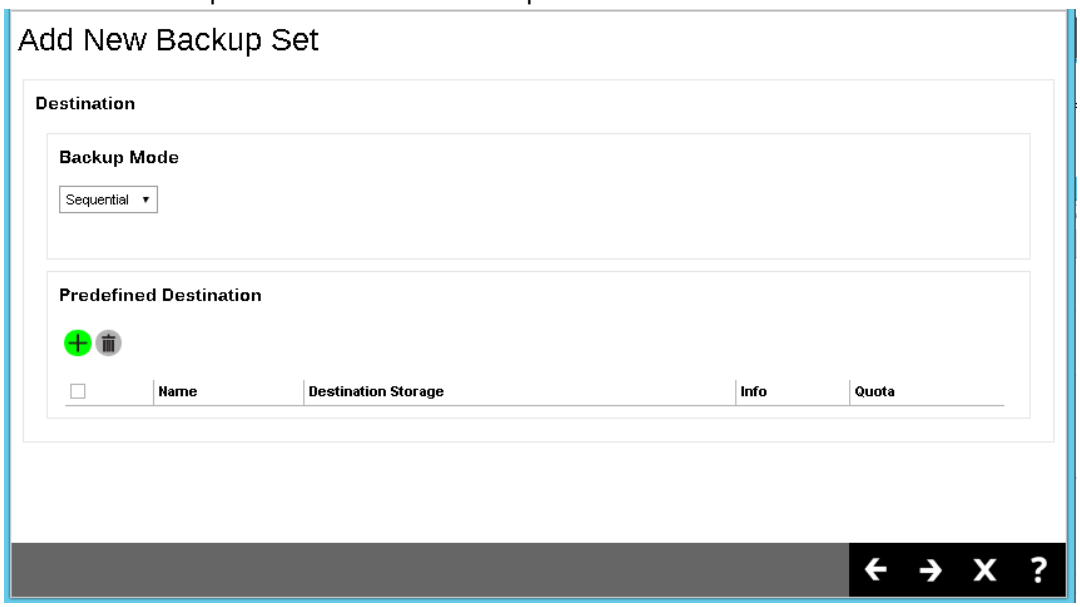


- The new backup schedule, **Backup-Schedule-1** in our example, can be seen under the **Manage schedule** list.

Click to continue.



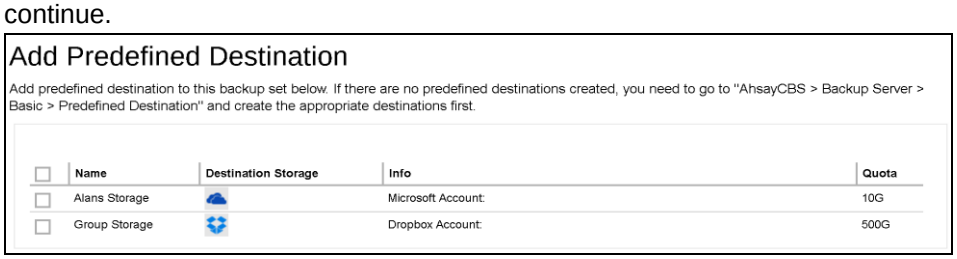
7. Add a new backup destination for this backup set.



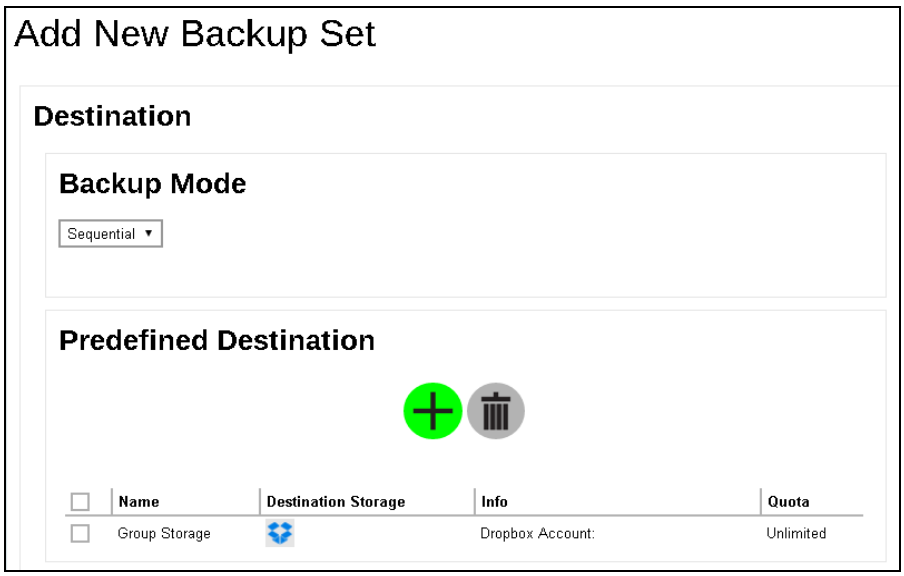
- From the **Backup Mode** dropdown box, select either **Sequential** or **Concurrent**. In our example, we select **Sequential**.

- Add a Predefined Destination set by your backup service provider by clicking .

  Check the box next to the predefined destination you want, then click to continue.



- The new predefined destination, **Group Storage** in our example, can be seen under the **Predefined Destination** list.



If you would like to choose other standard destination, you will have to configure in the client backup agent (AhsayOBM/AhsayACB) after you finish creating the backup in AhsayCBS.

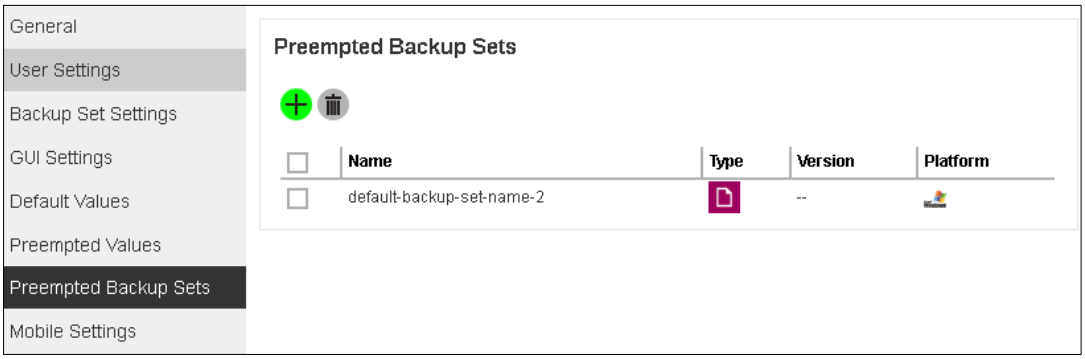
Click to continue.

8. Select to enable or disable to encrypt the backup data. If you choose to enable this feature, you can select either **Default** or **Custom** for the Encryption Type. Refer to Others section under the Default Values section for details on configuration.

9. Enter the Windows User Authentication information. This is needed for backup set with backup schedule and network shared drive selected as backup source. Enter the domain name and user name for AhsayOBM to access the network location.

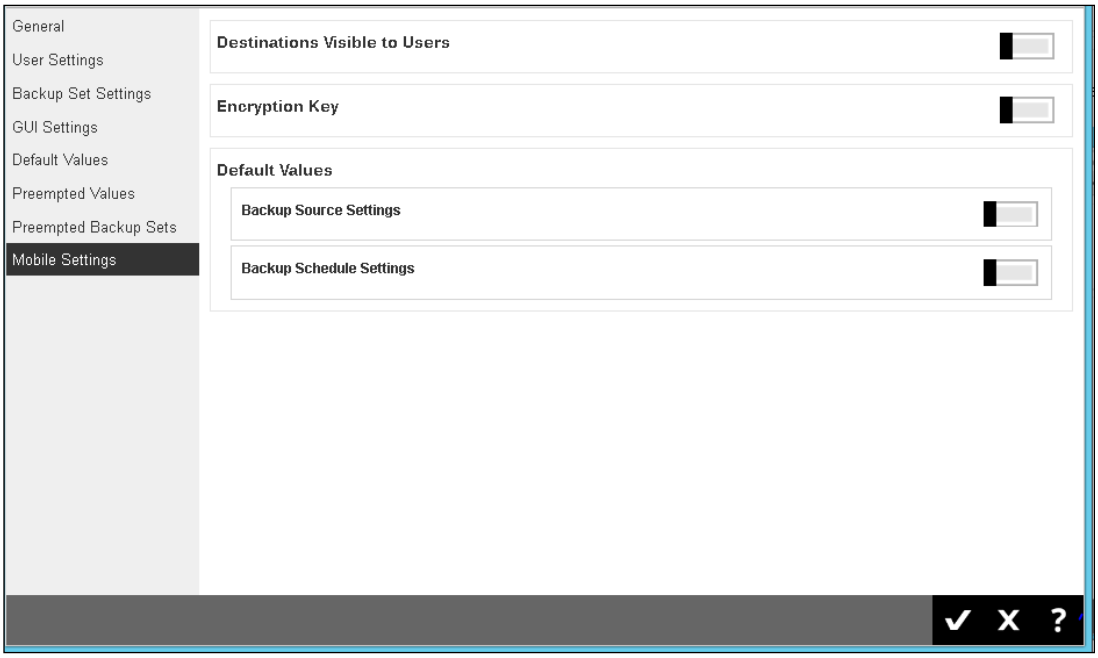
10. Click to save.

11. A new backup set called **default-backup-set-name-2** is created and can be seen in the Preempted Backup Sets list.



Mobile Settings

This section allows administrator to configure settings for AhsayMOB backup users.



➢ Destinations Visible to Users

There are two kinds of destinations backup users can choose from when creating a backup set, they are the Predefined Destination and Standard Destination. Only the destinations selected in this menu will be available for backup users to choose from when they are creating a backup set.

Below is a brief explanation on the differences between the Predefined Destination and Standard Destination.

Predefined Destination vs Standard Destination

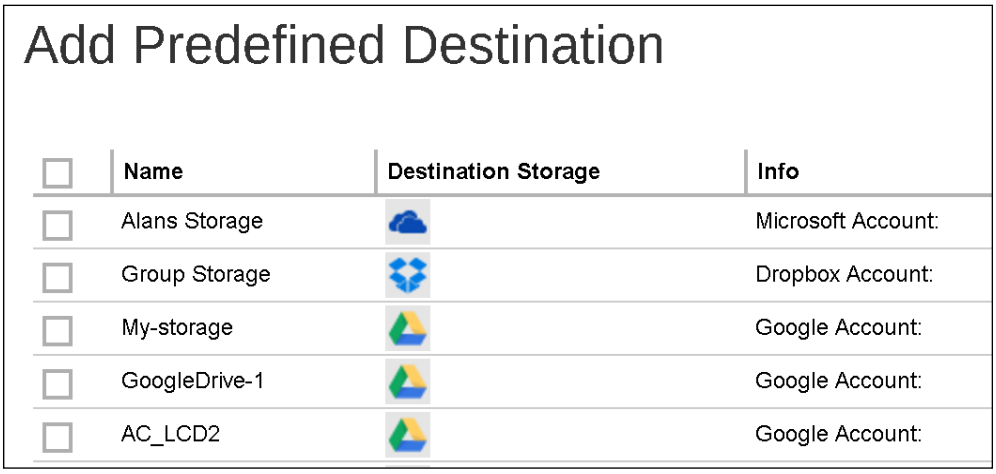
- **Predefined Destination** - The predefined destination can be a single storage destination on the local drive where CBS is installed, mapped drive, cloud storage or FTP server, or a destination pool with a mix of storage options mentioned above. Before you can select a predefined destination in this menu, it must first be configured under the **System Settings** > **Backup** > **Predefined Destinations**. Refer to Predefined Destinations Tab for details on configuration.

- **Standard Destination** - Except for the AhsayCBS storage option, all other storage options under the Standard Destination belong to the backup users, whether it could be a single storage destination on the mapped drive, cloud storage or FTP server, or a destination pool with a mix of storage options mentioned above.

To configure the Predefined Destination

1. Turn on the switch on the right under the **Destinations Visible to Users** section.
2. Click on the button under the **Predefined Destination** section.

3. Select the desired destination option, which has been defined in the **System Settings** > **Backup** > **Predefined Destinations** menu, by checking the box on the desired destination item.



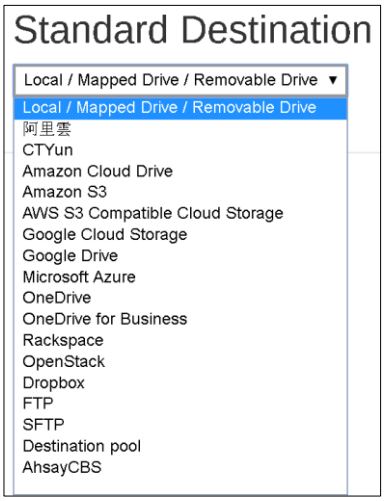
4. Click the button to confirm adding the predefined destination.
5. If you have multiple predefined destinations to add, repeat steps 3 -4 until all desired destinations have been selected.
6. Click to confirm.

To configure the Standard Destination

1. Turn on the switch on the right under the **Destinations Visible to Users** section.

2. Click on the button under the **Standard Destination** section.

3. Select the desired storage option from the drop-down menu as shown below.



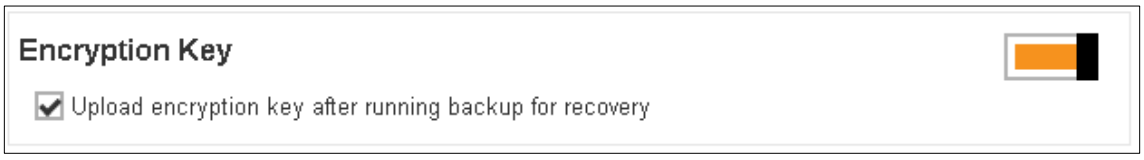
4. Click the button to add the selected standard destination storage.

5. If you have multiple destination storages to add, repeat steps 3 – 4 until all desired storages have been selected.

6. Click to confirm.

➢ Encryption Key

Once you enabled the encryption recovery option, the encryption key file is uploaded to the backup server. In case the user forgot the encryption key, you can still contact us to have it recovered. The recovered encryption key will be sent directly to the email address registered on the user account. Refer to the Encryption key section for further details.



➢ Default Values

You may configure the default values of the following two options which will apply to the AhsayMOB backup sets.

Backup Source Settings	
Mode	**Read Only** – backup users can only read the backup source settings set by the system administrator but CANNOT edit the settings. **Editable** – backup users will be able to edit the settings on their own during the backup set creation process
Backup Source	Select the backup source type from the following choices: • Audio* • Contact • Photo • SMS* • Video • WhatsApp* ***Only available for AhsayMOB installed on the Android platform**

Backup Schedule Settings	
Mode	**Read Only** – backup users can only read the backup source settings set by the system administrator but CANNOT edit the settings. **Editable** – backup users will be able to edit the settings on their own during the backup set creation
Backup on these days of the week	**Backup on these days of the week** - select the days(s) in a week when you wish to perform backup (select from Sun to Sat) **Start backup at** – select a specific time when backups will be performed on the days you have selected from the previous setting item

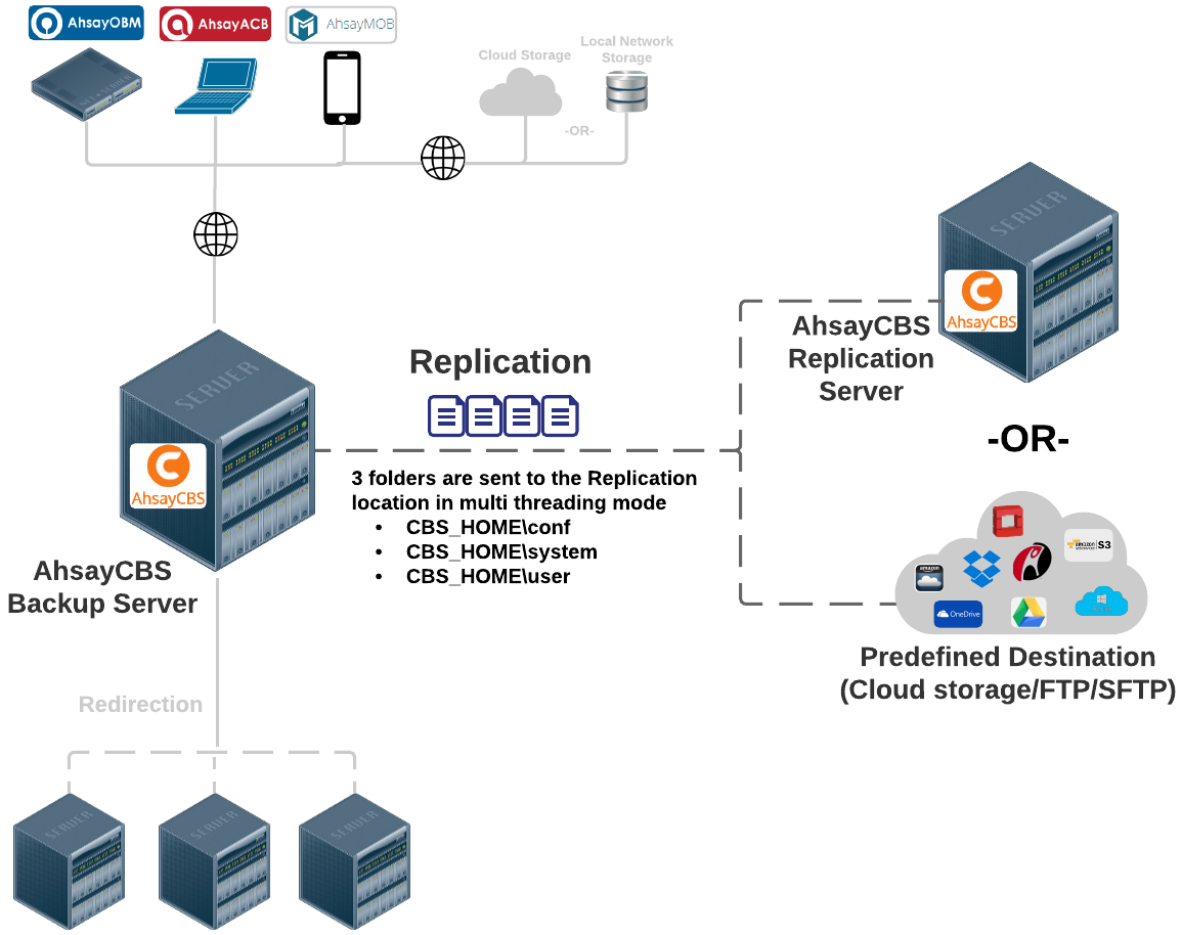
7 Replication

Overview

What is Replication?

AhsayCBS replication server provides an additional layer of data protection by providing an offsite backup store for synchronizing data from either a single or multiple AhsayCBS servers to provide high availability for your business needs. The replication feature is specially designed for replicating user home data hosted physically on AhsayCBS to either another AhsayCBS (Replication Server) or a predefined destination (e.g. cloud storage, FTP/SFTP or local/network storage) configured in the AhsayCBS backup server. The replication process is close to real-time and therefore can reduce the possibilities of significant data loss in the event of an AhsayCBS server outage. In case the AhsayCBS backup server is down, the replication server can be quickly converted into a backup server with minimal down time.

This feature is designed to provide replication services for AhsayCBS only and it does not provide general replication service for other files within the system. This means that you cannot use AhsayCBS replication to replicate your Windows/Linux/Unix system to another machine.



What technology is used for Replication?

During the **Resync** stage of the replication process (refer to How does Replication Work below for details), snapshot images of users' backup sets will be created and then sent to the replication server. By utilizing the snapshot image technology, the data on the backup server can be replicated in a rather short time and therefore close to real-time replication is made possible.

By utilizing the multi-threading technology, replication can now be processed faster than the traditional single thread replication. Refer to Multiple Threads Replication for further details.

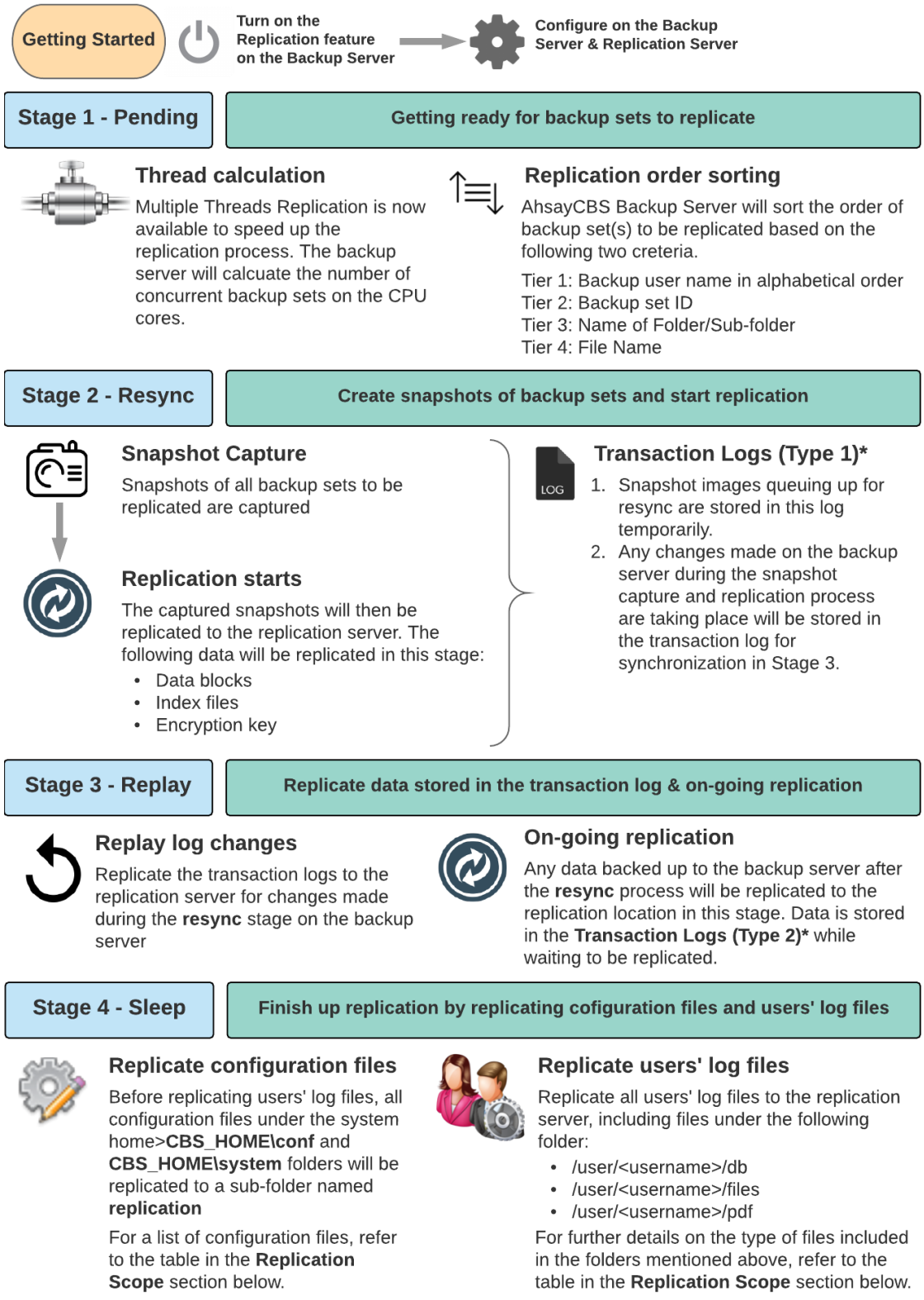
Differences between v6 and v7 on Replication

Since AhsayCBS v7, the replication service has been revamped to empower you with a more reliable and secure replication experience. The table below explains the major feature differences between v6 and v7 on replication.

	Version 6	Version 7
Multi Threads Replication	Replication process is performed over single thread mode which takes longer time to complete.	The replication process is performed over multi threads mode where multiple backup sets are sent to the replication location concurrently. The number of threads for replication is also configurable by the backup user.
Support Replication to Cloud Storage	Only replication to AhsayRPS is possible.	Supports replication to either another AhsayCBS server or cloud storage (as defined in the predefined destination).
Replication Port	A dedicated port has to be defined for replication receiver to perform replication.	Replication is performed via the **http/https** (ports 80 and 443 by default) defined on AhsayCBS. No additional ports are required.
Real-time Monitoring Progress	Real-time replication progress cannot be monitored.	The real-time replication progress of each backup set can now be monitored on the AhsayCBS web console.
Replication of Individual Backup Sets Only	**User Level** - all backup sets from all backup users must be replicated when the replication feature is turned on.	**Backup Set Level** - replication of only selected backup sets is now possible.

How does Replication Work

Replication runs in 4 stages, namely **Pending**, **Resync**, **Replay** and **Sleep**. Refer to the diagram below for an overview of the replication process.



*** For more details on the differences between Transaction Logs Type 1 and Type 2, refer to Transaction Log Location.**

Replication Scope

The following three folders on the local file system are included in the replication process.

IMPORTANT

1. Please be reminded that **ALL** 3 folders will be **CRITICAL** and **REQUIRED** if you need to rebuild AhsayCBS from scratch, or to recover system settings.
2. Only user data hosted physically on AhsayCBS will be replicated. Local drive includes, for example, local hard disk, mapped network drive, removable drive, external storage device connected to AhsayCBS with UNC path, etc. Certain types of external storage connection, for example FTP/SFTP, are not regarded as local drive even if it is connected through LAN, and therefore will not be included for replication.

- **%CBS_INSTALL%\conf**

  The table below shows a list of files included in this folder.

Server Configuration	
Path	**Description**
/conf/server.xml	Connector setting file
/conf/afc.opt /conf/cbs.opt	CBS option files
/conf/cbssvc.ini	Runtime setting file
/conf/ca.crt /conf/ssl.crt /conf/ssl.key	Default certificate files
/conf/cbs.json	CBS setting files
/conf/lfsConfig.xml	Redirector configuration files
CBS Configuration	
Path	**Description**
/conf/obs.json	Backup Server setting files
/conf/lic.json /conf/license.xml	License files
/conf/cbs.opt	CBS/OBS option files
/conf/autoUpdate.bdb	Autoupdate index
/conf/rpsSend.xml	Replication configuration files
/conf/users.xml	Users' profile

RPS Configuration	
Path	**Description**
/conf/rps.xml /conf/rpsRecv.xml /conf/rps-recv.json	Replication configuration files
RDR Configuration	
Path	**Description**
/conf/rdr.xml /conf/rdr.json	Redirector configuration files
/conf/rdr-lic.json /conf/rdr-license.xml	License files
Others	
Path	**Description**
/conf/Branding/*.*	Branding directory
/conf/Backup/*.*	Auto Save snapshot file
/conf/certs	Only created after administrator importing a SSL certificate or generating a new CSR (Certificate Signing Request)

- **%CBS_INSTALL%\system**

The table below shows a list of files included in this folder.

Group Policy Settings	
Path	**Description**
/system/obs/policies/userGroup.xml	User group definition
/system/obs/policies/policyList.xml	Policy group definition

- **%USER_HOME%**

The table below shows a list of files included in this folder.

CBS User Profile	
Path	**Description**
/user/%username%/db	This sub-folder contains files with the following info: ➢ Backup logs of all backup sets ➢ All logs and statistics records of all backup sets created on different client locations ➢ Records of email notification for backup/restore/setting change ➢ Restore logs ➢ Monthly storage record of each backup set ➢ Daily activities log

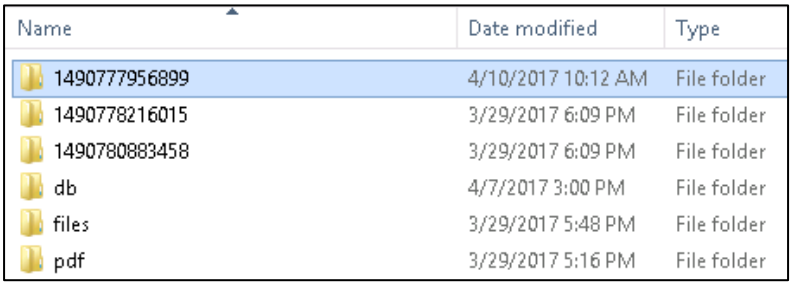
/user/%username%/files	This sub-folder contains info files for all backup sets, with the following info: ➢ Backup set name ➢ Backup set ID ➢ Backup set type ➢ Version of the client's machine running the backup set
/user/%username%/pdf	This sub-folder contains all backup and restore reports in pdf format
/user/%username%/ %backup set ID%	This sub-folder contains files with the following info: ➢ Data blocks and index file of all backups ➢ Encryption key file (if uploaded) ➢ Replication snapshots (if applicable)

Coexistence of v6 and v7 Formats Backup Data

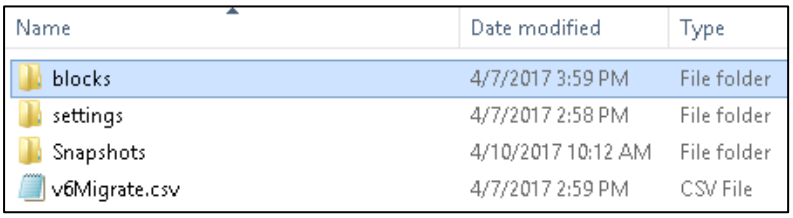
When you have enabled replication for v6 backup sets on AhsayCBS v7, the backup data will be replicated to your replication destination in v6 data format. If, afterwards, a v7 upgrade of the AhsayOBM/AhsayACB is done and backup is performed for those backup sets, the backup data will be produced and replicated in v7 format. In that case, there will be two sets of backup data stored for the same backup set in separate locations under the **CBS_HOME\user**. The following illustrations show the location where the v6 and v7 format backup data stored.

- **v7 format backup data**

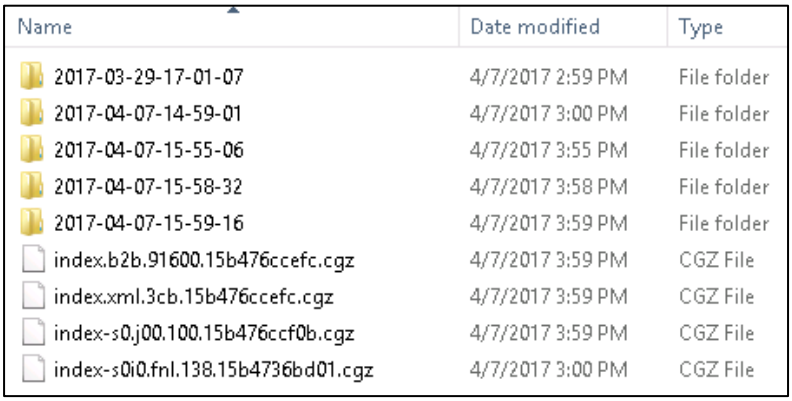
Backup set ID – unique ID for individual backup set



Data blocks folder

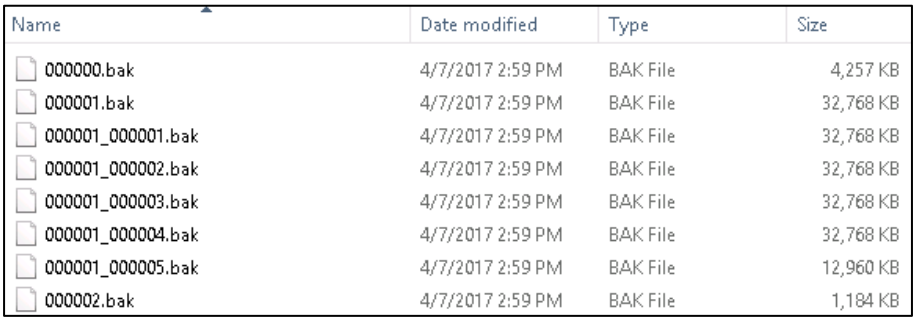


A new folder created every time when a backup is run, indicated by date and time in the folder name



Name	Date modified	Type
2017-03-29-17-01-07	4/7/2017 2:59 PM	File folder
2017-04-07-14-59-01	4/7/2017 3:00 PM	File folder
2017-04-07-15-55-06	4/7/2017 3:55 PM	File folder
2017-04-07-15-58-32	4/7/2017 3:58 PM	File folder
2017-04-07-15-59-16	4/7/2017 3:59 PM	File folder
index.b2b.91600.15b476ccefc.cgz	4/7/2017 3:59 PM	CGZ File
index.xml.3cb.15b476ccefc.cgz	4/7/2017 3:59 PM	CGZ File
index-s0.j00.100.15b476ccf0b.cgz	4/7/2017 3:59 PM	CGZ File
index-s0i0.fnl.138.15b4736bd01.cgz	4/7/2017 3:00 PM	CGZ File

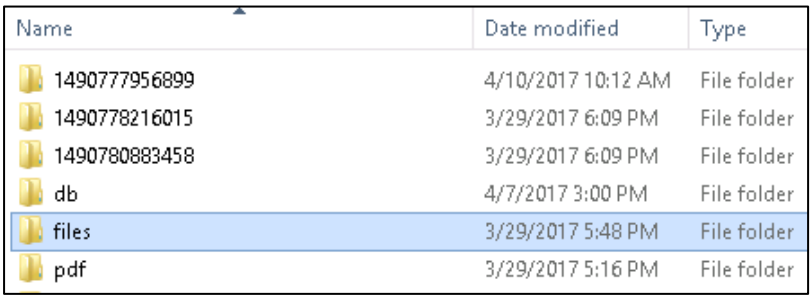
Data block in v7 format



Name	Date modified	Type	Size
000000.bak	4/7/2017 2:59 PM	BAK File	4,257 KB
000001.bak	4/7/2017 2:59 PM	BAK File	32,768 KB
000001_000001.bak	4/7/2017 2:59 PM	BAK File	32,768 KB
000001_000002.bak	4/7/2017 2:59 PM	BAK File	32,768 KB
000001_000003.bak	4/7/2017 2:59 PM	BAK File	32,768 KB
000001_000004.bak	4/7/2017 2:59 PM	BAK File	32,768 KB
000001_000005.bak	4/7/2017 2:59 PM	BAK File	12,960 KB
000002.bak	4/7/2017 2:59 PM	BAK File	1,184 KB

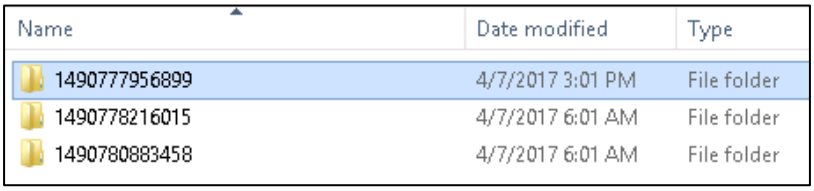
- **v6 format backup data**

Under the files folder



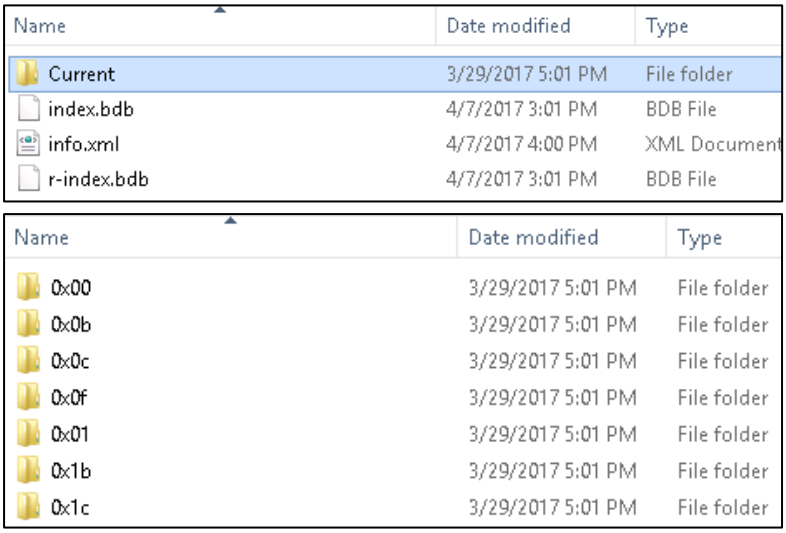
Name	Date modified	Type
1490777956899	4/10/2017 10:12 AM	File folder
1490778216015	3/29/2017 6:09 PM	File folder
1490780883458	3/29/2017 6:09 PM	File folder
db	4/7/2017 3:00 PM	File folder
files	3/29/2017 5:48 PM	File folder
pdf	3/29/2017 5:16 PM	File folder

Backup set ID – unique ID for individual backup set



Name	Date modified	Type
1490777956899	4/7/2017 3:01 PM	File folder
1490778216015	4/7/2017 6:01 AM	File folder
1490780883458	4/7/2017 6:01 AM	File folder

Backup data stored under the ***Current*** folder



NOTE

When data migration for v6 data is completed and AhsayCBS has replicated the v6 backup data, the v6 data will be deleted from both the backup server and replication server.

Transaction Log Location

Transaction log is a location storing backup data temporarily before they are enter the replication cycle mentioned in How does Replication work.

There are two different kinds of transaction logs which are located separately under the AhsayCBS folder. Refer to the information below for further elaboration.

Type 1 – transaction log stored in USER HOME

Location
%USER_HOME%/%BACKUP_SET_ID%/rps/{%DELETE_TIME%.%LOG_SEQ%}
What kind of transaction log does it store?
This folder stores the transaction log entries produced during the **Stage 2 – Resync** of the replication process. In specific, the transaction logs are the changes made on the backup server during the snapshot capture and replication process are taking place. This kind of data will only be replicated to the replication location in **Stage 3 – Replay**.

Type 2 – transaction log stored in SYSTEM HOME

Location
%SYSTEM_HOME%/%USER_ID%/%BACKUP_SET_ID%/rps/replay-XXXXXX.log
What kind of transaction log does it store?
This folder stores the transaction log entries produced in **Stage 3 - Replay** mode where it stores data from the backup server pending for replication to the replication location in the on-going replication process.

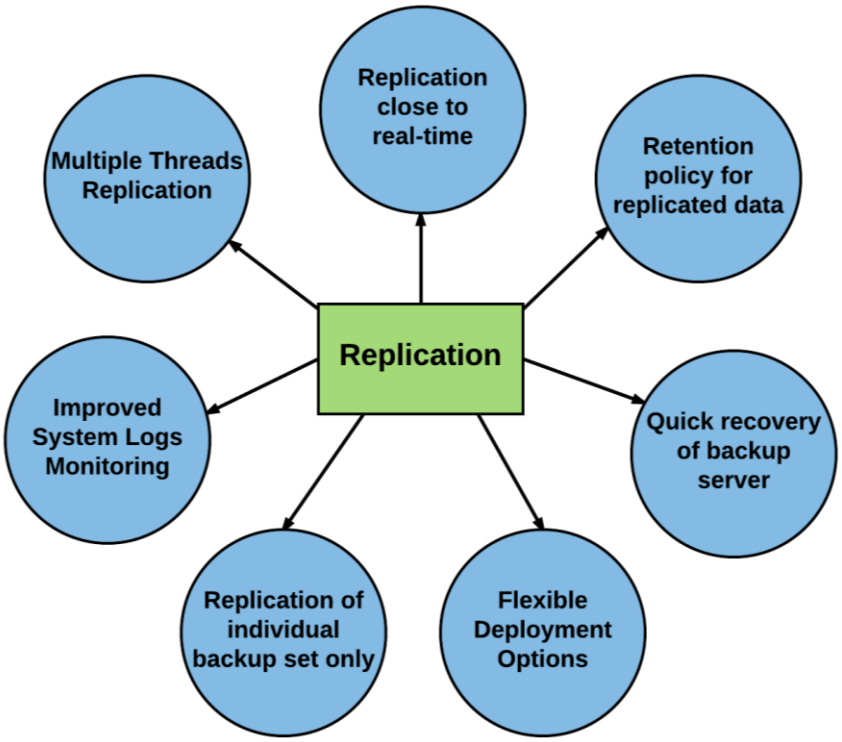
Replication Order

Replication is performed in the order of the tiers as shown in the table below.

Tier 1	Backup User Name
Tier 2	Backup Set ID
Tier 3	Name of Folder/Sub-folder
Tier 4	File Name

Within each tier, the order of replication is performed according to the standard defined by the **American Standard Code for Information Interchange (ASCII)**, refer to http://www.ascii-code.com/ for details of the order.

Benefits of using Replication?



Multiple Threads Replication

1. From version 7.5.0.0 AhsayCBS has a new feature to offer multiple threads replication. This is an enhanced feature which speeds up the replication by allocating a process thread to handle a backup set's replication and to ensure the replication did not have a negative impact on the overall performance of AhsayCBS backup server. The number of concurrent backup sets to handle will be proportional to the number of CPU cores which is calculated by the following formula.

   Number of concurrent backup set to replicate = INT ((N+1)/2)

   NOTE

   INT is the function to calculate the integer value, while **N** is the number of cores in the CPU. For example, an AhsayCBS server with a 16 core CPU, up to 8 concurrent replication threads can be configured.

   For replication of v6 backup sets on AhsayCBS v7, only single thread replication is supported.

   The number of backup sets to replicate concurrently can also be configured by the backup user. Refer to Setting the Number of Backup Sets to Replicate Concurrently for further instructions.

2. From AhsayCBS v7.13.0.6 or above, for underutilized AhsayCBS backup servers running on high performance hardware and storage configurations, with spare network bandwidth capacity, there is an option to increase the maximum number of replication threads equal to **N**, the total number of CPU cores. For example, an AhsayCBS server with a 16 core CPU, up to 16 concurrent replication threads can be configured.

Warning

Please consider carefully before increasing the maximum number of concurrent replication threads on your AhsayCBS backup server. As this change could have a negative impact on your AhsayCBS backup server and therefore your backup service, for example:

- The AhsayCBS backup server could become unresponsive or sluggish.
- Slow AhsayOBM/AhsayACB backup/restore performance.
- Your AhsayOBM/AhsayACB clients may be unable to connect to the backup server, resulting in missed backups.

The AhsayCBS replication server may become overloaded if it is unable to process the increased number of threads and data sent from the AhsayCBS backup server.

Example:

iii. **Assumptions:**

- AhsayCBS v7.13.0.6 or above is installed.
- AhsayCBS Java heap size setting.

  Increasing the number of concurrent replication threads will result in increased Java memory usage. As a general rule of thumb, twice as many replication threads will utilize twice as the amount of Java memory. Therefore, it is highly recommended to increase your Java heap size setting before using a higher replication thread setting, if the peak Java memory usage on your AhsayCBS server is over 50% of the maximum Java heap size setting. (The peak Java memory usage can be obtained from **[Monitoring] > [Dashboard] > [Memory]**)

  For example:

  - If current maximum Java heap setting is 4096M and the peak Java memory usage exceeds 2048M, then you should consider increasing the maximum Java heap size up to 8192M.
  - If current maximum Java heap setting is 4096M and the peak Java memory usage is only 1500M, you may not need any maximum Java heap size adjustment in the short term.

    Please refer to the following link to check about the details of how to modify the Java heap size of AhsayCBS : How to modify the Java FAQheap size of AhsayCBS?
- AhsayCBS installation path: %CBS_INSTALL_PATH%
  - Windows: C:\Program Files\AhsayCBS
  - Linux/Unix: /usr/local/cbs
  - AhsayUBS: /ubs/mnt/eslsfw/obsr

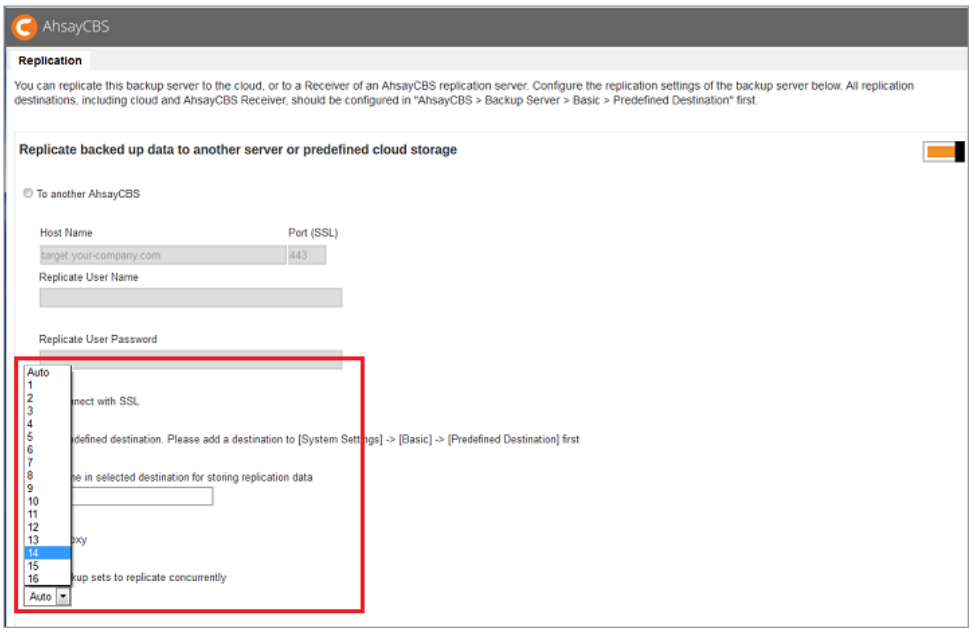
iv. **Steps:**

- Shutdown the AhsayCBS service.

- Using a text editor open the ***%CBS_INSTALL_PATH%/conf/cbs.opt*** file
- Add the following setting to the end of the file and save: ***com.ahsay.cbs.obs.config.Index.RepMaxThreads=true***
- Restart the AhsayCBS service.
- Login to the AhsayCBS web management console.

  Go to **[Replication] > [Sending Data]** and click on the "**No. of backup sets to replicate concurrently**" and select the number of replication threads you wish to configure.

  Example: An AhsayCBS backup server with 16 core CPU



Improved System Logs Monitoring

The Replication Logs section in the AhsayCBS console provides a consolidated view of all replication sending and receiving logs to allow a one-stop monitoring of the replication activities.

Replication Close to Real-Time

The synchronization process does not require stopping or interrupting any backup/restore operations. As the replication module will be replicating the backup data in 4 modes, pending, sleep, resync and replay mode. These 4 modes are used to identify the mode of the replicating backup.

- **Pending** — backup set pending for replication
- **Resync** — responsible to create a snapshot of the current system configuration and user backup files
- **Replay** — replay the changes that happened during the resync mode
- **Sleep** — Backup sets that have finished replicating the backup data

When new backup data are available on the backup server, it will arrange into the above mode of replication which will be replicated to another AhsayCBS (Replication Server) or a predefined storage immediately. Refer to the How does Replication Work section for further details on the 4 replication modes.

Replication of Individual Backup Set Only

Instead of replicating all backup sets from all backup users, you now have the flexibility to select specific user's backup set(s) from the Backup Server to replicate to either another Replication Server or a predefined storage.

You can select the desired backup sets for replication when you create a replication sending account, refer to Configuration on the Replication Sending End for further details.

Retention Policy for Replicated Data

When a snapshot of the backup data on the backup server is replicated to the replication server, the older version of the snapshot will be moved to the retention area for a set period of time before it will be deleted permanently from the replication server. This feature is useful in case if you have to recover data on the backup server from the past.

This configuration can be set when you create a replication receiver, refer to the Create a Replication User Account section for further details.

**This feature applies only to replication to CBS server.*

Flexible Deployment Options

The replication service can be deployed in various options, including another AhsayCBS server, cloud storage, NAS storage connected via FTP/SFTP/local network, etc. It is also possible for multiple backup servers to replicate data to a single AhsayCBS replication server.

Since AhsayCBS v7.11.0.0, you can even replicate v6 backup sets to a receiver on a v7 replication server before the backup sets undergo the data migration process. This new deployment option gives you greater flexibility to gradually migrate the backup sets in v6 format to v7 format after the backup server is upgraded to v7, while the backup sets in v6 format will still be replicated to provide you with data protection.

For more details on deployment, refer to the Deployment Options and Comparison section.

Quick Recovery of Backup Sever

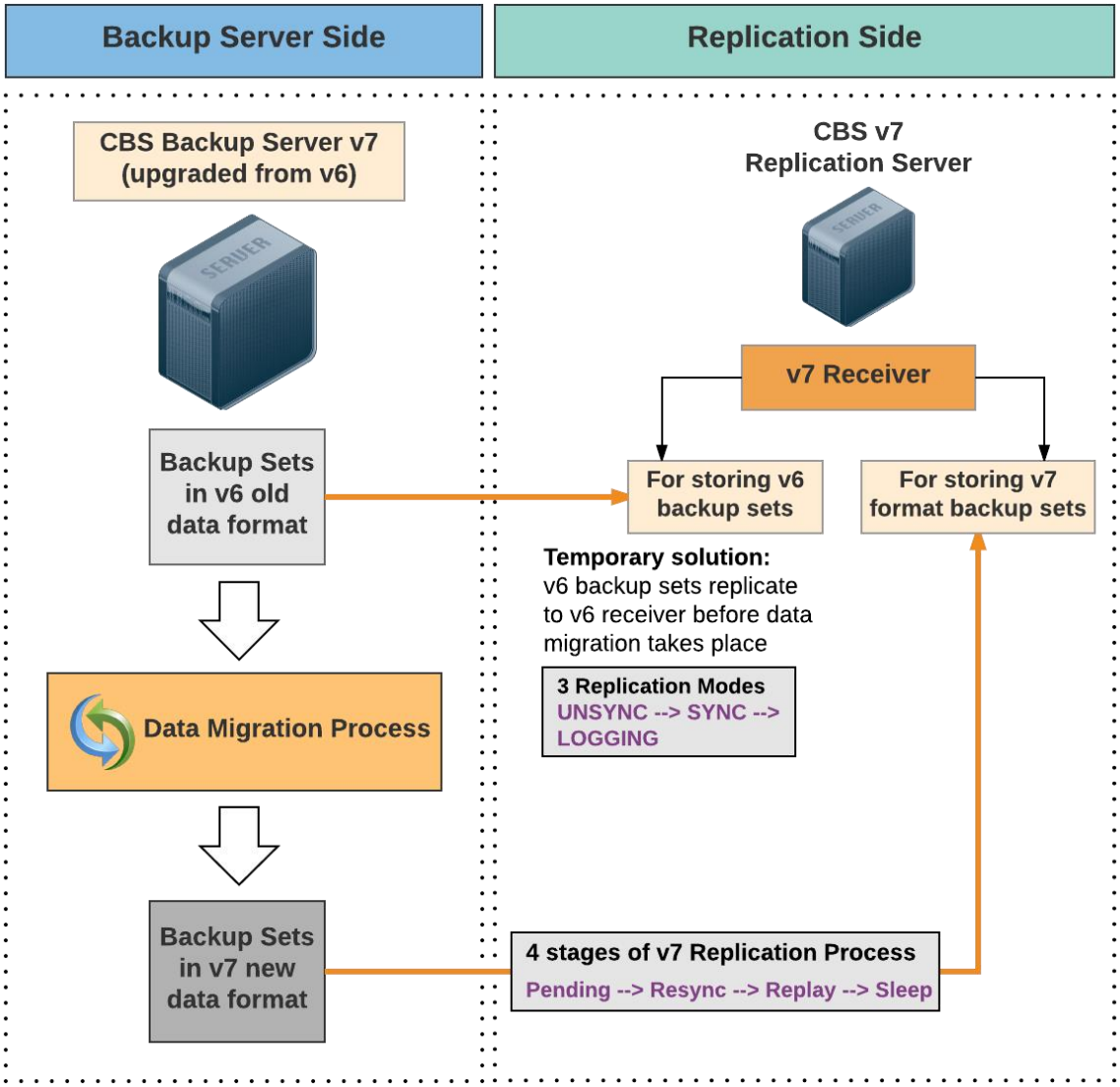
The primary purpose of replication is to provide an extra layer of protection to the data on the backup server in case of disaster like power outage or data corruption. We also understand that it is critical to keep the data recovery process fast so as to minimize interruption to your backup services to clients, that is why we have taken another step forward to simplify the transitioning between replication server and backup server to make the recovery process as fast and seamless as possible. Refer to the Recovery Method section for further details.

Replication of v6 backup sets on AhsayCBS v7

From v7.11.0.0 or above you can replicate v6 backup sets to a receiver on a v7 replication receiver, this feature can be set under the **[Backup / Restore] > [Sending Data] > [Replication]** page.

The v6 backup set replication feature is designed as a temporary solution to provide extra protection during data migration (conversion from v6 data format to v7 data block format) on a v7 backup server after an upgrade from v6 to v7, it is not intended to be used as a permanent replication solution. Once the data migration process is completed for all backup user accounts, the v6 replication feature should be disabled as v6 backup set data would already have been automatically removed post data migration.

Details of the v6 replication status can be viewed under **[Monitoring] > [Replication Logs] > [Replication Sending].**



Note: For further details and instructions on backup set data migration from v6 to v7 format, refer to the Backup Data Migration section.

Requirements

1. Both the AhsayCBS Backup Server (sender) and AhsayCBS Replication Server (receiver) must be on v7.11.0.0 or above.

2. v6 backup set replication must be enabled on both the backup server and replication server.

3. Replication license modules are required for replication of v6 backup sets.

4. The v7 replication on AhsayCBS must be enabled to another replication server.

5. A separate dedicated replication port (default port 9444) is required.

Limitations

1. v7 replication must be enabled to another AhsayCBS server in order to use the feature. As replication to predefined destination does not support replication of v6 backup sets.

2. Replication of v6 backup sets is supported using a single thread.

3. Only v6 backup set data found in the **%USER_HOME%\%USERNAME%\files** folder will be replicated. The replication of other folders and files are handled by v7 replication process.

Before Getting Started

Requirements and Best Practices

License Information

The pricing unit of AhsayCBS Replication Server module is per device to be replicated. If you will replicate to another AhsayCBS, a CBS module license will also be required.

For inquiries please contact the Sales team at Ahsay by email at sales-kb@ahsay.com or call our International Sales Hotline +852 3580 8091.

Version / Platform Compatibility

While AhsayCBS can be deployed on Windows, Linux, FreeBSD, or Solaris x64 platform, it should be noted that only some of the version and platform combinations are supported as illustrated below.

Backup Server		Replication Server		Compatible?
Version	**Platform**	**Version**	**Platform**	
V7	Windows	V7	Windows	**Yes**
V7	Linux/FreeBSD/Solaris x64	V7	Linux/FreeBSD/Solaris x64	**Yes**
V7	Windows	V7	Linux/FreeBSD/Solaris x64	**Yes**
V7	Linux/FreeBSD/Solaris x64	V7	Windows	**No***
V6	Windows	V7	Linux/FreeBSD/Solaris x64	**Yes**
V6	Linux/FreeBSD/Solaris x64	V7	Windows	**No***

** The incompatibility is a result of the limitations on Windows operating systems handling of Linux file/folder naming conventions.*

Replication Server Storage Requirement

There is a possibility that after your backup data is replicated to replication server, the final data size on the replication server may be larger than the original data size on backup server. This situation could arise if there are differences in the way each respective storage device is formatted, i.e. different default block sizes or different files systems.

Your retention policy settings would also determine the storage required on the replication server. You will need to weight the advantages of using smaller **Restore Point Interval** which allows for a greater chances of recovery and or the **Retention Customization Policy** setting is configured for a large number of days against your replication server storage limitations.

Considering the factors mentioned above, the disk capacity of your replication server should by default be greater than your backup server to accommodate the replication data.

Location of the Replication Server

In terms of disaster recovery situation, the restore media should not be stored or located on the same premises, and these rules would also depend on different compliances, regulations or terms with your customers.

Here are some suggestions that you may need to consider:

- Set up the AhsayCBS Replication Server in another data center. In case you need to host the Replication Server with your Backup Server, you may consider hosting it in another server rack or another server room if possible.

  - **Dedicated Server for Replication**

    Following are the pros and cons on setting up replication on a dedicated server.

    Pros:

    - Able to switch from Replication Server to Backup Server
    - Fast in recovery hence small recovery window and short downtime
    - Able to keep replicated snapshots in retention area in case recovery of data in past snapshots becomes necessary

    Cons:

    - Relatively more complex setup; requires datacenter hosting and maintenance cost
    - Relatively expensive to expand storage
    - Downtime required for regular maintenance and upgrade
    - Upfront investment in hardware storage

  - **Predefined Destination (Cloud Storage / FTP / SFTP) for Replication**

    Following are the pros and cons on setting up replication on a predefined destination.

    Pros:

    - Quick setup; low hosting and maintenance cost
    - Cheaper cost for storage expansion
    - No upfront hardware investment required

    Cons:

    - To recover the replicated data, it is required to set up new backup server and restore data from the predefined destination
    - Slow in recovery hence large recovery window and longer downtime.

For more information and comparison on different replication environment setup, please refer to the Appendix G.

AhsayCBS Replication Partitioning

The AhsayCBS replication module makes heavy use of the **User Home** directory to process the snapshots of the backup sets during the Resync stage. During Resync stage, snapshots of backup sets will be written to the User Home in the form of transactions log files.

It is not recommended to use the O/S partition or drive as the System Home. If the System Home folder fills up, this will cause your O/S to become unstable and may even crash your AhsayCBS server. It is strongly recommended the System Home directory should be located on a dedicated local drive.

Replication Performance Tuning

The connection speed between the backup server and the replication location (whether it is an AhsayCBS server or a cloud storage) is typically the primary factor of the replication performance. However, even with a fast and stable connection between the backup server and replication location, the replication performance could be affected by the following factors:

- Poor disk I/O on the backup server – when scanning and retrieving data files to be sent to the replication server.
- Poor disk I/O on the replication server – when receiving and committing files to the receiver home.

  Poor disk I/O can be attributed to:

  - The use of network drives as AhsayCBS user and system homes on the backup server side
  - The use of network drives as AhsayCBS receiver home(s) on the replication side.
  - The use of a single large disk or volume for AhsayCBS user home.
  - The use of a single large disk or volume for multiple AhsayCBS receiver home(s) on the replication side.
  - Slow performing local hard drives or storage devices.

  In order to improve overall replication performance, the following is recommended:

  - A separate local drive for each AhsayCBS user home on the backup server side
  - Distributing user accounts across multiple user homes to balance the I/O load
  - A separate local drive for AhsayCBS system home on the backup server side
  - A separate local drive for each receiver on the replication side

AhsayCBS Java Heap Size Setting

The machine with the Replication server installed may require more memory for additional feature such as retention policy to run.

- For a replication server with single receiver, a maximum Java heap size setting of at least 1024M is recommended.
- For a replication server with multiple receivers, a maximum Java heap size setting of at least 2048M is recommended.

When setting the maximum Java heap size for the replication server, please ensure this value does not exceed 50% of the RAM on the server, to allow sufficient memory for O/S processes and operations.

It is not recommended to set excessively high values for the maximum Java heap size, as this could result in performance issues on the replication server during internal Java VM garbage collection or memory recycling routines.

Firewall Settings

Since replication is performed via the http/https ports defined on the AhsayCBS backup server, after you have finished setting up your replication server, please ensure you have updated your firewall settings to allow network traffic through the those ports, which are typically **port 80** for **http** and **port 443** for **https**.

Don't Deploy the Backup and Replication Servers on a Single Machine

It is not recommend to configure and use both services on one single machine because it will completely defeat the purpose of the replication service as a backup or standby server for your backup server.

Moreover, the two services will compete for system resources, such as CPU and memory. This could affect the performance and stability of your backup service.

Dedicated Restore Drive on Replication Server

In order to facilitate a fast restore of snapshots from the retention area on the replication server, it is recommended the files are not restored to an existing receiver home drive to avoid affecting replication performance. Your replication server should be configured with a dedicated disk for restore purposes. Alternatively, an external USB drive can also be used.

Storage Requirement on Replication Server

The amount of space required to keep these replication depends on the amount of data changed on your Backup Server.

To calculate the amount of storage required for the retention settings, we can base on the following assumption and formula.

Assumption
There is a 2% data change in the backup server daily.
Formula
Total data storage required = $(1+0.02)^n$ x original data size, where **n** = number of days of the retention customization policy For n=30 days, it will be around 1.81 times of the original data size, and 3.28 times if n=60.

Replication Server with Multiple Receivers

If you have configured multiple receivers on your replication server to server more than one backup servers, it is recommended that each receiver is located on its own individual disk. The major advantage of this kind of setup is that it will minimize the I/O on each disk and therefore improve the replication performance.

Replication Using Cross Over Cable

It is not recommended to set up a connection between the backup server and replication server using a cross over cable. As from our experience this setup will result in connection and performance issues.

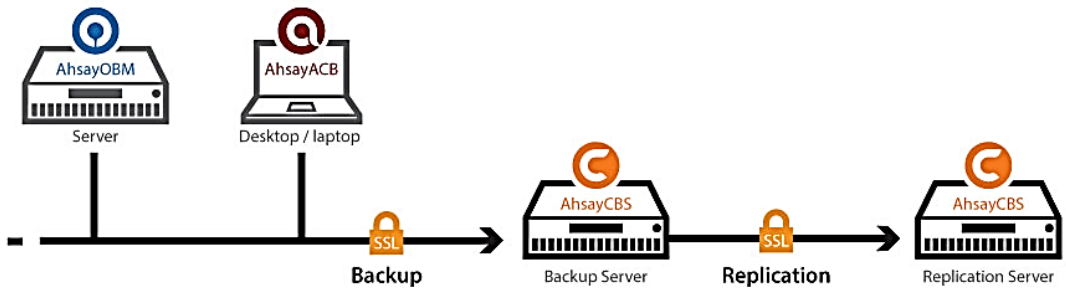
If the backup server and replication server are located on the same site, they should be connected via a switch.

Deployment Options and Comparison

There are three major methods to deploy the replication service. This chapter presents you with all the available deployment options, deployment combination and features comparison on different deployment methods, to help you decide which option to use.

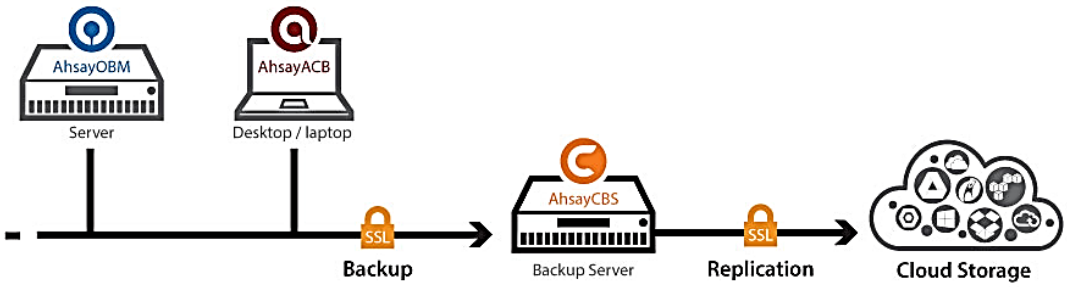
Deployment Method

There are three methods to deploy the replication service as described below.

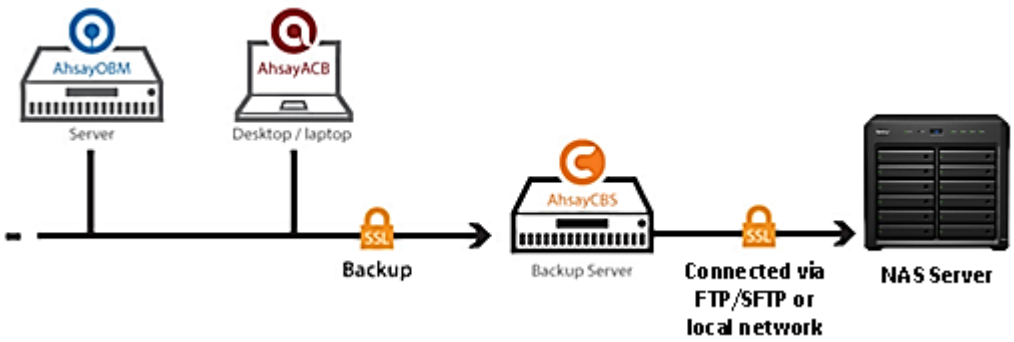
<table>
<tr><th colspan="2">Method 1 (Recommended) – Deploy on a single AhsayCBS Backup Server replicate to another AhsayCBS Replication Server</th></tr>
<tr><td colspan="2">Introduction</td></tr>
<tr><td colspan="2">This is the typical deployment option, as well as the most recommended one, which features replication between a single AhsayCBS backup server and AhsayCBS replication server.</td></tr>
<tr><td colspan="2">System Architecture</td></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td colspan="2">Requirement</td></tr>
<tr><td colspan="2">Set up a new machine where you wish to host the replication server, and install AhsayCBS on it. In other words, you will have two AhsayCBS services running. One on the backup server, and the other on the replication server where you would like to have the backup data replicated to.</td></tr>
<tr><td colspan="2">Pros</td></tr>
<tr><td>Speed for Replication and Restore</td><td><u>Multiple Threads Replication</u>
Multiple threads replication is supported to improve the replication speed. The actual number of threads that are available for use depends on the CPU power of the backup server. The more CPU cores the backup server has, the more threads it will have for replication. Refer to Multiple Threads Replication for more details.

<u>High Hardware Performance for High Replication Speed</u>
A direct attached storage and SAN storage would provide good replicating speed.</td></tr>
</table>

Recovery	**Fast Recovery in a Few Clicks** In case of a backup server outage, the replication server can be switched as the backup server in a short time to minimize the system down time and interruption to backup users. For instructions to switch a replication server to backup server, refer to Method 3 - Startup Replication Server as Backup Server.
Cons	
Cost	**Higher Cost** ➢ Setup cost is higher ➢ Cost for hardware storage expansion is relatively higher Although this option involves higher setup cost, consider the higher replication/restore speed and recovery switching, it may be worth the investment.
Storage Provisioning	**Slower Storage Provisioning** Compared to cloud storage deployment, it takes more time and effort to assign the additional storage acquired when you need to expand the hardware storage.

Method 2 – Deploy on a single AhsayCBS Backup Server replicate to a Predefined Destination
Introduction
This deployment option allows you to replicate your backup data on the backup server to a cloud storage, local/mapped drive/removable storage, or FTP/SFTP server. Refer to the list below for all the available redefined destination options.
System Architecture
Method 2a – Cloud Storage as Replication Destination connected via Internet


Method 2b – NAS Server as Replication Destination connected via FTP/SFTP or local network



Requirement

First, you need to have cloud storage account, a local/network/removable drive, or a FTP/SFTP server in place. Then, the predefined destination must have been set under the **System Settings** > **Predefined Destinations** menu so it can be used for the replication purpose.

Available Predefined Destinations

Aliyun (阿里云)	CTYun (中国电信天翼云)	Amazon Cloud Drive	Amazon S3
Amazon Compatible Cloud Storage	Google Cloud Storage	Google Drive	Microsoft Azure
OneDrive	OneDrive for Business	Rackspace	OpenStack
Dropbox	FTP	SFTP	Local / Mapped Drive / Removable Drive

Pros

Multiple Threads Replication	Multiple threads replication is supported to improve the replication speed. The actual number of threads that are available for use depends on the CPU power of the backup server. The more CPU cores the backup server has, the more threads it will have for replication. Refer to Multiple Threads Replication for more details.
Cost	**Low Cost** ➢ Setup cost is low ➢ Cost for storage expansion, especially on cloud storage, is relatively cheaper

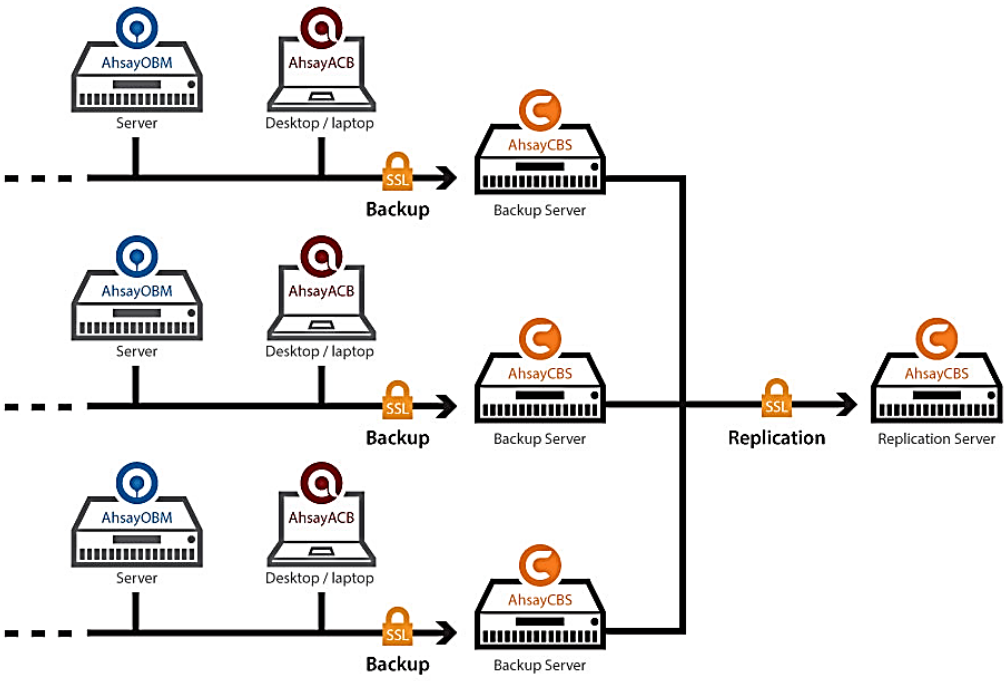
Cons	
Speed of Replication and Restore	**<u>Slower Upload Bandwidth</u>** The replication and restore speed is subject to the connection speed to the predefined destination, and administrator may not always have control over the bandwidth.
Recovery	**<u>Longer Recovery Process</u>** There is no quick way to restore the replicated data from the predefined destination to the backup server. To recover the replicated data on a predefined destination, you have to: 1. Setup a new machine. 2. Install Ahsay CBS. 3. Download the replicated files from the predefined destination back to the Backup Server.

Method 3 – Deploy on multiple AhsayCBS Backup Servers replicating to another AhsayCBS Replication Server

Introduction

This deployment option allows you to replicate backup data from multiple AhsayCBS backup servers to an AhsayCBS Replication Server.

System Architecture



Requirement	
Set up a new machine where you wish to host the replication server, and install AhsayCBS on it. In other words, you will have multiple AhsayCBS services running. Each backup server runs on its own license, while the replication server where you would like to have the backup data replicated to requires another license as well.	
Pros	
Cost	**Lower Setup Cost** You only require to have one replication server to accommodate replication from multiple backup servers, instead of one-to-one replication between backup server and replication server.
Single Replication Point Management	With only a single replication server, this deployment option allows you to centrally manage the replication settings and view replication status on the replication server web console, As opposed to the Method 1 deployment where you have to access multiple AhsayCBS web console pages for settings and management.

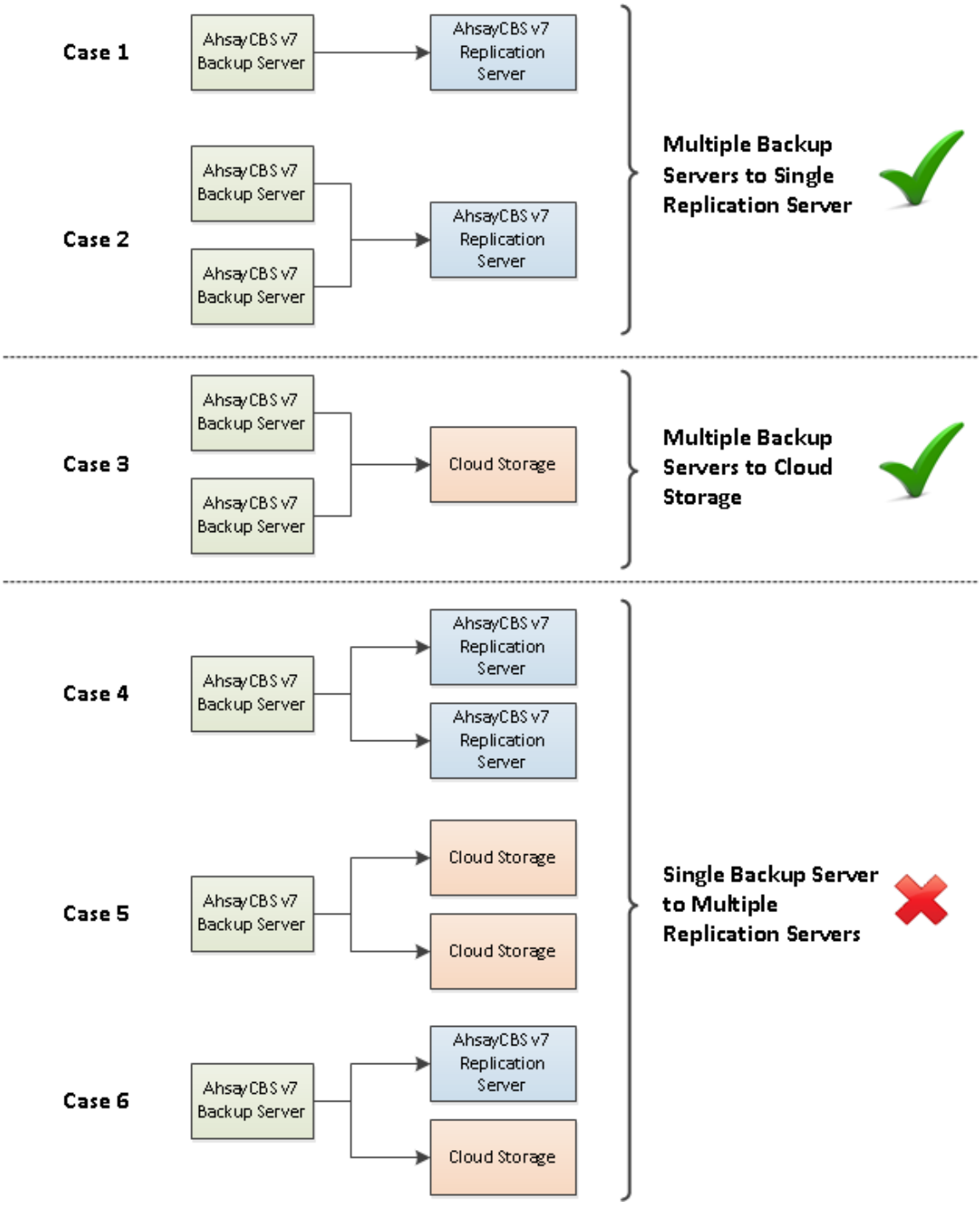
Comparison between Deployment on AhsayCBS and Cloud Storage

	Deploy on AhsayCBS Replication Server	Deploy on Cloud Storage
Replication Retention	✓	✘
The replication server creates snapshot of the replication data. Under the Replication Retention configurations, **Restore Point Interval** can be configured to define the number of days between each retention snapshot; **Retention Customization Policy** can be configured to define the number of days before an existing retention snapshot is removed from the replication server. Click here to see details of this configuration.		
Startup Replication Server as Backup Server	✓	✘
This feature allows you to quickly convert your AhsayCBS replication server into AhsayCBS backup server in the event of a backup server down, so that you can keep serving the backup users to minimal impact to your business. Refer to Method 3 - Startup Replication Server as Backup Server for detailed steps to perform this recovery.		
Replicate Multiple Backup Servers	✓	✓
It is possible to replicate backup data from multiple AhsayCBS backup servers to another AhsayCBS replication server or cloud storage. This gives you the convenience of hosting backup data of multiple backup servers in one single replication server for the purposes of cost saving and easier management. Refer to Deployment Combinations of Backup and Replication Servers for more details.		

