Administrator Guide

Amazon SageMaker Unified Studio

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon SageMaker Unified Studio: Administrator Guide

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is Amazon SageMaker Unified Studio? ... 1
How does it work? ... 1
Terminology and concepts ... 2
Prerequisites ... 16
Setting up ... 17
Sign up for an AWS account ... 17
Supported Regions ... 18
Domains ... 19
Identity Center-based domains ... 20
Create a Amazon SageMaker Unified Studio domain - quick setup ... 20
Create a Amazon SageMaker Unified Studio domain - manual setup ... 22
Create an Amazon DataZone domain ... 23
Domain administration for Identity Center-based domains ... 24
Edit domains ... 34
Delete domains ... 35
Upgrade Amazon DataZone domains to Amazon SageMaker unified domains ... 35
Trusted identity propagation ... 38
IAM-based domains and projects ... 40
Overview of IAM-based domains ... 41
Set up IAM-based domains in Amazon SageMaker Unified Studio ... 43
Manage data encryption in IAM-based domains ... 50
Access the Domain Administration Page ... 60
Set up single sign-on for IAM-based domains ... 61
Manage Projects from Domain Administration ... 62
Configure Domain Settings ... 63
Projects in IAM-based domains ... 64
VPC networking ... 71
Network settings ... 71
Prerequisites ... 72
Add VPC ... 72
Update VPC configuration and projects ... 73
Update VPC ... 73
Update project with VPC configuration ... 74
View VPC networking details ... 74

View VPC configuration ... 74
Domain units and authorization policies ... 76
Create domain units ... 77
Edit domain units ... 77
Delete domain units ... 78
Manage domain unit owners ... 78
Assign authorization policies to users and groups within a domain unit ... 79
Assign authorization policies to projects within a domain unit ... 80
Assign authorization policies to asset types ... 81
User management ... 82
User profiles ... 82
Group profiles ... 83
Managing users for Identity Center-based domains ... 84
Enable IAM Identity Center ... 85
Enable SAML ... 86
Update Root Domain Unit Owner ... 87
Managing users for IAM-based domains ... 88
Viewing and filtering users ... 88
Adding a user ... 88
Editing a user ... 89
Associated accounts ... 90
Request association with other AWS accounts ... 90
Accept an account association request from an Amazon SageMaker Unified Studio domain and enable an environment blueprint ... 91
Reject an account association request from an Amazon SageMaker Unified Studio domain ... 92
Remove an associated account in Amazon SageMaker Unified Studio ... 92
Configure Amazon Bedrock in SageMaker Unified Studio in an associated account ... 93
Local IDE Support ... 96
Key Concepts ... 96
Configuring Amazon SageMaker Unified Studio for Remote Access ... 96
Prerequisites ... 16
Network Configuration for Remote Access ... 99
Source control and file storage ... 102
Storage options ... 102
S3 shared storage ... 103
Repositories ... 103

Default S3 storage 103
Access model 103
Enabling S3 bucket versioning 103
Next steps 103
Git connections 104
Account requirements 104
Creating a connection 104
Connection tagging 105
Supported providers 105
Creating a GitHub connection 105
Creating a GitHub Enterprise Server connection 106
Creating a GitLab connection 107
Creating a GitLab self-managed connection 108
Creating a Bitbucket connection 109
Enabling a connection for project access 109
Disabling or deleting a connection 110
Cross-account and cross-region Git configurations 111
RAM permission version 111
IAM permissions 111
Cross-region support 112
Legacy experience and migration 112
Legacy experience 113
Migrating to the new repository experience 122
Project profiles 124
All capabilities project profile 124
Configure all capabilities for your Amazon SageMaker unified domain 125
Create an All capabilities project profile 127
Generative AI application development project profile 130
Configure Amazon Bedrock in SageMaker Unified Studio for your domain 130
Create a generative AI application development project profile 135
SQL analytics project profile 137
Configure SQL analytics for your Amazon SageMaker unified domain 137
Create a SQL analytics project profile 139
Custom project profile 141
Update project profiles 143
Disable or enable project profiles 144

Delete project profiles ... 144
Edit blueprint deployment settings ... 145
Add blueprint deployment settings ... 146
Project resource tags ... 147
IAM permissions for project resource tags ... 147
Configure project resource tags ... 150
Update project resource tags ... 151
Update the project ... 151
Delete project resource tags ... 152
Blueprints ... 154
Supported blueprints ... 154
Custom blueprints ... 159
Register a custom blueprint in the console ... 160
Register a custom blueprint with the API ... 161
Reserved parameters ... 162
Trust policy for the provisioning role ... 165
Sample template ... 166
Enable or disable blueprints ... 171
Specify PEM certificate for EmrOnEc2 blueprint ... 171
Getting started with Amazon EMR on EKS ... 172
Configure project profiles in Amazon SageMaker Unified Studio for Amazon EMR on EKS ... 173
Enable Amazon EKS cluster access for Amazon EMR on EKS and Amazon SageMaker Unified Studio ... 174
Enable cross-account access using associated domains ... 177
Enable cross-network access using VPC peering connections ... 178
Configuring monitoring with Spark History Server ... 179
Configuring fine-grained access controls ... 180
Configuring trusted identity propagation ... 180
Configuring user background sessions ... 181
Manage blueprint authorization ... 182
Tooling blueprints ... 182
Custom blueprints as Tooling ... 185
Tooling capabilities ... 199
Managed blueprint compatibility ... 220
Enable Tooling blueprint ... 221

Manage Tooling blueprint parameters ... 223
Configure Tooling blueprint parameters ... 223
Configure IAM permissions boundaries ... 225
Modify the OnDemandWorkflows blueprint for creating workflow environments in a shared VPC ... 227
Account pools ... 229
Considerations ... 229
Use cases ... 230
Create an account pool ... 230
Create an account pool with a custom handler source ... 231
Create an account pool with a static list of account and region pairs ... 233
View an account pool ... 234
List account pools for a domain ... 235
View the list of accounts in an account pool ... 236
Delete an account pool ... 237
Create a project profile with an account pool ... 237
Create a project profile with an account pool (Console) ... 238
Create a project profile with an account pool (CLI) ... 238
Onboarding data ... 240
Generative AI assistance ... 242
Amazon Q ... 242
Disable Amazon Q ... 242
SageMaker Data Agent ... 243
Disable the SageMaker Data Agent ... 243
Amazon Bedrock in SageMaker Unified Studio ... 246
Configure access to your Amazon Bedrock serverless models for the selected AWS accounts and regions ... 248
Set default models for the generative AI playgrounds in Amazon SageMaker Unified Studio . 249
Publishing models from associated accounts ... 250
Amazon Quicksight in SageMaker Unified Studio ... 251
Security ... 255
Identity and access management ... 256
Audience ... 257
Authenticating with identities ... 257
Managing access using policies ... 258
How Amazon SageMaker Unified Studio works with IAM ... 260

Identity-based policy examples ... 265
AWS managed policies ... 268
IAM roles for Amazon SageMaker Unified Studio ... 341
Access control patterns Amazon SageMaker Unified Studio ... 350
Troubleshooting ... 357
Data protection ... 359
KMS Permissions for resources provisioned by Amazon SageMaker Unified Studio ... 360
KMS permissions for exporting asset metadata in Amazon SageMaker Unified Studio ... 365
Amazon Bedrock in SageMaker Unified Studio KMS Permissions ... 369
Authorization in Amazon SageMaker Unified Studio ... 377
Authorization in the Amazon SageMaker Unified Studio console ... 377
Authorization in Amazon SageMaker Unified Studio ... 377
Amazon SageMaker Unified Studio profiles and roles ... 378
Compliance validation ... 378
Compliance programs ... 378
Security Best Practices ... 379
Implement least privilege access ... 379
Use IAM roles ... 380
Implement Server-Side Encryption in Dependent Resources ... 380
Use CloudTrail to Monitor API Calls ... 380
Resilience ... 380
Infrastructure Security ... 381
Network isolation ... 381
Prerequisites ... 381
Restrict Amazon SageMaker Unified Studio network traffic to within the AWS network ... 382
Public internet access ... 389
Amazon VPC troubleshooting ... 393
Configuration and vulnerability analysis in for Amazon SageMaker Unified Studio ... 398
Cross-service confused deputy prevention ... 399
Quotas and limits ... 400
Resource quotas ... 400
Amazon DataZone quotas ... 400
Amazon DataZone API rate limits ... 401
Document history ... 403

What is Amazon SageMaker Unified Studio?

As a part of the next generation of Amazon SageMaker, Amazon SageMaker Unified Studio is a unified development experience that brings together AWS data, analytics, artificial intelligence (AI), and machine learning (ML) services. It provides a place to build, deploy, execute, and monitor workflows from a single interface. This helps drive collaboration across teams and facilitate agile development.

In Amazon SageMaker Unified Studio, administrators manage the users and groups that can access Amazon SageMaker Unified Studio, and they set up resources for teams to use. When your administrator grants you access to Amazon SageMaker Unified Studio, you can contribute to Amazon SageMaker Unified Studio projects. Within Amazon SageMaker Unified Studio projects, you can collaborate on business use cases by creating and sharing data, computation work, and other resources.

This guide provides information for Amazon SageMaker Unified Studio administrators on using the Amazon SageMaker management console to set up resources in Amazon SageMaker Unified Studio and on managing users and groups and their access to Amazon SageMaker Unified Studio and its configured resources.

For more information about the user experience and flow of using projects to create and share data, perform computation work, and complete other tasks, see the Amazon SageMaker Unified Studio User Guide.

Administrators can also configure Amazon SageMaker Unified Studio programmatically by invoking the HTTPS APIs.

How does it work?

Amazon SageMaker Unified Studio administrators can use the Amazon SageMaker management console to configure and customize the following Amazon SageMaker Unified Studio capabilities:

- Data analytics, machine learning, SQL, and generative AI
- Data and AI governance
- Generative AI app development using Amazon Bedrock serverless models
- Amazon Q
- Authentication via AWS IAM, AWS IAM Identity Center, or SAML

Amazon SageMaker Unified Studio terminology and concepts

As you get started with Amazon SageMaker Unified Studio, it is important that you understand its key concepts, terminology, and components.

Amazon SageMaker Unified Studio

This is a browser-based web application where you can use all your data and tools for analytics and AI. Amazon SageMaker Unified Studio can authenticate you with your IAM user credentials or with credentials from your identity provider through the AWS IAM Identity Center or with your SAML credentials. You can obtain the Amazon SageMaker Unified Studio URL for you domains by accessing the Amazon SageMaker management console at https://console.aws.amazon.com/datazone.

Amazon SageMaker management console

You can use the Amazon SageMaker management console at https://console.aws.amazon.com/datazone to access and configure your domains for user management, account associations, project profiles, blueprints, Amazon Bedrock models, Git connections, and Amazon Q usage.

Amazon Bedrock in SageMaker Unified Studio

Amazon Bedrock in SageMaker Unified Studio in Amazon SageMaker Unified Studio enables you to easily build and scale generative AI applications. Amazon Bedrock in SageMaker Unified Studio provides a web interface that allow users to interact with Amazon Bedrock foundation models and use Amazon Bedrock tools, such as Agents, Guardrails, Prompts, Flows, Evaluation, and Functions in a seamless unified fashion. Users can interact with models in a generative AI playground or collaborate on developing generative AI applications in projects. For more information, see Amazon Bedrock in SageMaker Unified Studio.

Amazon Q

Amazon Q Developer is an AI coding assistant that can chat about code, provide inline code completions, generate net new code, scan your code for security vulnerabilities, and make code upgrades and improvements. For more information, see Generative AI assistance in Amazon SageMaker Unified Studio.

In the current release of Amazon SageMaker Unified Studio, by default, all users of an Amazon SageMaker Unified Studio domain have access to the Free Tier release of Amazon Q.

Amazon SageMaker lakehouse architecture

Amazon SageMaker Lakehouse unifies your data across Amazon S3 data lakes and Amazon Redshift data warehouses. Amazon SageMaker Lakehouse helps you build powerful analytics, machine learning (ML), and generative AI applications on a single copy of data.

Amazon SageMaker Lakehouse is accessible via Amazon SageMaker Unified Studio.

Amazon SageMaker Data Processing Visual ETL

Amazon SageMaker Unified Studio allows you to author highly scalable extract, transform, load (ETL) data integration flows for distributed processing without becoming an Apache Spark expert. You can define your data integration flow in the simple visual interface and Amazon SageMaker Unified Studio automatically generates the code to move and transform your data. The code is generated in Python and written for Apache Spark. Additionally, you can choose to author your visual flows in English using generative AI prompts from Amazon Q.

Asset

In Amazon SageMaker Unified Studio, an asset is an entity that presents a single physical data object (for examples, a table, a dashboard, a file) or virtual data object (for example, a view).

Asset type

Asset types define how assets are represented in the Amazon SageMaker catalog. An asset type defines the schema for a specific type of asset. When assets are created, they are validated against the schema defined by their asset type (by default, the latest version). When an asset update occurs, Amazon SageMaker Unified Studio creates a new asset version and enables Amazon SageMaker Unified Studio users to operate on all asset versions.

Associated accounts

Account association in Amazon SageMaker Unified Studio enables you to publish data from other AWS accounts into the Amazon SageMaker catalog and create projects to work with data across multiple AWS accounts. Account association requests are initiated from AWS accounts from which Amazon SageMaker unified root domains are created. You can request association from the Amazon SageMaker management console. Account association requests must be accepted by the administrators of the AWS accounts invited for account association. You can authorize the domain account to use data or allow infrastructure deployment with the right IAM permissions as part of approval. Once an associated account is linked to a domain, projects in Amazon SageMaker Unified Studio can use resources from those accounts and also other types

of assets. You can deploy resources in specific AWS accounts through project profiles. For more information, see Associated accounts in Amazon SageMaker Unified Studio.

Authorization policy

Authorization policies are a set of controls within Amazon SageMaker Unified Studio applied to entities such as projects, blueprints, environments, glossary, and metadata forms.

Within an Amazon SageMaker Unified Studio domain unit, you can assign the following authorization policies to your users and groups to grant them specific permissions:

- Domain unit creation policy
- Project creation policy
- Project membership policy
- Domain unit ownership assumption policy
- Project ownership assumption policy

Within an Amazon SageMaker Unified Studio domain unit, you can assign the following authorization policies to your projects to grant them specific permissions:

- Glossary creation policy
- Metadata forms creation policy
- Custom asset type creation policy

Within a specific blueprint configuration, you can assign the following authorization policies to projects and domain unit owners:

- Create environment profiles using this blueprint - this policy can be assigned to Amazon SageMaker Unified Studio projects and it authorizes them to create environment profiles using this blueprint.
- Grant permissions to create environment profiles using this blueprint - this policy can be assigned to domain unit owners and it authorizes them to grant permissions to projects to create environment profiles using this blueprint.

AWS account owner

In Amazon SageMaker Unified Studio, AWS account owners create roles, policies, and permissions in their AWS accounts that enable these AWS accounts to be associated with Amazon SageMaker Unified Studio domains. For more information, see Managing users in Amazon SageMaker Unified Studio.

Blueprint

A blueprint with which the project profile is created defines what AWS tools and services members of the project to which the project profile belongs can use as they work with data in the Amazon SageMaker catalog. For more information, see Blueprints in Amazon SageMaker Unified Studio.

In the current release of Amazon SageMaker Unified Studio the following default blueprints are supported:

Blueprint name	Description	Resources created
AmazonBedrockGenerativeAI	This is the combined Amazon Bedrock blueprint which contains seven sub-Amazon Bedrock blueprint s. It enables users to build generative AI applications using tools such as Agents, Knowledge Bases, Guardrail s, Flows, Functions, and Model Evaluation.	
AmazonBedrockChatAgent	Provides a reusable AWS CloudFormation template to create an Amazon Bedrock Agent and supportin g resources, including an execution role and a consumption role.	Bedrock Agent, Bedrock Agent Execution role, Bedrock Agent Consumption role
AmazonBedrockEvaluation	Creates one IAM role as the service role for an Amazon Bedrock evaluation job.	Bedrock Evaluation job execution role
AmazonBedrockFlow	Provides a reusable AWS CloudFormation template to create an Amazon Bedrock	Amazon Bedrock Flow, Amazon Bedrock Flow Execution role

Blueprint name	Description	Resources created
	Prompt Flow and supportin g resources such as an execution role.	
AmazonBedrockFunction	Provides a reusable AWS CloudFormation template to create an AWS Lamda function and supportin g resources, such as an execution role, and a secret manager.	Secrets Manager secret, AWS Lambda function, AWS Lambda function execution role, Log group
AmazonBedrockGuardrail	Provides an AWS CloudForm ation template to create an Amazon Bedrock Guardrail and supporting resources such as an execution role.	Amazon Bedrock Guardrail
AmazonBedrockKnowl edgeBase	Provides an AWS CloudForm ation template to create a reusable Amazon Bedrock Knowledge Base and supporting resources such as an execution role.	Amazon Bedrock Knowledge Base, OpenSearch Serverless collection, Amazon Bedrock Knowledge Base Execution role, AWS Lambdas, including OpenSearch Index Lambda and KB Ingestion Trigger Lambda, AWS Lambda Execution role, Amazon Bedrock Knowledge Base data source

Blueprint name	Description	Resources created
AmazonBedrockPrompt	Provides a reusable AWS CloudFormation template to create an Amazon Bedrock Prompt and supportin g resources, such as an execution role, and a consumption role.	Amazon Bedrock Prompt, Amazon Bedrock Prompt Consumption role
LakeHouseDatabase	Provides a reusable AWS CloudFormation template to create a data lake environme nt with a AWS Glue database for data management and an Amazon Athena workgroup for querying data.	AWS Glue databases, lake formation permissions, Amazon Athena workgroups
EMRonEC2	Provides a reusable AWS CloudFormation template to create an Amazon EMR on EC2 cluster to run and scale Apache Spark, Hive, and other big data workloads. For more information about enabling this blueprint see, Specify PEM certificate for EmrOnEc2 blueprint	EMR on EC2 clusters
EMRServerless	Provides a reusable AWS CloudFormation template to create an Amazon EMR Serverless application that is ready to serve Apache Spark batch jobs and interactive sessions.	EMR on Serverless applicati ons

Blueprint name	Description	Resources created
LakehouseCatalog	Provisions a new catalog in the Amazon SageMaker Lakehouse that is backed by Amazon Redshift Managed Storage	
MLExperiments	Provides OnDemand blueprint to enable MLflow tracking server for the experimentation inside a project.	MLflow tracking server (on demand)
PartnerApps	Creates an IAM role and a Connection that enables access to Partner AI Apps. Through Partner AI Apps you can leverage integrate d and fully-managed thrid-party solutions for AI/Ml development.	Amazon SageMaker Partner AI Apps IAM role, Amazon SageMaker Partner AI Apps Connection
RedshiftServerless	Provides a reusable AWS CloudFormation template to create an Amazon Redshift Serverless environment to get insights from data without managing infrastru cture.	Amazon Redshift Serverless warehouses
Tooling	Creates resources for the project, including IAM user roles, security groups, and Amazon SageMaker unified domains.	IAM user roles, Amazon SageMaker unified domains, security groups

Blueprint name	Description	Resources created
Workflows	Provides an AWS CloudFormation template to create the MWAA environment for Airflow based Workflows	Enables project workflows on MWAA

Business data catalog

This is a catalog of all the published assets from various projects. The scope of the business data catalog is the domain therefore published assets are discoverable by all projects in that domain. Business data catalog enables discovery that crosses the account and region boundary. Assets can be published to the business data catalog and subsequently be subscribed to as well. Every asset that lives in the business data catalog has an owner project (also known as the producer project) which controls policies around how subscriptions can be fulfilled. A subscriber (also known as a consumer project) is able to make a request to the owner project to gain access to the asset. Once the request is approved, the owner project provides the necessary permissions to subscriber project so that it may gain access to that asset.

Business glossary

In Amazon SageMaker Unified Studio, a business glossary is a collection of business terms that may be associated with assets. A business glossary helps ensure that the same terms and definitions are used across an organization throughout its various data analytics tasks. The terms in a business glossary can be added to assets and columns to classify or enhance the identification of those attributes during search. Glossary can be selected as the value type for a field in a metadata form that is associated with an asset. When a particular term is selected as the value for an asset's metadata form field, users can search for the business glossary term and find the associated assets.

Git connection

Git connections enable you to check in and check out files, and manage your code repository. When you create an Amazon SageMaker unified domain, a default git connection to CodeCommit is provided for you to manage your code. You can also create and enable new 3P Git connections to GitHub, GitHub Enterprise Server, GitLab, and GitLab Self-Managed. For more information, see Creating a GitHub connection.

When you enable a Git connection, all users who can sign in to any domain in the account have read and write access to all repositories on that connection. This access applies regardless of the user's project membership or permission level. To enforce isolation between repositories, use separate AWS accounts.

Data source

An entity which brings in metadata from a source and adds metadata forms (e.g. ingestion job). This entity allows publishers to capture ingestion configuration including what metadata forms to attach, whether to run BNG, etc. Since this configuration has a 1 to many mapping with the credentials provided by the publisher, we believe that it should be captured in a separate entity.

In Amazon SageMaker Unified Studio, you can use data sources to import technical metadata of assets (data) from the source databases or data warehouses into Amazon SageMaker Unified Studio. In the current release of Amazon SageMaker Unified Studio, you can create and run data sources for AWS Glue and Amazon Redshift. By creating a data source, you establish a connection between Amazon SageMaker Unified Studio and the source (AWS Glue Data Catalog or Amazon Redshift Warehouse) which enables you to read technical metadata, including tables names, columns names, and data types. By creating a data source you also kick off the initial data source run that creates new or updates existing assets in Amazon SageMaker Unified Studio. While creating a data source or after the data source is successfully created, you also have the option to specify a schedule for your data source runs.

Data source run

In Amazon SageMaker Unified Studio, a data source run is a task that Amazon SageMaker Unified Studio performs in order to create assets in project inventories and also optionally to publish project inventory assets to the Amazon SageMaker catalog. Data source runs can be automated (kicked off when a data source is initially created) or scheduled or manual. Data selection criteria enables you to fine-tune the existing and future data sets to be ingested into project inventories or the Amazon SageMaker catalog and the frequency of metadata updates to those inventory or catalog assets.

Domain

In Amazon SageMaker Unified Studio, a domain is the organizing entity for connecting together your assets, users, and their projects. With Amazon SageMaker unified domains, you have the flexibility to reflect the data and analytics needs of your organizational structure, whether it's creating a single Amazon SageMaker unified domain for your enterprise or multiple domains for different business units. For more information, see Domains in Amazon SageMaker Unified Studio.

Domain administrator

The IAM principal ID that has the super administrative permissions to edit entities in the domain.

In Amazon SageMaker Unified Studio, an IAM principal who creates an Amazon SageMaker Unified Studio domain is the default domain administrator of that domain. Domain administrators in Amazon SageMaker Unified Studio perform key functionalities for the domain, including creating domains, assigning other domain administrators, creating and managing project profiles, configuring blueprints, user management, account associations, Amazon Bedrock models, Git connections, and Amazon Q.

Domain unit

Domain units enable you to easily organize your assets and other domain entities under specific business units and teams. To set up secure and efficient data sharing within and across business units of your organization, you can create domain units within Amazon SageMaker Unified Studio and enable selected users within each business unit to login and share their assets to the catalog. Domain units can also be used to enable resource owners, such as AWS account owners, to set up Amazon SageMaker Unified Studio authorization permissions on their resources. Domain units provide a delegated authority from account owners to domain unit owners and they can set up authorization permissions on behalf of account owners.

