MongoDB®

Configuring MongoDB Atlas for Government for FedRAMP Compliance

Details and technical references to help comply with all FedRAMP Moderate requirements

August 2023

US 866-237-8815 • INTL +1-650-440-4474 • info@mongodb.com.

Table of Content

Introduction

The purpose of this whitepaper is to provide details and technical references for how MongoDB customers, such as Federal Agencies and ISVs, can use MongoDB Atlas for Government (US) to comply with all FedRAMP Moderate requirements.

What is MongoDB Atlas for Government?

MongoDB Atlas for Government (US) is a dedicated environment of MongoDB's multi-cloud, modern database, MongoDB Atlas, and is built for U.S. government requirements. Atlas for Government (US) has achieved a FedRAMP Moderate Authorization (see MongoDB Trust Center, FedRAMP Marketplace Listing). It allows customers to configure MongoDB deployments in AWS GovCloud regions as well as AWS US East/West regions. To maintain logical separation, customers cannot deploy clusters across AWS GovCloud and AWS US East/West in the same Atlas Project.

Similar to Atlas, this environment provides an integrated set of data and application services that share a unified developer experience and supports a wide range of use cases such as transactional workloads, time series data, search, and petabyte data storage. MongoDB Atlas for Government also has all the security capabilities of MongoDB Atlas. These capabilities include always-on authentication, authorization, encryption in transit and at rest, and no access to MongoDB deployments from the Internet by default. Additionally, MongoDB provides automated patching of the underlying infrastructure and MongoDB deployments with zero downtime. MongoDB Atlas for Government is architected to provide automated database resilience and mitigate the downtime risks associated with hardware failures or unintended actions.

Achieve FedRAMP Moderate Faster

The FedRAMP Moderate Control Implementation Summary (CIS) Workbook template has hundreds of controls and enhancements. Configuring a cloud provider in accordance with these controls can be a significant effort. MongoDB has strived to take the maximum burden of FedRAMP responsibilities, so customers can focus on application development and business requirements instead of on FedRAMP controls and enhancements. Specifically, customers are only responsible for configuring only 10% of the total FedRAMP controls and enhancements with minimal effort. If you would like to request a copy of the

Control Implementation Summary (CIS) /Customer Responsibility Matrix (CRM) for MongoDB Atlas for Government, please reach out to your MongoDB Account Team.

Definitions

The following are terms that are used throughout this document. Any capitalized terms that are not defined in this document have the meaning that will be provided in your MongoDB Atlas for Government Agreement.

1. **“Control Plane”** means the Atlas for Government UI or API that you use to manage their MongoDB deployments.

2. **"Customer Data"** means any data you or your end users upload into the data plane of MongoDB Atlas for Government.

3. **“Data Plane”** refers to your Atlas for Government MongoDB deployments.

4. **"MongoDB Atlas Deployment"** means each replica set or sharded cluster of data-bearing nodes running the MongoDB database software that is managed by MongoDB Atlas for Government, subject to your selected configurations.

MongoDB for FedRAMP Moderate CIS Tables

Customer Responsibilities Table

This table outlines controls along with relevant information and MongoDB links highlighting the actions that the customer's engineering team needs to take to achieve FedRAMP compliance using Atlas for Government.

Control	Customer Responsibility
AC-02 AC-03	You are responsible for managing user access and other account management activities for both the control plane and data plane: **For the control plane:** You can configure Federation Authentication using SAML. You are responsible for creating Project(s) to your Organization(s) within Atlas for Government and assigning Project and Organization roles to teams. You are responsible for creating Admin API keys and managing Atlas role assignment to these API keys. **For the data plane:** You are responsible for managing database users within a Project and assigning them built-in or custom database roles.
AC-06	Atlas for Government monitors your deployment out-of-the-box. You must configure your account to receive alerts for these monitoring in different systems.
AU-02	You are responsible for monitoring Project and Organization Activity Feed and Database Access History as well as enabling fine-grained database auditing and ingesting the database audit logs into your SIEM via API.
CA-03	Your Atlas for Government database deployments are in a dedicated VPC for your Atlas for Government Project. You can set up network connectivity with the database deployments via IP access lists, VPC peering, or Private Endpoint in order to meet the FedRAMP TIC 2.0 Architecture.
CP-06 CP-07 CP-09	You are responsible for enabling cloud backups for your database deployments during cluster creation or during the modification of an existing cluster, configuring backup policies, including frequency intervals, and duration of the retention.
IA-02 IA-04 IA-05 IA-07	You are responsible for enabling two-factor authentication for your account and configuring MFA for network access to non-privileged accounts. You are responsible for configuring disabling inactive accounts if you use MongoDB Federated Authentication.