Support v6 Backup Set Replication	✓	✘
This feature gives you the flexibility to back up not only v7 format backup sets, but also the v6 ones to the replication server, before the v6 format backup sets undergo the data migration process. Refer to Replication of v6 backup sets on AhsayCBS v7 for further details.		
Quick Storage Provisioning	✘	✓
As time goes by, your replication data may fill up the capacity on your AhsayCBS replication server or cloud storage and you will have to expand the storage capacity to accommodate the replication data. Comparing to AhsayCBS deployment, cloud deployment allows a hassle-free storage upgrade where you only have to pay your cloud storage service provider to get the upgrade done.		
Upfront Hardware Investment	✓	✘
Depending on your organization's budget on deploying the replication service, it is generally more cost-saving to deploy the replication service on cloud storage instead of the AhsayCBS as you do not need to invest on hardware and hosting upfront.		

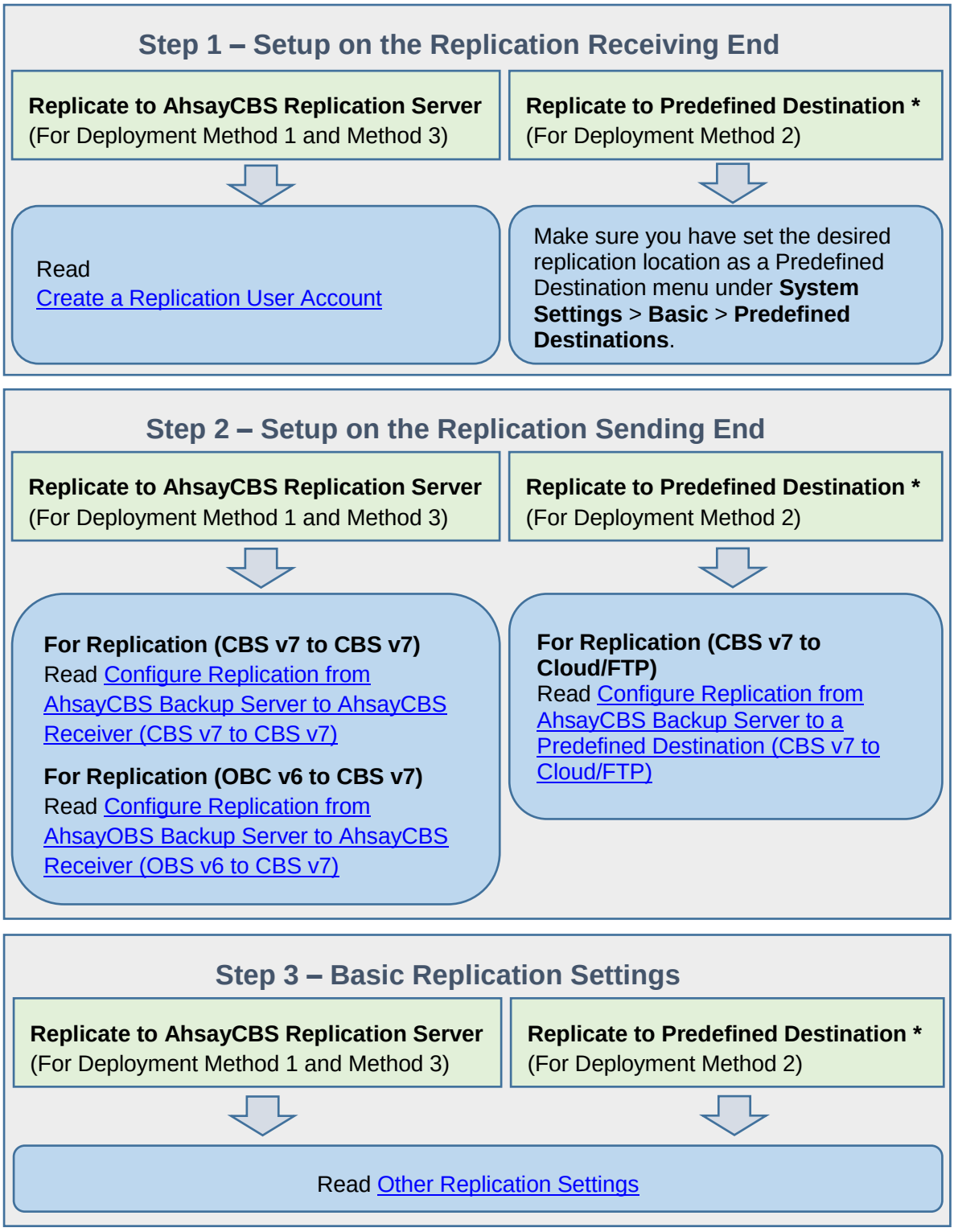
Deployment Combinations of Backup and Replication Servers

It is only possible for a single replication server or cloud storage to host replication data from multiple backup servers, but not the other way around, i.e. a single backup server replicating to multiple replication servers or cloud storage destinations. Refer to the illustration below for details on the possible deployment combinations.



Deployment

Major Steps to Deploy a Replication Service



* Replication to Predefined Destination **DOES NOT** support deployment for v6 backup sets on CBS v7

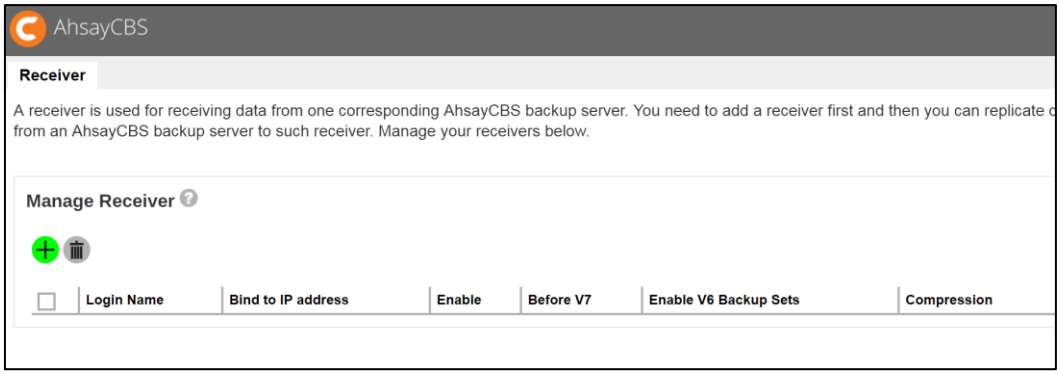
Configuration on the Replication Receiving End

Create a Replication User Account

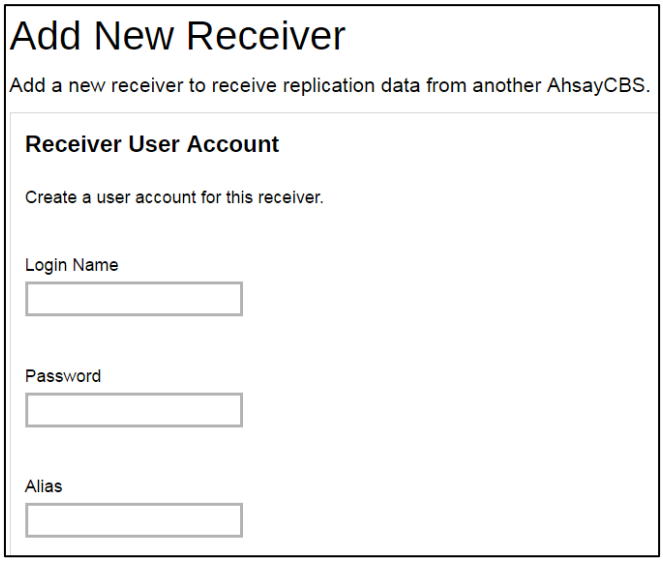
Before an AhsayCBS/AhsayOBS backup server can replicate backup data to another AhsayCBS replication server, a receiver user account must be created on the AhsayCBS replication server first. Follow the steps below to create a replication receiver account.

1. Log in to the web console on the replication receiving end, go to **Replication > Accepting Data**.

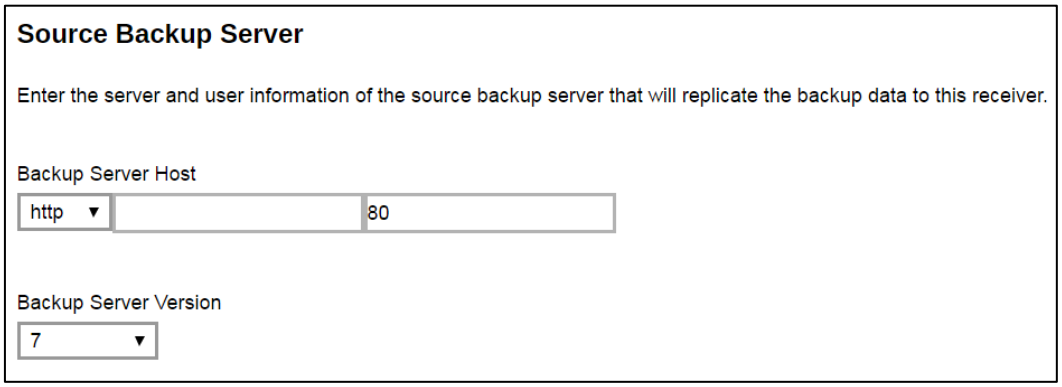
2. Click the **Create** (**+**) button in the **Manage Receiver** section. The **Add New Receiver** page appears.



3. Set the login name, password and alias of the receiver account.



4. Configure the source backup server host settings, including the http/https protocol, source backup server host name and port number.



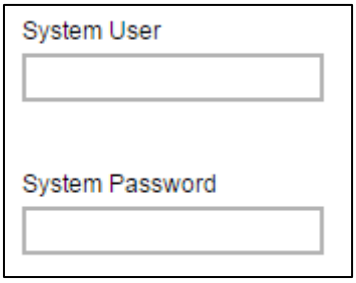
Backup Server Host – IP address / host name of the backup server

Backup Server Version – select the source backup server version.

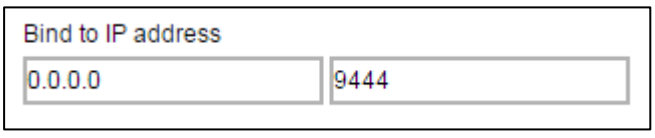
- If you select **7**, it means the source backup server is an AhsayCBS version 7 backup server.

  If you have upgraded your backup server to v7 from v6, and still wish to replicate backup sets in v6 format before they are migrated to v7 format, make sure you select **7** in this menu.

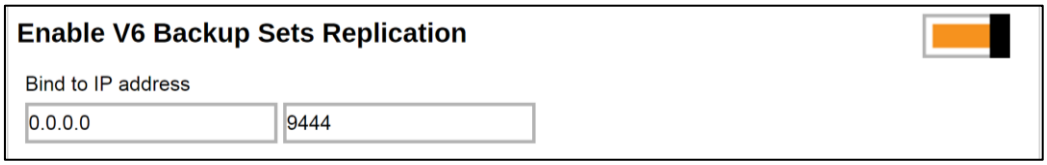
  - **System User** – the system user login of the source backup server
  - **System Password** - the system user password of the source backup server



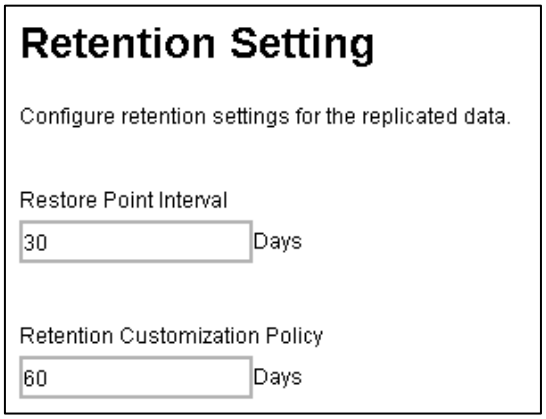
- If you select **Before 7** as the backup server version, enter the bind to IP address and the replication port. "0.0.0.0" and "9444" are the default values, you can assign a specific IP if you have multiple network cards. For multiple backup servers' replication, a unique replication port number is required to set, such as "9444".



5. Switch the **Enable V6 Backup Sets Replication** on if you will replicate v6 backup sets to the replication server.



6. Configure the retention settings for the replicated data.



- **Restore Point Interval** – defines the number of days before new snapshot of the replicated data will be taken and stored in the retention area. A retention snapshot will be taken only when the following two conditions are met:
  - There is data received from the backup server
  - Restore Point Interval has reached

  No retention snapshot will be taken if there is no data received, even when the Restore Point Interval has reached.

- **Retention Customization Policy** – defines the number of days the old snapshot copies to be retained in the retention area.

7. Click the icon at the bottom right corner to proceed when you are done with settings.

8. Set the default home directory for this replication, and set up the path to store the user homes.

   - The following is an example of a v7 receiver setup. In v7 receiver setup, you will be able to configure the default home directory, as well as replication home directory for individual backup server user home.

NOTE

If AhsayCBS is receiving multiple backup servers, please use unique path for each receiver's "Replication Home".

   - In v6 receiver, you can only set up the default home directory.

NOTE

It is recommended to configure the default home directory to a non-system drive (i.e. not C:\ drive), especially when there are v6 backup sets, as the replication transaction log files may fill up the disk space and cause the operating system become unstable.

9. Click and at the bottom right corner to confirm the configuration.

Editing Replication Receiver

You can edit the configurations of the replication receiver after it has been set up.

1. Go to **Replication > Accepting Data** on the AhsayCBS web console on the replication receiver side.

2. Click on the replication receiver account under the **Manage Receiver** section which you wish to edit configurations for.

3. Revise the desired replication receiver item, then click and at the bottom right corner to confirm the changes.

Configuration on the Replication Sending End

Enable and configure the replication feature on the backup server side by following the corresponding sub-chapter below depending on the backup server version or replication destination.

AhsayCBS v7 Backup Server to AhsayCBS v7 Receiver

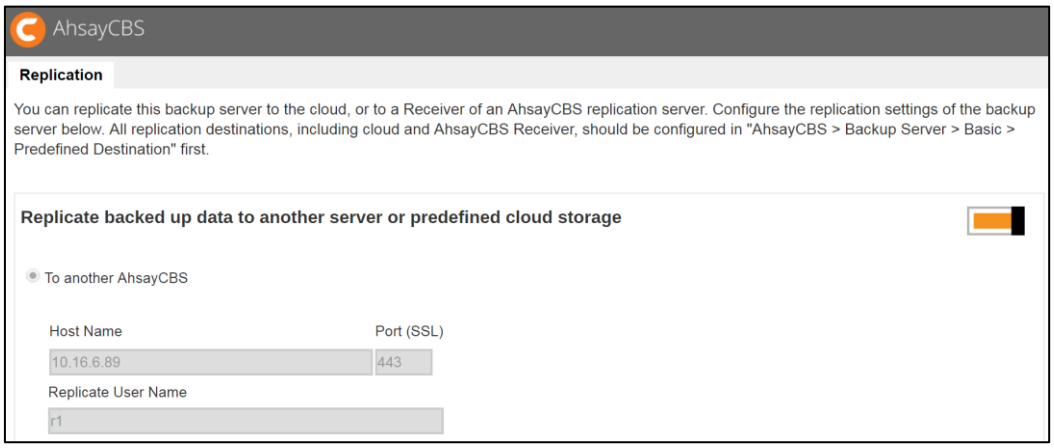
The following example is a v7 (backup server) to v7 (replication server) replication setup. For earlier version setup, please refer to Configure Replication from AhsayOBS Backup Server to AhsayCBS Receiver (OBS v6 to CBS v7) for details.

Note: If you will replicate v6 backup sets on CBS v7 server to another CBS v7 replication server, follow the steps below for setup and make sure you turn on the **Replicate v6 backup sets to v7 server** option in step 7.

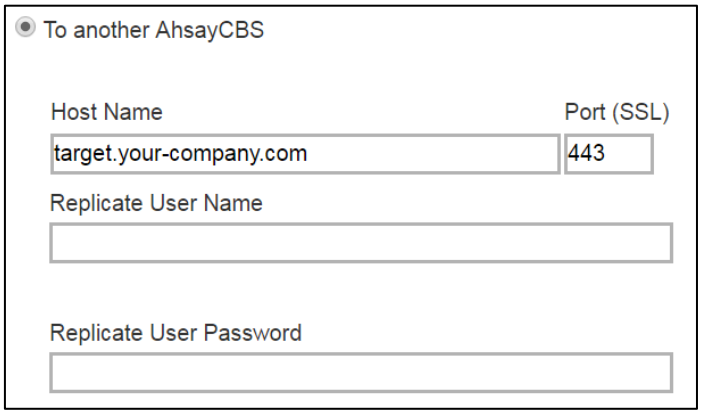
1. Make sure you have created a replication receiver account on the receiving end of the AhsayCBS server first. Refer to Create a Replication User Account for detailed instructions.

2. Click on the **Sending Data** icon under the Replication section on the AhsayCBS web console of the backup server.

3. Switch the Replicate backed up data to another server or predefined cloud storage on. The Replication configuration page shows as below.

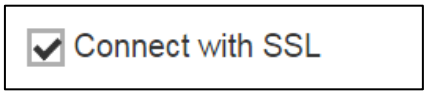


4. Select the **To another AhsayCBS** option, and then enter the **Host Name**, **Port**, **Replicate User Name**, **Replicate User Password** of the replication receiver.

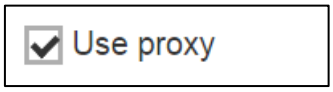


- **Host Name** – IP address or host name of the replication server with AhsayCBS installed
- **Replicate User Name** – the username of the receiver created on the AhsayCBS replication server
- **Replicate User Password** – the password to log in to the receiver create don the AhsayCBS replication server.

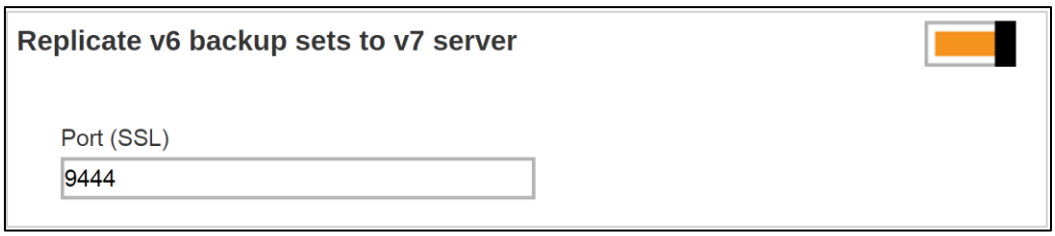
5. Check the Connect with SSL checkbox if you need to connect to the replication server with SSL.



6. If proxy is required to access the replication server, mark the **Use proxy** checkbox.



7. If there are backup sets in v6 format to be replicated to the replication server, make sure you switch the **Replicate v6 backup sets to v7 server** on. The default port is set as "9444".



8. If you wish to configure the following replication settings, refer to Other Replication Settings.

- **Traffic limit for replication** – which limits the amount of bandwidth used by replication.
- **Selectable backup set for replication** – which allows you to choose individual backup set from selected users for replication.

- **Concurrent backup set for replication** – which allows you to configure the maximum number of backup set allowed for replication at the same time.

- **Cyclic Redundancy Check (CRC) Checking** – which allows you to enable this checking to run automatically for verifying the integrity of the replicated data.

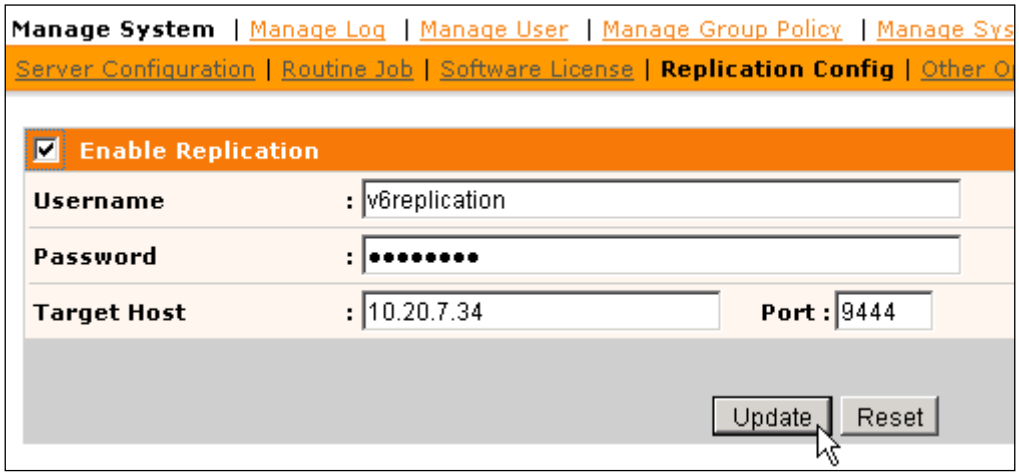
9. Click the icon at the bottom right corner to confirm the configuration.

AhsayOBS v6 Backup Server to AhsayCBS v7 Receiver

It is suggested to upgrade your v6 backup server to v7 so that you can enjoy the latest features provided by the AhsayCBS. If you still wish to continue using the v6 backup server to replicate to a v7 receiver, follow the steps below for configuration of the v6 backup server.

1. Make sure you have created a replication receiver account on the receiving end of the AhsayCBS server first. Refer to Create a Replication User Account for detailed instructions.

2. In your backup server, navigate to **Manage System** -> **Replication Config**, then enter the username, password, target host and connecting port.



3. Click **Update** to confirm the settings.

NOTE

The index files stored in the v6 backup server will not be replicated to the AhsayCBS (Replication Server) nor any cloud storage.

There is no multiple threads replication.

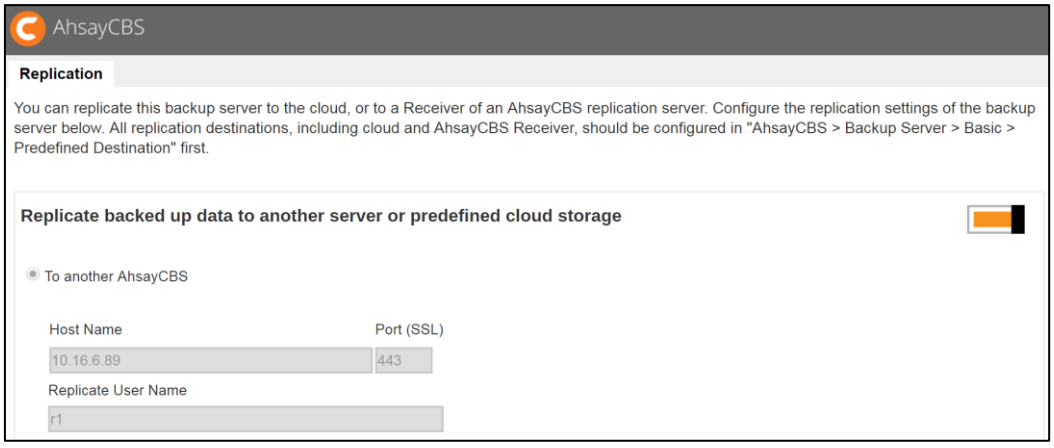
The AhsayCBS replication server cannot be started as a v6 backup server.

AhsayCBS v7 Backup Server to a Predefined Destination

1. Make sure you have created a replication receiver account on the receiving end of the AhsayCBS server first. Refer to Create a Replication User Account for detailed instructions.

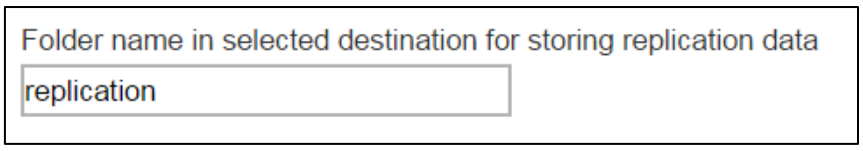
2. Click on the **Sending Data** icon under the Replication section on the AhsayCBS web console of the backup server.

3. Switch the Replicate backed up data to another server or predefined cloud storage on. The Replication configuration page shows as below.

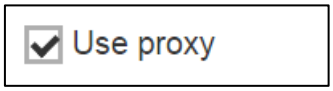


4. Select the **To a predefined destination** option as shown below. You will then see a list of predefined destination you have set under the **System Settings** > **Basic** > **Predefined Destinations** menu.

5. You can configure the folder name in the selected predefined destination to store the replication data.



6. If proxy is required to access the replication server, mark the **Use proxy** checkbox.



7. If you wish to configure the following replication settings, refer to Other Replication Settings.

   - **Traffic limit for replication** – which limits the amount of bandwidth used by replication.
   - **Selectable backup set for replication** – which allows you to choose individual backup set from selected users for replication.
   - **Concurrent backup set for replication** – which allows you to configure the maximum number of backup set allowed for replication at the same time.
   - **Cyclic Redundancy Check (CRC) Checking** – which allows you to enable this checking to run automatically for verifying the integrity of the replicated data.

8. Click the icon at the bottom right corner to confirm the configuration.

Other Replication Settings

The following replication settings can only be set when the replication feature has been enabled on the AhsayCBS backup server.

Traffic Limit

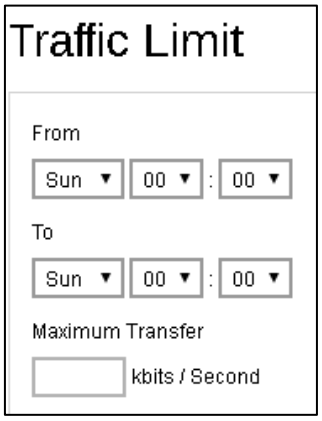
This is an optional setting that allows you to limit the amount of bandwidth used by replication traffic between a specified periods of your choice.

1. Click on the **Sending Data** icon under the Replication section on the AhsayCBS web console of the backup server.

2. Click the button in the **Set traffic limit** section to turn the replication feature on. You will then see the configuration menu as shown.

3. Click on the icon for configuration.

4. You will then see the configuration page as shown.



- **From** – set the start time to apply the traffic limit by selecting a day of the week and time in hh:mm (24-hr format)
- **To** – set the end time to apply the traffic limit by selecting a day of the week and time in hh:mm (24-hr format)
- **Maximum Transfer** – set the maximum bandwidth allowed for data transfer in the format of kbits /second.

5. Click the icon then the icon at the bottom right corner to confirm the changes.

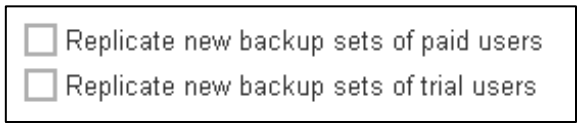
Replicate Individual Backup Sets

By default, all backup sets of all users on all use homes will be replicated to the replication location (either another AhsayCBS or a predefined destination). However, it is possible to select specific backup users and their specific backup sets for replication.

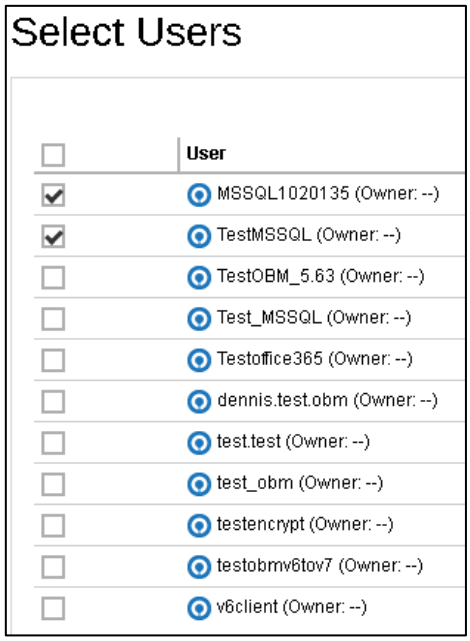
1. Click on the **Sending Data** icon under the Replication section on the AhsayCBS web console of the backup server.

2. Click the button in the **Replicate individual backup sets** section to turn the replication feature on. You will then see the configuration menu as shown.

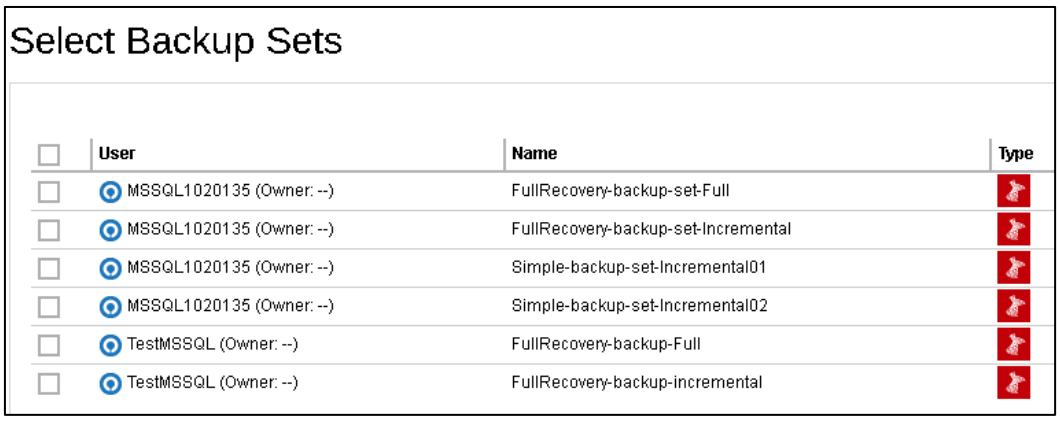
3. Firstly, you can set to replicate the backup data of either the paid users or trial users, or both by checking the corresponding checkbox(s).



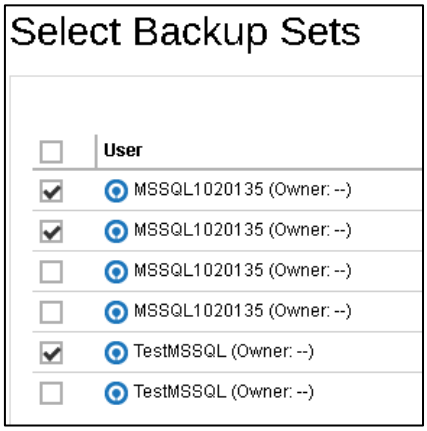
4. Now, you can start selecting specific backup sets(s) to replicate. Click on the icon to select the desired backup users first. Multiple selections is possible. Click on the icon at the bottom right corner to proceed when you are done with the selection.



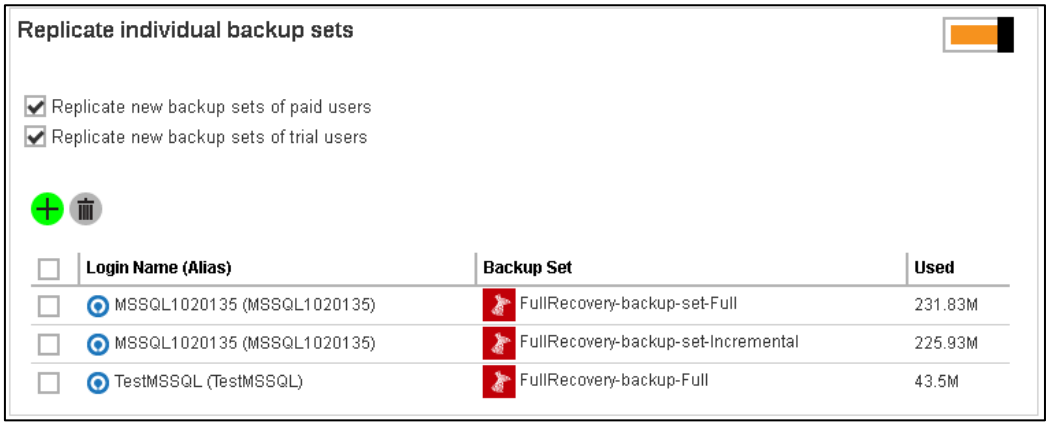
5. You will then see a page listing all the backup sets of the backup user(s) you have selected from the last step. Each individual row shows the name of the backup user, the name of the backup set, and the backup set type in the corresponding icon.



6. Select the desired backup sets by clicking the corresponding checkbox, then click the icon at the bottom right corner to confirm the selection.



7. You will then see the selected backup sets being added to the **Replicate individual backup sets** section as shown if they are added successfully. Each row of the entry shows the corresponding backup user name, backup set name and the size of the backup set.

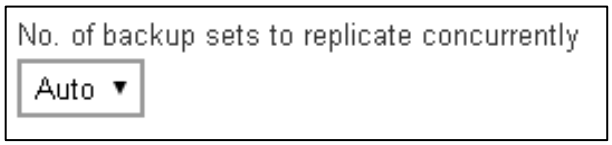


8. Click the icon then the icon at the bottom right corner to confirm the changes.

Setting the Number of Backup Sets to Replicate Concurrently

You are able to change the number of backup sets to replicate concurrently on the AhsayCBS backup server web console under **Replication > Sending Data**.

Under the Replicate backed up data to another server or predefined cloud storage section, there is a drop-down menu for the No. of backup sets to replicate concurrently setting.



If you are running on an 8-core CPU, then the number of concurrent backup set to replicate is 4. When you use the default values **Auto**, it will allow your replication to run with 4 concurrent backup sets. In case you find the replication causing performance issues such as hard disk I/O or network bandwidth, you may adjust the concurrent backup set value from the drop- down menu as highlighted above.

NOTE

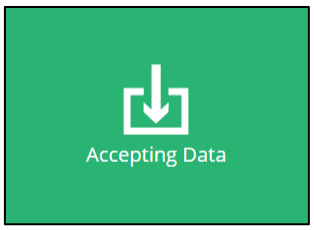
The multiple threads feature supports the backup set that is created/converted in V7 format. This feature does not support users who are still using v6 backup clients, as their backup sets are still using the legacy v6 backup set data format. Refer to the Backup Data Migration section for further information on converting backup set format.

Cyclic Redundancy Check (CRC) Checking

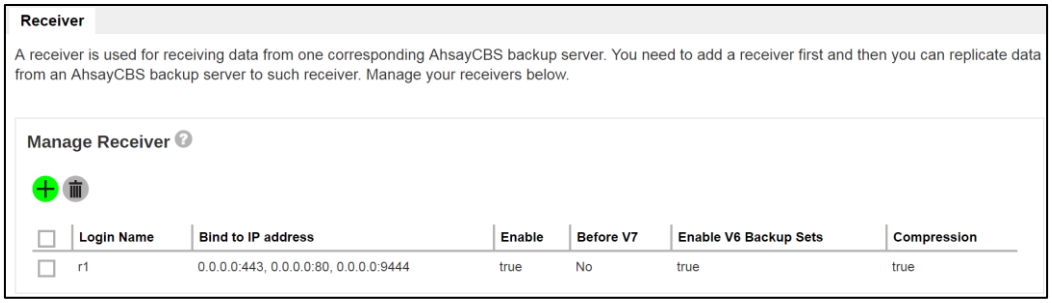
The **Cyclic Redundancy Check (CRC) Checking** job will check all new files replicated to the AhsayCBS receiver since the last CRC job. This checking can be run automatically for verifying the integrity of the replicated data.

A replication receiver must have been set before you can enable the Cyclic Redundancy Check (CRC) Checking.

1. Click on the **Accepting Data** icon under the Replication section on the AhsayCBS web console of the backup server.

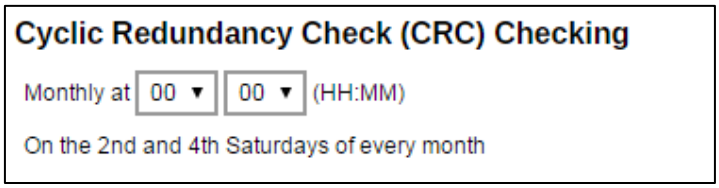


2. Click on the receiver which you wish to enable the CRC checking feature.



3. Scroll to the **Cyclic Redundancy Check (CRC) Checking** section and switch on the feature by sliding the icon on the right.

4. The CRC checking is set to run on the second and forth Saturdays of every month by default. You can configure the time for the checking to run on the specified dates.



5. Click the icon then the icon at the bottom right corner to confirm the changes.

Recovery Process Overview

After you have deployed the replication server, data from the backup server will be replicated to the replication destination you have selected. In the event of a system down on your backup server, or you wish to retrieve deleted data from the replication destination, you can recover the configurations and backup data replicated from the backup server by using any one of the recovery methods below.

Method 1 – Rebuild AhsayCBS from Replication

Introduction

This recovery method rebuilds the AhsayCBS by extracting AhsayCBS configuration, system files, user profiles and backup data from the replication destination then restoring it either to the Backup Server or restoring the raw data alone using a Backup Client Agent (AhsayOBM / AhsayACB).

Steps

Step 1: Confirm Replication Status by Checking Replication Logs

Step 2: Extract Data from Replication Destination

- From AhsayCBS Replication Server
- From a Predefined Destination - Cloud storage
- From FTP/SFTP
- From Local/Mapped Drive/Removable Drive
- From v6 Replication
- From Snapshot in Retention Area

Step 3: Restore replication data extracted from the previous step using either method below

- Restore Data to the Backup Server

  -OR-

- Restore the Raw Data Alone using a Backup Client Agent

Pros

Selective Backup Set Restore
After extracting the backed up data from the replication destination, you have the flexibility to restore only the selected backup sets from selected backup users, instead of restoring all data at once.

Restore as Raw Data
Instead of restoring the backed up data to the backup server, you can only restore the raw data by using a client backup agent (AhsayOBM / AhsayACB).

Cons

Relatively Time and Effort Consuming
As opposed to Method 3 where you can quickly convert the replication server as backup server, this recovery method takes more time and effort to rebuild the backup server.

Method 2 – Rebuild from Auto Save

Introduction

This recovery method only restores the AhsayCBS configuration, system files and user profiles but not the users' backed up data. Users' backed up data will have to be re-uploaded again to complete the recovery.

Steps

Step 1: Select the desired Auto Save snapshot by date

Step 2: Select the desired configuration and/or user profile

Step 3: Override the existing configuration files

-OR-

Manually restore the configuration files

Step 4: Restart AhsayCBS service

Refer to Method 2 - Rebuild from Auto Save section for detailed steps.

Pros

Quick Rebuild of AhsayCBS
AhsayCBS can be quickly rebuilt by applying only the configuration files and user profiles.

Cons

Longer Time to Re-upload Backup Data
Since the users' backup data is not restored and required to be re-uploaded again, it is going to take a longer time to complete the whole recovery process.

Method 3 – Start up Replication Server as Backup Server

Introduction

This recovery method allows you to quickly convert AhsayCBS in replication receiver mode to a backup server. This is a quick and direct way to access your backup data in the event of a system down on your backup server.

Steps

Refer to Method 3 - Startup Replication Server as Backup Server for detailed steps.

Pros

Fastest Recovery
This recovery method is the fastest way to turn the replication server as a backup server so as to minimize the system down time in the event of a backup server disaster.

Recovery Methods

Method 1 - Rebuild AhsayCBS from Replication

1. Set up a new AhsayCBS on a new machine with similar hardware specification, and sufficient hard disk space as the original backup server.

2. Make sure replication has been performed before you start restoring any replication data. Refer to To check replication logs on the Backup Server: and To check the replication logs on the Replication Server: for details.

3. Extract data in the 3 folders ("**conf**", "**system**" and "**user**") from the replication destination. Below are the links that can quickly direct you to the corresponding section for the detailed steps.
   - From AhsayCBS Replication Server
   - From a Predefined Destination - Cloud storage
   - From FTP/SFTP
   - From Local/Mapped Drive/Removable Drive
   - From v6 Replication
   - From Snapshot in Retention Area

4. Stop AhsayCBS server on the new machine.

5. To rebuild the AhsayCBS on the new machine by restoring the extracted data, continue to read through the rest of the steps in this section.

   -OR-

   To restore the backup raw data alone using a Backup Client Agent, disregard the steps below and skip to Restore Raw Data Using AhsayOBM / AhsayACB for further steps.

6. Copy all the contents in 3 folders backup to your new server as instructed below:
   - **system -> CBS_HOME\system**
   - **user -> CBS_HOME\user**
   - **conf\conf.zip -> CBS_HOME\conf**

   Note: *Expand the conf.zip first.*

7. Start the AhsayCBS server on the new machine after copying the data instructed above.

8. Logon to the AhsayCBS web management console.

9. You will notice that there is a license error. This is because your AhsayCBS is running on the new machine with hardware and settings changed. Please contact our support with your licensee name and license key. We shall relax the license for you. There is a 14 days grace period before the license deactivates.

Here is a list of suggested items to check after you started up your AhsayCBS.

1. Check SMTP settings in AhsayCBS web console by navigating to **System Settings** > **Basic** > **Email**.

2. Check all users' profile, backup and policy group settings in AhsayCBS web console by navigating to **Backup/Restore** > **Users, Groups & Policies**.

3. Check https connection to the AhsayCBS on different browsers (IE, Firefox and Chrome).

4. Connect AhsayOBM/AhsayACB to AhsayCBS with both http and https connections.

Method 2 - Rebuild from Auto Save

Comparing with the rebuilding from the replication server, this option can only restore the AhsayCBS configuration, system files and user profiles. Users' backed up data will not be restored and therefore users need to re-upload all backup data again on their next schedule backup.

So it is very important to configure a replication for your AhsayCBS if you need to restore everything that was originally on the Backup Server.

REMINDERS

1. As the system keeps only a maximum of 30 Auto Save snapshots on software vendor's cloud, if you want to keep these snapshot(s) on your server, you need to download these snapshots manually.
2. If you restore an earlier snapshot, all the snapshots beyond the restore date will not be able to restore again.

   Example: If today is Jan 21st 2016, after you restore the snapshot on Jan 19th, 2016, the snapshot on Jan 20th and Jan 21st will not be able to select from the dropdown list.

The table below shows all the major system configuration files that are saved on the cloud daily by the Auto Save system job:

Server Configuration	
Description	**Path**
Connector setting file	/conf/server.xml
CBS option files	/conf/afc.opt /conf/cbs.opt
Runtime setting file	/conf/cbssvc.ini
Default certificate files	/conf/ca.crt /conf/ssl.crt /conf/ssl.key
CBS setting files	/conf/cbs.json
Redirector configuration files	/conf/lfsConfig.xml
CBS Configuration	
Description	**Path**
Backup Server setting files	/conf/obs.json
License files	/conf/lic.json /conf/license.xml
CBS/OBS option files	/conf/cbs.opt
Autoupdate index	/conf/autoUpdate.bdb
Replication configuration files	/conf/rpsSend.xml

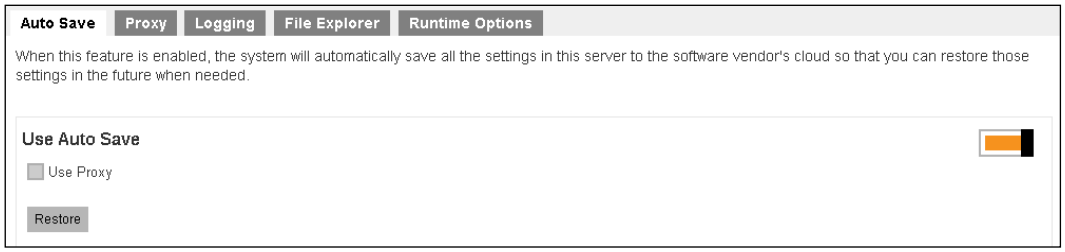
RPS Configuration	
Description	**Path**
Replication configuration files	/conf/rps.xml /conf/rpsRecv.xml /conf/rps-recv.json
RDR Configuration	
Description	**Path**
Redirector configuration files	/conf/rdr.xml /conf/rdr.json
License files	/conf/rdr-lic.json /conf/rdr-license.xml
CBS User Profile	
Description	**Path**
Users' profile	/conf/users.xml
Others	
Description	**Path**
Branding directory	/conf/Branding/*.*
User group definition	/system/obs/policies/userGroup.xml
Policy group definition	/system/obs/policies/policyList.xml

Please note that there are no options to restore the "Others" category, however it will be restored automatically every time when you need to restore the auto save files.

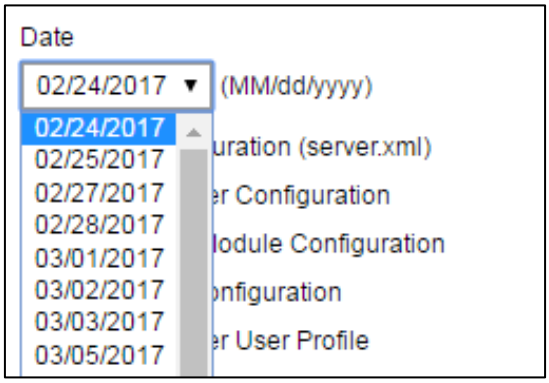
Steps to restore the Auto Save snapshot

1. Login to AhsayCBS management console, and go to **System Settings** -> **Advanced** -> **Auto Save**.

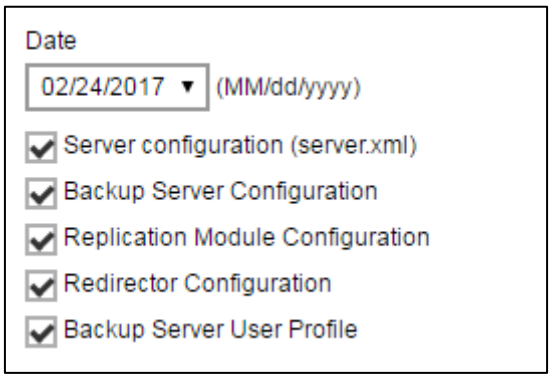
2. Turn on the **Use Auto Save** switch, then click on the **Restore** button.



3. Select the snapshot that you want to restore.



4. Select the items that you need to restore. Select all the items if you need to restore the configuration exactly on that restore point.



5. Click on the **Next** button.

6. Select to download the snapshot file or to overwrite the existing configuration.

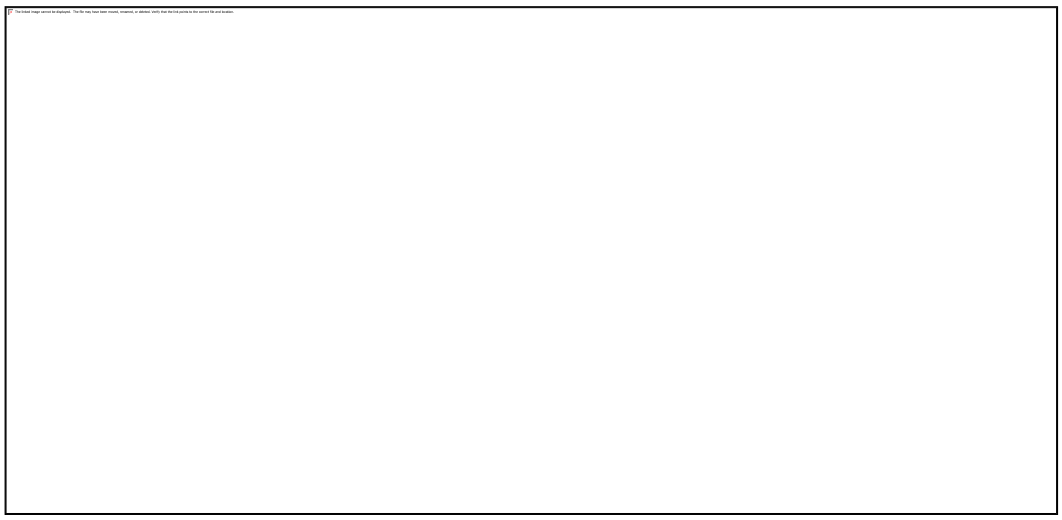
- In this example, we have selected the **Overwrite existing configuration files** option.
- Skip to the **Manual Restore** section below if you want to restore the downloaded file manually.

7. Click on the **Restore** button if you want to overwrite the existing configuration.

8. Restart the AhsayCBS service, and the configuration will be overwritten.

Manual Restore

1. Here is an example of the downloaded configuration file, it is named as dr-YYYY-MM-DD.zip date format.



2. (Optional) If you need to restore the file manually, you can unzip the 2 folders "**conf**" and "**policies**" into the **CBS_HOME\system\recovery**. After the restart of the AhsayCBS service, the configuration will be imported to the AhsayCBS.

Method 3 - Startup Replication Server as Backup Server

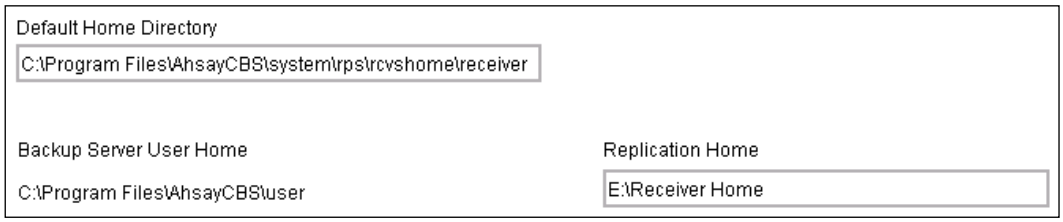
Refer to the following steps to convert your AhsayCBS in replication receiver mode to a backup server.

NOTE

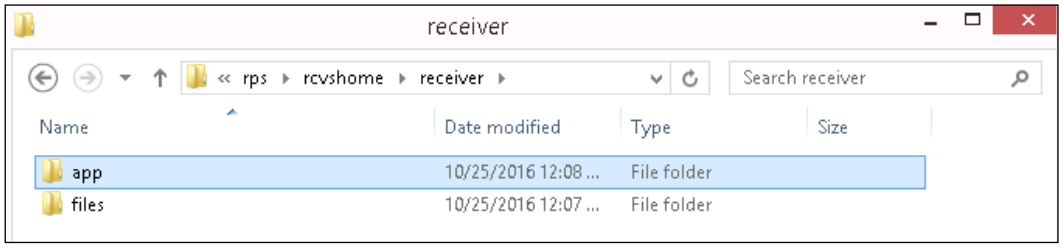
It is assumed that the first cycle of replication from the sender to the receiver had been completed.

1. Check on the Receiver's Setting by following the steps below, and make note of the **Default Home Directory** and **Replication Home** settings.

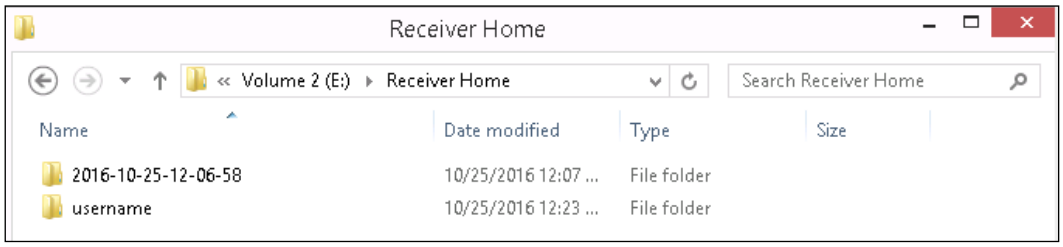
   - On the AhsayCBS in replication receiver mode, login to the AhsayCBS web console.
   - Confirm on the replication receiver's settings. Under **Replication**, select **Accepting Data**.
   - Check on the **Default Home Directory** setting, as well as the **Replication Home** setting.



Default Home Directory is where the replication sender's system home, user settings, and configuration settings are stored (in the app folder).



Replication Home is the location where users' backup data and logs are stored.



In the example above, the following settings are used:

- Default Home Directory is set to:
  C:\Program Files\AhsayCBS\system\rps\rcvshome\receiver
- Replication Home is set to:
  E:\Receiver Home

2. Configure the Software License by following the steps below.

   - On the AhsayCBS in replication receiver mode, login to the AhsayCBS web console.
   - Under **System Settings**, select **Licenses**, then apply the AhsayCBS license (the license from the AhsayCBS in backup server mode).

     This will ensure that there are sufficient **Client Software** and **Add-on Modules** available to the backup users after the switch.
   - Press **Update**, then click .

     Ensure that the license information are properly applied by checking the Client Software and Add-on Modules settings under License Details.

     IMPORTANT

     Before continuing with the next step, ensure that the license is properly applied. Failure to do so may result in backup accounts being suspended and all backup settings being reset.

     Also, ensure to shut down the AhsayCBS on the backup server, so that you are not running two servers with the same AhsayCBS license.

3. Convert the AhsayCBS in Replication Receiver Mode to Backup Server Mode by following the steps below.

   - Shutdown the AhsayCBS service.

     Note: *For AhsayCBS version 7.9.0.0 or above, shutdown the AhsayCBS and AhsayCBS NFS services.*
   - Copy the replicated system **config** files to the corresponding location.

     - Extract the content of the **conf.zip** file from the **Default Home Directory** to the AhsayCBS installation **conf** folder.

       Extract
       %Default Home Directory%\app\conf\conf.zip

       to

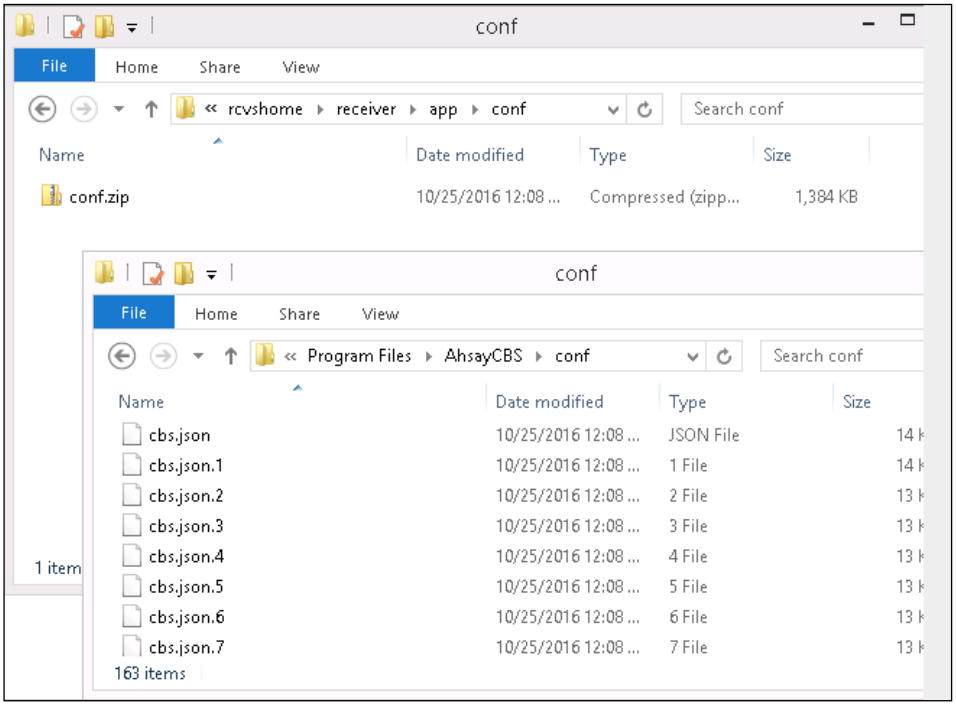
       %AhsayCBS Install Home%*

       Using the example in Step 1, extract content of

       C:\Program Files\AhsayCBS\system\rps\rcvshome\receiver\app\conf\conf.zip

       to

       C:\Program Files\AhsayCBS\conf



➢ Copy the replicated system home to the corresponding location by following the steps below.

- Copy the replicated system home from the **Default Home Directory** to the AhsayCBS system home folder.

  Copy
  %Default Home Directory%\app\system*

  to

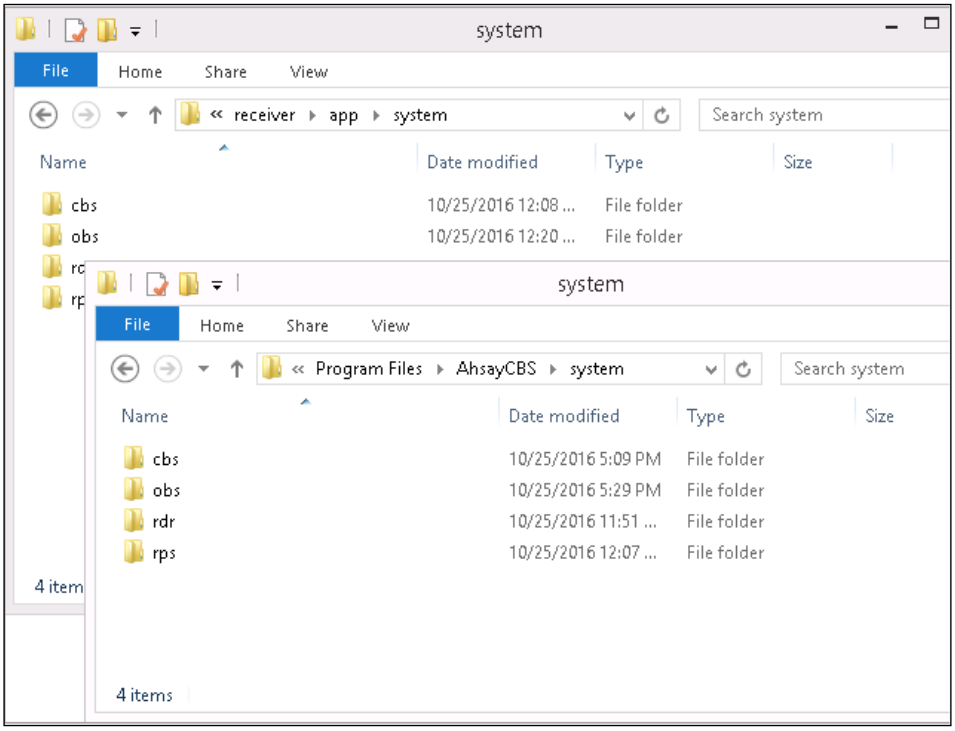
  %AhsayCBS System Home%*

  Using the example in Step 1, copy the content of

  C:\Program Files\AhsayCBS\system\rps\rcvshome\receiver\app\system*

  to

  C:\Program Files\AhsayCBS\system



NOTE

If you are planning to change the system home location, copy the replicated system home to the new system home location instead.

➢ Copy the replicated user home to the corresponding location.

- Copy the replicated user home from the **Replication Home** to the AhsayCBS user home folder.

  Copy
  %Replication Home%\%username%

  to

  %AhsayCBS User Home%*

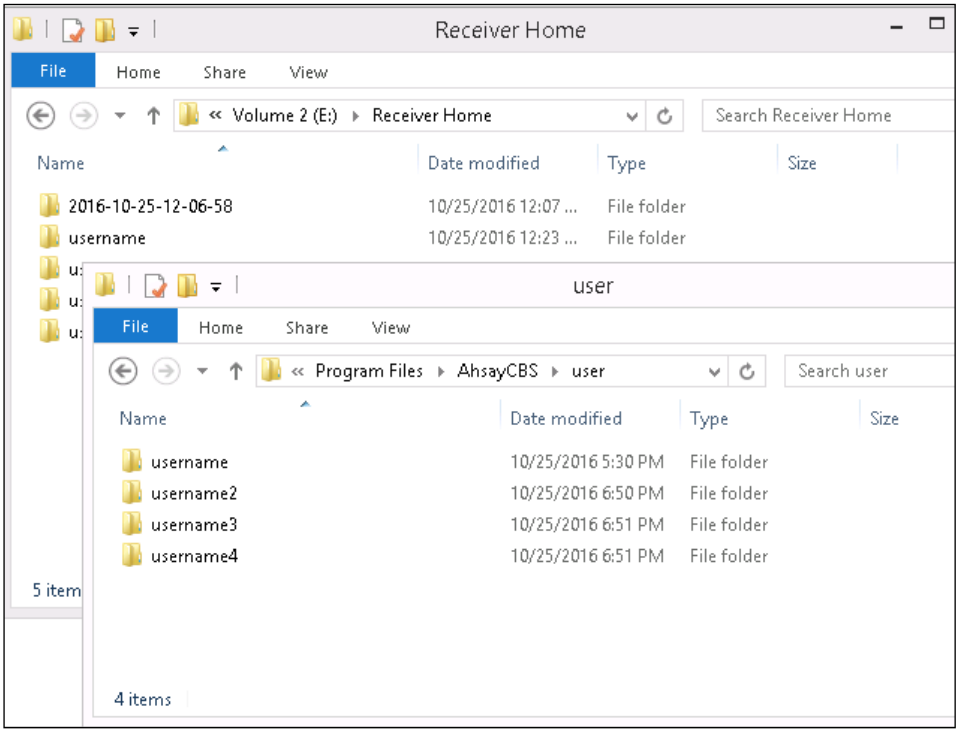
  Important: *Do not copy over the folder in YYYY-MM-DD-hh-mm-ss format.*

  Using the example in Step 1, copy the content of

  E:\Receiver Home*

  to

  C:\Program Files\AhsayCBS\user



NOTE

If you are planning to change the user home location, copy the replicated user home to the new user home location instead.

- Startup the AhsayCBS service.

  Note: *For AhsayCBS version 7.9.0.0 or above, startup the AhsayCBS and AhsayCBS NFS services.*

- Login to the AhsayCBS web console, confirm on the settings.

  - Confirm the system settings under the **System Settings** > **Basic** and **System Settings** > **Advanced** menus.

    Modify the **System Home** setting under **System Settings** > **Basic** if necessary (e.g. if you had copied the replicated system home to a new location in the previous step).

  - Confirm the user and policy settings under **Backup / Restore** > **Users, Groups & Policies** menu.

    Modify the **User Home** setting under **Backup / Restore > Basic** if necessary (e.g. if you had copied the replicated user home to a new location in the previous step).

NOTE

For AhsayCBS installation on Linux platforms, the conversion procedure is the same except all directory paths are in the Linux convention.

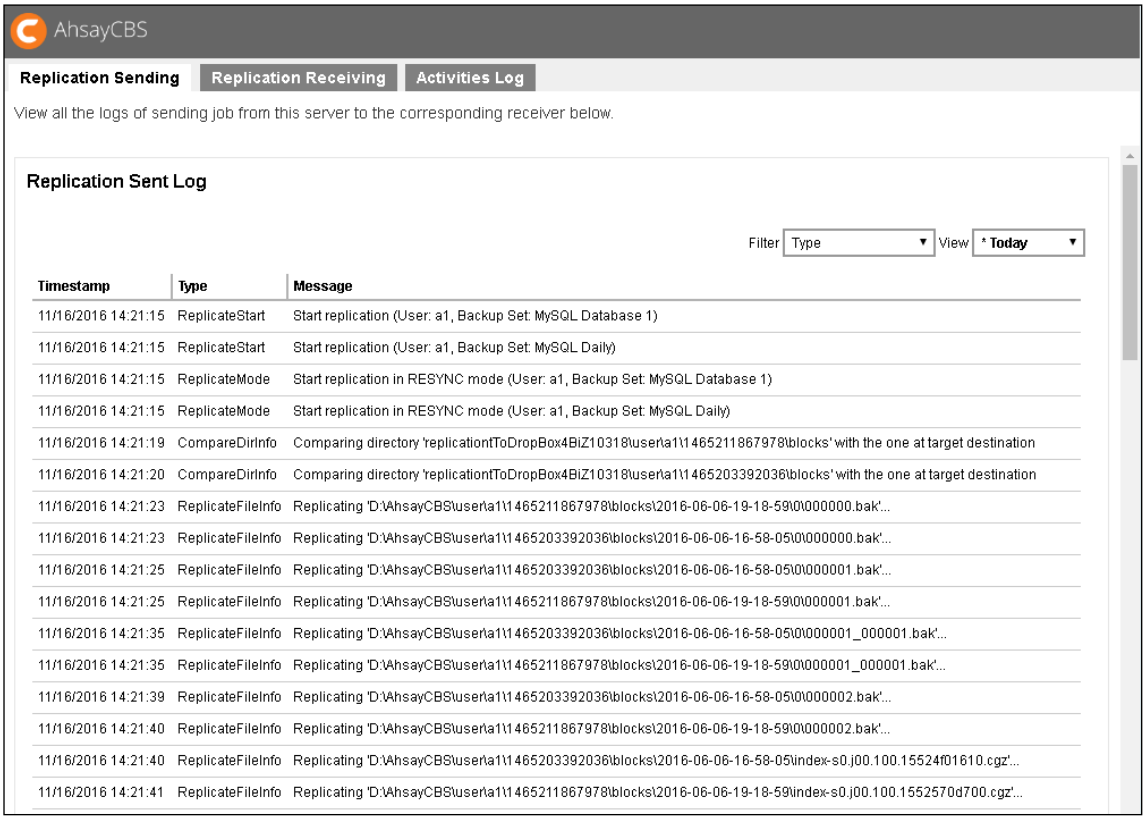
Extract Data from Replication Destination

Getting Started

If you have chosen to recover your replication data using Method 1 - Rebuild AhsayCBS from Replication, you will have to extract the replication data from the replication destination first. Before getting started, make sure replication has been performed before you start restoring any replication data by performing the following checking.

To check replication logs on the Backup Server:

Log in to the AhsayCBS web console, navigate to **Monitoring** > **Replication Logs** > **Replication Sending**.



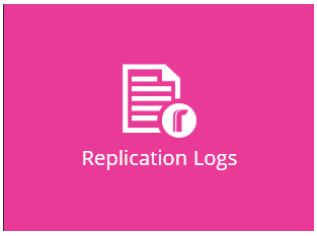
Viewing option

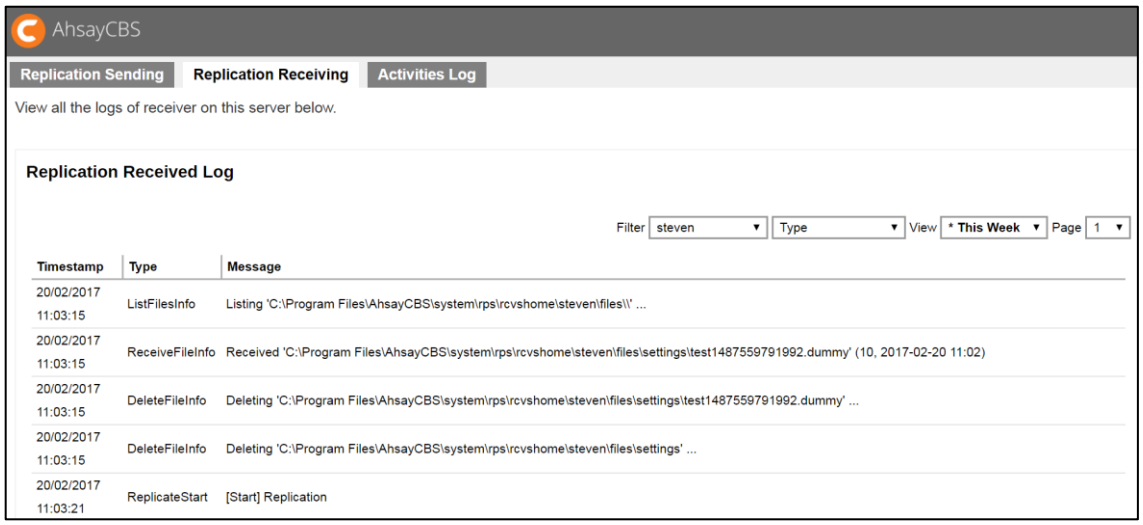
Use the drop-down filters at the top right corner to filter the desired replication sending logs:

Type	Select the desired type of replication log to display
View	Select a specified date or range of time of the replication logs

To check the replication logs on the Replication Server:

Log in to the AhsayCBS web console, navigate to **Monitoring** > **Replication Logs** > **Replication Receiving**.





Viewing option

Use the drop-down filters at the top right corner to filter the desired replication receiving logs:

Receiver Name	Select the receiver name of whom the replication data is from
Type	Select the type of replication log to display
View	Select a specified date or range of time of the replication logs

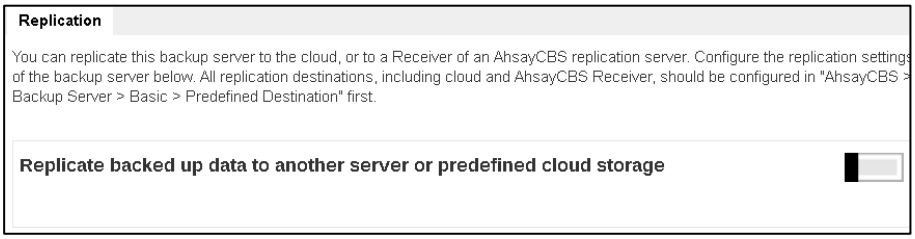
Extract from AhsayCBS Replication Server

1. Follow the steps below to disable the replication service on both the Backup Server and the Replication Server.

- **To Disable on the <u>Backup Server Side</u>**

v. Click on the **Sending Data** icon under the Replication section on the AhsayCBS web console of the backup server.

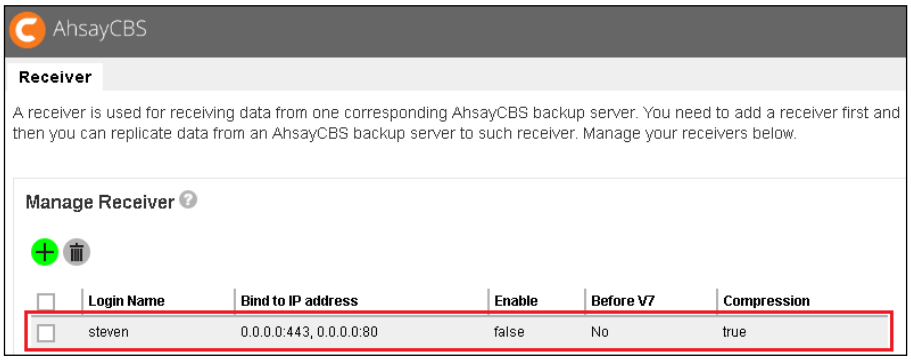
vi. Click the button in the **Replicate individual backup sets** section to turn the replication feature off. You will then see the configuration menu as shown.



- **To Disable on the <u>Replication Server Side</u>**

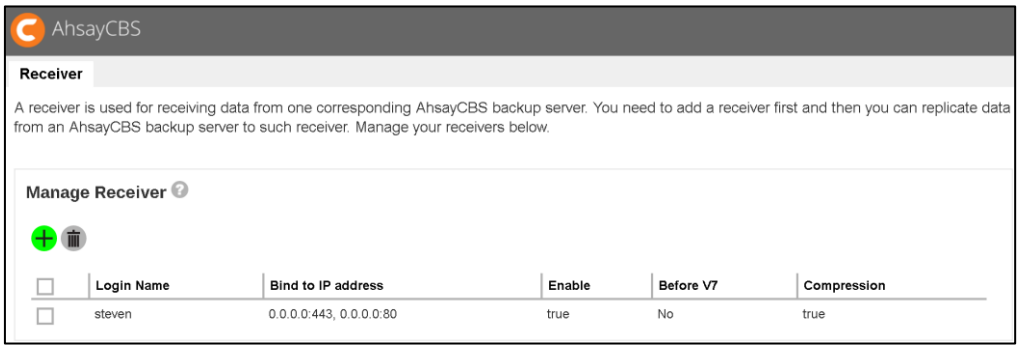
i. Click On the replication receiving end, go to **Replication > Accepting Data** on the AhsayCBS web console to create a replication user account.

ii. Click on the replication receiver item under the **Manage Receiver** section which you wish to turn off.



iii. Uncheck the **Enable Replication** checkbox under the **Receiver User Account** section.

