

Grandstream Networks, Inc.

Amazon S3 Storage Integration Guide



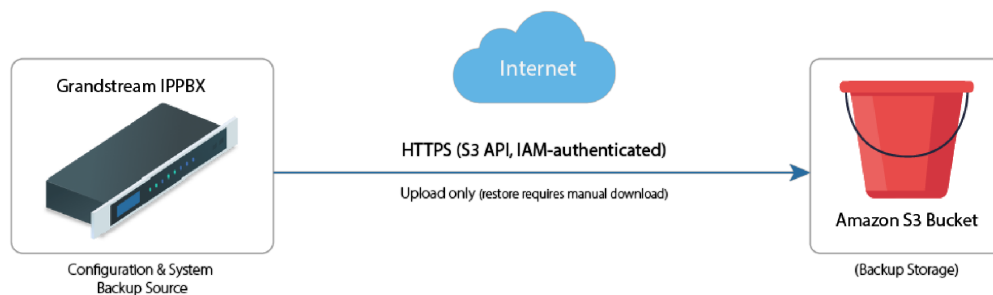
INTRODUCTION

This guide explains how to integrate Grandstream IPPBX systems with Amazon Storage Service (S3) to store system backup files in customer-owned cloud storage. This integration is intended for recovery, compliance, and long-term retention, independent of the primary Grandstream IPPBX storage.

Amazon S3 provides highly durable, off-site storage, allowing administrators to maintain an additional copy of PBX configuration data outside the appliance or cloud instance. When configured, the PBX automatically uploads backup archives to a designated S3 bucket using secure IAM credentials.

The procedures in this guide walk through:

- Preparing an Amazon S3 bucket and IAM user.
- Configuring the PBX to connect securely to that bucket.
- Performing manual and scheduled backups to S3.



Overview of PBX backup integration with Amazon S3

PREREQUISITES

To complete this integration, please ensure the following:

- The Grandstream PBX is upgraded to a firmware release that introduces Amazon S3 storage integration (*For more information, refer to the [Supported Models](#) section*).
- Administrator access to the PBX web UI with integration privileges.
- An AWS account with the ability to create and manage S3 buckets, as well as IAM users and access credentials.
- Stable internet access from the PBX to AWS.
- A dedicated IAM user limited to access only the target S3 bucket.

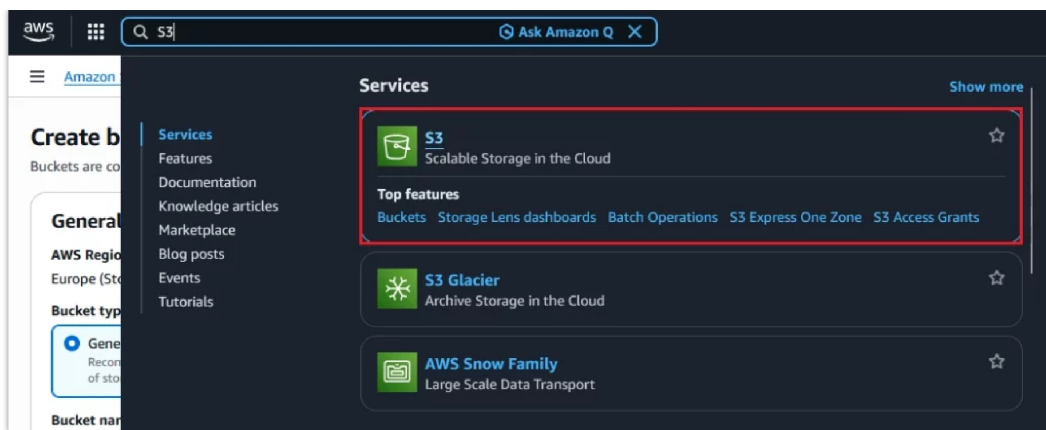
AMAZON S3 CONFIGURATION

This section covers the preparation steps required in Amazon S3 before the PBX can store backups. You will create a dedicated backup bucket and an IAM user with restricted permissions that the PBX will use to upload backup files securely.

