Last updated on ***Jan 15, 2026***

Databricks on AWS GovCloud (FedRAMP High)

This page describes the Databricks on AWS GovCloud offering and its compliance controls.

AWS GovCloud overview

AWS GovCloud gives United States government customers and their partners the flexibility to architect secure cloud solutions that comply with the FedRAMP High baseline and other compliance regimes, including United States International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR). For details, see AWS GovCloud.

Databricks on AWS GovCloud provides the Databricks platform deployed in AWS GovCloud with compliance and security controls. Databricks on AWS GovCloud is operated exclusively by US citizens on US soil.

Databricks on AWS GovCloud consists of two distinct Databricks environments:

- Databricks for AWS GovCloud: For customers that are not Department of Defense (DoD) agencies with FedRAMP High and Impact Level 5 (IL5) requirements.
- Databricks for AWS GovCloud DoD: For DoD agencies with IL5 requirements. This environment is connected to the Non-classified Internet Protocol Router Network (NIPRNet).

NOTE

The Databricks GovCloud Help Center is where you submit and manage support cases. Go to https://help.databricks.us/s/. Do not share any export-controlled data regarding support cases through channels other than the Databricks GovCloud Help Center. For more information on support, see Support.

When a Databricks on AWS GovCloud account is provisioned, the account owner receives an email with a short-lived login URL.

Compliance security profile

The compliance security profile is enabled on all Databricks on AWS GovCloud workspaces by default. The compliance security profile has additional monitoring, enforced instance types for inter-node encryption, a hardened compute image, and other features that help meet the requirements of FedRAMP High compliance. Automatic cluster update and enhanced security monitoring are also automatically enabled.

The compliance security profile enforces the use of AWS Nitro instance types that provide both hardware-implemented network encryption between cluster nodes and encryption at rest for local disks in cluster and Databricks SQL SQL warehouses. Fleet instances are not available in AWS Gov Cloud. The supported instance types are:

- **General purpose:** `M5dn`, `M5n`, `M5zn`, `M6i`, `M7i`, `M6id`, `M6in`, `M6idn`
- **Compute optimized:** `C5a`, `C5ad`, `C5n`, `C6i`, `C6id`, `C7i`, `C6in`
- **Memory optimized:** `R6i`, `R7i`, `R7iz`, `R6id`, `R6in`, `R6idn`
- **Storage optimized:** `D3`, `D3en`, `P3dn`, `R5dn`, `R5n`, `I4i`, `I3en`
- **Accelerated computing:** `G4dn`, `G5`, `P4d`, `P4de`, `P5`

For more information on the compliance security profile, see Compliance security profile.

FedRAMP High compliance

The FedRAMP High authorization status of Databricks on AWS GovCloud is **Authorized**.

Customers are responsible for implementing and operating applicable FedRAMP HIGH compliance controls as documented in the **Control Implementation Summary / Customer Responsibility Matrix** in SSP Appendix J of the Databricks FedRAMP authorization documentation package. US Government agencies can obtain access to the Databricks FedRAMP High authorization documentation through the FedRAMP package access request form. Follow the instructions on the Databricks FedRAMP Marketplace listing (package ID: FR2324740262).

DoD IL5 compliance

Databricks for AWS GovCloud DoD provides Department of Defense (DoD) agencies with FedRAMP High and Impact Level 5 (IL5). AWS GovCloud DoD is a completely separate environment from other Databricks environments. To onboard to AWS GovCloud DoD, contact your Databricks account team.

Requirements

You must configure the following on Databricks on AWS GovCloud and AWS GovCloud DoD workspaces:

- Single sign-on authentication, see Configure SSO in Databricks
- PrivateLink for both back-end and front-end connections, see Enable private connectivity using AWS PrivateLink.
- You are solely responsible for verifying that sensitive information is never entered in customer-defined input fields, such as workspace names, compute resource names, tags, job names, job run names, network names, credential names, storage account names, and Git repository IDs or URLs. These fields might be stored, processed, or accessed outside the compliance boundary.