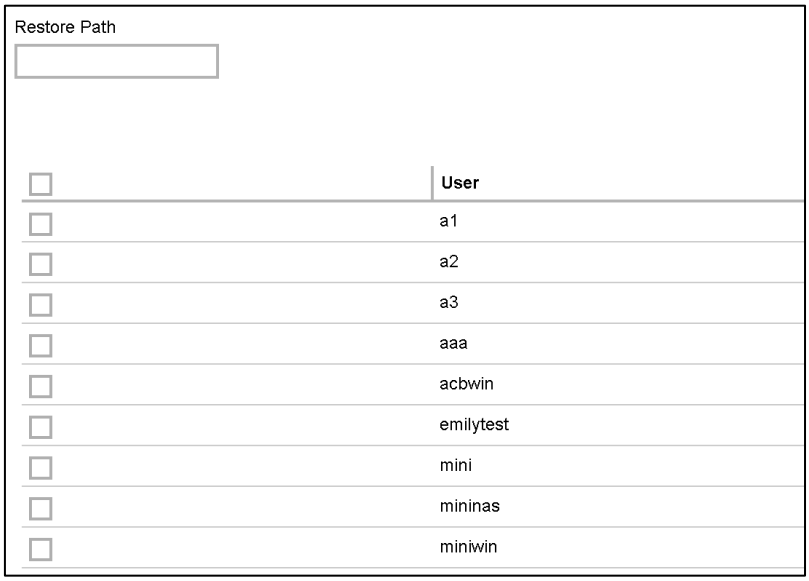
2. Go to the Replication Server web console > **Accepting Data** > **Manage Receiver** > **%receiver_name%**.



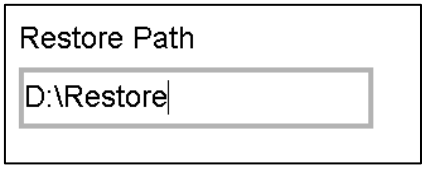
3. Locate the **Restore** section at the bottom of the page.

4. Click on the Snapshot "**Current**", you will see all the replicated users.

5. Select the user(s) that you want to recover, select all if you want to recover all the users for the Backup Server.



6. Enter the path you want to restore the data to (e.g. D:\Restore).



7. Click the button at the bottom right corner to start the restoration.

8. It will then go back to the **Edit Receiver** page and you will see the restore progress under the **Restore** section.

9. When you see the **Finished restoration !!** message, the restore is completed.

10. The data of the selected users and the server configuration are restored to the specified restore path on the Replication Server.

    You will find folder structure as:

    - **D:\Restore\Retention_Current\system**
      (It contains “CBS_HOME\conf” and “SYSTEM_HOME”.)
    - **D:\Restore\Retention_Current\users**
      (It contains user folders.)

11. Copy the whole restored folder “**D:\Restore**” to a free space on your Backup Server first, e.g. C:\Desktop.

12. After extracting the replication data, you can follow the instructions in Restore Replication Data to the Backup Server to restore the replication data to your AhsayCBS backup server.

    -OR-

    Refer to the Restore Raw Data Using AhsayOBM / AhsayACB if you wish to recover the raw data alone without restoring them to AhsayCBS.

Extract from a Predefined Destination - Cloud storage

In this example, we use Google drive as the cloud storage. Other cloud storage should have similar capability.

Prerequisite: Google drive is installed

1. Disable the replication on the Backup Server by following the steps below.

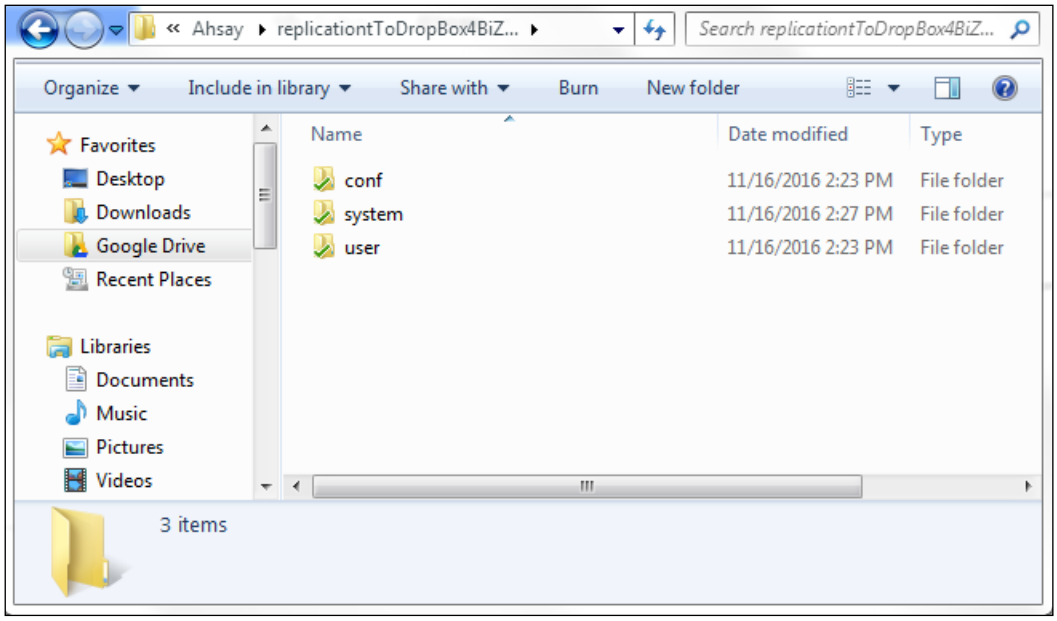
   i. Click on the **Sending Data** icon under the Replication section on the AhsayCBS web console of the backup server.

   ii. Click the button in the **Replicate individual backup sets** section to turn the replication feature off. You will then see the configuration menu as shown.

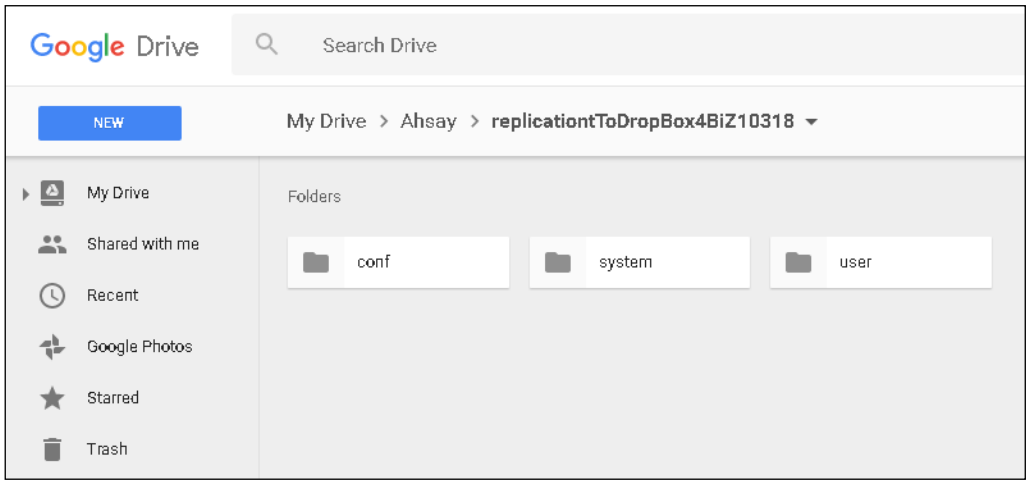
2. Go to your Google drive folder or login to the Google drive web interface to access to your storage.

3. You will be able to find the following path such as **Google drive** > **Ahsay** > **replication**. ('**replication**' is the replication profile name)

   Google drive file explorer



Google drive web interface



4. You will see the following 3 folders.
   - **conf**
   - **system**
   - **user**

5. You may download all the 3 folders to your local drive if you need to restore all the files. Select the folder to download according to your requirement.

> **NOTE**
>
> The **conf** and **system** folders are AhsayCBS configuration or system related files. The **user** folder contains the replicated user folders.

6. After extracting the replication data, you can follow the instructions in Restore Replication Data to the Backup Server to restore the replication data to your AhsayCBS backup server.

   -OR-

   Refer to the Restore Raw Data Using AhsayOBM / AhsayACB if you wish to recover the raw data alone without restoring them to AhsayCBS.

Extract from the FTP/SFTP

In this example, we use SFTP server as an example, the restore method is basically the same for FTP and SFTP.

Assumption: The WinSCP is installed on the system. Other FTP tools can be used.

1. Disable the replication on the Backup Server by following the steps below.

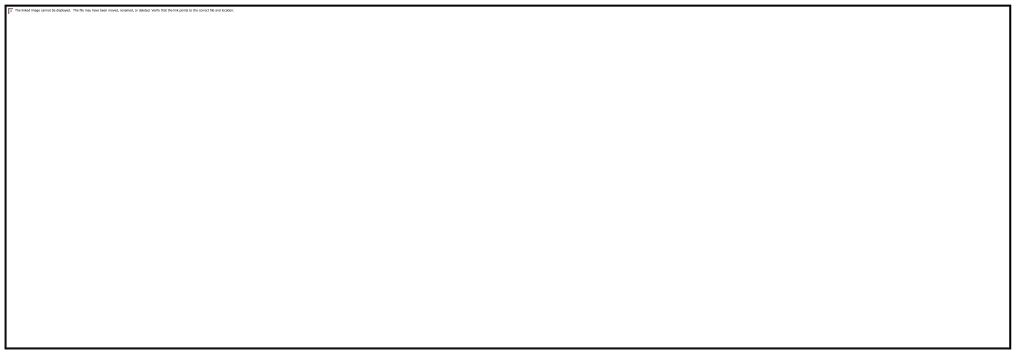
   i. Click on the **Sending Data** icon under the Replication section on the AhsayCBS web console of the backup server.

   ii. Click the button in the **Replicate individual backup sets** section to turn the replication feature off. You will then see the configuration menu as shown.

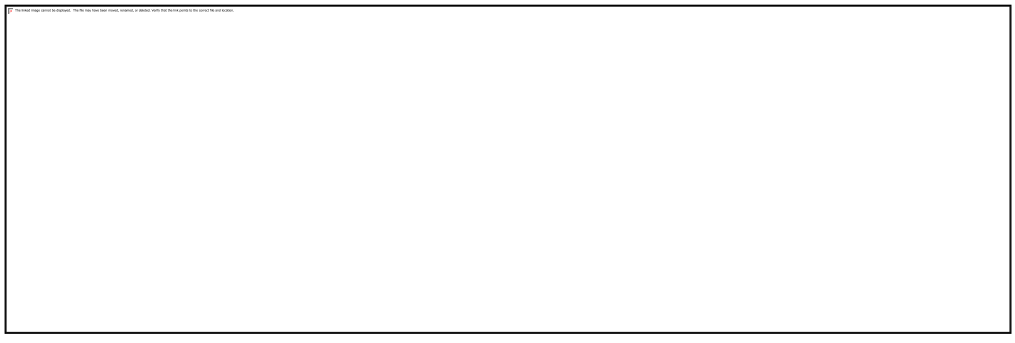
2. Login to the WinSCP and locate the replication folder. If the FTP/SFTP server is on your LAN, you may map the drive on your FTP/SFTP server.

3. You will be able to find the following path such as /sftp_root/Ahsay/replication. ('replication' is the replication profile name)

   WinSCP

   Mapped the SFTP share folder

4. You will see the following 3 folders.
   - **conf**
   - **system**
   - **user**
5. You may download all the 3 folders to your local drive if you need to restore all the files. Select the folder to download according to your requirement.

> **NOTE**
>
> The **conf** and **system** folders are AhsayCBS configuration or system related files. The **user** folder contains the replicated user folders.

6. After extracting the replication data, you can follow the instructions in Restore Replication Data to the Backup Server to restore the replication data to your AhsayCBS backup server.

   -OR-

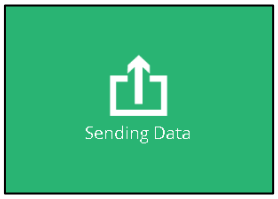
   Refer to the Restore Raw Data Using AhsayOBM / AhsayACB if you wish to recover the raw data alone without restoring them to AhsayCBS.

Extract from the Local/Mapped Drive/Removable Drive

In this example, we use local drive as an example, the restore method is basically the same for mapped drive and removable drive.

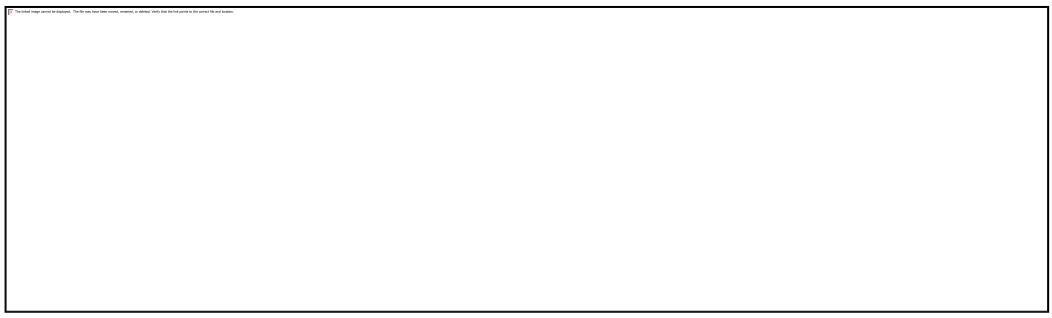
1. Disable the replication on the Backup Server by following the steps below.

   i. Click on the **Sending Data** icon under the Replication section on the AhsayCBS web console of the backup server.

   ii. Click the button in the **Replicate individual backup sets** section to turn the replication feature off. You will then see the configuration menu as shown.

2. Open your replication home folder e.g.: E:\rpshome\replication ('replication' is the replication profile name).

3. You will see the following 3 folders.

   - **conf**
   - **system**
   - **user**

4. You may copy all the 3 folders if you need to restore all the files on your AhsayCBS. Select the folder to download according to your requirement.

   NOTE

   The **conf** and **system** folders are AhsayCBS configuration or system related files. The **user** folder contains the replicated user folders.

5. After extracting the replication data, you can follow the instructions in Restore Replication Data to the Backup Server to restore the replication data to your AhsayCBS backup server.

   -OR-

   Refer to the Restore Raw Data Using AhsayOBM / AhsayACB if you wish to recover the raw data alone without restoring them to AhsayCBS.

Extract from v6 Replication

This section provides steps on restoring replication data in v6 format to a v6 version backup server.

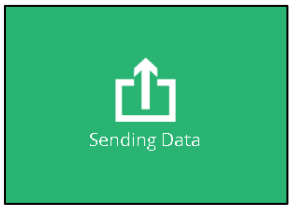
IMPORTANT

Please be reminded that the steps in this section apply only if you are restoring the replication data in v6 data format back to a backup server in v6 version.

If the backup server has been upgraded to v7, the replication data in v6 data format cannot be restored in the upgraded backup server due to the fundamental differences of the system structure and data format between v6 and v7. If you have upgraded your backup server to v7, you will have to configure the replication receiver again and make sure to select the Backup Server Version as 7 during the receiver creation process. Refer to the Create a Replication User Account section for further details on the configuration.

1. Disable the replication on the Backup Server by following the steps below.

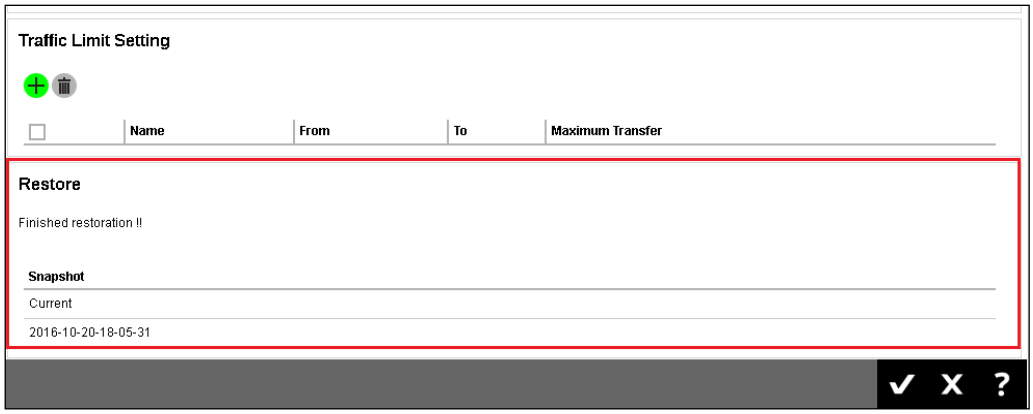
   i. Click on the **Sending Data** icon under the Replication section on the AhsayCBS web console of the backup server.

   ii. Click the button in the **Replicate individual backup sets** section to turn the replication feature off. You will then see the configuration menu as shown.

2. Go to the Replication Server web console, then navigate to **Replication** > **Accepting Data** > **Manage Receiver** > **%receiver_name%**.

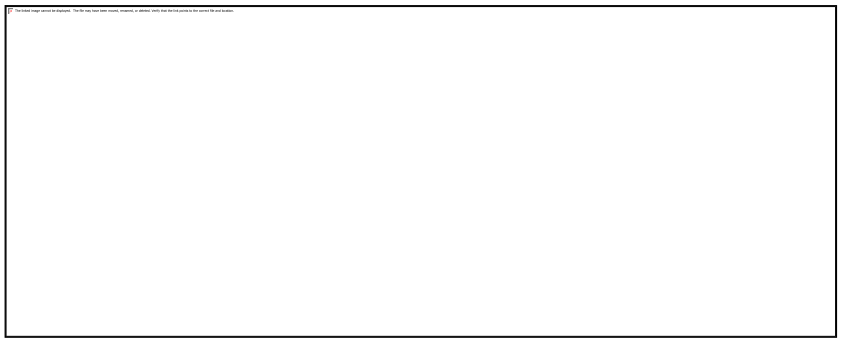
3. Locate the **Restore** section at the bottom of the page.



4. Click on the Snapshot “Current”, you will see all the replicated users.

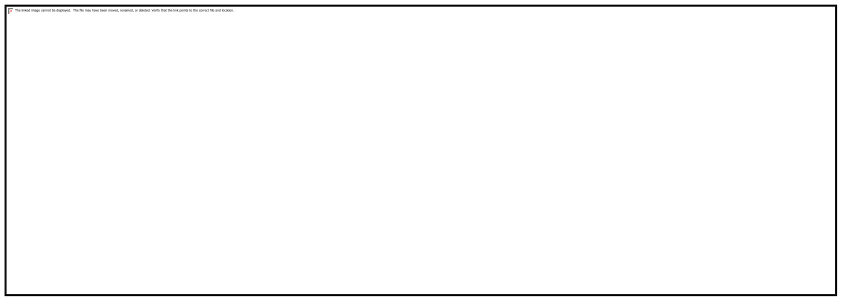
5. Select the user(s) that you want to recover, select all if you want to recover all the users for the Backup Server.

6. Enter the path you want to restore the data to (e.g. F:\v6rps).

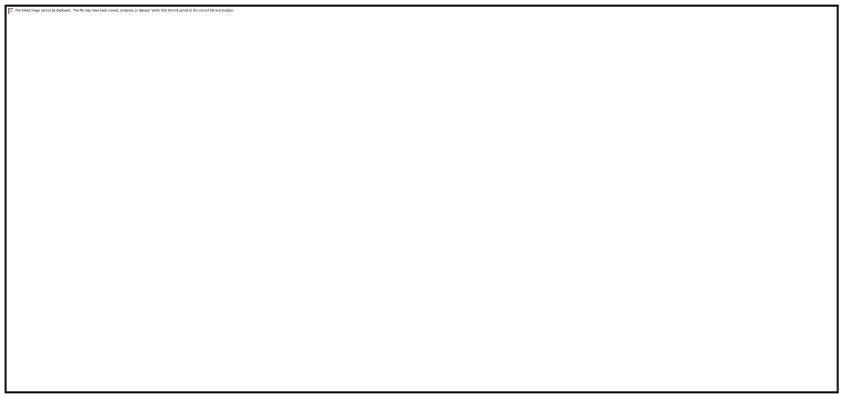


7. Click the [Restore] button to start.

8. It will then go back to the “Edit Receiver” page and you will see the restore progress under the “Restore” section.

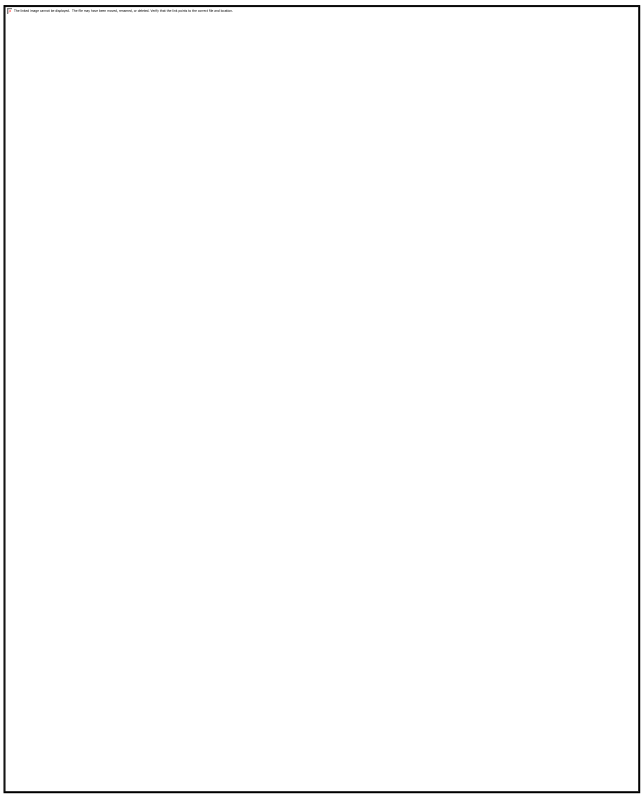


9. Once you see the "**Finished restoration !!**" message, the restore is completed.



10. The data of the selected users and the server configuration are restored to the restore path on Replication Server.

11. You will find folder structure as:



NOTE

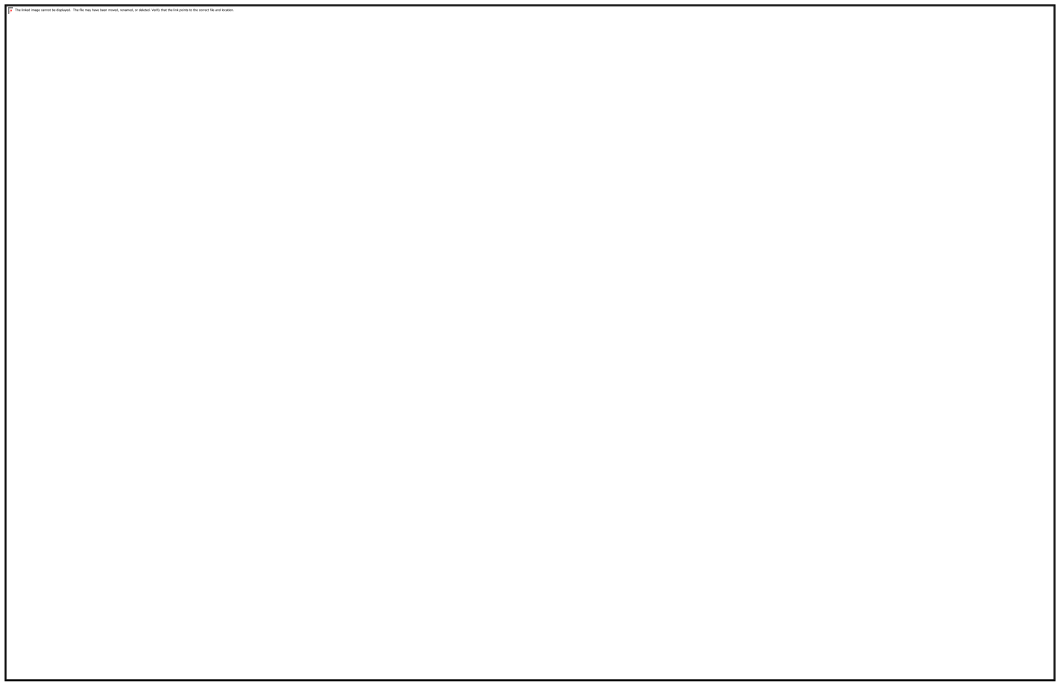
The folder F:\v6rps\Retention_Current\ contains all the restore materials for your v6 OBS. Under the folder, F:\v6rps\Retention_Current\system, you can see the folder “C%3A” which indicate the drive letter of the installation, %3A is the URL encoding for the colon character which means “C:”.

Here is a summary of the restored folders under the path “F:\v6rps\Retention_Current\system\C%3A\Program Files\AhsayOBS and AhsayRPS”:

Folder name	Description
bin	It contains startup scripts.
conf	OBS server configuration files.
java	Bundled Java for the OBS.
system	System configuration and policy settings.
tomcat	Bundled Tomcat for the OBS.
webapps	OBS and RPS application folders, OBC installer files etc.
work	Cache folder.

12. Copy the whole restored folder “F:\v6rps” to your OBS machine.

13. Locate the OBS installation directory in the OBS machine, **conf** folder, **system** folder and **user** folder.



In this case, all the 3 folders are located in the same directory. If you have changed the OBS system home or user home folder, you can check this information in your **OBS Management Console** > **Manage System** > **Server Configuration** page.

14. After extracting the replication data, you can follow the instructions in Restore Replication Data to the Backup Server to restore the replication data to your AhsayCBS backup server.

-OR-

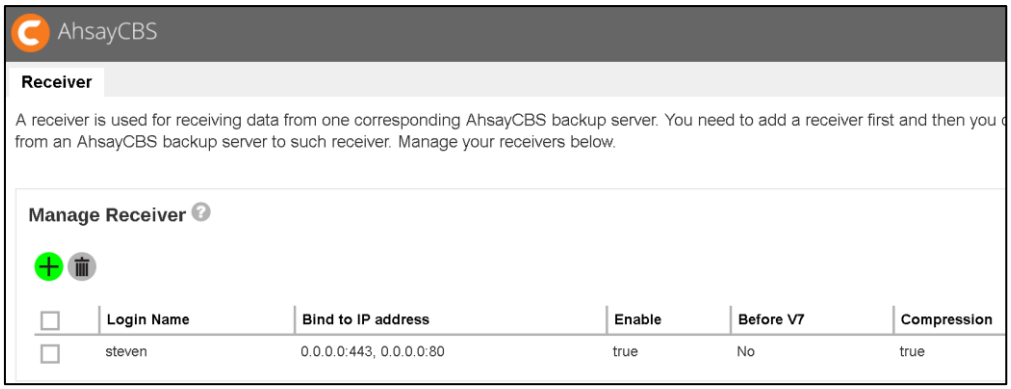
Refer to the Restore Raw Data Using AhsayOBM / AhsayACB if you wish to recover the raw data alone without restoring them to AhsayCBS.

Extract Snapshot from Retention Area

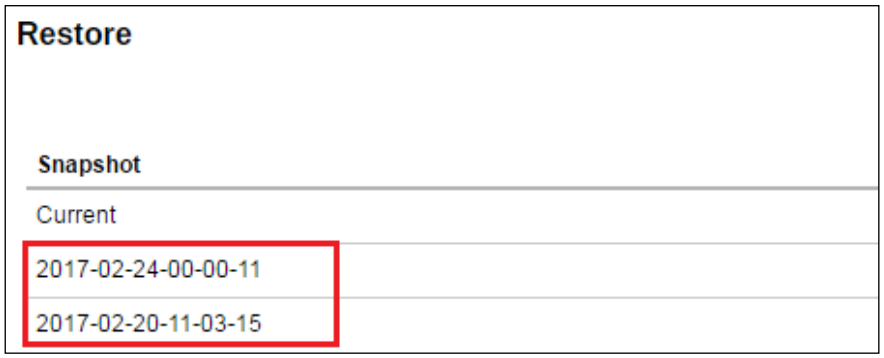
A snapshot of the replicated data is taken and stored in the retention area for a certain period of time of your configuration. This gives you an extra layer of protection in case you need to retrieve the old replication data. For details of the retention policy setting, refer to the Retention Setting under the Create a Replication User Account section.

Follow the instructions below to recover replication data from the retention area.

1. Go to the Replication Server web console > **Accepting Data** > **Manage Receiver** > **%receiver_name%**.

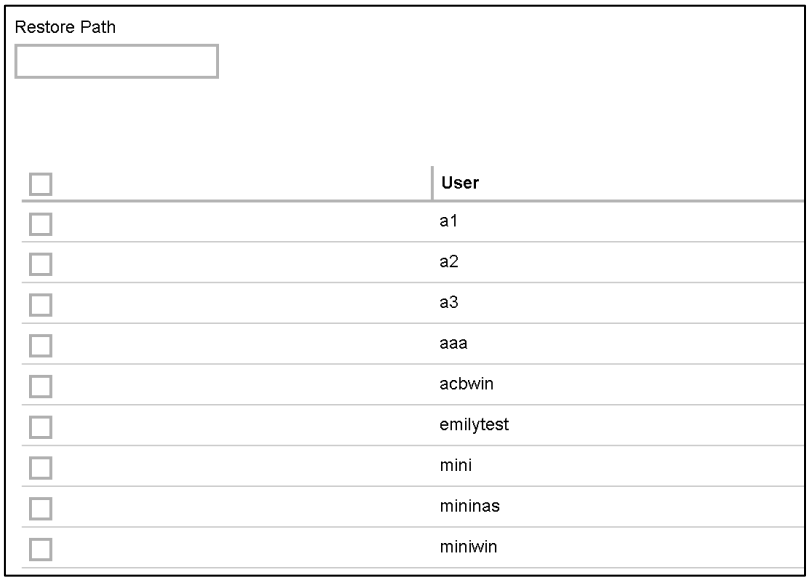


2. Locate the **Restore** section at the bottom of the page and you will see the snapshots that have been captured for your replication data.

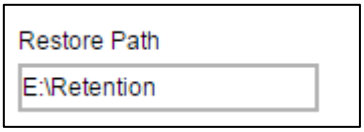


3. The past snapshots are named in date and time when it was captured. Click on the desired snapshot you wish to extract the replication data from.

4. Select the user(s) that you want to recover, select all if you want to recover all the users for the Backup Server.



5. Enter the path you want to restore the data in the retention area (e.g. E:\Retention).

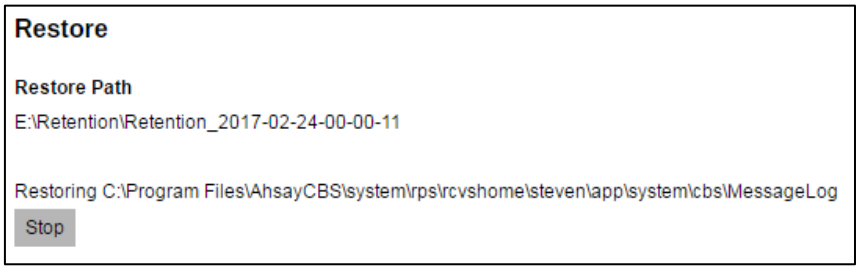


NOTE

Do not restore the retention data to the same folder where you normally store the extracted replication data so as to avoid any possible confusion.

6. Click the button at the bottom right corner to start the restoration.

7. It will then go back to the **Edit Receiver** page and you will see the restore progress under the **Restore** section.



8. When you see the **Finished restoration !!** message, the restore is completed.

9. The data of the selected users and the server configuration are restored to the specified restore path on the Replication Server.

You will find folder structure as:

- **E:\Retention\Retention_YYYY-MM-DD-HH-MM-SS\system**
  (It contains “CBS_HOME\conf” and “SYSTEM_HOME”.)
- **E:\Retention\Retention_YYYY-MM-DD-HH-MM-SS\users**
  (It contains user folders.)

10. Copy the whole restored folder “**E:\Retention**” to a free space on your Backup Server first, e.g. C:\Desktop.

11. After extracting the replication data, you can follow the instructions in Restore Replication Data to the Backup Server to restore the replication data to your AhsayCBS backup server.

    -OR-

    Refer to the Restore Raw Data Using AhsayOBM / AhsayACB if you wish to recover the raw data alone without restoring them to the backup server.

Restore Replication Data

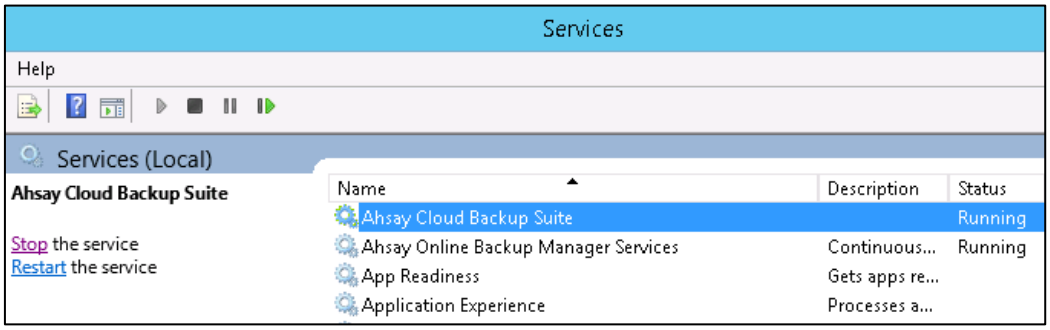
Restore Replication Data to the Backup Server

IMPORTANT

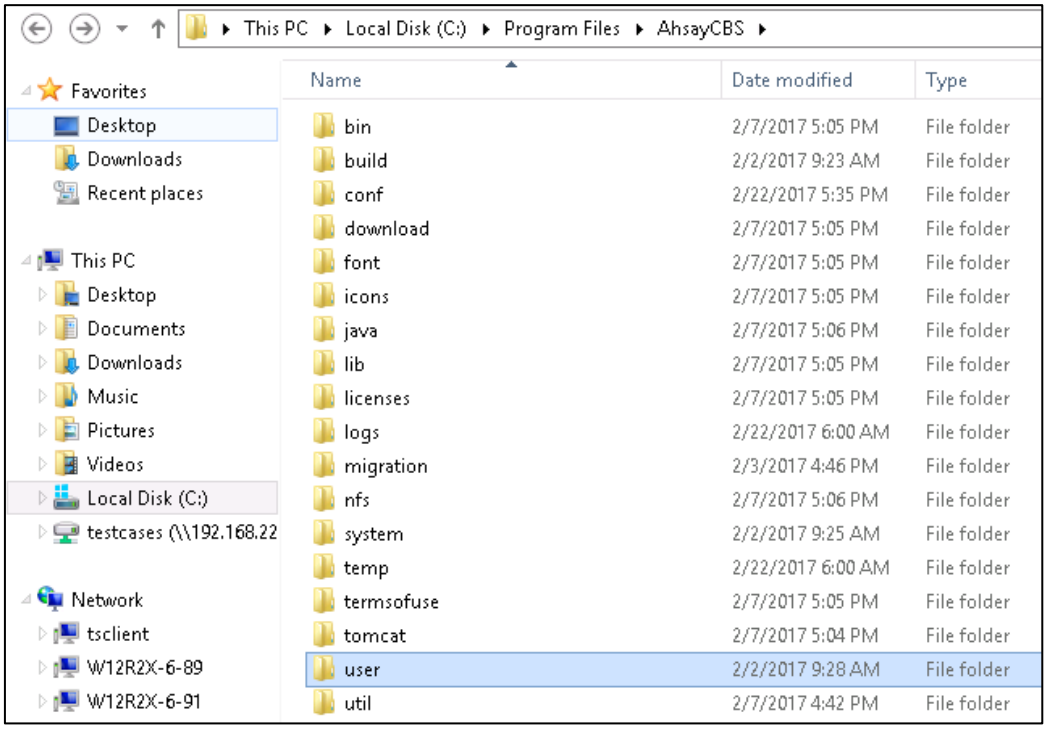
Make sure you have extracted the replication data from the replication destination before you start with the restore. Refer to the instructions in the Extract Data from the Replication Destination for details.

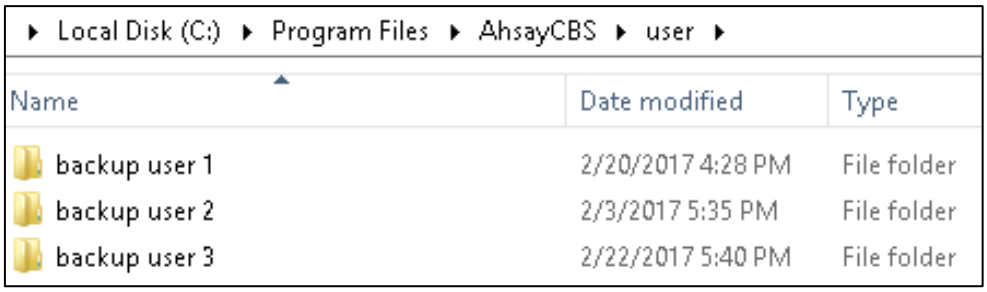
Follow the instructions below to restore replication data to your AhsayCBS backup server.

1. Stop the AhsayCBS service on the Backup Server by going to the **Services** console, click on Ahsay Cloud Backup Suite then click the **Stop** button on the left.

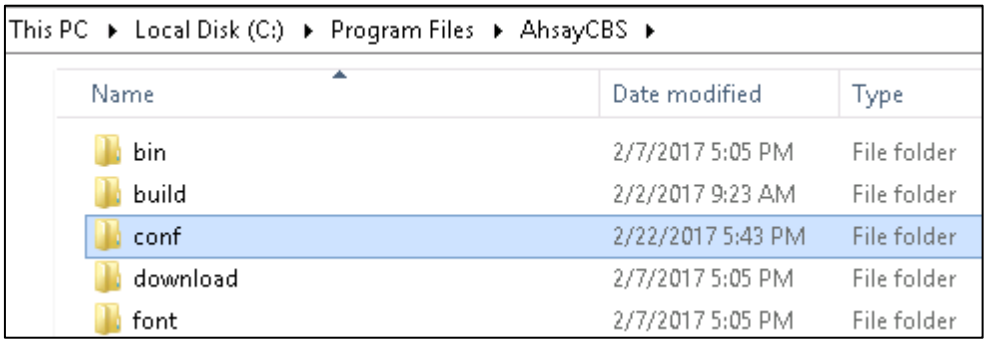


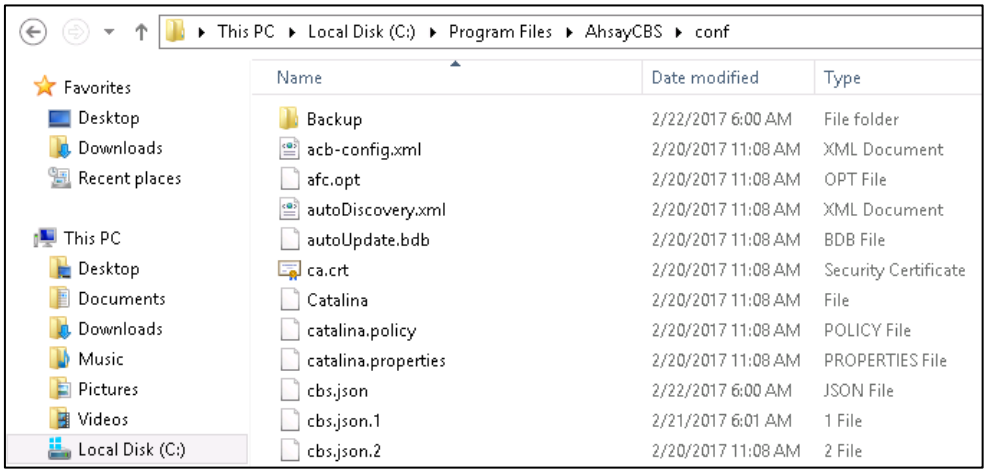
2. If you want to recover the user data, copy the **%user_name%** folder from the "**%Restored_folder%\Retention_Current\users**" folder, then paste it to the User Home folder located in "**\AhsayCBS\user**"on your backup server machine.



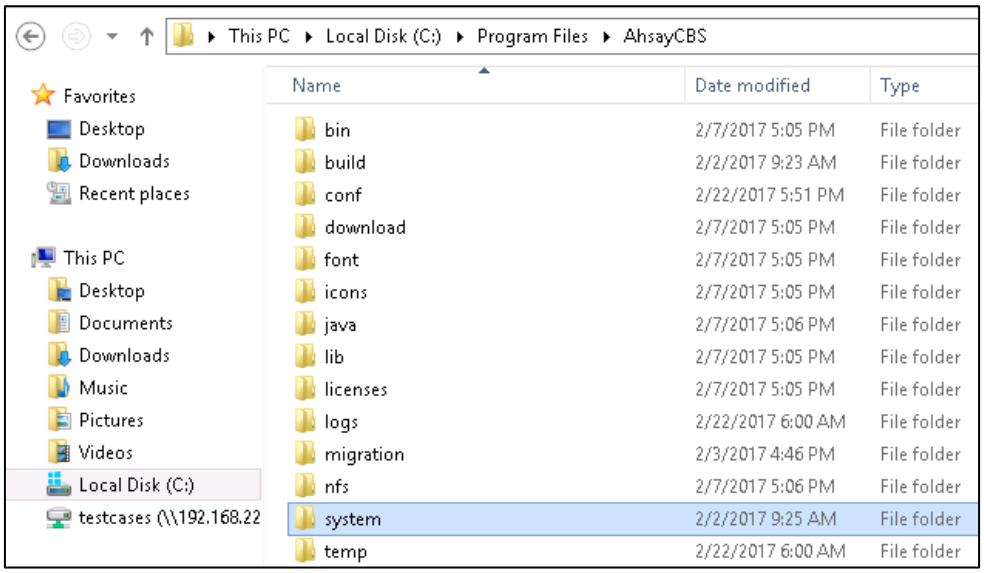


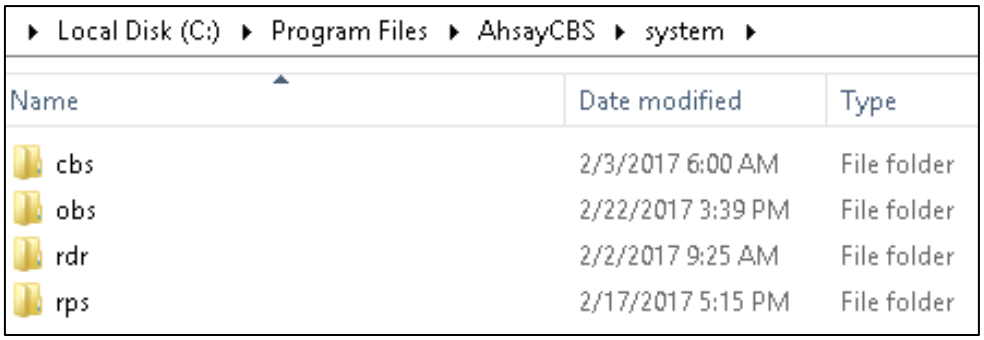
3. If you want to recover the server configuration, extract the "**%Restored_folder%\Retention_Current\system\conf\conf.zip**", then unzip the file and replace all the unzipped files with those located on **"\AhsayCBS\conf\"**.



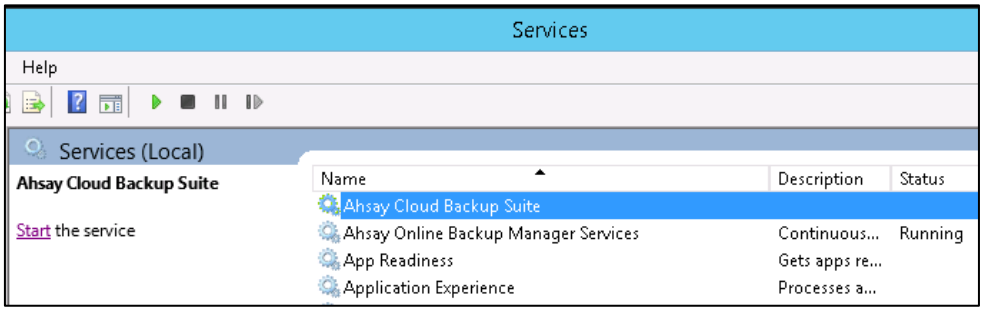


4. If you want to recover the system home, copy the content of the "**%Restored_folder%\Retention_Current\system\system**" folder in the restored folder, then paste it in the system folder located in **"AhsayCBS\system\"**on your backup service machine.





5. Restart the AhsayCBS service on the Backup Server by going to the **Services** console, click on Ahsay Cloud Backup Suite then click the **Start** button on the left.



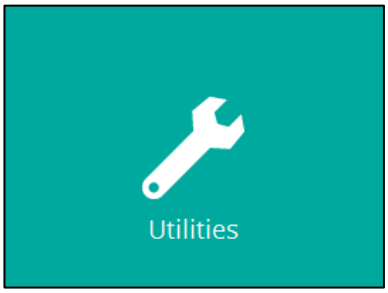
Restore Raw Data Using AhsayOBM / AhsayACB

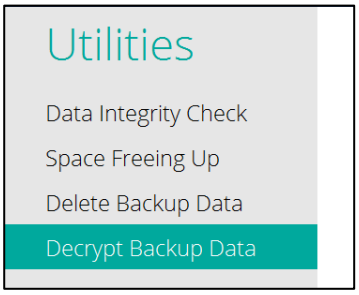
Besides restoring the replication data back to the backup server, you can also restore the raw data alone using either of the client backup agent (AhsayOBM / AhsayACB).

Make sure you have extracted the replication data from the replication destination before you start with the restore. Refer to the instructions in the Extract Data from the Replication Destination. Once you have extracted the replication data, follow the steps below to restore the raw data.

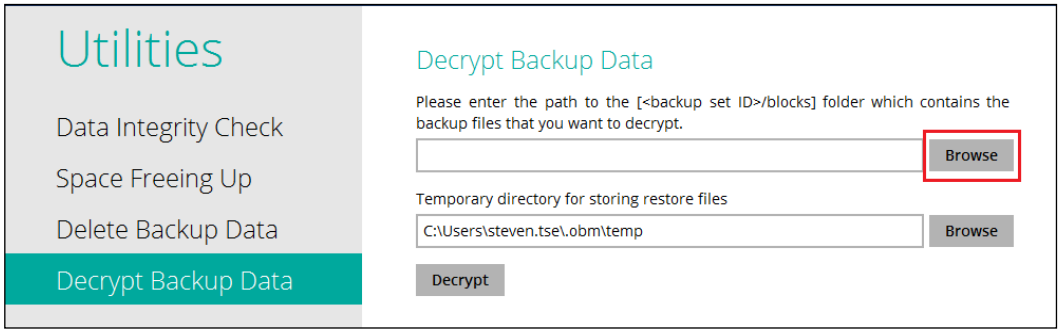
AhsayOBM is used in the following instructions for decrypting the data. The procedures work basically the same for AhsayACB.

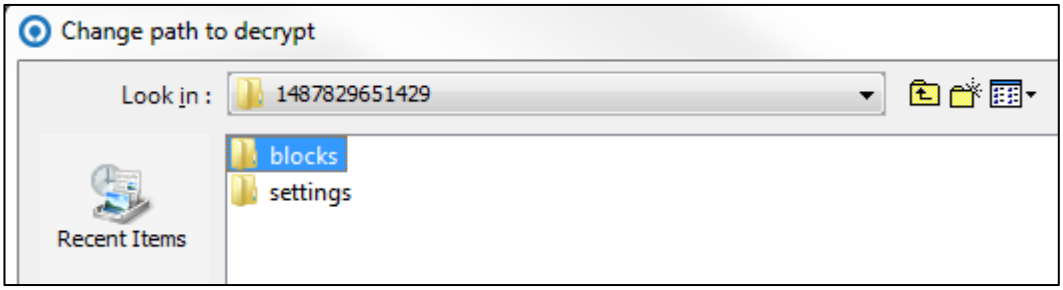
1. Log in to the AhsayOBM client backup agent, then navigate to the **Utilities** icon on the main interface, then go to the **Decrypt Backup Data** section.



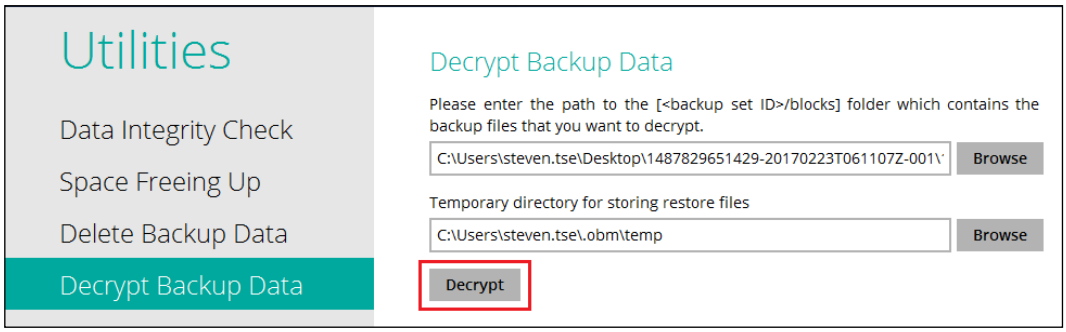


2. Click Browse to locate the backup set you wish to decrypt replication data you have extracted, then navigate to the **[%backup set ID%/blocks]** level of the backup set you wish to restore data from.

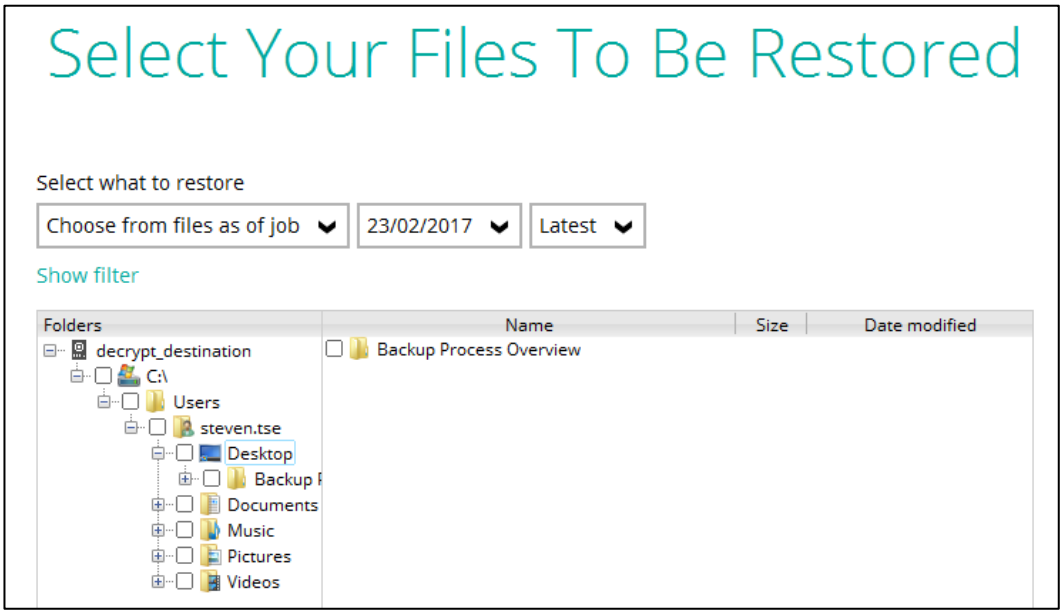




3. Click **Decrypt** to proceed.



4. Select the file(s)/folder(s) you wish to restore from the selected source, then click Next to proceed.



5. Select to restore to the Original location or an alternate location of your choice. Click **Restore** to start the decryption process when you have done with the settings.

8 Configuring Redirector

As your business keeps growing, the capacity of an AhsayCBS machine may reach its physical limit such as the I/O, disk space, etc. In that case, you may consider adding a machine to solve the problem.

A common practice for server administrator will name their server in the following way when a new server is added for backup service, for example:

server1.mybackup.com
server2.mybackup.com
server3.mybackup.com
:

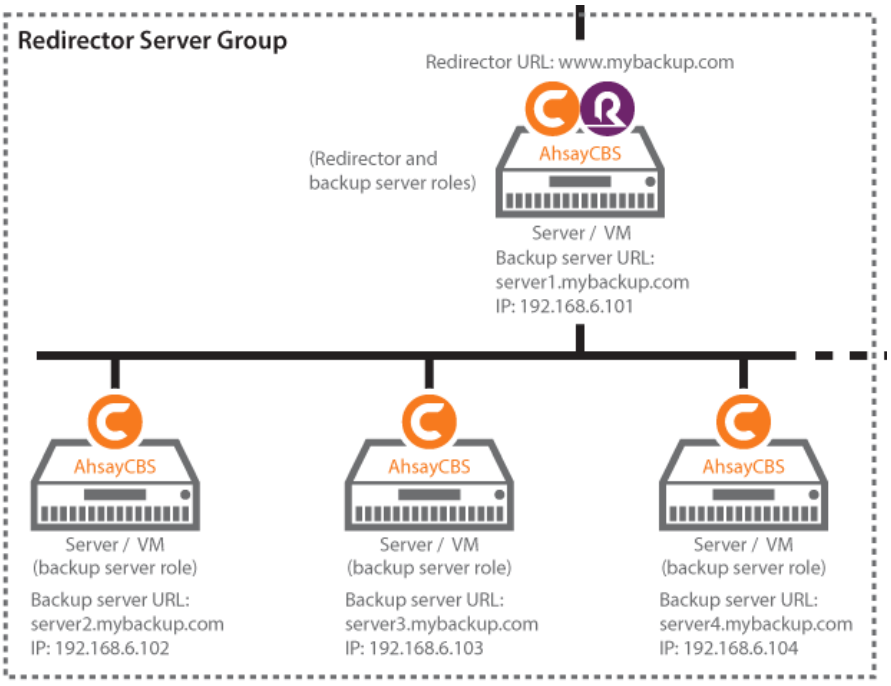
With mybackup.com being the domain name of the backup service in the above example. This is only a solution to resolve physical limit of a server but is not flexible to apply into a high scalable backup system. This is because if a user has hosted in, for example, server1.mybackup.com and later on wants to add more backup quota, however, only server2.mybackup.com has enough storage for expansion. In that case, you will need to migrate the user to server2 and your backup users will need to change the backup server URL from server1 to server2 in the login screen of the client interface to get access to the new server.

A high scalable backup system should make this kind of transition seamless to users, for example, you can set up a domain name www.mybackup.com for your client to connect which is able to redirect users to the correct backup server to backup. Our Redirector is exactly designed to work for this solution.

By setting up a Redirector Server:

1. All new clients can use the backup URL e.g.: www.mybackup.com when they set up the backup client interface.

2. Administrator can add backup machines to the Redirector as the number of user grows.



The dotted area shows the redirector server group.

server1.mybackup.com
server2.mybackup.com
server3.mybackup.com
:
:

As the CPU utilization for a Redirector Server is low, you can dedicate one of the AhsayCBS as the redirector host. In the above example, server1.mybackup.com also serves as a redirector host. The domain name www.mybackup.com is also pointed to this server.

Administrator will require setting up the following in the DNS, for example:

Name	Type	Value
www.mybackup.com.	CNAME	server1.mybackup.com.
server1.mybackup.com.	A record	192.168.6.101
server2.mybackup.com.	A record	192.168.6.102
server3.mybackup.com.	A record	192.168.6.103
server4.mybackup.com.	A record	192.168.6.104

Notes:

1. The IP address of server1 to server4 are ranged from 192.168.6.101 to 192.168.6.104.
2. The Redirector Server is hosted on the server1.mybackup.com machine.

In the following chapters, we shall guide you to set up a Redirector host, and how to join your existing servers to this Redirector host.

Limitation

1. Existing users can continue to back up to their existing server, for example, server2.mybackup.com in the above example. However if they want to use the redirector feature, they are required to change the connecting host name to e.g.: www.mybackup.com . The redirector setup can only benefit new users as you will distribute the URL, i.e. www.mybackup.com to new users, you may not want to bother the existing users on applying the settings immediately.
2. Administrators need to ensure the same user name (case sensitive) has not been used within the backup servers in the same redirector group. This limitation includes all the users created by the resellers.

License information

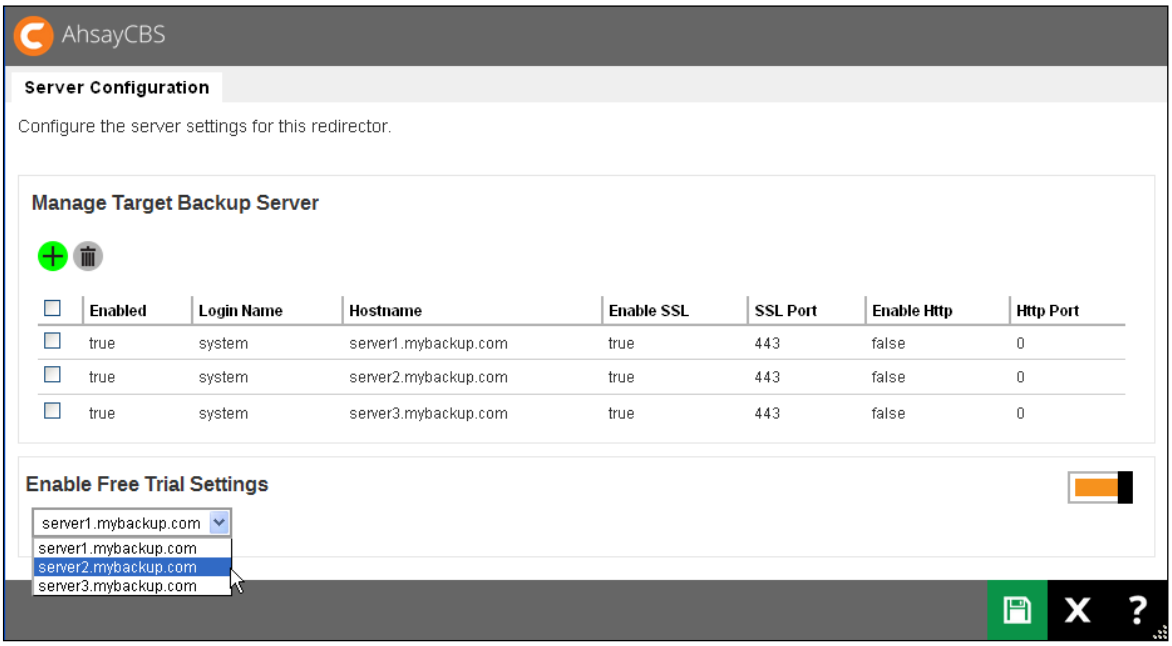
The pricing unit of AhsayCBS Redirection Server module is per device to be redirected.

For meter key inquiries please contact the Sales team at Ahsay by email at sales-kb@ahsay.com or call our International Sales Hotline +852 3580 8091.

Hosting a Redirector

First of all, you need to assign an AhsayCBS to be set up as a Redirector role. In our example, server1.mybackup.com also serves as a redirector host. The domain name www.mybackup.com is also pointed to this server.

In the following steps, we will set up the connection channel between the redirector host and the backup servers. In the AhsayCBS of server1, you need to register your Backup Server(s) with the Redirector in AhsayCBS management console under **Redirection** -> **Hosting a Redirector**.



1. Add a Backup Server in the Redirector by clicking the **Create** button, then entering the login credentials and host name, and the ports of that Backup Server.

2. Repeat the above steps until all the Backup Servers in your environment are registered with the AhsayCBS with the Redirector role.

Option: You can dedicate one of the AhsayCBS (Backup Server) to host free trial users, by enabling this feature and assign one of your Backup Servers in the list.

Joining Redirector

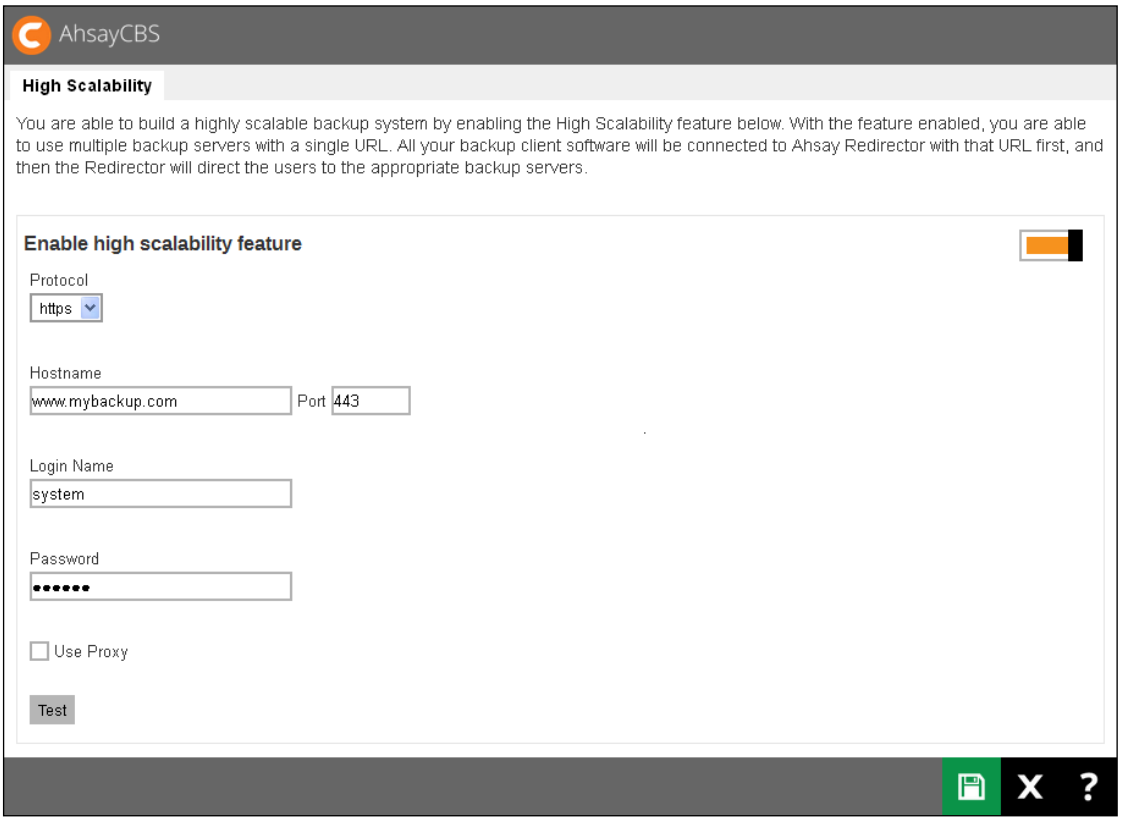
In the following steps, we will set up the connection channel between the redirector host and the backup servers.

Limitation:

Administrators need to ensure the same user name (case sensitive) has not been used within the backup servers in the same redirector group, this limitation includes all the users created by the resellers.

To join your Backup Servers to a Redirector, please enter your AhsayCBS management console under **Redirection** -> **Joining Redirectors**.

Note: Even your redirector is hosted in server1, you still need to perform the following setup.



1. Turn on the Enable high scalability feature button.
2. Enter the protocol, host name, and port number of the Redirector machine.
3. Enter the login credentials to the Redirector machine.
4. Repeat the above steps on all other backup server that needs to join the redirector server.

Advanced Setup

Setup Wild Card Certificate

In the Redirector with a number of Backup Servers setup scenario, you need to apply a wild card certificate for all your AhsayCBS servers. When you add a new backup server or Redirector into the redirector server group, you need to apply the wild card certificate to the new server. This is cost efficient and do not require to purchase a new certificate for a new server.

Setup Replication in Redirector Server Group

Since the user profile and local user data are hosted on individual Backup Servers, if you need to setup replication in this environment, you need to setup a dedicated replication profile for each Backup Server. In our example, 4 dedicated replication profiles are required to setup.

Note: The replication can be replicated to another replication server or predefined storage.

For more information about the replication setup, please refer to the CONFIGURING REPLICATION section for details.

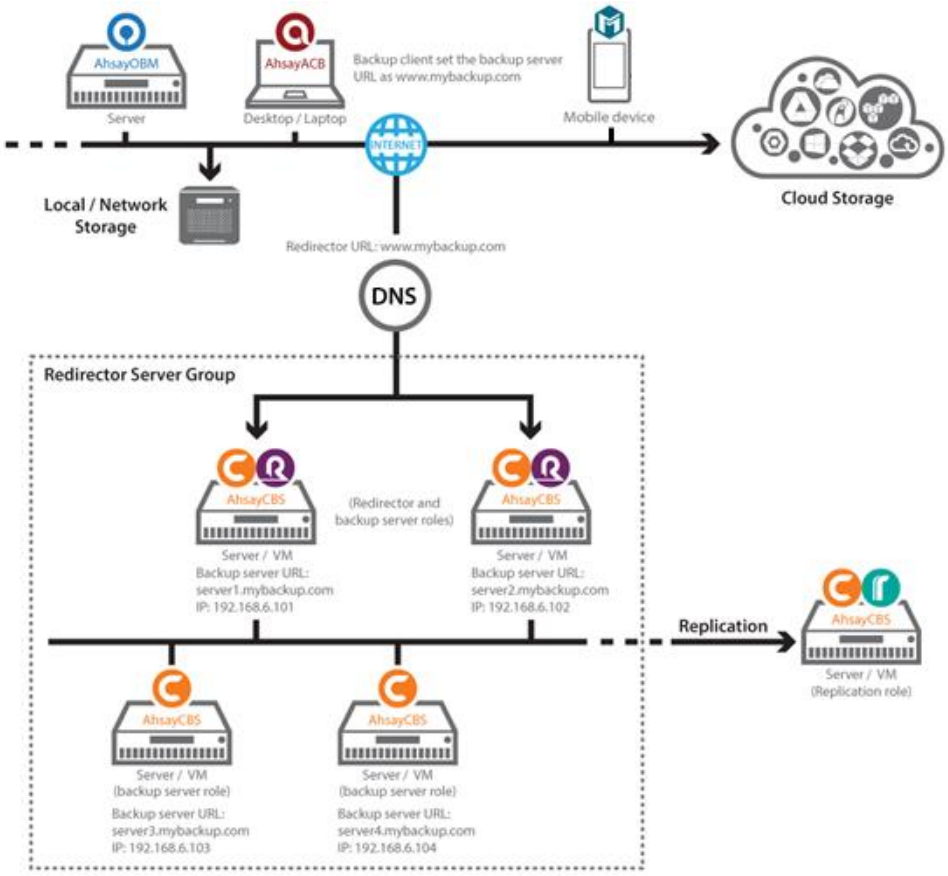
Multiple Redirector Setup

The following is an example on setting up a multiple redirector server group. The main reason is to maintain a high availability redirector.

Assumption and requirement:

In this example, we assumed that you are using a DNS round robin setup, when there is a request from the Internet, e.g.: www.mybackup.com , it will be able to redirect either to the first redirector (e.g.: server1.mybackup.com) or second redirector (e.g.: server2.mybackup.com).

For each Redirector Server, it is required to have its own redirector license key. If you setup 2 Redirector Servers, you will need 2 times of your redirector licenses.



Administrator will require setting up the following in the DNS, for example:

Name	Type	Value
www.mybackup.com.	A record	192.168.6.101
www.mybackup.com.	A record	192.168.6.102
server1.mybackup.com.	A record	192.168.6.101
server2.mybackup.com.	A record	192.168.6.102
server3.mybackup.com.	A record	192.168.6.103
server4.mybackup.com.	A record	192.168.6.104

Notes:

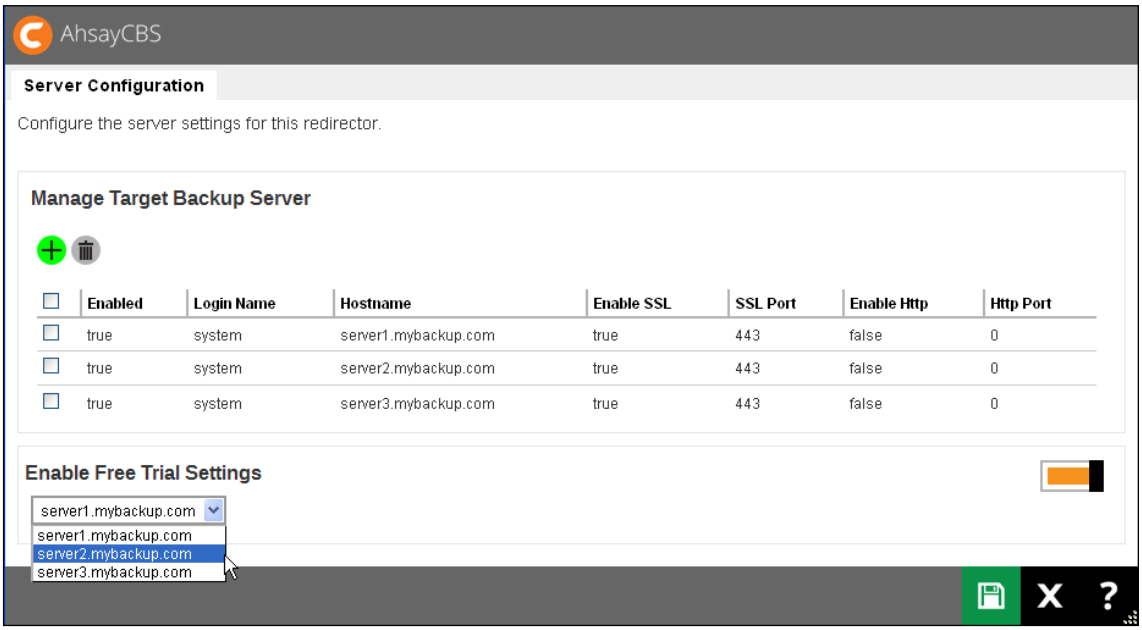
1. The round robin setting is required to redirect the traffic to either server1.mybackup.com (192.168.6.101) or server2.mybackup.com (192.168.6.102).

2. The IP address of server1 to server4 are ranged from 192.168.6.101 to 192.168.6.104.

3. The Redirector Servers are hosted on the server1.mybackup.com and server2.mybackup.com machine.

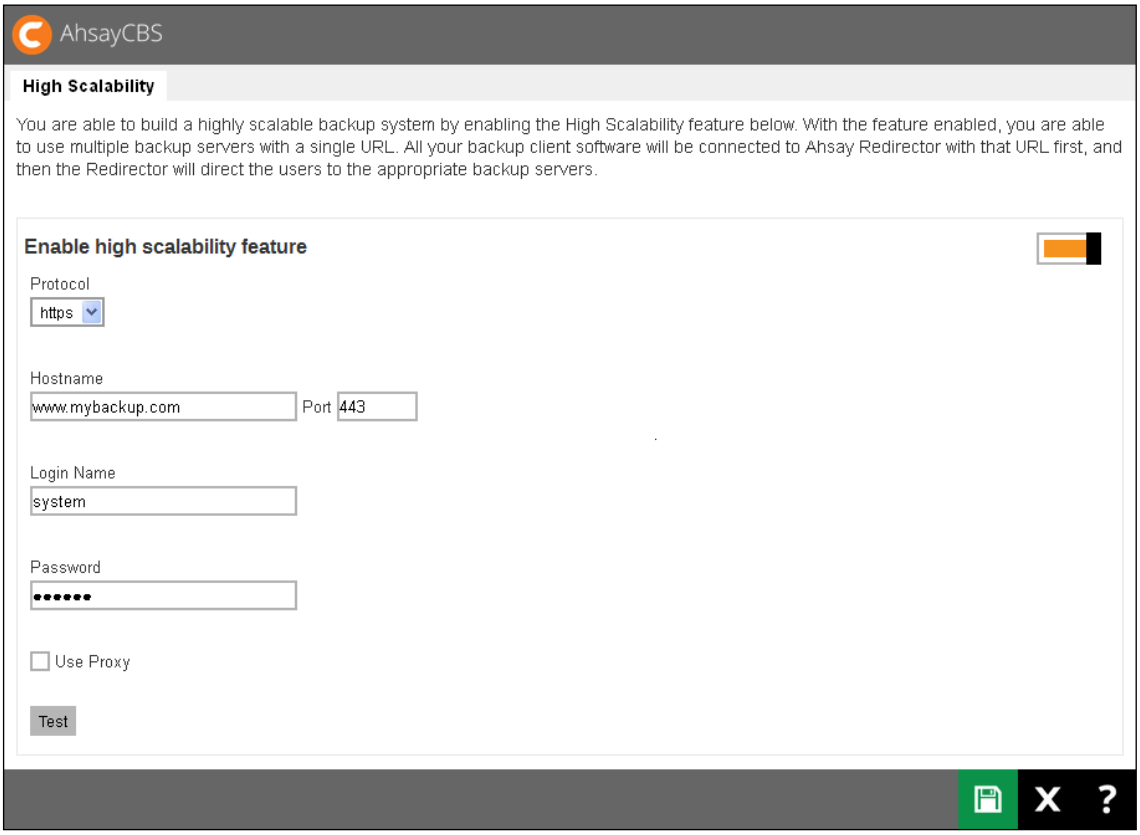
When you configure the redirector hosting on the first redirector, which we have described in the Hosting a Redirector section, same configuration is required to apply on the second redirector.

Example:



On other backup servers, you need to join the redirector.