Create an S3 Bucket

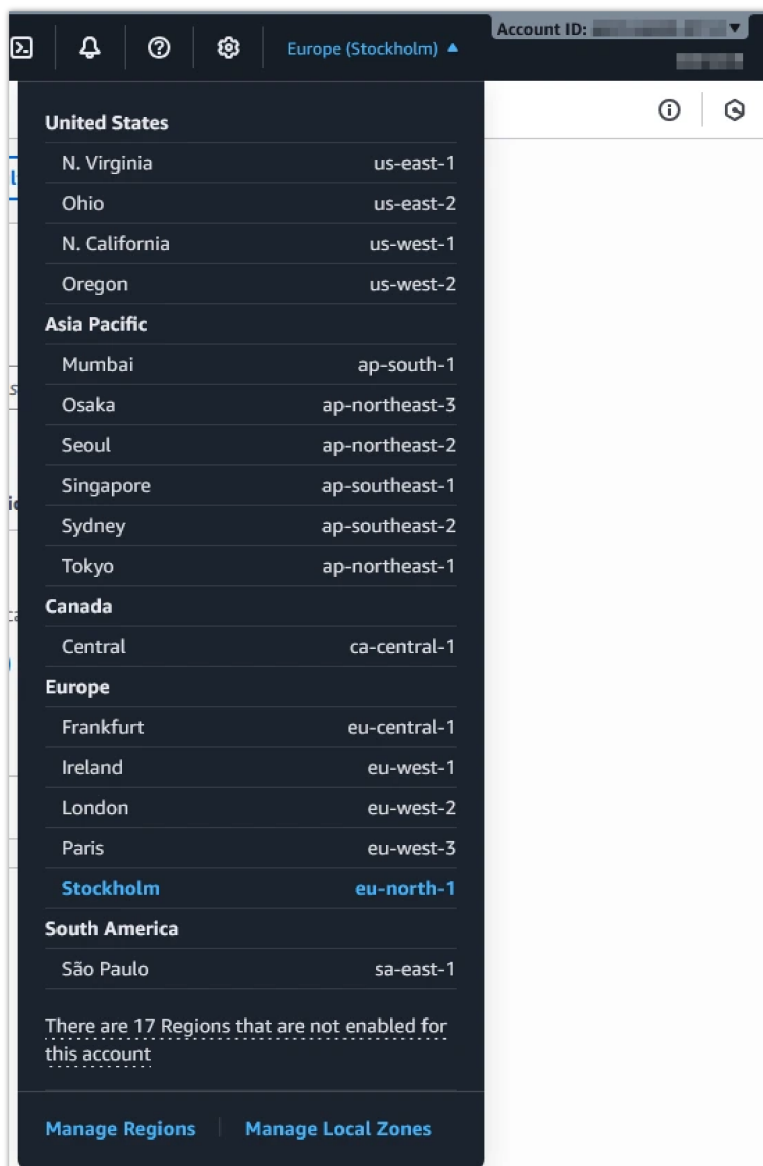
Follow the steps below to create the bucket that will store IPPBX backup files.

1. Sign in to the AWS Console and open **Amazon S3**.



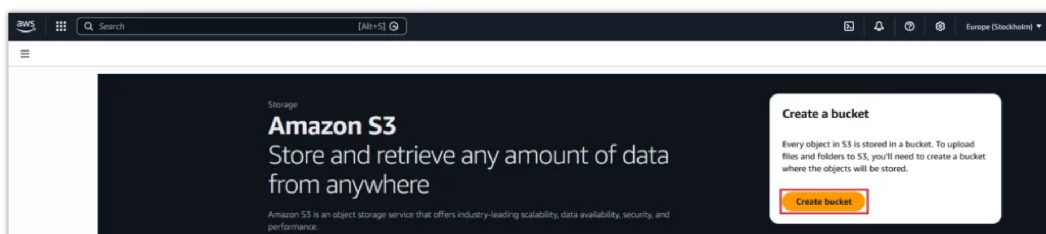
Navigating to the Amazon S3 Service from the AWS Console

- Before creating the bucket, select the correct **AWS Region** in the console header (top-right). The bucket will be created in this region.