Databricks for AWS GovCloud region and URLs

The Databricks AWS account ID for Databricks on AWS GovCloud is `044793339203` and the account ID for Databricks for AWS GovCloud DoD is `170661010020`. The account ID is required to create and configure a cross-account IAM role for Databricks workspace deployment. See Create a credential configuration.

Databricks on AWS GovCloud and AWS GovCloud DoD workspaces are in the `us-gov-west-1` region. For region information, see Databricks clouds and regions.

Databricks on AWS GovCloud and AWS GovCloud DoD URLs differ from Databricks URLs on the commercial offering. Use the following URLs for Databricks on AWS GovCloud:

- Account console URL and base URL for rest APIs: `https://accounts.cloud.databricks.us/`
- Workspace URL and base URL for workspace-level REST APIs: `https://<deployment-name>.cloud.databricks.us/`

  For example, if the deployment name you specified during workspace creation is `ABCSales`, your workspace URL is `https://abcsales.cloud.databricks.com.us`.

Use the following URLs for Databricks on AWS GovCloud DOD:

- Account console URL and base URL for rest APIs: `https://accounts-dod.cloud.databricks.mil/`
- Workspace URL and base URL for workspace-level REST APIs: `https://<deployment-name>.cloud.databricks.mil/`

  For example, if the deployment name you specified during workspace creation is `ABCSales`, your workspace URL is `https://abcsales.cloud.databricks.com.us`.

For terraform deployments, see Security Reference Architectures (SRA) - Terraform Templates.

Feature availability

Notable features that are supported:

- Unity Catalog
- Databricks Runtime latest versions and LTS versions
- Databricks SQL
- Dashboards
- MLflow experiments
- OAuth authentication
- Genie
- Databricks Assistant
- Foundation Model APIs pay-per-token support with Claude Sonnet 4.5

Supported preview features

Only the preview features listed in this section are supported for processing data regulated in Databricks on AWS GovCloud. All other preview features are not supported.

- Unity Catalog attribute-based access control (Public Preview)
- Serverless SQL warehouses (Public Preview in Databricks for AWS GovCloud and Beta in Databricks for AWS GovCloud DoD). See What are Serverless SQL warehouses?.
- Serverless compute for notebooks, jobs, and Lakeflow Spark Declarative Pipelines (Public Preview). See Connect to serverless compute.
- Serverless egress control (Beta)

> **NOTE**
>
> You can enable the serverless compute for notebooks, jobs, and Lakeflow Spark Declarative Pipelines Public Preview in **Settings > Feature enablement** in the account console. See Serverless SQL warehouses

Supported system tables

The following system tables are available in Databricks on AWS GovCloud for monitoring, governance, and cost management:

- **system.access schema**: `audit`, `column_lineage`, `outbound_network`, `table_lineage`
- **system.billing schema**: All tables
- **system.compute schema**: `clusters`, `job_run_timeline`, `job_task_run_timeline`, `job_tasks`, `jobs`, `node_timeline`, `node_types`, `pipeline_update_timeline`, `pipelines`, `warehouse_events`, `warehouses`
- **system.query schema**: `history`
- **system.serving**: All tables

For more information about system tables, see Monitor account activity with system tables.

Unsupported features

- In-product messaging
- Databricks Marketplace
- Partner Connect

- Compute metrics
- In-product support ticket submission
- HTML notebook export
- Managed Apache Iceberg
- AI Gateway-enabled inference tables and the `ai_query` function.

Delta Sharing support

Databricks-to-Databricks Delta Sharing is only supported within the same environment type: commercial-to-commercial, GovCloud-to-GovCloud, DoD-to-DoD, or Azure China-to-Azure China. For details on supported sharing scenarios, see Databricks-to-Databricks Delta Sharing support matrix for cloud environments.

The Delta Sharing open sharing protocol is supported between cloud environment types, for example from AWS commercial clouds to AWS GovCloud or Azure China.