JupyterLab

Amazon SageMaker Unified Studio provides a JupyterLab interactive development environment (in SageMaker Unified Studio) for you to use as you perform data integration, analytics, or machine learning in your projects. JupyterLab IDE is built on JupyterLab spaces and Amazon SageMaker Distribution.

Metadata form type

A metadata form type is a template that defines the metadata that is collected and saved when assets are created as inventory or published in an Amazon SageMaker unified domain. Metadata form types can be associated with a data asset. Metadata form types help domain administrators to define metadata forms needed for that domain such as compliance information, regulation information, or classifications. It enables domain administrators to customize additional metadata for their assets. Amazon SageMaker Unified Studio has system metadata form types such as asset-common-details-form-type, column-business-metadata-form-type, glue-table-form-type, glue-view-form-type, redshift-table-form-type, redshift-view-

form-type, s3-object-collection-form-type, subscription-terms-form-type, and suggestion-form-type.

Metadata form

In Amazon SageMaker Unified Studio, metadata forms define the metadata that is collected and saved when assets are created as inventory or published in an Amazon SageMaker unified domain. Metadata form definitions are created in the catalog domain by a domain administrator. A metadata form definition is composed of one or more field definitions, with support for boolean, date, decimal, integer, string, and business glossary field value data types. A domain administrator applies a metadata form to assets in their domain by adding the metadata form to their domain. Asset publishers then provide any optional and required field values in the metadata form.

Project profile

In Amazon SageMaker Unified Studio, a project profile defines an uber template for projects in your Amazon SageMaker unified domains. A project profile is a collection of blueprints which are configurations used to create projects. A project profile can define if a particular blueprint is enabled during the creation of the project, or available later for the project users to enable on-demand. For more information, see Project profiles in Amazon SageMaker Unified Studio.

You must be an administrator of a Amazon SageMaker Unified Studio domain to create and manage project profiles. In the current release of Amazon SageMaker Unified Studio, you can create the following project profiles:

- All capabilities project profile
- SQL analytics project profile
- Generative AI application development project profile
- Custom project profile

Projects in Identity Center-based domains

The project entity is the mechanism by which Amazon SageMaker Unified Studio users organize their work and provide business context over the jobs they are performing. A project is a container for all the users code including notebooks, queries, dashboards, workflows etc. A project provides three capabilities: 1) business context for the user's work which provides a level of audit to the functionality being performed, 2) collaboration boundary where the users can work with each other by interacting with the project's source control repository and 3) a permission boundary which gives users access to all the project artifacts and data/compute permissions once the users are added to the project. A project exists within a domain. A single

Amazon SageMaker unified domain can have several projects and each user can be added to multiple projects.

Each project is created using a template called project profile which is enabled by an administrator during the setup phase. A project profile controls the tools available within the project. Project members can request access to assets from the business data catalog and produce new artifacts using one or more of the tools available inside the project. Artifacts in a project are not accessible outside of the project unless they are published to the business data catalog which is discussed later.

Each project has one or multiple owners, who can add or remove other users (called Project Members) as owners or contributors and can modify or delete projects. Other restrictions on contributors can be defined with policies. When a user creates a project, they become the first owner of that project.

Project S3

The purpose of the project S3 path in Amazon SageMaker Unified Studio is to provide a secure, project-isolated location for storing temporary execution data and other project-related artifacts. The project S3 path follows a standardized structure of "<bucket>/<domain_id>/<project_id>/<project_scope>/" to ensure separation between projects and prevent objects from being shared across projects. The project S3 path is also used to store specific types of data, such as the location for the provisioned consumer AWS Glue database, Athena Workgroup output, and temporary storage for individual workflow runs.

Project Git repository

A project includes a dedicated git repository which serves as a central hub for users to manage version control for the code associated with their Amazon SageMaker Unified Studio projects. This enables collaboration across users within a project. All tools that generate file-based assets must use the project git repository for version control, e.g. Query Editor, JupyterLab in SageMaker Unified Studio, etc. By default, Amazon SageMaker Unified Studio uses AWS CodeCommit as the project's repository which is created when a project is created. However, administrators can modify this to connect a third-party Git repository such as Github, Github Enterprise Server, GitLab, and BitBucket instead of the default repository.

> **Note**
>
> You can't create new projects with AWS CodeCommit. Existing projects that were created using CodeCommit will continue to work.

Project member

A project member is any user who has been added to a project and given access to the project data and resources. Users can be enterprise users sourced from the IDP or IAM Principals from one of the domain associated accounts. Project owners can add members either by adding them directly or by selecting enterprise groups. A project member is added to a project with a designation that defines the set of permissions it has within the project. Users can collaborate on various activities such as accessing data assets, performing data analysis or machine learning activities.

Subscription request

A request to use a data product.

In Amazon SageMaker Unified Studio, a subscription request is a process that an Amazon SageMaker Unified Studio project must follow in order to be granted access to a specific asset. Subscription requests can be approved, rejected, revoked, or granted.

Subscription grant

An object representing a fulfilled request for a particular project.

Querybook

Querybooks allow you to develop, run, and share multiple SQL queries in a single interactive notebook. They provide an environment for data scientists, analysts, and developers to query, analyze, and visualize data using Amazon Redshift or Amazon Athena as the query engine. Cells in a Querybook contain SQL statements or markdown and can be run individually, like a traditional query editor, or sequentially. Query results appear in-line with each cell, where you can toggle between multiple results and create data visualizations. To accelerate query development, Querybooks integrate with Amazon Q to generate SQL queries from natural language input, and provide auto-complete suggestions for table names, column names, and SQL keywords as you type. Amazon SageMaker Unified Studio automatically saves your work as you progress. When ready, you can publish your Querybook to your project for collaboration with teammates.

Space

A space in Amazon SageMaker Unified Studio refers to a personalized workspace that provides an isolated, sandboxed environment for users to run arbitrary code without interfering with other workers in a project. Each space consists of a compute instance, an EBS volume, and the JupyterLab application. Users can access their spaces through various entry points in Amazon

SageMaker Unified Studio, the developer tools section, or by clicking on Notebook files. The project Git repository is cloned into the space on first time creation of space. SageMaker Distribution is the image that is used to provide all the libraries, extensions, packages in the in SageMaker Unified Studio application.

Prerequisites

To get started with a new Amazon SageMaker Unified Studio domain, choose an IAM role which will be used to administer the Amazon SageMaker Unified Studio domain. This is the role you will use to login and setup Amazon SageMaker Unified Studio as an administrator.

Use the following steps to update the chosen IAM role with the necessary permissions to setup Amazon SageMaker Unified Studio following these steps to

1. Verify your current role has AWS IAM administrator privileges or ask your AWS IAM administrator to perform the next step.
2. Navigate to the IAM console. Choose "Add permission" followed by "Attach policy" and search for the managed policy AWS policy: SageMakerStudioAdminIAMConsolePolicy. Select it to add it to your existing role.

This policy provides initial administrative and individual setup privileges for Amazon SageMaker Unified Studio via the AWS Management Console and SDK. It grants permissions for launching Amazon SageMaker Unified Studio. To view the permissions for this policy, see SageMakerStudioAdminIAMConsolePolicy in the AWS Managed Policy Reference.

Setting up Amazon SageMaker Unified Studio

To configure Amazon SageMaker Unified Studio with authentication through AWS IAM Identity Center, perform these steps.

Topics

- Sign up for an AWS account

Sign up for an AWS account

To get started with AWS, you need an AWS account. There are two ways to sign up for AWS. If you want complete control over account configuration and where your content is stored, or if you have regulated workloads such as HIPAA or FedRAMP, use Sign up for AWS (advanced). If you are a new user and want to use a login you already own to sign in to AWS and create an AWS environment with preconfigured defaults in select AWS Regions, use Sign up for AWS.

Regions where Amazon SageMaker Unified Studio is supported

In the current release, Amazon SageMaker Unified Studio is supported in the following AWS regions:

- Asia Pacific (Tokyo)
- Europe (Ireland)
- US East (N. Virginia)
- US East (Ohio)
- US West (Oregon)
- Europe (Frankfurt)
- South America (São Paulo)
- Asia Pacific (Seoul)
- Europe (London)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Canada (Central)
- Asia Pacific (Mumbai)
- Europe (Paris)
- Europe (Stockholm)

Domains in Amazon SageMaker Unified Studio

In Amazon SageMaker Unified Studio, a domain is the organizing entity for connecting together your assets, users, and their projects. With Amazon SageMaker unified domains, you have the flexibility to reflect the data and analytics needs of your organizational structure, whether it's creating a single Amazon SageMaker unified domain for your enterprise or multiple domains for different business units.

Amazon SageMaker Unified Studio supports two distinct domain types to accommodate different organizational needs and authentication approaches:

- **Identity Center-based domains** - Uses AWS IAM Identity Center for user authentication and management. These domains support single sign-on (SSO) through identity providers and provide centralized user management capabilities. You can create these domains using either quick setup or manual setup options through the Amazon SageMaker management console.

  > **Note**
  >
  > The Amazon SageMaker domain can reside in a different AWS Region than where the IAM Identity Center organization instance is located using IAM Identity Center multi-Region support. To use this feature, your IAM Identity Center instance must be connected to an external identity provider (IdP). For information about setting up IAM Identity Center multi-Region, see Using IAM Identity Center across multiple AWS Regions.

- **IAM-based domains** - Uses AWS Identity and Access Management (IAM) roles and AWS IAM Identity Center for authentication and access control. These domains provide an additional path to set up and manage your data and AI development environment using federated IAM roles for the execution IAM role. Only one IAM-based domain is available per AWS Account.

Both domain types provide access to the same core Amazon SageMaker Unified Studio capabilities for data analytics, machine learning, and AI development, but use different authentication mechanisms and setup processes. Choose the domain type that best fits your organization's identity management strategy and security requirements.

Topics

- Identity Center-based domains
- IAM-based domains and projects

Identity Center-based domains

Identity Center-based domains use AWS IAM Identity Center for user authentication and management. These domains support single sign-on (SSO) through identity providers, and also support IAM credentials. They provide centralized user management capabilities. You can use the Amazon SageMaker management console to create either Amazon SageMaker unified domains or Amazon DataZone domains by using either quick setup or manual setup options.

Once your domain is created, you can navigate to the Amazon SageMaker Unified Studio (a browser-based web application) where you can use all your data and configured tools for analytics and AI.

Topics

- Create a Amazon SageMaker Unified Studio domain - quick setup
- Create a Amazon SageMaker Unified Studio domain - manual setup
- Create an Amazon DataZone domain
- Domain administration for Identity Center-based domains
- Edit domains
- Delete domains
- Upgrade Amazon DataZone domains to Amazon SageMaker unified domains
- Trusted identity propagation

Create a Amazon SageMaker Unified Studio domain - quick setup

Complete the following procedure to create an Amazon SageMaker unified domain with the Quick setup option.

> **Important**
>
> Note that there is an additional charge for any VPC or resources that AWS sets up if you chose the Quick setup option for domain creation. The Quick setup option is intended for testing purposes and we recommend deleting the domain after initial tests.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **Create a Unified Studio domain** and then choose **Quick setup**.

   With this option, you're choosing to create an Amazon SageMaker unified domain and you're letting Amazon SageMaker Unified Studio configure your domain with the following default capabilities that you can customize later:

   - Data analytics, machine learning, SQL, and generative AI
   - Data and AI governance
   - Generative AI app development using Amazon Bedrock serverless models
   - Amazon Q - Free tier
   - Authentication via AWS IAM or AWS IAM Identity Center
3. If you see the following note **No VPC has been specifically set up for use with Amazon SageMaker Unified Studio**, you can use the **Choose VPC** or **Create VPC** buttons to **Create a new VPC (recommended)** or choose an existing properly-configured VPC.

   If you plan to choose your own VPC, Amazon SageMaker Unified Studio enables you to choose VPCs within the same account as well as shared VPCs from other member accounts of the AWS organization. For more information, see Share your VPC subnets with other accounts.

   > **Note**
   >
   > If you choose to create a new VPC, note that the VPC template with which it is created is not intended for production use. You can use this template as a start and modify it for your organization's purposes.

   If you see the following note **No models accessible**, you can use the **Grant model access** button to grant access to Amazon Bedrock serverless models for use in Amazon SageMaker Unified Studio.
4. Expand the **Quick setup settings** section and review the selected configurations, including domain name, domain execution role, domain service role, and domain data encryption information under **Domain resources**, user role policy, provisioning role, manage access role, Amazon S3 bucket for projects, and Virtual private cloud (VPC) information under **Data**

analytics, machine learning, and SQL analytics resources, and the model provisioning role and model consumption role under **Generative AI resources**. Modify as needed or leave the defaults, and then choose **Continue**.

5. Expand the **Onboard your data - optional** section and review the selected configuration. This allows you to make your existing AWS data available and ready for use in Amazon SageMaker Unified Studio. You can specify where you data is stored - in the current release, AWS Glue (SageMaker Lakehouse) is supported, make your data discoverable by other users in the domain, and note the owner project that is auto-created for you and where this onboarded data will be accessible in Amazon SageMaker Unified Studio. For more information, see Onboarding data in Amazon SageMaker Unified Studio.
6. On the **Create IAM Identity Center user** page, create a single sign-on user (account with IAM Identity Center) or choose an existing single sign-on user to log in to Amazon SageMaker Unified Studio. The single sign-on user that you choose here serves as the administrator in Amazon SageMaker Unified Studio.

> **Note**
>
> The Amazon SageMaker domain can reside in a different AWS Region than where the IAM Identity Center organization instance is located using IAM Identity Center multi-Region support. To use this feature, your IAM Identity Center instance must be connected to an external identity provider (IdP). For information about setting up IAM Identity Center multi-Region, see Using IAM Identity Center across multiple AWS Regions.

7. Choose **Create domain**.

Create a Amazon SageMaker Unified Studio domain - manual setup

Complete the following procedure to create a Amazon SageMaker Unified Studio domain with the quick setup option.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **Create a Unified Studio domain** and then choose **Manual setup**.

With this option, you're choosing to create an Amazon SageMaker unified domain and your'e claiming full control over customizing your domain settings, including the following:

- Customize data analytics, machine learning, SQL, Generative AI, and more
- Data and AI governance
- Configure Amazon Bedrock generative AI playgrounds and application development
- Amazon Q - Free tier
- Authentication via AWS IAM, AWS IAM Identity Center, or SAML

3. In **Name**, specify the domain name.
4. In **Description**, specify the domain description.
5. Under **Permissions**, specify the domain execution role. For more information, see AmazonSageMakerDomainExecution role.
6. Under **Permissions**, specify the domain service role. For more information, see AmazonSageMakerDomainService role.
7. Under **Data encryption**, specify the data encryption settings. Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.
8. Under **Tags**, specify the tags for your domian.
9. Choose **Create domain**.

Once your domain is created, you can proceed to customizing your domain settings, including SSO, project profiles, blueprints, account associations, Amazon Bedrock models, connections, and AmazonQ.

Create an Amazon DataZone domain

Complete the following procedure to create a Amazon SageMaker Unified Studio domain with the quick setup option.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **Create domain** and then choose **Create an Amazon DataZone domain** - choose this option if you want to create a new Amazon DataZone domain. For detailed steps on working

with Amazon DataZone domains, including how to create Amazon DataZone domains, see Domains and user access in Amazon DataZone.

Domain administration for Identity Center-based domains

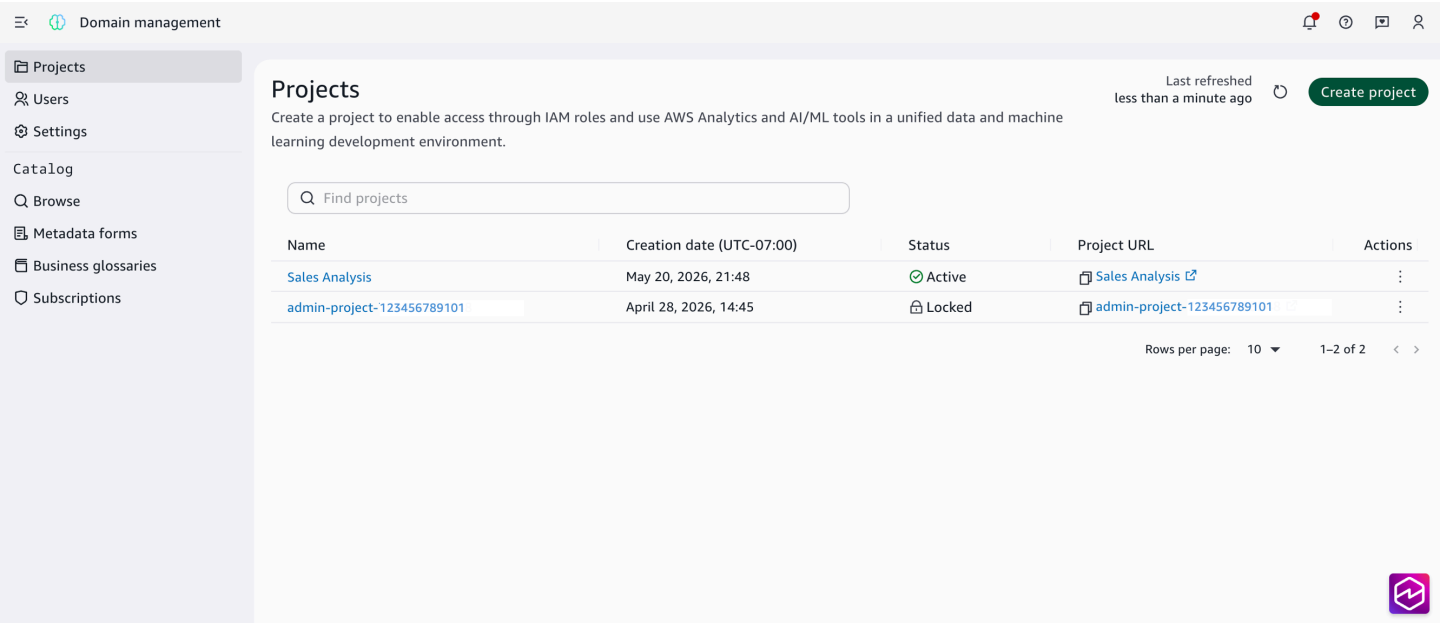
The domain administration page in Amazon SageMaker Unified Studio provides administrators with centralized management capabilities for domains, projects, and settings. Domain administrators can create and manage projects, configure domain-level settings including networking, and manage users and permissions.

Access to the domain administration page is restricted to domain users with the designation Administrator. The IAM role used to create the domain will have this designation by default and access to the domain administration page.

1. Log in to your Amazon SageMaker Unified Studio Identity Center-based domain.
2. From the Amazon SageMaker Unified Studio left navigation, choose **Domain management**.

From the domain administration page, you can access:

- **Projects** — Manage existing projects and create new projects
- **Users** — Manage user access and permissions
- **Settings** — Configure network settings and account associations



Topics

- Accessing domain management
- Set up projects within an Identity Center-based domain
- View and manage project details
- Edit project configuration
- Delete a project

Accessing domain management

Access to domain management requires an administration project named `admin-project-`*`accountID`* to be present in your domain. Amazon SageMaker Unified Studio creates this project automatically, and it controls who can access domain management.

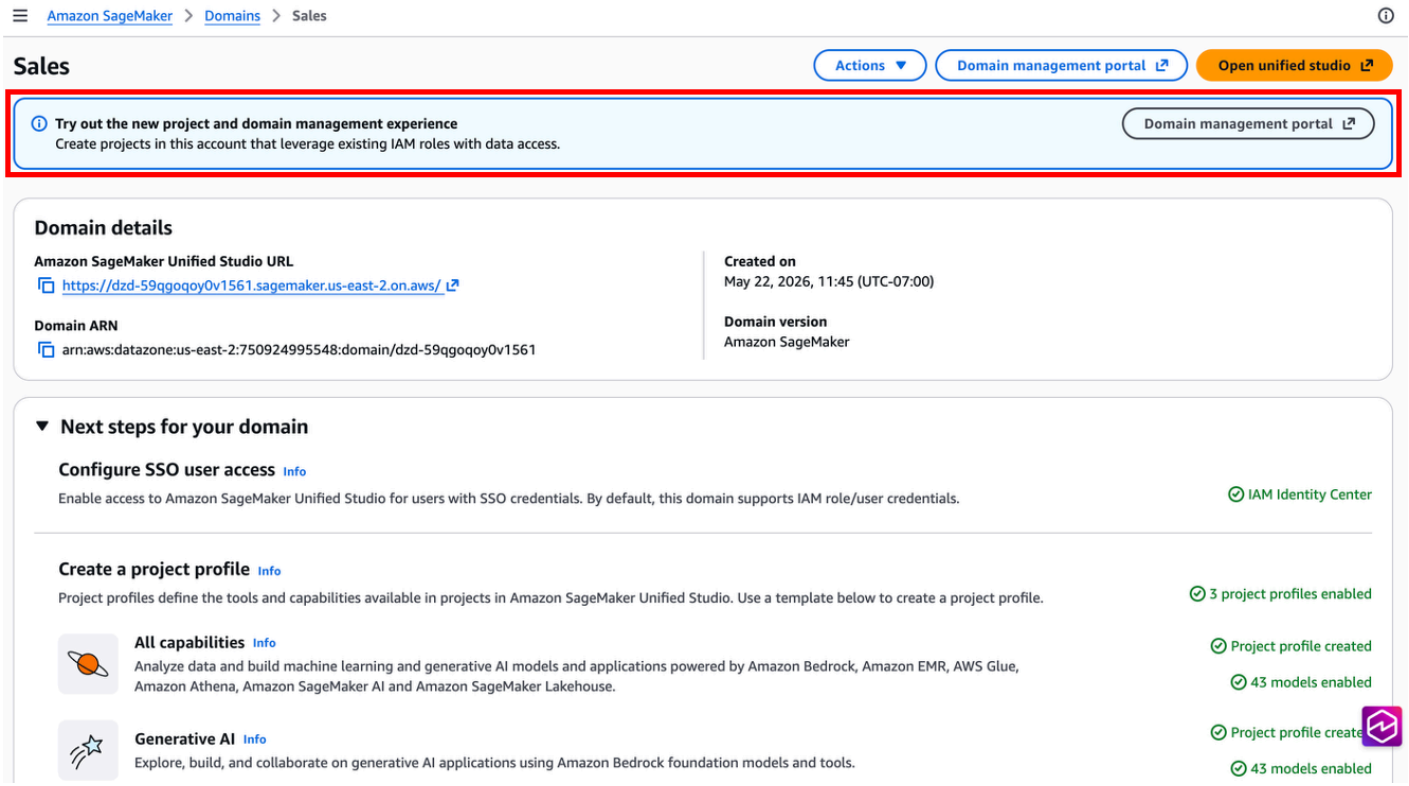
All members of the administration project are granted access to domain management and have a designation of Administrator. To remove a user's access to domain management, remove them from this project.

The administration project is created under the following conditions:

- **Quick setup flow** – The project is created automatically for new domains.
- **Manual setup flow** – The project is created when you enable the Tooling blueprint.