Selecting the AWS Region

- Click **Create bucket**.



- On the Create bucket page, review the value shown under **AWS Region** (for example: eu-north-1, us-east-2, etc.)
- Under **Bucket type**, select *“General purpose”*.

General-purpose buckets are recommended because they automatically store data across multiple Availability Zones (for high durability) and support the full set of standard Amazon S3 features used by the PBX backup integration.

- Enter a **Bucket name**.
- Leave **Object Ownership** set to *“ACLs disabled (recommended)”*. This ensures the bucket owner always retains control of backup files and access is managed using IAM policies instead of object-level ACLs, reducing complexity and misconfiguration risk.

Create bucket info
Buckets are containers for data stored in S3.

General configuration

AWS Region
Europe (Stockholm) eu-north-1

Bucket type info

☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name info
ucm-backup-storage-bucket

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn more](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Object Ownership info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

Object Ownership

☒ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

Bucket Creation Configuration Settings

- Ensure that **Block all public access** remains enabled. This setting enforces private-only access paths since backups must never be exposed publicly.

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will ignore new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Bucket Public Access Settings

- (Optional but recommended) **Enable Versioning and Default Encryption** before creating the bucket. Versioning allows rollback to previous backups if one becomes corrupted, and encryption ensures backup data is protected at rest.
- (Optional) Enable **Object Lock** only if your organization requires immutable backups. Object Lock prevents backup files from being deleted or overwritten for a defined retention period. It is typically used in regulated environments (WORM compliance).

Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning
☒ Disable
☐ Enable

Tags - optional
You can use bucket tags to analyze, manage and specify permissions for a bucket. [Learn more](#)

Tags
 You can use s3:ListTagsForResource, s3:TagResource, and s3:UntagResource APIs to manage tags on S3 general purpose buckets for access control in addition to cost allocation and resource organization. To ensure a seamless transition, please provide permissions to s3:ListTagsForResource, s3:TagResource, and s3:UntagResource actions. [Learn more](#)

No tags associated with this bucket.

[Add new tag](#)
You can add up to 50 tags.

Default encryption
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type
☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)
☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)
☐ Disable
☒ Enable

Advanced settings
Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)
☒ Disable
☐ Enable
 Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.

Bucket Versioning Encryption and Object Lock Settings

11. Click *Create bucket*. After creation, you will see a confirmation message and be redirected to the bucket details page.

Successfully created bucket "ucm-backup-storage-bucket"
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

General purpose buckets [All AWS Regions](#) **Directory buckets**

General purpose buckets (1)
Buckets are containers for data stored in S3.

[Find buckets by name](#)

Name	AWS Region	Creation date
ucm-backup-storage-bucket	Europe (Stockholm) eu-north-1	December 29, 2025, 15:09:38 (UTC+01:00)

Account snapshot
Storage Lens provides visibility into storage usage and activity trends.

External access summary - new
External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Bucket Creation Confirmation Page

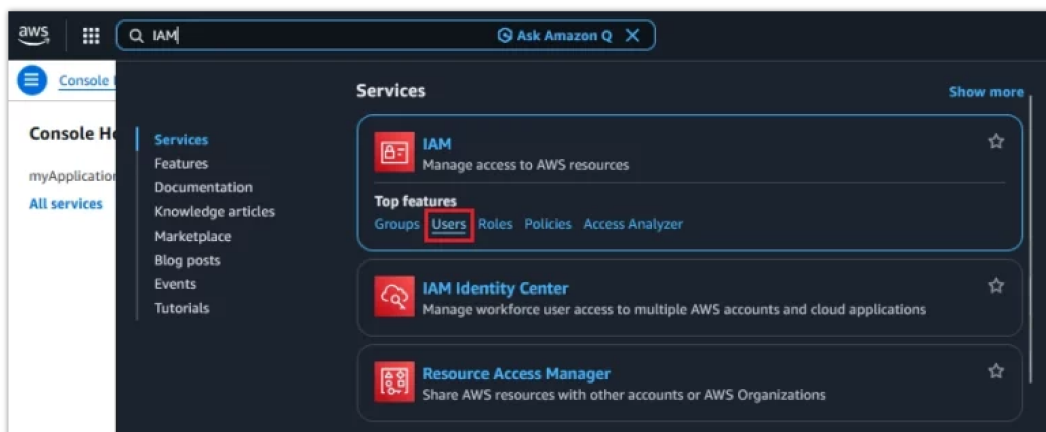
12. Record the **bucket name** and **region**, both of which are required when configuring Amazon S3 on the PBX.

