Access management for AWS resources

[**PDF**](https://docs.aws.amazon.com/IAM/latest/UserGuide/iam-ug.pdf#access)[**RSS**](https://docs.aws.amazon.com/IAM/latest/UserGuide/aws-iam-release-notes.rss)

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. When a [principal](https://docs.aws.amazon.com/IAM/latest/UserGuide/intro-structure.html#intro-structure-principal) makes a request in AWS, the AWS enforcement code checks whether the principal is authenticated (signed in) and authorized (has permissions). You manage access in AWS by creating policies and attaching them to IAM identities or AWS resources. Policies are JSON documents in AWS that, when attached to an identity or resource, define their permissions. For more information about policy types and uses, see [Policies and permissions in IAM](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html).

For details about the rest of the authentication and authorization process, see [Understanding how IAM works](https://docs.aws.amazon.com/IAM/latest/UserGuide/intro-structure.html).


      AccessManagement_Diagram
    

During authorization, the AWS enforcement code uses values from the [request context](https://docs.aws.amazon.com/IAM/latest/UserGuide/intro-structure.html#intro-structure-request) to check for matching policies and determine whether to allow or deny the request.

AWS checks each policy that applies to the context of the request. If a single policy denies the request, AWS denies the entire request and stops evaluating policies. This is called an *explicit deny*. Because requests are *denied by default*, IAM authorizes your request only if every part of your request is allowed by the applicable policies. The [evaluation logic](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html) for a request within a single account follows these rules:

* By default, all requests are implicitly denied. (Alternatively, by default, the AWS account root user has full access.)
* An explicit allow in an identity-based or resource-based policy overrides this default.
* If a permissions boundary, Organizations SCP, or session policy is present, it might override the allow with an implicit deny.
* An explicit deny in any policy overrides any allows.

After your request has been authenticated and authorized, AWS approves the request. If you need to make a request in a different account, a policy in the other account must allow you to access the resource. In addition, the IAM entity that you use to make the request must have an identity-based policy that allows the request.