At creation and by default, all S3 resources are private and only accessible to the resource owner and account administrator. With S3 access management tools, you can enable access to an S3 bucket or object, define user policies, and block all public access requests.

**Create access policies to your S3 resources**

**Resource-based policies**
Define and grant user access within an AWS account

**User policies**
Enforce access policies to all objects in an S3 bucket

**S3 Access Points**
Manage access to your shared data sets on S3. Create Access Points with permissions for each application or groups of applications, or limit access to a Virtual Private Cloud (VPC).

**Access Control Lists (ACLs)**
Define what users and accounts have read and/or write permissions Configure at the object and bucket levels

**Query String Authentication**
Grant time-limited access to third parties with temporary URLs

**Use S3 Batch Operations**
To manage ACLs for hundreds to billions of objects — in minutes

**AWS Identity and Access Management (IAM)**
Create users, groups, and roles within your AWS account Define permissions to S3 and AWS resources

**Use AWS CloudTrail**
To monitor account activities Track who is accessing what data, from where, and when

**Access Analyzer for S3**
Reviews and alerts you to all buckets that allow access to anyone on the internet or other AWS customers

**Receive a report showing the source and level of public or shared access of your buckets**
With one click, block all unintended public access to your bucket or drill down for granular levels of access

**AWS CloudTrail**
Reports on actions taken by users, roles, and AWS services Includes calls from the S3 Management Console and S3 APIs

**Enable continuous delivery of events or view most recent events on demand**
Learn details about an S3 access request, including requester, IP address, time, and error code

**Amazon Macie**
Discover, classify, and protect sensitive stored data

**Monitor data access patterns for anomalies**
Receive alerts when unauthorized access or inadvertent data leaks are detected

**Receive detailed records of requests made to a bucket (and store them in S3)**
See requester, bucket name, request time, request action, and error code

**Enforce a “no public access” policy with a few clicks**
Discover publicly accessible buckets with Amazon Macie

**Block access to specific buckets or an entire AWS account**
Override all other access policies

**Block all public access requests**
S3 Block Public Access

**S3 Block Public Access**
Trusted Advisor bucket permission check
S3 Management Console’s access indicator

**S3 Event Notifications**
Configure events to occur when changes are made to S3 resources
Trigger workflows and alerts, and invoke AWS Lambda

Learn more about Amazon S3 security features