Create an IAM User and Access Keys

The PBX connects to Amazon S3 using an IAM user. It is strongly recommended to create a dedicated IAM user with restricted permissions instead of using a root or administrative account.

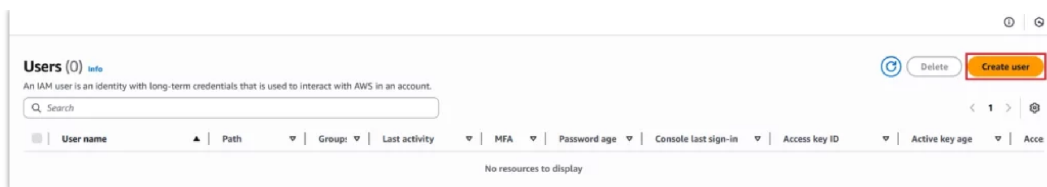
Follow the steps below to create credentials for the PBX.

1. Open the AWS Console and go to **IAM→Users→Add users**.



Navigating to IAM Users in the AWS Console

2. Click on "Create user".



Creating a new IAM user in the AWS Console

3. Enter a username (for example: *ucm-s3-backup*).
4. Leave "Provide user access to the AWS Management Console" unchecked.

Configuring IAM User Details

5. On the **Set permissions** page, select *Add user to group*. Using a group makes it easier to manage backup permissions later if additional systems are added.
6. Click **Create group** and name the group something descriptive, such as *"ucm-backup-group"*.
7. Select Create policy to configure the permissions for this user group.