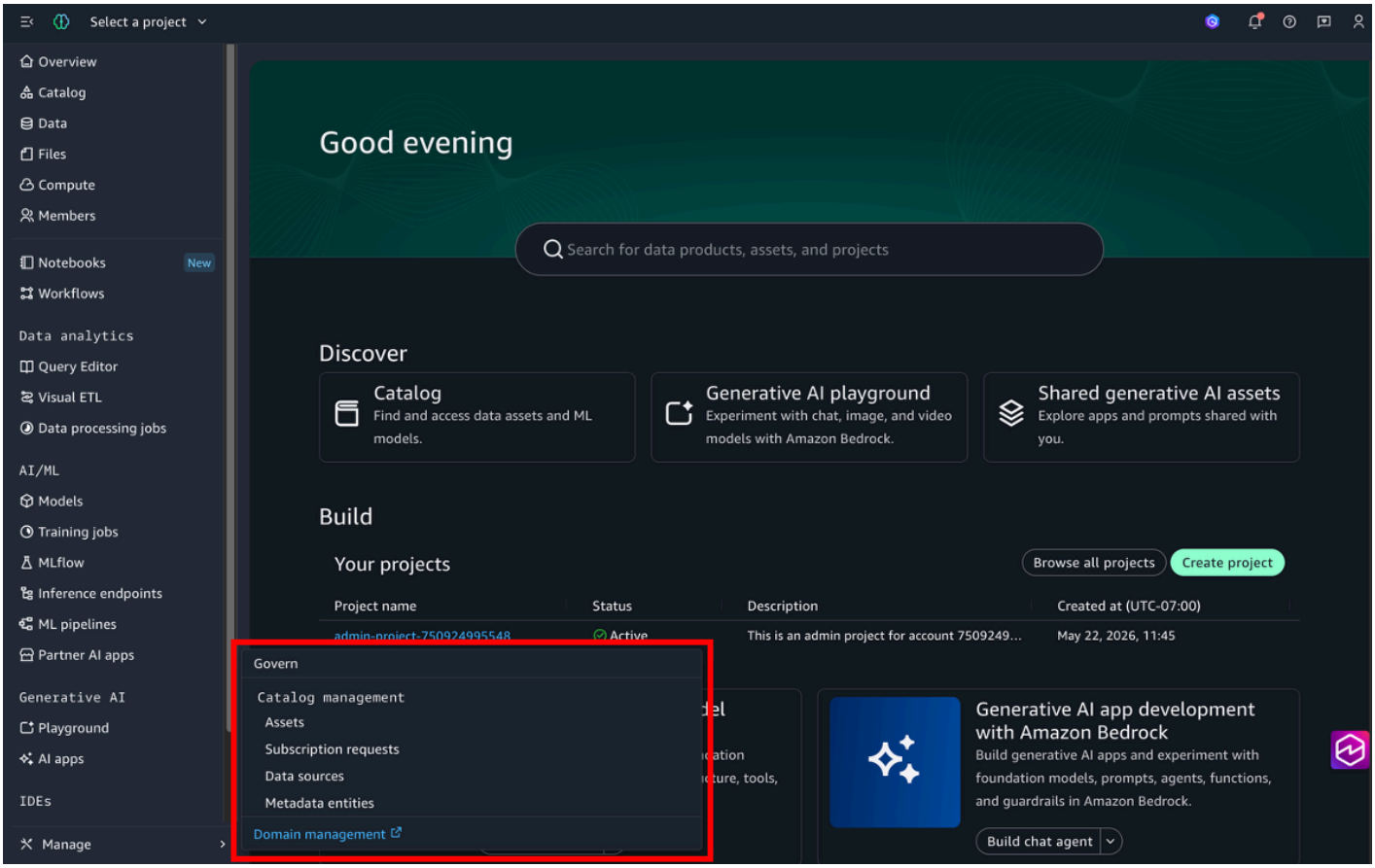
After the administration project is created, you can access domain management from two locations:

- **From the AWS SageMaker console** – Navigate to your domain in the SageMaker console. In the domain details page, choose **Domain management** at the top of the page. This opens domain management in a new tab.



- **From the Amazon SageMaker Unified Studio portal** – Log in to the Amazon SageMaker Unified Studio portal. In the left navigation panel, choose **Domain management**. This opens domain management in a new tab.

  If the **Domain management** link is not present, your user either doesn't have access to domain management or the administration project has not been created. For more information, see the section called “Setting up access to domain management”.



Setting up access to domain management

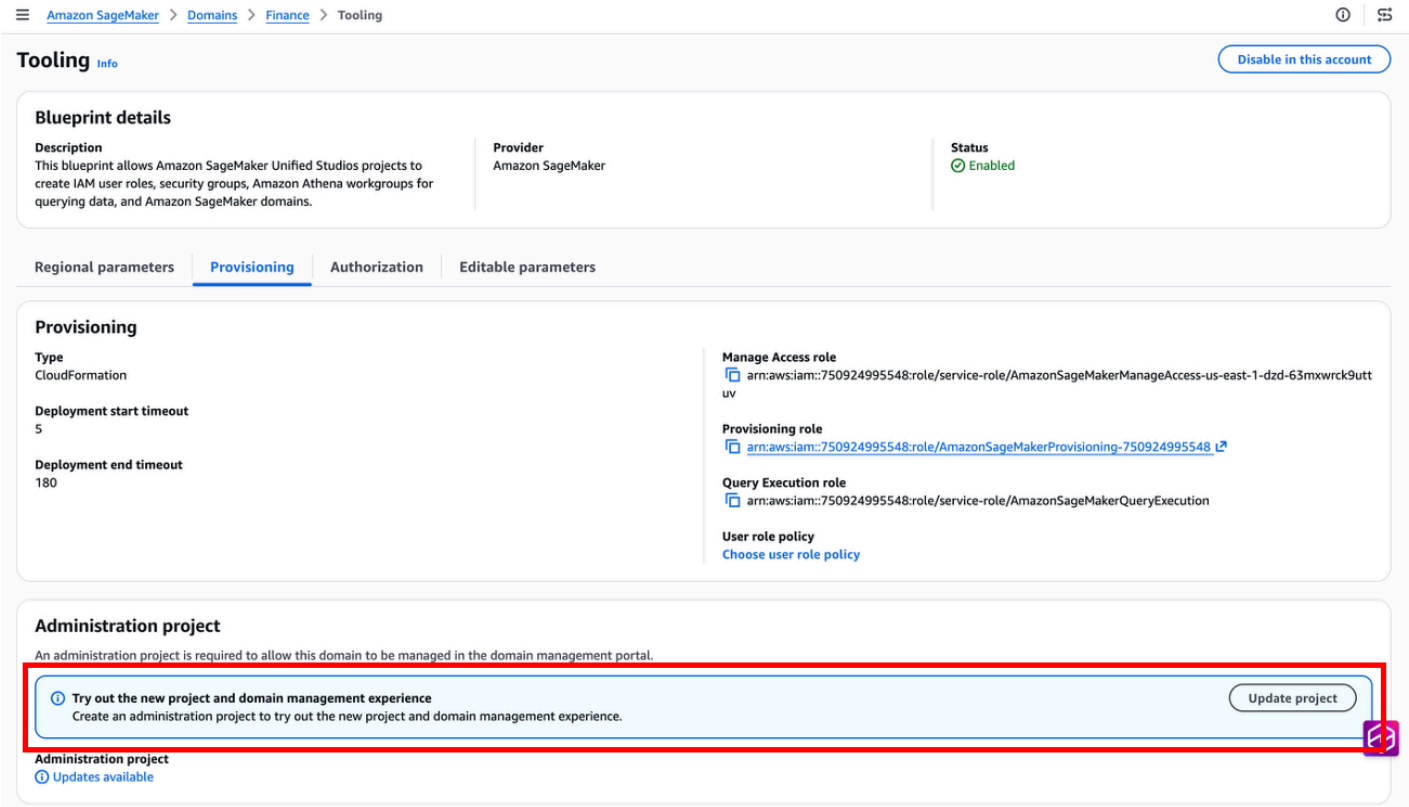
To access domain management, an administration project named `admin-project-`*`accountID`* must exist in the domain. This project controls who can access domain management. You might need to take additional steps to set up access to domain management in the following scenarios.

> **Note**
>
> To set up access to domain management, the Tooling blueprint must first be enabled. Choose the **Domain management** button in the banner of the domain details page in the SageMaker console. You are prompted to enable the Tooling blueprint. As part of the blueprint enablement, an administration project named `admin-project-`*`accountID`* is created. Return to the domain details page and choose the **Domain management** button in the banner to access domain management.

If an administration project exists in the domain

If an administration project (for example, `admin-project-accountID`) already exists in your domain, take the following steps to set up access to domain management:

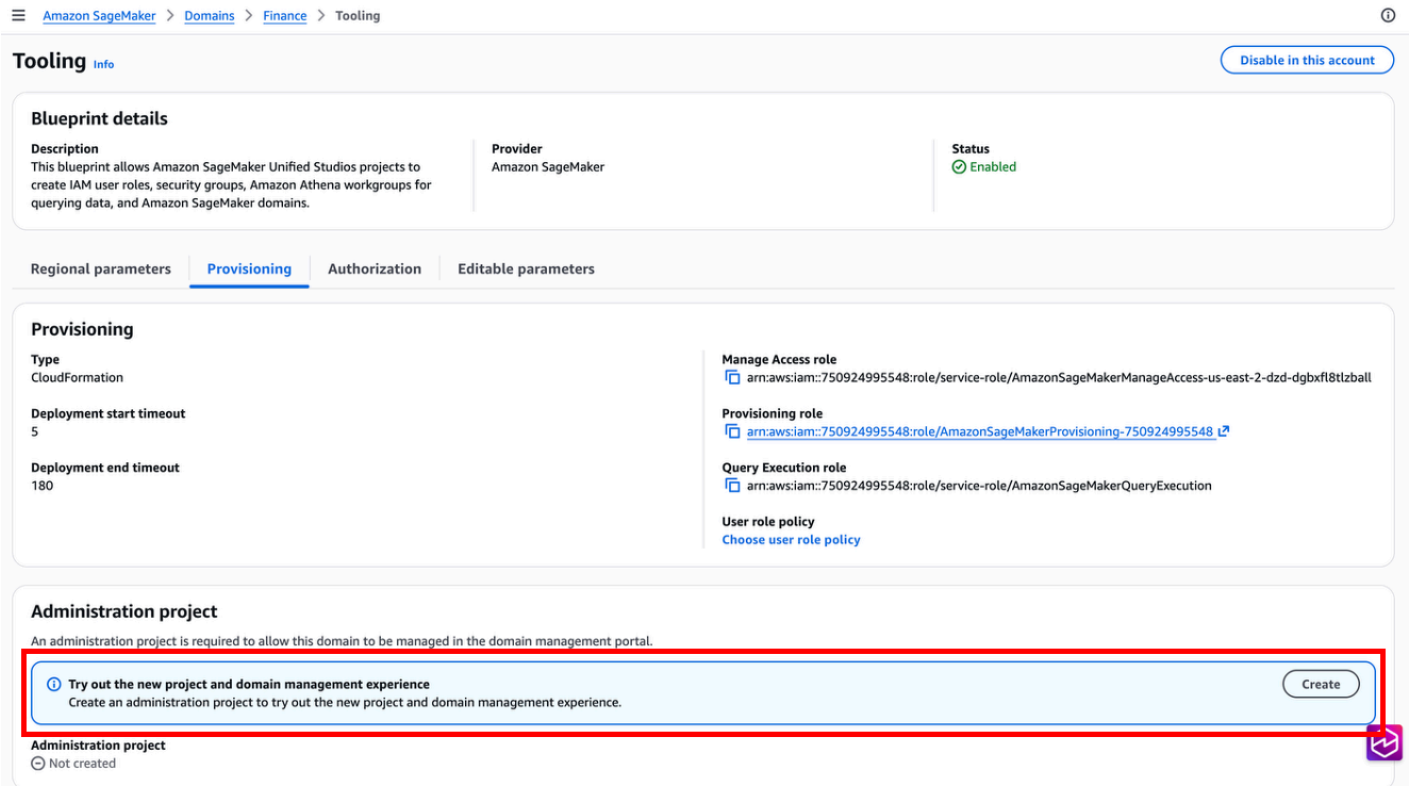
- In the AWS SageMaker console on the domain details page, choose the **Domain management** button in the banner at the top. The SageMakerStudioAdminIAMDefaultExecutionPolicy IAM policy is updated for the administration project's provisioning IAM role. This also runs an update project action on the administration project, which can take a few minutes to complete. Domain management is not accessible until the project update completes.
- You can also set up access to domain management from the Tooling blueprint. On the **Provisioning** tab, choose **Update project**. This performs an update project action to attach the SageMakerStudioAdminIAMDefaultExecutionPolicy AWS managed policy to the administration project's execution role.



If an administration project does not exist in the domain

If an administration project does not exist in your domain, take the following steps to create it and set up access to domain management:

- In the AWS SageMaker console on the domain details page, choose the **Domain management** button in the banner at the top. Choose **Set up** to create the administration project. This begins the process to create the `admin-project-`*`accountID`* project for your domain. A banner confirmation appears when domain management is successfully set up. You can now access domain management using the methods described in the section called "Accessing domain management".
- You can also set up access to domain management from the Tooling blueprint. On the **Provisioning** tab, choose **Create** to create the administration project. After the project is successfully created, you can access domain management using the methods described in the section called "Accessing domain management".



- From the Amazon SageMaker Unified Studio portal, a banner displays for root domain owners with an action button to domain management. If the administration project has not been created, a popup directs you to the AWS Management Console to create the project using the steps above.

Set up projects within an Identity Center-based domain

Projects in IAM-based domains provide isolated environments for data analytics and AI/ML development work. Each project has one IAM role for accessing data and resources, IAM and SSO

credentials for login, and storage configurations. These configurations determine what resources and data project members can access from within the project. All members of a project within an IAM-based domain have the same access to data and compute. This access is managed through the execution IAM role for the project.

Projects within IAM-based domains require a project member and an Execution IAM role:

- **Project member** — An IAM role or user that provides access to the Amazon SageMaker Unified Studio project. For IAM, the role or user must have the SageMakerStudioUserIAMConsolePolicy managed policy attached, or equivalent permissions through another policy. Log in to Amazon SageMaker Unified Studio to view the projects that you have access to.
- **Execution IAM role** — Defines which AWS analytics, AI, and ML service data the project can access. This role determines available data and resources in the portal. Amazon SageMaker Unified Studio assumes this role to make service calls on behalf of project users. The execution IAM role requires the SageMakerStudioUserIAMDefaultExecutionPolicy managed policy (or equivalent permissions) and a trust policy that allows Amazon SageMaker Unified Studio and related AWS services to assume the role.

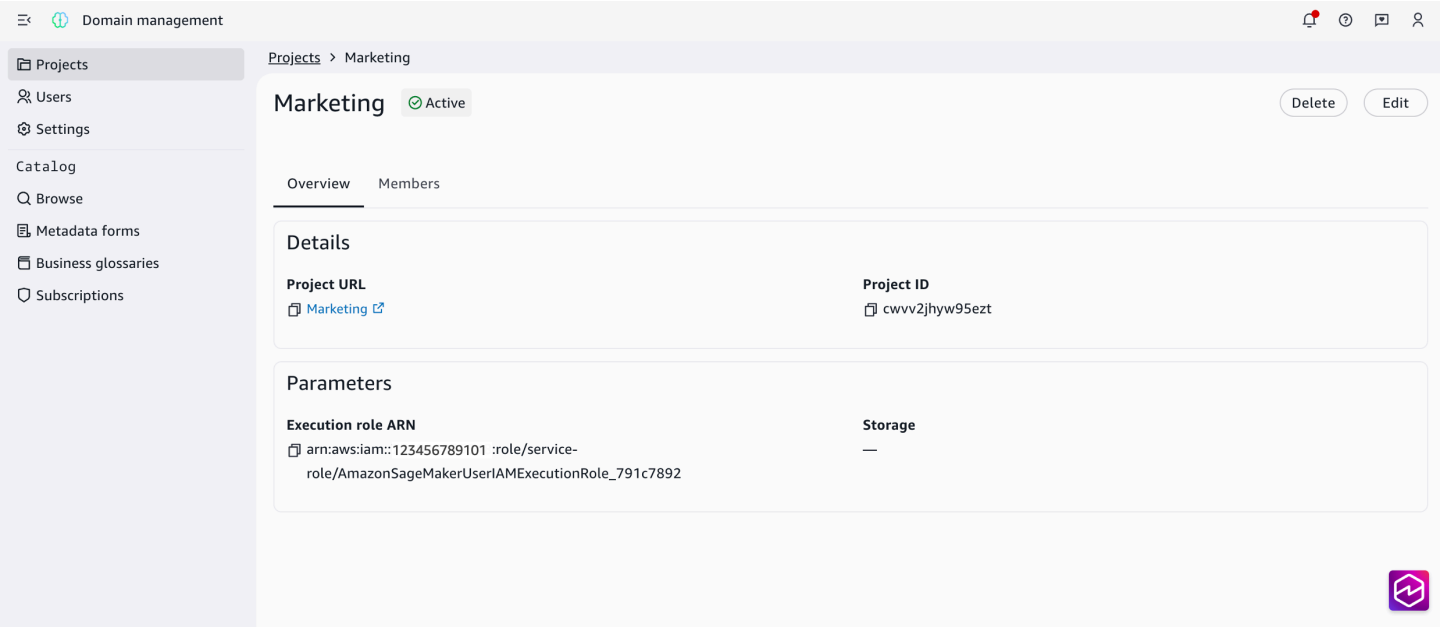
Preparing IAM roles

Project Members

- For IAM role or user project members, SageMakerStudioUserIAMConsolePolicy must be attached or have the same permissions added through another policy.

Execution IAM role

- When Amazon SageMaker Unified Studio creates this role for you, this policy will be attached, SageMakerStudioUserIAMDefaultExecutionPolicy.
- When you provide your own role, SageMakerStudioUserIAMConsolePolicy must be attached. An inline policy is needed to allow this role to pass itself to other services. A trust policy is needed to allow Amazon SageMaker Unified Studio and related services to assume this execution IAM role.
- During project creation, the Amazon SageMaker Unified Studio service creates the project IAM role as a group profile and adds the group as a project member. An IAM role session user profile is created for the project IAM role. Any logic that depends on the project role being present as a user profile must be updated to handle its presence as a group profile. For more information about user profiles, see *User management*.



To create a project, complete the following procedure:

1. From the domain administration page, choose **Projects** in the left navigation pane.
2. Choose **Create project**.
3. Enter a project name and description, and then choose **Next**.
4. Select the Region.
5. For **Execution role**, choose either **Auto-create a new role with permissions** or **Use an existing role**.
6. For **Storage**, choose either to create a new Amazon S3 bucket or use an existing Amazon S3 bucket, and then choose **Next**.
7. Add members to your project. Choose IAM or single sign-on users to add as members. You can assign up to 8 members at a time. You can add more members after the project is created.
8. For each member, assign a **Designation**.
9. Choose **Create**.

> **Note**
>
> Projects created through the domain administration portal for Identity Center-based domains do not allow you to specify a project profile. The default project profile will be used with access to Notebooks, Data Analytics and AI/ML capabilities.

View and manage project details

Project details include storage configuration, execution role assignments, and member information that determine how resources within the project operate.

To view project details, complete the following procedure:

1. From the domain administration page, choose **Projects** in the left navigation pane.
2. In the Projects list, choose the project name you want to view.
3. The project details page displays the following information:
   a. **Project Header:**
      - Project name and status (Active, Creating, Deleting)
      - Project description
      - Action buttons: Delete, Edit
   b. **Details Section:**
      - Project URL - Link to access the project portal
      - Project ID
      - AWS Region - Region where the project resources exist
      - Account - The AWS account where the project resources exist
   c. **Parameters Section:**
      - Execution role ARN - IAM role that defines data access permissions
      - Storage - Amazon S3 bucket location for project files
   d. **Members tab:**
      - Member - IAM role, IAM user, SSO user, or SSO group that can login and access the project
      - Description of member access capabilities
4. To perform actions on the project, use the buttons in the project header:
   - Choose **Edit** to modify project settings
   - Choose **Delete** to remove the project
5. To return to the Projects list, choose **Projects** in the breadcrumb navigation.

Edit project configuration

You can edit the project name and description, or modify the project members to reflect changes in business context or project scope.

To edit project details, complete the following procedure:

1. From the domain administration page, choose **Projects** in the left navigation pane.
2. Choose the project name that you want to edit from the Projects list.
3. On the project details page, choose **Edit**.
4. In the **Edit Project** dialog, modify the **Project name** and **Description**.
5. Choose **Save** to apply your changes.

To edit project members, complete the following procedure:

1. From the domain administration page, choose **Projects** in the left navigation pane.
2. Choose the project name that you want to edit from the Projects list.
3. On the project details page, choose the **Members** tab.
4. Choose **Add members**.
5. For **Type**, select IAM or SSO.
6. For **Members**, select the user to add. If you are adding IAM roles or users, the role or user must have the SageMakerStudioUserIAMConsolePolicy managed policy attached.
7. Choose **Add** to apply your changes.

Your changes are applied immediately. If you added project members, the new members have access to the project.

Delete a project

Before deleting a project, ensure that all important data and resources have been backed up or migrated, as the deletion process removes all project content permanently.

To delete a domain, complete the following procedure:

1. From the domain administration page, choose **Projects** in the left navigation pane.
2. Choose the project name you want to delete from the Projects list.

3. On the project details page, choose **Delete**.
4. In the Delete project confirmation dialog:
   a. Review the warning message: "Deleting a project is final and removes all resources and assets created in the project"
   b. In the confirmation field, type **`confirm`** to acknowledge the deletion
   c. Choose **Delete** to permanently delete the project.
5. The project status changes to "Deleting" and the project is removed from the domain.

> **Warning**
>
> Deleting a project is final and removes all resources and assets created in the project. This action cannot be undone by you or by AWS.

The project and all associated resources are permanently removed from your Amazon SageMaker Unified Studio domain.

Edit domains

After you create a domain, you can edit its description or further customize your domain settings, including SSO, project profiles, blueprints, account associations, Amazon Bedrock models, connections, and AmazonQ.

To edit a domain, complete the following steps:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose the domain's name from the list. The name is a hyperlink.
3. On the details page for the domain, Expand **Actions** and then choose **Edit**. You can use the **Edit domain** page to change the description or manage tags. Once you've made your edits, choose **Update domain**.
4. You can use the domain's details page to further customize your domain settings, including SSO, project profiles, blueprints, account associations, Amazon Bedrock models, connections, and AmazonQ.

Delete domains

When deleting a domain, note that the act of deleting a domain is final. Another important note to remember is that not all items created by Amazon SageMaker Unified Studio are deleted. The following items can only be deleted in their service consoles:

- AWS resources - except for this domain - will NOT be deleted.
- Subscription grants will NOT be removed.
- Resource shares of this domain to associated accounts will NOT be deleted.

To prevent someone from deleting a domain maliciously, deleting a domain requires administrative IAM permissions for Amazon SageMaker Unified Studio, which you can configure with IAM.

To delete a domain, complete the following procedure:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose the domain's name from the list. The name is a hyperlink.
3. On the details page for the domain, expand **Actions** and then choose **Delete**.
4. Note that deleting a domain cannot be undone and if you want to proceed, confirm the deletion by typing in the domain name in the text field, and then choose **Delete**.