Example:



9 Monitoring Activities

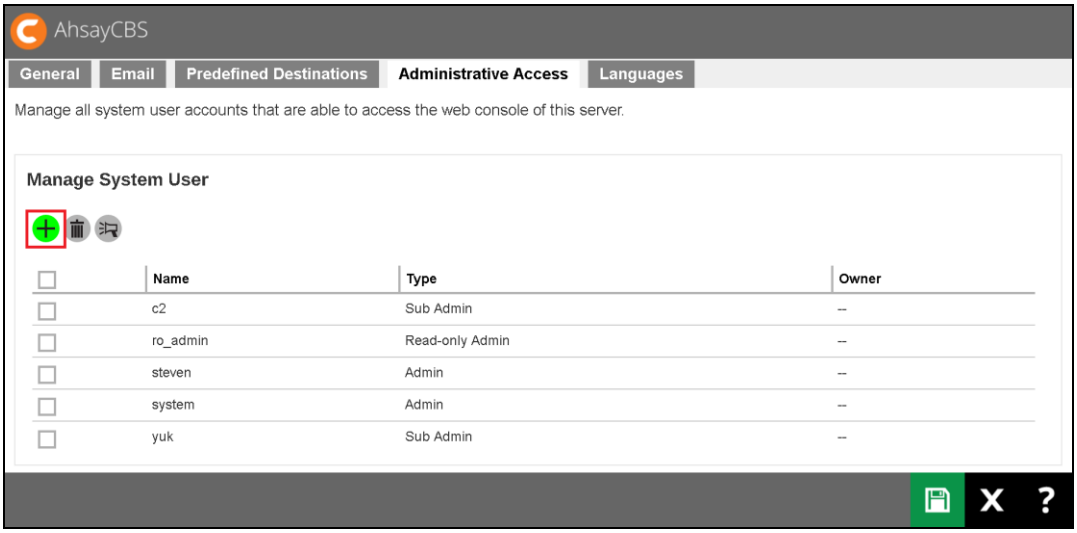
Set up a Read-only Admin Account for Operators

For daily monitoring on the AhsayCBS management console, you can assign your staff/operators with a read-only admin role account. This read-only admin role system account shares similar accessibility as its creator, except it has read-only permission. This feature is designed to help you with monitoring on the backup and restore jobs, Live Activities on the AhsayCBS server, Administration logs and Reporting etc.

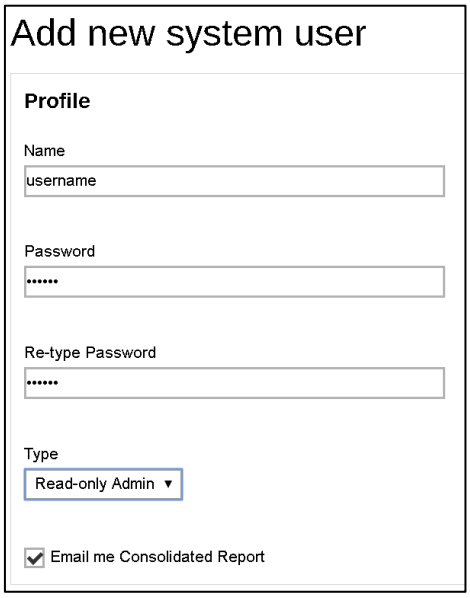
Follow the steps below to create a system user with read-only admin role:

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

2. Navigate to the **Administrative Access** tab, then click on the button under Manage System User to create a new system user.

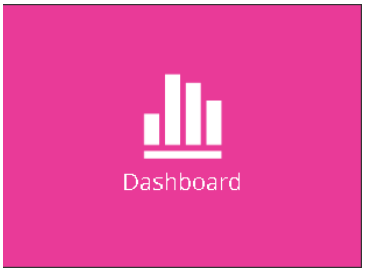


3. Fill in the details of the system user profile on the page as shown below. Make sure you have selected **Read-only Admin** under the **Type** field.



4. Click the button then the button at the bottom of the page to confirm. The system user with read-only admin role has been added.

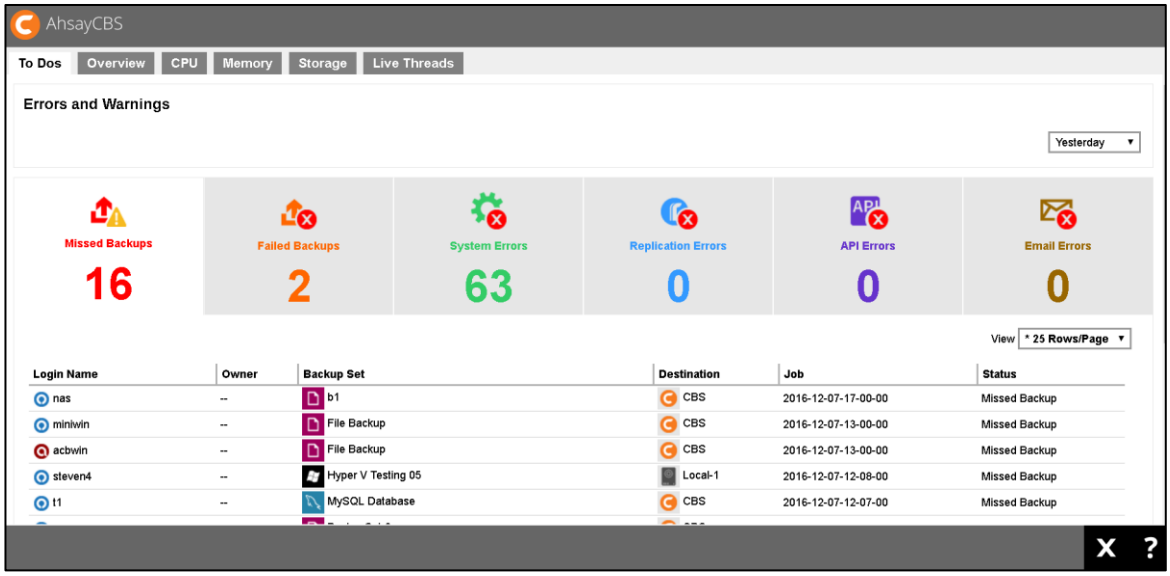
Dashboard



The dashboard is a one-stop overview providing important information that the system administrator should have attention to, for example, system errors/warnings, the system health conditions and real-time activities of the system. With this information, system administrator can quickly identify the potential issues that might pose thread to the CBS system and therefore can react accordingly to fix the issues. Below is a summary of the information that the dashboard section provides.

To Dos

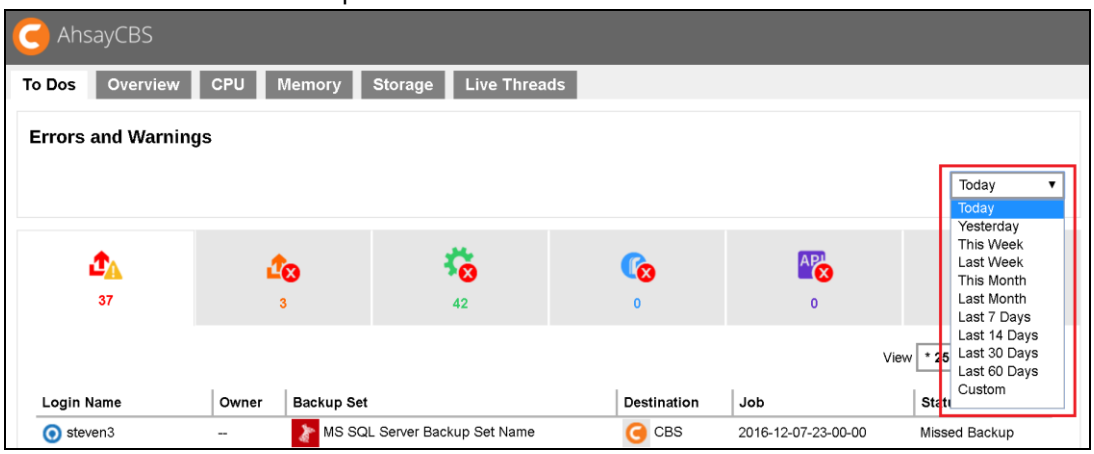
It contains system announcement, errors and warning such as "**Missed Backups**", "**Failed Backups**", "**System Errors**", "**Replication Errors**", "**API Errors**" and "**Email Errors**". Administrator or operators can base on these messages to take corresponding actions.



Viewing options

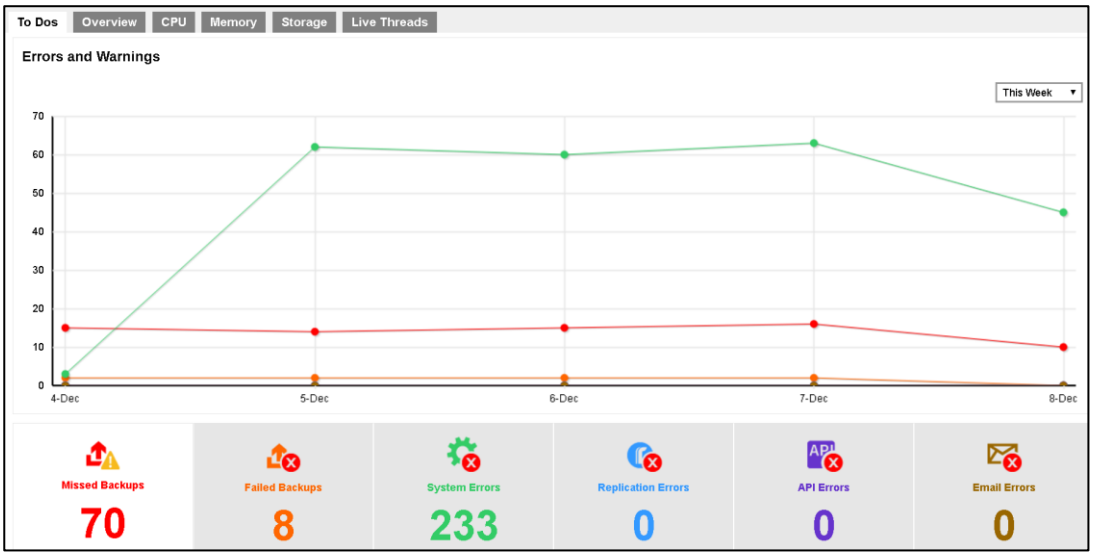
Selectable Logs Period

You can select to display the log entries of the errors and warnings from a period of time you selected. Click the drop-down menu on the right under the **Errors and Warnings** section to select the desired period of time.



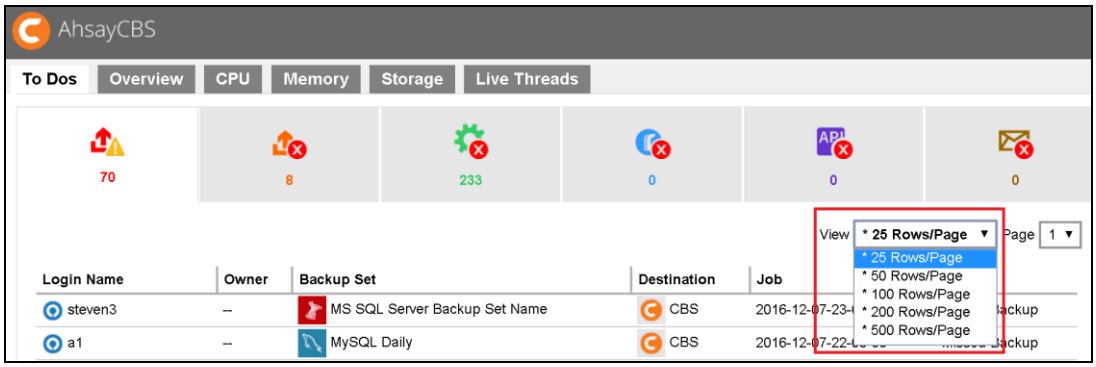
Besides selecting **Today** and **Yesterday** from the above mentioned drop-down menu, you will see a chart illustrating the number of errors for different types of errors/warning within the selected period of time.

In the chart below, for example, the **vertical axis** denotes the number of errors/warnings while the **horizontal axis** denotes the date. The lines on the chart in different colors correspond to the different types of errors/warnings as shown in the number counter below the chart in their respective colors.



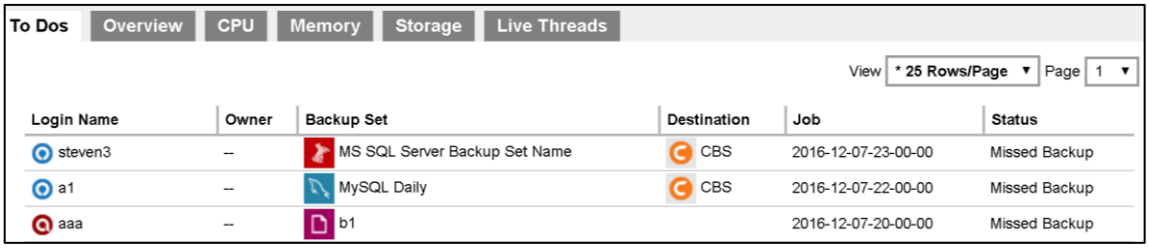
Selectable Number of Row per Page

You can also select the number of rows (i.e. the number of entries) to display on each page. Click on the drop-down menu as shown in the screen shot below to select the desired setting.



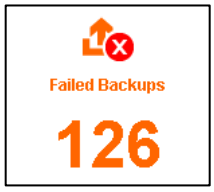
Missed Backups

This page shows all details on all missed backups from all backup users using this CBS server. Missed backup refers to backup jobs that were failed to perform according to the set backup schedules. Any backup jobs failed to perform backup 6 hours after the scheduled backup time is considered as missed backup.

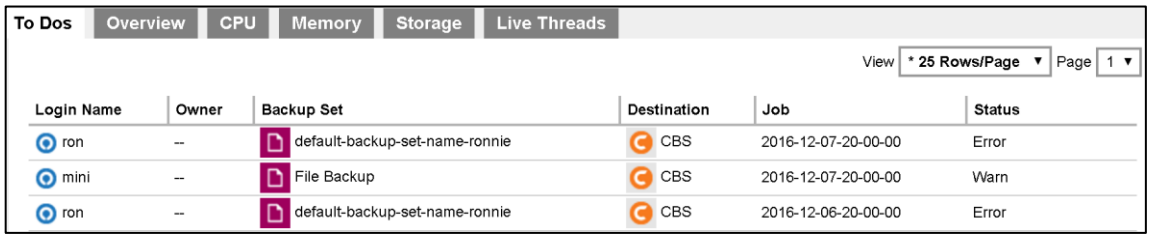


Login Name	Login name of the backup user
Owner	Ownership of the backup account
Backup Set	Name of the backup set that has missed the scheduled backup
Destination	Backup destination of the missed backup
Job	Date and time when the backup job was classified as a missed backup
Status	Status of the missed backup job

Failed Backups



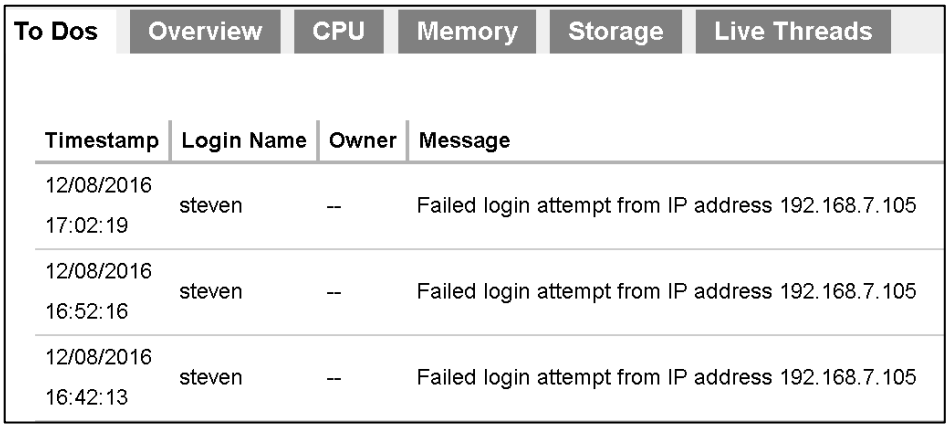
This page shows all details on all failed backups from all backup users using this CBS server. Failed backup refers to backup jobs that are not performed successfully. The backup failure could be caused by various reasons, such as storage capacity on the backup destination, Internet connection between the client backup agent and the CBS server/backup destination, user interruption during backup, etc.



Login Name	Login name of the backup user
Owner	Ownership of the backup account
Backup Set	Name of the backup set that failed to back up
Destination	Backup destination of the failed backup
Job	Date and time when the backup job failed to back up
Status	Status of the failed backup job

System Errors

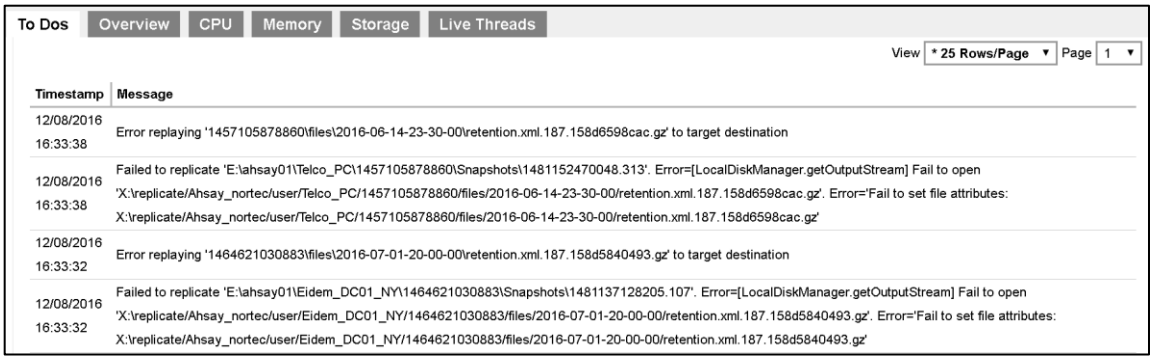
This page shows all details of system errors related to backup/restore for this CBS server. System errors include, for example, fail login attempt, login authentication failed, etc.



Timestamp	Date and time when the system error recorded
Login Name	Name of backup user in relation to the system error
Owner	Ownership of the backup account
Message	Message showing the system errors in details

Replication Errors

This page shows all details of replication error for this CBS server.



Timestamp	Date and time when the replication error recorded
Message	Message showing the replication errors in details

API Errors

This page shows all details of API errors for this CBS server.

Timestamp	Date and time when the API error recorded
Login Name	Name of backup user in relation to the API error
Owner	Ownership of the backup account
Message	Message displaying the API errors in details

Email Errors

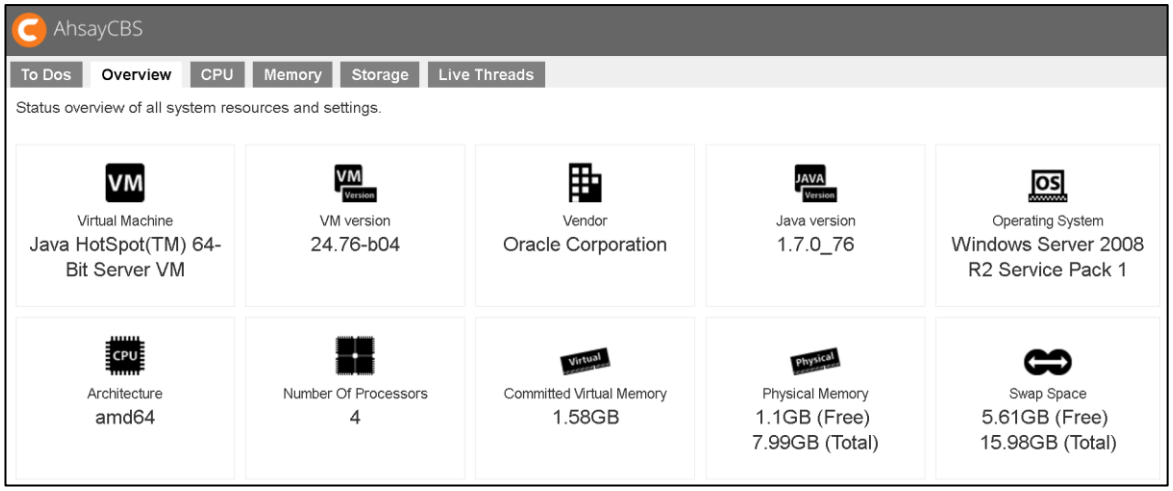
This page shows all details of email errors for this CBS server. Email errors could be caused by invalid email entered by the backup users, storage capacity of the backup user's email account, etc.

Timestamp	Date and time when the Email error recorded
Login Name	Name of backup user in relation to the Email error
Owner	Ownership of the backup account
Message	Message displaying the Email errors in details

Overview

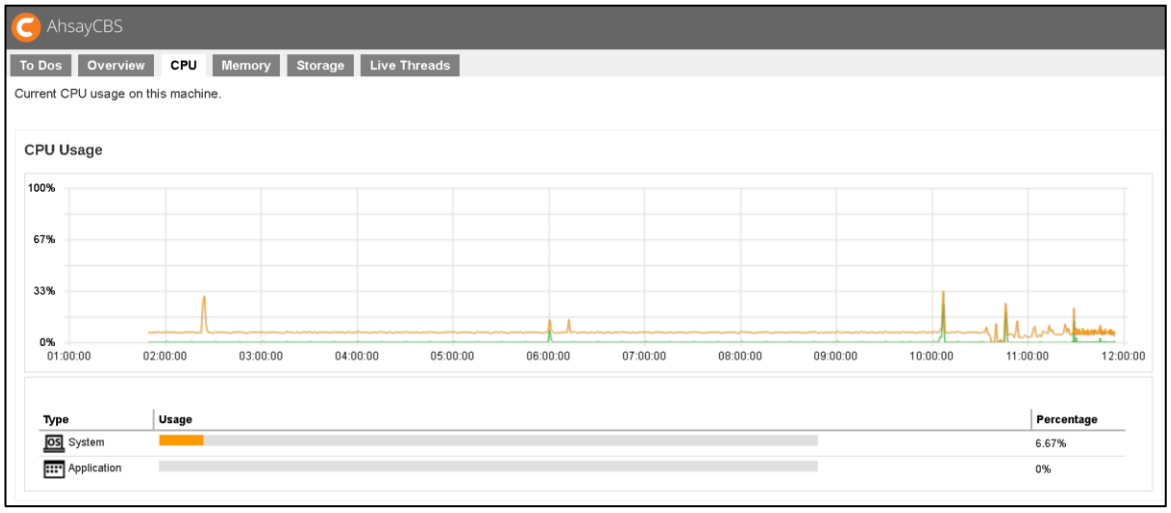
This is an overview of the system resource and system settings. These are useful information for administrator or support staff to collect machine information. This information include “Java virtual machine”, “**Java VM version**”, “**vendor of the Java**”, “**Java version**”, “**Operating System**”, “**CPU Architecture**”, “**Number of Processors**”, “**Committed Virtual Memory**”, “**Physical Memory**”, and “**Swap Space**”.

In addition, a list of system settings such as “**VM Arguments**”, “**Class Path**”, “**Library Path**”, “**Boot Class Path**” and “**System Properties**” are shown for reference.



CPU

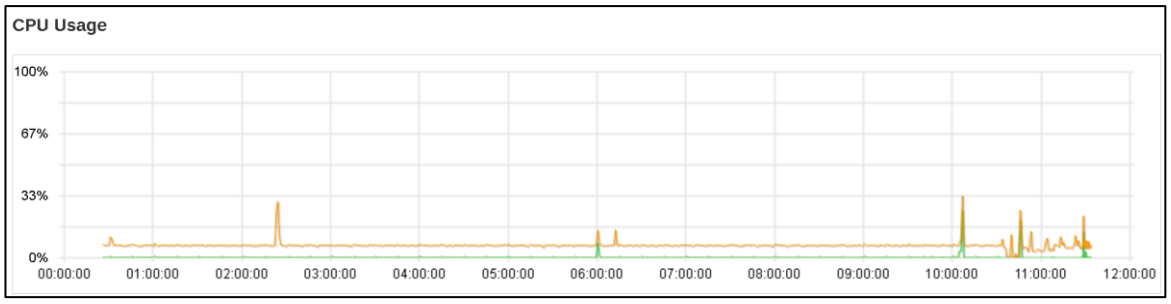
In the CPU page, you can see the current CPU utilization, the percentage that system and application occupied



There are two parts of information from this page.

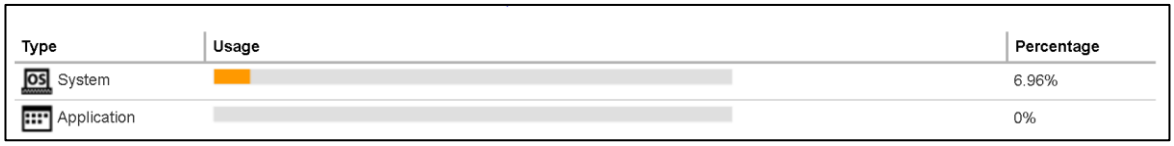
CPU Usage Chart

The CPU Usage shows the daily usage of the machine's CPU where the AhsayCBS is installed, with the vertical axis denotes and CPU utilization rate while the Y axis denotes the time.



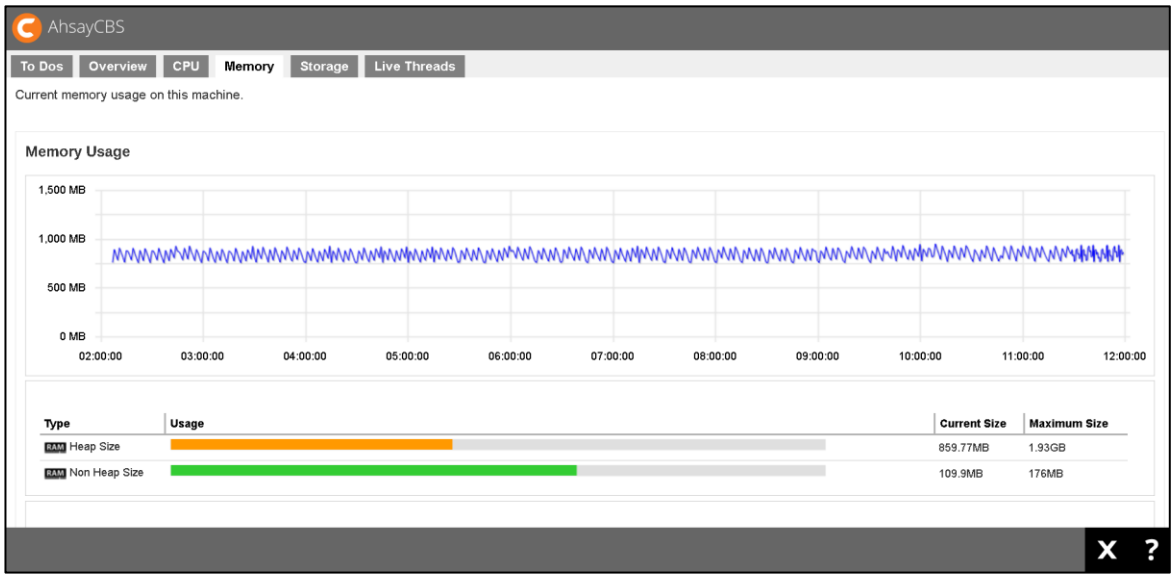
Usage Distribution

This chart shows the CPU usage distribution in percentage on System and Application.



Memory

This is a graphical view of the memory pool/managers usage on this machine.



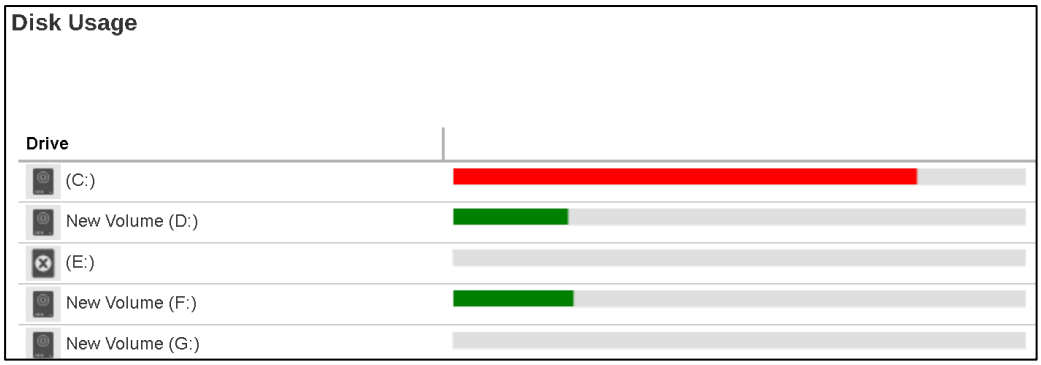
Heap memory	The heap memory is the runtime data area from which the Java VM allocates memory for all class instances and arrays.
Non-heap memory	Non-heap memory includes a method area shared among all threads and memory required for the internal processing or optimization for the Java VM.
Par Eden Space	The pool from which memory is initially allocated for most objects.
Par Survivor Space	The pool containing objects that have survived the garbage collection of the Eden space.
CMS Old Gen	The pool containing objects that have existed for some time in the survivor space.
Code Cache	The HotSpot Java VM also includes a code cache, containing memory that is used for compilation and storage of native code.
CMS Perm Gen	The pool containing all the reflective data of the virtual machine itself, such as class and method objects. With Java VMs that use class data sharing, this generation is divided into read-only and read-write areas.
Reference	Oracle JConsole documentation

Storage

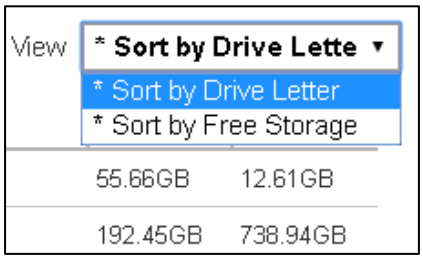
This is a local storage and predefined destination usage overview.

➢ Disk Usage

Under the Disk Usage section, it shows all the drives on the machine where the AhsayCBS is installed. You can see the capacity used (**Used**) and capacity remain (**Free**) for each drive.

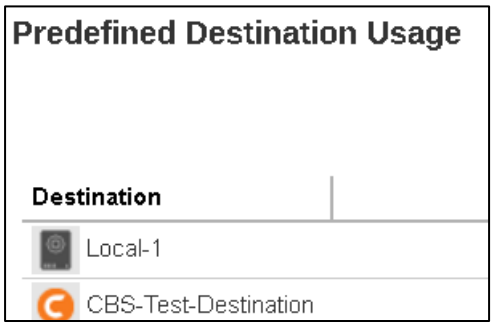


You can select to view the entries in the Disk Usage section by sorting the Drive Letter or Free Storage



➢ Predefined Destination Usage

Under the Predefined Destination Usage section, it shows all the predefined destinations that you have added under the **System Settings** > **Basics** > **Predefined Destination**.



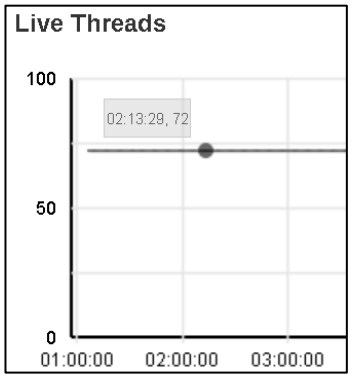
You can select to view the predefined destination entries by sorting the **Destination Name** or **Free Storage**.

Live Threads

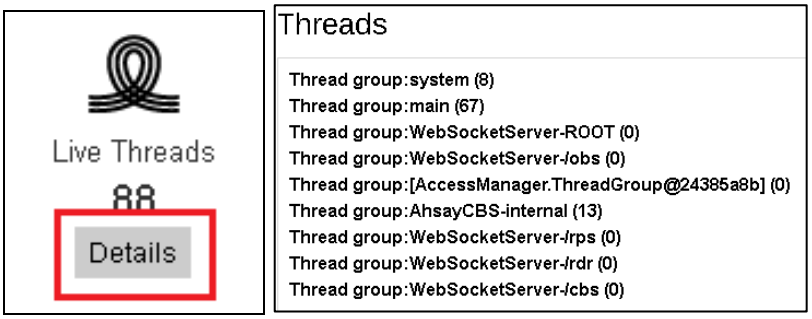
This page shows all live threads that are running on this machine.

Live Threads	Active process threads
Peak	The largest number of live threads record in the above period
Daemon Threads	Threads that are handled in the background
Total Threads Started	The total number of started threads

You can use mouse over at aby point of the curve to obtain the number of live threads at the particular time.



If you click on the Details button below the Live Threads icon, you will see a breakdown of all live threads that are running on this machine. It is shown as thread groups for developers or administrators reference.



Live Activities

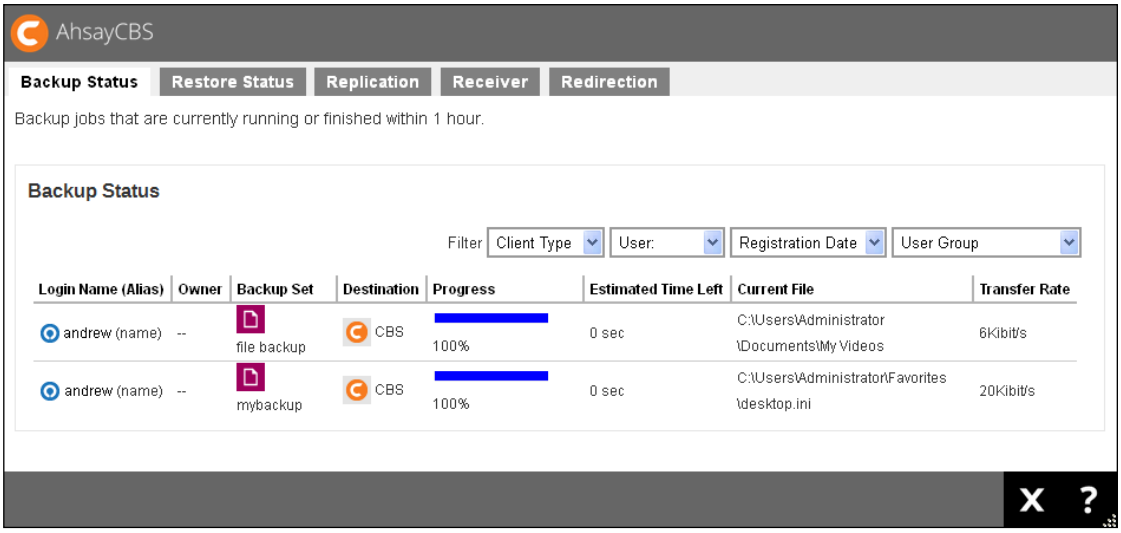
You can check on recent backup and restore status with the progress monitor in percentage, replication (both send and receive) and redirection status.

Backup Status

Available Backup Jobs Can Be Monitored by Live Activities			
Backup Type	**AhsayOBM**	**AhsayACB**	**AhsayMOB**
File Backup	✓	✓	✓
Cloud File Backup	✓	✓	NA
IBM Lotus Domino Backup	✓	NA	NA
IBM Lotus Notes Backup	✓	✓	NA
MS Exchange Server Backup	✓	NA	NA
MS Exchange Mail Level Backup	✓	NA	NA
MS SQL Server Backup	✓	NA	NA
MS Windows System Backup	✓	✓	NA
MS Windows System State Backup	✓	NA	NA
MS Hyper-V Backup	✓	NA	NA
MySQL Backup	✓	NA	NA

Office 365 Exchange Online Backup	✓	✓	NA
Oracle Database Server	✓	NA	NA
ShadowProtect System Backup	✓	NA	NA
VMware Backup	✓	NA	NA

This section shows a list of backup job(s) that is currently running or has finished within the past 1 hour.



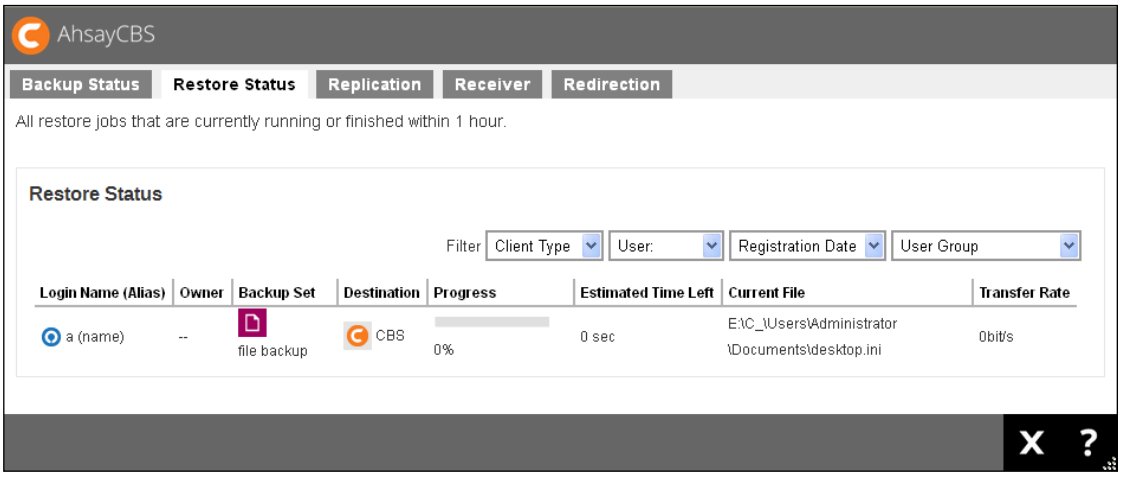
Restore Status

Available Restore Jobs Can Be Monitored by Live Activities					
Restore Type		**AhsayOBM**	**AhsayACB**	**AhsayOBR**	**AhsayMOB**
File	**Normal Restore**	✓	✓	✓	✓
	OpenDirect Restore	✗	✗	✗	NA
Cloud File Backup		✓	✓	✓	NA
IBM Lotus Domino Backup		✓	NA	✓	NA
IBM Lotus Notes Backup		✓	✓	✓	NA
MS Exchange Server Backup		✓	NA	✓	NA

MS Exchange Mail Level Backup		✓	NA	✓	NA
MS SQL Server Backup		✓	NA	✓	NA
MS Windows System Backup		✓	✓	✓	NA
MS Windows System State Backup		✓	NA	✓	NA
MS Hyper-V	**Normal Restore**	✓	NA	✓	NA
	Run Direct Restore	✓	NA	✓	NA
	Granular Restore with AhsayOBM File Explorer	✓	NA	✓	NA
	Granular Restore with Windows File Explorer	✗	NA	✗	NA
MS SQL Server Backup		✓	NA	✓	NA
MySQL Backup		✓	NA	✓	NA
Office 365 Exchange Online Backup		✓	✓	✓	NA
Oracle Database Server		✓	NA	✓	NA
ShadowProtect System Backup		✓	NA	✓	NA
VMware	**Normal Restore**	✓	NA	✓	NA
	Run Direct Restore	✓	NA	✓	NA
	Granular Restore with AhsayOBM File Explorer	✓	NA	✓	NA

	Granular Restore with Windows File Explorer	✗	NA	✗	NA

This section shows a list of restore job(s) that is currently running or has finished within the past 1 hour.

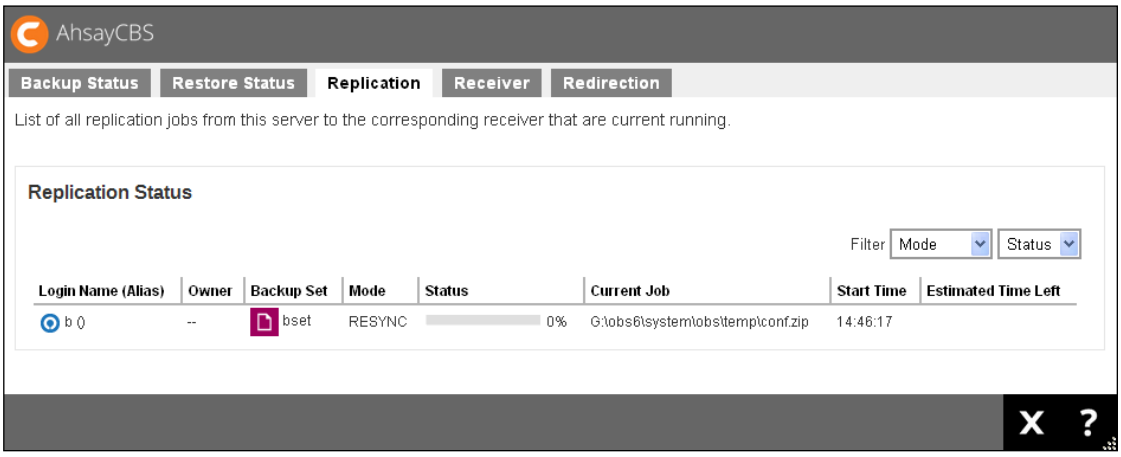


NOTE

OpenDirect restore of file backup sets or granular restore from VMware and Hyper-V backup sets performed using Windows File Explorer will not show up on the [**Restore Status**] tab in Live Activities. This only applies to restores performed directly through AhsayOBM/AhsayACB/AhsayOBR/ AhsayMOB or AhsayCBS User Web Console.

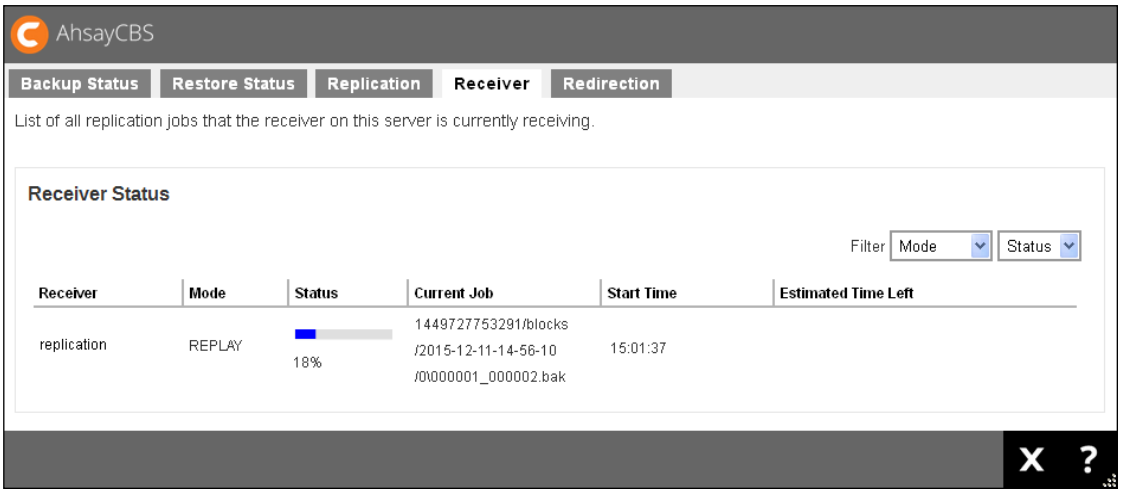
Replication

Here is the replication jobs status from the backup server to the corresponding receiver.



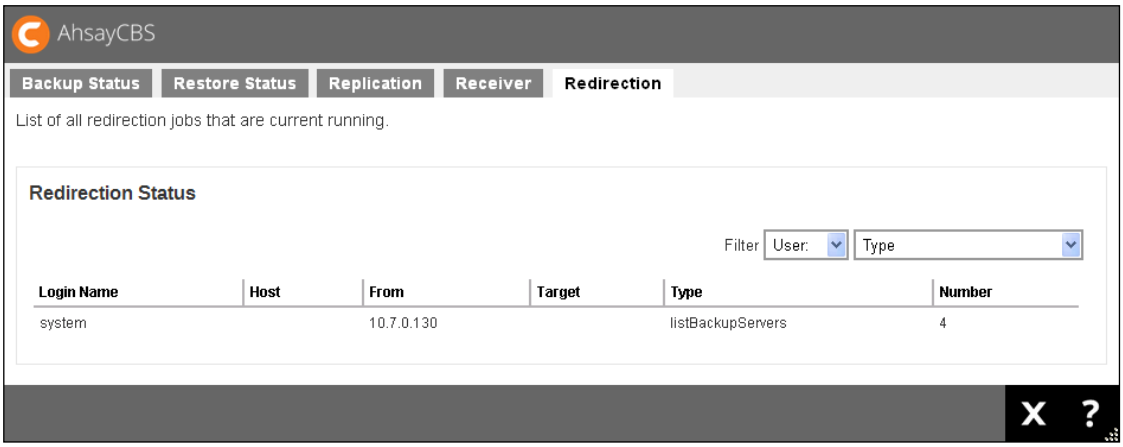
Receiver

In this menu, you will see all the replication jobs that the receiver on this server is currently running.

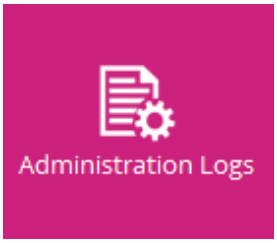


Redirection

You can see a list of all redirection jobs that are currently running.



Administration Logs



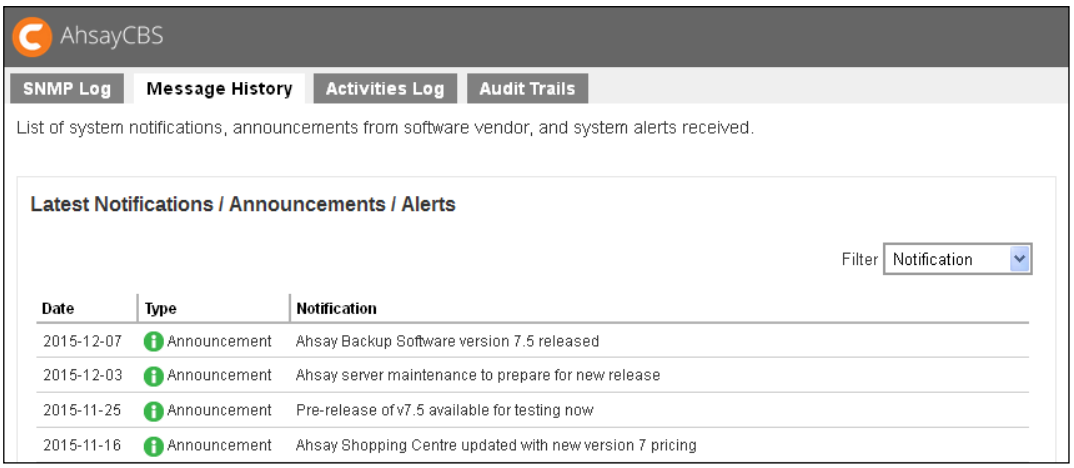
You can check on the SNMP logs, list of notifications/announcements/alerts, and activities log (system logs) and audit trails.

SNMP Log

You can see a list of SNMP log message in this page. You need to enable the SNMP log in **Settings** -> **Advanced** -> **Logging** -> **Enable SNMP Service**, and need to download the MIB definition file and pass to your SNMP machine.

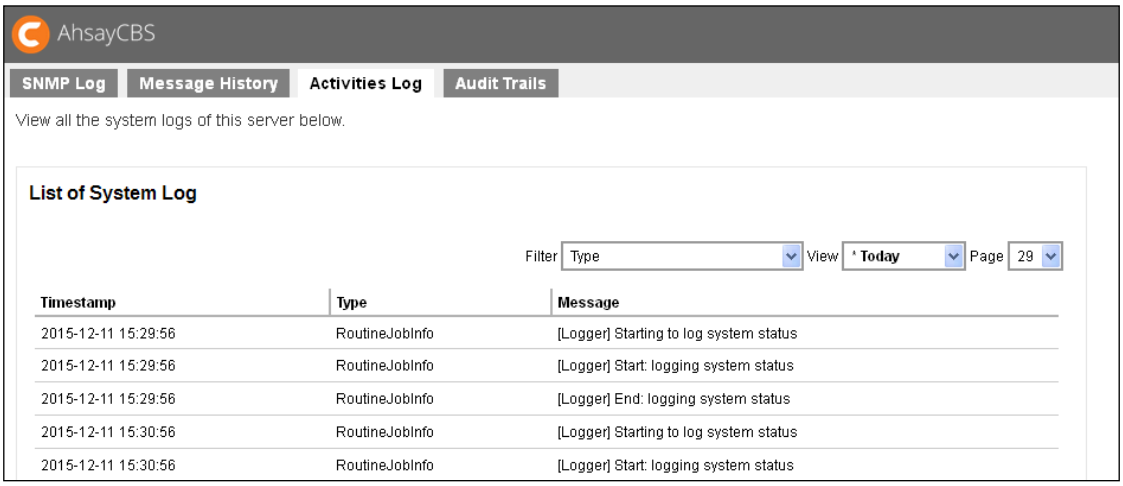
Message History

This page contains a list of notifications, announcements and alerts.



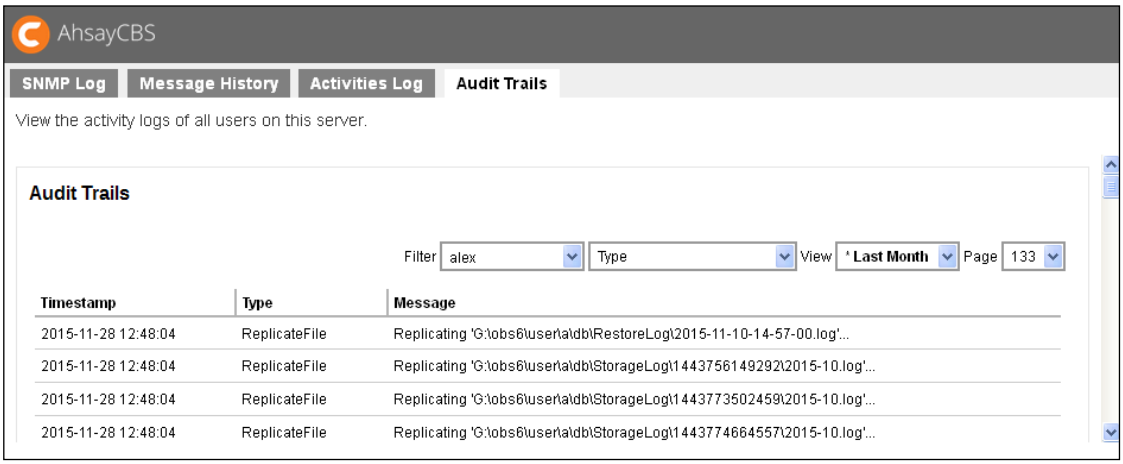
Activities Log

In this page, you will see a list of activities/system logs generated by the system events, v6 migration or other user activities.

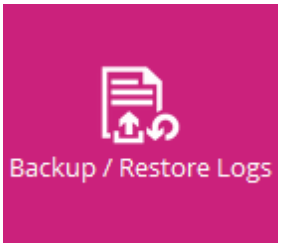


Audit Trails

In this page, you can see the activity logs of all users on this server.



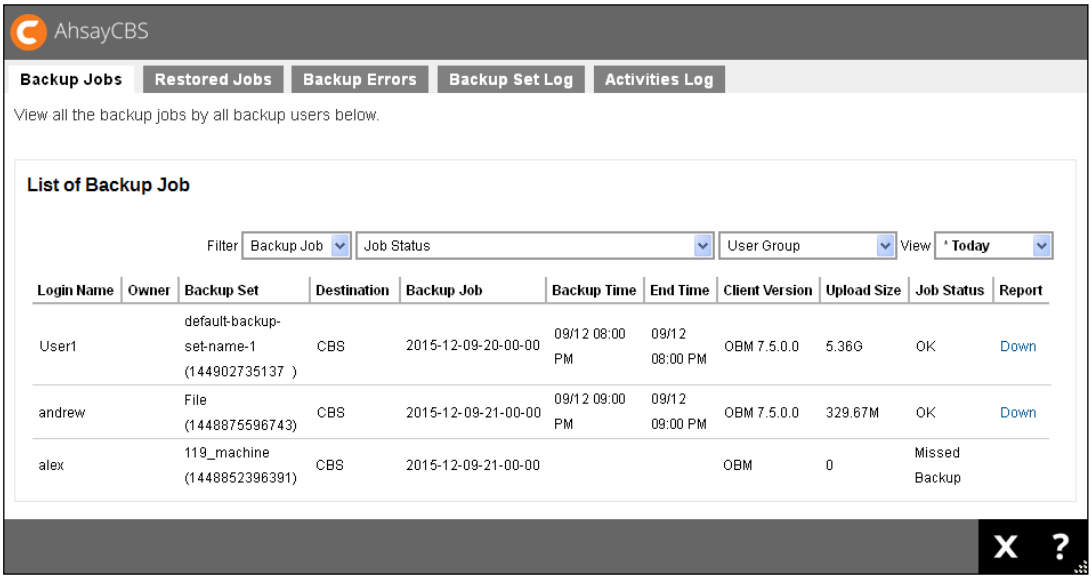
Backup / Restore Logs



You can check on a list of backup and restore jobs, backup errors, backup set logs, and activities logs.

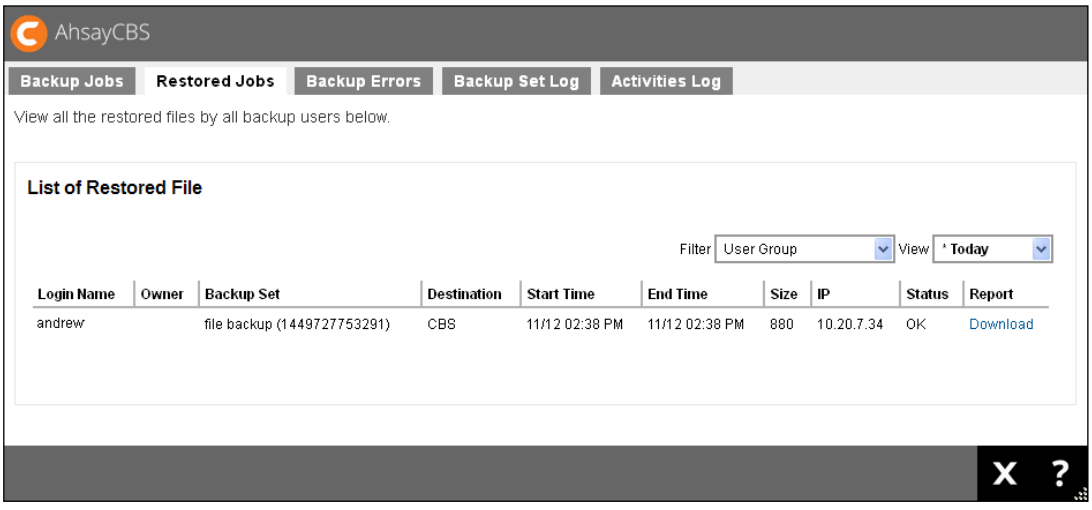
Backup Jobs

Here is summary of the backup jobs.



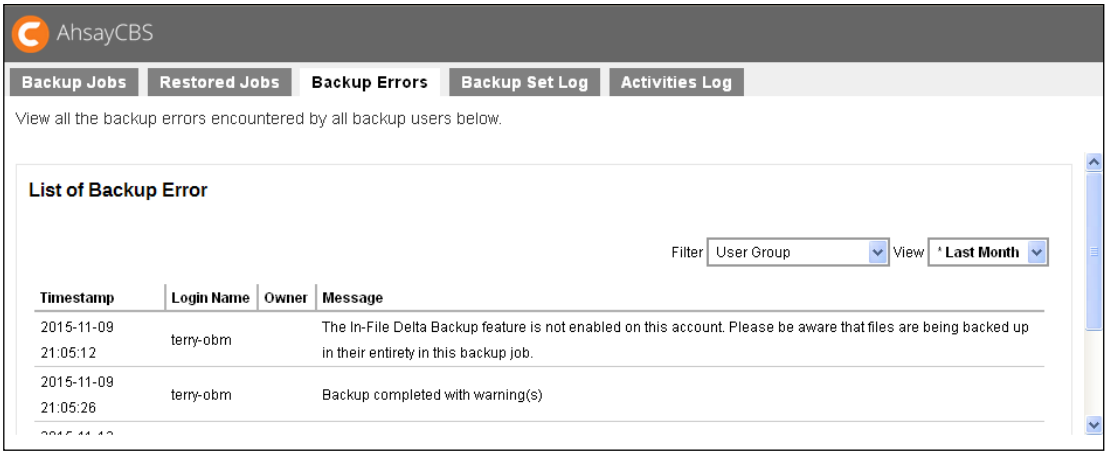
Restored Jobs

Here is a summary of the restored jobs.



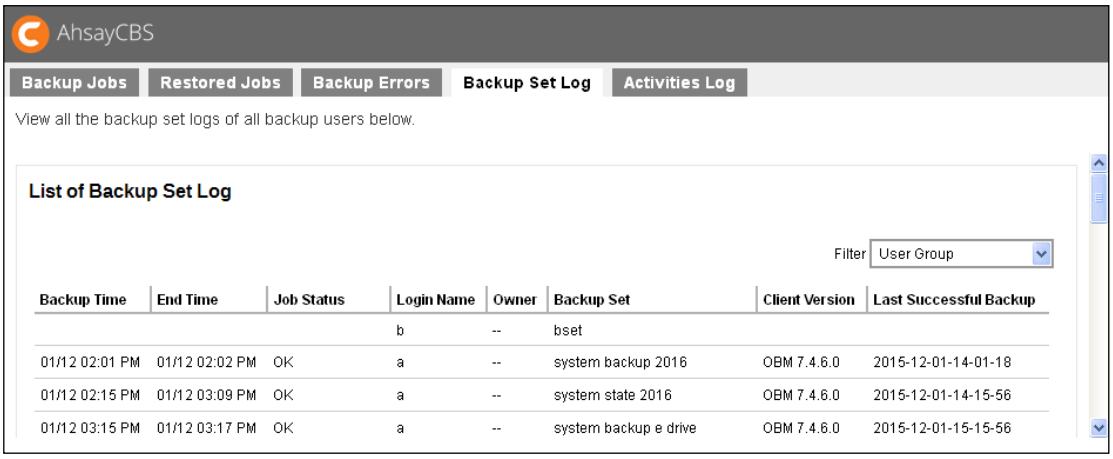
Backup Errors

Here is a summary of the backup errors encountered by all backup users.



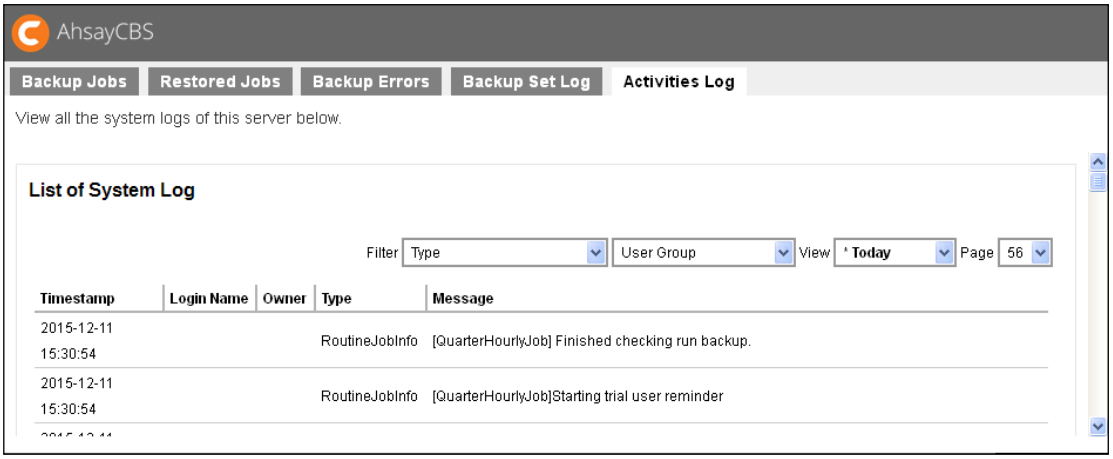
Backup Set Log

Here is a summary of backup set logs of all the backup users.

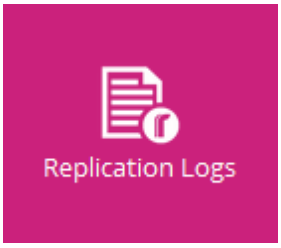


Activities Log

Here is a list of user backup/restore related system activities logs.



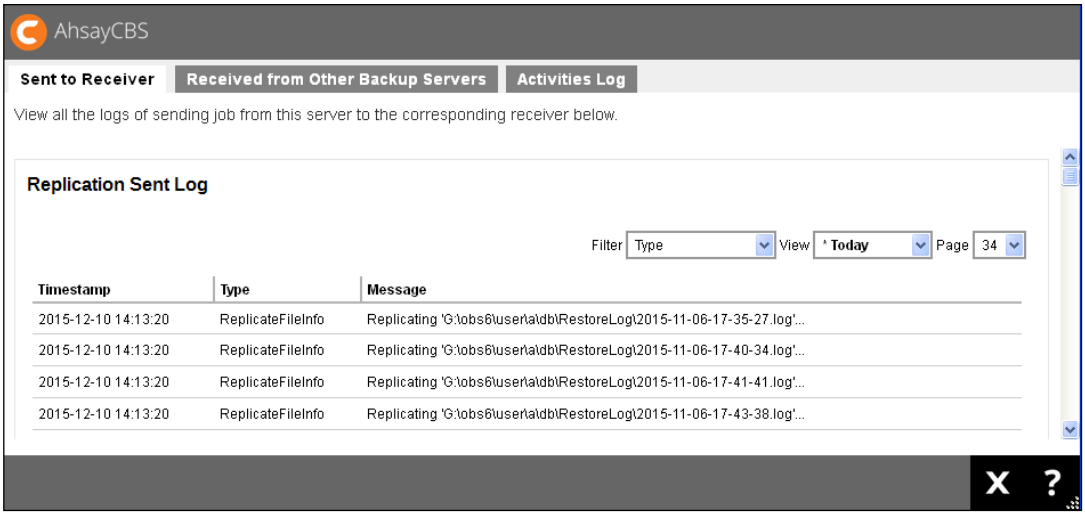
Replication Log



You can check on both send and receiver logs, and activities logs.

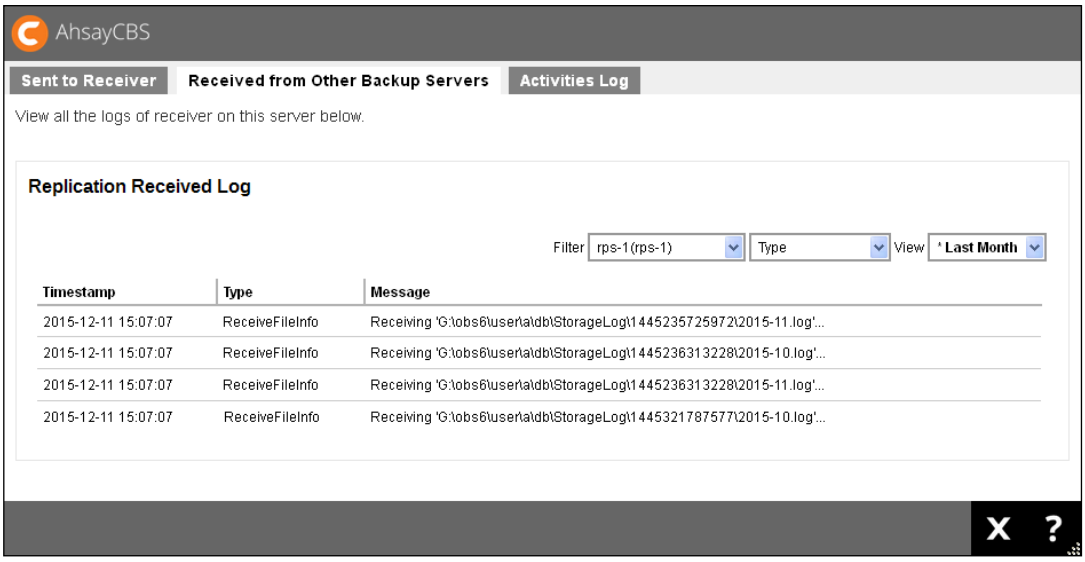
Sent to Receiver

You can see a list of sending job from the AhsayCBS to the corresponding receiver.



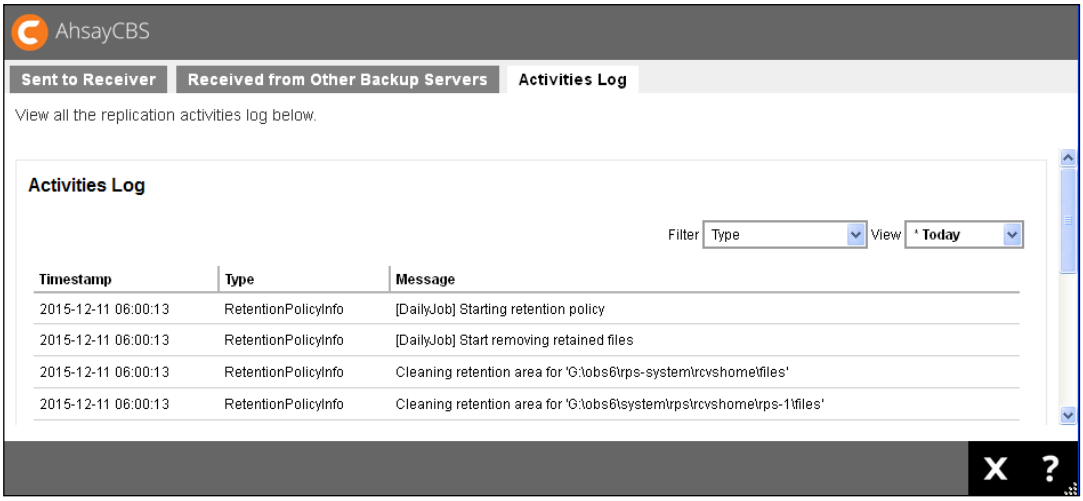
Received from Other Backup Servers

Here is the log of receiver on the AhsayCBS.

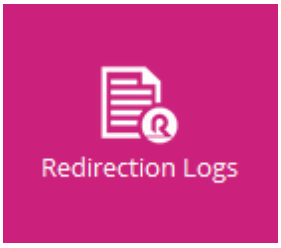


Activities Log

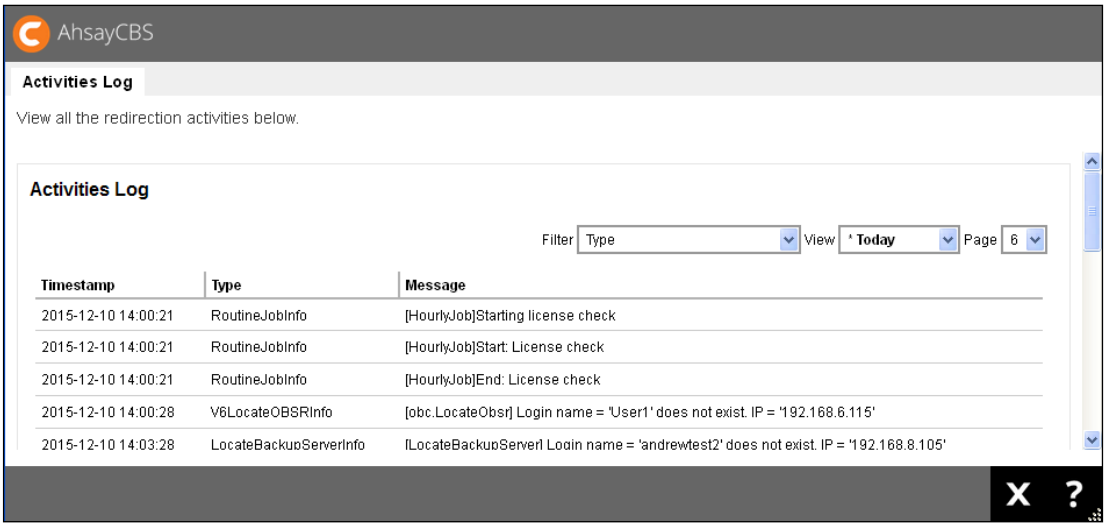
Here is the page to view all the replication activities log, such as retention policy job.



Redirection Logs

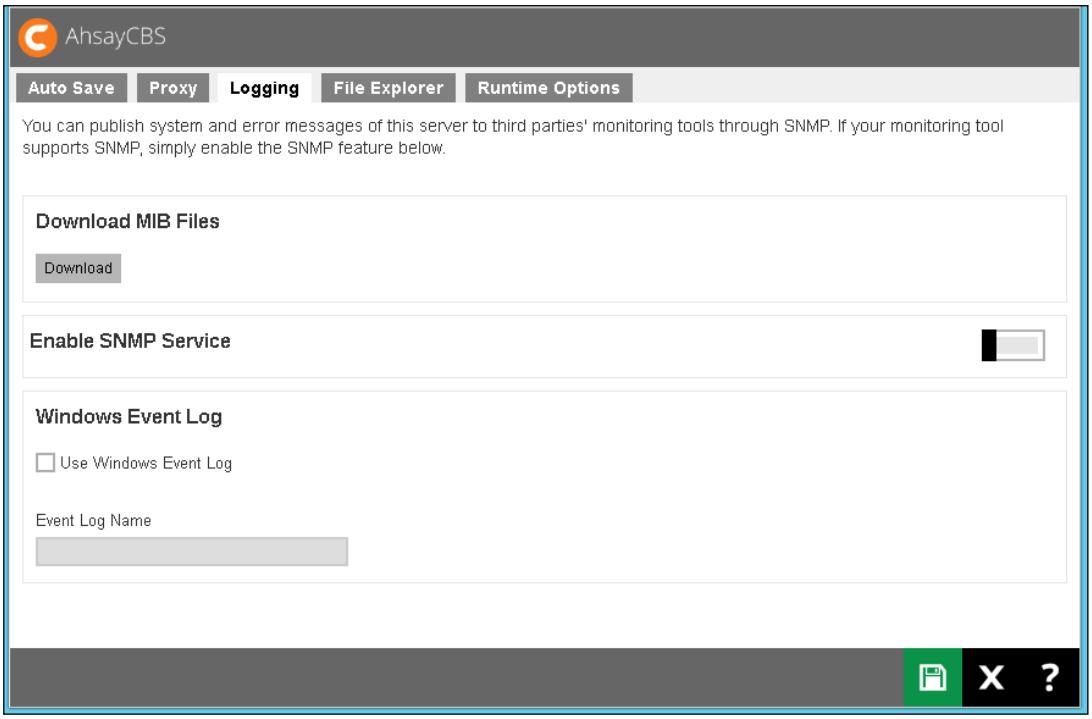


You can check on the redirection activities logs in this menu.



Enable Third Party Monitoring Tools

You can set up third party monitoring tools such as SNMP and Windows Event Log (Windows only) in **System Settings -> Advanced -> Logging**.



10 Branding the AhsayCBS

This chapter describes the steps to brand the AhsayCBS/AhsayUBS.

Since version 7.7, you can brand the AhsayCBS and generate new AhsayCBS installers and AhsayUBS image files from the AhsayCBS interface.

Prerequisite

A Rebranding license is required for this feature to work. Evaluation license does not support this feature. If you do not have a license yet, visit the Ahsay Shopping Centre – Rebranding page to purchase one.

Before Getting Started

Here are the suggested steps for you to complete the process.

1. Prepare the logos, properties, application settings and digital signature to be applied in the **Rebrand Clients** section, which will be reflected in the Client Backup Agents (AhsayACB/AhsayOBM).
2. Generate the AhsayOBM/AhsayACB installers for testing.
3. Prepare the logos, properties, cascade style sheet, connector/SSL certificate settings and customized report templates to be applied in the **Rebrand Web Console** section, which will be reflected in the AhsayCBS web console.
4. Generate the AhsayCBS installer for testing.
5. **Optional:** AhsayUBS image file generation. Select either 'ISO' or 'IMG' as the format for image file generation. The image file will be the installation file for the AhsayUBS.

AhsayUp Upgrade Service and AhsayUp+ Upgrade Service

Subscribe our premium upgrade service to enjoy a smooth and effortless upgrade experience. Click here to learn more about the differences between the AhsayUp Upgrade Service and AhsayUp+ Upgrade Service, or visit the Ahsay Shopping Centre directly to subscribe the service.

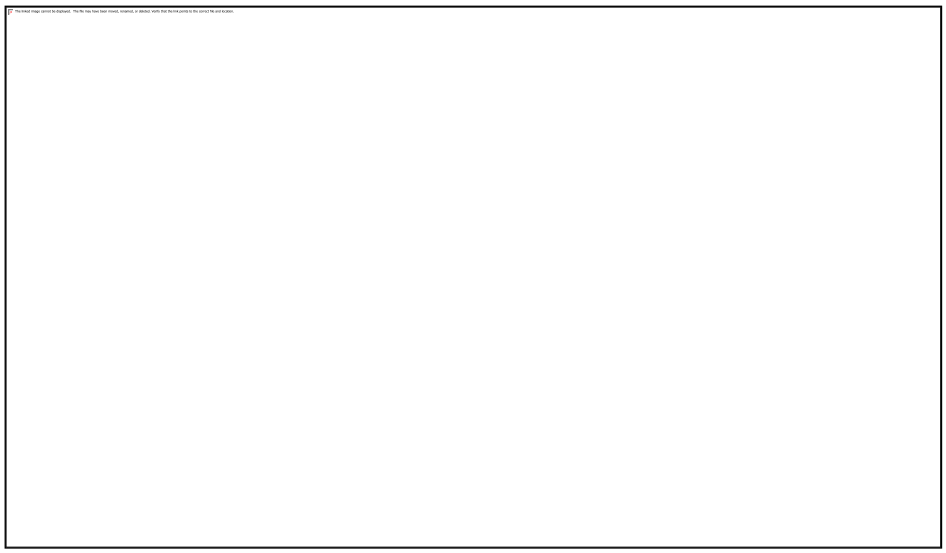
For the images specifications, please refer to the Appendix F.

