

# AWS Security Checklist Report

## AWS Security Checklist - Athena

Item	Description
Limit access to Athena	Ensure that access to Athena is limited to only the necessary users and roles.
Use IAM policies to control access	Use IAM policies to control access to Athena resources.
Use encryption	Use encryption to protect sensitive data at rest and in transit.
Enable CloudTrail logging	Enable CloudTrail logging for Athena to track usage and changes to the service.
Enable VPC access	Enable VPC access for Athena to limit access to resources within your VPC.
Enable query result encryption	Enable query result encryption to protect sensitive data in query results.
Use AWS Glue to manage Athena data catalog	Use AWS Glue to manage the Athena data catalog and ensure that it is up-to-date and accurate.
Enable Amazon S3 server-side encryption	Enable Amazon S3 server-side encryption to protect data stored in S3 that is accessed by Athena.
Use parameterized queries	Use parameterized queries to protect against SQL injection attacks.