Upgrade Amazon DataZone domains to Amazon SageMaker unified domains

Considerations before you upgrade your domain

Before upgrading your Amazon DataZone domain to an Amazon SageMaker unified domain, review these important considerations to ensure a smooth upgrade process.

- The upgrade process is available only through the AWS management console. Currently, no API support is offered for upgrading your domain. You can initialize the upgrade process from the domain details page of your Amazon DataZone domain.
- The upgrade process requires the following roles to be configured (you can select existing roles or have Amazon SageMaker Unified Studio create the roles on your behalf):

  - Domain Execution role - for an Amazon DataZone domain, you're using the AmazonDataZoneDomainExecutionRole that is required by Amazon DataZone to catalog, discover, govern, share, and analyze data in your domain. With an Amazon SageMaker unified domain, you must either use the existing of create a new AmazonSageMakerDomainExecution role.
  - Domain Service role - Amazon DataZone does not require a Domain Service role. With an Amazon SageMaker unified domain, you must either use the existing of create a new AmazonSageMakerDomainService role. This is a service role for domain level actions performed by Amazon SageMaker Unified Studio.
- Root domain ownership considerations – You can optionally assign IAM users or SSO users and groups as root domain owners during the upgrade process.
- Associated accounts and AWS Resource Access Manager (AWS RAM) changes:
  - Associated accounts use resource shares from AWS RAM to permit API actions from the root domain account.
  - The upgrade process changes the underlying managed permissions for the AWS RAM share that is created and managed by Amazon DataZone. The affected managed permissions are `AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess` and `AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess`.
- Amazon Q subscription changes - the upgraded domain will have Amazon Q subscription defaulted to the free-tier. Domain administrators can change this after the domain upgrade is complete.
- After the upgrade, the domain's `domainVersion` attribute changes from `V1` to `V2`.

Upgrade your Amazon DataZone domain to an Amazon SageMaker unified domain

For detailed steps on now to initialize the domain upgrade process, see Upgrade Amazon DataZone domains to Amazon SageMaker unified domains.

Frequently asked questions about upgrading Amazon DataZone domains to Amazon SageMaker unified domains

- **Which properties and configurations carry over with the domain after the upgrade?**

All properties configured on the Amazon DataZone domain carry over to the upgraded Amazon SageMaker unified domain. This includes data encryption properties, authentication application properties, etc.

- **Do I need to set up single sign-on (SSO) access again for my users?**

  No. Your IAM Identity Center SSO application associated to the domain will carry over to the upgraded Amazon SageMaker unified domain. Additionally, any IAM user or role assigned to the domain will be available in the upgraded Amazon SageMaker unified domain.

- **Can I still use the Amazon DataZone portal after the upgrade?**

  Yes. After the upgrade both Amazon DataZone portal and Amazon SageMaker Unified Studio will be available for end users to interact with. Both portals will remain open until a domain administrator deactivates the Amazon DataZone portal from the Amazon SageMaker management console.

- **Will I see the projects and other entities that were created in the Amazon DataZone portal in Amazon SageMaker Unified Studio?**

  Yes. Most entities (projects, metadata forms, glossaries, domain units) created through the Amazon DataZone portal will be visible in Amazon SageMaker Unified Studio. Projects will carry over all assets, metadata forms and glossaries associated to assets, subscriptions to assets, members, etc. These projects require querying the data from AWS Athena or Amazon Redshift query editors. Metadata forms and glossaries will appear in Amazon SageMaker Unified Studio and they can be edited from Amazon SageMaker and assigned to assets from projects created through Amazon SageMaker. Environments and environment profiles from Amazon DataZone will not show in Amazon SageMaker Unified Studio - these entities have been replaced by Amazon SageMaker project profiles. Projects created in the Amazon SageMaker Unified Studio will not be visible through the Amazon DataZone portal.

- **What happens to the domain identifier and the project identifiers after the upgrade to Amazon SageMaker unified domain?**

  All entity identifiers, including the domain and projects, will remain the same after the upgrade.

- **Will my AWS CloudFormation (CFN) stacks continue to work for the newly upgrade Amazon SageMaker unified domain?**

  Amazon SageMaker Unified Studio uses the same APIs as Amazon DataZone. However, some modifications to the logic within CFN templates will be needed. For example, domains from

Amazon DataZone are distinguished from Amazon SageMaker unified domains by an attribute named domainVersion (values V1 | V2).

- **What happens when the upgrade is rolled back?**
  - Rolling back the upgrade changes the domain version from V2 to V1. Amazon SageMaker Unified Studio will no longer be accessible. The console view for the domain will return to the Amazon DataZone view. Resources created before the roll back will remain so long as they are not tied to a project that was created from Amazon SageMaker Unified Studio - rolling back is only permitted when no projects that were created from within Amazon SageMaker Unified Studio are present.
  - Settings such as AWS Q subscription will also persist after the roll back.
  - If VPCs were created for the use of Amazon SageMaker, these will persist after the roll back. VPC's created by the SageMaker service will have tag: Name = SageMakerUnifiedStudioVPC
  - The managed permission under the RAM resource share will not be rolled back. The managed permission is a superset of both Amazon DataZone and Amazon SageMaker Unified Studio.
  - A domain that had been rolled back can again be upgraded to Amazon SageMaker unified domain.

Trusted identity propagation

Trusted identity propagation in IAM Identity Center enables administrators of AWS services to grant permissions based on user attributes, such as user ID or group associations. With trusted identity propagation, identity context is added to an IAM role to identify the user requesting access to AWS resources. This context is propagated to other AWS services.

Starting on 9/30/2025, Amazon SageMaker Unified Studio supports trusted identity propagation for tasks that include Amazon Athena, Amazon Redshift, AWS Glue, Amazon EMR on EC2, and Amazon EMR Serverless. To enable trusted identity propagation within your Amazon SageMaker unified domains, you can do either of the following:

- Create a new Amazon SageMaker unified domain - from 9/30/2025 and beyond, all newly created Amazon SageMaker unified domains support trusted identity propagation with IdC for tasks that include Amazon Athena, Amazon Redshift, AWS Glue, Amazon EMR on EC2, and Amazon EMR Serverless. Other than creating a new domain, no further action is required from the administrator to configure trusted identity propagation for their new domain.
- Update your existing Amazon SageMaker unified domain - if your domain was created prior to 9/30/2025, navigate to your domain's details page and locate the update notification banner. To

update your domain to support Trusted Identity Propagation in AWS Glue, Amazon EMR on EC2, and Amazon EMR Serverless as well as Amazon Athena and Amazon Redshift, choose the **Update now** button.

Once this update is complete, you must set the `enableTrustedIdentityPropagationPermissions` property in your project profile's default Tooling blueprint To do this, complete the following procedure:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose the domain that contains the project profile whose Tooling blueprint you want to update.
3. Choose the **Project profiles** tab and then choose the project profile that you want to update.
4. In the project profile details page, choose **Edit**.
5. On the project profile's edit page, in the **Tooling blueprint parameters** section, choose the **enableTrustedIdentityPropagationPermissions** parameter and then choose **Edit**.
6. On the **Edit blueprint parameter** page, set the **enableTrustedIdentityPropagationPermissions** parameter value to **True**.
7. Optional - to enforce authorization based on trusted identity propagation identity, you can make the **enableTrustedIdentityPropagationPermissions** parameter non-editable by unchecking the **Editable** checkbox under **Editable value**.
8. Choose **Save** in the **Edit blueprint parameter** page.

> **Important**
>
> In the current release, trusted identity propagation within Amazon SageMaker unified domains is only supported for SQL analytics, interactive Spark sessions, and end-to-end machine learning lifecycle tasks with Amazon Athena, Amazon Redshift, AWS Glue, Amazon EMR on EC2, and Amazon EMR Serverless. Therefore, even though you can set the "enableTrustedIdentityPropagationPermissions" parameter value to "True" in the Tooling blueprint of any of your project profiles, such as All capabilities, Generative AI application development, SQL analytics, or any custom project profile, trusted identity propagation and authorization based on Trusted Identity Propagation is only supported for the Amazon

Athena, Amazon Redshift, AWS Glue, Amazon EMR on EC2, and Amazon EMR Serverless tools within the chosen project profile.
We recommend creating a dedicated project profile for trusted identity propagation supported tools and setting enableTrustedIdentityPropagationPermissions to True. This approach clearly establishes trusted identity propagation as the data authorization method for all projects using this profile.
Additionally, AWS Lake Formation does not support attribute-based (conditional) grants to AWS IAM Identity Center principals. For more information, see Attribute-based access control for Lake Formation. Amazon SageMaker Unified Studio relies on these grants. These grants give project members access to AWS Glue Data Catalog resources, such as catalogs, databases, and tables associated with your project. As a result, project members that are IAM Identity Center principals do not receive this access automatically. Therefore, when `enableTrustedIdentityPropagationPermissions` is set to `True`, an administrator must grant Lake Formation permissions directly to the IAM Identity Center user or group. For instructions on granting permissions to IAM Identity Center users and groups, see Granting permissions to IAM Identity Center users and groups. These grants apply to the user or group in every project they belong to. Limit the grants to only the catalogs, databases, tables, or Amazon S3 locations that the user needs.

Notebooks in Amazon SageMaker Unified Studio support trusted identity propagation for SQL analytics (Amazon Athena, Amazon Redshift) and interactive Spark sessions (Amazon EMR Serverless). When you run these tasks from a notebook in a project whose profile has `enableTrustedIdentityPropagationPermissions` set to **True**, the engine uses your IAM Identity Center identity for fine-grained data access control. AWS Glue and Amazon EMR on EC2 do not support trusted identity propagation from notebooks. These services use compatibility permission mode for data access instead.

IAM-based domains and projects

IAM-based domains in Amazon SageMaker Unified Studio provide another configuration option to setup and manage your data and AI development environment. IAM-based domains automate creation of a Amazon SageMaker Unified Studio domain using AWS Identity and Access Management (IAM) roles, and also use IAM roles to access data and resources for a project within an IAM-based domain.

> **Note**
>
> A project in Amazon SageMaker Unified Studio is a boundary within a domain where you can collaborate with other users to work on a business use case. In projects, you can create and share data and resources. For more details, see Projects.

By default, Amazon SageMaker Unified Studio will create a domain configured with an AWS IAM role. You can use an existing IAM role or choose to create a new IAM role for the domain setup. Projects within this IAM-based domain also use an IAM role to access data and infrastructure within Amazon SageMaker Unified Studio. In addition, each project is assigned an IAM role for login, this federated IAM role is used to authenticate and access the assigned IAM project. Only one IAM-based domain is available per AWS Account per region. Each IAM-based domain supports multiple projects, and each project can be assigned to only one IAM-role for authentication and execution.

Amazon SageMaker Unified Studio also supports domains configured with AWS IAM Identity Center (IdC). Projects within this Identity Center-based domain use the project role to access data and resources, or Identity-based data authorization using AWS IAM Trusted Identity Propagation. End users login using their identity provided directly by Identity Center or through SSO to an identity provider. Additional details to setup an Identity Center based domain are available in Identity Center-based domains.

Topics

- Overview of IAM-based domains
- Set up IAM-based domains in Amazon SageMaker Unified Studio
- Manage data encryption in IAM-based domains
- Access the Domain Administration Page
- Set up single sign-on for IAM-based domains
- Manage Projects from Domain Administration
- Configure Domain Settings
- Projects in IAM-based domains

Overview of IAM-based domains

IAM-based domains provide the following capabilities:

- Setup using existing IAM roles and resources
- Authentication through federated IAM roles used for login
- Project creation and management interface within Amazon SageMaker Unified Studio

IAM-based domains require two IAM roles to function properly:

Login IAM role

This role authenticates users and provides access to Amazon SageMaker Unified Studio. The login role must have specific managed policies attached and inline policies configured to enable domain and project operations. Users use this role to access the project assigned to that IAM role when accessing the Amazon SageMaker Unified Studio interface.

Execution IAM role

This role defines the AWS services and data that can be accessed through Amazon SageMaker Unified Studio projects. The execution role determines which tools, compute resources, data sources, and AI/ML assets project members can access. Amazon SageMaker Unified Studio assumes this role to make service calls on behalf of users within projects.

> **Note**
>
> The Execution IAM role can be the same IAM role as the Login IAM role.

Both roles require specific policy attachments and trust relationships to function correctly within the IAM-based domain architecture. The system validates these permissions during setup and provides guidance for any missing configurations.

Considerations:

- For the role used as the admin Login IAM role, consider a role with a smaller population of users who will be responsible for administering the domain.
- For the role used as the admin Execution IAM role, again consider a role with a smaller population of users because the role will grant access to a broader set of data within the account. A default project will be created for this Execution IAM role. Consider a role that has access to the appropriate data resources (Glue, Athena, etc.). This role will automatically be assigned AWS Lake Formation administrator permission enabling further data access.

Set up IAM-based domains in Amazon SageMaker Unified Studio

Setting up an IAM-based domain in Amazon SageMaker Unified Studio requires an IAM roles used for domain administration tasks. The setup process validates your IAM role configurations and guides you through any necessary policy attachments. You can choose to create new execution IAM role with default permissions or use existing roles that meet the service requirements.

In addition, you must choose encryption settings before you can complete setup. The setup typically completes in minutes and automatically provisions the required AWS resources.

Prepare the Login IAM role for your IAM-based domain:

1. Login to the IAM role (defined in Overview of IAM-based domains) with AWS IAM administrator privileges defined in the pre-requisites.
2. Navigate to the IAM console.
3. Choose **Add permission** followed by **Attach policy** and search for the managed policy `SageMakerStudioAdminIAMConsolePolicy`. Select it to add it to your existing role.
4. Do one of the following:

   - Add the following inline policy to your Login IAM role if you are choosing to use a new role as the Execution IAM role:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateRoleStatement",
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/AmazonSageMaker*",
                "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
            ]
        },
        {
            "Sid": "AttachRolePolicyStatement",
            "Effect": "Allow",
```

```
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::aws:policy/SageMakerStudio*",
                        "arn:aws:iam::*:policy/service-role/AmazonSageMaker*"
                    ]
                }
            }
        }
    ]
}
```

- Add the following inline policy to your Login IAM role if you are choosing to use an existing role as the Execution IAM role:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IAMPassRoleStatement",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:role/<execution_role>"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "datazone.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

5. Add the following inline policy to your Login and Execution IAM roles to enable KMS key usage.

```
{
    "Version": "2012-10-17",
    "Statement": [
          {
             "Sid": "KMSDescribePermissions",
             "Effect": "Allow",
             "Action": "kms:DescribeKey",
             "Resource": [
               "arn:aws:kms:us-east-1:111122223333:key/key-id"
             ]
         },
         {
             "Sid": "KMSPermissions",
             "Effect": "Allow",
             "Action": [
                 "kms:Decrypt",
                 "kms:GenerateDataKey"
             ],
             "Resource": [
               "arn:aws:kms:us-east-1:111122223333:key/key-id"
             ],
             "Condition": {
                 "ForAnyValue:StringEquals": {
                     "kms:EncryptionContextKeys": "aws:datazone:domainId"
                 }
             }
         }
     ]
 }
```

Prepare the Execution IAM role for your IAM-based domain:

Amazon SageMaker Unified Studio provides two methods to configure the Execution IAM role (defined in Overview of IAM-based domains), first you can choose to create a new Execution IAM role for your IAM-based domain. Choosing this option will create a new role with default permissions and policies to administer your IAM-based domain. This auto-created role will contain the following permission details:

1. Managed policy: Data access and permission will be defined by `SageMakerStudioAdminIAMPermissiveExecutionPolicy`. It will not have the data access of the login
2. Add the following trust policy to allow Amazon SageMaker Unified Studio and related services to assume this Execution IAM role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "datazone.amazonaws.com",
                    "sagemaker.amazonaws.com",
                    "glue.amazonaws.com",
                    "bedrock.amazonaws.com",
                    "scheduler.amazonaws.com",
                    "lakeformation.amazonaws.com",
                    "airflow-serverless.amazonaws.com",
                    "athena.amazonaws.com",
                    "redshift.amazonaws.com",
                    "emr-serverless.amazonaws.com",
                    "access-grants.s3.amazonaws.com",
                    "elasticmapreduce.amazonaws.com"
                ]
            },
            "Action": [
                "sts:AssumeRole",
                "sts:TagSession",
                "sts:SetContext",
                "sts:SetSourceIdentity"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "<domain_account>"
                }
            }
        }
    ]
}
```

3. AWS Lake Formation administrator: This role will be assigned as an administrator to enable data discovery and access management.

Alternatively, Amazon SageMaker Unified Studio can use an existing IAM role as the Execution IAM role for your IAM-based domain. Choosing this option will require additional permissions and policies to be added to your existing IAM role to administer your IAM-based domain

1. Login to the IAM role with AWS IAM administrator privileges defined in the pre-requisites.
2. Navigate to the IAM console.
3. Choose **Add permission** followed by **Attach policy** and search for the managed policy `SageMakerStudioAdminIAMDefaultExecutionPolicy`. Select it to add it to your existing role.
4. Add the following inline policy to allow this role to pass itself to other services.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PassRoleSelf",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:role/<role_name>"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "sagemaker.amazonaws.com",
                        "glue.amazonaws.com",
                        "lakeformation.amazonaws.com",
                        "bedrock.amazonaws.com",
                        "scheduler.amazonaws.com",
                        "airflow-serverless.amazonaws.com",
                        "athena.amazonaws.com",
                        "redshift.amazonaws.com",
                        "emr-serverless.amazonaws.com",
                        "access-grants.s3.amazonaws.com"
                    ]
                }
```

```
            }
        }
    ]
}
```

5. Add the following trust policy to allow Amazon SageMaker Unified Studio and related services to assume this Execution IAM role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "datazone.amazonaws.com",
                    "sagemaker.amazonaws.com",
                    "glue.amazonaws.com",
                    "bedrock.amazonaws.com",
                    "scheduler.amazonaws.com",
                    "lakeformation.amazonaws.com",
                    "airflow-serverless.amazonaws.com",
                    "athena.amazonaws.com",
                    "redshift.amazonaws.com",
                    "emr-serverless.amazonaws.com",
                    "access-grants.s3.amazonaws.com",
                    "elasticmapreduce.amazonaws.com"
                ]
            },
            "Action": [
                "sts:AssumeRole",
                "sts:TagSession",
                "sts:SetContext",
                "sts:SetSourceIdentity"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "<domain_account>"
                }
            }
        }
    ]
```

```
}
```

6. Recommended: Navigate to AWS Lake Formation and grant this role AWS Lake Formation administrator permission to enable data discovery and access management within the domain.

Create Your Domain:

1. Login to the AWS Management Console and choose the Login IAM role (defined in Overview of IAM-based domains) you created for the Administrator.
2. Navigate to the Amazon SageMaker console and use the region selector to choose your desired AWS Region.
3. Choose **Get started** from the Amazon SageMaker Unified Studio section.
4. You should see a screen with the title **Set up Amazon SageMaker Unified Studio**.
5. Choose and select the Execution IAM Role for the Admin

> **Note**
>
> If role manager is enabled in your account, Amazon SageMaker Unified Studio attaches the role for you, and the role options described here are replaced by a **Customize** option. To use a different role, choose **Customize**. For more information, see IAM role creation in the *IAM User Guide*.

6. **Setup S3 table integration with AWS analytics services**. This option is enabled by default, and will allow Amazon SageMaker Unified Studio to access table buckets and integrate the table buckets with AWS analytics services using AWS Glue. If S3 Tables analytics integration has already been configured in your account and Region (that is, the `s3tablescatalog` already exists in the AWS Glue Data Catalog), this option will not be shown. Learn more.
7. In the **Data encryption** section, configure your encryption preferences:
   - Leave **Customize encryption settings (advanced)** unchecked to use AWS-managed encryption
   - Check **Customize encryption settings (advanced)** to specify a custom AWS KMS key

   If using custom encryption, see Manage data encryption in IAM-based domains
8. Choose **Set up** to begin the domain creation process.

9. Monitor the setup progress in the **Setting up Amazon SageMaker Unified Studio** dialog. The process typically takes 1-2 minutes to complete.
10. Once the setup is completed, project will automatically be created using the same Execution role. Then you will be redirected to the Administrative pages for managing the domain. See Access the Domain Administration Page for details.
11. You can also access the project associated with your Login IAM role by choosing on the first project. See **Navigating within Amazon SageMaker Unified Studio** for details.

Amazon SageMaker Unified Studio also supports domains configured with AWS IAM Identity Center (IdC). Additional details to setup an Identity Center based domain are available in Identity Center-based domains.

Manage data encryption in IAM-based domains

Data encryption in IAM-based domains protects your data at rest and in transit within Amazon SageMaker Unified Studio. You can choose between AWS-managed encryption keys for simplified management or customer-managed AWS KMS keys for enhanced control over encryption operations. Encryption settings are configured during domain setup and cannot be changed after domain creation.

AWS-managed encryption provides automatic key management with no additional configuration required. Customer-managed encryption enables you to control key policies, rotation schedules, and access permissions while requiring additional IAM policy configuration for your roles.

All data stored in the default Amazon S3 bucket created by Amazon SageMaker Unified Studio is encrypted according to your chosen encryption configuration. The encryption settings apply to all projects and resources within the domain.

Prerequisites:

- Understanding of AWS KMS key management concepts
- Appropriate IAM permissions to use or create KMS keys
- Decision on encryption approach based on your security requirements

Configure AWS-managed encryption (default):

1. During domain setup, leave the **Customize encryption settings (advanced)** option unchecked.

2. The system automatically configures encryption using AWS-owned and managed keys.
3. No additional IAM policy configuration is required for AWS-managed encryption.