Prepare Branding for AhsayCBS Interface

After you have installed the AhsayCBS, you can upload the graphics and customize the properties.

1. Login to the AhsayCBS management console as "**system**" user.

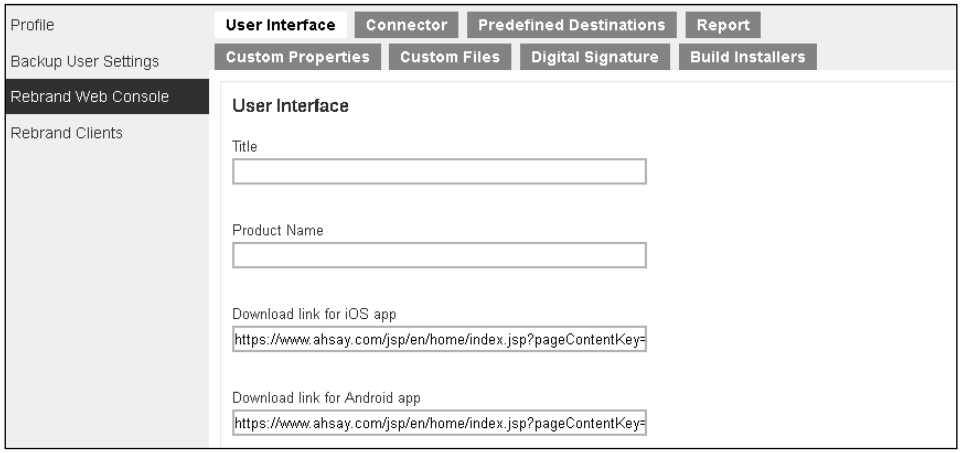
2. Click in System Settings -> Basic -> Administrative Access.



3. Click on the "**system**" user to brand the AhsayCBS.

   If you are testing this feature, please create a sub admin user and test the following steps, this is because when new installers are generated, the existing installers will be overwritten with the new ones.

4. Click on the **Rebrand Web Console** section on the left.



5. Enter the following fields under the **User Interface** tab.

6. **Title** – The name to be displayed on the title bar of the browser.

7. **Product Name** – The name to be displayed in the software license page.

8. **Download link for iOS app –** The URL link directs users to iOS App Store to download AhsayMOB.

9. **Download link for Android app –** The URL directs users to Android Google Play to download AhsayMOB.

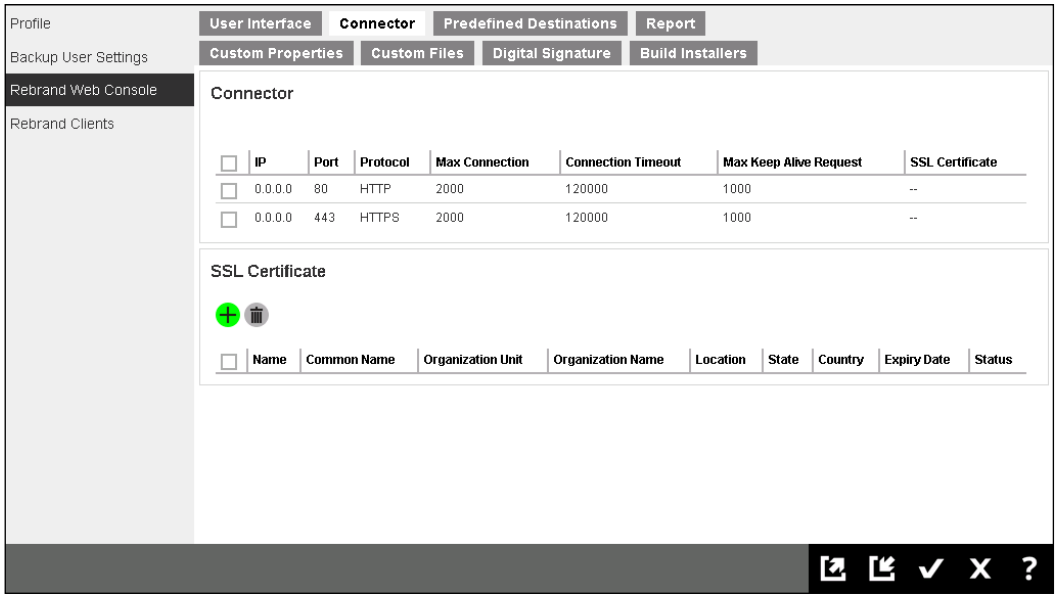
NOTE

Although it is possible to define the URLs to download the AhsayMOB application from iOS and Android platforms, please kindly note that AhsayMOB is not brandable.

10. Upload the branding image for the AhsayCBS interface. Please refer to the branding image specifications listed on Appendix F, you can download the default logo/icon for reference.

11. At the bottom of this page, you can upload the Cascade Style Sheet (CSS) for the AhsayCBS interface.

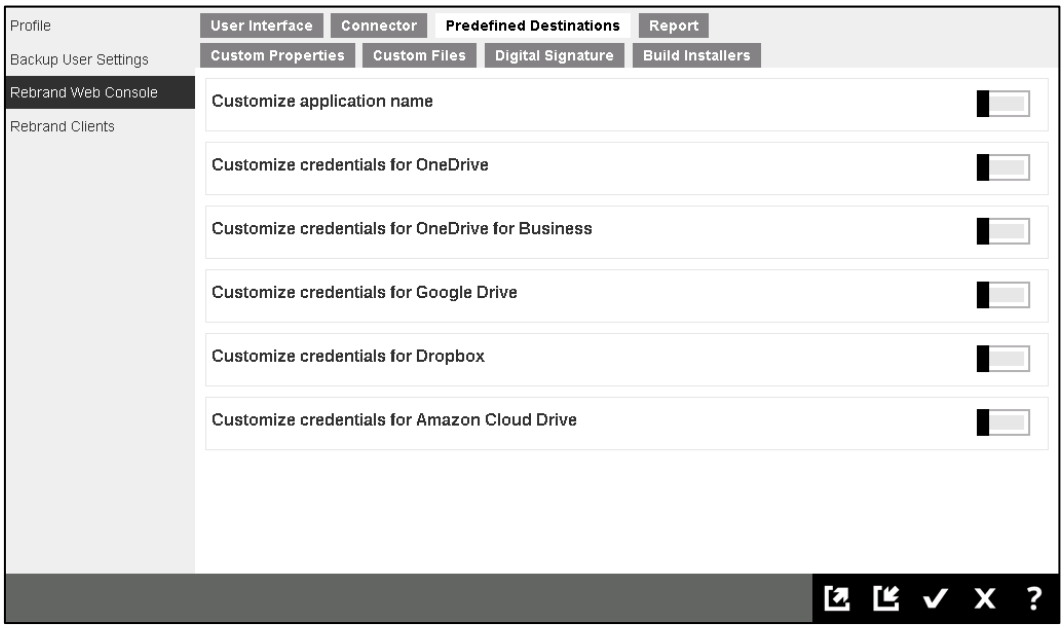
12. Click on the **Connector** tab if you need to change the connector settings and SSL settings. These settings will be applied to your new installers.



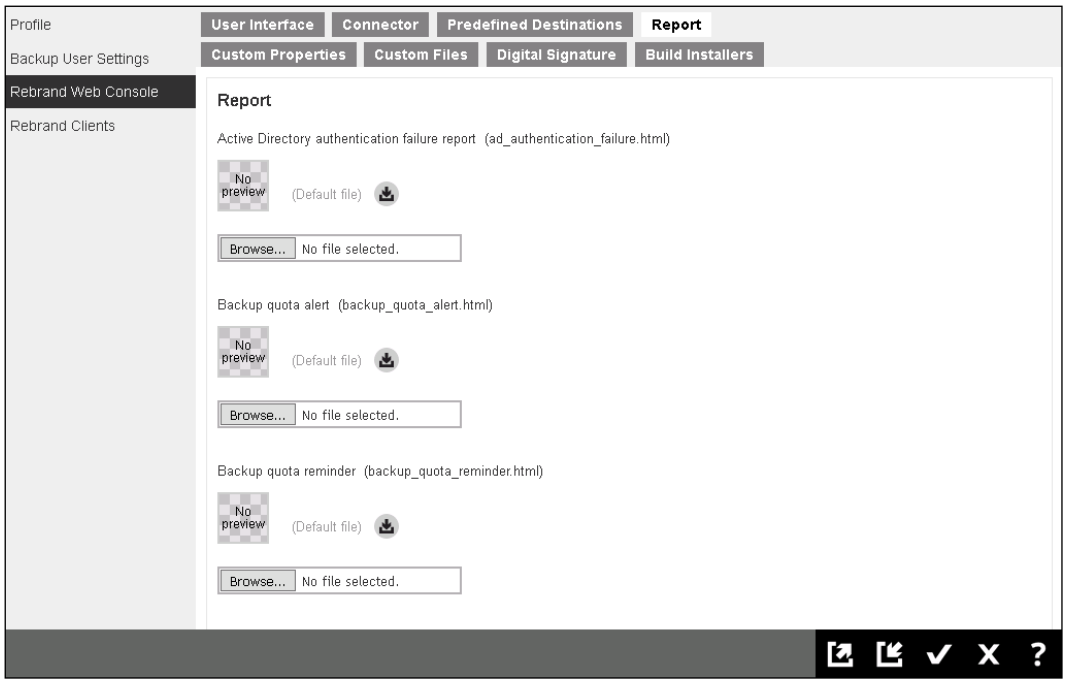
If you will generate the AhsayUBS installer, please reserve the port 8080 for the AhsayUBS web admin interface.

13. Click on the **Predefined Destinations** tab if you need to customize the application name for standard destinations or the credentials for Cloud storage. Please refer to the Customize Application Name on Cloud Storages for instruction.

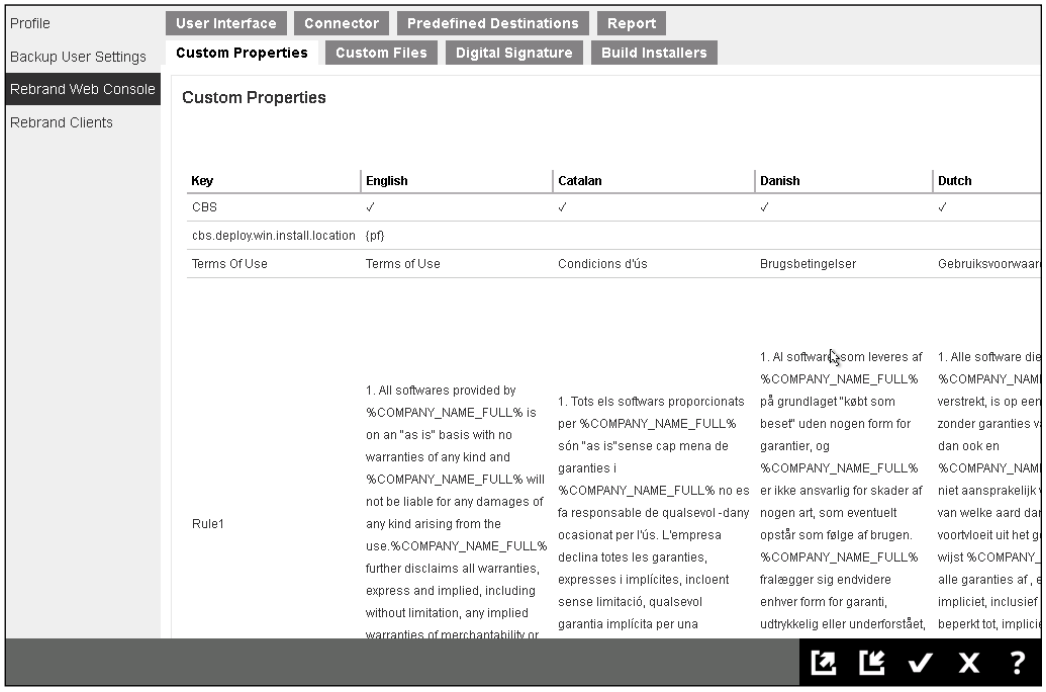
Note: OpenStack, Dropbox, Local, AhsayCBS, Destination Pool and OneDrive destinations cannot be customized.



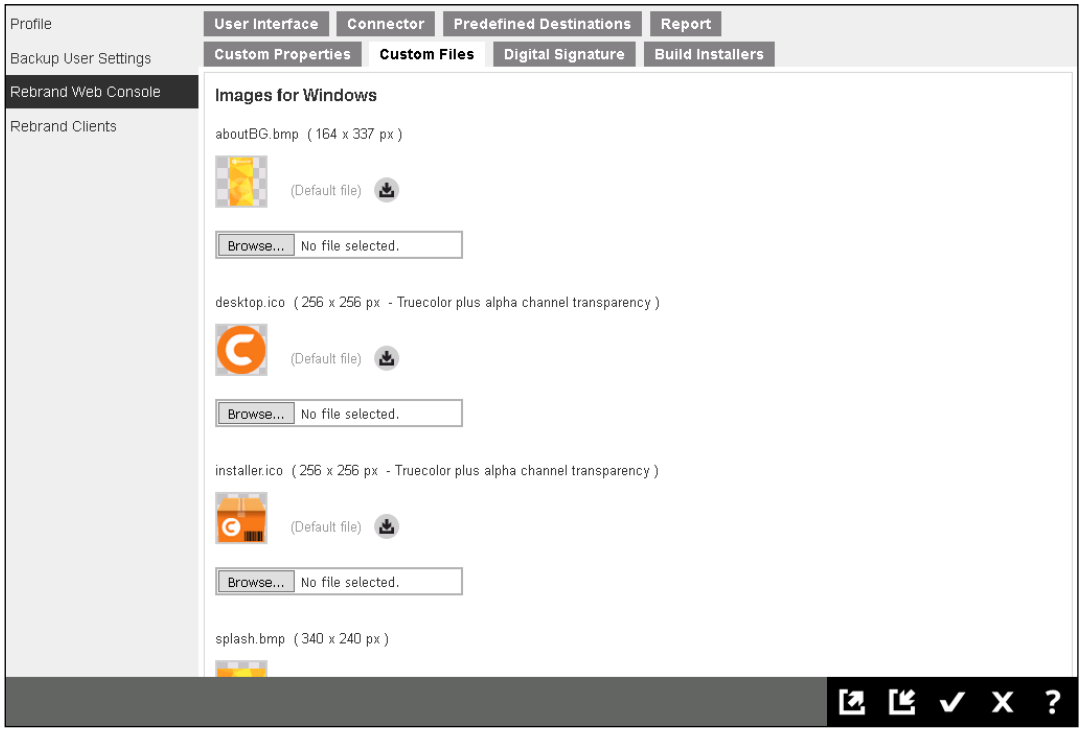
14. Click on the **Report** tab if you want to modify the HTML template. These templates will be applied to your new installers.



15. Click into the **Custom Properties** tab if you want to modify the properties on the AhsayCBS. These properties will be applied to your new installers.



16. Click into the **Custom Files** tab. Upload the branding image for the AhsayCBS installer/AhsayUBS image file. Please refer to the branding image specifications listed on the Appendix F, you can download the default logo/icon for reference.

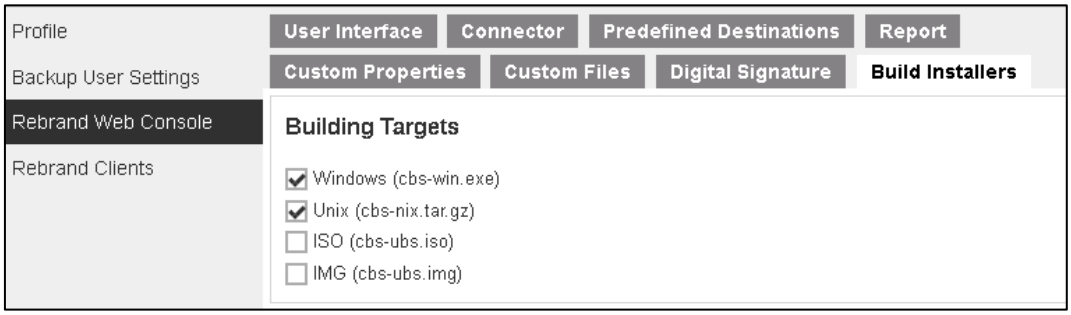


17. If you have uploaded the digital signature in **Rebrand Clients** > **Digital Signature**, it will be applied to your new Windows installer.

18. Click on the **Build Installer** tab.

Note: The new AhsayOBM/AhsayACB will be generated and overwrite your existing installers.

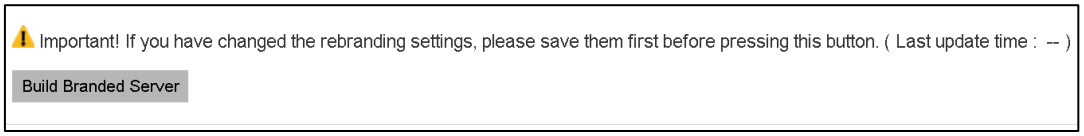
19. Select the installer(s) or image file(s) to generate. You can also select the AhsayUBS image file generation. Before you use this option, you may test the AhsayCBS installer generation first, this can save the generation time and download time before you can finalize your branding work.



20. If you wish to rebrand the AhsayCBS to resellers using your own branding and to prevent resellers from knowing the software is from Ahsay and changing the branding, you can check the **Disable branding feature on customized web management console** checkbox. With this feature enabled, the **Rebrand Web Console** and **Rebrand Clients** sections in the web management console of the CBS installer to be generated will be disabled. In that case, backup users will not see any Rebrand parameters with Ahsay wording.

21. Click and to save all the settings before generating the installer.

22. Go back to the **Build Installers** tab, click on the **Build Branded Server** button to generate new AhsayCBS installer or AhsayUBS image file.



Please be patient, the installer generation process should take around 10 to 15 minutes for each installer/image. The generation time would depend on the traffic condition on the customization portal.

23. You can download branded AhsayCBS installer from the download page.

24. In case there are any problems when building the installer, you will be able to see the logs by clicking on the **Download Log** button.

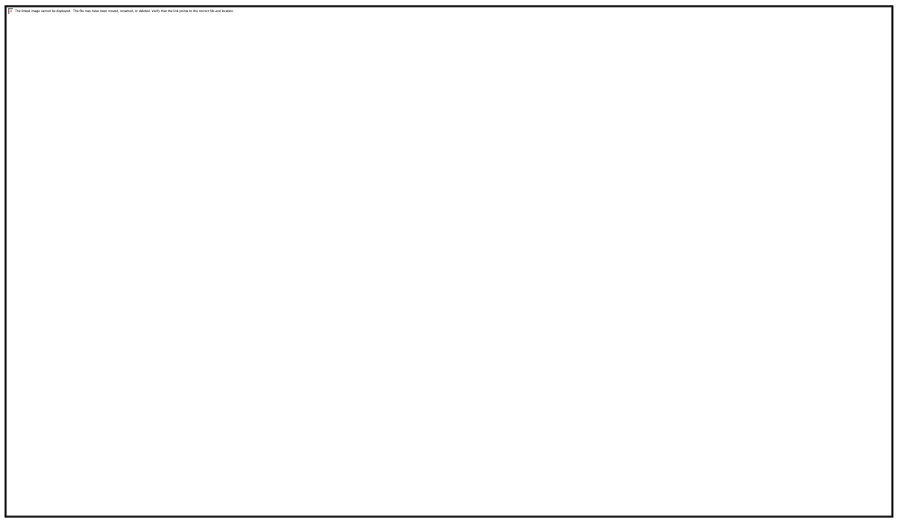
By clicking on the **Download Log** button, you can download the branding log file "**cbs-log.zip**" and you can take a look into the log for troubleshooting the branding issue.

Prepare Branding for AhsayOBM/AhsayACB

Follow the steps below to brand the AhsayOBM/AhsayACB.

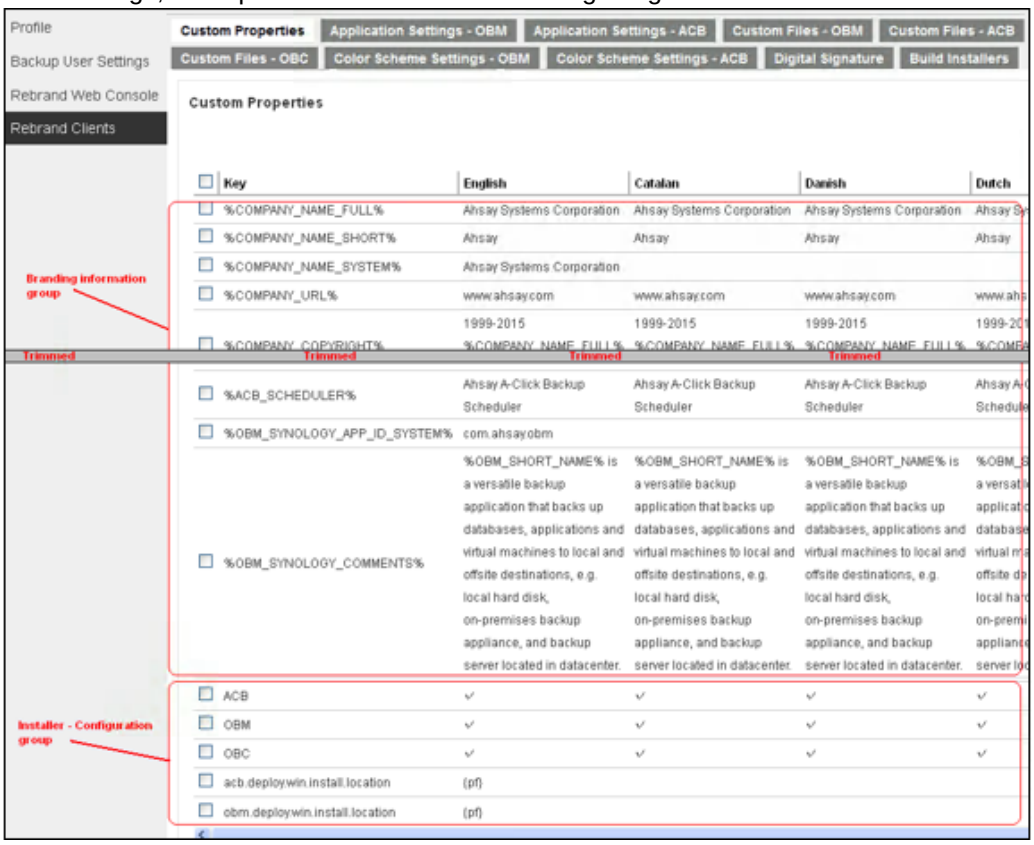
1. Login to the AhsayCBS management console with “system” account.

2. Click in **System Settings -> Basic -> Administrative Access**.

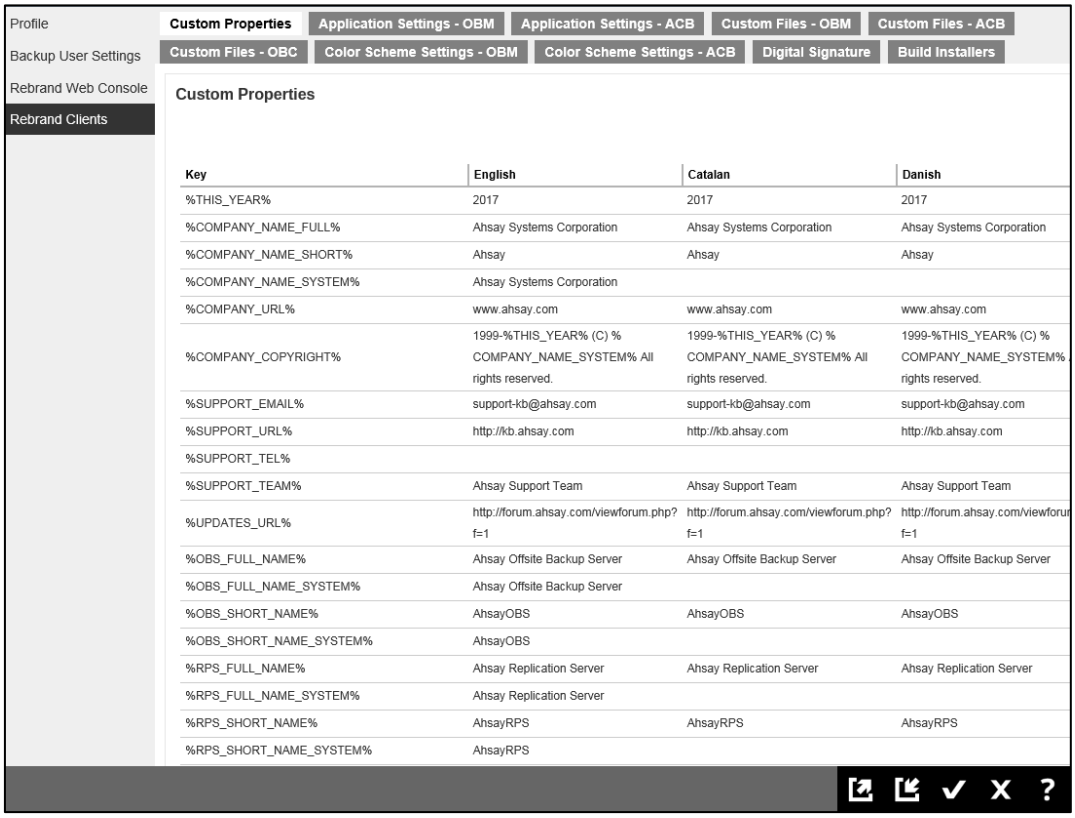


3. Click on the “**system**” user to brand the client. If you are testing this feature, please create a sub admin user and test the following steps, this is because when new installers are generated, the existing installers will be overwritten with the new ones.

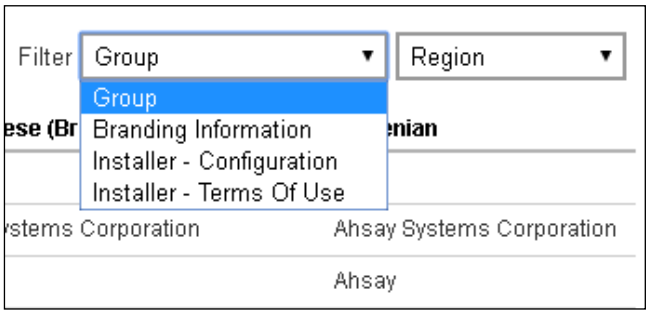
4. Click on the **Branding Clients** where you can customize the properties, apply the OBM, ACB settings, and upload OBM and ACB branding images.



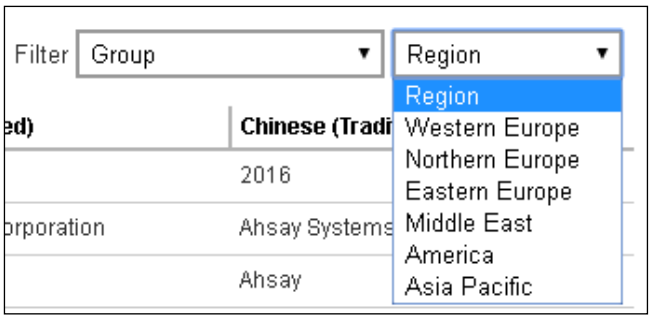
5. First, click on the **Custom Properties** tab.



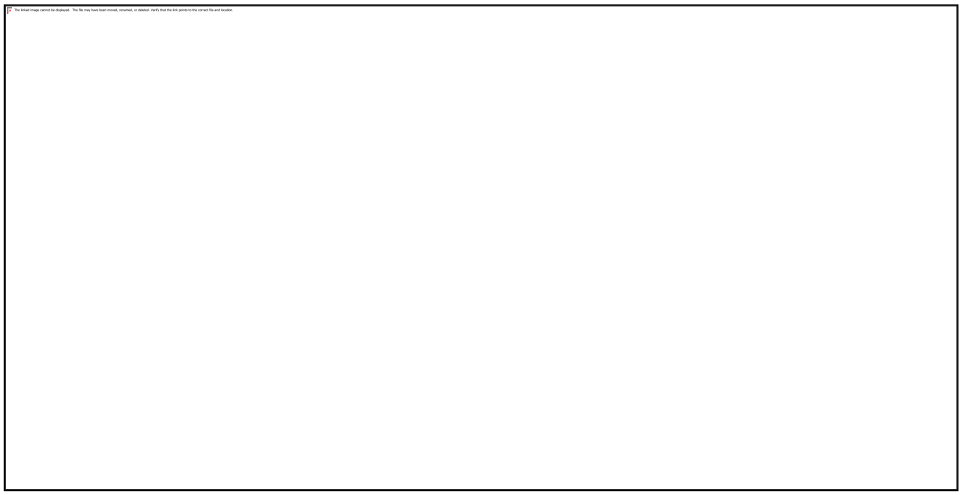
i. There are three categories of branding properties on this page, they are "**Branding information**", "**Installer – Configuration**" and "**Installer - Terms of Use**". By default, you will be able to branding properties of all categories, you can also select the desired category by using the filter on the right hand side of the page.



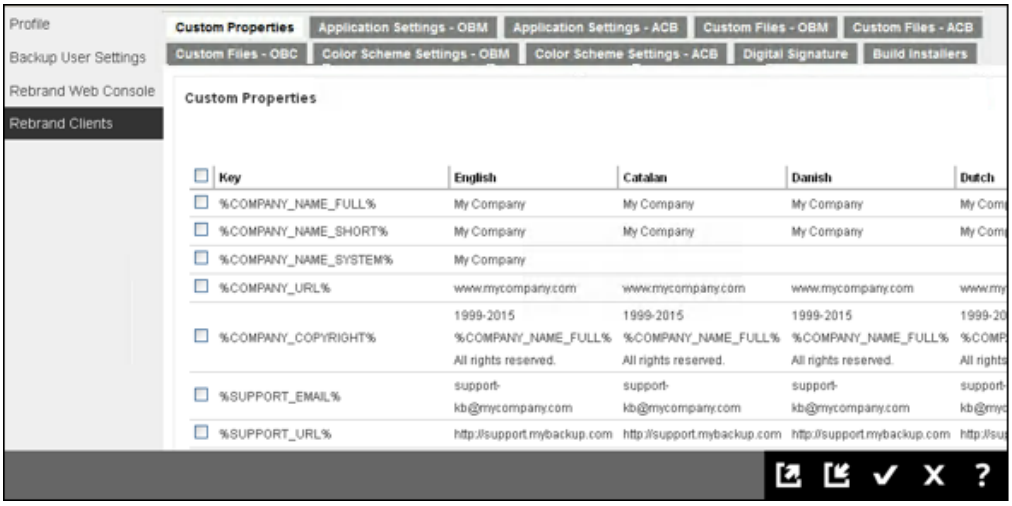
ii. You can also filter the language displayed on this page by using the **Region** drop-down menu.



iii. By clicking into each item, you can modify the name of each property in different languages. Click on ✔ at the bottom right corner to continue.



iv. You will be able to see the modified branding properties as shown.



NOTE

From v7.15.0.0, AhsayCBS makes some constraints for the system properties, which are defined as follow:

Short System Property (%XXX_SHORT_NAME_SYSTEM%)

- Accepts alphabet and/or numeric character(s)

General System Property (%XXX_SYSTEM%, except for Short System Property, %OBM_SYNOLOGY_APP_ID_SYSTEM% and %SOCIAL_MEDIA_LINK_XXX_SYSTEM%)

- Only accept alphabet, numeric and/or space character(s)

%OBM_SYNOLOGY_APP_ID_SYSTEM%

- Accepts alphabet, numeric and/or dot character(s)
- The length cannot exceed 128 characters

Install Location Properties (i.e. acb.deploy.win.install.location and obm.deploy.win.install.location)

- Cannot be empty

In order to meet the above constraints, some default values of system properties are modified:

%ACB_FULL_NAME_SYSTEM%

- From “Ahsay A-Click Backup” to “Ahsay AClick Backup”

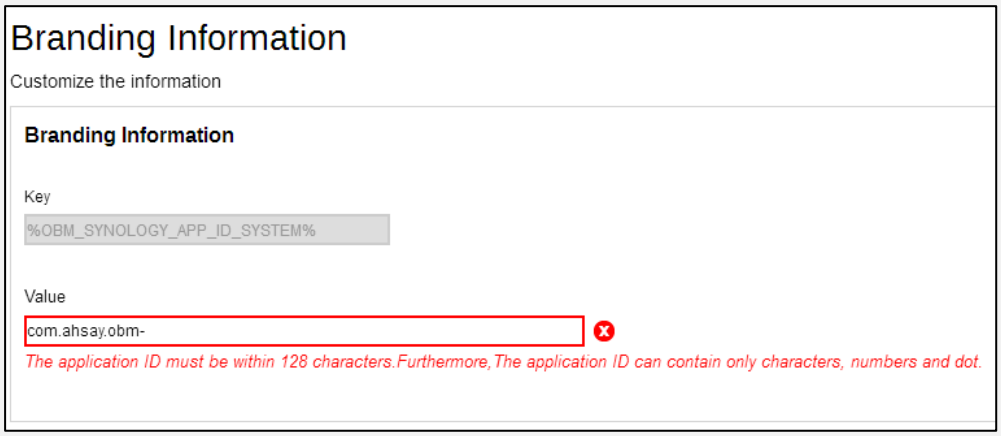
%OBSR_SHORT_NAME_SYSTEM%

- From “AhsayOBS and AhsayRPS” to “AhsayOBSR”

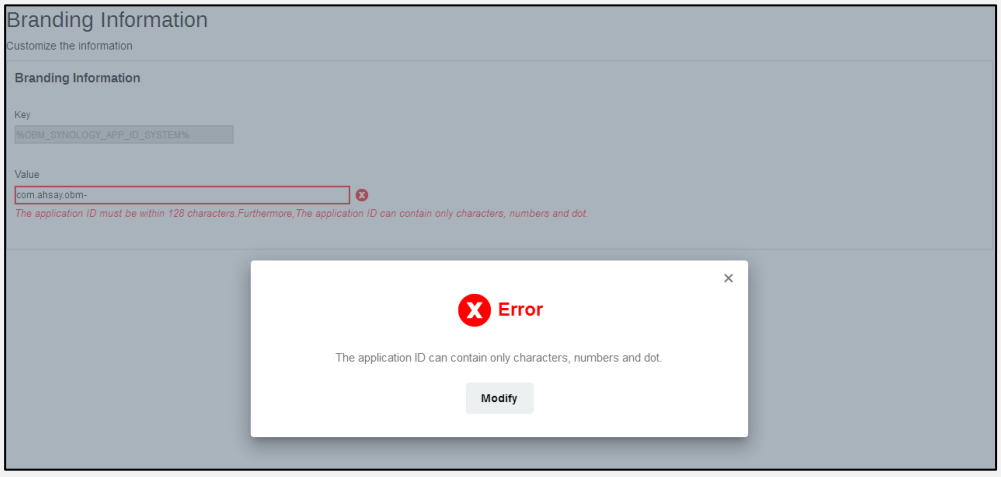
%ACB_COMMENTS_SYSTEM%

- From “Ahsay A-Click Backup” to “Ahsay AClick Backup”

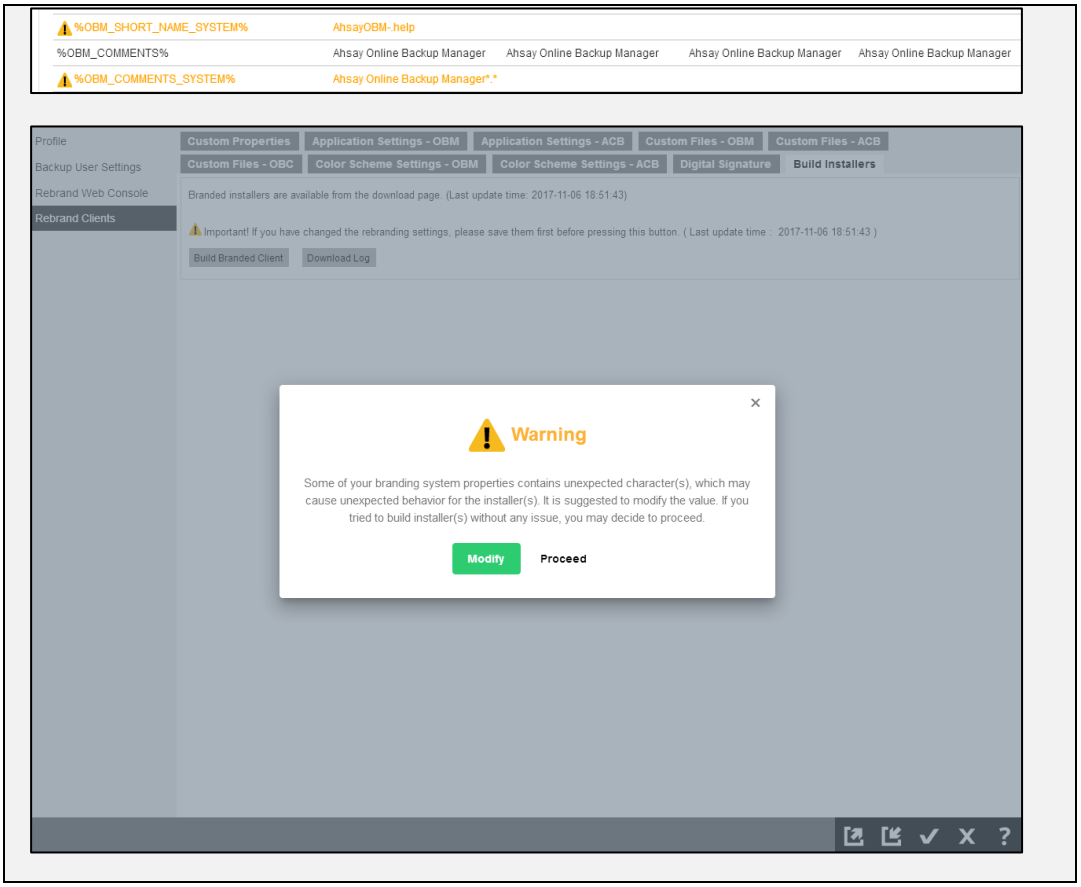
There will be warning shown if the character is incorrect.



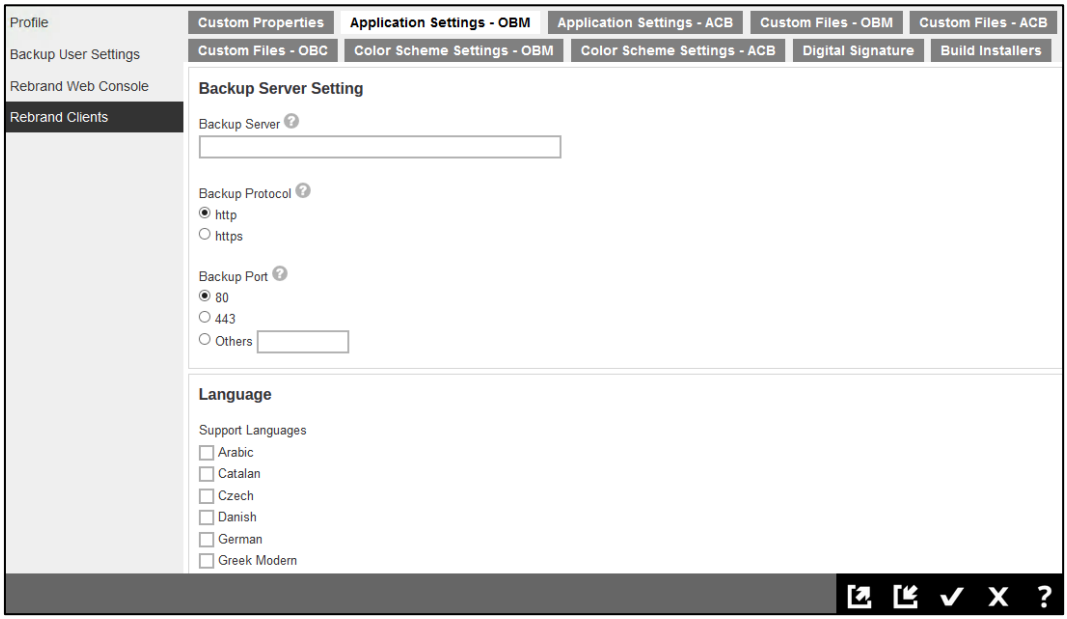
It is not allowed to save the incorrect value as the warning **Error** will pop out.



If there is still some unexpected character(s) in the branding system properties, which may cause unexpected behavior for installer(s), the warning will pop out to suggest modify the value when click on **Build Branded Client** in **Builder Installers**.

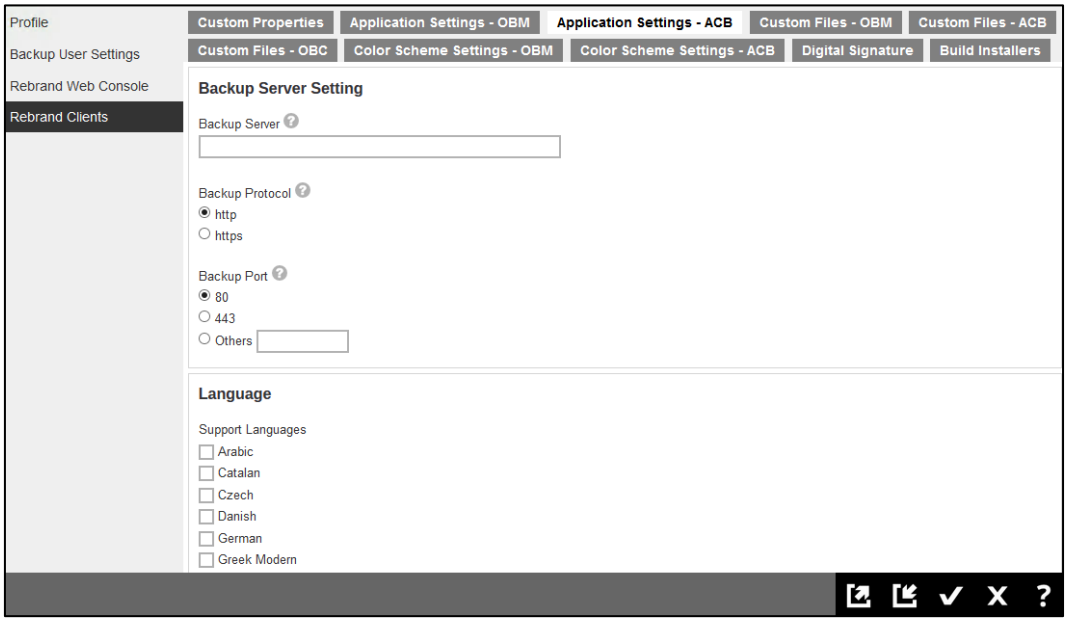


6. After you completed properties, you can click into the **Application Settings – OBM** tab.



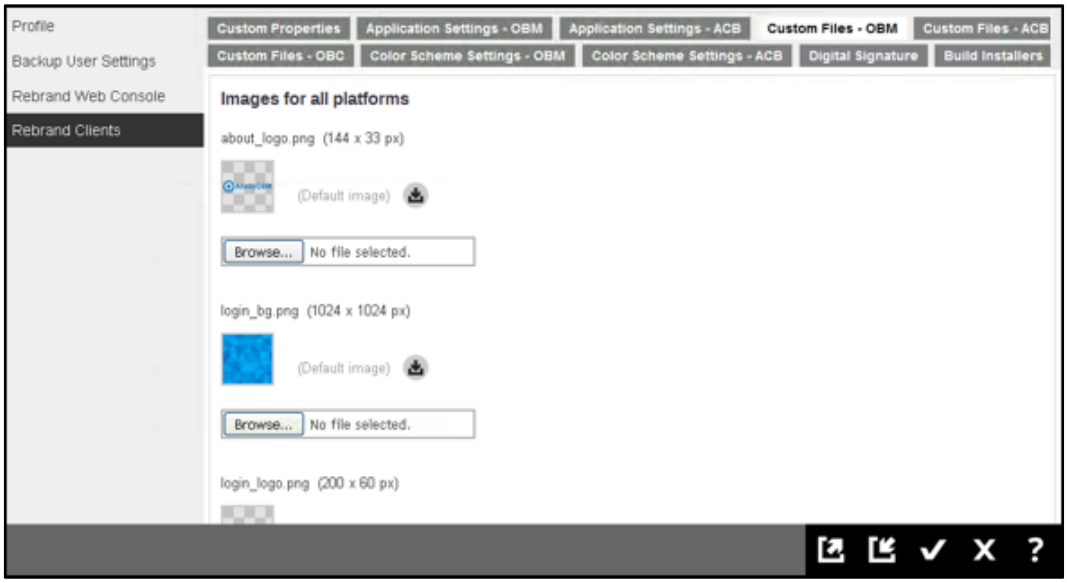
You can customize the default connection settings, supported languages, and GUI features such as show backup server URL or select language drop down list.

7. Click into the **Application Settings – ACB** tab.



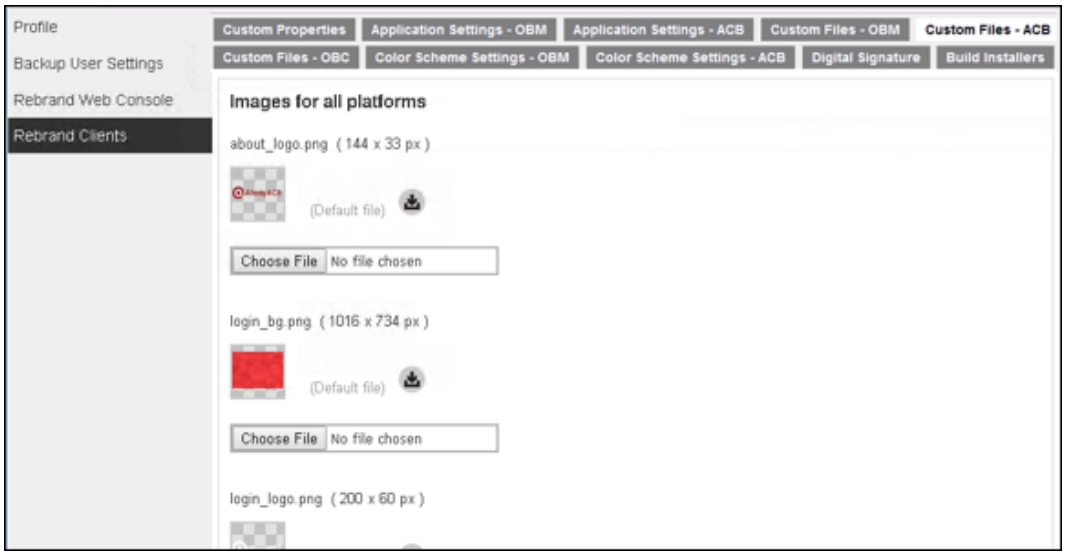
Similar to the previous step, you can customize the default connection settings, supported languages, and GUI features such as show backup server URL or select language drop down list.

8. Click on the **Custom Files – OBM** tab.



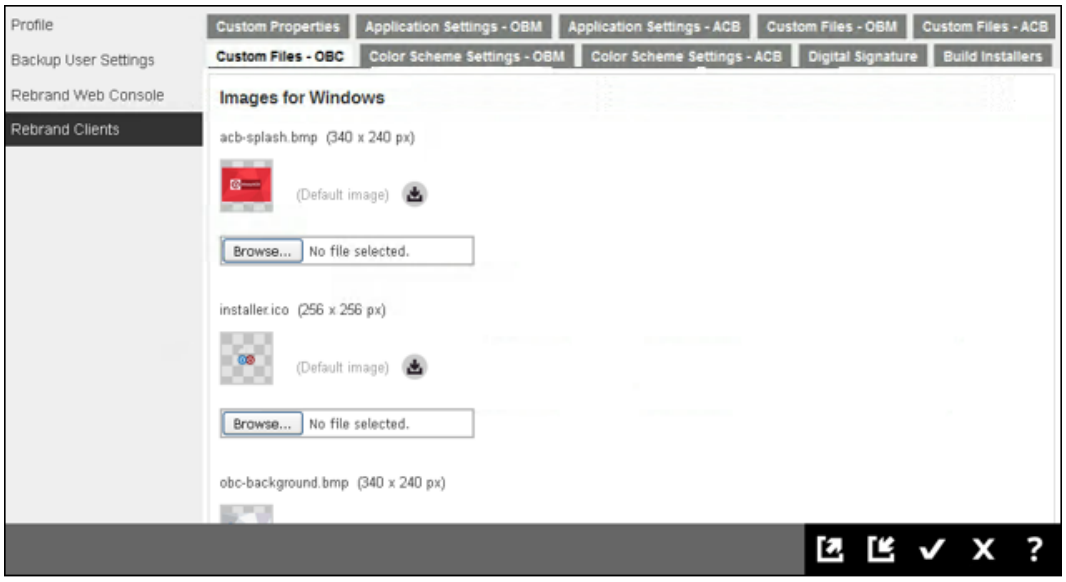
You can upload the branded images for your OBM installer/application. Please refer to the branding image specifications listed on Appendix F , you can download the default logo/icon for reference.

9. Click on the **Custom Files – ACB** tab.



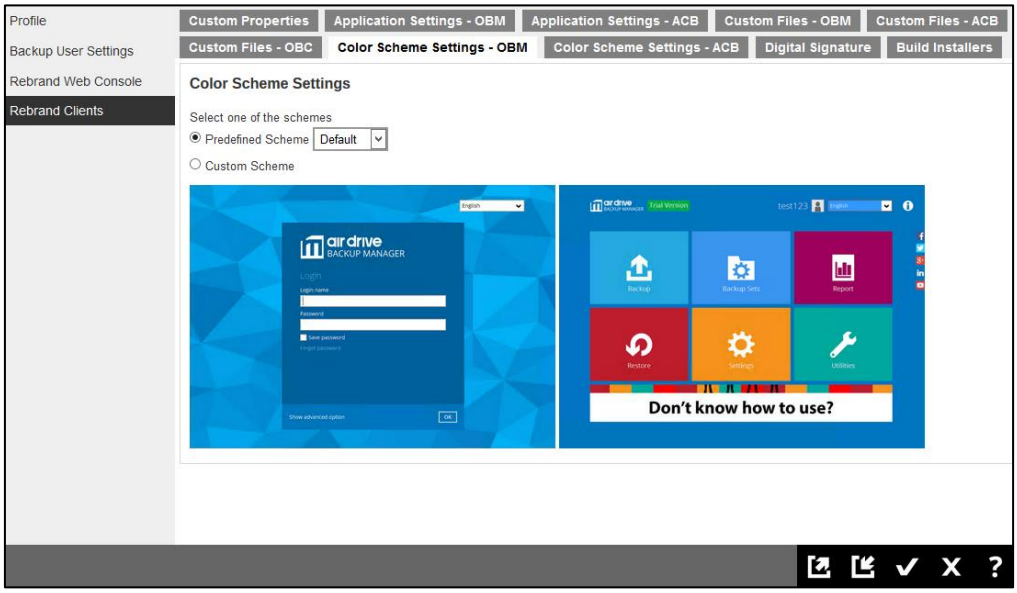
You can upload the branded images for your ACB installer/application. Please refer to the branding image specifications listed on Appendix F, you can download the default logo/icon for reference.

10. Click on the **Custom Files – OBC** tab.



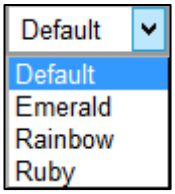
You can upload the branded images for your OBC installer. Please refer to the branding image specifications listed on Appendix F, you can download the default logo/icon for reference.

11. Click on the **Color Scheme Settings – OBM** tab**.**

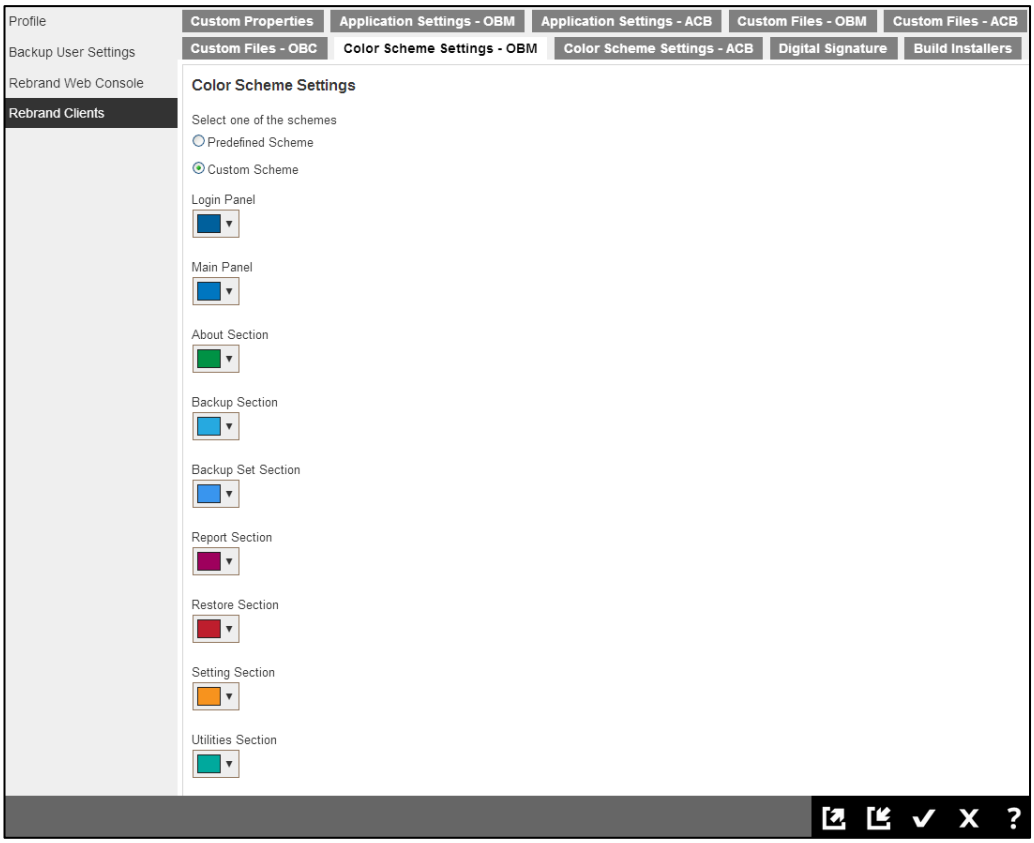


From v7.15.0.0 onwards AhsayCBS supports changing the color scheme for backup clients. You can select the color scheme settings from "Predefined Scheme" or "Custom Scheme".

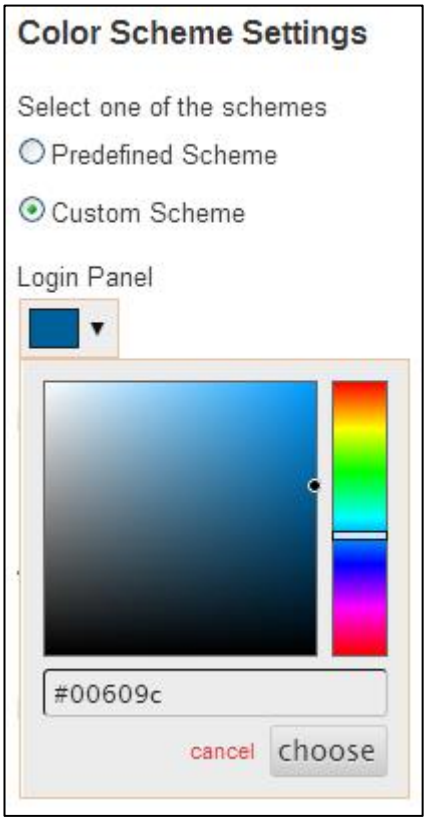
i. For **Predefined Scheme**, you can click on the dropbox to choose from the predefined options.

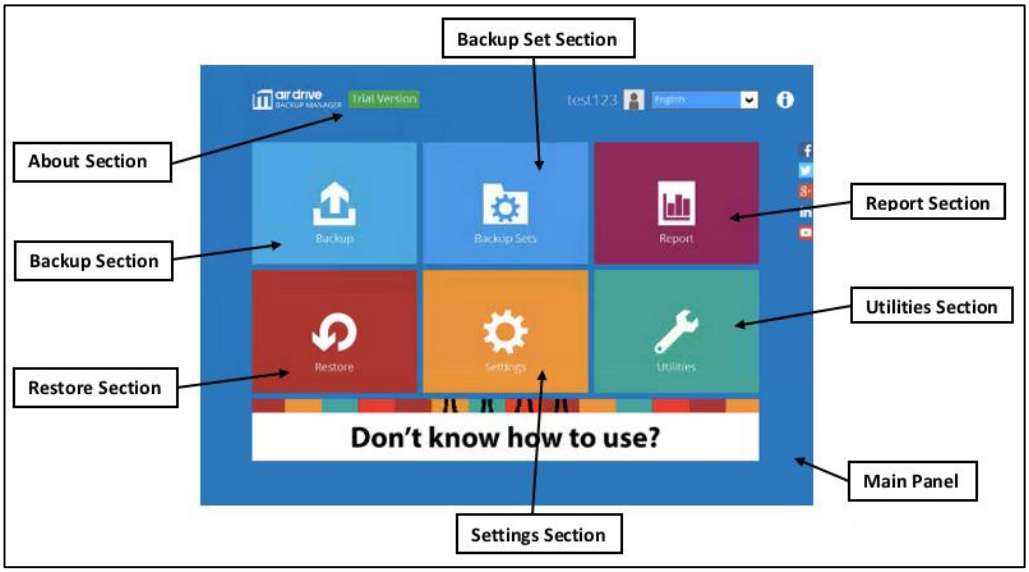


ii. For **Custom Scheme**, you can choose color for each section.



The color setting is based on hex color codes and you can either select the color using the palette or just input the hex color code. Please refer to the following link for details of hex color code: http://www.color-hex.com/





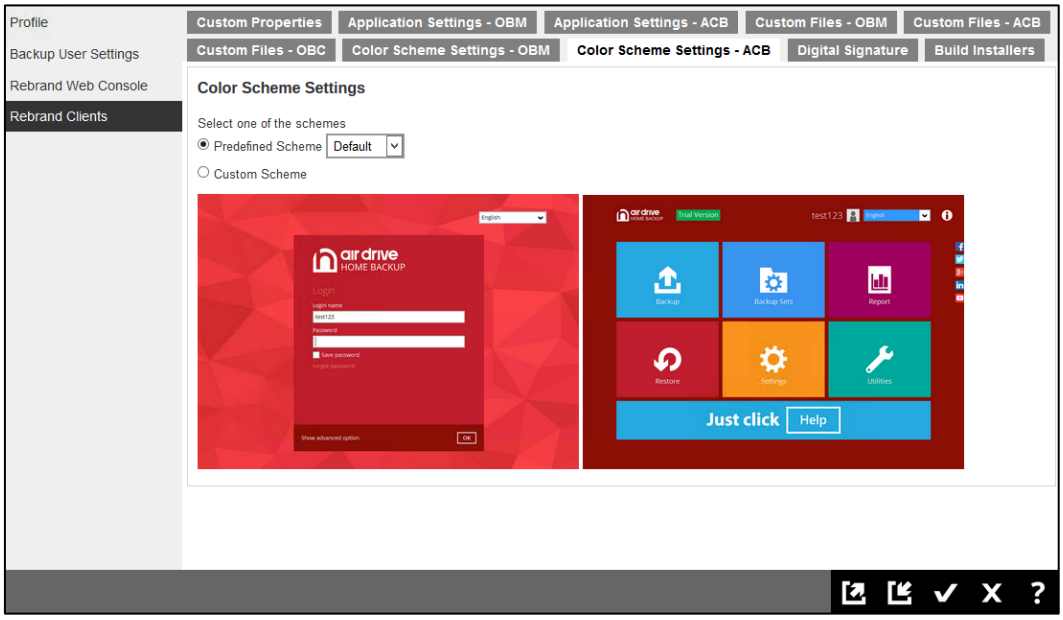
Click on ✔ at the bottom right corner to continue.

NOTE

After changing and saving the configuration of **Color Scheme Settings – OBM**, administrator can provide available online/ offline installer with according color scheme for client user to download and run after finishing **[Build Installers]** > **[Build Branded Client]** successfully.

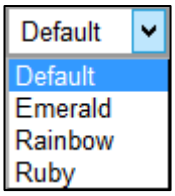
AhsayOBR will follow the same color scheme settings with AhsayOBM.

12. Click on the **Color Scheme Settings – ACB** tab.

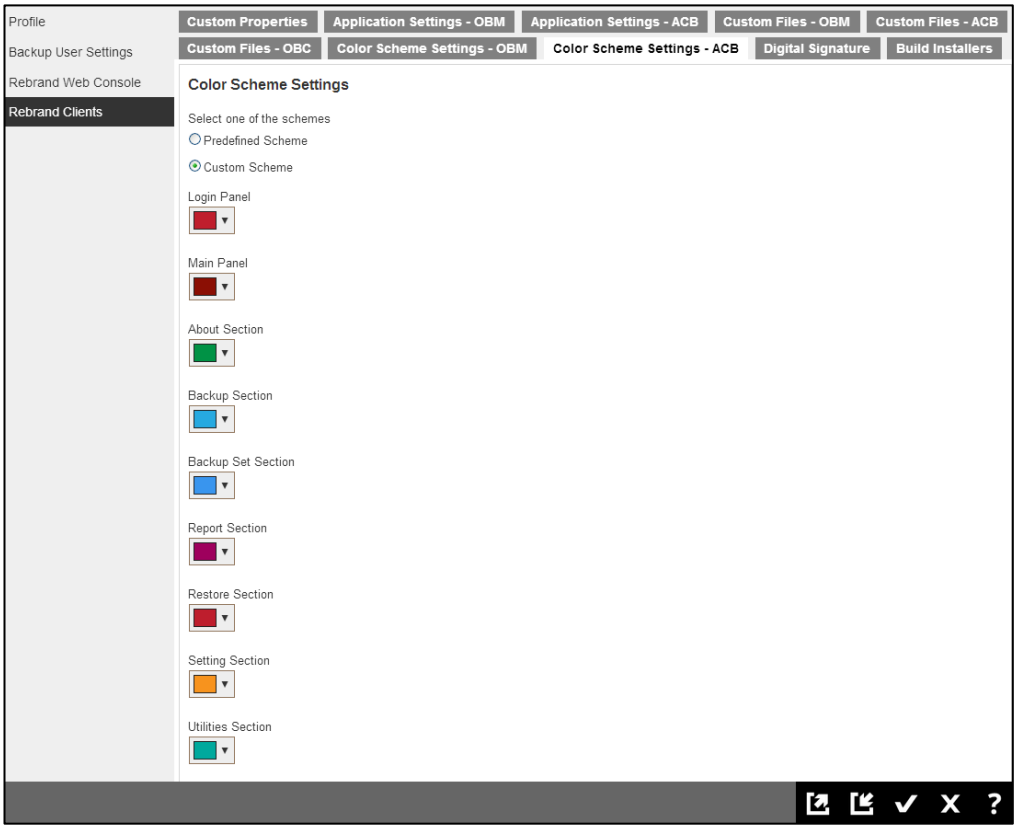


From v7.15.0.0 onwards AhsayCBS supports changing the color scheme for backup clients. You can select the color scheme settings from “Predefined Scheme” or “Custom Scheme”.

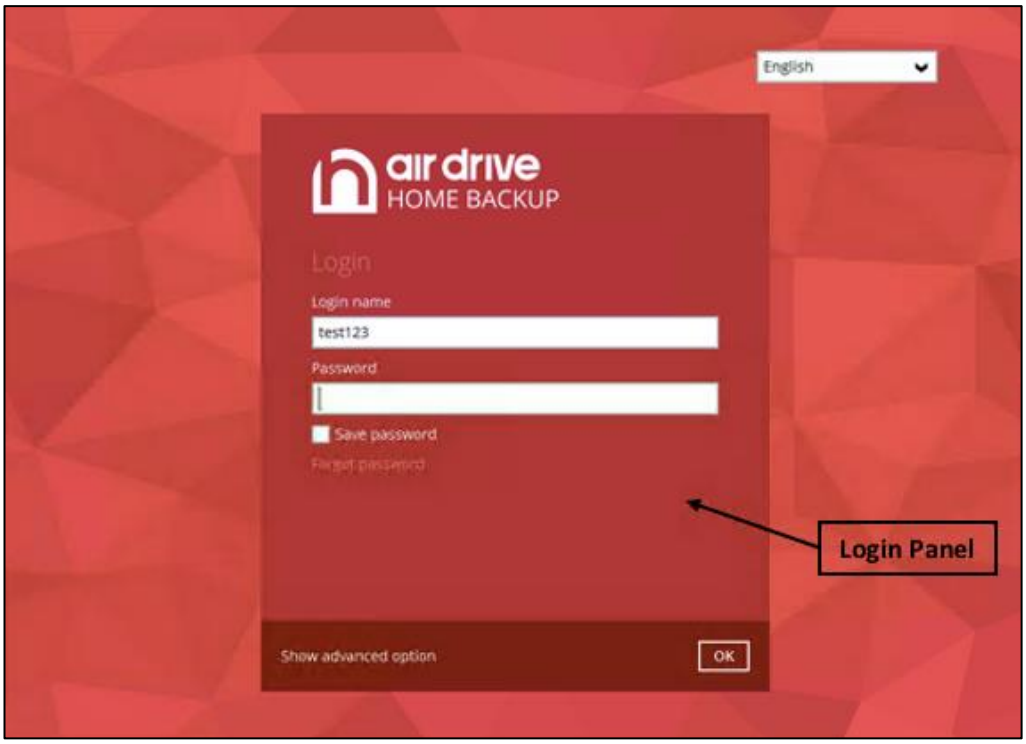
i. For **Predefined Scheme**, you can click on the dropbox to choose from the predefined options.



ii. For **Custom Scheme**, you can choose color for each section.



The color setting is based on hex color codes and you can either select the color using the palette or just input the hex color code. Please refer to the following link for details of hex color code: http://www.color-hex.com/

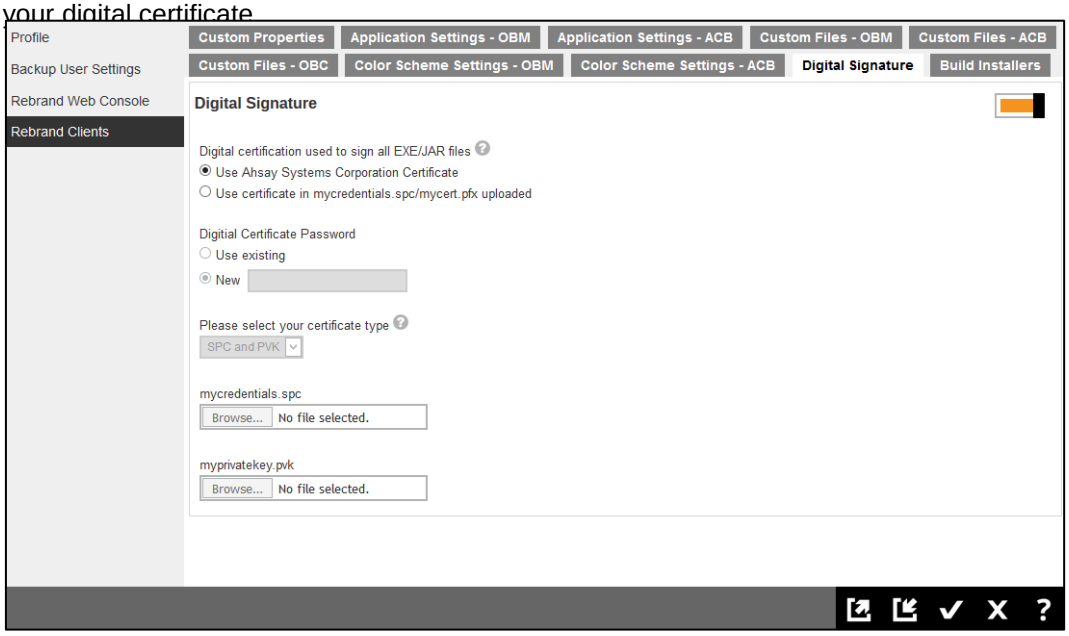


Click on ☑ at the bottom right corner to continue.

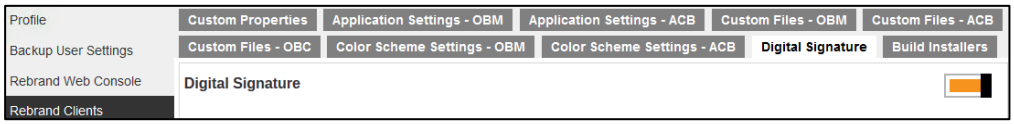
NOTE

After changing and saving the configuration of **Color Scheme Settings – ACB**, administrator cannot provide available online/ offline installer with according color scheme for client user to download and run until finish **[Build Installers]** > **[Build Branded Client]** successfully.

13. **Optional:** Click on the **Digital Signature** tab if you need to generate the installers with your digital certificate.



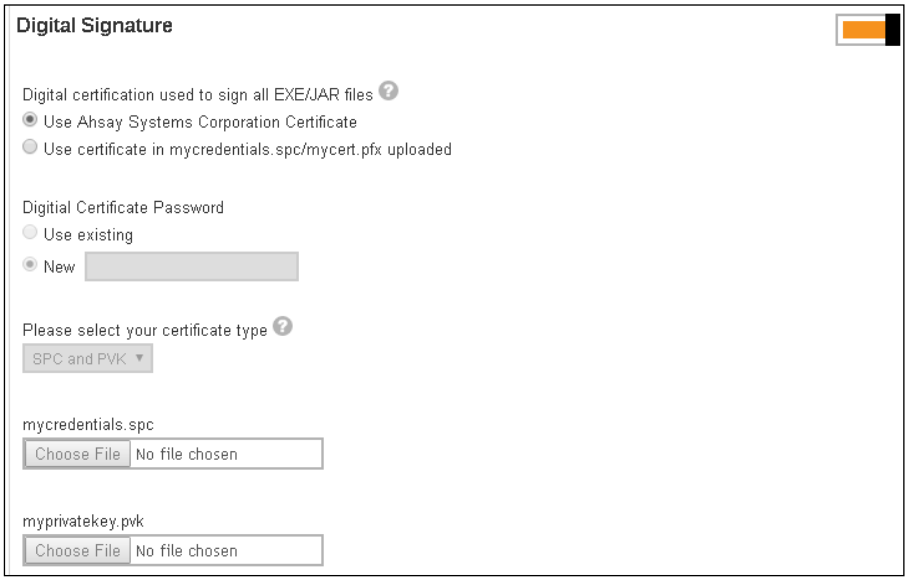
i. Switch on the **Digital Signature** button.



ii. You can use our default digital certificate by selecting the **Use Ahsay Systems Corporation Certificate**.

-OR-

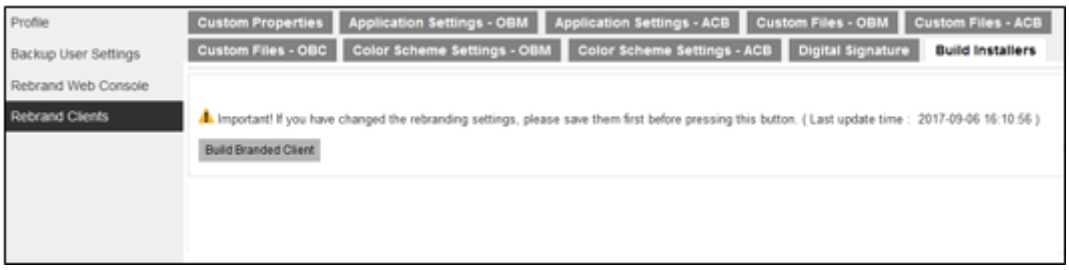
If you prefer to use your own digital certificate, you can select **Use certificate in mycredentials.spc/mycert.pfx upload** option.



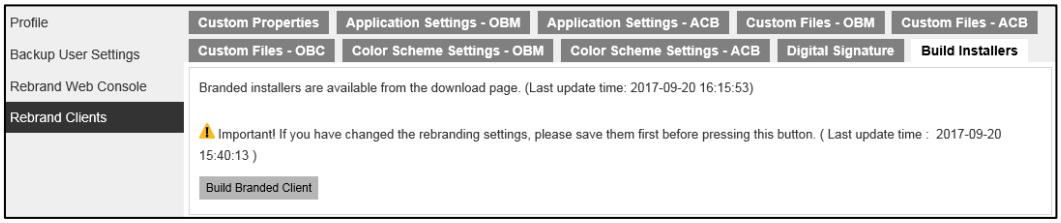
Enter the digital certificate password and select the whether you are uploading a "SPC and PVK" or "PFX" digital certificate, then you can upload your digital certificate file.

14. Click and to save all the settings.

15. Go back to the **Build Installers** tab and click on the **Build Branded Client** button. AhsayCBS will request our customization portal to generate new installers.