	You are responsible for configuring users, rotating passwords, and implementing access controls on all instances of in-scope Atlas for Government services in the Control and Data Plane. If you are using your own identity provider, you are responsible for configuring password reuse. You are responsible for configuring authentication for data plane users using supported authentication types: **For human access:** we recommend that you use AWS-IAM or OpenID Connect. **For programmatic access:** we recommend that you use SCRAM, X.509, or AWS-IAM.
MA-04	You are responsible for authorizing direct access to resources within your Atlas for Government deployments for MongoDB personnel to perform maintenance and support activities.
RA-05	In regards to vulnerability scanning, which includes database scanning, you are responsible for: - Configuring network access - Checking appropriate TLS setting (default TLS is 1.2) - Configuring and managing database user authentication and authorization
SA-04	Agency customers who are required to use a hardware-based PIV card or CAC can integrate their card with the SSO capability using identity federation through SAML.
SC-02 **SC-07**	You are responsible for monitoring and controlling all network traffic for applications and VPCs that connect to your MongoDB-managed deployments in the Atlas for Government Data Plane from customer-managed application environments: - Manage established Private Endpoint or VPC Peering connections to your Atlas for Government deployments - Control access that has been established via IP Whitelisting - Configure resources within your environment to establish a one-way connection from your VPC to the Atlas for Government Data Plane using an AWS PrivateLink - Configure your firewalls to allow outbound access from your application environment to Atlas for Government. This will grant applications access to databases stored on Atlas for Government.
SC-04 **SC-06**	You are responsible for creating and destroying Atlas for Government deployments within your dedicated Atlas for Government Organization.

Optional Security Features Table

These are optional additional security configurations that are not needed for FedRAMP compliance, but they provide an additional level of security for your Atlas for Government deployments.

Control	Optional Customer Responsibility
AC-02 **AC-04**	Atlas for Government MongoDB database users can configure idle timeout using maxIdleTimeMS. If you use LDAP for authentication or authorization to database deployments: - You are responsible for configuring secure LDAP to allow network access from Atlas for Government deployments using public or private IPs, and ensuring that a public DNS hostname points to an IP that the Atlas for Government deployments can access - You are responsible for creating LDAP groups on your admin database and mapping LDAP groups to MongoDB roles on your Atlas for Government databases
SC-12 **SC-28**	Atlas for Government provides the ability to use an AWS KMS instance in your AWS account to encrypt and decrypt data stored in MongoDB's storage engine. The database storage engine encryption can be configured in addition to always-on encrypted volume encryption. MongoDB provides the optional ability to encrypt sensitive data fields in your application before you send it over the network to MongoDB using Client-Side Field Level Encryption (CSFLE). With CSFLE enabled, MongoDB deployment does not have access to your data in an unencrypted form. Your employees (DBAs) for Atlas for Government deployments also do not have access to the encrypted fields unless they have access to the encryption key.
CP-06 **CP-07** **CP-09**	Atlas for Government supports an optional Backup Compliance Policy that can be tailored to meet organizational requirements. When a Policy is enabled, no user, regardless of role, can modify the policy without MongoDB support involvement. You can download backups of your deployments into an S3 bucket that you manage. You can also configure your backups to be stored in a region other than the region of your deployment. AWS GovCloud backups can only be copied to other GovCloud regions.

MongoDB Default Controls Table

This table provides information on inherited controls for FedRAMP compliance.

Control	MongoDB Responsibility
AC-02 (03)	IDaaS solution utilized by MongoDB is configured to disable customer accounts after 90 days of inactivity.
AC-02 (07)	Built-in and user-defined roles can be leveraged by application users.
AC-11 AC-12	Customers are timed out of the Atlas for Government application after thirty (30) minutes of idle time.
AC-04	MongoDB provides always-on role-based access controls (RBAC) with predefined roles for both the control and data plane. MongoDB provides the ability to create custom roles for the data plane. MongoDB deployments in Atlas for Government are deployed in a dedicated VPC for an Atlas Project. This VPC is managed by MongoDB. This mechanism provides a level of network isolation among different tenants of Atlas for Government.
AU-02 AU-06	Account activity within an Atlas Organization is tracked in Project or Organization Activity Feed. This helps you determine what your users did within your Atlas Project and Organization.
CP-06 CP-07 CP-09	In addition to the backups for the entire information system that are retained by MongoDB, Atlas for Government also provides customers the ability to back up and restore data stored on Atlas deployments.
IA-02	MongoDB Atlas for Government provides single sign-on (SSO) integration options with both control and data plane, but it requires customer configuration. SSO via SAML 2.0 can be enabled to allow customer end users to sign in using Personal Identity Verification (PIV) card or Common Access Card (CAC) through the IDaaS solution to the web interface for Atlas. MongoDB personnel can also access the production environment through the Atlas UI. MongoDB Atlas for Government Organization Owners have the capability to require all MongoDB Atlas for Government users within their organization to enable multi-factor authentication for their account.
IA-04	MongoDB disables accounts that have been inactive for 90 days.
IA-05	MongoDB Atlas for Government prevents the reuse of the last twenty four (24) passwords for the users of MongoDB Atlas for Government control plane.
RA-05	MongoDB scans databases using a CIS benchmark to check for secure configuration.

SC-07	MongoDB maintains a running log of events, including entries such as incoming connections, commands run, and issues encountered.