Configure customer-managed encryption:

1. During domain setup, check **Customize encryption settings (advanced)**.
2. Choose **Choose an AWS KMS key** and select one of the following options:
   - Select an existing KMS key from the dropdown menu
   - Enter a KMS key ARN directly in the text field
   - Choose **Create new KMS Key** to create a new key
3. If creating a new key, configure the key policy to allow access from your IAM roles.
4. Add the following inline policy to your Login and Execution IAM roles to enable KMS key usage.

```
{
    "Version": "2012-10-17",
    "Id": "key-consolepolicy",
    "Statement": [
        {
            "Sid": "ListAndDescribe",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListGrants"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                }
```

```
            }
        },
        {
            "Sid": "CloudWatchLogs",
            "Effect": "Allow",
            "Principal": { "Service": "logs.us-east-1.amazonaws.com" },
            "Action": [
                "kms:Encrypt*",
                "kms:Decrypt*",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:Describe*"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:*:*:log-
group:/aws/mwaa-serverless/*"
                }
            }
        },
        {
            "Sid": "S3Table",
            "Effect": "Allow",
            "Principal": {
                "Service": "maintenance.s3tables.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DataZone",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:Encrypt",
                "kms:GenerateDataKeyWithoutPlaintext",
```

```
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "kms:EncryptionContextKeys": "aws:datazone:domainId"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                }
            }
        },
        {
            "Sid": "S3Kms",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "s3.*.amazonaws.com"
                },
                "Null": {
                    "kms:EncryptionContext:aws:s3:arn": "false"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "SchedulerKms",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "kms:EncryptionContext:aws:scheduler:schedule:arn": "false"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                }
            }
        },
        {
            "Sid": "SecretsKms",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "secretsmanager.*.amazonaws.com"
                },
                "Null": {
                    "kms:EncryptionContext:SecretARN": "false"
                },
                "ArnLike": {
```

```
                    "aws:PprincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                }
            }
        },
        {
            "Sid": "SageMakerKms",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "sagemaker.*.amazonaws.com"
                },
                "Null": {
                    "kms:EncryptionContextKeys": "false"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                }
            }
        },
        {
            "Sid": "SageMakerCreateGrant",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
```

```
            },
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "sagemaker.*.amazonaws.com"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                }
            }
        },
        {
            "Sid": "DataZoneCreateGrant",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "datazone.*.amazonaws.com"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Encrypt",
                        "Decrypt",
                        "ReEncryptFrom",
```

```
                        "ReEncryptTo",
                        "GenerateDataKeyWithoutPlaintext",
                        "GenerateDataKey",
                        "DescribeKey",
                        "RetireGrant",
                        "CreateGrant"
                    ]
                }
            }
        },
        {
            "Sid": "GlueKms",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "glue.*.amazonaws.com"
                },
                "Null": {
                    "kms:EncryptionContextKeys": "false"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                }
            }
        },
        {
            "Sid": "BedrockKms",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
```

```
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "bedrock.*.amazonaws.com"
                },
                "Null": {
                    "kms:EncryptionContextKeys": "false"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                }
            }
        },
        {
            "Sid": "WorkflowsCreateGrant",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "airflow-serverless.*.amazonaws.com"
                },
                "ForAnyValue:StringEquals": {
                    "kms:EncryptionContextKeys": "aws:airflow-serverless:workflow-
arn"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "Encrypt",
```

```
                        "GenerateDataKey",
                        "GenerateDataKeyWithoutPlaintext",
                        "RetireGrant"
                    ]
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                }
            }
        },
        {
            "Sid": "WorkflowsKms",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "kms:EncryptionContextKeys": "aws:airflow-serverless:workflow-
arn"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::111122223333:role/service-role/
AmazonSageMaker*",
                        "arn:aws:iam::111122223333:role/role_name"
                    ]
                }
            }
        }
    ]
}
```

Replace the following placeholder values with your own:

111122223333

Your 12-digit AWS account ID.

role_name

The name of the IAM role that requires AWS KMS key access, in addition to the `AmazonSageMaker*` service roles.

us-east-1

The AWS Region of your Amazon SageMaker Unified Studio domain.

Each statement (`Sid`) grants the required AWS KMS permissions to a specific integrated service — for example, Amazon S3 (`S3Kms`), AWS Glue (`GlueKms`), Amazon Bedrock (`BedrockKms`), AWS Secrets Manager (`SecretsKms`), and workflows (`WorkflowsKms`, `WorkflowsCreateGrant`) — scoped to the SageMaker principals in the `aws:PrincipalArn` condition.

5. Replace the resource ARN with your actual KMS key ARN.
6. Complete the domain setup process with your encryption configuration.

> **Warning**
> Encryption settings cannot be modified after domain creation. Choose your encryption approach carefully based on your long-term security requirements.

Access the Domain Administration Page

The domain administration page in Amazon SageMaker Unified Studio provides administrators with centralized management capabilities for domains, projects, and settings. Domain administrators can create and manage projects, configure domain-level settings including networking, and oversee the overall domain configuration.

Access to the domain administration page is restricted to the IAM role, specified as the domain login role, used to create the domain. This IAM role is the project member in the default admin project created for the domain.

1. Log in to your Amazon SageMaker Unified Studio IAM-based domain.
2. From the Amazon SageMaker Unified Studio left navigation, choose **Domain management**.
3. Alternatively, from the Amazon SageMaker Unified Studio header, locate the project dropdown menu and choose **Manage projects**.

From the domain administration page, you can access:

- Projects - Manage existing projects and create new projects
- Users - Manage user access and permissions
- Settings - Configure network settings

Set up single sign-on for IAM-based domains

Enable AWS IAM Identity Center single sign-on (SSO) for your IAM-based domain to onboard users from your corporate identity workforce. After you connect to IAM Identity Center, you can add SSO users and groups to projects, enabling them to collaborate on project data and resources.

You can set up IAM Identity Center integration from the Amazon SageMaker Unified Studio domain administration page. To complete this procedure, you must have domain administrator permissions.

Connecting to IAM Identity Center

Complete the following procedure to connect your IAM-based domain to an IAM Identity Center instance.

1. From the domain administration page, choose **Users** in the left navigation pane.
2. In the **AWS IAM Identity Center connect** section, review the connection status.
3. Choose **Connect**.
4. For the instance type, select one of the following options:
    - **Organization instance** (recommended) — Uses the organization-level IAM Identity Center instance.

- **Account instance** — Uses an account-level IAM Identity Center instance.

5. Review the user and group assignment setting. By default, assignments are set to *Requires assignment*, which means that users must be explicitly added to the domain. To disable required assignments, use the API during initial Identity Center enablement.
6. Choose **Connect**.

Viewing SSO connection details

After you connect to an IAM Identity Center instance, a **View SSO connection** button appears on the **Users** page. Choose this button to view the following connection details:

- **Instance type** — The type of IAM Identity Center instance (organization or account).
- **User and group assignments** — The current assignment setting for the connection.

Manage Projects from Domain Administration

The Projects section in domain administration provides centralized management of all projects within your Amazon SageMaker Unified Studio domain. Domain administrators can view project details, monitor project status, create new projects, and manage project configurations.

Projects in Amazon SageMaker Unified Studio enable users to collaborate on various business use cases. Within projects, users can manage data assets, perform data analysis, organize workflows, and develop machine learning models.

From the domain administration perspective, you can oversee all projects in the domain and ensure proper configuration.

Prerequisites:

- Domain administrator permissions for Amazon SageMaker Unified Studio
- IAM role or user with the `SageMakerStudioAdminIAMDefaultExecutionPolicy` policy attached

Perform the following procedure:

1. From the domain administration page, choose **Projects** in the left navigation pane.
2. The Projects page displays:

- Domain details section showing account information, region, domain ID, admin roles, and creation date
- Projects section listing all projects in the domain with details including:
  - Project name
  - Creation date (UTC-08:00)
  - Status (Active, Creating, Deleting)
  - Project URL
  - Actions menu

3. To view project details, choose the project name from the list.
4. To create a new project, choose **Create project** in the upper right corner of the Projects section.
5. Use the search functionality by entering terms in the **Find** search box to locate specific projects.
6. To perform actions on a project, choose the **Actions** menu (three dots) next to the project name for available options.
7. Monitor project status in the Status column to track project lifecycle states.

Configure Domain Settings

The Settings section in domain administration provides access to domain-level configuration options that apply across all projects in your Amazon SageMaker Unified Studio domain. Domain administrators can view domain details and configure networking settings.

1. From the domain administration page, choose **Settings** in the left navigation pane.
2. The Settings page displays the **Domain details** section with the following information:

   - Account - AWS account ID where the domain is hosted
   - Region - AWS region where the domain is deployed
   - Domain ID - Unique identifier for the Amazon SageMaker Unified Studio domain
   - Admin login role - IAM role ARN for domain administrator login
   - Admin execution role - IAM role ARN for domain administrator execution
   - Creation date - When the domain was created
   - KMS key ARN - AWS KMS key used for domain encryption

3. Review the **Networking** section to view or configure:
   - VPC configuration settings
   - Subnet assignments
   - Network security parameters

Projects in IAM-based domains

Projects in IAM-based domains provide isolated environments for data analytics and AI/ML development work. Each project has one IAM role for accessing data and resources, IAM and SSO credentials for login, and storage configurations. These configurations determine what resources and data project members can access from within the project. All members of a project within an IAM-based domain have the same access to data and compute. This access is managed through the execution IAM role for the project.

Projects can be created in the following ways:

1. The Amazon SageMaker Unified Studio admin creates the project on behalf of users from the Domain administration page.
2. The Amazon SageMaker Unified Studio admin prepares IAM roles for self-setup of projects created directly from AWS services - Amazon Athena, Amazon S3 Tables, and Amazon Redshift.

Projects within IAM-based domains require a project member and an Execution IAM role:

- **Project member** – An IAM role or user that provides access to the Amazon SageMaker Unified Studio project. For IAM, the role or user must have the SageMakerStudioUserIAMConsolePolicy managed policy attached, or equivalent permissions through another policy. Log in to Amazon SageMaker Unified Studio to view the projects that you have access to.
- **Execution IAM role** – Defines which AWS analytics, AI, and ML service data the project can access. This role determines available data and resources in the portal. Amazon SageMaker Unified Studio assumes this role to make service calls on behalf of project users. The execution IAM role requires the SageMakerStudioUserIAMDefaultExecutionPolicy managed policy (or equivalent permissions) and a trust policy that allows Amazon SageMaker Unified Studio and related AWS services to assume the role.

> **Note**
>
> The Execution IAM role can be the same IAM role as the Member IAM role. Both roles require specific policy attachments and trust relationships to function correctly within the IAM-based domain architecture. The system validates these permissions during setup and provides guidance for any missing configurations.

Set up projects within an IAM-based domain

To create a project within an IAM-based domain, you assign project members (IAM or single sign-on) and an Execution IAM role, configure execution permissions, and set up storage options. By default, projects can access resources within the domain's AWS account. You can configure the project execution IAM role to access data and resources across AWS accounts and Regions.

Preparing IAM roles

Project Members

- For IAM role or user project members, SageMakerStudioUserIAMConsolePolicy must be attached or have the same permissions added through another policy.

Execution IAM role:

- When Amazon SageMaker Unified Studio creates this role for you, this policy will be attached, SageMakerStudioUserIAMDefaultExecutionPolicy.
- When you provide your own role, SageMakerStudioUserIAMConsolePolicy must be attached. An inline policy is needed to allow this role to pass itself to other services. A trust policy is needed to allow Amazon SageMaker Unified Studio and related services to assume this execution IAM role.
- During project creation, the Amazon SageMaker Unified Studio service creates the project IAM role as a group profile and adds the group as a project member. An IAM role session user profile is created for the project IAM role. Any logic that depends on the project role being present as a user profile must be updated to handle its presence as a group profile. For more information about user profiles, see *User management*.

Create a project from the domain administration page

1. From the domain administration page, choose **Projects** in the left navigation pane.

2. Choose **Create project**.
3. Enter a project name and description, and then choose **Next**.
4. For **Execution role**, choose either **Auto-create a new role with permissions** or **Use an existing role**.
5. For **Storage**, choose either to create a new Amazon S3 bucket or use an existing Amazon S3 bucket, and then choose **Next**.
6. Add members to your project. Choose IAM or single sign-on users to add as members. You can assign up to 8 members at a time. You can add more members after the project is created.
7. For each member, assign a **Designation**.
8. Choose **Create**.

Prepare IAM roles and users for self-service project setup

You can configure IAM roles and users in your account to set up their own Amazon SageMaker Unified Studio project within your IAM-based domain. You must add permissions and policies to the existing IAM roles and users to allow them to set up their own project using the project member for login and the execution IAM role for accessing data and resources within the project. This configuration enables users to create projects from the AWS Management Console using these roles and users, or from AWS services such as Amazon Athena, Amazon S3 Tables, and Amazon Redshift.

Project member IAM role and user:

1. Login to the IAM role (defined in Overview of IAM-based domains) with AWS IAM administrator privileges defined in the pre-requisites.
2. Navigate to the IAM console.
3. Choose Add permission followed by Attach policy and search for the managed policy SageMakerStudioUserIAMConsolePolicy. Select it to add it to your existing role.

Execution IAM role:

1. Login to the IAM role with AWS IAM administrator privileges defined in the pre-requisites.
2. Navigate to the IAM console.
3. Choose Add permission followed by Attach policy and search for the managed policy SageMakerStudioUserIAMDefaultExecutionPolicy. Select it to add it to your existing role.

4. Add the inline policy to allow this role to pass itself to other services.
5. Add a trust policy: Allow Amazon SageMaker Unified Studio and related services to assume this Execution IAM role.

View and Manage Project Details

Project details include storage configuration, execution role assignments, member information, and networking settings that determine how resources within the project operate.

Viewing Project Details

1. From the domain administration page, choose **Projects** in the left navigation pane.
2. In the Projects list, choose the project name you want to view.
3. The project details page displays the following information:
   a. **Project Header:**
      - Project name and status (Active, Creating, Deleting)
      - Project description
      - Action buttons: Delete, Edit, Share info
   b. **Details Section:**
      - Project URL - Link to access the project portal
      - Project ARN - Amazon Resource Name for the project
      - Storage - Amazon S3 bucket location for project files
      - Execution role ARN - IAM role that defines data access permissions
   c. **Members Section:**
      - Member ARN - IAM role or user that can login and access the project
      - Description of member access capabilities
   d. **Networking Section:**
      - VPC - Virtual Private Cloud configuration status
      - Network settings that apply to resources created in the project
4. To perform actions on the project, use the buttons in the project header:

- Choose **Edit** to modify project settings
- Choose **Share info** to generate welcome message for users
- Choose **Delete** to remove the project

5. To return to the Projects list, choose **Projects** in the breadcrumb navigation.

Edit project configuration

You can edit the project name and description, or modify the project members to reflect changes in business context or project scope.

Edit project details

1. From the domain administration page, choose **Projects** in the left navigation pane.
2. Choose the project name that you want to edit from the Projects list.
3. On the project details page, choose **Edit**.
4. In the **Edit Project** dialog, modify the **Project name** and **Description**.
5. Choose **Save** to apply your changes.

Edit project members

1. From the domain administration page, choose **Projects** in the left navigation pane.
2. Choose the project name that you want to edit from the Projects list.
3. On the project details page, choose the **Members** tab.
4. Choose **Add members**.
5. For **Type**, select IAM or SSO.
6. For **Members**, select the user to add. If you are adding IAM roles or users, the role or user must have the SageMakerStudioUserIAMConsolePolicy managed policy attached.
7. Choose **Add** to apply your changes.

Your changes are applied immediately. If you added project members, the new members have access to the project.

Share Project Information

This feature simplifies user onboarding by providing all necessary access information in a formatted message that can be copied and shared via email or other communication channels.

1. From the domain administration page, choose **Projects** in the left navigation pane.
2. Choose the project name from the Projects list.
3. On the project details page, choose **Share info**.
4. In the Share project information dialog, review the generated welcome message that includes:
   - Welcome text explaining the project setup
   - URL - Direct link to the Amazon SageMaker Unified Studio portal
   - IAM role - The specific IAM role the user should use to access the project
5. Choose **Copy message** to copy the entire welcome message to your clipboard.
6. Choose **Close** to close the dialog.
7. Paste the copied message into your preferred communication method (email, chat, documentation) to share with project members.

The welcome message provides users with complete information needed to access their project, including login instructions and the specific IAM role they should use.

Delete a Project

Before deleting a project, ensure that all important data and resources have been backed up or migrated, as the deletion process removes all project content permanently.

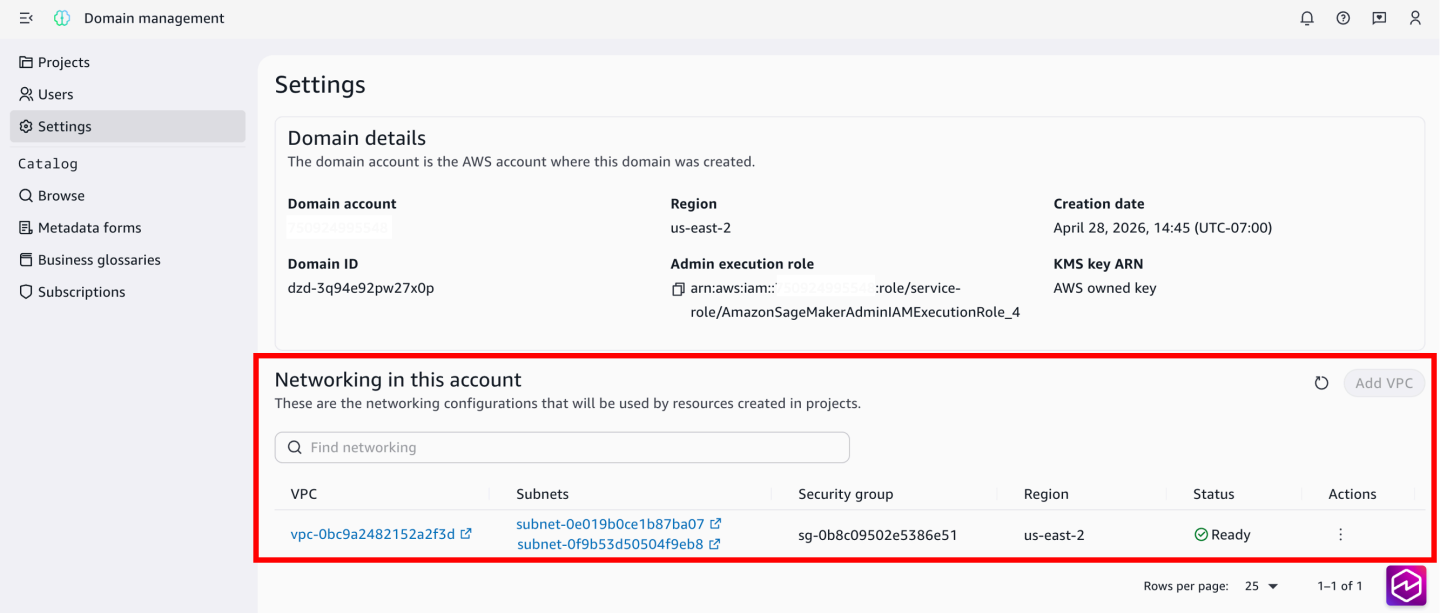
1. From the domain administration page, choose **Projects** in the left navigation pane.
2. Choose the project name you want to delete from the Projects list.
3. On the project details page, choose **Delete**.
4. In the Delete project confirmation dialog:
   a. Review the warning message: "Deleting a project is final and removes all resources and assets created in the project"
   b. In the confirmation field, type **`confirm`** to acknowledge the deletion
   c. Choose **Delete** to permanently delete the project.
5. The project status changes to "Deleting" and the project is removed from the domain.

> **Warning**
>
> Deleting a project is final and removes all resources and assets created in the project. This action cannot be undone by you or by AWS.

The project and all associated resources are permanently removed from your Amazon SageMaker Unified Studio domain.

Configure VPC Networking for Amazon SageMaker Unified Studio Domain

Amazon Virtual Private Cloud (Amazon VPC) networking with subnets is required when using certain compute services within Amazon SageMaker Unified Studio. You configure VPC networking at the domain level to provide network isolation and connectivity for compute resources, database connections, and other AWS services.



Topics

- Network settings
- Update VPC configuration and projects
- View VPC networking details

Network settings

When you configure VPC networking for your domain, all projects created after the configuration will automatically use the specified VPC. You can choose to update existing projects that do not have a VPC configured — see the section called “Update VPC configuration and projects”.

VPC configuration applies to the life of a project. VPC connection information can change the VPC itself, the subnets within, or the security group. These changes apply to projects created after the VPC is modified.

Prerequisites

- Domain administrator permissions for Amazon SageMaker Unified Studio
- An existing VPC that meets the following requirements:
  - At least 2 private subnets in different Availability Zones
  - DNS hostname and DNS support enabled
  - At least 5 free IP addresses per Amazon SageMaker Unified Studio project
- Appropriate IAM permissions to access VPC resources

Add VPC

To add a VPC, complete the following steps:

1. From the domain administration page, choose **Settings** in the left navigation pane.
2. In the **Networking** section, choose **Add VPC**. IAM-based domains support only one VPC configuration at a time. Identity Center-based domains can have a VPC per Region to support accounts that are associated with the domain.
3. In the **VPC** section, choose **Select** and select the VPC where your compute resources will be housed.

   > **Note**
   >
   > If no VPC has been set up for use with Amazon SageMaker Unified Studio, you can choose **Create VPC** to create a new VPC using AWS CloudFormation.

4. In the **Subnets** section, choose **Select** and select at least two subnets in different Availability Zones.

   > **Warning**
   >
   > Your subnets must be private or some functionality will not be available. Select subnets configured with the required VPC endpoints to establish connectivity to AWS services.

5. In the **Security group** section, select a security group. If a security group is not selected, the service creates one for the VPC.

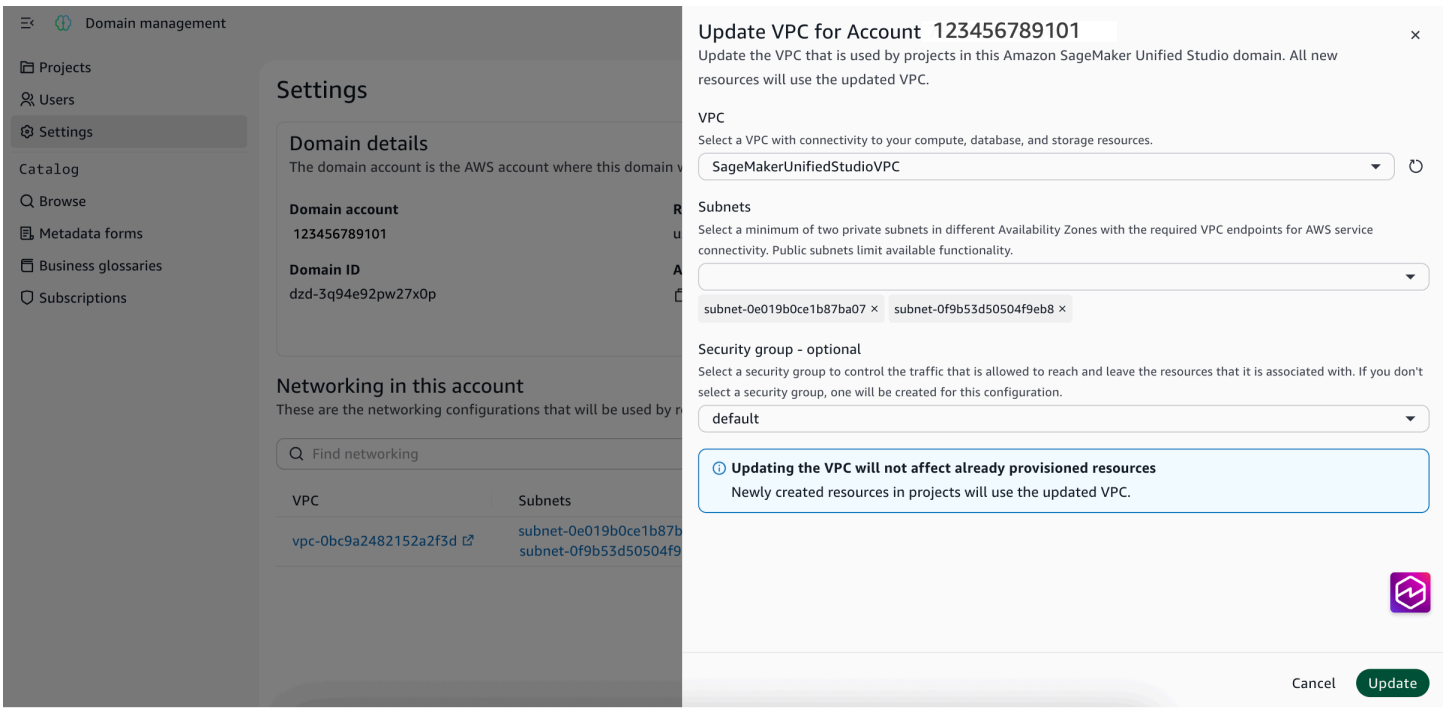
6. Choose **Save**.