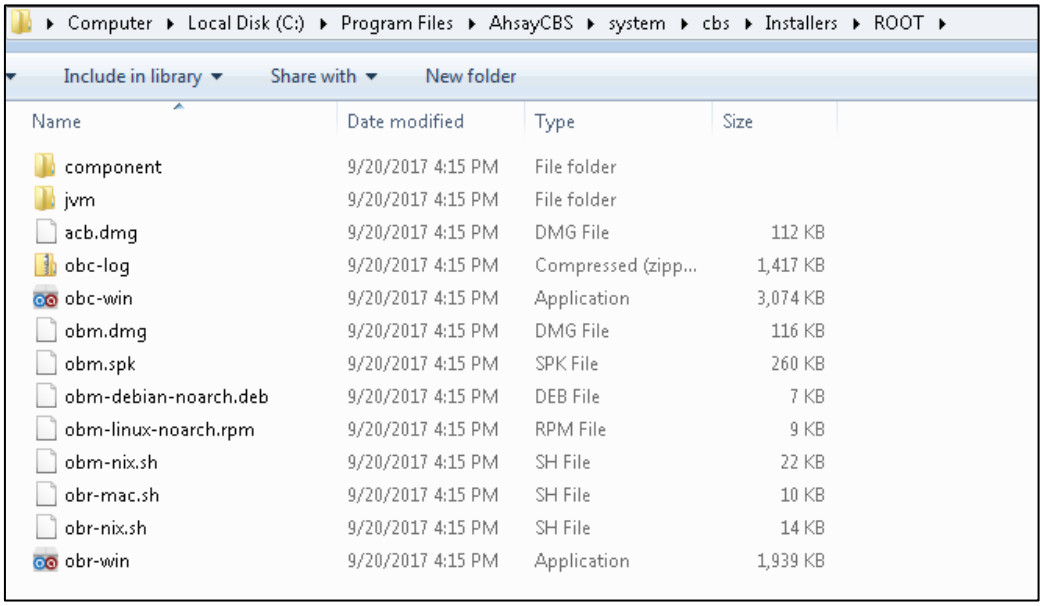


Please be patient as the installer generation process should take around 5 to 10 minutes. The generation time depends on the traffic condition on the customization portal. The option will be greyed-out. You will be able to see the following message when the installer generation is completed.



You will be able to find the installers under the following path, **CBS_HOME\system\cbs\Installers\ROOT**

Example:



16. Please leave them inside this folder and it is forbidden to move them to other folders. When your customers access the web console by the system account's hostname, AhsayCBS will arrange the corresponding branded installers for users to download.

17. Download new installers from the installer download page in your AhsayCBS.

18. After you tested your installers, you can enable the client auto-update or update your client manually.

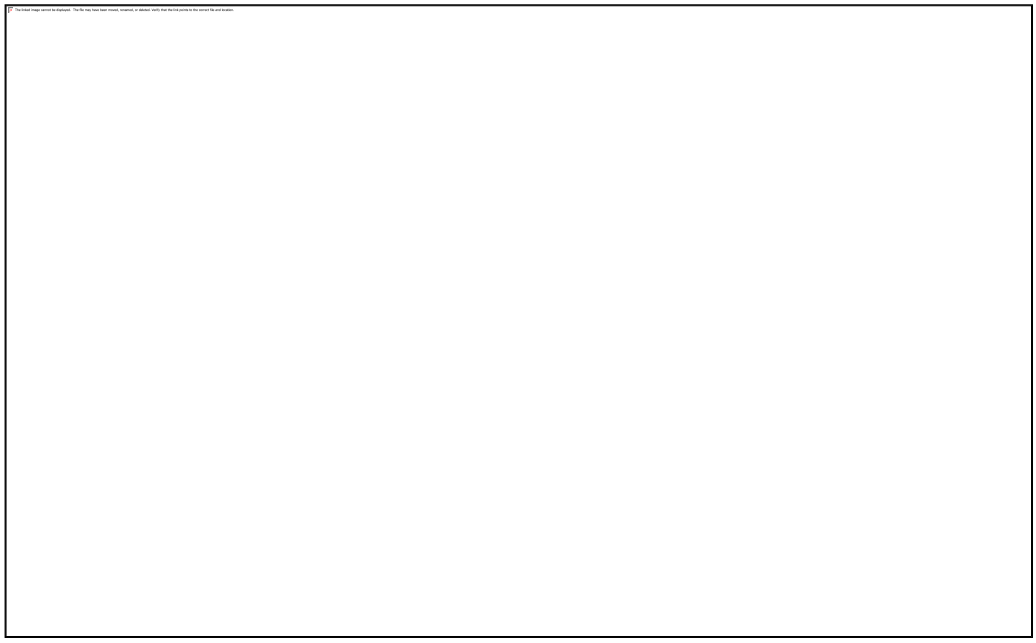
19. In case of any problems when the installer is being built, you will see the **Download Log** button.

Click on the **Download Log** button and you can download the branding log file **obc-log.zip** and you can take a look into the log for troubleshooting the branding issue.

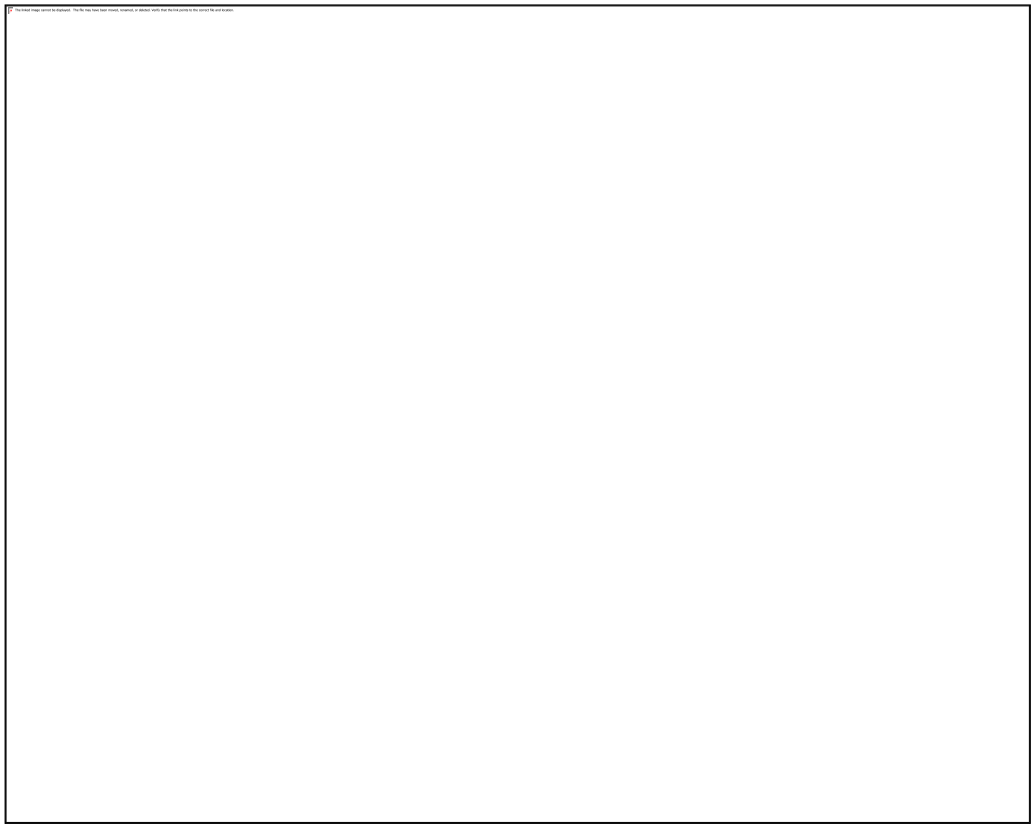
Brand the AhsayCBS Interface and AhsayOBM/AhsayACB Installers for your Resellers

1. Click in **System Settings** > **Basic** > **Administrative Access**.

2. Click into the sub admin account that you want to apply the branding.



3. Make sure there is a correct hostname in sub admin **Profile** page.



4. Please follow the steps in previous chapters to brand their own web console, and rebrand the AhsayOBM/AhsayACB installers. The branded installers is stored in **CBS_HOME\system\cbs\Installer\%Reseller_ID%**

Example:

Please leave them inside this folder and it is forbidden to move them to other folders. When your reseller's customer access to the web console by the system account's hostname, AhsayCBS will arrange the corresponding branded installers for users to download.

Customize Application Name on Cloud Storages

Request for Permission Pages

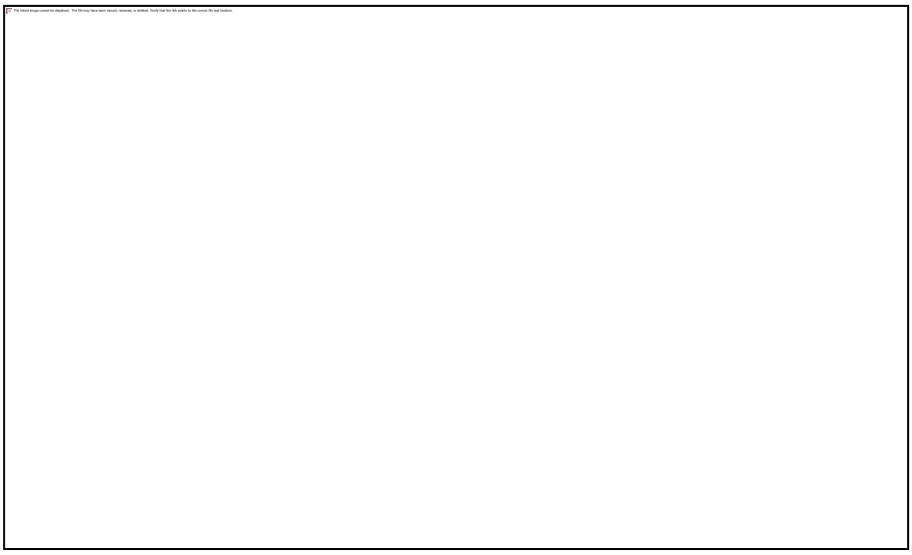
When your client set up the cloud storage on

1. Amazon Cloud Drive
2. Dropbox
3. Google Drive
4. OneDrive
5. OneDrive for Business

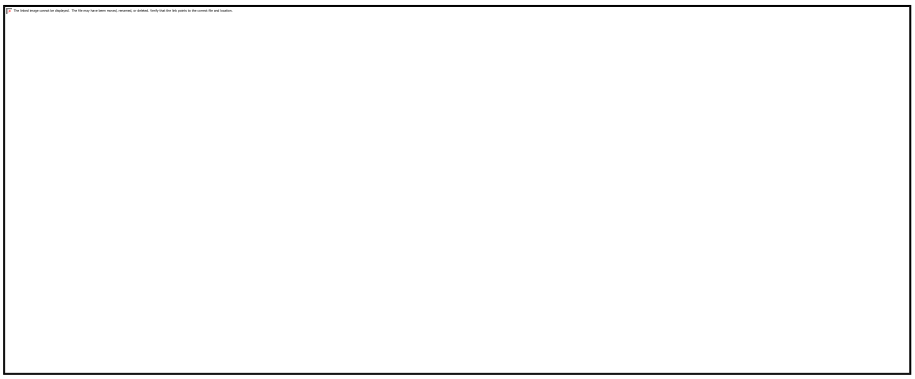
AhsayOBM / ACB would forward an URL through the browser to the cloud storage. The cloud storage would require your client to login and/or prompt the following page to get client's approval for the AhsayOBM / ACB to access the cloud storage.

For example:

Google Drive



One Drive



In these request for permission pages, you can see the “Ahsay” logo and the “Ahsay” wording. You can setup the destination settings in the policy group in your AhsayCBS to customize the branding.

Preparation

Before you customize the logo and application name on the request for permission page, you need to collect the following details:

Amazon Cloud Drive

- Client ID
- Client Secret
- Native application redirect URI

Dropbox

- Application key
- Application secret

Google Drive

- Client ID
- Client Secret

OneDrive

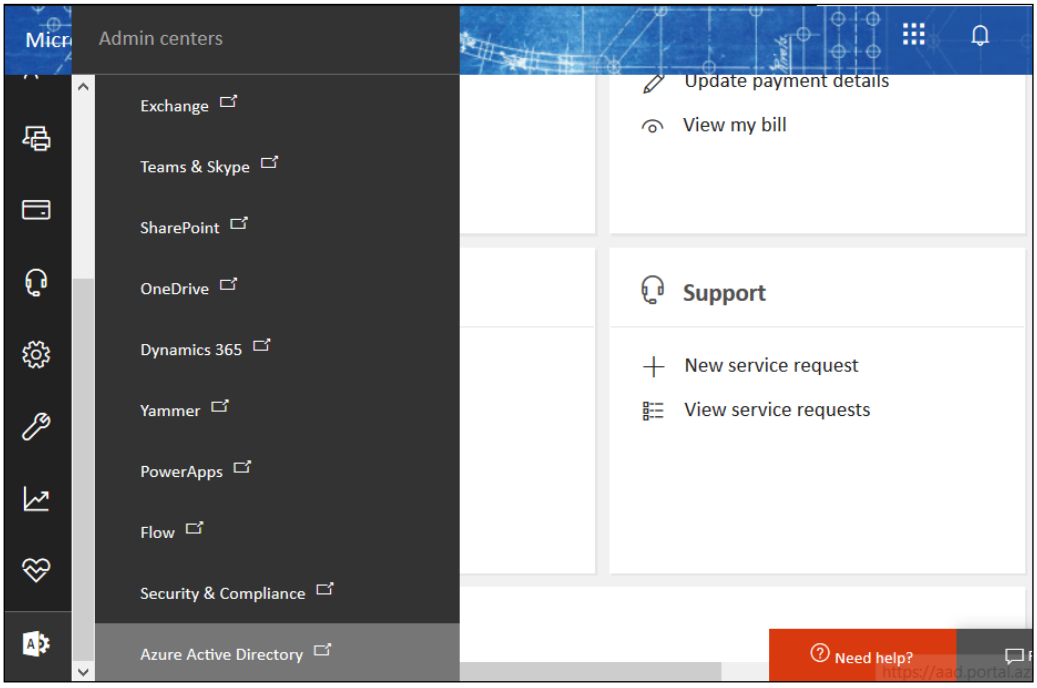
- Client ID
- Client Secret
- Native application redirect URI

OneDrive for Business

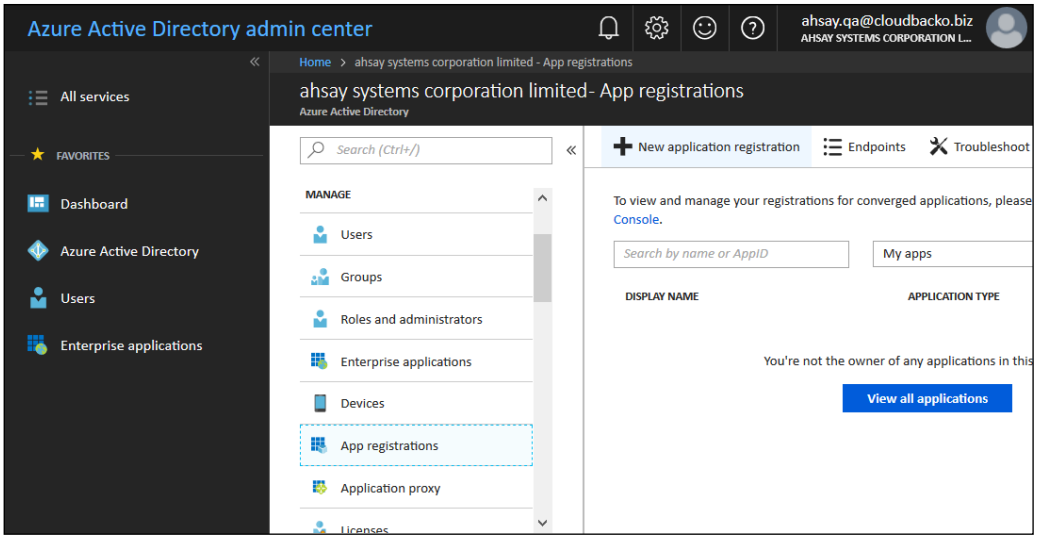
- Client ID

  To retrieve the Client ID:

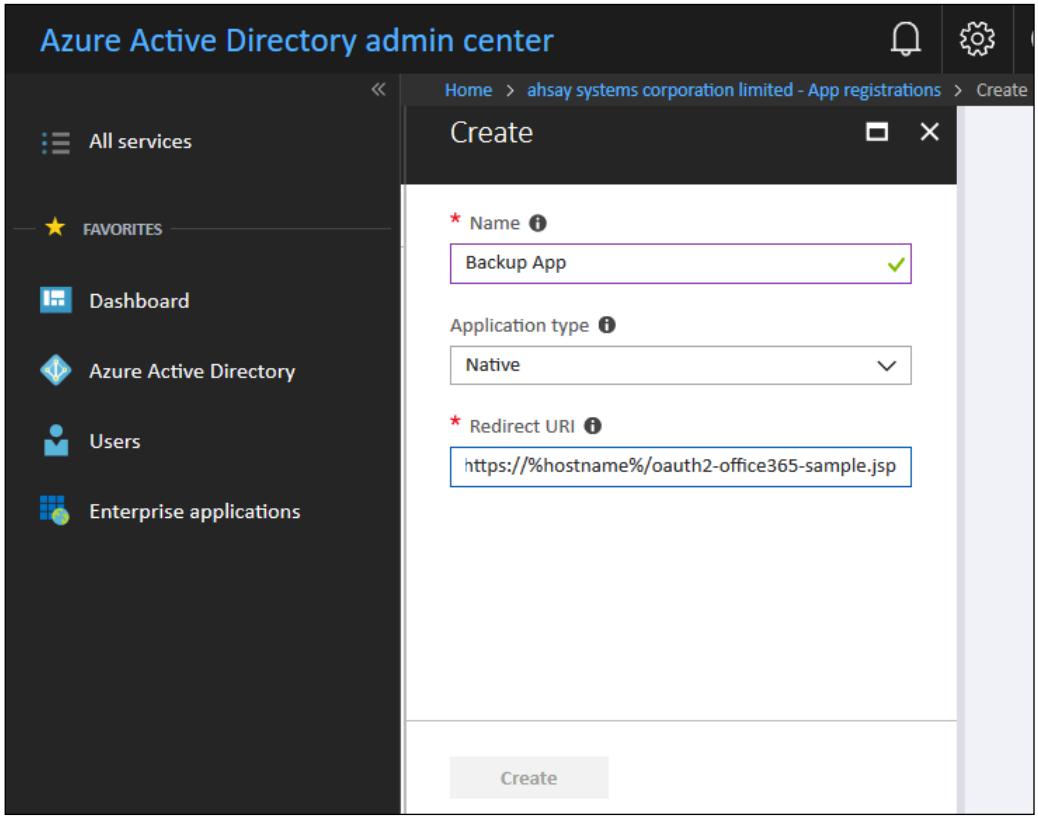
  1. Login to the OneDrive for Business portal (Microsoft 365 Admin Center): http://portal.office.com
  2. Select **Admin Centers** at the bottom of the left panel, then select **Azure Active Directory**.



3. Click on **Azure Active Directory** from the left panel, then **App registrations**.



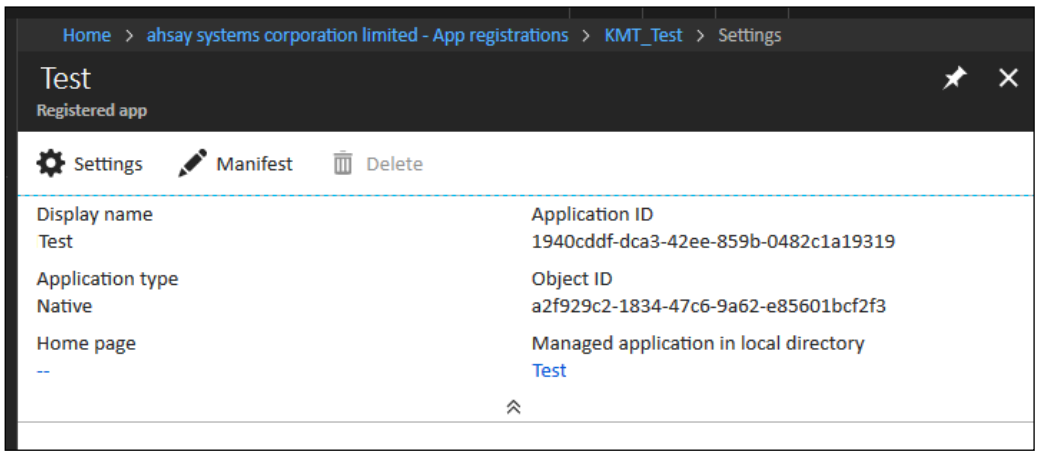
4. Select **New application registration**, then enter the following:



- **Name**: Enter a name for your customized application.
- **Application type**: Select **Native**.
- **Redirect URI**: Enter the path to the corresponding .jsp file on the AhsayCBS server (obtained from the next step), for example:

  https://%hostname%/oauth2-office365-sample.jsp

5. Click **Create** afterward.
6. The **Application ID** will be displayed, which is the **Client ID** required for the OneDrive for Business customization



7. Finally, configure the permission required, select **Settings**.

8. Under **API ACCESS**, select **Required permission**. Enable the following API settings:

   Windows Azure Active Directory

   - **Sign in and read user profile**
   - **Access the directory as the signed-in user**

   Office 365 SharePoint Online

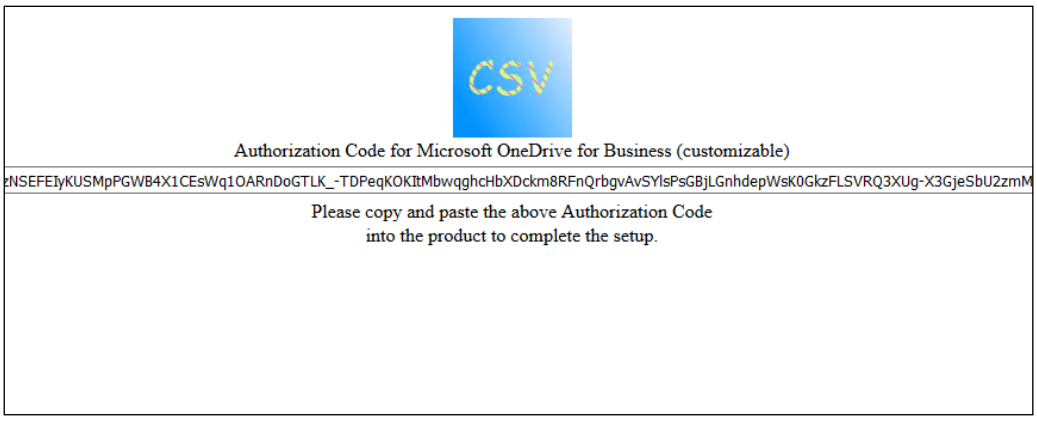
   - **Read and write user files**

9. Save the changes afterward.

➢ Native application redirect URI

To retrieve the Native application redirect URI:

1. Create a web page (.jsp) for request of the Authorization Code.



A sample format of the page:

```
<html>
<head>
<title>Authorization Code for Office 365</title>
</head>
<body>
<table width="100%" border="0" align="center">
  <tr>
    <td align="center">
    <img src="ahsay-120px-oauth.gif" /><br>
    Authorization Code for Microsoft OneDrive for Business</td>
  </tr>
  <tr>
    <td align="center"><input onClick="this.select()" id="authcode" type="text" size="30" value="<%=
request.getParameter("code") %>"></td>
  </tr>
  <tr>
            <td align="center"><p>Please copy and paste the above Authorization Code <br>into the
```

```
product to complete the setup.</p></td>
  </tr>
 </table>
 </body>
</html>
```

You can obtain a sample jsp file by Clicking Here.

Important:
The line value="<%= request.getParameter("code") %> are used for retrieving / displaying the authorization code, you must include this on the page.

It is expected that you have basic HTML knowledge to create the authorization code request page.

2. Once you have created the customized page, copy and place the jsp file to the AhsayCBS server at:

   For CBS on Windows: %CBS_Install_Home%\webapps\ROOT

   For CBS on Linux: %CBS_Install_Home%/webapps/ROOT

3. The Native application redirect URI will be:

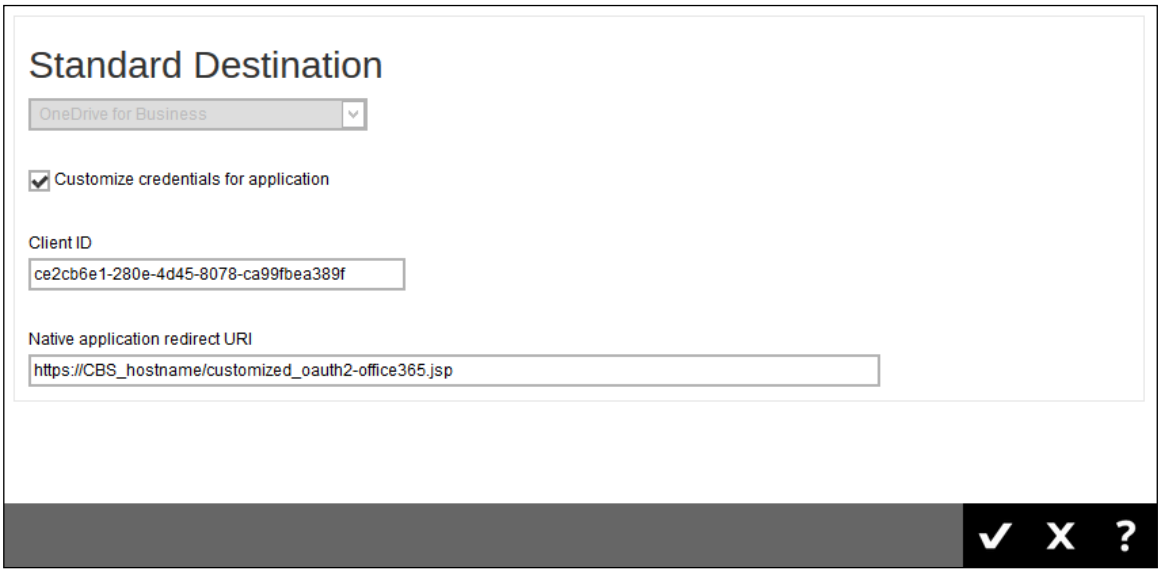
   https://%CBS_hostname%/%customized_page_name%.jsp

   Where CBS_hostname is the hostname or IP address of your AhsayCBS server and customized_page_name is the name of the jsp file.

   For example:

   https://backup.server.com/oauth2-office365-sample.jsp

The **Client ID** and **Native application redirect URI** can now be entered in



For other cloud vendors, refer to the following websites for information on how to collect the required information.

Reference

Dropbox
https://www.dropbox.com/developers/support

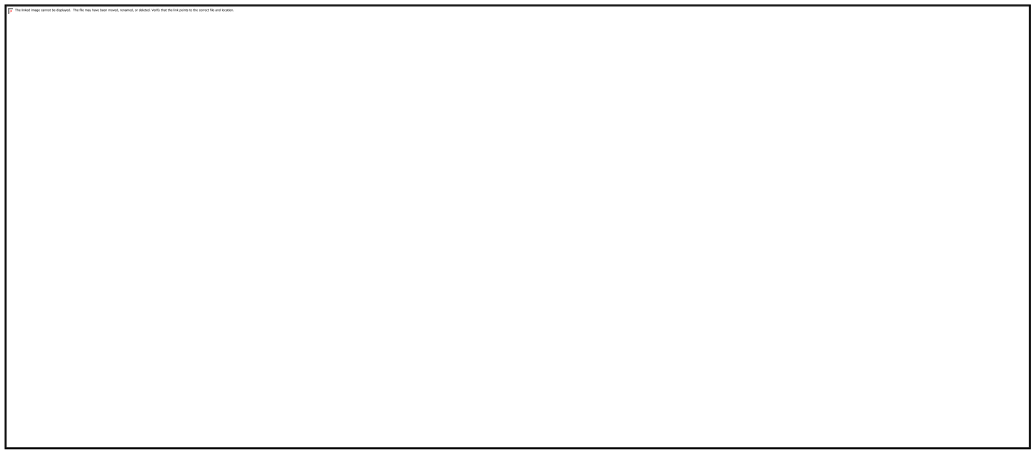
Google Drive
https://developers.google.com/drive/v3/web/enable-sdk#enable_the_drive_api
https://auth0.com/docs/connections/social/google

OneDrive and OneDrive for Business
https://dev.onedrive.com/app-registration.htm

Configure the storage

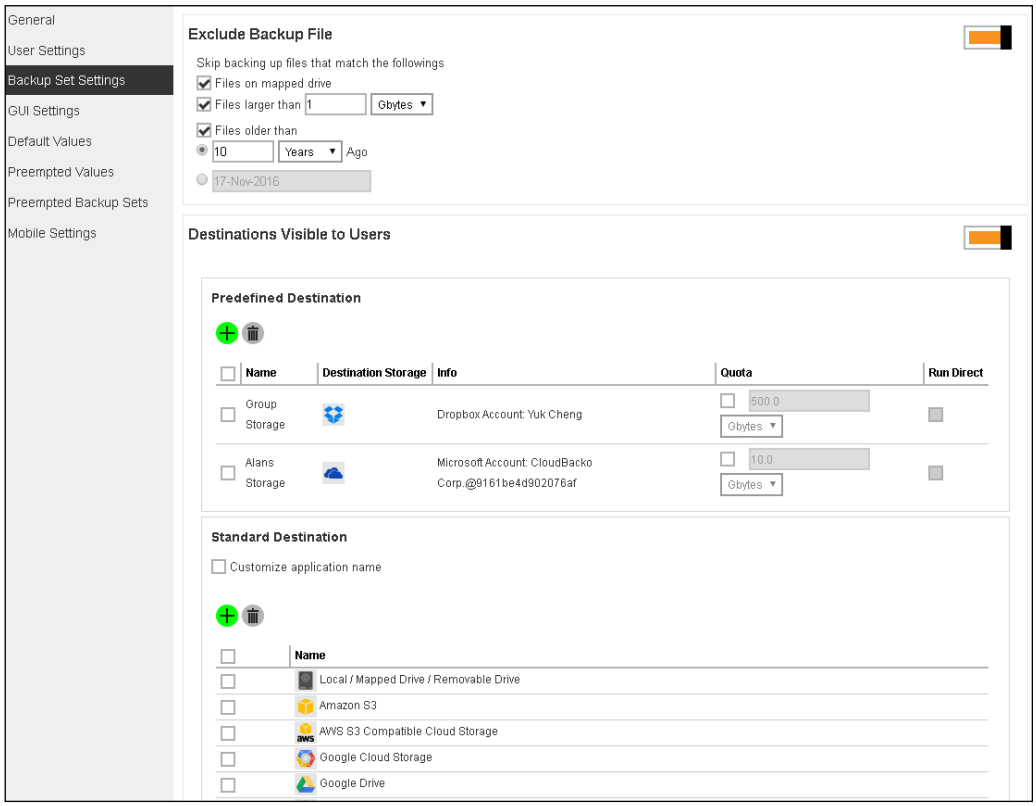
After you have collected the above information from your cloud / developer account, you can put the relevant information in the policy settings of your AhsayCBS.

1. Navigate to **Backup / Restore** > **Users, Group & Policies**, then select the **Policy Group** tab.



2. Select the policy group that you want to apply the setting.

3. Click into **Backup Set Settings** tab.



4. Turn on the switch "**Destinations Visible to Users**"

5. Scroll to the bottom part of "**Destinations Visible to Users**"

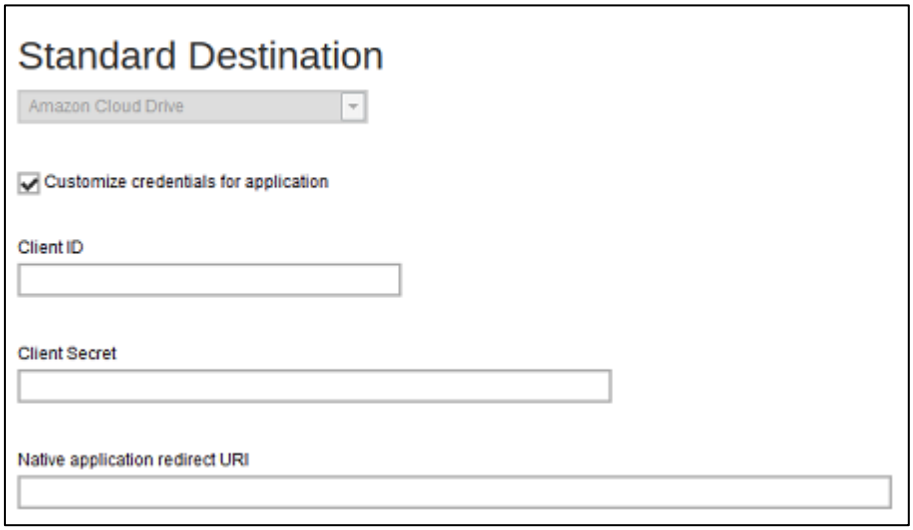
You can select one of the following cloud storage to customize

- Amazon Cloud Drive
- Dropbox
- Google Drive
- OneDrive
- OneDrive for Business

Amazon Cloud Drive

1. Click into Amazon Cloud Drive

2. Enable the “Customize credentials for application”



3. Enter the “Client ID”

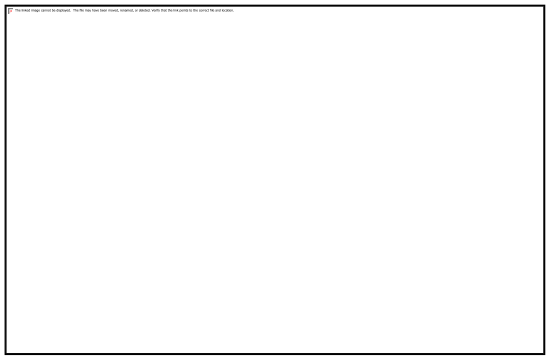
4. Enter the “Client Secret”

5. Enter the “Native application redirect URI”

6. Click ✔ to continue.

Dropbox

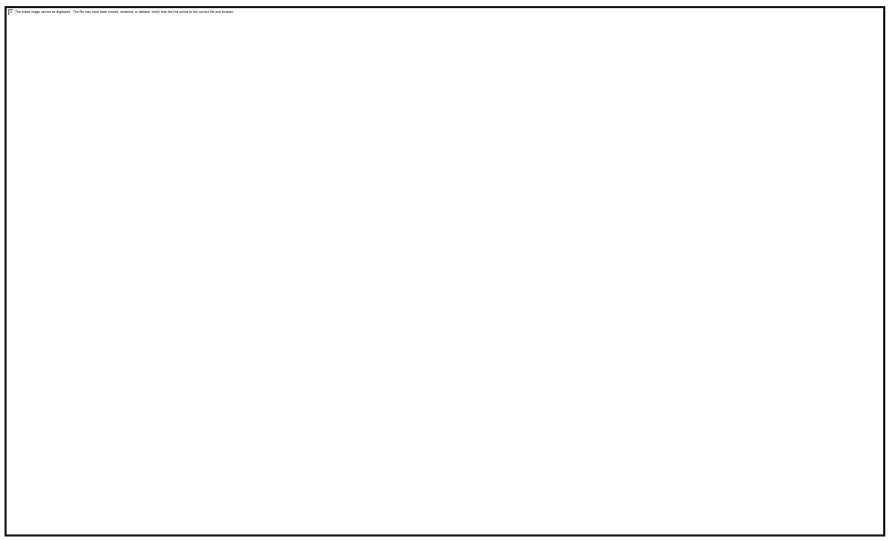
1. Click into Dropbox
2. Enable the “Customize credentials for application” option.



3. Enter the “Application Key”
4. Enter the “Application Secret”
5. Click ✔ to continue.

Google Drive

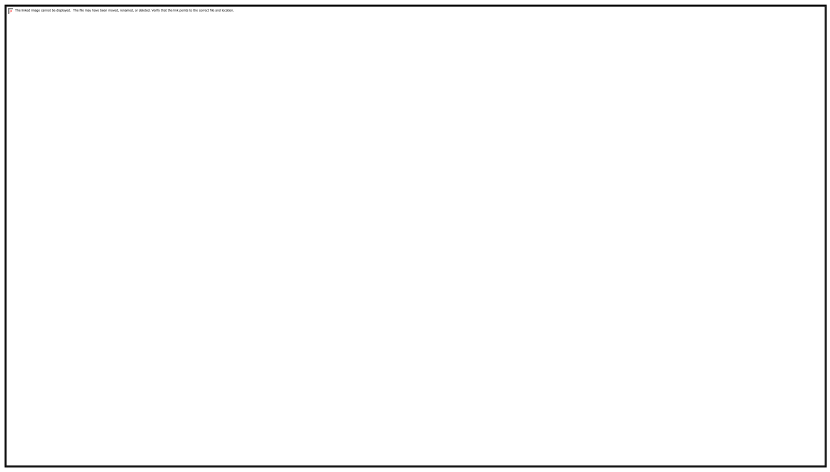
1. Click into Google Drive
2. Enable the “Customize credentials for application”



3. Enter the “Client ID”
4. Enter the “Client Secret”
5. Click ✔ to continue.

OneDrive

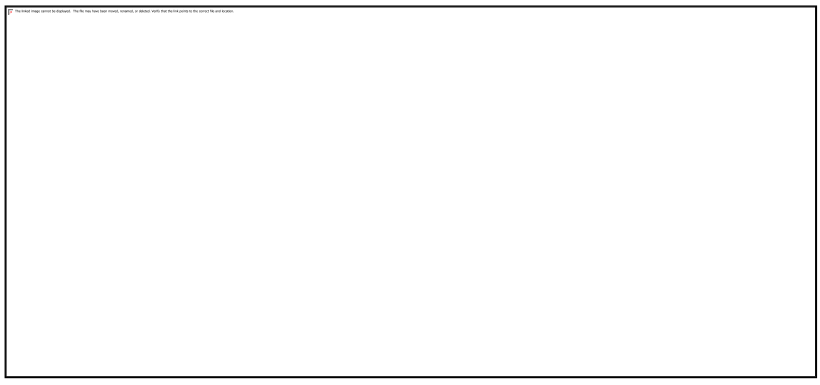
1. Click into OneDrive
2. Enable the “Customize credentials for application”



3. Enter the “Client ID”
4. Enter the “Client Secret”
5. Enter the “Native application redirect URI”
6. Click ✔ to continue.

OneDrive for Business

1. Click into OneDrive for Business
2. Enable the “Customize credentials for application”

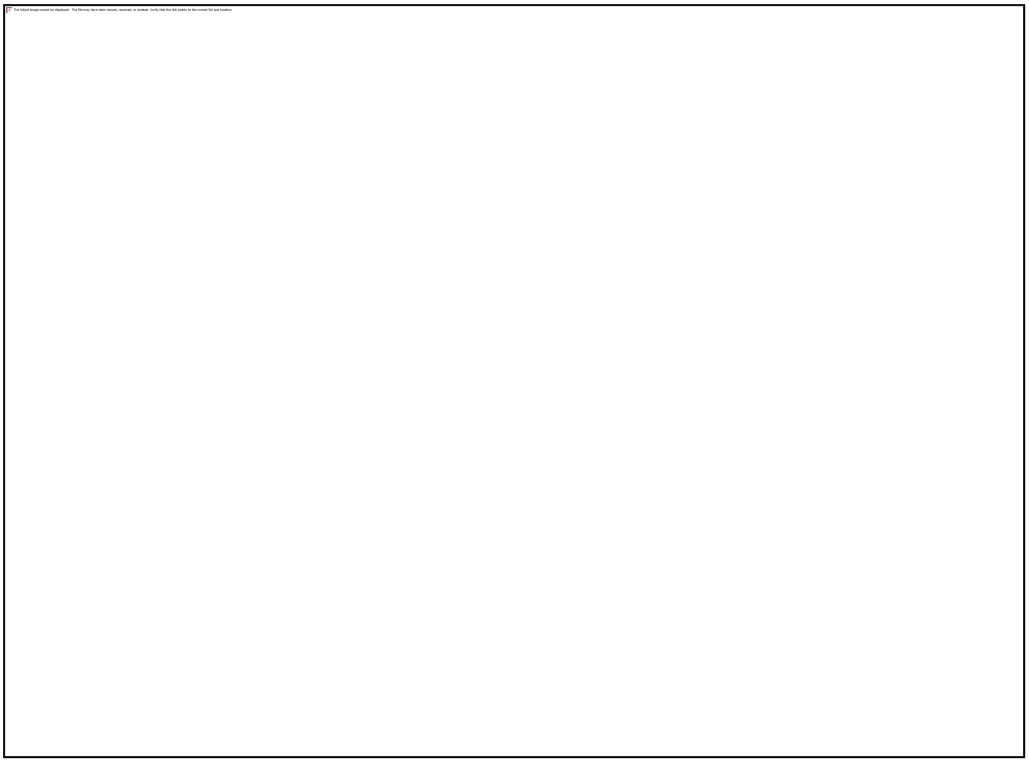


3. Enter the “Client ID”
4. Enter the “Native application redirect URI”
5. Click ✔ to continue.

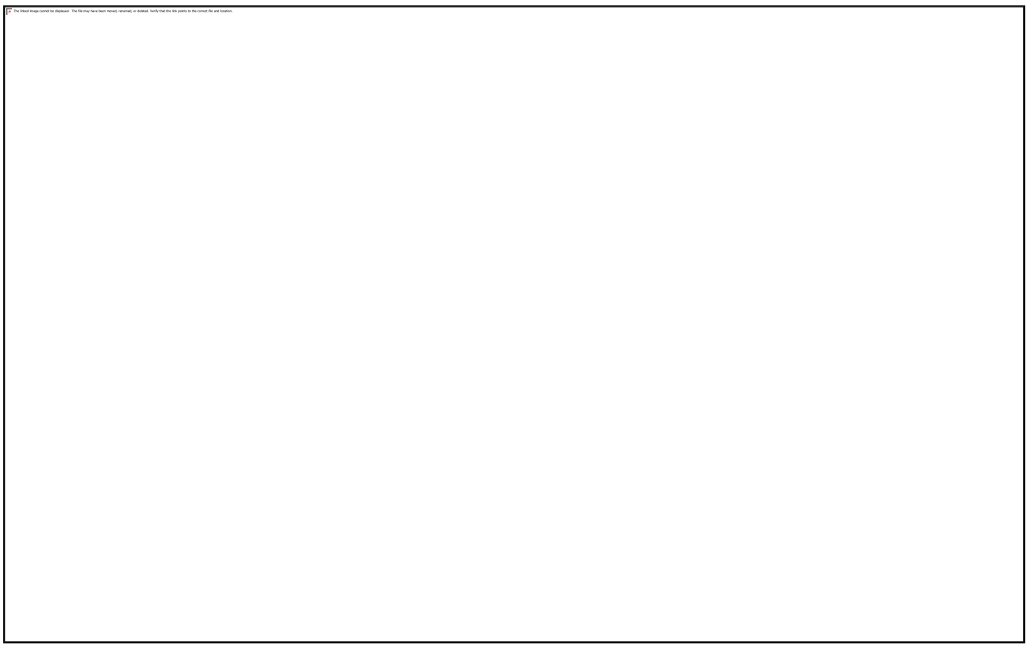
Customize the Folder/Bucket name in Standard Destination

Navigate to **Backup/Restore** -> **Users, Group & Policies**, then select the **Policy Group** tab. Click on the desired Policy Group, then select the **Backup Set Settings** section on the left. You can customize the application name (folder/bucket name) in different storages from there.

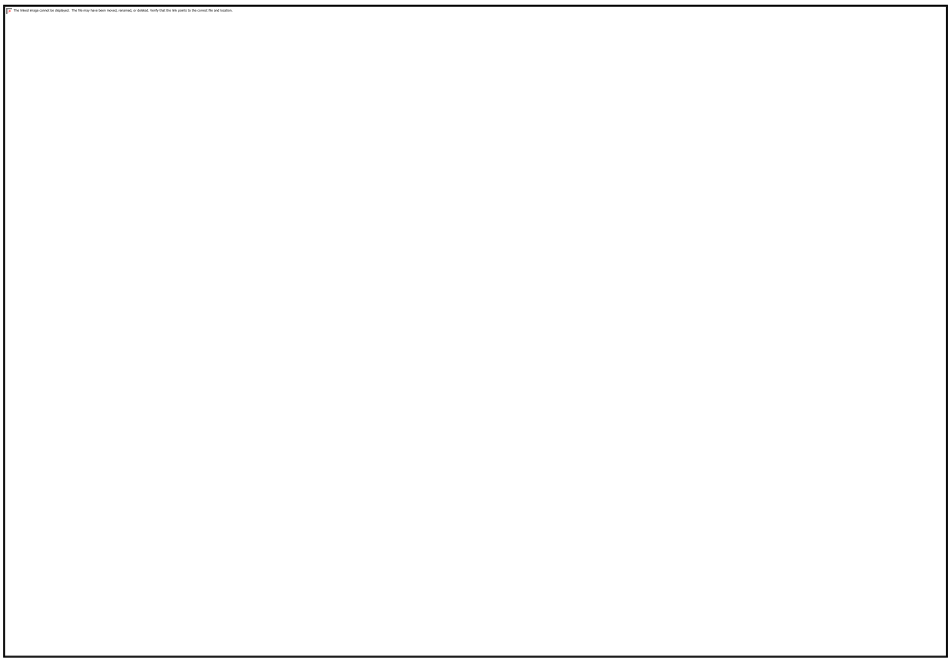
In the following example, we set the “Customize application name” as “mybackup”, when backup to the cloud storage (e.g.: Google Drive), the folder name “mybackup” will be created.



E.g.: Google Drive

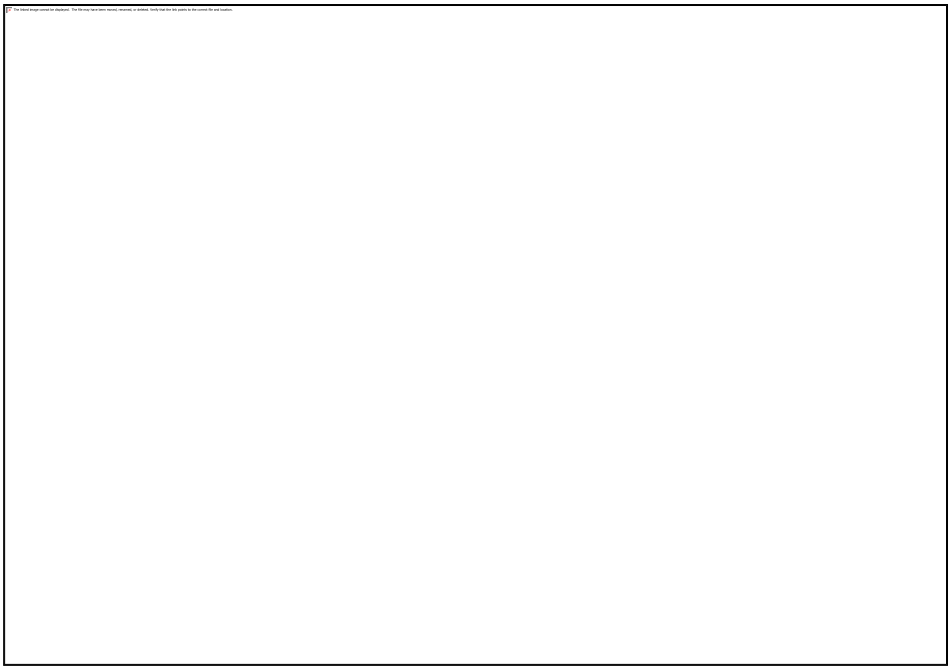


Customize the Storage in Predefined Destination



Navigate to **Backup / Restore** > **Users, Group & Policies**, then select the **Policy Group** tab. Click on the desired Policy Group, then select the **Backup Set Settings** section on the left. You can add a predefined destination for your clients, and your clients will be able to select the predefined destination when they create a new backup set.

Example:



NOTE

You need to add a predefined destination in advance, after that you can set the predefined destination visible to your user group.

11 API

In this release, new APIs (now in JSON format) are introduced in the AhsayCBS, if you have written API in previous version, please test and modify your API calls on AhsayCBS v7 in your testing environment first, so that it will not affect your current CRM, billing systems etc. when new AhsayCBS is upgraded. Please download the AhsayCBS API guide from our website for reference.

12 Contacting Ahsay

Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the following website:
https://www.ahsay.com/jsp/en/contact/kbQuestion.jsp

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

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/jsp/en/contact/kbQuestion.jsp

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

Appendix

Appendix A Supported Language Code

Language Code	Language
ar	Arabic
ca	Catalan
cs	Czech
da	Danish
de	German
el	Greek Modern
en	English
es	Spanish
eu	Euskara/Basque
fr	French
iw	Hebrew
hu	Hungarian
it	Italian
ja	Japanese
ko	Korean
lt	Lithuanian
nl	Dutch
no	Norwegian
pl	Polish
pt_BR	Portuguese (Brazil)
pt_PT	Portuguese (Portugal)
sl	Slovenian
sv	Swedish
tr	Turkish
zh_CN	Chinese (Simplified)
zh_TW	Chinese (Traditional)

Appendix B Supported Time Zone

Timezone String	Timezone Name
GMT-11:00 (WST)	Western Standard Time
GMT-11:00 (NUT)	Niue Time
GMT-11:00 (SST)	Samoa Standard Time
GMT-10:00 (HADT)	Hawaii-Aleutian Daylight Time
GMT-10:00 (HST)	Hawaiian Standard Time
GMT-10:00 (TKT)	Tokelau Time
GMT-10:00 (HST)	Hawaiian Standard Time
GMT-10:00 (CKT)	Cook Islands Time
GMT-10:00 (THAT)	Tahiti Time
GMT-09:00 (AKST)	Alaska Standard Time
GMT-09:00 (GAMT)	Gambier Time
GMT-08:00 (PST)	Pacific Standard Time (North America)
GMT-07:00 (PDT)	Pacific Daylight Time (North America)
GMT-07:00 (MST)	Mountain Standard Time
GMT-07:00 (MDT)	Mountain Day Time
GMT-06:00 (CST)	Central Standard Time
GMT-06:00 (CDT)	Central Daylight Time
GMT-06:00 (EAST)	Easter Island Time
GMT-06:00 (GALT)	Galapagos Time
GMT-05:00 (EST)	Eastern Standard Time (North America)
GMT-05:00 (EDT)	Eastern Daylight Time (North America)
GMT-05:00 (COT)	Colombia Time
GMT-05:00 (ECT)	Ecuador Time
GMT-05:00 (CDT)	Central Daylight Time (North America)
GMT-05:00 (PET)	Peru Time
GMT-05:00 (ACT)	Atlantic/Proto Acre
GMT-05:00 (GMT-05:00)	GMT -05:00
GMT-04:00 (AST)	Atlantic Standard Time

GMT-04:00 (PYT)	Paraguay Time
GMT-04:00 (VET)	Venezuela Time
GMT-04:00 (GYT)	Guyana Time
GMT-04:00 (ADT)	Acre Daylight Time
GMT-04:00 (BOT)	Bolivia Time
GMT-04:00 (AMT)	Armenia Time
GMT-04:00 (CLT)	Chile Time
GMT-04:00 (FKT)	Falkland Islands
GMT-03:00 (ART)	Argentina Time
GMT-03:00 (GFT)	French Guiana Time
GMT-03:00 (BRT)	Brasilia Time
GMT-03:00 (WGST)	West Greenland Summer Time
GMT-03:00 (PMDT)	Pierre & Miquelon Daylight Time
GMT-03:00 (UYT)	Uruguay Time
GMT-03:00 (SRT)	Suriname Time
GMT-02:00 (FNT)	Fernando de Noronha Time
GMT-02:00 (GST)	Gulf Standard Time
GMT-01:00 (EGST)	East Greenland Summer Time
GMT+00:00 (GMT)	Greenwich Mean Time
GMT+00:00 (WET)	Western European Time
GMT+00:00 (WEST)	Western European Summer Time
GMT+00:00 (IST)	Israel Standard Time
GMT+00:00 (BST)	Brazil Standard Time
GMT+00:00 (UTC)	Coordinate Universal Time
GMT+01:00 (CET)	Central European Time
GMT+01:00 (WAT)	West Africa Time
GMT+01:00 (CEST)	Central European Summer Time
GMT+02:00 (EEST)	Eastern European Summer Time
GMT+02:00 (CAT)	Central Africa Time
GMT+02:00 (SAST)	Soft Africa Standard Time

GMT+02:00 (EET)	Eastern European Time
GMT+02:00 (IDT)	Israel Daylight Time
GMT+03:00 (EAT)	East Africa Time
GMT+03:00 (AST)	Acre Standard Time
GMT+03:00 (ADT)	Acre Daylight Time
GMT+03:00 (MSD)	Moscow Daylight Time
GMT+04:00 (AQTST)	Aqtau Time
GMT+04:00 (AZST)	Azerbaijan Summer Time
GMT+04:00 (GST)	Gulf Standard Time
GMT+04:00 (GEST)	Georgia Time
GMT+04:00 (AMST)	Armenia Summer Time
GMT+04:00 (SAMST)	Samara Time
GMT+04:00 (SCT)	Seychelles Time
GMT+04:00 (MUT)	Mauritius Time
GMT+04:00 (RET)	Reunion Time
GMT+05:00 (TMT)	Turkmenistan Time
GMT+05:00 (KGST)	Kirgizstan Time
GMT+05:00 (TJT)	Tajikistan Time
GMT+05:00 (PKT)	Pakistan Time
GMT+05:00 (UZT)	Uzbekistan Time
GMT+05:00 (YEKST)	Yekaterinburg Time
GMT+05:00 (IDT)	Indian Standard Time
GMT+05:00 (TFT)	French Southern & Antarctic Lands Time
GMT+05:00 (MVT)	Maldives Time
GMT+06:00 (MAWT)	Mawson Time
GMT+06:00 (LKT)	Lanka Time
GMT+06:00 (BDT)	Bangladesh Time
GMT+06:00 (NOVST)	Novosibirsk Time
GMT+06:00 (BTT)	Bhutan Time
GMT+07:00 (ICT)	Indochina Time

GMT+07:00 (JAVT)	Java Time, Indonesia Time
GMT+07:00 (KRAST)	Krasnoyarsk Time
GMT+07:00 (CXT)	Christmas Island Time
GMT+08:00 (HKT)	Hong Kong Time
GMT+08:00 (CST)	Cuba Standard Time
GMT+08:00 (BNST)	Brunei Time
GMT+08:00 (WST)	West Samoa Time
GMT+08:00 (IRKST)	Irkutsk Time
GMT+08:00 (MYT)	Malaysia Time
GMT+08:00 (PHT)	Philippine Time
GMT+08:00 (SGT)	Singapore Time
GMT+08:00 (BORT)	Borneo Time
GMT+08:00 (ULAT)	Ulan Bator Time
GMT+08:00 (JAYT)	Jayapura Time
GMT+09:00 (KST)	Korean Standard Time
GMT+09:00 (JST)	Japan Standard Time
GMT+09:00 (YAKST)	Yakutsk Time
GMT+09:00 (PWT)	Palau Time
GMT+10:00 (EST)	Eastern Standard Time (Australia)
GMT+10:00 (DDUT)	Dumont-d'Urville Time
GMT+10:00 (VLAST)	Vladivostok Time
GMT+10:00 (ChST)	Chamorro Standard Time
GMT+10:00 (PGT)	Papua New Guinea Time
GMT+10:00 (TRUST)	Truk Time
GMT+11:00 (MAGST)	Magadan Time
GMT+11:00 (VUT)	Vanuatu Time
GMT+11:00 (KOSST)	Kosrae Time
GMT+11:00 (NCT)	New Caledonia Time
GMT+11:00 (PONT)	Ponape Time (Micronesia)
GMT+12:00 (NZST)	New Zealand Standard Time

GMT+12:00 (ANAST)	Anadyr Time
GMT+12:00 (PETST)	Petropavlovsk-Kamchatski Time
GMT+12:00 (FJT)	Fiji Time
GMT+12:00 (TVT)	Tuvalu Time
GMT+12:00 (MHT)	Marshall Islands Time
GMT+12:00 (NRT)	Nauru Time
GMT+12:00 (GILT)	Gilbert Island Time
GMT+12:00 (WAKT)	Wake Time
GMT+12:00 (WFT)	Wallis and Futuna Time

Appendix C Error Code 1011 and 1012

Internal Error 1011

This error could occur when one of the following conditions is true:

- The license key has been used on more than one machine.
- Change of network card of the server machine or moving the AhsayCBS system to a new server.

Solution:

In the cases where the license key was used on a second server for testing purposes, please use an evaluation key instead.

Alternatively, please shutdown the AhsayCBS service on the second server, and then contact our Support Engineer with your "License Name" and "License Key", and we shall update the license server to allow your key to be used again.

In the cases where the network card of the server machine is changed, or an AhsayCBS relocation has been performed. Please also contact our Support Engineer with your "License Name" and "License Key", and we shall update the license server to allow your key to be used again.

If the problem still persists, please ensure that there are no connectivity issues from the AhsayCBS server to the Internet and that you can connect to lic.ahsay.com with HTTPS from the AhsayCBS backup server. There is a connection test button underneath the license field entry box to test the connection to our license server. The testing result will be displayed next to the test button.

Please also verify if the machine in concern contain any software that would create virtual MAC address, for example, VPN software. If yes, please disable them such software, and notify us again.

Internal Error 1012

Internal Error 1012 can occurs when one of the following conditions is true:

- The license key has been used on more than one machine.
- Change of the MAC address, local / remote IP address, or local port that AhsayCBS is installed on.

Solution:

Persistent 1012 license errors can occur if your AhsayCBS server is operating in a network environment where network traffic is routed to the Internet via multiple external IP addresses. For example, network load balancing is implemented using, i.e. a dual WAN router, Round Robin routing, or network card with multiple external IP.

For these cases, we would suggest setting up a static route for the server's connection to lic.ahsay.com, so that the remote IP address on the server will remain the same every time a connection to lic.ahsay.com is established.

Appendix D Differences between AhsayOBS v6 vs AhsayCBS v7

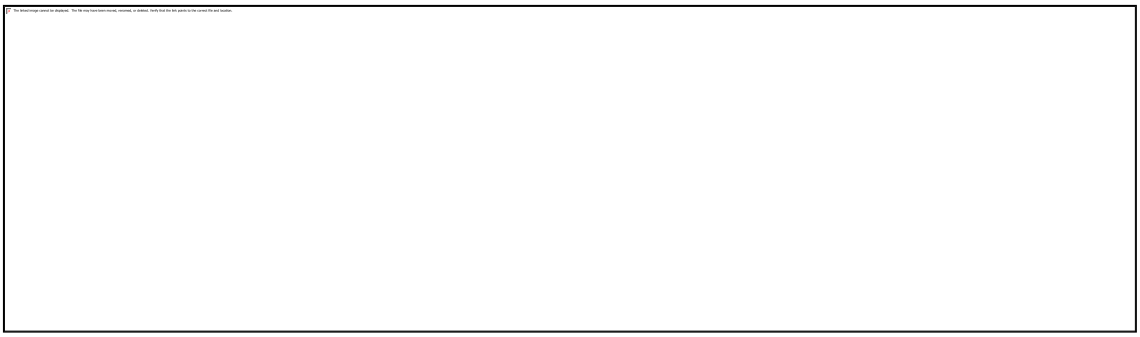
AhsayCBS has been totally re-designed from the ground upwards to provide the best cloud backup solution with changes to core functions, such as file storage system, indexing, backup set features, replication, group policy, system user and branding. To understand the differences between AhsayCBS and previous version of our product, please visit our website for details.

For a list of key differences between the AhsayOBS v6 and AhsayCBS v7, refer to Differences Between v6 & v7.

Appendix E Setting up Cloud Storage

In the following examples, we are demonstrating how to setup cloud storage in predefined destinations.

Add a predefined destination in **System Settings** -> **Basic** -> **Predefined Destinations**, click on the **Add** button.



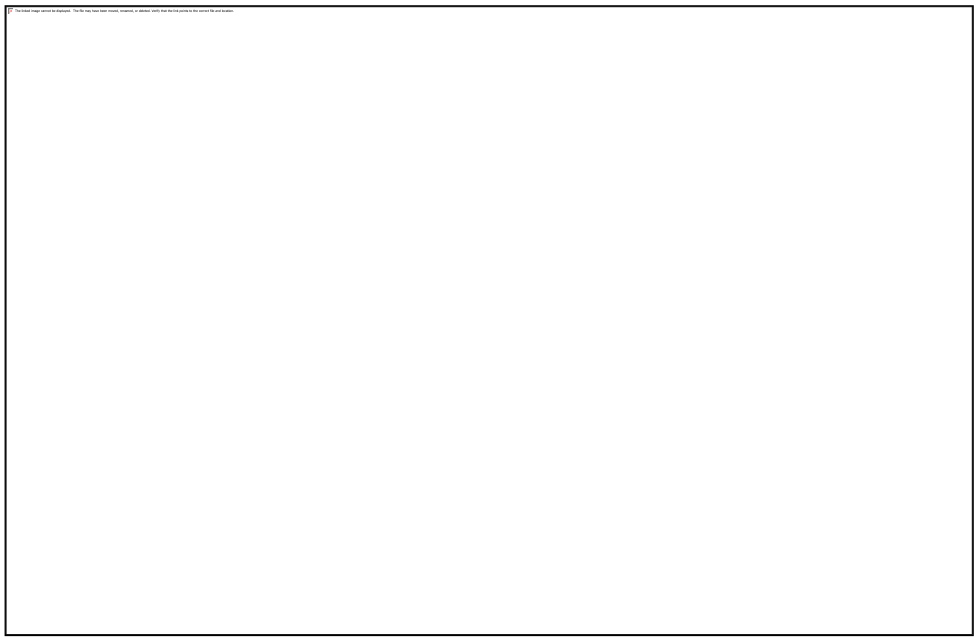
Aliyun (阿里云)

This storage option is available on computers with China or Hong Kong locale settings.

1. If you do not have the Aliyun (阿里云), please click on the link 'Sign up for 阿里云' to create an account.

2. Select '阿里云' from the **Destination storage** drop down box.

3. Enter name of the backup destination.



4. Select Single storage destination.

   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

5. Enter the Access Key ID.

6. Enter the Access Key Secret.

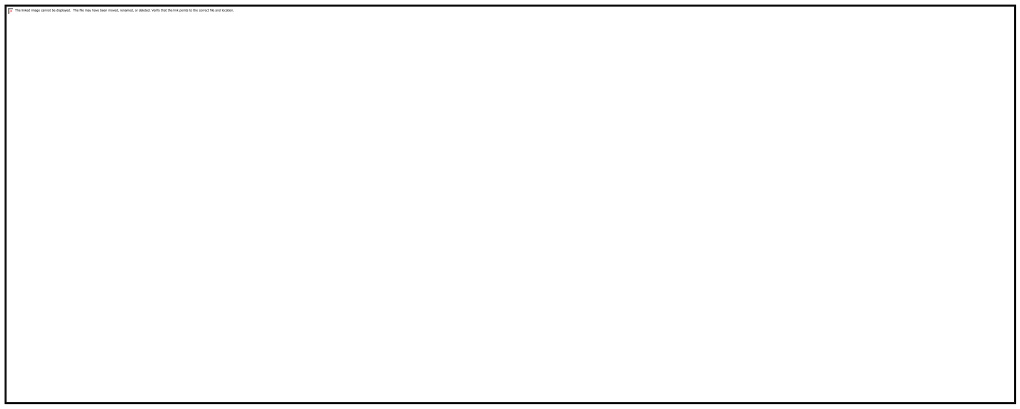
7. Select the region from the dropdown box.

8. Click **Add** to continue the setup.

9. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

   (By applying the changes to the "**Default settings**", all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

10. Add the newly created predefined storage "Aliyun-1" into the **Backup Set Settings** -> **Destinations Visible to Users** -> **Predefined Destinations**.



11. Enable the quota and apply the quota.

12. When you create a backup set for a user, you will be able to see the new predefined destination.

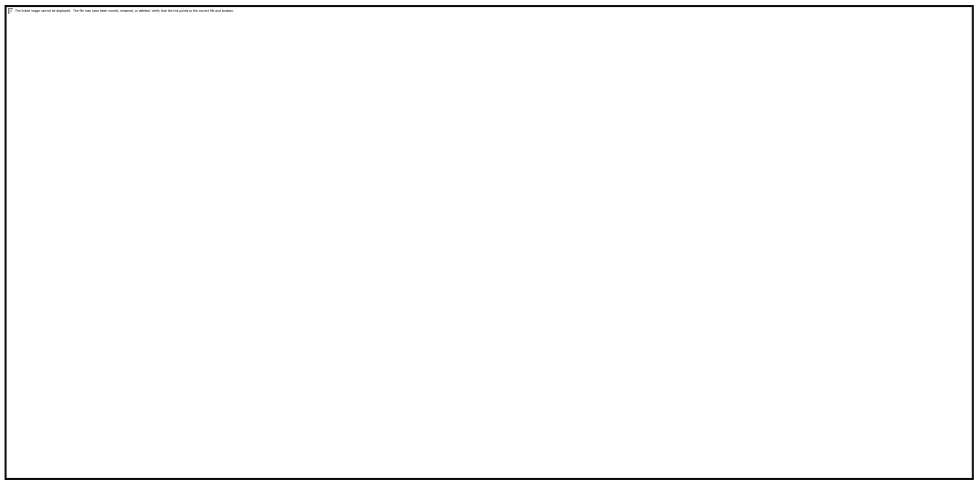
CTYun (中国电信天翼云)

This storage option is available on computers with China or Hong Kong locale settings.

1. If you do not have the CTYun (中国电信天翼云), please click on the link 'Sign up for 中国电信天翼云' to create an account.

2. Select '中国电信天翼云' from the [Destination storage] drop down box.

3. Enter name of the backup destination.



4. Select Single storage destination.

   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

5. Enter the Access Key ID.

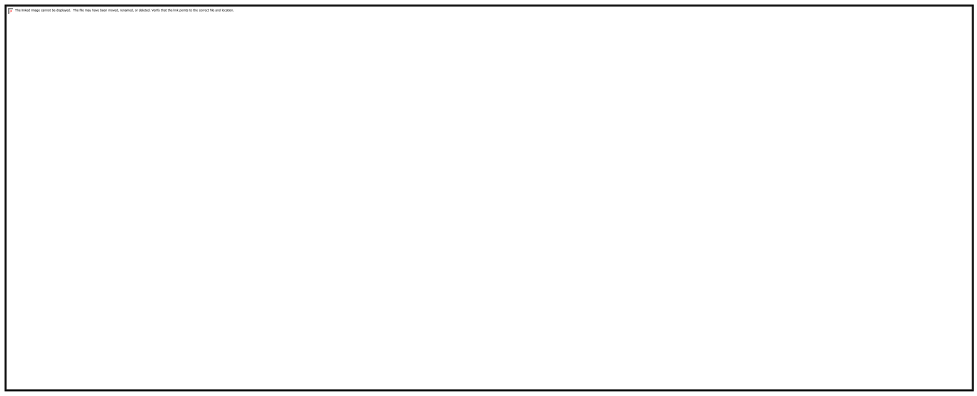
6. Enter the Secret Access Key.

7. Click [**Add**] to continue the setup.

8. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

   (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

9. Add the newly created predefined storage “CTYun-1” into the **Backup Set Settings** -> **Destinations Visible to Users** -> **Predefined Destinations**.



10. Enable the quota and apply the quota.

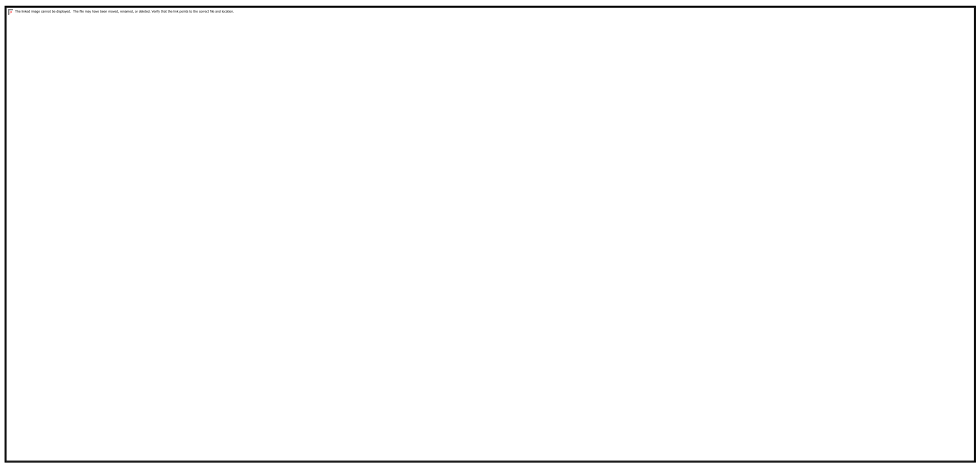
11. When you create a backup set for a user, you will be able to see the new predefined destination.

Amazon Cloud Drive

1. If you do not have the Amazon Cloud Drive, please click on the link **Sign up for Amazon Cloud Drive** to create an account.

2. Select 'Amazon Cloud Drive' from the [Destination storage] drop down box.

3. Enter name of the backup destination.

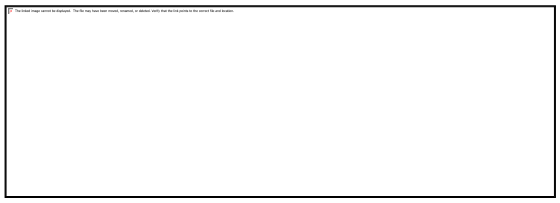


4. Select “Single storage destination”.

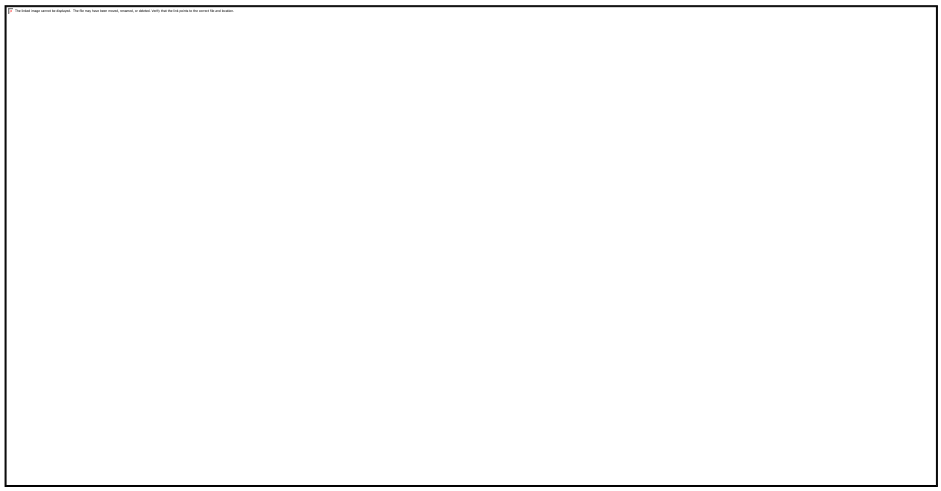
   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

5. Click [**Add**] to continue the setup.

   On the browser, a code is displayed, copy it and paste into the “**create predefined destination**” page in the AhsayCBS.



(Sample authentication code)

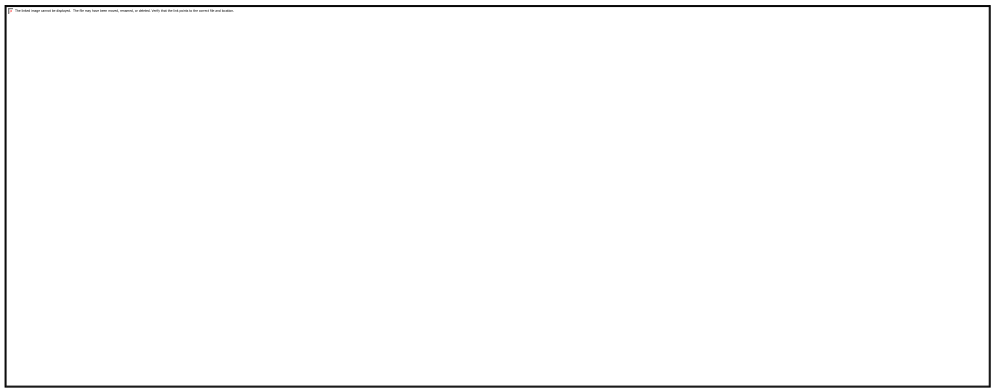


6. Click **Add** to continue.

7. Enter to the Backup/Restore -> Users, Groups & Policies -> Policy Group -> Manage Policy Group, edit the Default settings policy.

8. (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

9. Add the newly created predefined storage “AmazonCloudDrive-1” into the [**Backup Set Settings**] -> [**Destinations Visible to Users**] -> [**Predefined Destinations**].