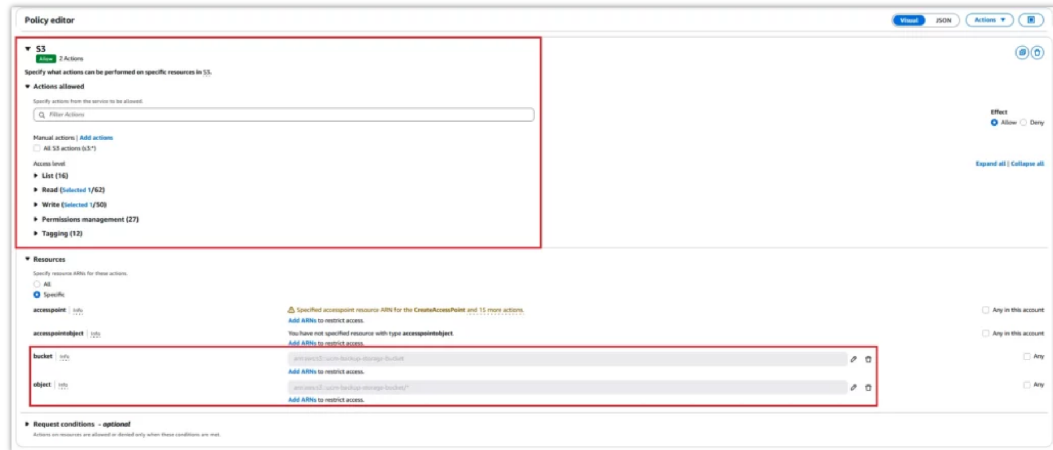
Create User Group Policy

8. On this page, name the policy and define permissions using either the **Visual editor** or the **JSON editor (advanced)**.
 - o **Method 1 (Visual editor):**
 - o Choose **Service** → **S3**, then enable:
 - o *GetBucketLocation* (under Read)
 - o *PutObject* (under Write)
 - o Specify the resources by clicking "Add ARN" under **bucket**, entering the previously created bucket name, then repeat under **object** and enter the same bucket name with *** as "Resource object name" to allow access to objects inside the bucket.
 - o **Method 2 (JSON editor):** Paste the policy below and replace *YOUR-BUCKET-NAME* with your S3 bucket name.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::YOUR-BUCKET-NAME",
        "arn:aws:s3:::YOUR-BUCKET-NAME/*"
      ]
    }
  ]
}

```



Visual Policy Configuration



JSON Code Policy Configuration

9. Save the policy, return to the **Create user group** window, refresh the list, select your new policy, and click **Create user group**.

Create user group ✕

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

User group name
Enter a meaningful name to identify this group.

ucm-backup-group

Maximum 128 characters. Use alphanumeric and '+,=, @, _' characters.

Permissions policies (1111) ↻ [Create policy](#)

Filter by Type ✕ Customer ma... 1 match < 1 > ⚙️

☐	Policy name ↗	Type ▼	Use... ▼	Description
☐	+ backup-policy	Customer man...	Permis...	-

[Cancel](#) [Create user group](#)

Creating an IAM User Group

10. Complete the user creation wizard by assigning the created group and confirming.

Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

- ☒ **Add user to group**
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- ☐ **Copy permissions**
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- ☐ **Attach policies directly**
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1) ↻ [Create group](#)

☒ [ucm-backup-group](#) 0 [backup-policy](#) 2025-12-29 (Now)

▼ Set permissions boundary - optional
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

☐ Use a permissions boundary to control the maximum permissions.
You can select one of the existing permissions policies to define the boundary.

[Cancel](#) [Previous](#) [Next](#)

Assigning the IAM User to the Backup Group

11. Open the user, go to **Security credentials**, and click **Create access key**.

Identity and Access Management (IAM) Search IAM

ucm-s3-backup [info](#) [Delete](#)

Summary

ARN: [arn:aws:iam::640168432112:user/ucm-s3-backup](#) Console access: Disabled
Created: December 29, 2025, 16:39 (UTC-01:00) Last console sign-in: -

Permissions **Groups (1)** **Tags** **Security credentials** **Last Accessed**