You can now view the configured VPC details in the **Networking** section of the Settings tab. All new projects created in the domain will use this VPC configuration.

Update VPC configuration and projects

Updating the VPC configuration for the domain will apply to new projects created after that point automatically. Projects that had been created when a VPC configuration did not exist will have the VPC configuration applied only after the project is updated.

Update VPC



To update a VPC, complete the following steps:

1. From the domain administration page, choose **Settings** in the left navigation pane.
2. Under the **Actions** column, select **Update**.
3. Update the VPC, Subnets, or Security group.
4. Choose **Update**.

Update project with VPC configuration

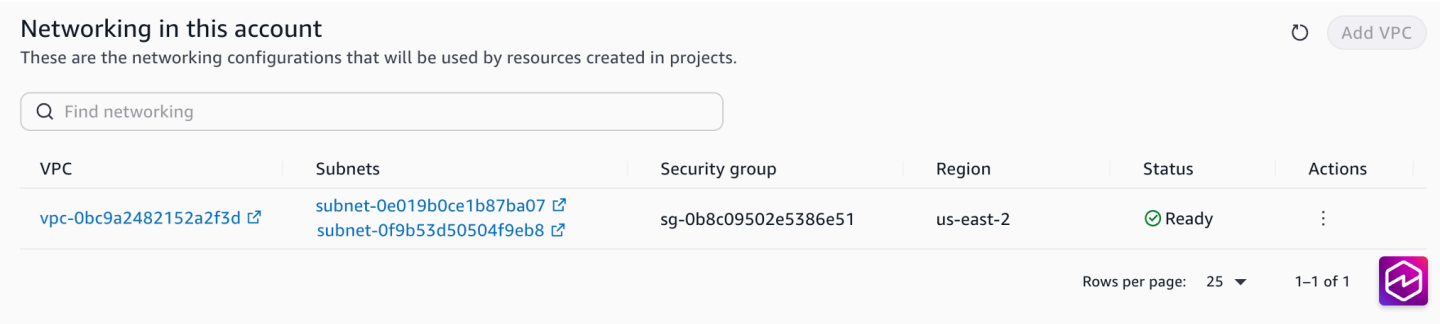
To a project with VPC configuration settings, complete the following steps:

1. From the domain administration page, choose **Projects** in the left navigation pane.
2. From the projects list, choose the project you want to update.
3. On the project detail page, you will see a banner at the top indicating "Configurations have changed. Please update this project to access the latest configuration."
4. In the banner, choose **Update**.
5. Confirm the update when prompted.

View VPC networking details

After configuring VPC networking for your Amazon SageMaker Unified Studio domain, you can view the VPC and subnet details from the domain settings. This information shows the current networking configuration that will be used by projects and compute resources.

View VPC configuration



To view VPC configurations, complete the following steps:

1. From the domain administration page, choose **Settings** in the left navigation pane.
2. In the **Networking** section, review the configured VPC details:
   - VPC - Shows the VPC ID and provides a link to view the VPC in the Amazon VPC console
   - Subnets - Lists all configured subnets with links to view each subnet in the Amazon VPC console

- Security group - The security group that was either chosen at the time the VPC configuration was saved or the security group that was automatically created if one was not provided at the time the VPC configuration was saved.
- Region - The Region where the VPC exists. Projects created in the same Region will use this VPC.
- Status - The status of the VPC configuration. A status of Ready means the VPC will apply to projects.

3. To view additional VPC configuration details, choose the VPC ID link to open the Amazon VPC console.
4. To view subnet configuration details, choose any subnet ID link to open the specific subnet in the Amazon VPC console.

Domain units and authorization policies in Amazon SageMaker Unified Studio

Use *domain units* to organize your assets and other domain entities under specific business units and teams. To set up secure and efficient data sharing within and across business units of your organization, create domain units within Amazon SageMaker Unified Studio and grant access to selected users within each business unit so they can log in and share their assets to the catalog. Users from anywhere in the enterprise can search for assets under those business units and request access to those assets.

Resource owners such as AWS account owners can use domain units to set up Amazon SageMaker Unified Studio authorization permissions on their resources. Domain units provide a delegated authority from account owners to domain unit owners, and they can set up authorization permissions on project profiles (created using blueprint configurations) on behalf of account owners. This way, you can limit who can create and use project profiles depending on the business units to which they belong. Amazon SageMaker Unified Studio authorization permissions can also be used to enforce metadata standards and enable only selected projects to create metadata forms and glossary. This can help maintain consistent and quality metadata. For more information, see Amazon SageMaker Unified Studio terminology and concepts.

Within an Amazon SageMaker Unified Studio domain unit, you can assign the following authorization policies to your users and groups to grant them specific permissions:

- Domain unit creation policy
- Project creation policy
- Project membership policy
- Domain unit ownership assumption policy
- Project ownership assumption policy

Within an Amazon SageMaker Unified Studio domain unit, you can assign the following authorization policies to your projects to grant them specific permissions:

- Glossary creation policy
- Metadata forms creation policy
- Custom asset type creation policy

Topics

- Create domain units in Amazon SageMaker Unified Studio
- Edit domain units in Amazon SageMaker Unified Studio
- Delete domain units in Amazon SageMaker Unified Studio
- Manage domain unit owners in Amazon SageMaker Unified Studio
- Assign authorization policies to users and groups within an Amazon SageMaker Unified Studio domain unit
- Assign authorization policies to projects within an Amazon SageMaker Unified Studio domain unit
- Assign authorization policies to asset types

Create domain units in Amazon SageMaker Unified Studio

To create a domain unit

1. Navigate to Amazon SageMaker Unified Studio using the URL from your administrator and log in using your SSO or AWS credentials.
2. In the left navigation pane, choose **Manage**, then under **Govern**, choose **Domain units**.
3. Choose **Create domain unit**.
4. Specify the following:
   - Under **Domain unit details**, for **Name**, specify the domain unit name.
   - Under **Domain unit details**, for **Description**, specify the domain unit description.
   - Under **Parent domain unit**, navigate through the domain unit tree and select the child domain unit that you want. This populates the parent domain unit.
5. Choose **Create**.

Edit domain units in Amazon SageMaker Unified Studio

To edit a domain unit

1. Navigate to Amazon SageMaker Unified Studio using the URL from your administrator and log in using your SSO or AWS credentials.

2. In the left navigation pane, choose **Manage**, then under **Govern**, choose **Domain units**.
3. Choose the domain unit that you want to edit.

> **Note**
>
> You cannot edit the root domain unit.

4. Expand **Actions** and choose **Edit**.
5. Make your changes to the domain unit name and description, then choose **Save changes**.

Delete domain units in Amazon SageMaker Unified Studio

To delete a domain unit

1. Navigate to Amazon SageMaker Unified Studio using the URL from your administrator and log in using your SSO or AWS credentials.
2. In the left navigation pane, choose **Manage**, then under **Govern**, choose **Domain units**.
3. Choose the domain unit that you want to delete.
4. Expand Actions and choose **Delete domain unit**.
5. In the **Delete domain unit** window, confirm the deletion, then choose **Delete**.

Manage domain unit owners in Amazon SageMaker Unified Studio

To add owners to a domain unit in Amazon SageMaker Unified Studio, complete the following steps.

1. Navigate to Amazon SageMaker Unified Studio using the URL from your administrator and log in using your SSO or AWS credentials.
2. In the left navigation pane, choose **Manage**, then under **Govern**, choose **Domain units**.
3. Choose the domain unit that you want to add owners to.
4. On the domain details page, navigate to the **Owners** tab.
5. Choose **Add owner**. In the **Add domain unit owners** panel, search for and select the users or groups that you want to make domain unit owners. Each selection appears with a running

count of how many you have selected, so that you can review your selections before you confirm.

6. Choose **Add owners**.

Assign authorization policies to users and groups within an Amazon SageMaker Unified Studio domain unit

In an Amazon SageMaker Unified Studio domain unit, you can assign the following authorization policies to your users and groups to grant them various authorization permissions within this domain unit:

- Domain unit creation policy
- Project creation policy
- Project membership policy
- Domain unit ownership assumption policy
- Project ownership assumption policy

To assign authorization policies to users and groups within a domain unit, complete the following procedure:

1. Navigate to Amazon SageMaker Unified Studio using the URL from your administrator and log in using your SSO or AWS credentials.
2. In the left navigation pane, choose **Manage**, then under **Govern**, choose **Domain units**.
3. Choose the domain unit that you want to add an authorization policy grant in.
4. On the domain unit details page, choose the authorization policy that you want to assign to users or groups.
5. Choose **Add users and groups**.
6. In the **Add users and groups** window, do one of the following:
   - Choose **Select users and groups**, specify the users and groups, then choose **Add grant**.
   - Choose **All users**, then choose **Add grant**.
7. You can enable or disable cascade permissions for the selected users. When you add users and groups, select the **Apply to child domain units** checkbox. You can also enable it in the

Authorized users and groups table by setting the dropdown in the **Cascade permissions** column to **True**. The selected users then have the permissions granted by this policy in all child domain units under this domain unit. To turn it off, set the dropdown in the **Cascade permissions** column to **False**.

To view examples of project membership policies in domain unit hierarchies, see Project membership policy in the hierarchy of domain units in Amazon DataZone in the Amazon Amazon DataZone User Guide.

Assign authorization policies to projects within an Amazon SageMaker Unified Studio domain unit

In an Amazon SageMaker Unified Studio domain unit, you can assign the following authorization policies to your projects to grant these entities various authorization permissions within this domain unit:

- Glossary creation policy
- Metadata forms creation policy
- Custom asset type creation policy

To assign authorization policies to projects within a domain unit, complete the following procedure:

1. Navigate to Amazon SageMaker Unified Studio using the URL from your administrator and log in using your SSO or AWS credentials.
2. In the left navigation pane, choose **Manage**, then under **Govern**, choose **Domain units**.
3. Choose the domain unit that you want to add an authorization policy grant in.
4. On the domain unit details page, choose the authorization policy that you want to assign to projects, then choose **Add projects and designations**.
5. In the **Add projects and designations** window, select the **Domain unit** dropdown to choose a project in a given domain unit. Then do one of the following:
   - Choose **Selected projects in a domain unit**, specify the projects and allowed designations, then choose **Add policy grant**.
   - Choose **All projects in a domain unit**, then choose **Add policy grant**.

> **Note**
>
> The **Domain unit** dropdown appears only when the domain contains more than one domain unit.

Assign authorization policies to asset types

Asset types define how the SageMaker catalog represents assets — an asset type defines the schema for a specific type of asset. Only domain unit owners and project members with adequate permissions can edit asset types. All other project members can view them but cannot edit them.

1. Navigate to Amazon SageMaker Unified Studio using the URL from your administrator and log in using your SSO or AWS credentials.
2. In the left navigation pane, choose **Manage**, then under **Catalog management**, choose **Custom asset types**.
3. Choose an existing asset type, then choose the **Permissions** tab.
4. Choose **Add usage permission**. In the **Add projects and designations** window, specify the authorized projects (**Select projects in a domain unit** or **All projects in a domain unit**), the specific domain unit, and the allowed designations — which designations a project member must have to use this policy.

   > **Note**
   >
   > The **Domain unit** dropdown appears only when the domain contains more than one domain unit.

5. Choose **Add policy grant** to save the changes.

Managing users in Amazon SageMaker Unified Studio

Users can access the Amazon SageMaker Unified Studio data portal by using either their AWS credentials or single sign-on (SSO) credentials. For IAM-based domains, see the section called "Managing users for IAM-based domains" to manage users in the domain management portal. For Identity Center-based domains, see the section called "Managing users for Identity Center-based domains" to manage users in the Amazon SageMaker Unified Studio console.

Amazon SageMaker Unified Studio supports IAM roles, IAM users, single sign-on users, and single sign-on groups. When these users are added to a domain, the service creates a unique profile for the user. These profiles are most relevant for programmatic interactions with Amazon SageMaker Unified Studio, where API requests accept a user or group profile identifier and responses return user or group profile information. The following types of profiles exist in Amazon SageMaker Unified Studio:

User profiles

Amazon SageMaker Unified Studio supports both IAM identities and single sign-on (SSO) identities to interact with the administration portal and the builder portal. Domain administrators use IAM identities to perform initial administrative domain-related work in the Amazon SageMaker Unified Studio administration portal, including creating projects, configuring VPCs, configuring metadata form types and glossaries, and managing users. Data workers use their SSO corporate identities through to log in to the Amazon SageMaker Unified Studio portal and access projects where they have memberships.

When an IAM identity or single sign-on identity is added as a user of the domain, a user profile is created. There are two types of user profiles:

User profile

Created from an IAM user or a single sign-on user. The first time an IAM user or single sign-on user logs in to the Amazon SageMaker Unified Studio portal, the service creates a user profile.

IAM role session user profile

When an IAM role principal is added to Amazon SageMaker Unified Studio, a group profile is created. For each user that federates with the IAM role, an IAM role session user profile is created. This allows the federated user to be identified when working within Amazon

SageMaker Unified Studio. For example, the IAM role session user profile has its own space within a notebook.

You can create user profiles programmatically through the `CreateUserProfile` API call:

- If `userType` is `IAM_USER` or `SSO_USER`, a user profile is created.
- If `userType` is `IAM_ROLE` and `sessionName` is provided, an IAM role group profile and an IAM role session user profile are created.
- If `userType` is `IAM_ROLE` and `sessionName` is not provided, an IAM role user profile is created.

Implicit and explicit user creation

Implicit user creation: When an IAM role logs in to the portal for the first time, the service creates a group profile for the new IAM role and IAM role session user profiles for the user federating into Amazon SageMaker Unified Studio through the IAM role. Previously, the service created the IAM role as a user profile that was not session-aware. This also applies to API calls. If a user of an IAM role submits a call to get programmatic access, the service creates the session user profile the first time they log in.

Explicit user creation: When you create users programmatically through the `CreateUserProfile` API, you can choose to create the IAM role as either a user profile that isn't session-aware or as a group profile with an IAM role session user profile. In the `CreateUserProfile` call:

- Passing only the IAM role ARN and type creates a user profile that isn't session-aware.
- Passing the IAM role ARN, the `sessionName`, and type creates a group profile (if one does not already exist) and an IAM role session user profile.

Group profiles

Group profiles represent groups of Amazon SageMaker Unified Studio users. Groups can be manually created or mapped to identity provider groups of enterprise customers. In Amazon SageMaker Unified Studio, groups serve two purposes:

- A group can map to a team of users in the organizational chart, reducing the administrative work of a project owner when employees join or leave a team.

- Corporate administrators use identity provider groups to manage and update user statuses, and domain administrators can use these group memberships to implement domain policies.

Group profiles are created by default for single sign-on groups and IAM roles that are added to the domain.

IAM roles

When an IAM role is added to the domain, a group profile is created. The first time a user belonging to the group logs in to the Amazon SageMaker Unified Studio portal, an IAM role session user profile is created for the user federating through that IAM role. Project membership and access policies are managed through the IAM role group profile. To create IAM roles programmatically through the `CreateGroupProfile` API, supply the `rolePrincipalARN` to support IAM role session user profiles.

Single sign-on groups

When a single sign-on group is added to the domain, a group profile is created. The first time a user belonging to the group logs in to the Amazon SageMaker Unified Studio portal, a user profile is created for the user. Project membership and access policies are managed through the single sign-on group profile. To create single sign-on groups programmatically through the `CreateGroupProfile` API, supply the `groupIdentifier`.

> **Note**
>
> During project creation, the Amazon SageMaker Unified Studio service creates the project IAM role as a group profile and adds the group as a project member. An IAM role session user profile is created for the project IAM role. Any logic that depends on the project role being present as a user profile must be updated to handle its presence as a group profile.

Managing users for Identity Center-based domains

Configure single sign-on (SSO) access to your Amazon SageMaker unified domain through IAM Identity Center or SAML federation. You can also manage root domain unit owners from this page.

Enable IAM Identity Center

To enable access to the Amazon SageMaker unified domains in the Amazon SageMaker Unified Studio for users with SSO credentials, complete the following procedure:

> **Note**
>
> The Amazon SageMaker Unified Studio domain can reside in a different AWS Region than where the IAM Identity Center organization instance is located using IAM Identity Center multi-Region support. Once IAM Identity Center multi-Region is set up, follow the same steps in the following procedure to enable single sign-on through IAM Identity Center for your domain. To use this feature, your IAM Identity Center instance must be connected to an external identity provider (IdP). For information on setting up IAM Identity Center multi-Region, see Using IAM Identity Center across multiple AWS Regions.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Either create a new or choose an existing Amazon SageMaker unified domain where you want to configure SSO user access.
3. On the domain's details page, either choose **Configure** next to the **Configure SSO user access** in the **Next steps for your domain section** or navigate to the **User management** tab and choose **Configure SSO user access**.
4. On the **Choose user authentication method**, choose the **IAM Identity Center**. With IAM Identity Center, users configured in IAM Identity Center can access the domain's Amazon SageMaker Unified Studio.

   You are either connecting to an organization instance of the IAM Identity Center or to an account instance of the IAM Identity Center.

   - If the account is the management account of an AWS Organization and IAM Identity Center organization instance is enabled, the IAM Identity Center organization instance is selected.
   - If the account is a member account of an AWS Organization and IAM Identity Center organization instance is enabled, an IAM Identity Center account instance is selected.
   - If the account is not a member account of an AWS Organization, an IAM Identity Center account instance is selected.

5. On the **Configure IAM Identity Center** details page, verify that your domain is connected to the IAM Identity Center and then choose user and group assignment method. You can choose either **Require assignments** - which allows only assigned IAM Identity Center users and groups access to this domain or **Do not require assignments** - which allows all authorized IAM Identity Center users and groups access to this domain.
6. On the **Review and save** page, review your choices and then choose **Save**. These settings cannot be changed once you save them.
7. If you've chosen to require assignments, use the **Add users and groups** to add IAM Identity Center users and groups to your Amazon SageMaker Unified Studio domain.

Enable SAML

Complete the following procedure to configure SAML user access to Amazon SageMaker Unified Studio for your Amazon SageMaker unified domain.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Either create a new or choose an existing Amazon SageMaker unified domain where you want to configure SAML user access.
3. On the domain's details page, either choose **Configure** next to the **Configure SSO user access** in the **Next steps for your domain** section or navigate to the **User management** tab and choose **Configure SSO user access**.
4. On the **Choose user authentication method** page, choose **SAML**. With SAML, users configured through external Identity Providers (IdPs) can access the domain's Amazon SageMaker Unified Studio. Choose **Next**.
5. On the **Configure SAML** page, specify the Identity Provider (IdP) SSO URL. You must first configure a new IdP in the IAM console. You must then also choose the user and group assignment method. You can choose either **Require assignments** - which allows only assigned IAM Identity Center users and groups access to this domain or **Do not require assignments** - which allows all authorized IAM Identity Center users and groups access to this domain.
6. On the **Review and save** page, review your choices and then choose **Save**. These settings cannot be changed once you save them.
7. If you've chosen to require assignments, use the **Add users and groups** to add SAML users and groups to your domain.

Update Root Domain Unit Owner

Complete the following procedure to manage root domain owners for your Amazon SageMaker unified domain.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Either create a new or choose an existing Amazon SageMaker unified domain and then navigate to the **User management** tab.
3. You can select existing owners and then expand the **Actions** menu and choose to **Remove** these owners.

   You can add new owners, by expanding **Add** and choosing the add SSO users and groups or IAM users and groups.

The root domain unit owner for your Amazon SageMaker domain can be changed using AWS CLI or API. This procedure is helpful when the original IAM role/user no longer exists and ownership needs to be replaced.

To use the AWS CLI to update the root domain unit owner, use the update-root-domain-unit-owner command. The IAM user or role initiating the call needs to have the datazone:UpdateRootDomainUnitOwner permission.

Considerations:

1. Domain ID, Current Owner, and New Owner are required.
2. The new owner needs to exist as a user in the domain.
3. SSO users/groups are referenced using their display name. IAM users/groups are referenced using their ARN.

Example command:

```
aws datazone update-root-domain-unit-owner \
--domain-identifier DOMAIN_ID \
--current-owner CURRENT_OWNER \
```

```
  --new-owner NEW_OWNER
```

Managing users for IAM-based domains

As a domain administrator, you can use the domain user management page for IAM-based domains to view all users that are active in the domain. From this page, you can manage access, update permissions, and modify project membership from a single screen.

To access user management, choose **Users** in the left navigation pane of the domain administration page.

Viewing and filtering users

The **Users** page displays all users in the domain. You can use the following options to find specific users:

- **Search** — Search across all users by name.
- **Filter by type** — Filter the list by user type: IAM, SSO user, or SSO group.
- **Filter by designation** — Filter by designation: Owner or Contributor.
- **Filter by status** — Filter users by their Active or Inactive status.

Adding a user

You can add IAM users and roles, SSO users, or SSO groups to your domain and assign permissions and project membership.

> **Note**
>
> If you are adding an IAM role or user, the SageMakerStudioUserIAMConsolePolicy managed policy must be attached to the role or user.

To add a new user to the domain, complete the following steps.

1. On the **Users** page, choose **Add user**.
2. For **Type**, select IAM or SSO, and then search for the user or group to add.
3. Choose **Next** to assign permissions and project membership.

4. (Optional) To make the user a domain administrator, select the **Administrator** designation.
5. (Optional) To add the user to existing projects, choose **Add project**. Select the project and assign the project designation. You can add the user to a maximum of 8 projects.
6. Choose **Add** to add the user to the domain.

The user now appears on the **Users** page.

Editing a user

You can modify user settings such as status, domain designation, and project membership.

1. On the **Users** page, choose the user name from the list.
2. Modify the user settings as needed:
   - **Status** — Set to *Active* to allow the user to log in to Amazon SageMaker Unified Studio, or *Inactive* to prevent access.
   - **Domain designation** — Update the user's domain-level designation.
   - **Project membership** — Add the user to existing projects or remove them from current projects.
3. Choose **Save** to apply your changes.

Associated accounts in Amazon SageMaker Unified Studio

In Amazon SageMaker Unified Studio, associated accounts are other AWS accounts that can be associated with an Amazon SageMaker unified domains so that resources can be created and accessed in these accounts for various purposes.

Complete the following procedures to manage account associations and configure domains in associated accounts in Amazon SageMaker Unified Studio.

Topics

- Request association with other AWS accounts
- Accept an account association request from an Amazon SageMaker Unified Studio domain and enable an environment blueprint
- Reject an account association request from an Amazon SageMaker Unified Studio domain
- Remove an associated account in Amazon SageMaker Unified Studio
- Configure Amazon Bedrock in SageMaker Unified Studio in an associated account

Request association with other AWS accounts

> **Note**
>
> By sending an association request to another AWS account, you are sharing your domain with the other AWS account with AWS Resource Access Manager (RAM). Be sure to check the accuracy of the account IDs that you enter.

Complete the following procedure to request association with other AWS accounts.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose an Amazon SageMaker unified domain name from the list. The name is a hyperlink.
3. Choose the **Account associations** tab and then choose **Request association**.

4. On the **Request association** page, enter the IDs of the accounts with which you want to associate this domain. When you are satisfied with the list of account IDs, choose **Request association**.