10. Enable the quota and apply the quota.

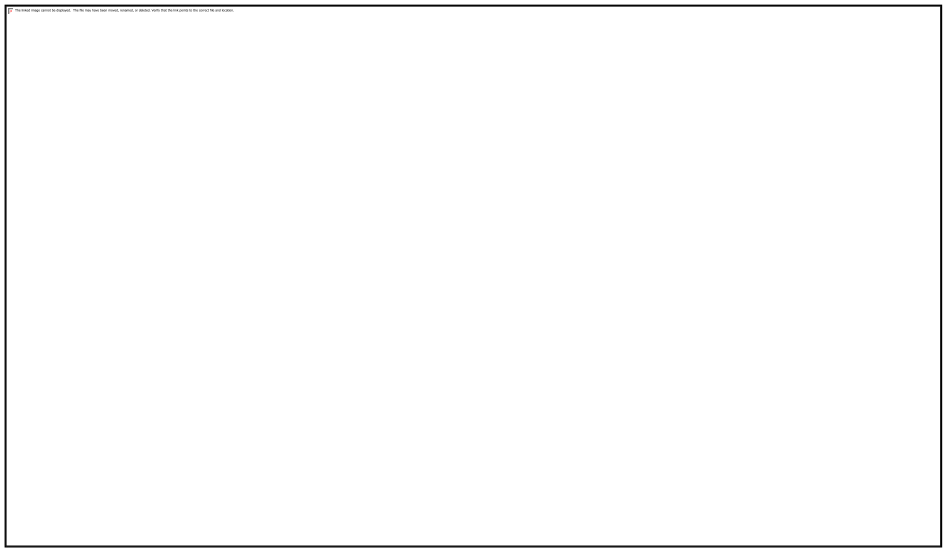
11. When you create a backup set for a user, you will be able to see the new predefined destination.

Amazon S3

1. If you do not have the Amazon S3, please click on the link **Sign up for Amazon S3** to create an account.

2. Select **Amazon S3** from the [**Destination storage**] drop down box.

3. Enter name of the backup destination



4. Select Single storage destination.

   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

5. Select the "**Location**" from the drop down box.

6. Enter the Access Key ID.

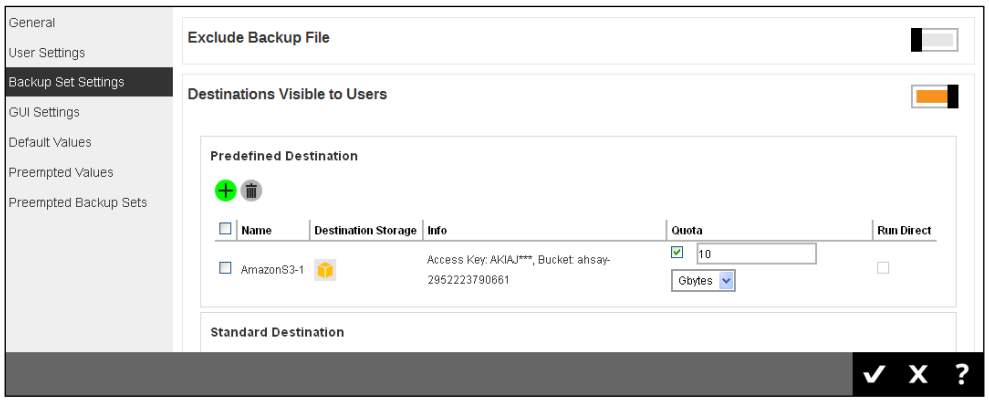
7. Enter the Secret Access Key.

8. Click [**Add**] to continue the setup.

9. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

10. (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

11. Add the newly created predefined storage "AmazonS3-1" into the [Backup Set Settings] -> [Destinations Visible to Users] -> [Predefined Destinations].



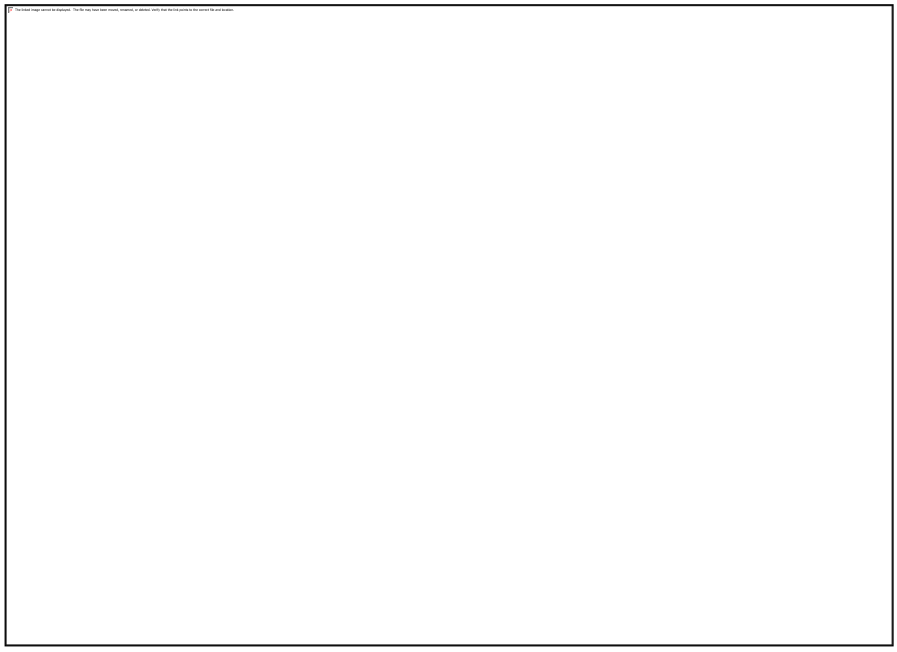
12. Enable the quota and apply the quota.

13. When you create a backup set for a user, you will be able to see the new predefined destination.

AWS S3 Compatible Cloud Storage

1. Select AWS S3 Compatible Cloud Storage from the Destination storage drop down box.

2. Enter name of the backup destination.



3. Select Single storage destination.

   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

4. Enter the Host and Port number.

5. Enter the Access Key ID.

6. Enter the Secret Access Key.

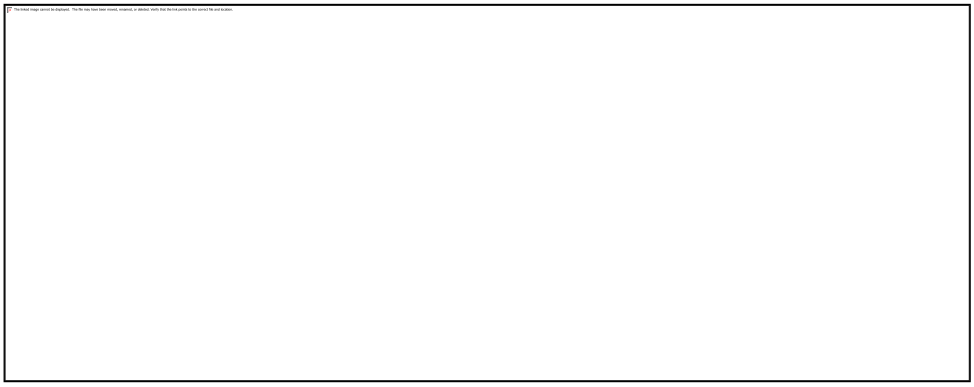
7. Enter the **Bucket Name** for the storage. (You need to create this bucket manually first).

8. Click [**Add**] to continue the setup.

9. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

   (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

10. Add the newly created predefined storage “AWSCompatible-1” into the [**Backup Set Settings**] -> [**Destinations Visible to Users**] -> [**Predefined Destinations**].



11. Enable the quota and apply the quota.

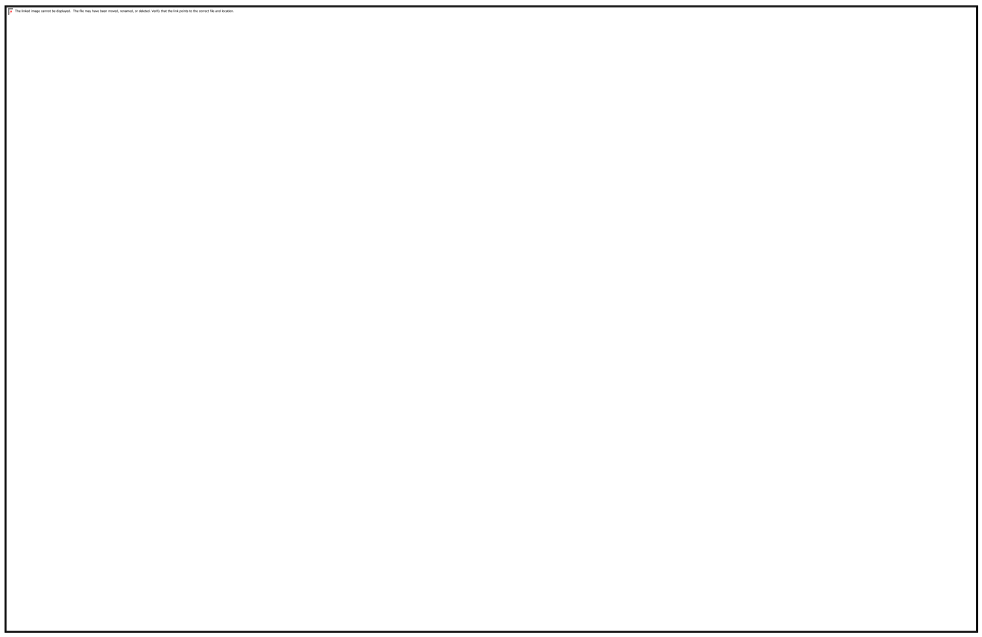
12. When you create a backup set for a user, you will be able to see the new predefined destination.

Dropbox

1. If you do not have the Dropbox, please click on the link 'Sign up for Dropbox' to create an account.

2. Select 'Dropbox' from the [Destination storage] drop down box.

3. Enter name of the backup destination.

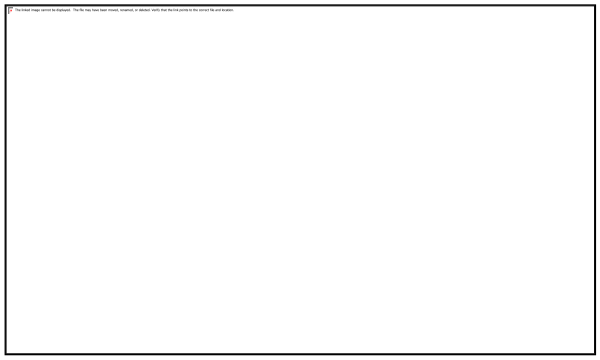


4. Select Single storage destination.

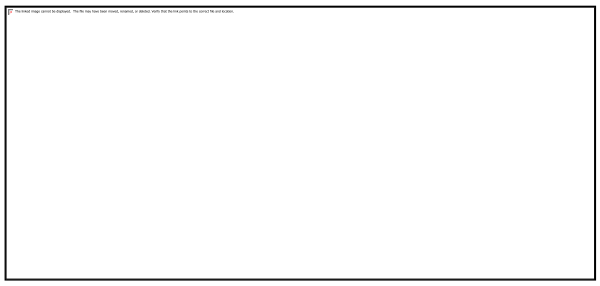
   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

5. Click [**Add**] to continue the setup.

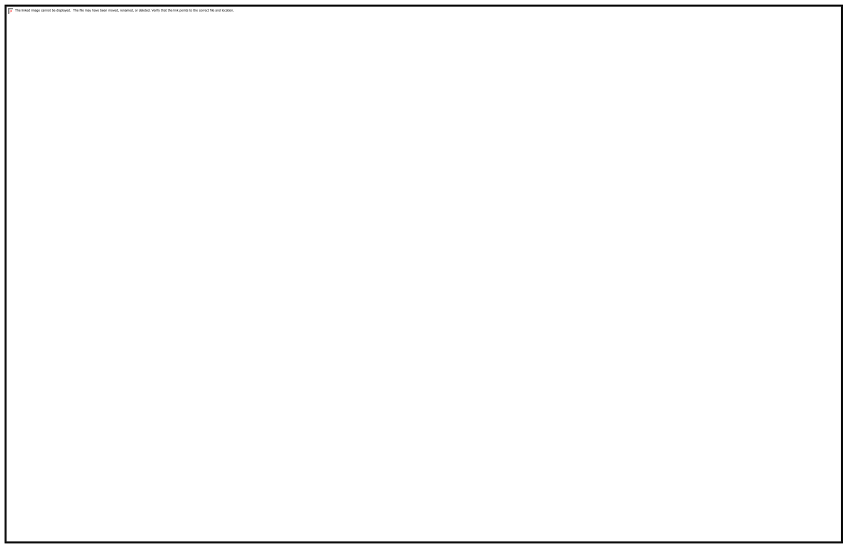
6. A browser will pop up and Dropbox will ask for your permission to access the storage, click on "Ahsay".



7. On the browser, a code is displayed, copy it and paste into the “create predefined destination” page in the AhsayCBS.



(Sample authentication code)

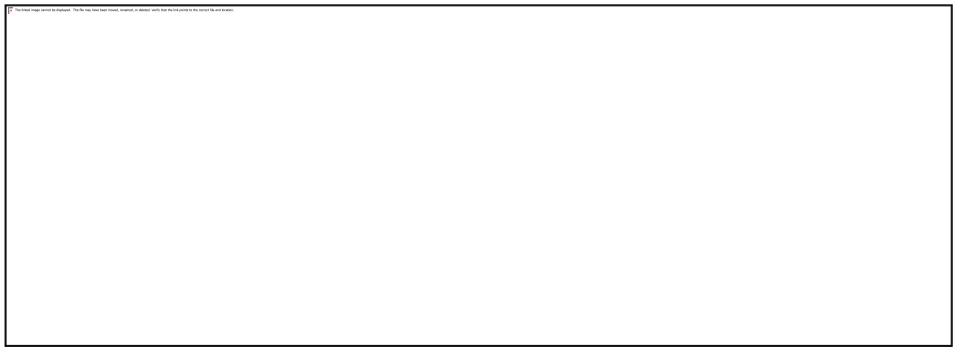


8. Click **Add** to continue the setup.

9. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

   (By applying the changes to the “**Default settings**”, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

10. Add the newly created predefined storage “Dropbox-1” into the **Backup Set Settings** -> **Destinations Visible to Users** -> **Predefined Destinations**.



11. Enable the quota and apply the quota.

12. When you create a backup set for a user, you will be able to see the new predefined destination.

Google Cloud Storage

** Before you set up the storage for Google Cloud Storage, please collect the Access Key and Secret Key from your Google Cloud Storage account first.

1. Go to the Google Developers Console.

2. Click the name of the project you would like to use as your default project.

3. In the left sidebar, click APIs & auth.

4. Find Google Cloud Storage JSON API and make sure it is enabled. When the JSON API is enabled, the Status will display "ON".

5. Next to the Google Cloud Storage JSON API service, click the settings gear icon.

6. Click Interoperable Access in the left sidebar.

7. Click Generate new key.

8. The access key part of the new developer key is displayed.

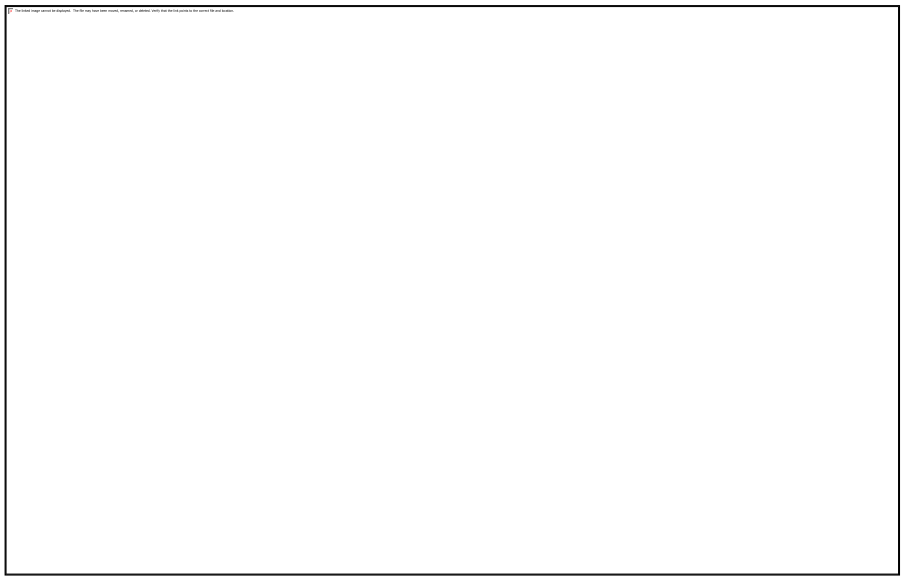
9. Click Show to show the secret part of the new developer key.

   Now, you can go back to add your predefined destination.

10. If you do not have the Google Cloud Storage, please click on the link **Sign up for Google Cloud Storage** to create an account.

11. Select Google Cloud Storage from the Destination storage drop down box.

12. Enter name of the backup destination.



13. Select Single storage destination.

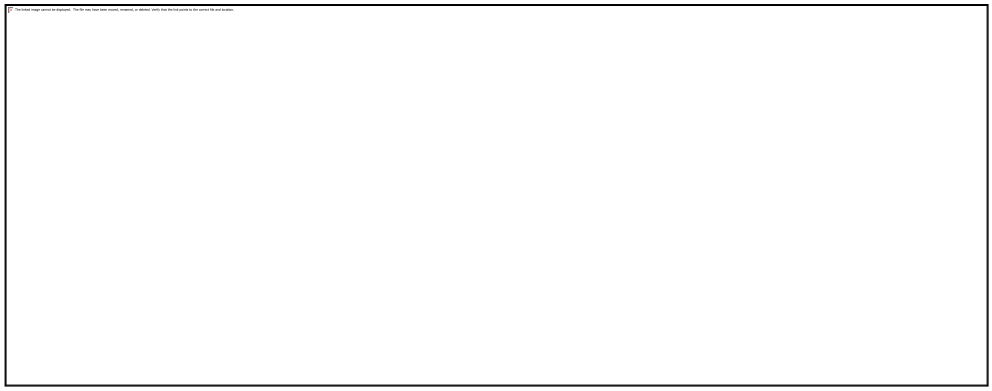
    Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

14. Click [**Add**] to continue the setup.

15. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

    (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

16. Add the newly created predefined storage “GoogleCloudStorage-1” into the [Backup Set Settings] -> [Destinations Visible to Users] -> [Predefined Destinations].



17. Enable the quota and apply the quota.

18. When you create a backup set for a user, you will be able to see the new predefined destination.

Google Drive

1. If you do not have the Google Drive, please click on the link **'Sign up for Google Drive'** to create an account.

2. Select 'Google Drive' from the [**Destination storage**] drop down box.

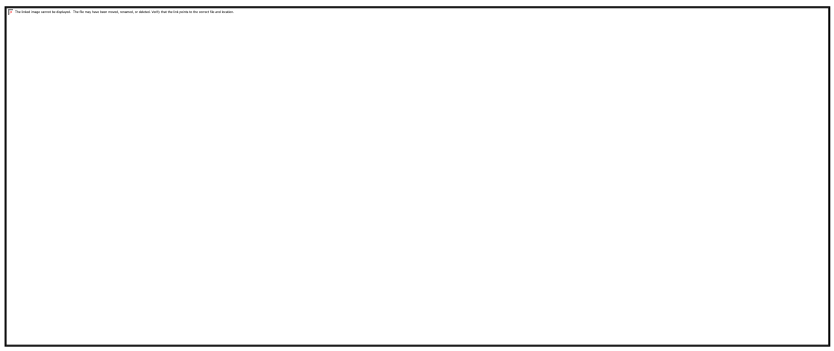
3. Enter name of the backup destination.

4. Select Single storage destination.

   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

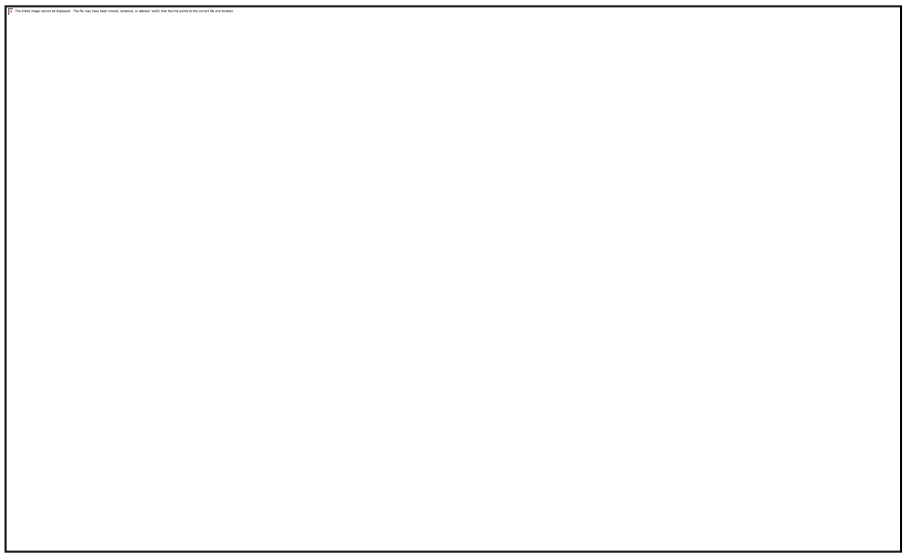
5. Click [**Add**] to continue the setup.

6. A browser will pop up and Google will ask for your permission to access the storage, click on "**Allow**".



7. On the browser, a code is displayed, copy it and paste into the “create predefined destination” page in the AhsayCBS.

(Sample authentication code)



8. Click [**Add**] to continue.

9. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

   (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

10. Add the newly created predefined storage “GoogleDrive-1” into the [**Backup Set Settings**] -> [**Destinations Visible to Users**] -> [**Predefined Destinations**].

11. Enable the quota and apply the quota.

12. When you create a backup set for a user, you will be able to see the new predefined destination.

Microsoft Azure

** Before you setup the storage for Microsoft Azure, please collect the Storage Account Name and Access Key from your Microsoft Azure account first.

1. Go to the Microsoft Azure web page.

2. Click the "portal" link at the top of the page.

3. Login to the portal.

4. Click on the "**MANAGE ACCESS KEYS**" link at the bottom of the page.

5. The "**STORAGE ACCOUNT NAME**" and "**PRIMARY ACCESS KEY**" are displayed. The Storage account name is the same as the node name when you create this Windows Azure account.

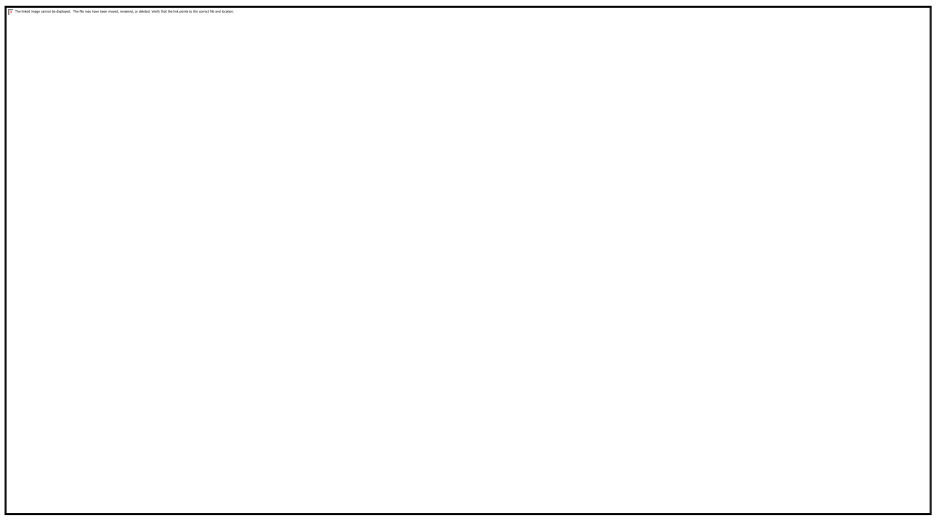
6. Copy the "**STORAGE ACCOUNT NAME**" and "**PRIMARY ACCESS KEY**" to your AhsayOBM application.

   (Suggested to copy and paste the name and key to avoid typographical errors.)

   Now, you can go back to add your predefined destination.

7. Select 'Microsoft Azure' from the [Destination storage] drop down box.

8. Enter name of the backup destination.



9. Select Single storage destination.

   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

10. Enter the Storage Account Name.

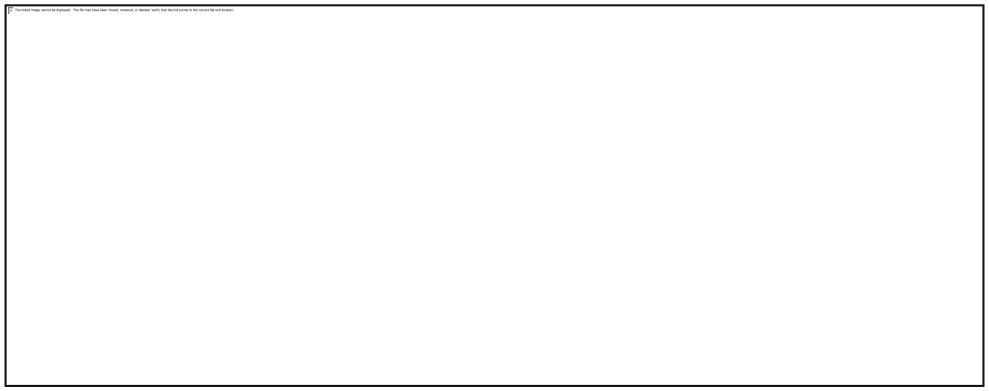
11. Enter the Access Key.

12. Click [**Add**] to continue the setup.

13. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

    (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

14. Add the newly created predefined storage “MicrosoftAzure-1” into the [**Backup Set Settings**] -> [**Destinations Visible to Users**] -> [**Predefined Destinations**].



15. Enable the quota and apply the quota.

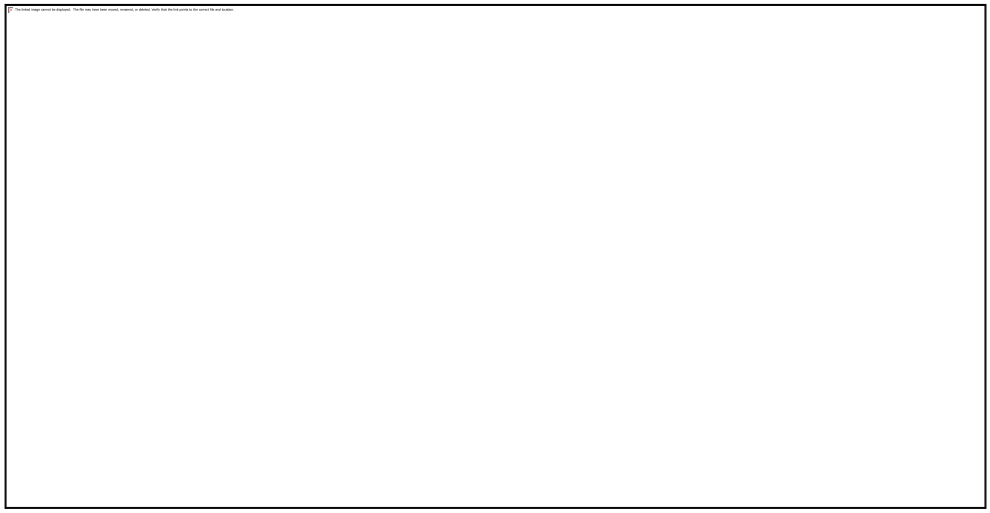
16. When you create a backup set for a user, you will be able to see the new predefined destination.

OneDrive

1. If you do not have the OneDrive, please click on the link 'Sign up for OneDrive' to create an account.

2. Select 'OneDrive' from the [**Destination storage**] drop down box.

3. Enter name of the backup destination.

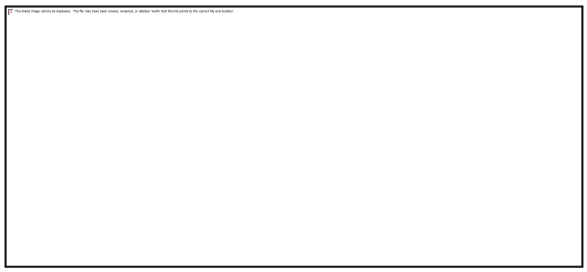


4. Select Single storage destination.

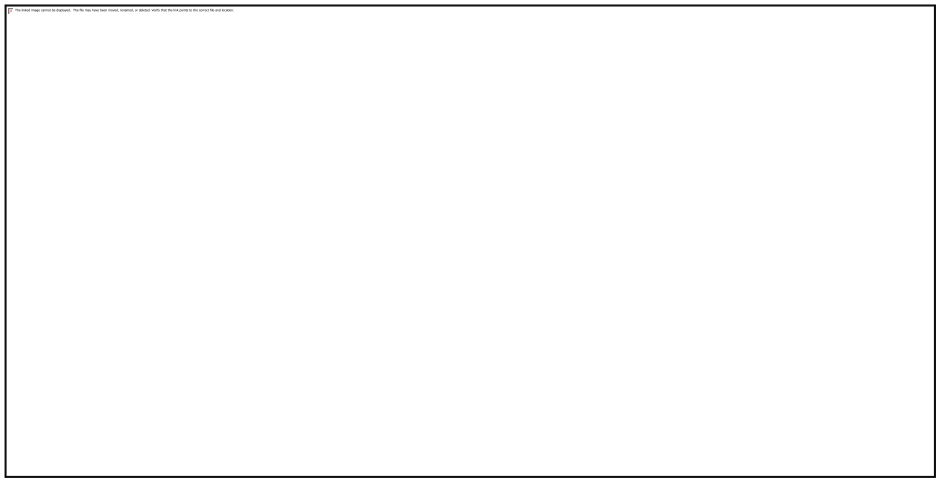
   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

5. Click [**Add**] to continue the setup.

6. A browser will popup and a code is displayed, copy it and paste into the "**create predefined destination**" page in the AhsayCBS.



(Sample authentication code)

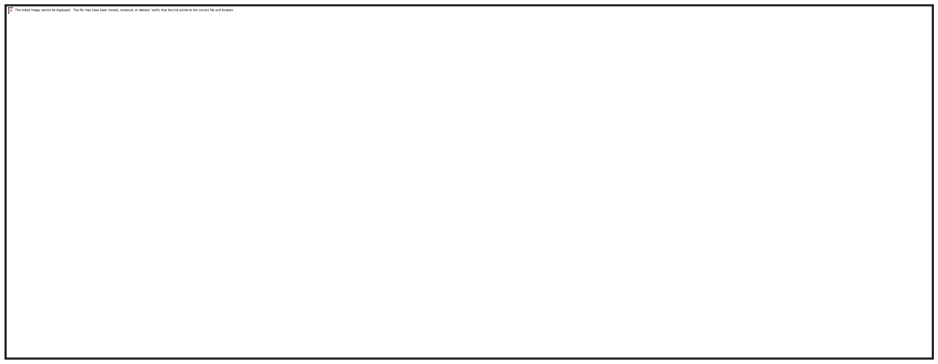


7. Click [**Add**] to continue the setup.

8. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

   (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

9. Add the newly created predefined storage “OneDrive-1” into the [**Backup Set Settings**] -> [**Destinations Visible to Users**] -> [**Predefined Destinations**].



10. Enable the quota and apply the quota.

11. When you create a backup set for a user, you will be able to see the new predefined destination.

OneDrive for Business

1. If you do not have the OneDrive for Business, please click on the link 'Sign up for OneDrive for Business' to create an account.

2. Select 'OneDrive' from the [**Destination storage**] drop down box.

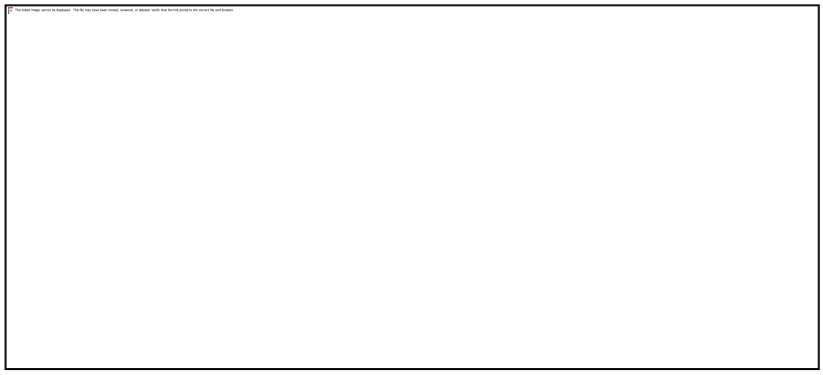
3. Enter name of the backup destination.

4. Select Single storage destination.

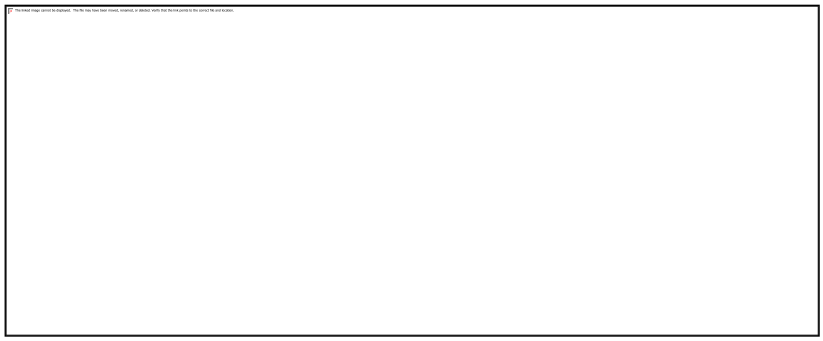
   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

5. Click [**Add**] to continue the setup.

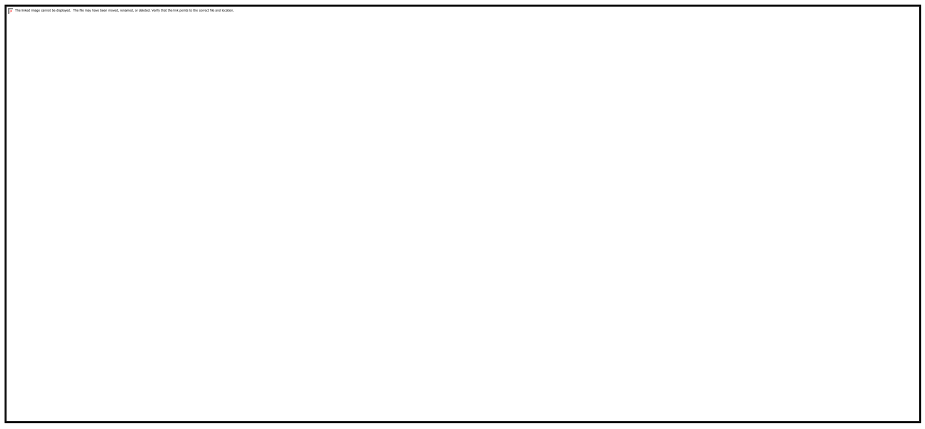
6. A browser will pop up and Microsoft will ask for your permission to access the storage, click on "**Accept**".



7. On the browser, a code is displayed, copy it and paste into the “create predefined destination” page in the AhsayCBS.



(Sample authentication code)

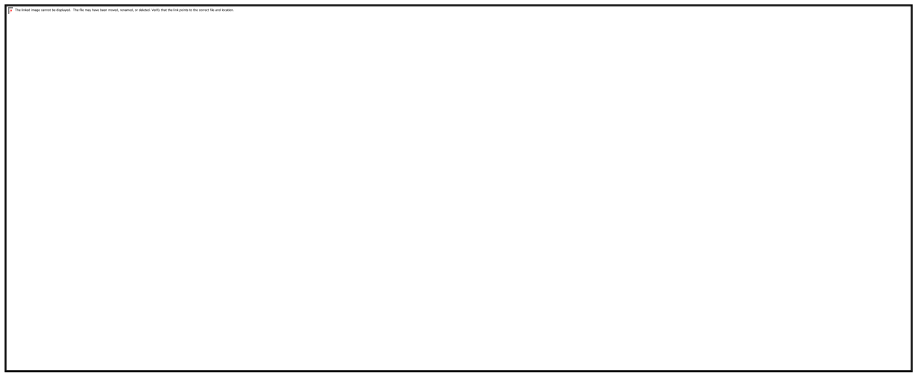


8. Click [**Add**] to continue.

9. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

   (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

10. Add the newly created predefined storage “OneDriveForBusiness-1” into the [**Backup Set Settings**] -> [**Destinations Visible to Users**] -> [**Predefined Destinations**].



11. Enable the quota and apply the quota.

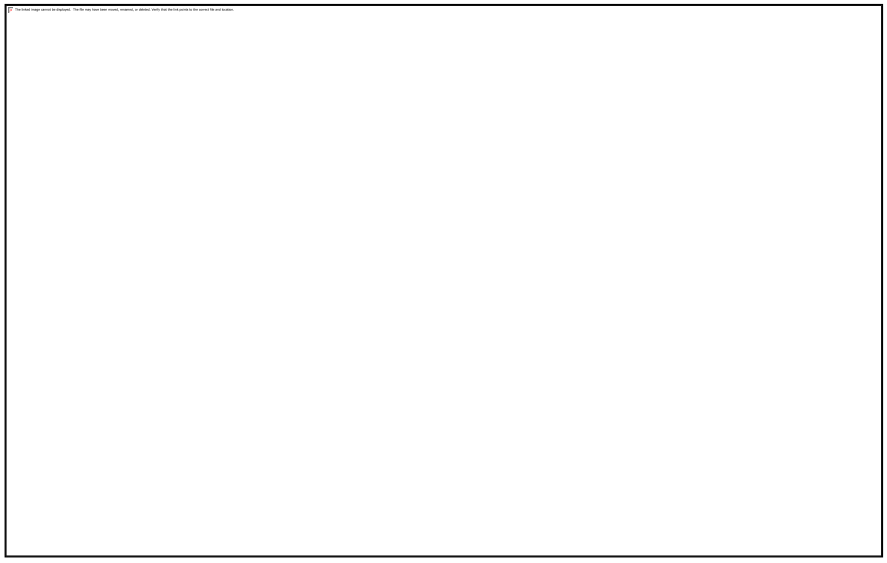
12. When you create a backup set for a user, you will be able to see the new predefined destination.

Rackspace

1. If you do not have the Rackspace, please click on the link 'Sign up for Rackspace' to create an account.

2. Select 'Rackspace' from the [**Destination storage**] drop down box.

3. Enter name of the backup destination.



4. Select Single storage destination.

   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

5. Enter the User Name.

6. Enter the API Key.

7. Click [**Add**] to continue the setup.

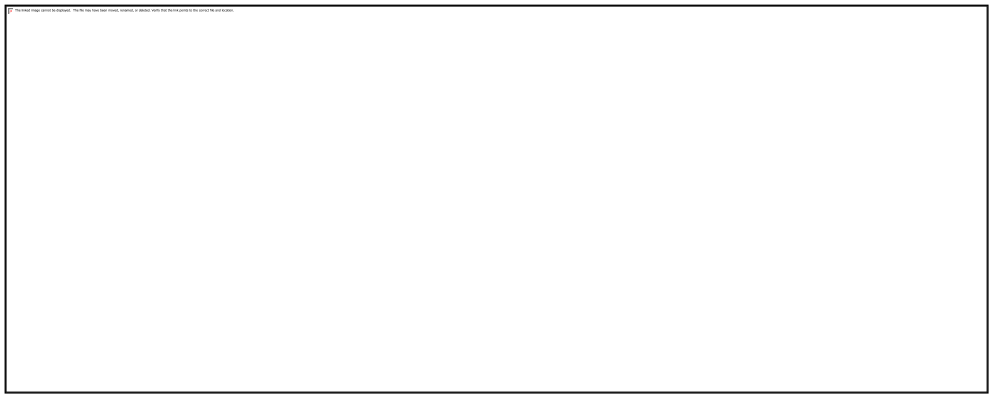
8. It will prompt for the “Region”, select the “Region” from the dropdown box.

9. Click [**Add**] to continue the setup.

10. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

    (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

11. Add the newly created predefined storage “Rackspace-1” into the [**Backup Set Settings**] -> [**Destinations Visible to Users**] -> [**Predefined Destinations**].



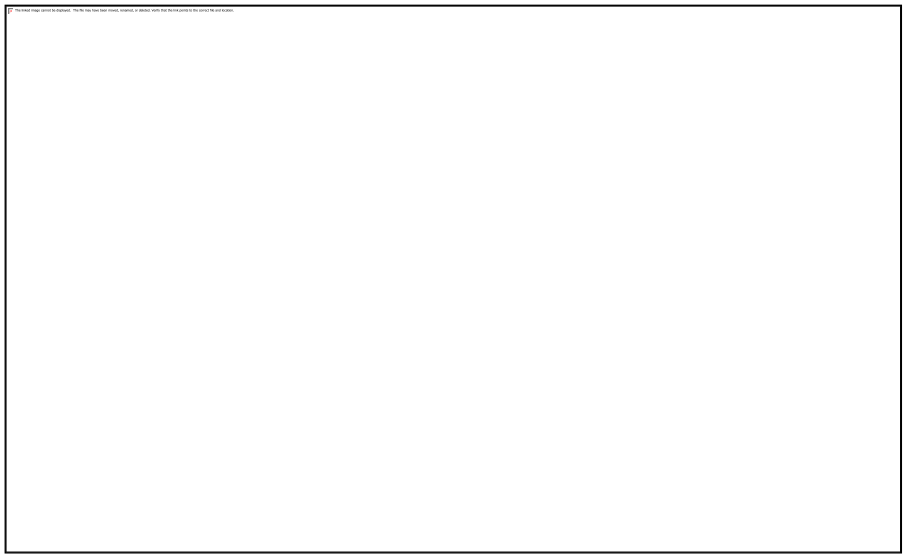
12. Enable the quota and apply the quota.

13. When you create a backup set for a user, you will be able to see the new predefined destination.

OpenStack

1. Select 'OpenStack' from the [**Destination storage**] drop down box.

2. Enter name of the backup destination.



3. Select Single storage destination.

   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

4. Enter the Host and Port number.

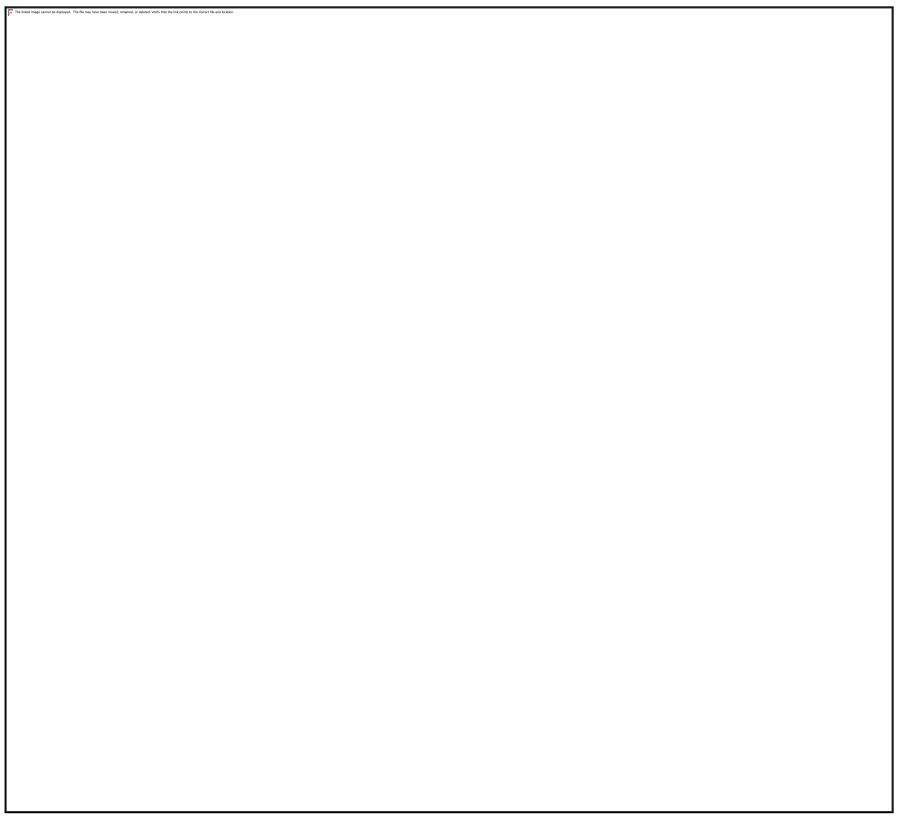
5. Enter the Username.

6. Enter the Password.

7. Option: Click on the check box "**Connect with SSL**" if necessary.

8. Click [**Add**] to continue the setup.

9. The page will request to enter more information after the initial connection.



10. Select the "**Project**" in the dropdown box.

11. Select the "**Region**" in the dropdown box.

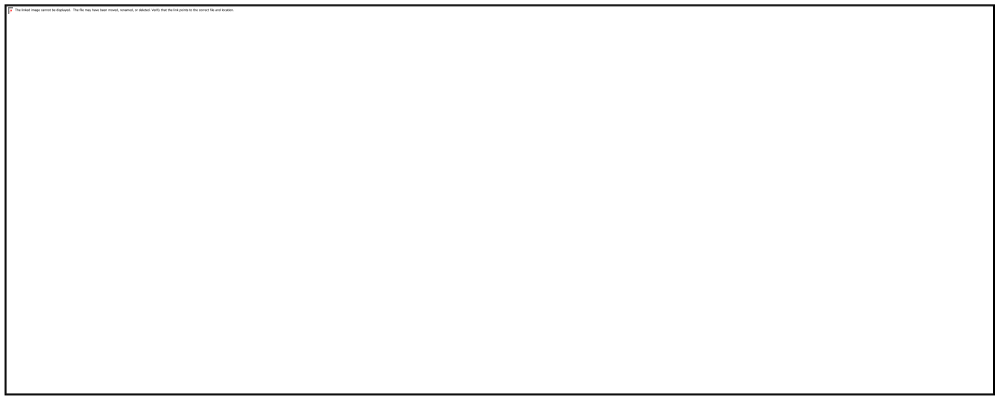
12. Enter the container name.

13. Click [**Add**] to continue the setup.

14. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

    (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

15. Add the newly created predefined storage “OpenStack-1” into the [**Backup Set Settings**] -> [**Destinations Visible to Users**] -> [**Predefined Destinations**].



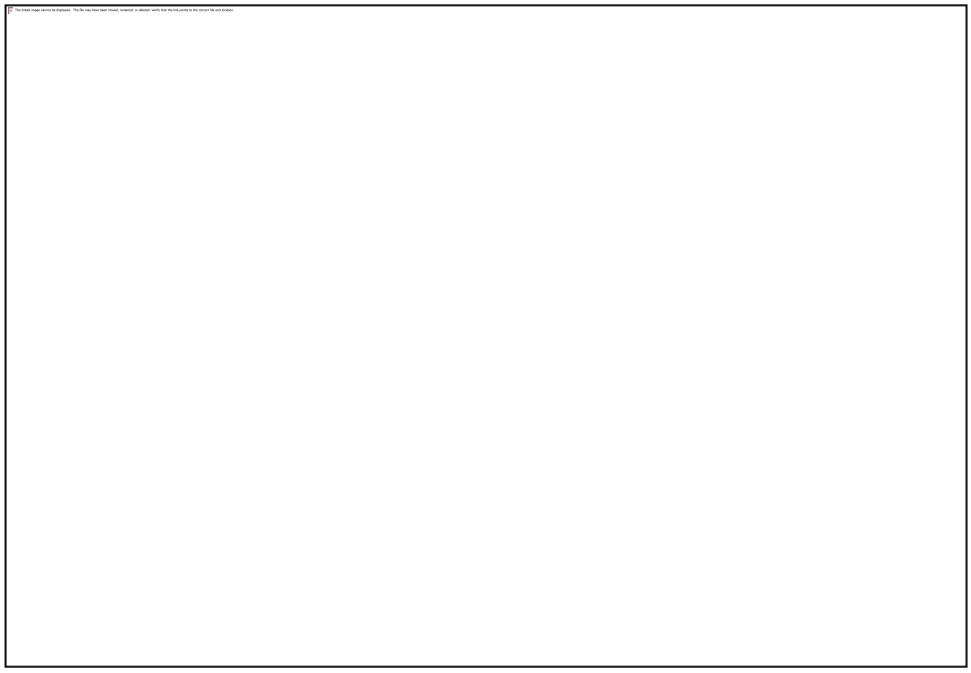
16. Enable the quota and apply the quota.

17. When you create a backup set for a user, you will be able to see the new predefined destination.

FTP

1. Select 'FTP' from the [**Destination storage**] drop down box.

2. Enter name of the backup destination.



3. Select Single storage destination.

   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*

4. Enter the Host and Port number.

5. Enter the Username.

6. Enter the Password.

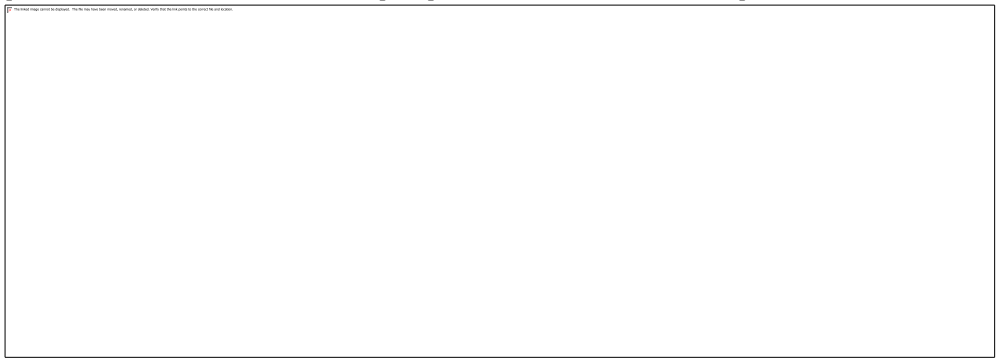
7. Option: Enter the FTP directory if you have one.

8. Click [**Add**] to continue the setup.

9. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

   (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

10. Add the newly created predefined storage “FTP-1” into the [**Backup Set Settings**] -> [**Destinations Visible to Users**] -> [**Predefined Destinations**].

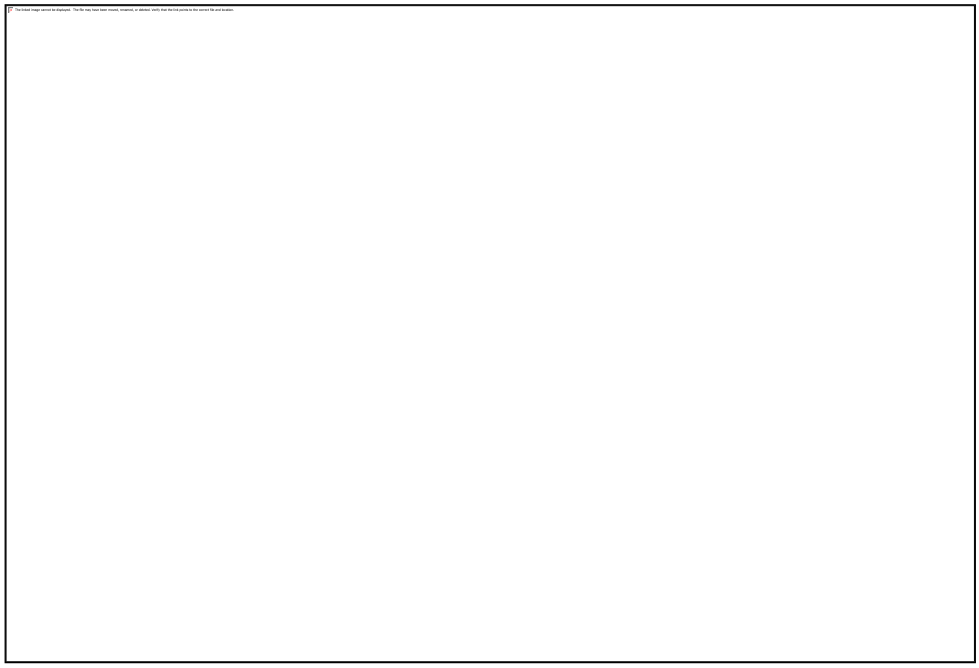


11. Enable the quota and apply the quota.

12. When you create a backup set for a user, you will be able to see the new predefined destination.

SFTP

1. Select 'SFTP' from the [**Destination storage**] drop down box.
2. Enter name of the backup destination.

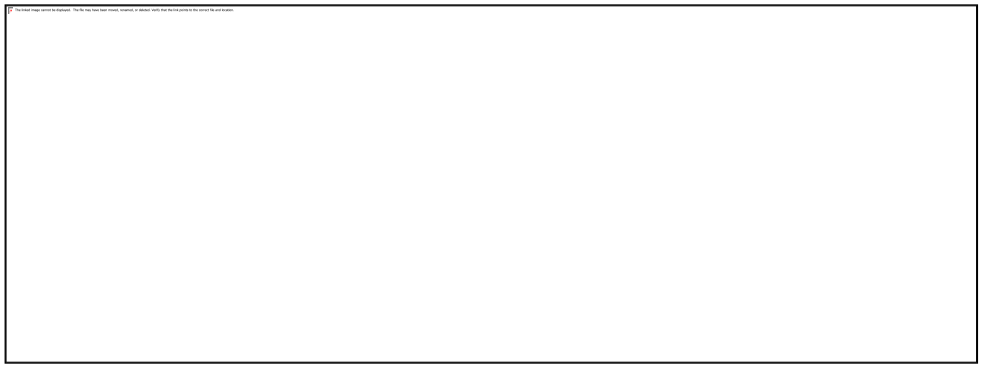


3. Select Single storage destination.

   Note: *The option* ***Destination Pool*** *is defined from a number of single storage destination.*
4. Enter the Host and Port number.
5. Enter the Username.
6. Enter the Password.
7. Option: Enter the SFTP directory if you have one.
8. Click [**Add**] to continue the setup.
9. Enter to the **Backup/Restore** -> **Users, Groups & Policies** -> **Policy Group** -> **Manage Policy Group**, edit the **Default settings** policy.

   (By applying the changes to the **Default settings**, all the users will be able to see and use the settings by default. If you need to create a predefined destination for a particular group of users, you need to create a new policy group and user group for this.)

10. Add the newly created predefined storage “SFTP-1” into the [**Backup Set Settings**] -> [**Destinations Visible to Users**] -> [**Predefined Destinations**].



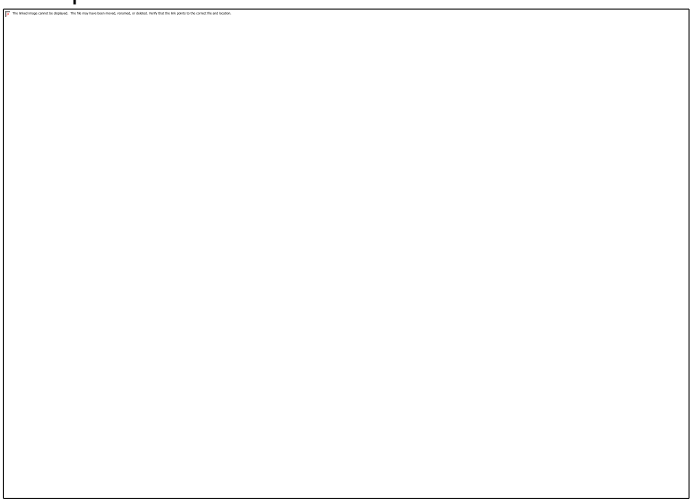
11. Enable the quota and apply the quota.

12. When you create a backup set for a user, you will be able to see the new predefined destination.

Appendix F Image Specifications

You can use common graphics editing tools that able to edit 32bit graphic files to generate these png format files with transparent background.

Example:



For those ico (Windows icon) and icns (Mac icon) files, you can use icon editing tools (available to download from Internet). Most of the icon files have multiple sizes of images. Please refer to the original icon format to replace your product logo into the files.

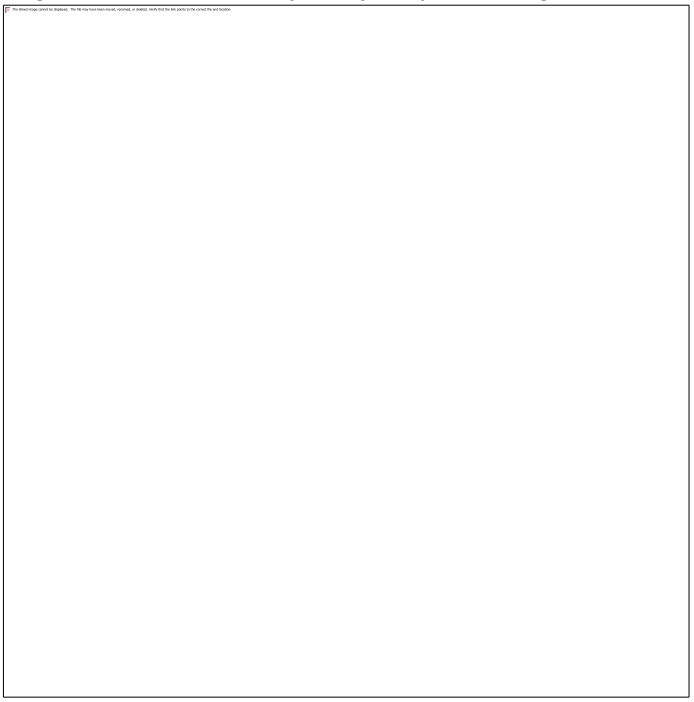
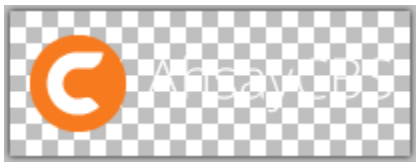


Image specifications for AhsayCBS (web interface, pdf and email report)

File name: ico_40_cbs_logo.png This logo has transparent background (checkered squares) with white text.	Format: png Width: 200 px Height: 72 px
	

File name: default.large.gif This logo has transparent background (checkered squares).	Format: gif Width: 129 px Height: 40 px

File name: ico_24_cbs.png This logo has transparent background (checkered squares).	Format: png Width: 24 px Height: 24 px

File name: ico_obm_16.png This logo has transparent background (checkered squares).	Format: png Width: 18 px Height: 18 px

File name: ico_acb_16.png	Format: png Width: 18 px Height: 18 px
This logo has transparent background (checkered squares).	

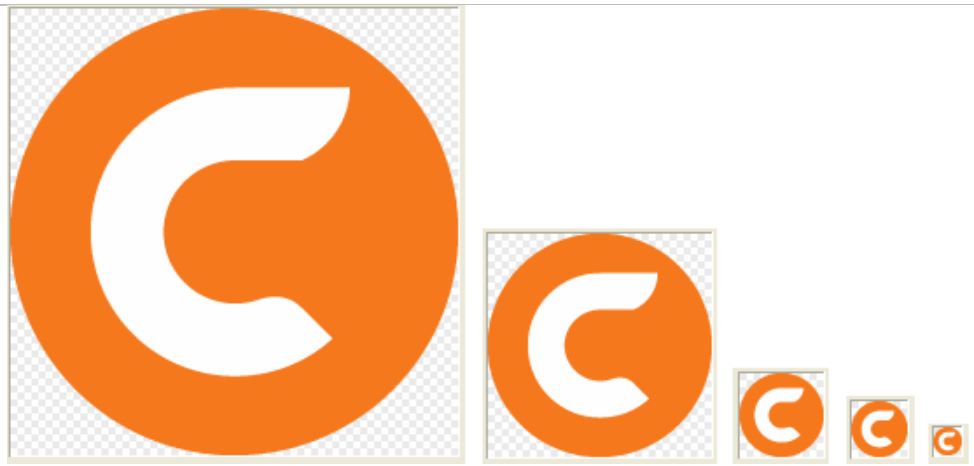
Image specifications for AhsayCBS (Installation graphics)

Images for Windows (Installation graphics)

File name: aboutBG.bmp	Format: Bitmap Width: 164 px Height: 337 px

(The size of this graphic is reduced to fit into this document.)

File name: desktop.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	



(The sizes of these logos are reduced to fit into this document.)

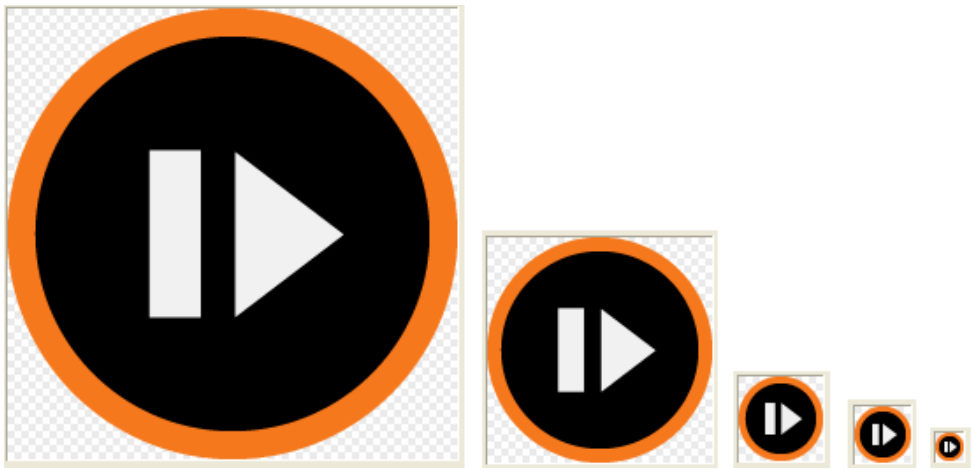
File name: installer.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

(The sizes of these logos are reduced to fit into this document.)

File name: splash.bmp	Format: Bitmap Width: 340 px Height: 240 px

(The size of this graphic is reduced to fit into this document.)

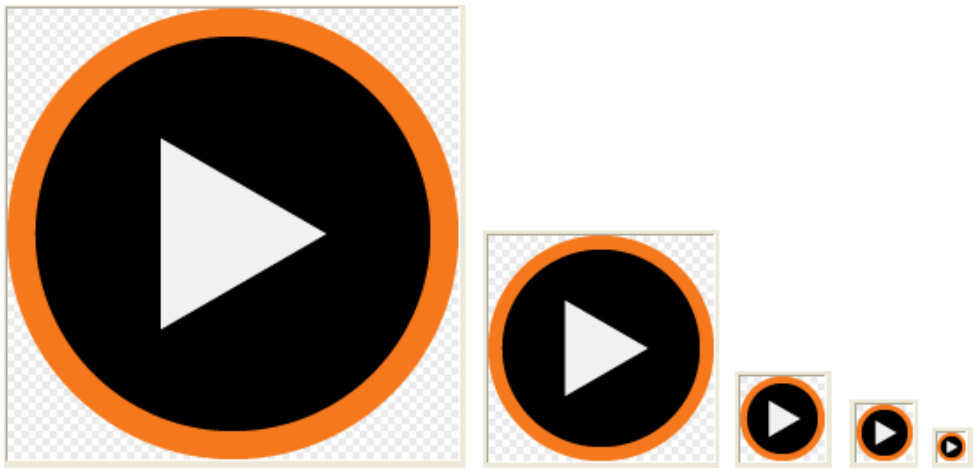
File name: restart.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	



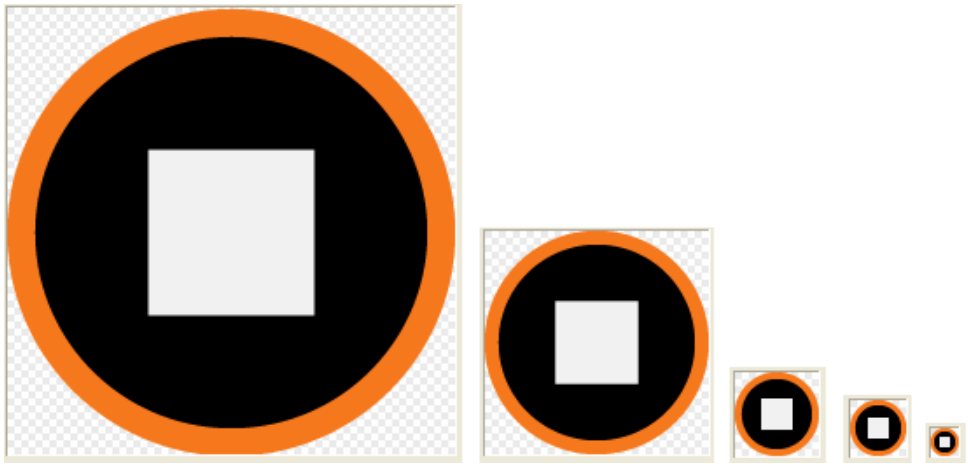
(The sizes of these logos are reduced to fit into this document.)

File name: small.bmp	

	Format: Bitmap Width: 55 px Height: 58 px

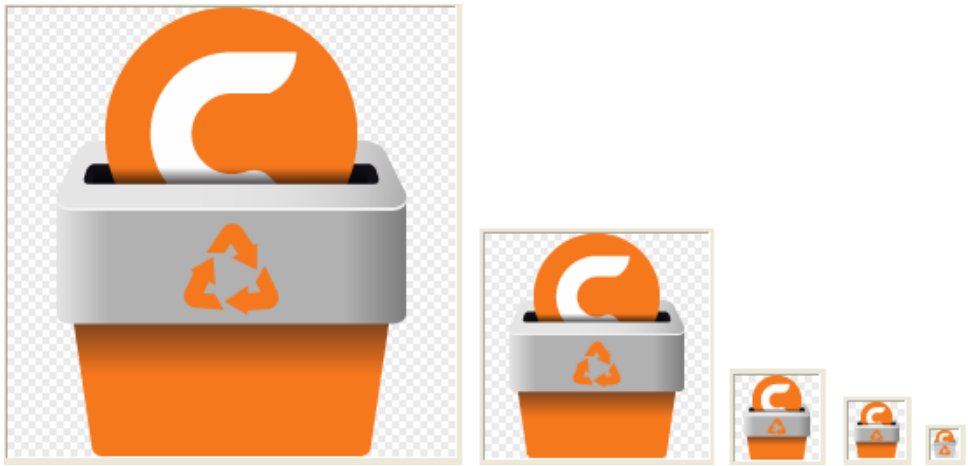
File name: start.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	
 (The sizes of these logos are reduced to fit into this document.)	

File name: stop.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	



(The sizes of these logos are reduced to fit into this document.)

File name: uninstall.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	



(The sizes of these logos are reduced to fit into this document.)

File name: webAdmin.ico This logo has transparent background (checkered squares).	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
  (The sizes of these logos are reduced to fit into this document.)	

Images for AhsayUBS (Installation graphics)

File name: favicon.ico This logo has transparent background (checkered squares).	Format: Website Icon Width: 16 px Height: 16 px or Width: 32 px Height: 32 px (True color plus alpha channel transparency)

File name: footer.png	Format: png Width: 127 px Height: 42 px

File name: header_bg.png	Format: png Width: 2400 px Height: 143 px

(The size of this graphic is reduced to fit into this document.)

File name: header_logo.png	Format: png Width: 524 px Height: 143 px
This logo has transparent background (checkered squares) with white text.	

(The size of this graphic is reduced to fit into this document.)

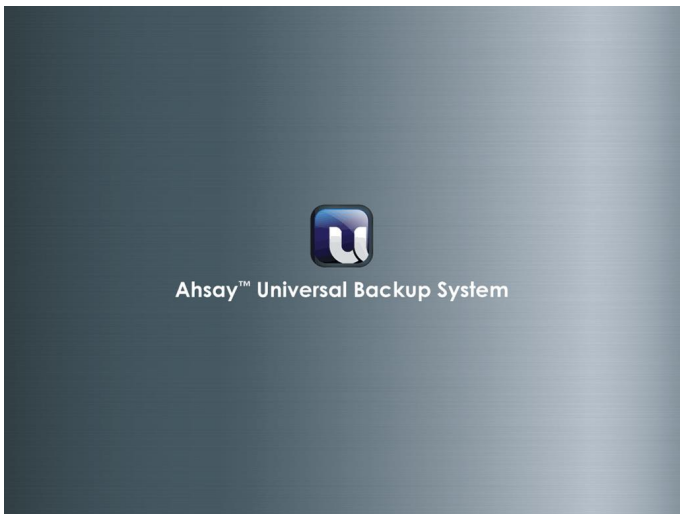
File name: login_bg.png	Format: png Width: 471 px Height: 340 px

(The size of this graphic is reduced to fit into this document.)

File name: login_logo.png	Format: png Width: 353 px Height: 140 px
This logo has transparent background (checkered squares) with white text.	

File name: splash_320x200.bmp	Format: Bitmap Width: 320 px Height: 200 px

File name: splash_1024x768.bmp	Format: Bitmap Width: 1024 px Height: 768 px



(The size of this graphic is reduced to fit into this document.)

Image specifications for AhsayOBM (Application graphics)

Images for all platforms

File name: about_logo.png	Format: png Width: 144 px Height: 33 px
This logo has transparent background (checkered squares).	

File name: login_bg.png	Format: png Width: 1016 px Height: 734 px
 (The size of this graphic is reduced to fit into this document.)	

File name: login_logo.png	Format: png Width: 200 px Height: 60 px
This logo has transparent background (checkered squares) with white text.	

File name: logo.png	Format: png Width: 32 px Height: 32 px
This logo has transparent background (checkered squares).	

File name: main_logo.png	Format: png Width: 148 px Height: 33 px
This logo has transparent background (checkered squares) with white text.	

File name: splash.png	Format: png Width: 420 px Height: 240 px
 (The size of this graphic is reduced to fit into this document.)	

File name: dstn_CBS_24.png	Format: png Width: 24 px Height: 24 px
This logo has transparent background (checkered squares) with white text.	

File name: dstn_CBS_32.png	Format: png Width: 32 px Height: 32 px
This logo has transparent background (checkered squares) with white text.	

File name: dstn_CBS_48.png	Format: png Width: 48 px Height: 48 px
This logo has transparent background (checkered squares) with white text.	

File name: fs16_root_CBS.png	Format: png Width: 16 px Height: 16 px
This logo has transparent background (checkered squares) with white text.	

Images for Linux, FreeBSD and Solaris (Application graphics)

File name: desktop.png This logo has transparent background (checkered squares).	Format: png Width: 128 px Height: 128 px

Images for Synology (Application graphics)

File name: logo_16.png This logo has transparent background (checkered squares).	Format: png Width: 16 px Height: 16 px

File name: logo_32.png This logo has transparent background (checkered squares).	Format: png Width: 32 px Height: 32 px

File name: logo_72.png This logo has transparent background (checkered squares).	Format: png Width: 72 px Height: 72 px

Images for QNAP (Application graphics)

File name: logo_72.png This logo has transparent background (checkered squares).	Format: png Width: 72 px Height: 72 px

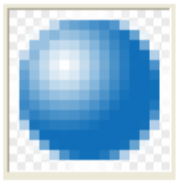
Images for Windows (System tray)

The following icons icon1.ico, icon2.ico, icon3.ico and icon4.ico will be used in the Windows system tray. Please arrange them in an animated sequence. The application will arrange the animation sequence when the backup job is run.