Console sign-in

Console sign-in link: [https://640168432112.signin.aws.amazon.com/console](#) Console password: Not enabled [Enable console access](#)

Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

[Assign MFA device](#)

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

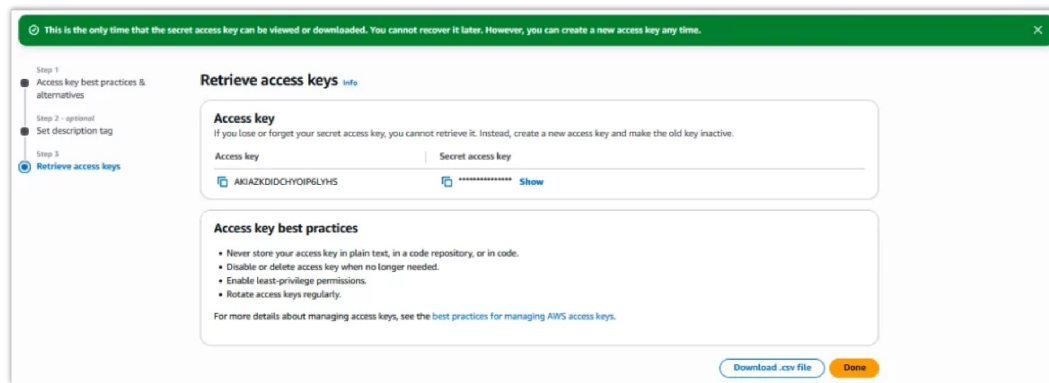
[Create access key](#)

Creating an IAM Access Key for the Backup User

12. Choose **Application running outside AWS**, then generate and save:

- Access Key ID
- Secret Access Key

13. Click *Download .csv* file and store it in a secure location.



Viewing and Downloading the IAM Access Key

Notes:

- This is the only time AWS will display the Secret Access Key. If it is lost, you must create a new access key.
- These keys will be entered later in the PBX Amazon S3 configuration.
- Keep these credentials secure. If exposed, disable and regenerate them immediately.

PBX CONFIGURATION

This section describes how to connect the PBX to the Amazon S3 bucket created earlier and how to use S3 as a backup destination. After configuration, the PBX will securely upload backup files to the designated S3 bucket.

Configure Amazon S3 Connection

Once the S3 bucket and IAM credentials are prepared, the next step is to configure the PBX so it can store backup files in Amazon S3.

Follow the steps below.

1. Log in to the PBX web UI using an administrator account with integration privileges.
2. Go to **PBX Settings**→**Storage Device Management**→**Amazon S3**.
3. Toggle **Enable** to activate the Amazon S3 configuration fields.
4. Fill in the fields as follows:

Region	Select the AWS Region where your bucket was created (for example: <i>Europe (Stockholm) eu-north-1</i>). If only a text field is available, enter the AWS Region code (for example: <i>eu-north-1</i> , <i>us-east-2</i>).
Bucket	Enter the exact name of the S3 bucket you created (for example: <i>ucm-backup-storage-bucket</i>). Bucket names are case-sensitive and must match exactly.
Key ID	Paste the Access Key ID from the IAM user created earlier. The field is masked immediately after entry for security.
Secret Key	Paste the Secret Access Key from the downloaded CSV file. The field is masked immediately after entry for security.

- Click **Start** under **Test Connection**. If the test succeeds, a confirmation banner appears, indicating that the PBX can reach the S3 bucket using the provided credentials.

Storage Device Management

NAS SFTP USB Disk/SD Card File Management **Amazon S3**

Enable ☒

* Region Please go to [AWS Documentation](#) to search the region

ⓘ If there is no option, enter the **AWS Region code**, for example, enter "us-east-2" for the eastern part of the United States (Ohio).