   Notice that the account IDs to which you sent an association request now appear in the list of accounts in the **Associated accounts** tab with the **Requested** status.

Accept an account association request from an Amazon SageMaker Unified Studio domain and enable an environment blueprint

Complete the following procedure to accept association with an Amazon SageMaker unified domain.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View requests** and select the inviting domain from the list of requests. The domain name is a hyperlink. You can also use the radio button next to the domain name and then choose **Review request**.
3. On the **Accept and configure AWS association page**, choose **Accept new permissions** to accept the association request.
4. Once the action completes and your account is associated with the inviting Amazon SageMaker unified domain, this domain's name appears in the **Associated domains** list on the **Associated domains** page. The name is a hyperlink. If you choose it, you then navigate to the Amazon SageMaker console for this domain as the associated account. You can perform the following configurations for this domain in your associated account:

   - Configure Data analytics and AI/ML model development capability under the **Next steps for your domain**. For more information, see All capabilities project profile.
   - Configure Generative AI application development capability under the **Next steps for your domain**. For more information, see Configure Amazon Bedrock in SageMaker Unified Studio in an associated account.
   - Configure SQL analytics capability under the **Next steps for your domain**. For more information, see SQL analytics project profile.

- View the permissions that govern the association between this account and the domain in the **Permissions** tab.
- Use the **Blueprints** tab to configure blueprints that contain the tools, resources and parameters that are used in this account. For more information, see Blueprints in Amazon SageMaker Unified Studio.
- Use the **Amazon Bedrock models** tab to configure access to your Amazon Bedrock serverless models for this account and set the default models for the generative AI playground model selector in this account. For more information, see Amazon Bedrock in SageMaker Unified Studio.

Reject an account association request from an Amazon SageMaker Unified Studio domain

Complete the following to reject an association request from an Amazon SageMaker unified domain.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View requests** and select the inviting domain from the list of requests. The domain name is a hyperlink. You can also use the radio button next to the domain name and then choose **Review request**.
3. On the **Accept and configure AWS association** page, choose **Reject new permissions** to reject the association request.

Remove an associated account in Amazon SageMaker Unified Studio

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose an Amazon SageMaker unified domain name from the list. The name is a hyperlink.

3. Choose the **Account associations** tab, choose the account that you want to disassociate, and then choose **Disassociate**. In the **Disassociate account** pop up window, confirm disassociation by typing **disassociate** in the field.

Configure Amazon Bedrock in SageMaker Unified Studio in an associated account

In Amazon SageMaker Unified Studio, Generative AI enables project users to explore, build, and collaborate on generative AI applications using Amazon Bedrock foundation models and tools.

> **Important**
>
> As a user from an associated account, you can complete the procedure below to configure the available generative AI blueprints in your associated account. However, in order to fully use the generative AI capability in your Amazon SageMaker Unified Studio projects, you must also have the Generative AI application development project profile created for your associated account by the domain administrator from the AWS account that owns this domain.
>
> In the current release of Amazon SageMaker Unified Studio, project profiles for the domain can only be created by domain administrators from the AWS account that owns the domain.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View associated domains** and then choose the associated domain where you want to configure Amazon Bedrock in SageMaker Unified Studio.
3. In the **Next steps for your associated domain** section, choose **Configure** next to **Generative AI**.
4. In the **Set up generative AI** page, in the **Generative AI blueprints** section, under **Provisioning role**, specify a new or existing service role that is to be used by Amazon SageMaker Unified Studio to provision and manage resources defined in the selected blueprints in your associated account. Enabling generative AI blueprints automatically configures default resources for the essential generative AI capabilities that projects need. The following blueprints powered by

Amazon Bedrock are included: Chat Agents, Knowledge Bases, Guardrails, Functions, Flows, Prompts, and Evaluations.

5. Locate the **Default tooling blueprint deployment settings** section that contains the Tooling bluepring deployment settings used to create projects from this project profile and review them and modify the following as needed. Note that if you have already enabled the Tooling blueprint, you cannot use this procedure to modify any of the Tooling blueprint settings.

   - Under **Manage access role**, specify a service role that gives Amazon SageMaker Unified Studio the authorization to create and configure project resources using AWS CloudFormation in the project account and region. If this service role already exists in this AWS account, it is selected by default.
   - For the Tooling blueprint deployment account and region, note that by configuring Amazon Bedrock in SageMaker Unified Studio for your associated domain, you can only enable the Tooling blueprint in the same AWS account and region as your associated domain.
   - In the **Amazon S3 bucket for blueprints** section, specify an Amazon S3 bucket for blueprints in your AWS account.
   - In the **Networking** section, in the **Virtual private cloud (VPC) setting**, choose a VPC in which to provision your Amazon SageManker unified domain. VPCs tagged with Amazon SageMaker Unified Studio should be correctly configured.

     In the **Subnets** section, select at least 3 subnets in different **Availability Zones** that contain required VPC Endpoints. Private subnets are recommended, not all functionality is available when selecting public subnets.
   - In the **Data encryption** section, your data is encrypted by default with a key that AWS owns and manages for you. Encryption cannot be changed after the domain is created. Choose either **Use AWS owned key** (a key that AWS owns and manages for you) or the **Choose a different AWS KMS key (advanced)** (a key that you have permissions to use, or create a new one) and then specify an existing or create a new AWS KMS key.

6. In the **Permissions for Amazon Bedrock model access** section, specify the permissions for users to interact with the enabled Amazon Bedrock models. The system can automatically create roles to control user access and interactions with these models or you can specify existing roles.

   For the **Model provisioning** role, you can create a new or use an existing role. The system uses the role you specify as the provisioning role to create an inference profile that has access to an

Amazon Bedrock model in a project. The role you specify here is used as the provisioning role for all the Amazon Bedrock models enabled for this domain.

For the **Model consumption** role, you can create a new or use an existing role. The system uses a consumption role to grant users access to Amazon Bedrock models in the playground in the Amazon SageMaker Unified Studio.

7. Choose **Submit**.

   Once the action is successfully completed and you've finished configuring Amazon Bedrock in SageMaker Unified Studio for this associated account, you are redirected to the associated domain's details page where you can find the enabled generative AI blueprints under the **Blueprints** tab and the enabled models listed in the **Amazon Bedrock models** tab. Note, that you can manage model access directly from **Amazon Bedrock models** tab. For more information, see Amazon Bedrock in SageMaker Unified Studio. Also, if you want to publish models from your associated account, the IAM identity of the associated account must be added to the **GenerativeAIModelGovernanceProject** project. For more information, see Publishing models from associated accounts.

Connect your local Visual Studio Code to Amazon SageMaker Unified Studio spaces with remote access

You can connect remotely from Visual Studio Code (VS Code) to Amazon SageMaker Unified Studio Spaces. You can use your customized local VS Code setup, including AI-assisted development tools and custom extensions, with the scalable compute resources in Amazon SageMaker Unified Studio.

Key Concepts

VPC

Amazon Virtual Private Cloud (VPC) is a fundamental building block, allowing you to provision a logically isolated virtual network within the AWS Cloud.

Amazon SageMaker Unified Studio Space

Amazon SageMaker Unified Studio provides compute Spaces for integrated development environments (IDEs) that you can use to author code. There are two IDE applications available in Amazon SageMaker Unified Studio: JupyterLab and Code Editor. A JupyterLab Space is created in your project by default, and you can create additional Spaces as desired.

Remote Connection

A secure SSH-over-SSM tunnel between your local VS Code and a SageMaker Unified Studio Space. This connection enables interactive development and code execution in VS Code using Amazon SageMaker Unified Studio compute resources.

Configuring Amazon SageMaker Unified Studio for Remote Access

Prerequisites

> **Note**
>
> Certain features in Amazon SageMaker Unified Studio may maintain active sessions even after you log out of Amazon SageMaker Unified Studio or the associated IAM Identity

Center/SSO session. Sometimes, these disconnected sessions can persist for up to 12 hours. Affected features include:

- Spaces
- Local IDE (Visual Studio Code) Support
- Workflows
- ML Experiments (MLFlow)
- Connections
- Hyperpod
- Amazon SageMaker partner applications

To ensure the security of your environment, administrators must review and adjust session duration settings where possible and be cautious when using shared workstations or public networks.

To establish a remote connection from VS Code to a Amazon SageMaker Unified Studio Space, you must have the following prerequisites:

- Access to a Amazon SageMaker Unified Studio Domain with proper network connectivity and AWS Identity Center setup. To create an Amazon SageMaker Unified Studio domain, see Domains.
  - By default, Amazon SageMaker Unified Studio Projects create Spaces in VpcOnly mode. To support remote connection, you have three network configuration options:
    - **Public Internet Access**: Configure your Amazon SageMaker Unified Studio Projects to allow public internet access by setting `sagemakerDomainNetworkType` to `PublicInternetOnly`.
    - **VPC with NAT Gateway**: Keep Spaces in `VpcOnly` mode and attach a NAT gateway to your VPC to provide internet access. This is the default configuration with Unified Studio Quick Setup for manually setting it up. For more details, see Internet gateways.
    - **Isolated VPC with VPC Endpoints**: Keep your domain completely isolated from the internet by configuring VPC endpoints. See Configuring Isolated VPC for Remote Access for detailed setup instructions.
- Project role permissions to call SageMaker StartSession. This is the API that enables remote connectivity to a Space. The Amazon SageMaker Unified Studio managed policy has already been

updated to provide you access to call this API for the Spaces they own. If you are managing your own roles, ensure the role has the following policy:

```
{
    "Sid": "AllowStartSessionForSpaceRemoteConnection",
    "Effect": "Allow",
    "Action": [
        "sagemaker:StartSession"
    ],
    "Resource": "arn:aws:sagemaker:*:*:space/*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AmazonDataZoneProject": "${aws:PrincipalTag/
AmazonDataZoneProject}",
            "aws:ResourceTag/AmazonDataZoneUser": "${aws:PrincipalTag/
datazone:userId}"
        }
    }
}
```

- VS Code with Microsoft Remote SSH (version 0.74.0 or higher), and AWS Toolkit (version 3.87.0 or higher) extension installed on your local machine.

> **Important**
>
> Remote Space connections are currently not supported for TIP (Trusted Identity Propagation) enabled project profiles. For instructions on how to set the `enableTrustedIdentityPropagationPermissions` to false to use remote connection for Spaces, see Trusted identity propagation.

VS Code specific network requirements

Remote VS Code connection requires VS Code remote development, which needs specific network access to install the remote server and extensions. See the remote development FAQ in the VS Code documentation for full network requirements. The following is a summary of the requirements:

- Access to Microsoft's VS Code server endpoints is required to install and update the VS Code remote server.

- Access to VS Marketplace and related CDN endpoints is required for installing VS Code extensions through the extension panel (alternatively, extensions can be installed manually using VSIX files without internet connection).
- Some extensions may require access to additional endpoints for downloading their specific dependencies. See the extension's documentation for their specific connectivity requirements.

Network Configuration for Remote Access

Configuring Amazon SageMaker Unified Studio Project Profiles to allow Internet Access

To allow Spaces to be created with internet access, you can set the tooling blueprint parameter `sagemakerDomainNetworkType` to `PublicInternetOnly`. By default, it is set to `VpcOnly`. To create an Amazon SageMaker Unified Studio project profile, see Project profiles. To update an existing project profile's `sagemakerDomainNetworkType`, you need to ensure there are no running Spaces in the project. For more details see Update Project Profiles.

> **Note**
>
> This configuration is only applicable for enabling Local IDE support in Identity Center based domains, not in IAM-based domains.

Configuring Isolated VPC for Remote Access

To configure a VPC isolated from the internet and also enable remote access from VS Code, you need to create VPC endpoints and attach them to the VPC along with security groups to allow traffic to flow through the SSH tunnel. The recommended network setup is:

Use service created project security group

- When you create a Project, the service always creates the Security group on your behalf. You can identify the security group by:
  - Searching for the Unified Studio `ProjectId` in the AWS VPC console. The `projectId` can be found in the project overview page in the portal/URL when accessing the Project through CLI/API.

- Run the command `cat /opt/ml/metadata/resource-metadata.json | jq .` in the Space terminal to identify which service-created security group has been attached to the Space.

- Attach the identified Security group to the VPC endpoints created above. This setup is needed only once per project and not for every Space as security is reused across the project.
- Refer to the following table and create VPC endpoints that you require for your use cases and attach them to the Amazon SageMaker Unified Studio Domain VPC:

Service	Endpoint	Purpose	Required for
STS	com.amazonaws.<REGION>.sts	Authentication and temporary credential management	Service authentication and role assumption
SSM	com.amazonaws.<REGION>.ssm	Parameter Store and configuration management	Runtime configuration retrieval
SSM-Messages	com.amazonaws.<REGION>.ssmmessages	Session Manager communication	Secure shell access and command execution
SM Studio	aws.sagemaker.<REGION>.studio	Studio service communication	Workspace management and orchestration
SM Runtime	com.amazonaws.<REGION>.sagemaker.runtime	Model inference and runtime operations	Code execution and model serving
SM API	com.amazonaws.<REGION>.sagemaker.api	SageMaker service API calls	Resource management and service operations
DataZone	com.amazonaws.<REGION>.datazone	DataZone service access	Data discovery, governance, and sharing capabilities

Service	Endpoint	Purpose	Required for
DataZone FIPS	com.amazonaws.<REGION>.datazone-fips	FIPS-compliant secure access to Amazon DataZone services	Secure data access compliant with Federal Information Processing Standards (FIPS)

To create your own security groups, ensure traffic is allowed to and from the service-created security group for the Project.

Source control and file storage in Amazon SageMaker Unified Studio

Every project in Amazon SageMaker Unified Studio includes S3 shared storage by default. S3 shared storage is active from the moment a project is created and requires no administrator configuration. All project members can immediately read, write, and share files.

Repositories are an optional, additive capability. When you configure a Git connection at the domain level, project members can add repositories to their projects for version control, branching, and commit-based collaboration. Adding repositories does not replace or disable S3 shared storage. Both options coexist in the same project.

As an administrator, your responsibilities include:

- Understanding the default S3 shared storage behavior (see the section called "Default S3 storage")
- Setting up Git connections if your teams need repository-based version control (see the section called "Git connections")
- Configuring cross-account permissions if your domain and tooling environments are in different accounts (see the section called "Cross-account and cross-region Git configurations")

> **Important**
>
> On July 30, 2026, Amazon SageMaker Unified Studio launched a new repository experience that provides per-artifact version control, multi-repository support, and branch-based collaboration. For documentation, see the section called "Git connections". If your domain uses the previous force-push based storage model (where every save pushes directly to the remote), see the section called "Legacy experience and migration" for documentation on that experience. For migration details, see the section called "Migrating to the new repository experience".

Storage options

Amazon SageMaker Unified Studio supports the following storage options for project files.

S3 shared storage

S3 shared storage is the default option. It uses Amazon Simple Storage Service to provide a shared storage area for project files. All project members have read, write, update, and delete access to the shared storage area. This storage operates on a last-write-wins principle, meaning that files are immediately visible to all project members when modified. Team members must coordinate when working on the same files to avoid overwriting each other's changes.

Repositories

Repositories provide version control through Code Connections to GitHub, GitHub Enterprise Server, GitLab, GitLab Self-Managed, and Bitbucket. Repositories are additive. Administrators make them available by configuring Git connections at the domain level.

Default S3 storage

Every project in Amazon SageMaker Unified Studio includes S3 shared storage by default. No additional configuration is required to use this storage option.

Access model

All project members have read, write, update, and delete access to the S3 shared storage area. This storage operates on a last-write-wins principle. When multiple team members modify the same file, the most recent save overwrites previous versions.

Enabling S3 bucket versioning

Administrators can turn on S3 bucket versioning from the Amazon S3 console under Account settings. Enabling versioning allows you to preserve, retrieve, and restore previous versions of files stored in the shared storage area.

Next steps

To make repositories available to project members, configure a Git connection. For more information, see the section called “Git connections”.

Git connections

Git connections enable project members to use Git repositories for source control in Amazon SageMaker Unified Studio. You can create connections to GitHub, GitHub Enterprise Server, GitLab, GitLab Self-Managed, and Bitbucket through the AWS CodeConnections service.

> **Important**
>
> Enabling a Git connection grants all users in the account read and write access to all repositories on that connection. For full details on access implications, see the section called "Enabling a connection for project access".

By default, all Git connections are initially disabled and cannot be accessed by project users. Enabling a Git connection makes it accessible in all domains that you own. Disabling a Git connection removes access to it in all domains that you own.

Account requirements

To create and manage Git connections, you must have the following:

- An AWS account with permissions to manage Amazon SageMaker Unified Studio domains
- An active account with the Git provider you want to connect (GitHub, GitLab, or Bitbucket)
- Administrator or owner permissions in your Git provider account to authorize AWS application installations

Creating a connection

You can create Git connections from the **Connections** tab on your domain's details page in the Amazon SageMaker Unified Studio console, or from the admin portal if it is configured for your domain. Each provider has a specific setup workflow. For detailed procedures, see the following sections for each supported provider.

By default, all added Git connections are initially disabled and cannot be accessed by project members. Enabling a Git connection makes it accessible in all domains and projects in that account. Disabling a Git connection removes access in all domains and projects in that account.

Connection tagging

You can add AWS tags to your Git connections during creation. Tags are key-value pairs that help you organize and identify your connections. You can use tags to categorize connections by environment, team, or purpose.

Supported providers

Amazon SageMaker Unified Studio supports Git connections to the following providers:

- GitHub
- GitHub Enterprise Server
- GitLab
- GitLab Self-Managed
- Bitbucket

Creating a GitHub connection

Complete the following procedure to create a Git connection to GitHub.

To create a GitHub connection

1. Open the Amazon SageMaker Unified Studio console and use the Region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add a Git connection to GitHub.
3. On the domain's details page, choose the **Connections** tab.
4. Expand the **Create Git connection** dropdown and then choose **GitHub**.
5. For **Connection name**, enter a name for the connection. Optionally, add any AWS tags you want to associate with the connection. Choose **Connect to GitHub**.
6. Enter your GitHub credentials if you are prompted to provide them.
7. For the app installation, either choose an existing AWS application or install a new application:
    - If you have an existing AWS application, search for and select that application.

- If you do not have an AWS application, choose **Install a new app**. In the popup window, select the account you want to connect, choose whether to connect to **All repositories** or **Only select repositories**, and then choose **Install**.

8. Choose **Connect**.

Close the popup window and refresh the **Connections** tab. The connection appears in the list with a connection status of **Available**. You must then enable the connection for project access.

Creating a GitHub Enterprise Server connection

Complete the following procedure to create a Git connection to GitHub Enterprise Server.

To create a GitHub Enterprise Server connection

1. Open the Amazon SageMaker Unified Studio console and use the Region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add a Git connection to GitHub Enterprise Server.
3. On the domain's details page, choose the **Connections** tab.
4. Expand the **Create Git connection** dropdown and then choose **GitHub Enterprise**.
5. For **Connection name**, enter a name for the connection.
6. For **URL**, enter the URL of your GitHub Enterprise Server instance.
7. If your GitHub Enterprise Server instance is only available in a VPC, choose **Use a VPC** and then specify the VPC ID.

(Optional) Under **TLS certificate**, specify your TLS certificate. Optionally, add any AWS tags. Choose **Connect to GitHub Enterprise Server**.

This takes you to the connection details page with a status of **Pending**. Complete the following procedure to activate the pending connection.

To update a pending GitHub Enterprise Server connection

1. Open the Amazon SageMaker Unified Studio console and use the Region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain with the pending connection.

3. On the domain's details page, choose the **Connections** tab and then choose the Git connection that you want to update.
4. Choose **Update pending connection**. A popup window appears.
5. If you have an existing AWS application, search for and select it, then choose **Connect**. If you do not have an AWS application, choose **Install a new application**.
6. In the popup window, choose **Leave page** to go to the new application installation.
7. Select the organization in which you want to install the application.

Select whether you want the app to connect to **All repositories** or **Only select repositories**, and then choose **Install**. The connection status changes to **Available**. You must then enable the connection for project access.

Creating a GitLab connection

Complete the following procedure to create a Git connection to GitLab.

To create a GitLab connection

1. Open the Amazon SageMaker Unified Studio console and use the Region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add a Git connection to GitLab.
3. On the domain's details page, choose the **Connections** tab.
4. Expand the **Create Git connection** dropdown and then choose **GitLab**.
5. For **Connection name**, enter a name for the connection. Optionally, add any AWS tags. Choose **Connect to GitLab**.
6. Enter your GitLab credentials when prompted. After authentication, choose **Authorize AWS connector for GitLab**.
7. On the **Connect to GitLab** page, choose **Connect**.

Close the popup window and refresh the **Connections** tab. The new GitLab connection appears in the list with a connection status of **Available**. You must then enable this connection for project access.

Creating a GitLab self-managed connection

Complete the following procedure to create a Git connection to GitLab Self-Managed.

To create a GitLab self-managed connection

1. Open the Amazon SageMaker Unified Studio console and use the Region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add a Git connection to GitLab Self-Managed.
3. On the domain's details page, choose the **Connections** tab.
4. Expand the **Create Git connection** dropdown and then choose **GitLab self-managed**.
5. For **Connection name**, enter a name for the connection. For **URL**, enter the endpoint of the server to connect to. Choose **Connect to GitLab self-managed**.

This takes you to the connection details page with a status of **Pending**. Complete the following procedure to activate the pending connection.

To update a pending GitLab self-managed connection

1. Open the Amazon SageMaker Unified Studio console and use the Region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain with the pending connection.
3. On the domain's details page, choose the **Connections** tab and then choose the Git connection that you want to update.
4. Choose **Update pending connection**. A popup window appears.
5. If you have an existing AWS application, search for and select it, then choose **Connect**. If you do not have an AWS application, choose **Install a new application**.
6. In the popup window, choose **Leave page** to go to the new application installation.
7. Select the organization in which you want to install the application.

Select whether you want the app to connect to **All repositories** or **Only select repositories**, and then choose **Install**. The connection status changes to **Available**. You must then enable the connection for project access.

Creating a Bitbucket connection

Complete the following procedure to create a Git connection to Bitbucket.

> **Note**
>
> You must have an existing Bitbucket workspace before you can complete this procedure. Amazon SageMaker Unified Studio only supports the Bitbucket Cloud hosting option. The Data Center hosting option is not supported. For more information, see Bitbucket hosting options.

To create a Bitbucket connection

1. Open the Amazon SageMaker Unified Studio console and use the Region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add a Git connection to Bitbucket.
3. On the domain's details page, choose the **Connections** tab.
4. Expand the **Create Git connection** dropdown and then choose **Bitbucket**.
5. For **Connection name**, enter a name for the connection. Choose **Connect to Bitbucket**.
6. For **Bitbucket apps**, specify an existing app or choose **Install a new app**. Choose **Connect**. This redirects you to the Bitbucket website where you can choose your existing Bitbucket workspace and grant access by choosing **Grant access**.

Enabling a connection for project access

After a Git connection is created and updated to become available, you can enable it for project members to use in your domain. Complete the following procedure to enable project access for a Git connection.

To enable a Git connection

1. Open the Amazon SageMaker Unified Studio console and use the Region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to enable a connection.

3. On the domain's details page, choose the **Connections** tab.
4. Choose the connection that you want to enable, and then choose **Enable**. A confirmation window appears.
5. Choose **Enable**. When you refresh the page, the connection appears as **Enabled**.