File name: icon1.ico This logo has transparent background (checkered squares).	Format: Windows Icon Width: 16 px Height: 16 px (True color plus alpha channel transparency)

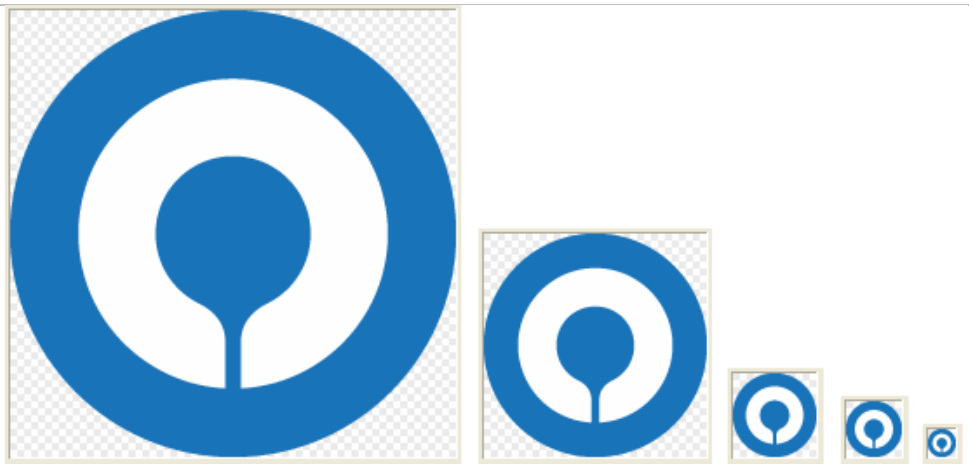
File name: icon2.ico	Format: Windows Icon Width: 16 px Height: 16 px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

File name: icon3.ico	Format: Windows Icon Width: 16 px Height: 16 px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

File name: icon4.ico This logo has transparent background (checkered squares).	Format: Windows Icon Width: 16 px Height: 16 px (True color plus alpha channel transparency)
Original  Image enlarged for easy reference	
File name: toast.ico This logo has transparent background (checkered squares).	Format: Windows Icon Width: 64 px Height: 64 px (True color plus alpha channel transparency)

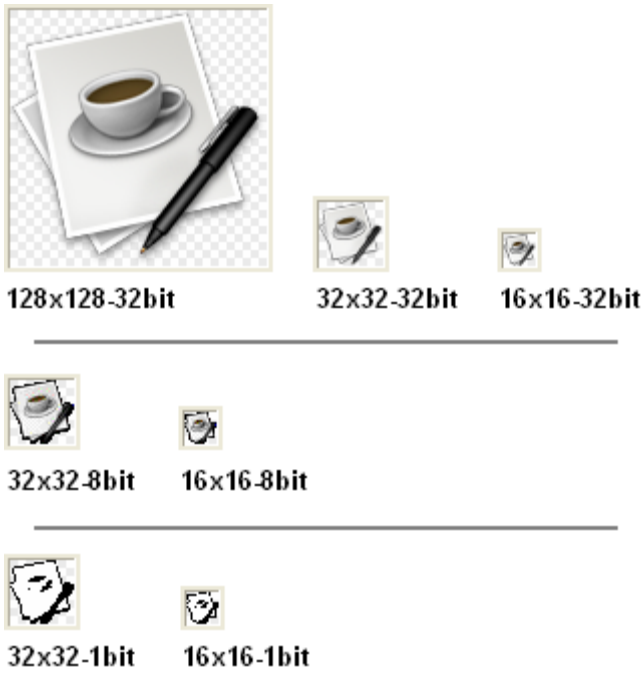
Images for Mac (Application and installation graphics)

File name: desktop.icns This logo has transparent background (checkered squares).	Format: Mac Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)

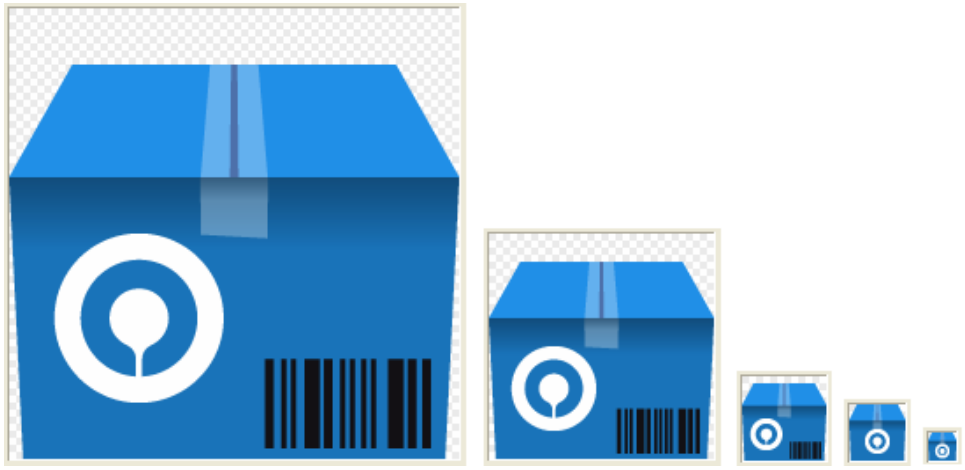


(The sizes of these logos are reduced to fit into this document.)

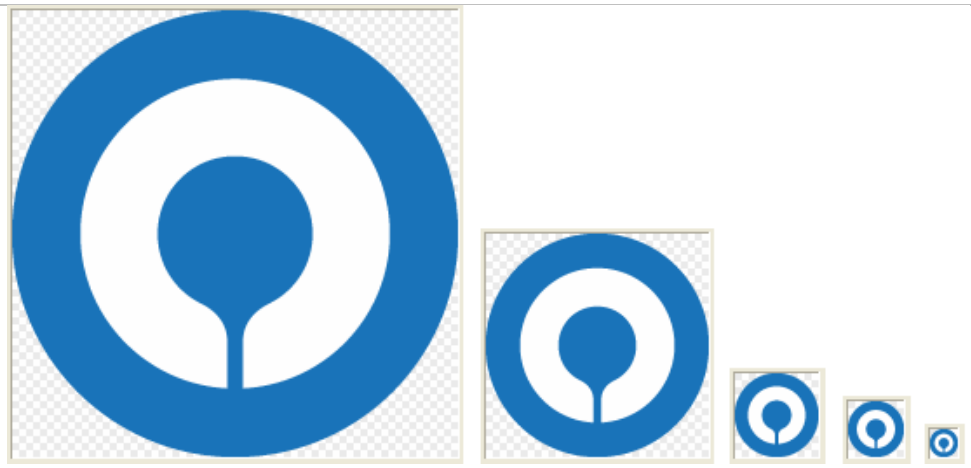
File name: GenericJavaApp.icns	Format: Mac Icon
This logo has transparent background (checkered squares).	



Note: These are default Java application icons, they will be displayed when there are icons missing. This is not directly related the product branding.

File name: installer.icns This logo has transparent background (checkered squares).	Format: Mac Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
 (The sizes of these logos are reduced to fit into this document.)	

File name: Logo.icns This logo has transparent background (checkered squares).	Format: Mac Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)



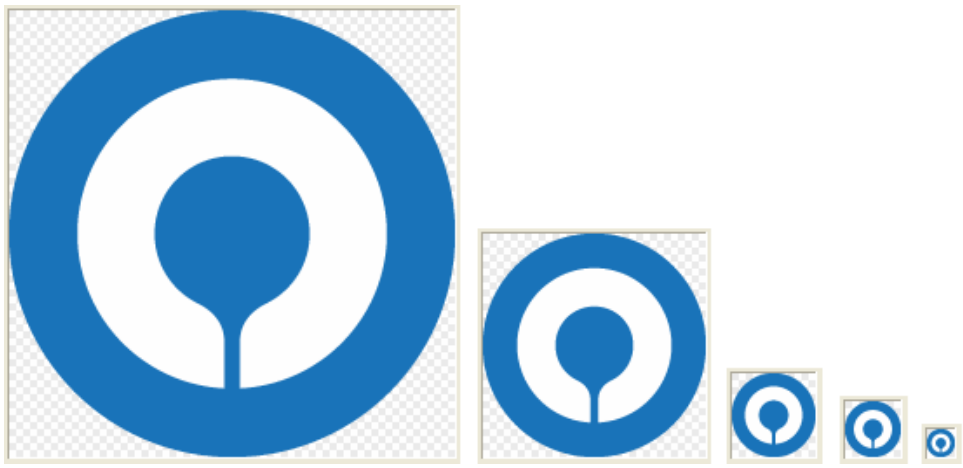
(The sizes of these logos are reduced to fit into this document.)

File name: uninstall.icns	Format: Mac Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

(The sizes of these logos are reduced to fit into this document.)

File name: OBMLogo.icns	

This logo has transparent background (checkered squares).	Format: Mac Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)



(The sizes of these logos are reduced to fit into this document.)

File name: background.jpg	Format: JPEG Width: 622 px Height: 420 px

(The size of this graphic is reduced to fit into this document.)

File name: logo.png	Format: png Width: 128 px Height: 128 px
 (The size of this graphic is reduced to fit into this document.)	

Images for Synology (Installation graphics)

File name: PACKAGE_ICON.PNG This logo has transparent background (checkered squares).	Format: png Width: 72 px Height: 72 px

File name: PACKAGE_ICON_120.PNG This logo has transparent background (checkered squares).	Format: png Width: 120 px Height: 120 px
File name: PACKAGE_ICON_256.PNG This logo has transparent background (checkered squares).	Format: png Width: 256 px Height: 256 px

Images for Synology (Installation graphics)

File name: PACKAGE_ICON_64.GIF	Format: png Width: 64 px Height: 64 px

File name: PACKAGE_ICON_64_GRAY.GIF	Format: png Width: 64 px Height: 64 px

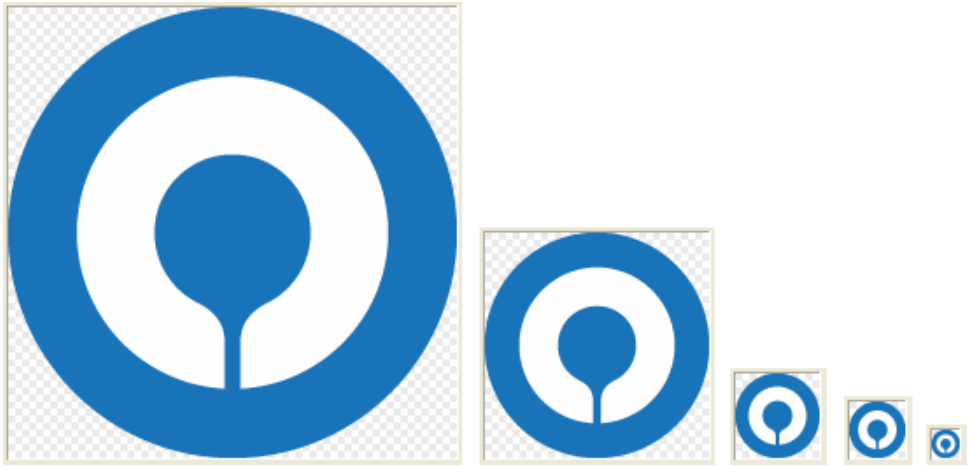
File name: PACKAGE_ICON_80.GIF	Format: png Width: 80 px Height: 80 px

Images for Windows (Installation graphics)

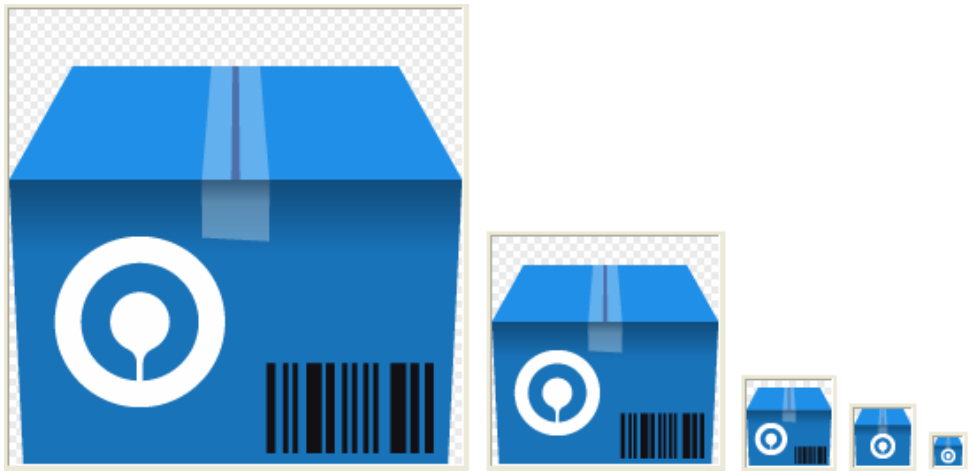
File name: aboutBG.bmp	Format: Bitmap Width: 164 px Height: 337 px

(The size of this graphic is reduced to fit into this document.)

File name: desktop.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	



File name: installer.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	



(The sizes of these logos are reduced to fit into this document.)

File name: small.bmp	Format: Bitmap Width: 55 px Height: 58 px

File name: uninstall.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

(The sizes of these logos are reduced to fit into this document.)

Image specifications for AhsayACB (Application graphics)

Images for all platforms

File name: about_logo.png This logo has transparent background (checkered squares).	Format: png Width: 144 px Height: 33 px

File name: login_bg.png	Format: png Width: 1016 px Height: 734 px
 (The size of this logo is reduced to fit into this document.)	

File name: login_logo.png This logo has transparent background (checkered squares) with white text.	Format: png Width: 200 px Height: 60 px

File name: logo.png	Format: png Width: 32 px Height: 32 px
This logo has transparent background (checkered squares).	

File name: main_logo.png	Format: png Width: 148 px Height: 33 px
This logo has transparent background (checkered squares) with white text.	

File name: splash.png	Format: png Width: 420 px Height: 240 px

(The size of this graphic is reduced to fit into this document.)

File name: dstn_CBS_24.png	Format: png Width: 24 px Height: 24 px
This logo has transparent background (checkered squares) with white text.	

File name: dstn_CBS_32.png	Format: png Width: 32 px Height: 32 px
This logo has transparent background (checkered squares) with white text.	

File name: dstn_CBS_48.png	Format: png Width: 48 px Height: 48 px
This logo has transparent background (checkered squares) with white text.	

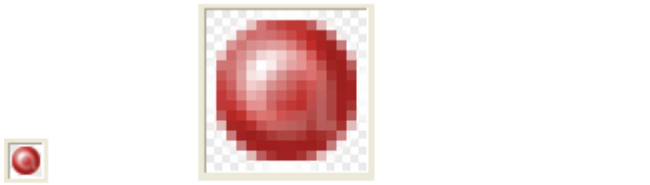
File name: fs16_root_CBS.png	Format: png Width: 16 px Height: 16 px
This logo has transparent background (checkered squares) with white text.	

Images for Windows (System tray)

The following icons icon1.ico, icon2.ico, icon3.ico and icon4.ico will be used in the Windows system tray. Please arrange them in an animated sequence. The application will arrange the animation sequence when the backup job is run.

File name: icon1.ico	Format: Windows Icon Width: 16 px Height: 16 px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	
Original Image enlarged for easy reference	

File name: icon2.ico	Format: Windows Icon Width: 16 px Height: 16 px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	
Original Image enlarged for easy reference	

File name: icon3.ico	Format: Windows Icon Width: 16 px Height: 16 px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	
 Original Image enlarged for easy reference	

File name: icon4.ico	Format: Windows Icon Width: 16 px Height: 16 px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	
 Original Image enlarged for easy reference	

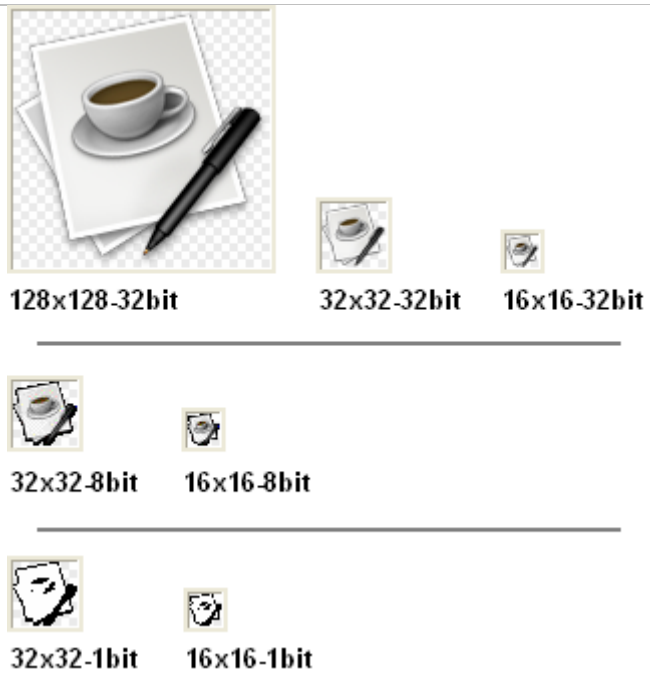
File name: toast.ico	Format: Windows Icon Width: 64 px Height: 64 px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

Images for Mac (Application and installation graphics)

File name: desktop.icns	Format: Mac Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

(The sizes of these logos are reduced to fit into this document.)

File name: GenericJavaApp.icns	Format: Mac Icon
This logo has transparent background (checkered squares).	



Note: These are default Java application icons, they will be displayed when there are icons missing. This is not directly related the product branding.

File name: installer.icns	Format: Mac Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

(The sizes of these logos are reduced to fit into this document.)

File name: Logo.icns	Format: Mac Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

(The sizes of these logos are reduced to fit into this document.)

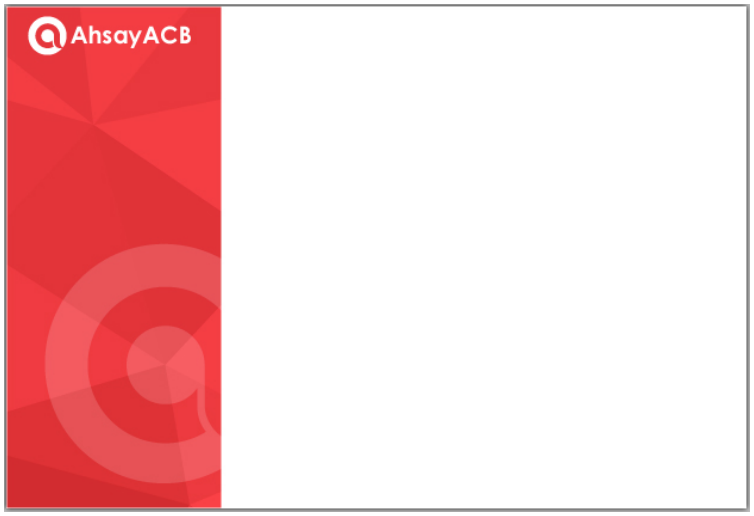
File name: uninstall.icns	Format: Mac Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

(The sizes of these logos are reduced to fit into this document.)

File name: ACBLogo.icns	Format: Mac Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

(The sizes of these logos are reduced to fit into this document.)

File name: background.jpg	Format: JPEG Width: 622 px Height: 420 px



(The size of this graphic is reduced to fit into this document.)

File name: logo.png	Format: png Width: 128 px Height: 128 px

(The size of this graphic is reduced to fit into this document.)

Images for Windows (Installation graphics)

File name: aboutBG.bmp	Format: Bitmap Width: 164 px Height: 337 px

(The size of this graphic is reduced to fit into this document.)

File name: desktop.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

(The sizes of these logos are reduced to fit into this document.)

File name: installer.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

(The sizes of these logos are reduced to fit into this document.)

File name: small.bmp	Format: Bitmap Width: 55 px Height: 58 px

File name: uninstall.ico	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
This logo has transparent background (checkered squares).	

(The sizes of these logos are reduced to fit into this document.)

Image specifications for AhsayOBC (Installation graphics)

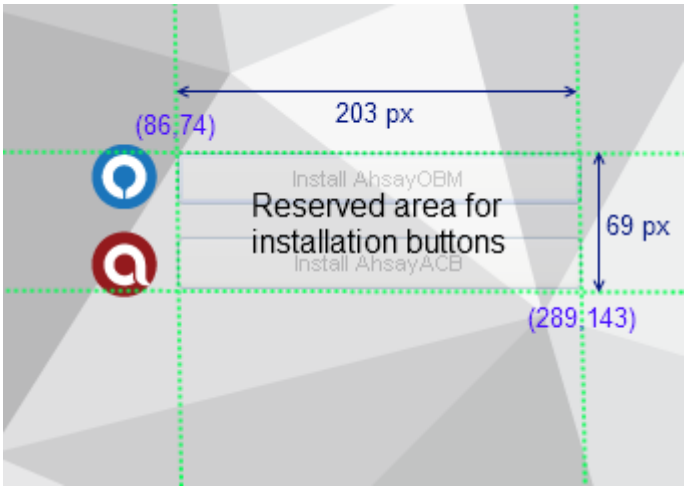
Images for Windows

File name: acb-splash.bmp	Format: Bitmap Width: 340 px Height: 240 px

File name: installer.ico This logo has transparent background (checkered squares).	Format: Windows Icon Width: 256,128,48,32,16px Height: 256,128,48,32,16px (True color plus alpha channel transparency)
 (The sizes of these logos are reduced to fit into this document.)	

File name: obc-background.bmp	Format: Bitmap Width: 340 px Height: 240 px

The central area inside the green dotted lines is reserved for the OBM/ACB installation buttons.



File name: obc-splash.bmp	Format: Bitmap Width: 340 px Height: 240 px

File name: obm-splash.bmp	Format: Bitmap Width: 340 px Height: 240 px

Appendix G Comparison on Different Replication Setup Environments

Here is a comparison table of the setup concerns on different replication environment.

	Ahsay CBS (Physical machine/Cloud)	**Ahsay CBS** (Existing VM)	**Cloud** (Storage)	**FTP/ SFTP**	**Ahsay CBS** (Physical machine/Cloud)	**Ahsay CBS** (Existing VM)	**Local FTP/ SFTP**	**Mapped Drive**	**Local/ Removable Drive**
Type of connection	Internet				LAN				N/A
	This is the type of connection with the Backup Server, for Internet connection, you may aware on the download speed which may affect the restore performance. N/A refers to a direct connection with the Backup Server and the replication storage is not located on the same disk of the user home.								
Cost	High	Medium	Medium*	Low	High	Medium	Low	Low	Low
	The cost is measured in terms of setup, hosting, storage media type and maintenance. * The cost would be affected if the cloud storage is charged base on bandwidth or amount of access.								
Replication Speed	Medium	Medium	Medium	Medium	Fast	Fast	Fast	Fast	Fast
	The replication speed over the Internet would mainly depend on the upload bandwidth. The replication speed is similar as file copying between 2 devices and the number of backup set to replicate. If fast replication is required, you can consider using the multiple threads replication (v7.7 onwards)								
Recovery Speed	Fast	Fast	Slow	Slow	Fast	Fast	Fast	Fast	Fast
	This is measured in terms of the Backup Server downtime. The bottleneck is mainly on the Internet bandwidth.								
Switch to Backup Server	Yes	Yes	No	No	Yes	Yes	No	No	No
Time to switch over by DNS	Slow **	Slow **	N/A	N/A	Fast	Fast	N/A	N/A	N/A
	** The speed would depend on the DNS propagation time. N/A refers to the device has no such capability and not applicable for the DNS switch over.								
Time to switch over by IP address	Fast	Fast	N/A	N/A	Fast	Fast	N/A	N/A	N/A
	Switch the IP address of the Replication Server to the IP address of the Backup Server, provided that the Backup Server is down and the IP address will not be used on the Backup Server again. N/A refers to the device has no such capability and not applicable for the IP switch over.								
Offsite replication	Yes	Yes	Yes	Yes	No	No	No	No	No
Replication snapshot	By Ahsay CBS	By Ahsay CBS	Depends ***	No	By Ahsay CBS	By Ahsay CBS	No	No	No
	*** Depends on the cloud service provider/setup.								

Appendix H System Job

Here is a summary of the system jobs on the AhsayCBS. For the daily job, it is scheduled at 06:00, while others will be performed hourly and quarter-hourly.

Quarter-hourly Job

Job Name	Description	Email
Low Disk Space Alert	When the disk space of the user home or system home is over 80%, email will be sent to administrator. Once the alert email is sent, email will not be sent within the next hour.	✔
Inactive Backup Set Report	Email users when backup set has not been run for a number of days. (The number of days can be set in policy group.)	✔
Settings Change Report	When user's profile or backup set settings is changed, Email will be sent to user.	✔
Restore Job Report	Send restore job report to user.	✔
Backup Job Report	Send backup job report to user.	✔
Remove Deleted Backup Set	This job scans removed backup sets from the storage.	✘

Hourly Job

Job Name	Description	Email
Missed Backup Report	Email will be sent if scheduled backup job has not been started after 6 hours.	✔
Remove Migrated v6 Data	(Version 7.7 or later) When v6 backup data has completely migrated to v7 format, this job will remove the old v6 backup data.	✘
License Check	License validation check.	✘

Daily Job

Job Name	Description	Email
Backup Quota Reminder Report	It will send report to user when the backup quota is over 80% or backup quota is full.	✔
Trial User Reminder Job	It will send report to trial users when trial users are going to expire or to those expired trial users.	✔
Low Destination Space Reminder	It will send disk space reminder email to administrator. It monitors the local and cloud storages such as Amazon Cloud Drive, Google Drive, OneDrive and OneDrive for Business.	✔

Configuration Archival	Perform AhsayCBS system configuration, user profile, and runtime settings to our cloud.	✘
Remove Trial User	Expired trial users will be removed by this job.	✘
Logs Removal	This job removes expired log entries such as backup error, backup job, CDP backup job, replication log, advertisement log and system logs etc.	✘
Meter license usage	Upload meter license usage to our cloud.	✘

Appendix I Daily User Report

If the user group your account belongs to has the Daily User Report selected in the Policy Group setting, you will receive a daily user report generated by the CBS system.

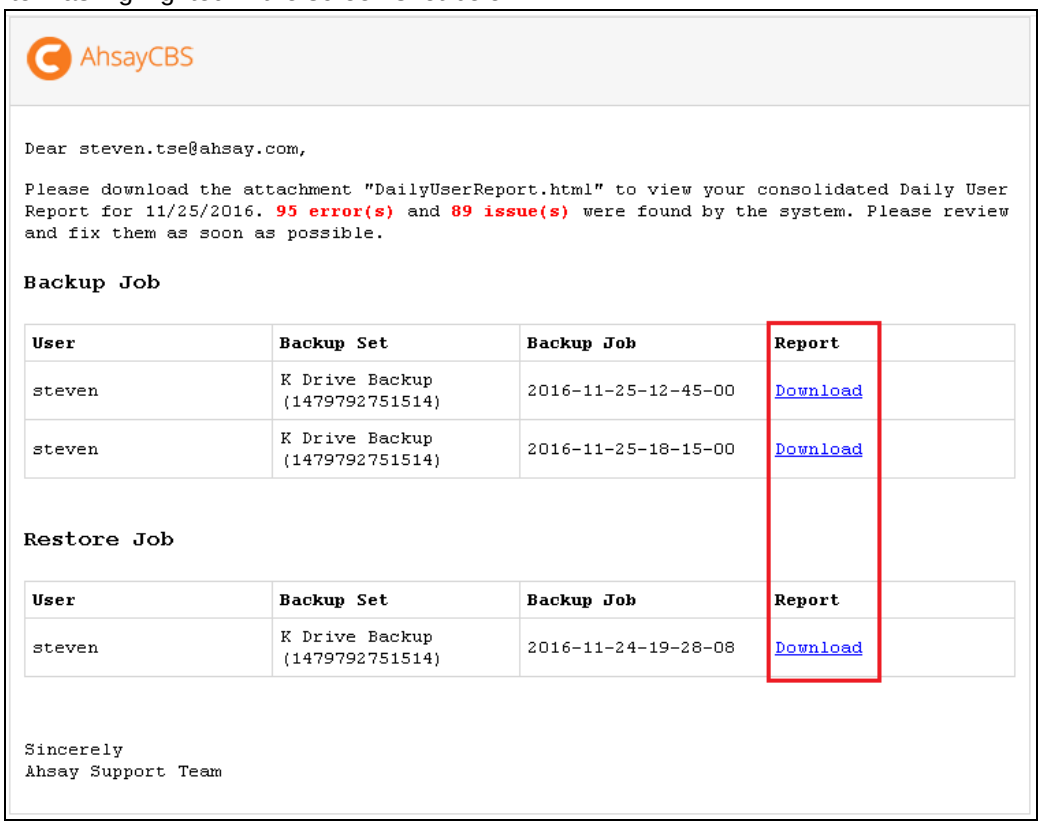
The daily user report is an interactive report to provide you with detailed information activities, statistics, problems or issues that your account is associated with.

There are two major types of reports you can find from the email, the **Backup/Restore Report** and the **Daily User Report**.

To access the Backup/Restore report

- **Download individual Backup or Restore report**

1. The content in the email shows a list of Backup and Restore jobs performed associated with your user. Simply click on the **Download** link in the individual backup or restore job item as highlighted in the screen shot below.



AhsayCBS

Dear steven.tse@ahsay.com,

Please download the attachment "DailyUserReport.html" to view your consolidated Daily User Report for 11/25/2016. **95 error(s)** and **89 issue(s)** were found by the system. Please review and fix them as soon as possible.

Backup Job

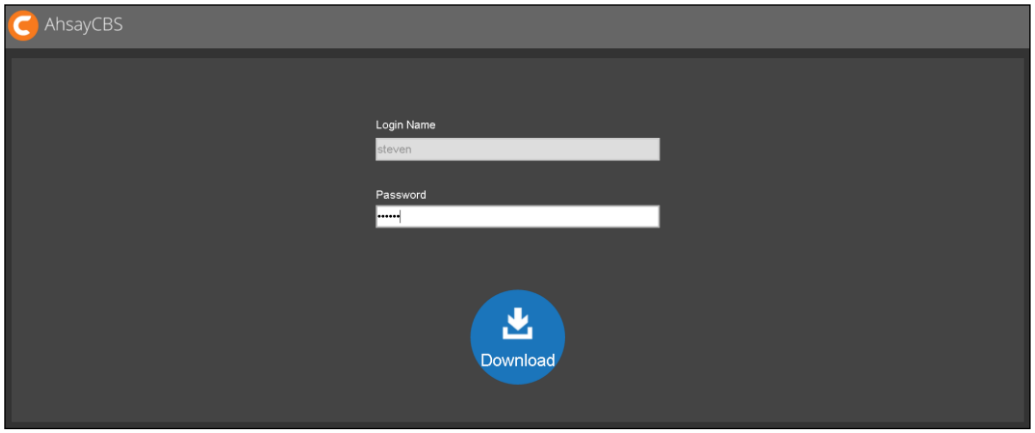
User	Backup Set	Backup Job	Report
steven	K Drive Backup (1479792751514)	2016-11-25-12-45-00	Download
steven	K Drive Backup (1479792751514)	2016-11-25-18-15-00	Download

Restore Job

User	Backup Set	Backup Job	Report
steven	K Drive Backup (1479792751514)	2016-11-24-19-28-08	Download

Sincerely
Ahsay Support Team

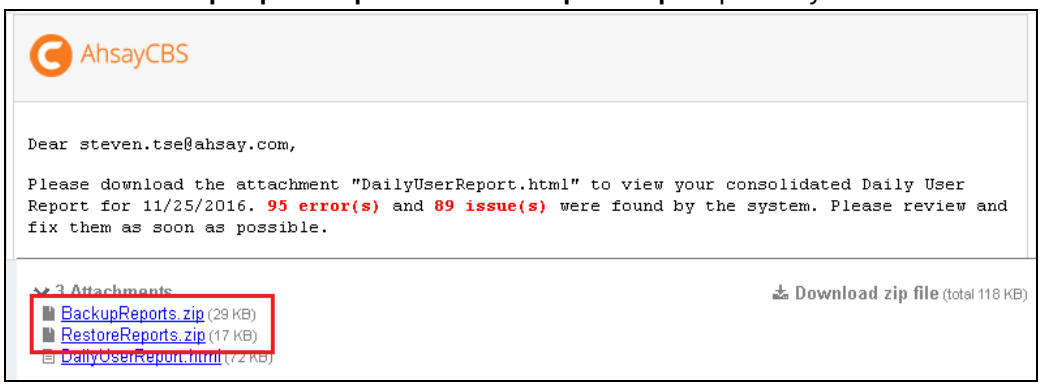
2. You will be prompted to enter the password of your backup user account as shown below. Click on the **Download** button after entering the password.



3. The Backup or Restore report in .zip format will be download.

➢ **Download Backup and Restore reports at once**

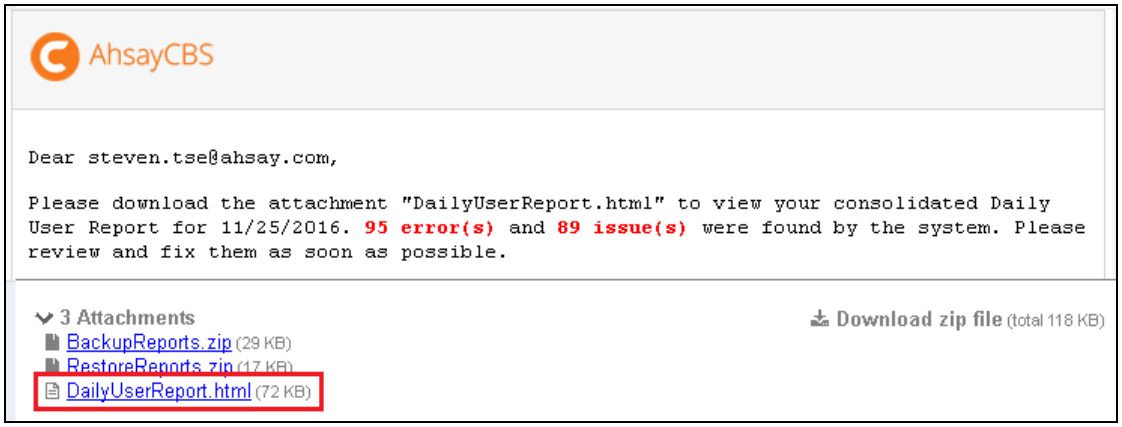
1. All backup reports and restore reports are grouped separate **.zip** attachments and are named as **BackupReports.zip** and **RestoreReports.zip** respectively.



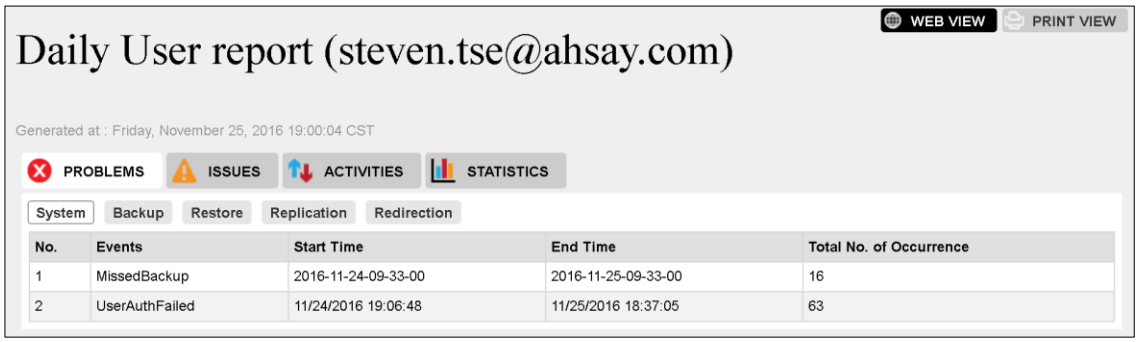
2. Unzip the downloaded file and you will find all the backup or restore reports.

To access the Consolidated Report

1. Click on the attachment **DailyUserReport.html** from the email to download the file.

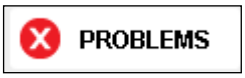


2. Launch the file with your Internet browser and you will see a screen similar to this.



About the Daily User Report

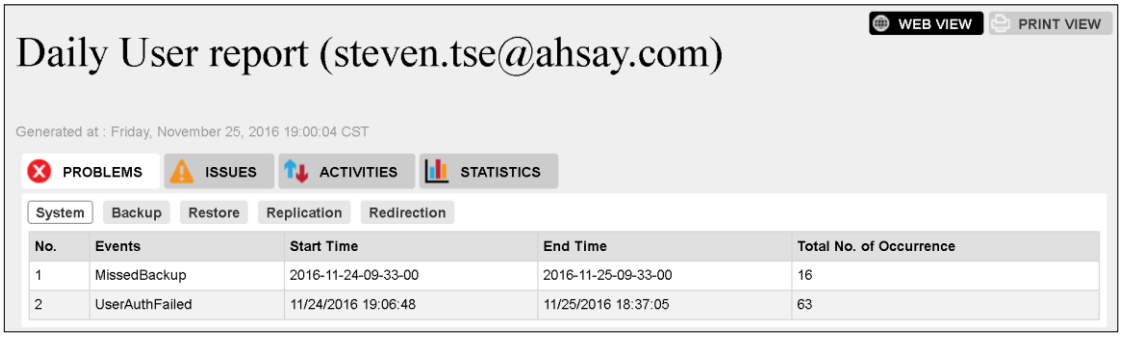
The daily user report has 4 major sections which are **PROBLEMS**, **ISSUES**, **ACTIVITIES** and **STATISTICS**.



All unsuccessful activities including system jobs, backup jobs, restore, replication and redirection are recorded under the PROBLEMS section. There are 5 tabs under this category.

- **System**

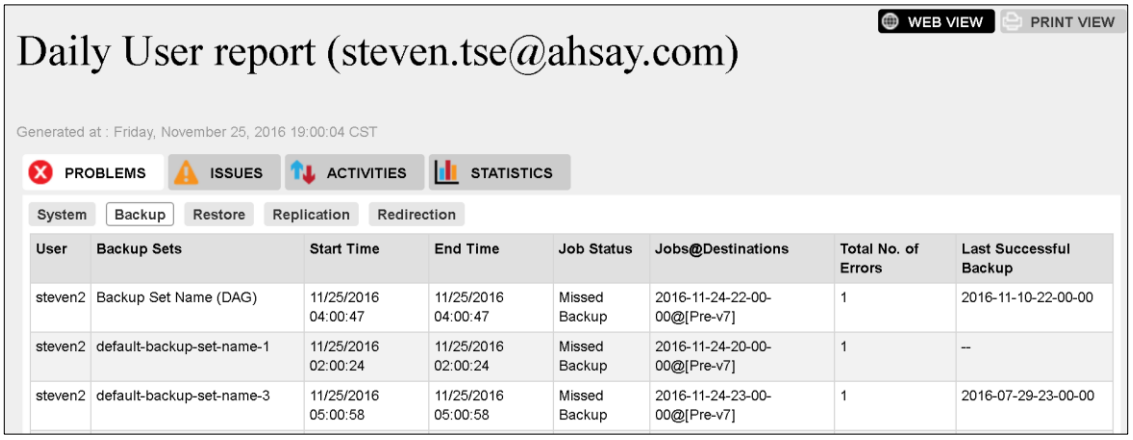
  This page shows the consolidated data for system job errors with the following details. All same type of system job error will be grouped as one entry.



No.	Sequential number of report item
Events	Type of system job error
Start Time	Start time of the first occurrence of the particular type of system job error
End Time	End time of the last occurrence of the particular type of system job error
Total No. of Occurrence	Number of occurrence of the particular type of system job error

➢ Backup

This page shows all the unsuccessful backup jobs with the following details.



User	Name of the backup user
Backup Sets	Name of the failed backup set
Start Time	Start time of the failed backup job (in backup server's time zone)
End Time	End time of the failed backup job (in backup server's time zone)
Job Status	Status of the failed backup job, e.g. Missed Backup
Job@Destinations	Backup time in client time zone
Total No. of Errors	Total number of backup error for the particular backup set
Last Successful Backup	Time of the last successful backup job for the particular backup set

➢ Restore

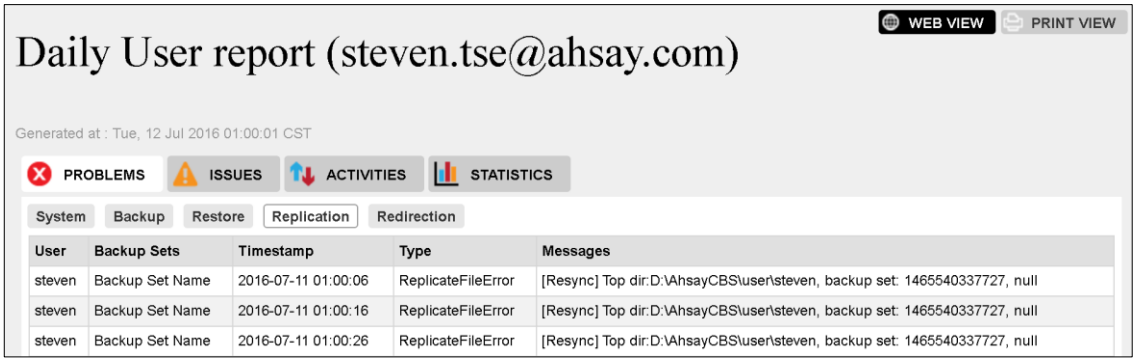
This page shows all the unsuccessful restore jobs with the following details.

User	Name of the backup user
Backup Sets	Name of the failed backup set
Start Time	Start time of the failed restore job (in backup server's time zone)

End Time	End time of the failed restore job (in backup server's time zone)
Job Status	Status of the failed restore job, e.g. User interrupted
Job@Destinations	Restore time in client backup agent's time zone
Total No. of Errors	Total number of restore error for the particular backup set

- **Replication**

This page shows all the unsuccessful replication jobs with the following details.



User	Name of the backup user
Backup Sets	Name of the backup set failed for replication
Timestamp	Recorded time of the replication error
Type	Type of the replication error
Messages	Error message showing details of the replication error

- **Redirection**

This page shows all the unsuccessful redirection jobs with the following details.

Timestamp	Recorded time of the redirection error
Events	Type of the redirection error
Users	Name of user failed for the redirection job
Total No. of Errors	Total number of redirection error for the particular user

ISSUES

This section shows issues in regard to system jobs, backup user account and backup sets that backup user should be aware of. There are 3 tabs under this category.

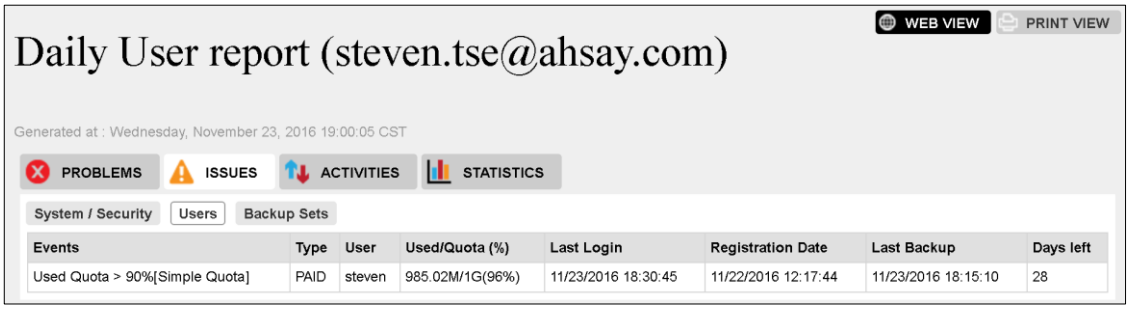
➢ System / Security

This page shows the consolidated data for system or security issues with the following details.

Event	Type of system / security issues
Users	Name of the backup user for the particular type of system/security issue
Start Time	Start time of the first occurrence of the particular type of system/security issue
End Time	End time of the last occurrence of the particular type of system/security issue
No. of Occurrence	Number of occurrence of the particular type of system/security of a backup user
Remote IP Address	IP address where Client Agent Application is installed
User Agent	Type of the Client Agent Application (AhsayOBM/AhsayACB)

➢ Users

This page shows a list of backup users whose account's storage quota is 90% or above full.

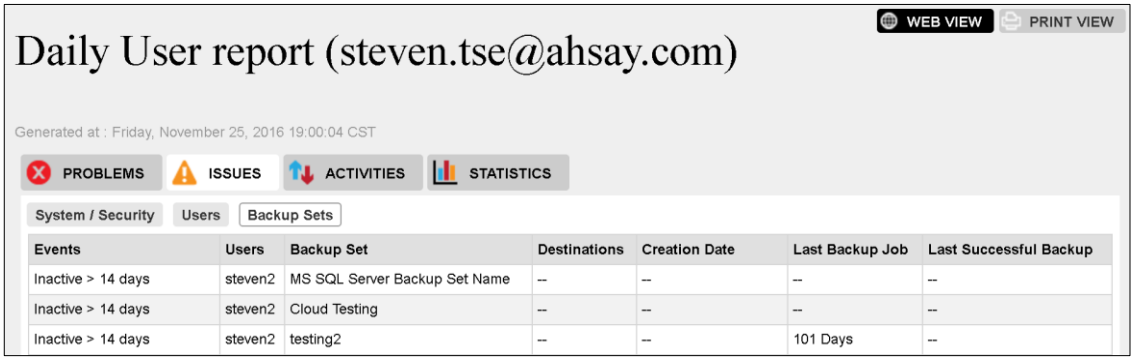


Event	Type of the issue
Type	User's subscription status, whether it is a paid or trial user
User	Name of the backup user

Used/Quota (%)	Storage used / Storage Quota (Utilization rate)
Last Login	Last login time of user
Registration Date	Backup account's registration date and time
Last Backup	Date and time of the last backup job performed
Days Left	➢ **Trial account** – number of days left before the trial account expires ➢ **Paid account** – number of days left before the account suspension date set by the system administrator

➢ **Backup Sets**

This page shows a list of missed scheduled backup and backup sets that have not been backed up for 14 days or more.



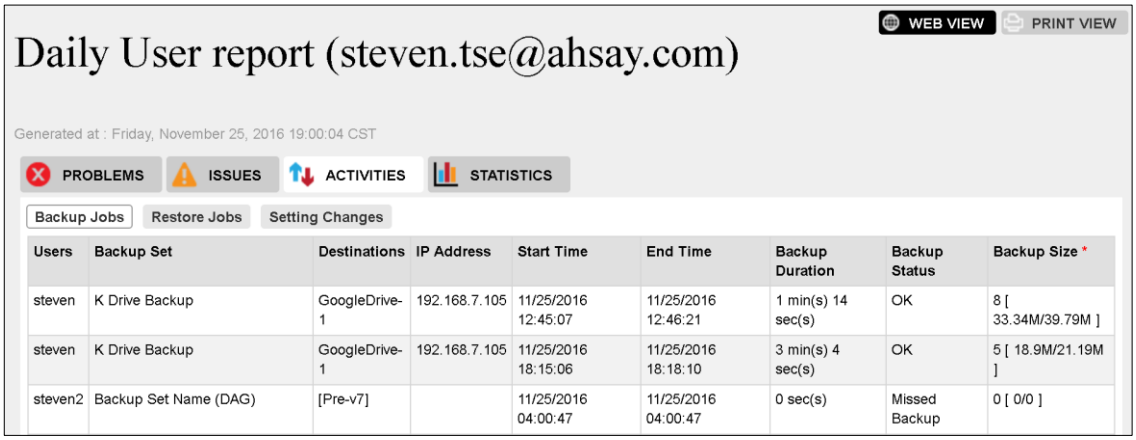
Events	Type of the issue
Users	Name of the backup user
Backup Set	Name of the backup set
Destination	Location of the backup destination
Creation Date	Date and time when the backup set was created
Last Backup Job	Number of day when a backup job was last performed
Last Successful Backup	Time of the last successful backup job for the particular backup set

ACTIVITIES

This section shows activities of all backup and restore jobs, both successful and unsuccessful ones, as well as all setting changes made. There are 3 tabs under this category.

➢ Backup Jobs

This page shows a list of all backup jobs activities.



Daily User report (steven.tse@ahsay.com)

WEB VIEW PRINT VIEW

Generated at : Friday, November 25, 2016 19:00:04 CST

PROBLEMS ISSUES ACTIVITIES STATISTICS

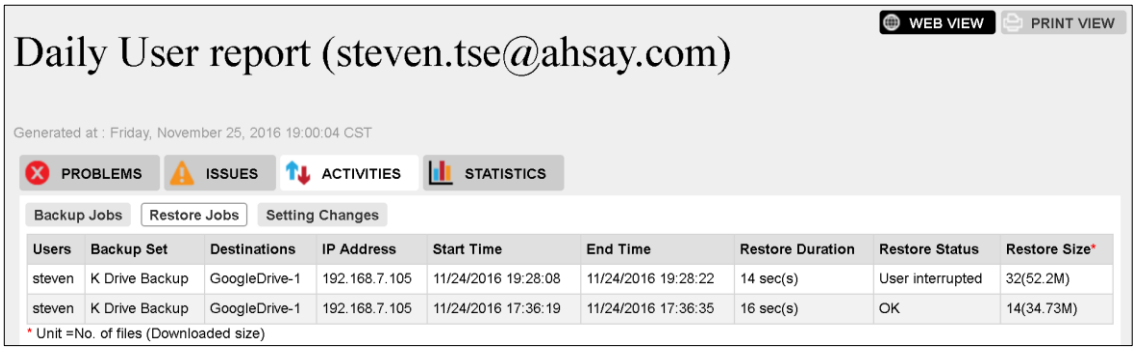
Backup Jobs Restore Jobs Setting Changes

Users	Backup Set	Destinations	IP Address	Start Time	End Time	Backup Duration	Backup Status	Backup Size *
steven	K Drive Backup	GoogleDrive-1	192.168.7.105	11/25/2016 12:45:07	11/25/2016 12:46:21	1 min(s) 14 sec(s)	OK	8 [33.34M/39.79M]
steven	K Drive Backup	GoogleDrive-1	192.168.7.105	11/25/2016 18:15:06	11/25/2016 18:18:10	3 min(s) 4 sec(s)	OK	5 [18.9M/21.19M]
steven2	Backup Set Name (DAG)	[Pre-v7]		11/25/2016 04:00:47	11/25/2016 04:00:47	0 sec(s)	Missed Backup	0 [0/0]

Users	Name of the backup user
Backup Set	Name of the backup set
Destinations	Location of the backup destination
IP Address	IP address where User Agent Application is installed
Backup Duration	Start time / End time of the backup and duration of the backup
Backup Status	Status of the backup job
Backup Size	No. of files [Compressed size / Uncompressed size]

➢ Restore Jobs

This page shows a list of all restore jobs activities.



Daily User report (steven.tse@ahsay.com)

WEB VIEW PRINT VIEW

Generated at : Friday, November 25, 2016 19:00:04 CST

PROBLEMS ISSUES ACTIVITIES STATISTICS

Backup Jobs Restore Jobs Setting Changes

Users	Backup Set	Destinations	IP Address	Start Time	End Time	Restore Duration	Restore Status	Restore Size*
steven	K Drive Backup	GoogleDrive-1	192.168.7.105	11/24/2016 19:28:08	11/24/2016 19:28:22	14 sec(s)	User interrupted	32(52.2M)
steven	K Drive Backup	GoogleDrive-1	192.168.7.105	11/24/2016 17:36:19	11/24/2016 17:36:35	16 sec(s)	OK	14(34.73M)

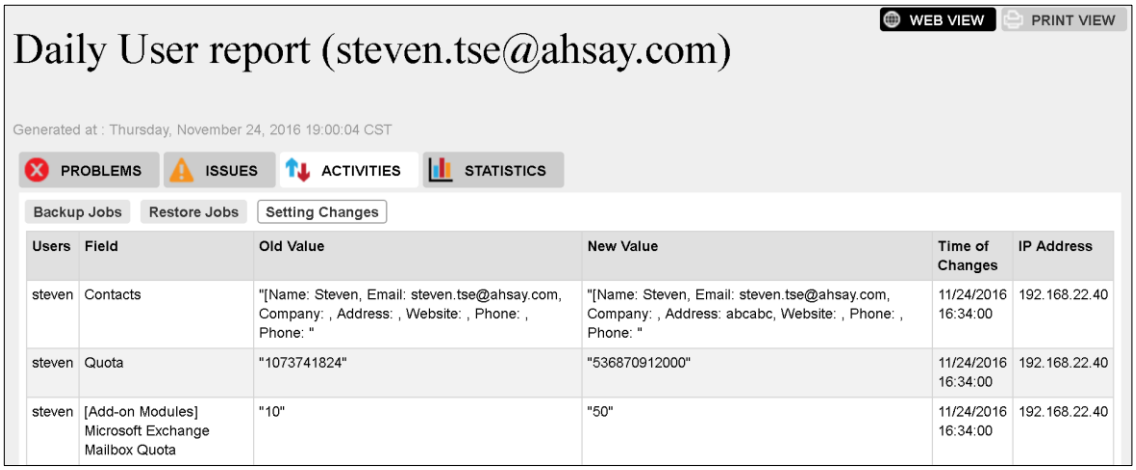
* Unit =No. of files (Downloaded size)

Users	Name of the backup user
Backup Set	Name of the backup set

Destinations	Location of the restore destination
IP Address	IP address where User Agent Application is installed
Start Time	Start time of the restore job
End Time	End time of the restore job
Restore Duration	Duration of the restore job
Restore Status	Status of the restore job
Restore Size	Number of files restored (Downloaded size)

➢ Setting Changes

This page shows a list of the settings changed by backup users.



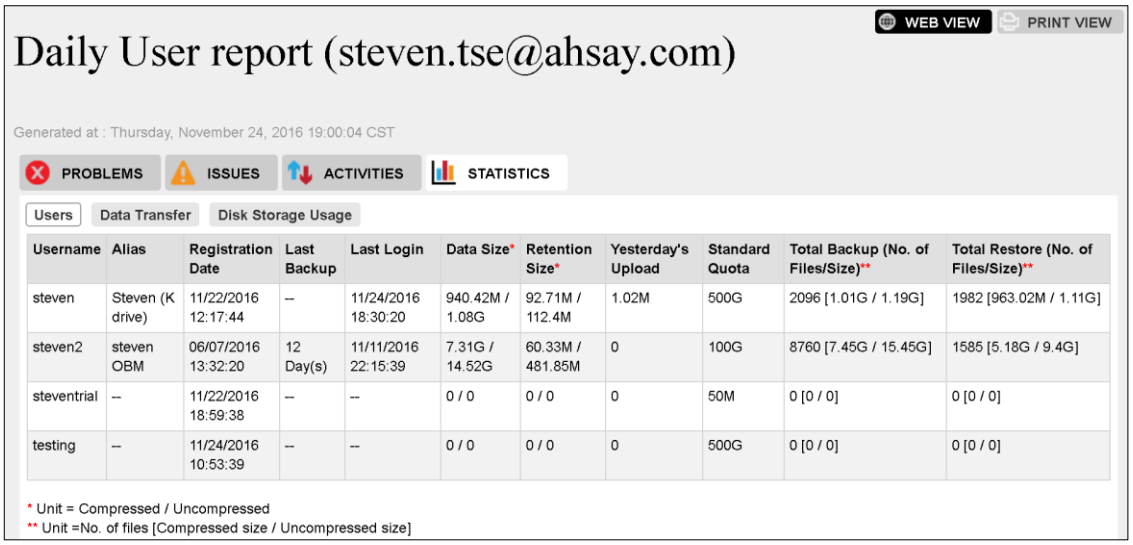
Users	Name of the backup user
Field	The field that has been changed
Old Value	Old Value before the change
New Value	New Value after the change
Time of Changes	Time of the changes made
IP Address	IP Address of the machine which initiated the changes

STATISTICS

This section shows statistics data of backup users, data transfer and disk storage usage.

➢ Users

This page shows a list of statistics data regarding the backup user account.



Daily User report (steven.tse@ahsay.com)

WEB VIEW | PRINT VIEW

Generated at : Thursday, November 24, 2016 19:00:04 CST

PROBLEMS | ISSUES | ACTIVITIES | STATISTICS

Users | Data Transfer | Disk Storage Usage

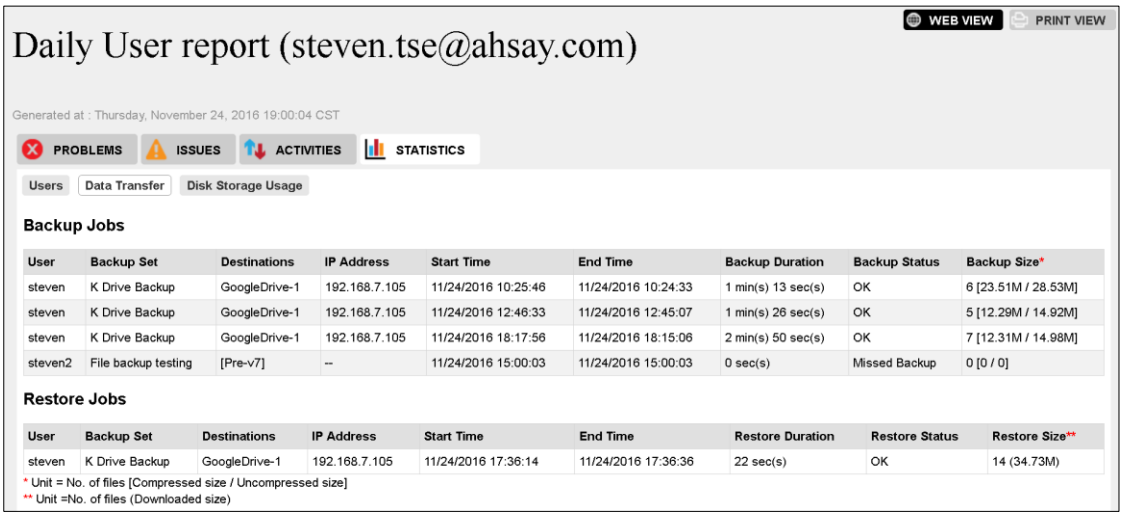
Username	Alias	Registration Date	Last Backup	Last Login	Data Size*	Retention Size*	Yesterday's Upload	Standard Quota	Total Backup (No. of Files/Size)**	Total Restore (No. of Files/Size)**
steven	Steven (K drive)	11/22/2016 12:17:44	--	11/24/2016 18:30:20	940.42M / 1.08G	92.71M / 112.4M	1.02M	500G	2096 [1.01G / 1.19G]	1982 [963.02M / 1.11G]
steven2	steven OBM	06/07/2016 13:32:20	12 Day(s)	11/11/2016 22:15:39	7.31G / 14.52G	60.33M / 481.85M	0	100G	8760 [7.45G / 15.45G]	1585 [5.18G / 9.4G]
steventrial	--	11/22/2016 18:59:38	--	--	0 / 0	0 / 0	0	50M	0 [0 / 0]	0 [0 / 0]
testing	--	11/24/2016 10:53:39	--	--	0 / 0	0 / 0	0	500G	0 [0 / 0]	0 [0 / 0]

* Unit = Compressed / Uncompressed
** Unit =No. of files [Compressed size / Uncompressed size]

Users	Name of the backup user
Alias	Another name of the backup user
Registration Date	Date and time when the backup account was registered
Last Backup	Number of day when a backup job was last performed with the particular user account
Last Login	Date and time when user logged in to the particular account
Data Size	Total size of backup data (Compressed size/Uncompressed size)
Retention Size	Total size of data in retention area (Compressed size/Uncompressed size)
Yesterday's Upload	Total size of backup uploaded by the particular backup user yesterday
Standard Quota	Storage quota set for the particular backup user
Total Backup (No. of Files/Size)	Total backup performed by this user [No. of files [Compressed size / Uncompressed size]
Total Restore (No. of Files/Size)	Total restore performed by this user [No. of files [Compressed size / Uncompressed size]

➢ Data Transfer

This page shows a list of statistics data regarding data transfer for backup jobs and restore jobs.



Daily User report (steven.tse@ahsay.com)

WEB VIEW PRINT VIEW

Generated at : Thursday, November 24, 2016 19:00:04 CST

PROBLEMS ISSUES ACTIVITIES STATISTICS

Users Data Transfer Disk Storage Usage

Backup Jobs

User	Backup Set	Destinations	IP Address	Start Time	End Time	Backup Duration	Backup Status	Backup Size*
steven	K Drive Backup	GoogleDrive-1	192.168.7.105	11/24/2016 10:25:46	11/24/2016 10:24:33	1 min(s) 13 sec(s)	OK	6 [23.51M / 28.53M]
steven	K Drive Backup	GoogleDrive-1	192.168.7.105	11/24/2016 12:46:33	11/24/2016 12:45:07	1 min(s) 26 sec(s)	OK	5 [12.29M / 14.92M]
steven	K Drive Backup	GoogleDrive-1	192.168.7.105	11/24/2016 18:17:56	11/24/2016 18:15:06	2 min(s) 50 sec(s)	OK	7 [12.31M / 14.98M]
steven2	File backup testing	[Pre-v7]	--	11/24/2016 15:00:03	11/24/2016 15:00:03	0 sec(s)	Missed Backup	0 [0 / 0]

Restore Jobs

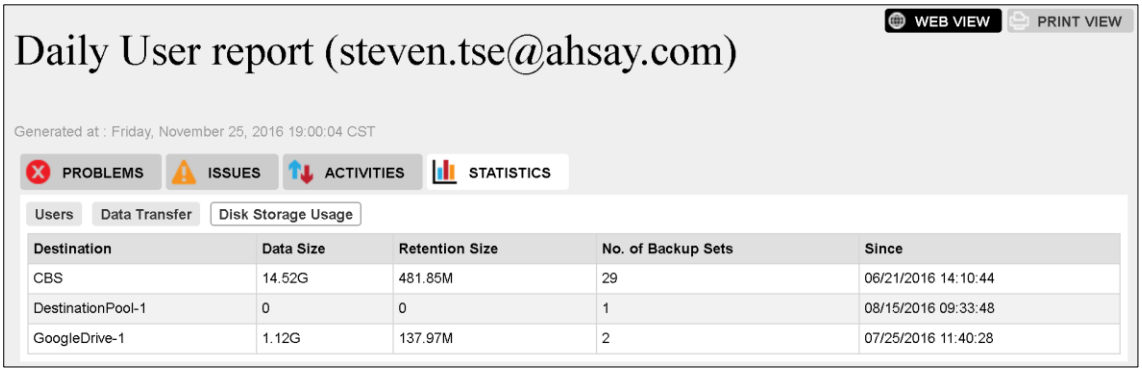
User	Backup Set	Destinations	IP Address	Start Time	End Time	Restore Duration	Restore Status	Restore Size**
steven	K Drive Backup	GoogleDrive-1	192.168.7.105	11/24/2016 17:36:14	11/24/2016 17:36:36	22 sec(s)	OK	14 (34.73M)

* Unit = No. of files [Compressed size / Uncompressed size]
** Unit =No. of files (Downloaded size)

Users	Name of the backup user
Backup Set	Name of the backup set
Destinations	Backup Destination of the particular backup set
IP Address	IP address of the client backup agent running the backup / restore
Start Time	Start time of the particular backup / restore
End Time	End time of the particular backup / restore
Backup Duration / Restore Duration	Duration of the backup / restore for the particular backup / restore
Backup Status / Restore Status	Status of the particular backup / restore job
Backup Size / Restore Size	Backup size / Restore size No. of files [Compressed size / Uncompressed size]

➢ Disk Storage Usage

This page shows a list of statistics data regarding disk storage usage.

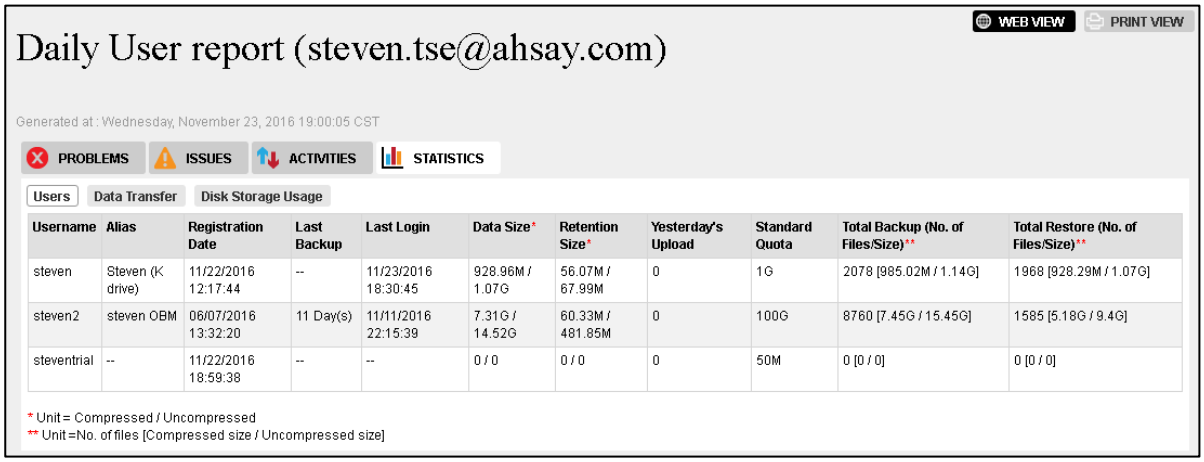


Destination	Backup destination used by the backup user
Data Size	Size of data backed up to the particular backup destination
Retention Size	Size of retention area on the particular backup destination
No. of Backup Sets	Number of backup set(s) on the particular backup destination
Since	The data and time when the particular backup destination was created

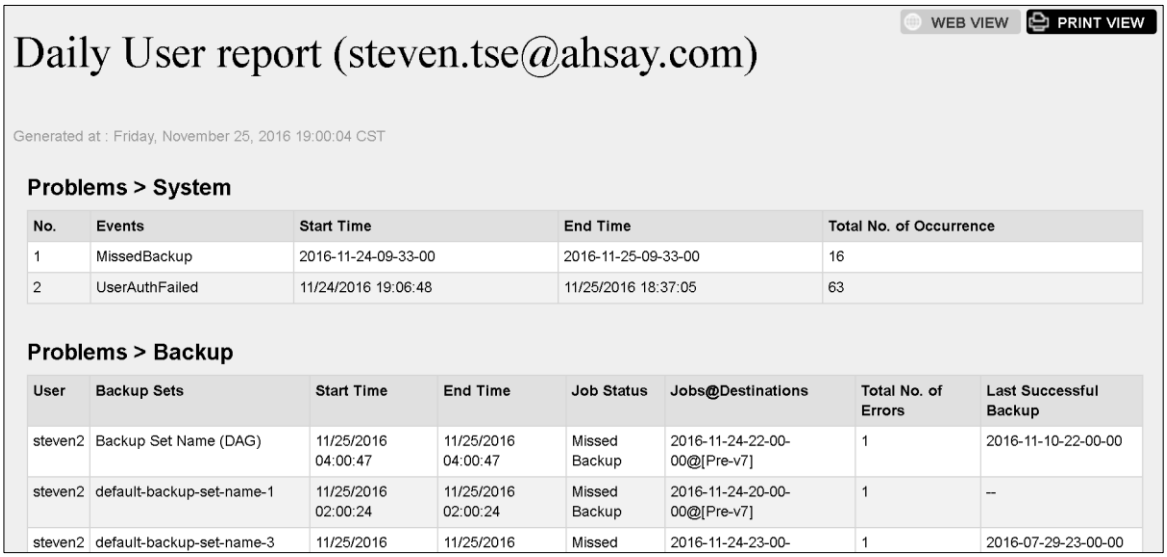
Daily Report Viewing Option

There are two viewing options for the daily report, namely the WEB VIEW and PRINT VIEW, which can be altered by click the corresponding icon at the top right corner.

The **WEB VIEW** is an interactive style report where data is presented under different categories while user navigates through the report.



The **PRINT VIEW** is a one-page report listing all the data from the different categories from the **WEB VIEW** report.



WEB VIEW PRINT VIEW

Daily User report (steven.tse@ahsay.com)

Generated at : Friday, November 25, 2016 19:00:04 CST

Problems > System

No.	Events	Start Time	End Time	Total No. of Occurrence
1	MissedBackup	2016-11-24-09-33-00	2016-11-25-09-33-00	16
2	UserAuthFailed	11/24/2016 19:06:48	11/25/2016 18:37:05	63

Problems > Backup

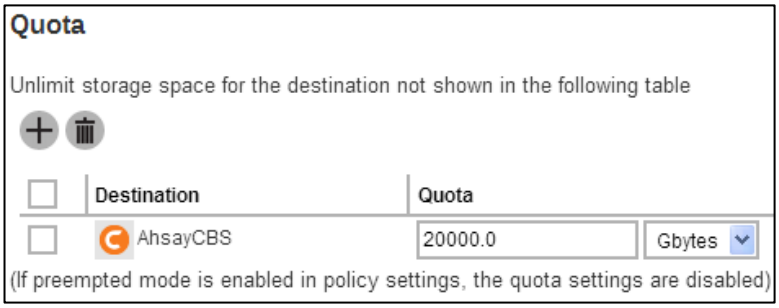
User	Backup Sets	Start Time	End Time	Job Status	Jobs@Destinations	Total No. of Errors	Last Successful Backup
steven2	Backup Set Name (DAG)	11/25/2016 04:00:47	11/25/2016 04:00:47	Missed Backup	2016-11-24-22-00-00@[Pre-v7]	1	2016-11-10-22-00-00
steven2	default-backup-set-name-1	11/25/2016 02:00:24	11/25/2016 02:00:24	Missed Backup	2016-11-24-20-00-00@[Pre-v7]	1	--
steven2	default-backup-set-name-3	11/25/2016	11/25/2016	Missed	2016-11-24-23-00-	1	2016-07-29-23-00-00

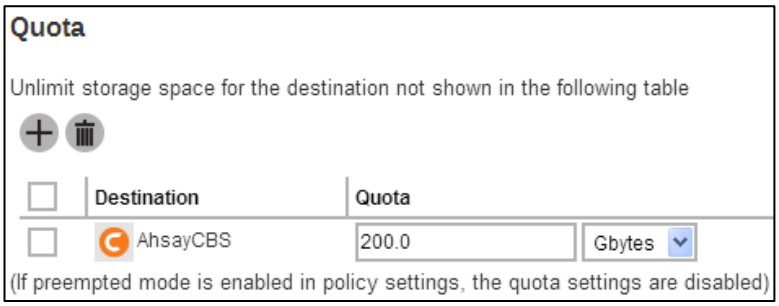
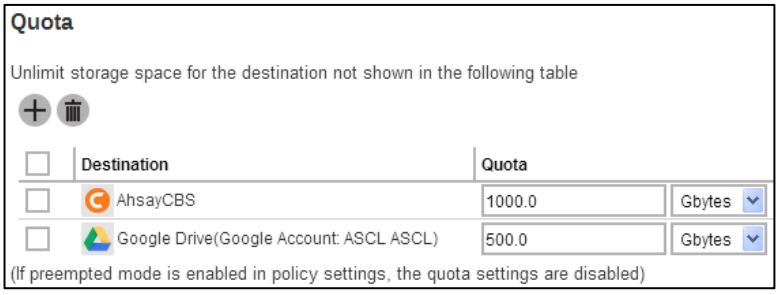
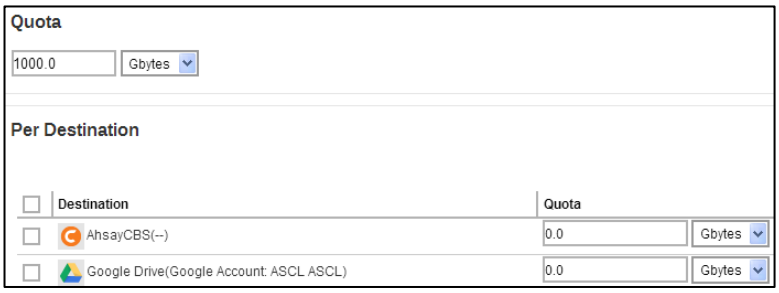
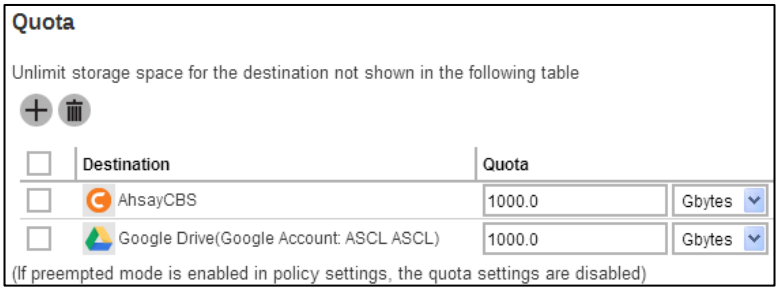
Appendix J System Files for Continuous Backup Exclusion

Below is a full list of system files you choose to exclude from performing the continuous backup.

- C:\Program Files
- C:\Windows
- Pagefile.sys
- hiberfil.sys
- *.tmp
- *.part
- System Volume Information
- $Recycle.Bin (Vista, 2008/R2, Win7)
- RECYCLER(2000, XP, 2003)
- RECYCLED
- C:\Documents and Settings\All Users\Application Data\Microsoft, C:\ProgramData\Microsoft
- C:\Documents and Settings\All Users\Application Data\Kaspersky Lab
- C:\Documents and Settings\All Users\Application Data\Symantec
- C:\Documents and Settings\All Users\Application Data\Avg7
- C:\Documents and Settings\All Users\Application Data\Avg8
- C:\Documents and Settings\All Users\Application Data\McAfee
- C:\Documents and Settings\All Users\Application Data\McAfee.com
- C:\Documents and Settings\All Users\Application Data\Sophos
- ntuser.dat ntuser.dat.log
- *\AppData\Local\Microsoft*
- *\AppData\Local\Temp*
- *\AppData\Roaming Data\Microsoft*
- *\Local Settings\Application Data\Microsoft*
- *\Local Settings\Temporary Internet Files
- *\Local Settings\Temp
- *\Local Settings\History
- *\LOCALS~1\Temp
- *\LOCALS~1\Tempor~1
- *\LOCALS~1\History
- ~$*.doc
- ~$*.ppt
- ~$*.xls
- ~$*.dot

Appendix K Comparison Screen Shot for Quota Management between Pre-v7.15.6.0 and Post- v7.15.6.0

<table>
<tr><th colspan="2">Backup/ Restore > Users, Groups & Policies > Backup User > %username% > User Profile > Backup Client Settings - Quota</th></tr>
<tr><td>Pre-v7.15.6.0</td><td><u>Example-1</u>: Total quota is 20000GB and AhsayCBS is default quota setting.
</td></tr>
<tr><td>Post- v7.15.6.0</td><td>AhsayCBS will be same value with total quota setting, 20000GB.
 
</td></tr>
<tr><td>Pre-v7.15.6.0</td><td><u>Example-2</u>: Total quota is 500GB and AhsayCBS is 200GB.
</td></tr>
</table>

Post- v7.15.6.0	AhsayCBS will maintain to be 200GB. 
Pre-v7.15.6.0	**Example -3**: Total quota is 1000GB and AhsayCBS is default quota setting while predefined destination of Google Drive is 500GB.
Post- v7.15.6.0	AhsayCBS will be same value with total quota setting, 1000GB, and predefined destination of Google Drive will maintain to be 500GB. 
Pre-v7.15.6.0	**Example -4**: Total quota is 1000GB and AhsayCBS and predefined destination of Google Drive is default quota setting. 

Post- v7.15.6.0	Both AhsayCBS and predefined destination of Google Drive will be same value with total quota setting, 1000GB.