* Bucket 3 - 63 characters, Supports lowercase letters, numbers and special characters.-

* Key ID

* Secret Key

Test Connection **Start**

ⓘ It is recommended to test connection during the initial setup and after changing settings to confirm it is working properly.

Successful Amazon S3 Connection Test

- After a successful test, click **Save**.

Using Amazon S3 for Backups

Once Amazon S3 is configured and enabled, the PBX can store backup archives directly in the configured S3 bucket.

Note:

Only backup files are uploaded to Amazon S3. Other system data (such as call recordings and voicemails) continues to use the primary storage configured on the PBX.

Create a Manual Backup to Amazon S3

To create a manual backup to Amazon S3, please follow the steps below:

- Log in to the PBX web UI.
- Navigate to **Maintenance**→**Backup**→**Backup/Restore**.
- Click **Backup** to create a new backup task.

Backup

Backup/Restore Data Sync

ⓘ Backup files must be .tar or .tgz, named with alphanumeric characters, dashes (-) and underscores (_).

Backup Schedule Backup Upload

Scheduled Backup Task List

Delete

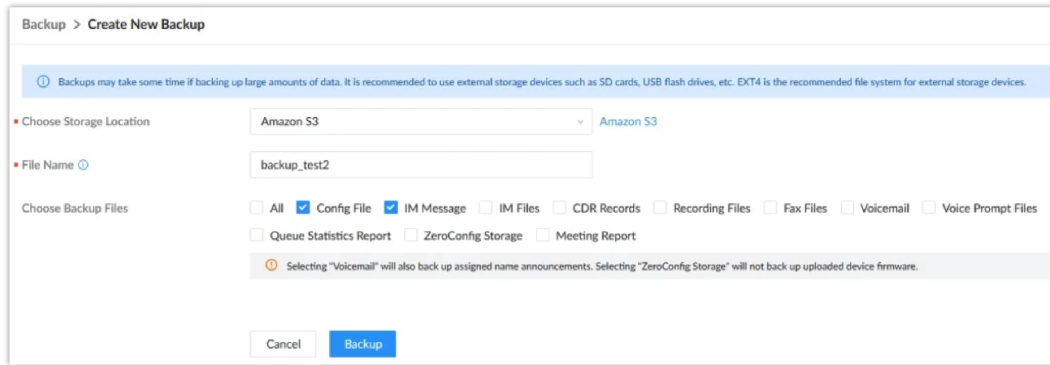
☐	Name	Storage Location	Start Time
--------------------------	------	------------------	------------

Creating a New Manual PBX Backup

- Select the configuration components you want included in the backup.
- Under **Storage Location**, choose **Amazon S3**.

Note:

Amazon S3 can be selected only when S3 integration is enabled and the connection test has succeeded.



Manual PBX Backup Settings

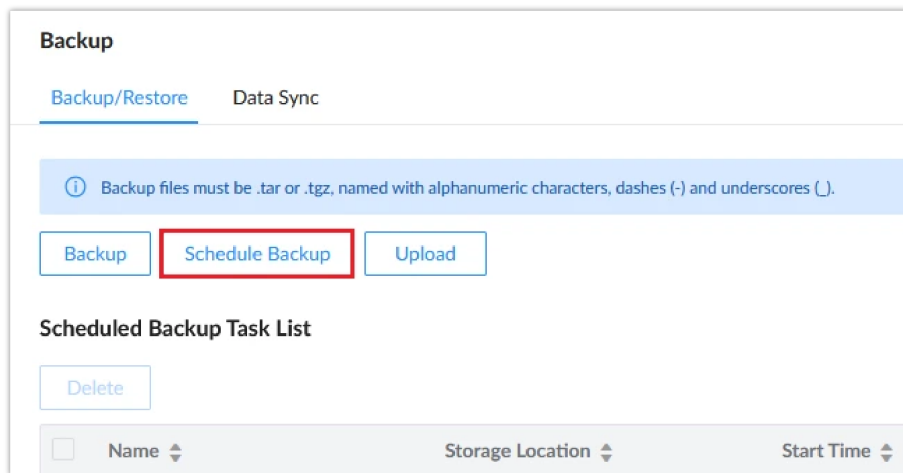
6. Click **Execute** to start the backup.

The PBX creates the backup file locally and uploads it to the configured S3 bucket using the IAM credentials provided. If the upload fails, check S3 connectivity, IAM permissions, and bucket region configuration.

Configure Scheduled Backups to Amazon S3

Scheduled backups allow regular automated upload to Amazon S3.

1. Go to **Maintenance**→**Backup/Restore**.
2. Click **Schedule Backup** to create a new scheduled backup.



Creating a New Scheduled PBX Backup

3. Specify the date, time, and recurrence (e.g., daily, weekly, monthly, or custom).
4. Select the components to include in the backup.
5. Under **Storage Location**, choose **Amazon S3**.

Backup > Create New Schedule Backup

ⓘ Backups may take some time if backing up large amounts of data. It is recommended to use external storage devices such as SD cards, USB flash drives, etc. EXT4 is the recommended file system for external storage devices.

ⓘ SFTP server can be configured in the PBX Settings->Storage Device Management-> SFTP page.

