What is an S3 Access Point?

An **S3 Access Point** is a **custom entry point** to a specific S3 bucket that you can create to:

- Control **who can access** the bucket
- Define **how** they can access it (e.g., via VPC, certain paths, or with restricted permissions)

It's like a **named gateway** to your S3 bucket with **custom access rules**, especially useful in **large-scale, multi-tenant, or VPC-restricted setups**.

Why Use Access Points?

Without Access Point (classic method):

- You set permissions directly on the **S3 bucket policy**, which can get complex and messy as users/applications grow.

With Access Point:

- You create **separate access configurations per app, user group, or service** — all pointing to the **same bucket**, but with their own rules.

Key Features

Feature	Description
Scoped Permissions	Define per-access-point IAM policies (instead of bloating bucket policies)
Isolation	Control access to a **specific prefix** (folder-like path) in the bucket
VPC Restrictions	Access point can be **limited to a VPC**, preventing public or internet access
Multiple per bucket	One bucket can have **many access points**, each with different rules
Simplifies security	Easier to audit and delegate access securely

Example Use Case

You have a bucket: `my-data-bucket`

You create:

- Access Point `logs-reader` — allows `GET` to `/logs/*` only from a VPC
- Access Point `uploads-writer` — allows `PUT` to `/uploads/*` for a specific IAM role

Each app/service uses **its access point ARN** instead of the bucket directly.

Access Point ARN Format

`arn:aws:s3:<region>:<account-id>:accesspoint/<access-point-name>`

Security Tip

Even with access points, the **bucket policy must allow the access point**. AWS automatically manages this if you use the console or CLI correctly.

When to Use Access Points

Use S3 Access Points when:

- You have **many apps or users** accessing the same bucket
- You want **fine-grained control** over prefixes (paths)
- You need to **limit access to a VPC**
- You're using **Amazon Lake Formation**, **analytics**, or **multi-tenant apps**

---

1. `bucket_policy.json` — S3 Bucket Policy

```
"Resource": [
  "arn:aws:s3:::yetanotherrandombucketbyps",
  "arn:aws:s3:::yetanotherrandombucketbyps/*"
],
"Condition": {
  "StringEquals": {
    "s3:DataAccessPointAccount": "686766985335"
  }
}
```

Purpose:

- **Allows access to the S3 bucket only through access points owned by account `686766985335`.**
- **Blocks direct access from clients that don’t use an access point.**

To use:

- **Go to S3 Console > Bucket > Permissions > Bucket Policy**
- **Paste this policy into the bucket to restrict access to Access Points only.**

---

2. `access_point_policy.json` — Access Point Policy

```
"Principal": {
  "AWS": "arn:aws:iam::686766985335:user/ps_user"
},
"Resource":
"arn:aws:s3:us-east-1:686766985335:accesspoint/ps-user-ap/object/folder1/*"
```

Purpose:

- **Allows `ps_user` to GET and PUT objects in `folder1/` via the access point `ps-user-ap`.**

To use:

- **Go to S3 Console > Access Points > ps-user-ap > Permissions**
- **Paste this as the Access Point Policy**

Note:
Make sure the Access Point is in the same account and region as defined in the ARN.

---

3. `iam_user_policy.json` — IAM User Policy

```
"Action": [
  "s3:ListAllMyBuckets",
  "s3:GetAccessPoint",
  "s3:ListAccessPoints",
  "s3:ListMultiRegionAccessPoints",
  "s3:ListBucket"
]
```

Purpose:

- **Grants basic S3 listing and access point discovery permissions to the IAM user `ps_user`.**

To use:

- **Go to IAM Console > Users > ps_user > Permissions**
- **Attach this as an inline policy or through a managed policy.**

Step 1: Create the S3 Bucket

1. Go to AWS S3 Console
2. Click "Create bucket"
3. Set the bucket name:
   `yetanotherrandombucketbyps`
4. Keep default settings (you can uncheck Block Public Access if needed)
5. Click "Create bucket"

Step 2: Attach Bucket Policy (restrict to Access Points)

1. Go to the bucket → Permissions tab → Bucket policy
2. Paste this policy (from `1bucket_policy.json`)

This blocks direct S3 access and only allows access via Access Points owned by your AWS account.

Step 3: Create the Access Point

1. Go to S3 Console > Access Points > Create access point
2. Set name: `ps-user-ap`
3. Bucket: select `yetanotherrandombucketbyps`
4. Network origin: choose `Internet` (or `VPC` if needed)
5. Click "Create access point"

Step 4: Attach Access Point Policy

1. **Open `ps-user-ap` > go to Permissions**
2. **Paste this policy (from `access_point_policy.json`)**

This grants the IAM user permission to upload/download files in `folder1/` via this access point only.

Step 5: Create or Modify the IAM User (`ps_user`)

1. **Go to IAM Console > Users**
2. **Create user or select `ps_user`**
3. **Attach this inline policy (from `iam_user_policy.json`)**

This enables the user to list and access buckets and access points.

Step 6: Upload/Download via access point