ⓘ Configuring multiple scheduled backups at the same time may affect performance. It is recommended to schedule them for non-working hours or to set intervals for different backup tasks.

Schedule Backup ☒

• Name 2 - 64 characters, only alphanumeric characters, chinese characters, space and special characters _ - are supported

• Choose Storage Location Amazon S3

• Date

• Time

• Repeat

Choose Backup Files

☐ All ☒ Config File ☒ IM Message ☒ IM Files ☐ CDR Records ☐ Recording Files ☐ Fax Files ☐ Voicemail ☒ Voice Prompt Files

☐ Queue Statistics Report ☒ ZeroConfig Storage ☐ Meeting Report

ⓘ Selecting "Voicemail" will also back up assigned name announcements. Selecting "ZeroConfig Storage" will not back up uploaded device firmware.

Scheduled PBX Backup Settings

Note:

Amazon S3 can be selected only when S3 integration is enabled and the connection test has succeeded.

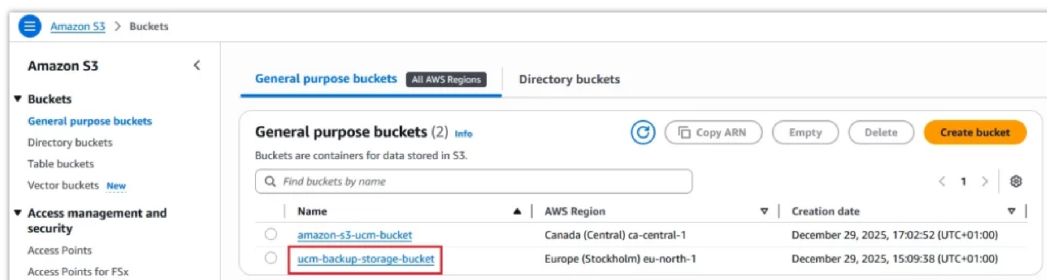
6. Save and apply the scheduled backup settings.

The PBX will automatically generate and upload backups to S3 at the configured times.

Verify Backups on Amazon S3

Once a backup task (manual or scheduled) completes, verify the S3 bucket to confirm that the backup file has been uploaded.

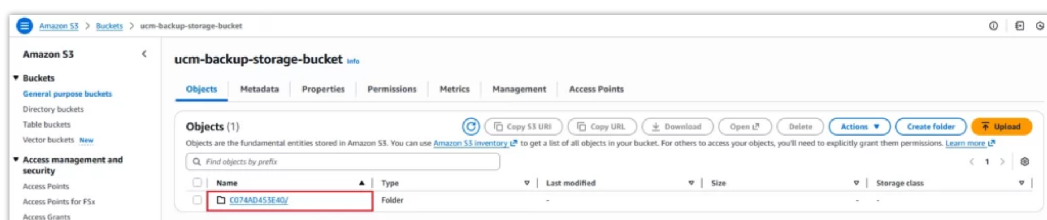
1. Sign in to the **AWS Console**.
2. Open **Amazon S3**→**Buckets**.
3. Select the bucket configured for PBX backups.



Selecting the S3 Bucket Used for PBX Backups

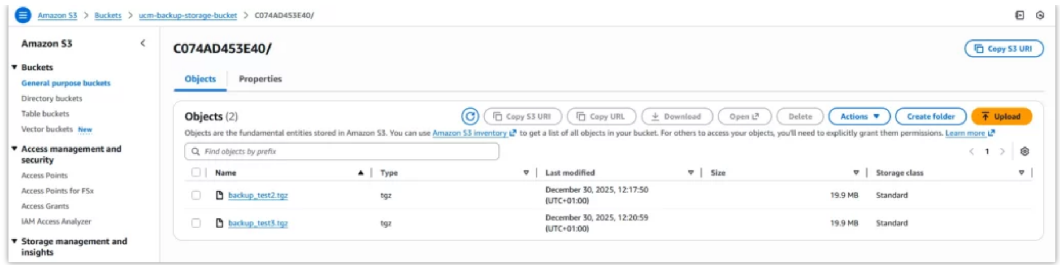
Inside the bucket, the PBX creates a folder named after its MAC address. This allows multiple devices to share the same S3 bucket without overwriting each other's backups.

4. Open the folder whose name matches the PBX MAC address.



Opening the Main PBX Backup Folder

5. Inside the folder, confirm that backup files exist.



Verifying Backup Files Stored in the PBX Folder

If the folder is empty or missing, check the backup job result in **Backup→Backup/Restore→Sync History**.

Sync History					
Name	Type	Task Status	Start Time	Repeat	Options
Realtime Backup	Backup	Executed	2025-12-30 12:21	No Repeat 12:21	
Realtime Backup	Backup	Executed	2025-12-30 12:18	No Repeat 12:18	
Realtime Backup	Backup	Failed	2025-12-30 12:16	No Repeat 12:16	
Realtime Backup	Backup	Failed	2025-12-30 12:14	No Repeat 12:14	
Realtime Backup	Backup	Failed	2025-12-30 12:12	No Repeat 12:12	
Realtime Backup	Backup	Executed	2025-12-30 12:10	No Repeat 12:10	

Reviewing Backup Sync History

SUPPORTED MODELS

The Amazon S3 integration is available only on specific Grandstream PBX platforms and firmware releases. Use the table below to verify whether your system supports this feature before proceeding with configuration.

Models	Firmware Requirement
UCM630x	1.0.31.7+
UCM630xA	1.0.31.7+
CloudUCM	1.0.29.7+
SoftwareUCM	1.0.33.7+