> **Important**
>
> When you enable a Git connection, all users who can sign in to any domain in the account have read and write access to all repositories on that connection. This access applies regardless of the user's project membership or permission level. There is no repository-level isolation within a single account. To enforce isolation between repositories, use separate AWS accounts. Do not store sensitive information in connected repositories unless all users in the account are authorized to access that information.

Disabling or deleting a connection

You can disable a Git connection to temporarily remove project access, or delete a connection to permanently remove it from your domain.

To disable or delete a Git connection

1. Open the Amazon SageMaker Unified Studio console and use the Region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain with the connection you want to modify.
3. On the domain's details page, choose the **Connections** tab.
4. Choose the connection that you want to disable or delete.
5. Choose **Disable** to remove project access, or choose **Delete** to permanently remove the connection.

> **Note**
>
> If you disable or delete a connection, the local repository clone remains in the user's IDE. However, users can no longer push or pull changes to or from the remote repository.

When you disable or delete a connection, projects that have repositories using that connection are affected as follows:

- Existing local clones remain in the project. Project members can continue viewing tracked artifacts.
- Push, pull, and branch operations fail because the connection is no longer available.
- Project members cannot add new repositories using that connection.
- If you re-enable the connection, repository operations resume without requiring project members to re-add repositories.

Cross-account and cross-region Git configurations

If your Amazon SageMaker Unified Studio domain uses Git connections from a different AWS account, you must configure AWS Resource Access Manager (RAM) sharing and ensure that the appropriate IAM permissions are in place.

RAM permission version

Cross-account Git configurations require RAM resource shares with the correct permission version. If you have existing RAM shares, they don't automatically update to newer permission versions. You must manually update the RAM share permissions to include the required CodeConnections actions.

To update your RAM share permissions, complete the following steps:

1. Open the AWS RAM console.
2. Navigate to your resource share for Amazon SageMaker Unified Studio.
3. Update the permission version to include the latest CodeConnections actions.

IAM permissions

AWS managed policies for Amazon SageMaker Unified Studio already include the required permissions for cross-account Git operations. If you use custom IAM policies, you must add the following permissions:

- `codeconnections:ListTagsForResource`

- `codeconnections:GetConnection`
- `codeconnections:UseConnection`
- `datazone:StartCompute`
- `datazone:GetCompute`
- `datazone:StopCompute`
- `datazone:StartNotebookSync`

> **Important**
>
> If these permissions are missing from your custom policies, Git operations in cross-account configurations fail silently or return authorization errors. Verify that all required permissions are included before troubleshooting connection issues.

Cross-region support

Cross-region Git connections are supported in IAM Identity Center (IDC) domains. You can connect to Git repositories hosted in a different AWS Region than your Amazon SageMaker Unified Studio domain.

> **Note**
>
> Self-hosted GitLab and GitHub Enterprise Server instances must be accessible from the tooling Region configured for your domain. Ensure that your self-hosted instance network configuration allows connectivity from the Region where your Amazon SageMaker Unified Studio compute resources run.

Legacy experience and migration

This section is for administrators managing projects that use the previous storage and Git connection experience. If you are configuring a new domain or have already migrated, see the section called "Git connections" for the current documentation. Below you will find the documentation for the previous force-push experience.

Legacy experience

Unified storage (Legacy)

> **Note**
>
> You can't create new projects with AWS CodeCommit. Existing projects that were created using CodeCommit will continue to work.

Configuring project storage options (Legacy)

Storage type selection guidelines

Choose S3 storage for teams with limited Git experience, simple projects without complex versioning needs, quick experimentation and ad-hoc analysis, and scenarios requiring maximum regional availability.

Choose Git-based storage for projects requiring strict version control, collaborative development with code reviews, integration with existing development workflows, and cross-project code sharing requirements.

Amazon S3 storage configuration

S3 storage is the default option and requires minimal configuration. As an administrator, you can enable S3 bucket versioning to configure basic versioning capabilities for projects that require file history tracking.

Git-based storage configuration

For projects requiring advanced version control, you can configure connections to existing Git repositories during project creation and set default branches and branching policies for effective branch management. Additionally, you can enable multiple projects to use the same repository when appropriate, allowing for efficient cross-project sharing of code and resources. However, it's important to note that Git-based storage availability is limited by the CodeConnections service, which may impose regional limitations on deployment options. For more information, see CodeConnections.

For storage organization, refer to Managing storage resources.

Performance and cost optimization (Legacy)

File size limitations

Files over 15 MB cannot be directly uploaded to shared folders through the Amazon SageMaker Unified Studio interface in space-based tools like JupyterLab and Code Editor. Large files must be uploaded to local folder in JupyterLab first, then copy or move to the shared folder if needed.

Cost management considerations

Heavy file read/write workloads in shared storage can incur additional S3 access costs, while frequent S3 operations may affect performance for collaborative workflows.

For space-based tools (like JupyterLab): Apart from the shared folder, space-based tools such as JupyterLab and Code Editor also have an EBS-based personal folder per user per project. We recommend using this local storage for intermediate and temporary files during development work, as it provides superior performance for frequent file operations. Only move final versions of files that are ready for sharing with other project users to the S3 shared folder. This approach minimizes S3 operations and associated costs while maintaining optimal performance for iterative development work.

> **Note**
>
> This storage strategy applies specifically to space-based tools like JupyterLab and Code Editor that have access to both local EBS storage and shared storage. For web-based tools like Query Editor, intermediate or temporary files are generated during normal operation, but since these tools don't have a dedicated personal folder, all files are saved directly to shared storage. Web-based tools rely entirely on the shared storage for file operations and don't have the option to use local EBS storage for performance optimization.

Feature comparison matrix (Legacy)

The following table provides a comprehensive comparison of key features between Git-based and S3 storage options to help you make informed decisions when configuring storage for your Amazon SageMaker Unified Studio projects.

Feature	Git-based projects	S3-based projects
Audit trail	Full Git commit history tracks all changes including author information, timestamp s, and detailed commit messages. Complete audit trail is maintained in the Git repository.	No systematic tracking of file changes or user attributi on. Basic file modification timestamps are available, but no detailed change history or commit messages are maintained.
Version history	Complete Git versioning with full commit history, branching , and merging capabilities. Version history is accessibl e through Git commands in JupyterLab or through the Git provider's web interface.	S3 bucket versioning must be enabled from the S3 console by administrators. When enabled, version history will be available from the S3 console, allowing you to view and restore previous versions of files.
Shared storage	All project members work through same Git repositor y. Files must be "Saved to project" or pushed to the repo	Shared folder (shared_f iles/) accessible by all project members. Direct file sharing.
Cross-project sharing	Multiple SMUS projects can connect to the same Git repository, enabling code and resource sharing across different project teams.	Each project has its own dedicated S3 storage location. Files cannot be directly shared between projects without manual copying.
Regional availability	Limited by availability of CodeConnections service.	Available in all regions where S3 is available.
Change documentation	All changes are documented through Git commit messages that developers write when saving changes. Provides	No built-in mechanism for documenting changes. File modifications occur without requiring or capturing change descriptions.

Feature	Git-based projects	S3-based projects
	detailed context for each modification.	
Setup complexity	Requires Git repository configuration	Minimal configuration required

Git connections (Legacy)

Git connections enable you to check in and check out files, and manage your code repository. When you create an Amazon SageMaker unified domain, a default git connection to CodeCommit is provided for you to manage your code. You can also create and enable new 3P Git connections to GitHub, GitHub Enterprise Server, GitLab, and GitLab Self-Managed.

> **Important**
>
> When you enable a Git connection, all users who can sign in to any domain in the account have read and write access to all repositories on that connection. This access applies regardless of the user's project membership or permission level. To enforce isolation between repositories, use separate AWS accounts.

> **Note**
>
> You can't create new projects with AWS CodeCommit. Existing projects that were created using CodeCommit will continue to work.

By default, all added Git connections are initially disabled and cannot be accessed by project users. Enabling a Git connection makes it accessible in all the domains that you own, and disabling a Git connection removes access to it in all the domains that you own.

You can use the following procedures to create 3P Git connections.

Github connections

Complete the following procedure to create a 3P Git connection to GitHub:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add a 3P Git connection to GitHub.
3. On the domain's details page, choose the **Connections** tab.
4. Expand the **Create Git connection** drop-down menu and then choose **Github**.
5. In the **Create a connection** window, in the **Connection name** field, specify the name of the connection. (Optional - enter in any AWS tags you want to add to the connection and then choose **Connect to Github**.
6. Enter in your GitHub credentials if you are prompted to provide them.
7. Optional - for the app installation, either choose an AWS application to connect to Amazon SageMaker Unified Studio that you previously installed, or install a new application.
   - If you have installed an AWS application, search for and select that application.
   - If you do not have an AWS application, choose **Install a new app**. A popup window appears.
     - Select the account you want to install the application and establish a connection to.
     - Select whether you want the app to connect to **All repositories** or **Only select repositories**.
     - Choose **Install**.
8. Choose **Connect**.
9. Close the popup window and refresh the **Connections** tab. The connection appears in the list with a connection status of **Available**. You then need to enable the connection for project access in the Amazon SageMaker Unified Studio.

Github Enterprise server connections

Complete the following procedure to create a 3P Git connection to GitHub Enterprise Server:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add a 3P Git connection to GitHub Enterprise Server.

3. On the domain's details page, choose the **Connections** tab.
4. Expand the **Create Git connection** drop-down menu and then choose **GitHub Enterprise**.
5. In **Connection name**, provide a name for the connection.
6. In **URL**, specify the URL of your GitHub Enterprise Server instance.
7. If your GitHub Enterprise Server instance is only available in a VPC, choose **Use a VPC** and then specify the VPC ID.
8. (Optional) Under **TLS certificate**, specify your TLS certificate.
9. (Optional) Specify any AWS tags you want to add to the connection.
10. Choose **Connect to GitHub Enterprise Server**. This brings you to the connection details page, and the status of the connection is **Pending**. You then need to update the pending connection to make it active.

Complete the following procedure to update a pending 3P Git connection to GitHub Enterprise Server:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add a 3P Git connection to GitHub.
3. On the domain's details page, choose the **Connections** tab and then choose the Git connection that you want to update.
4. Choose **Update pending connection**. A new popup window appears inviting you to enter information for your GitHub Enterprise Server.
5. If you have installed an AWS application to connect to Amazon SageMaker Unified Studio, search for it and select that application and choose **Connect**. If you do not have an AWS application to connect to Amazon SageMaker Unified Studio, choose **Install a new application**.
6. In the pop up window, choose **Leave page**. This takes you to the new application installation.
7. Select the organization in which you want to install the application and establish a connection.
8. Select whether you want the app to connect to **All repositories** or **Only select repositories**.
9. Choose **Install**.

This brings you to the connection details page, and the status of the connection changes to **Available**. You then need to enable the connection for project access in the Amazon SageMaker Unified Studio.

GitLab connections

Complete the following procedure to create a 3P Git connection to GitLab:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add a 3P Git connection to GitLab.
3. On the domain's details page, choose the **Connections** tab.
4. Expand the **Create Git connection** drop-down menu and then choose **GitLab**.
5. In **Connection name**, provide a name for the connection, optionally, enter in any AWS tags you want to add to the connection, and then choose **Connect to GitLab**.
6. Enter in your GitLab credentials when you are prompted to provide them. Once authenticated, choose **Authorize AWS connector for GitLab**.
7. On the **Connect to GitLab** page, choose **Connect**.
8. Close the popup window and refresh the **Connections** tab. The new GitLab connection appears in the list with a connection status of **Available**. You must then enable this connection for project access in the Amazon SageMaker Unified Studio.

GitLab self-managed connections

Complete the following procedure to create a 3P Git connection to GitLab Self-Managed:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add a 3P Git connection to GitLab self-managed.
3. On the domain's details page, choose the **Connections** tab.
4. Expand the **Create Git connection** drop-down menu and then choose **GitLab self-managed**.

5. On the **Connect to GitLab self-managed** page, in **Connection name**, specify the name for the connection, and in the **URL**, specify the endpoint of the server to connect to, and then choose **Connect to GitLab self-managed**. This brings you to the connection details page, and the status of the connection is **Pending**. You then need to update the pending connection to make it active.

Complete the following procedure to update a pending 3P Git connection to GitLab self-managed:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to update your pending connection.
3. On the domain's details page, choose the **Connections** tab and then choose the Git connection that you want to update.
4. Choose **Update pending connection**. A new popup window appears inviting you to enter information for your GitLab self-managed.
5. If you have installed an AWS application to connect to Amazon SageMaker Unified Studio, search for it and select that application and choose **Connect**. If you do not have an AWS application to connect to Amazon SageMaker Unified Studio, choose **Install a new application**.
6. In the pop up window, choose **Leave page**. This takes you to the new application installation.
7. Select the organization in which you want to install the application and establish a connection.
8. Select whether you want the app to connect to **All repositories** or **Only select repositories**.
9. Choose **Install**.

Bitbucket connections

Complete the following procedure to create a 3P Git connection to Bitbucket:

> **Note**
>
> You must have an existing Bitbucket workspace before you can complete this procedure.

Currently, Amazon SageMaker Unified Studio only supports the BitBucket Cloud hosting option. The Data Center hosting option is not supported in the currect release of Amazon SageMaker Unified Studio. For more information, see Bitbucket hosting options.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add a 3P Git connection to Bitbucket.
3. On the domain's details page, choose the **Connections** tab.
4. Expand the **Create Git connection** drop-down menu and then choose **Bitbucket**.
5. On the **Create a connection** page, in **Connection name**, specify the name for the connection, and then choose **Connect to Bitbucket**.
6. On the **Connect to Bitbucket** page, in **Bitbucket apps**, specify an existing app or choose **Install a new app** and then choose **Connect**. This redirects you to the bitbucket website where you can choose your existing **Bitbucket workspace** and grant Amazon SageMaker Unified Studio access to it by choosing **Grant access**.

Enable connections for project access

After a 3P Git connection is created and updated to become available, you can enable it for project members to use in your domain. Complete the following procedure to enable project access for a 3P Git connection:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to enable your connections for project members to use.
3. On the domain's details page, choose the **Connections** tab.
4. Choose the connection that you want to enable, and then choose **Enable**. A popup window appears so that you can confirm the decision.

5. Choose **Enable**. When you refresh the page, the connection then appears as **Enabled**. This means that project members have access to the connection and can use it in projects within that domain.

> **Important**
>
> When you enable a Git connection, all users who can sign in to any domain in the account have read and write access to all repositories on that connection. This access applies regardless of the user's project membership or permission level. There is no repository-level isolation within a single account. To enforce isolation between repositories, use separate AWS accounts. Do not store sensitive information in connected repositories unless all users in the account are authorized to access that information.

The following note describes the behavior when a connection is later disabled or deleted.

> **Note**
>
> When you create and enable a connection for Git access and the user accesses this connection in the JupyterLab in SageMaker Unified Studio in Amazon SageMaker Unified Studio, the repository is cloned, in other words, a local copy of the repository is created in the Amazon SageMaker Unified Studio project. If the administrator later disables or deletes this Git connection, the local repository remains in the user's IDE, but users can no longer push or pull files to or from it. For more information about Git operations in Amazon SageMaker Unified Studio, see Performing Git operations.

Migrating to the new repository experience

Migrating to the new repository experience requires a project update. The migration is initiated by the project owner from the Repositories page in their project. As an administrator, be aware of the following:

- **Cross-account prerequisites**: If your projects use cross-account configurations, you must update RAM permissions before projects can successfully migrate. Without updated permissions, the repository clone fails and the project remains in the previous mode. For details, see the section called “Cross-account and cross-region Git configurations”.

- **Project updates include the Git transition**: Any service-initiated or admin-initiated project update includes the migration to the new repository experience. Project owners cannot accept other updates selectively while excluding the repository experience change.
- **No forced migration**: The migration is opt-in. Projects that are not updated continue with the previous behavior indefinitely.

Project profiles in Amazon SageMaker Unified Studio

In Amazon SageMaker Unified Studio, a project profile defines an uber template for projects in your Amazon SageMaker unified domains. A project profile is a collection of blueprints which are configurations used to create projects. A project profile can define if a particular blueprint is enabled during the creation of the project, or available later for the project users to enable on-demand.

You must be an administrator of an Amazon SageMaker unified domain to create and manage project profiles. In the current release of Amazon SageMaker Unified Studio, you can create a set of template project profiles. These templates serve as pre-defined configurations that include specific combinations of capabilities. When you select a template, Amazon SageMaker creates the corresponding project profile in your domain based on that template's definition. Additionally, you can create custom project profiles that include any combination of capabilities tailored to your specific needs. In Amazon SageMaker Unified Studio, you can create the following template project profiles:

- All capabilities project profile
- SQL analytics project profile
- Generative AI application development project profile
- Custom project profile

All capabilities project profile

The All capabilities project profile enables your Amazon SageMaker Unified Studio users to analyze data and build machine learning and generative AI models and applications powered by Amazon Bedrock, Amazon EMR, AWS Glue, Amazon Athena, Amazon SageMaker AI, and Amazon SageMaker Lakehouse.

You can use the following procedures to create an all capabilities project profile.

Topics

- Configure all capabilities for your Amazon SageMaker unified domain
- Create an All capabilities project profile

Configure all capabilities for your Amazon SageMaker unified domain

Complete the following procedure to configure all capabilities for your Amazon SageMaker unified domain.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Either create a new domain or choose an existing domain where you want to configure all capabilities.
3. On the domain's details page, under the **Next steps for your domain** section, choose the **Configure** button next to the **All capabilities**.
4. On the **Create project profile: All capabilities** page, in the **All capabilities** section, review the on-create and on-demand capabilities for this project profile. On-create capabilities are configured and ready to use when the project is created. On-demand capabilities can be configured when needed after project creation to control cost.
5. On the **Create project profile: All capabilities**, expand the **Default tooling blueprint deployment settings** section and review the settings, including the Tooling blueprint deployment account and region.

   > **Important**
   >
   > Note that by configuring all capabilities for your domain (this procedure), you can only enable the Tooling blueprint in the same AWS account and region as your domain. To enable the Tooling blueprint in an account or region that's different from that of your domain's, see Create an All capabilities project profile or Custom project profile.

6. On the **Create project profile: All capabilities**, in the **Enable blueprints** section, review the following blueprints that will be enabled for this project profile.

   > **Important**
   >
   > Note that by configuring all capabilities for your domain (this procedure), you can only enable these blueprints in the same AWS account and region as your domain. To enable these blueprints in an account or region that's different from that of your domain's, see Create an All capabilities project profile or Custom project profile.

- MLExperiments
- Workflows
- LakehouseCatalog
- EmrOnEc2
- Tooling
- RedshiftServerless
- LakeHouseDatabase
- EmrServerless
- AmazonBedrockGenerativeAI

7. On the **Create project profile: All capabilities** page, in the **Manage access role** section, specify a service role that gives Amazon SageMaker Unified Studio authorization to ingest and manage access to datashares, tables and views in Amazon Redshift. You can create a new or using an existing role.
8. On the **Create project profile: All capabilities** page, in the **Provisioning role** section, specify a service role that gives Amazon SageMaker Unified Studio authorization to ingest and manage access to datashares, tables and views in Amazon Redshift.
9. On the **Create project profile: All capabilities** page, in the **Amazon S3 bucket for blueprints** section, specify an Amazon S3 bucket for blueprints in your AWS account.
10. On the **Create project profile: All capabilities** page, in the **Networking section**, specify a VPC in which to provision your Amazon SageMaker unified domain. VPCs tagged with Amazon SageMaker Unified Studio should be correctly configured. In the **Subnets** section, select at least 3 subnets in different **Availability Zones** that contain required VPC Endpoints. Private subnets are recommended, not all functionality is available when selecting public subnets.
11. In the **Data encryption** section, specify the encryption settings. Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.
12. In the **User role policy** section, you have the option to specify your own user role policy. Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, AI, and ML actions. You can attach your own AWS IAM policies to the role rather than using the default system-managed policy. This provides more granular control over permissions but requires knowledge of IAM policy configuration. The IAM policy must include all necessary permissions required for the service to function properly.

13. On the **Create project profile: All capabilities** page, in the **Authorization - optional** section, specify who can use this project profile to create projects in all domain units. This can also be done per domain unit in Amazon SageMaker Unified Studio. Choose either **Selected users and groups** (select which users and groups are authorized to use this project profile) or **Allow all users and groups** (allow any user to use this project profile).

> **Note**
>
> Projects do not provide strong security isolation. To limit cross-domain and cross-project resource discovery you can consider creating projects in separate accounts.

14. Choose **Create project profile**.

After you complete this procedure, your All capabilities project profile for this domain is created and all the supported blueprints for it are enabled. Your domain users can then proceed to use this project profile to create projects in Amazon SageMaker Unified Studio.

Create an All capabilities project profile

Complete the following procedure to create a All capabilities project profile for your Amazon SageMaker unified domain. Once this procedure is complete, your All capabilities project profile will only include the capabilities defined in the Tooling blueprint. To complete configuring all capabilities for your Amazon SageMaker unified domain, you must then use the **Blueprints** tab and configure the following blueprints for this project profile:

- MLExperiments
- Workflows
- LakehouseCatalog
- EmrOnEc2
- RedshiftServerless
- LakeHouseDatabase
- EmrServerless
- AmazonBedrockGenerativeAI

> **Important**
>
> Note that when you enable a blueprint, by default, you are enabling it in the same region as your domain. When you are enabling blueprints for a project profile that is created and enabled in a different region from your domain, you must enable these blueprints in same region where this project profile is enabled (in addition to enabling this blueprint in the same region as your domain). You can do this via the **Regions** tab in the blueprint details page. This applies to all blueprints, including the Tooling blueprint.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Either create a new domain or choose an existing domain where you want to create a All capabilities project profile.
3. On the domain's details page, choose the **Project profiles** tab and then choose **Create**.
4. On the **Create project profile** page, in the **Project profile name and description** section, specify the name of the project profile and the description.
5. On the **Create project profile** page, in the **Project profile creation options** section, choose **Create from a template**, and then under **Project profile templates**, choose **All capabilities**.
6. On the **Create project profile** page, in the **Default tooling blueprint deployment settings** section, review the selections for the default deployment settings for the Tooling blueprint.

   - On the **Create project profile** page, in the **Project files storage** section, choose a storage configuration type from Amazon S3 - new and Git repository. For more information on storage types, see ._unified-storage.xml

   > **Important**
   >
   > Note that by creating this project profile from a template, you can either enable the Tooling blueprint in the same AWS account and region as your domain (prepopulated by default) or you can enable the Tooling blueprint in a different AWS account and region from this domain (an associated account).

7. On the **Create project profile** page, in the **Authorization - optional** section, specify who can use this project profile to create projects in all domain units. This can also be done per domain

unit in the Amazon SageMaker Unified Studio. You can specify **Selected users and groups** or **Allow all users and groups** options.

> **Note**
>
> Projects do not provide strong security isolation. To limit cross-domain and cross-project resource discovery you can consider creating projects in separate accounts.

8. On the **Create project profile** page, in the **Project profile readiness** section, specify whether you want to enable this project profile on creation. Unless you check the **Enable project profile on creation** checkbox, your project profile is disabled and not available to use for Amazon SageMaker Unified Studio projects after its creation. Leaving a project profile in a disabled state upon creation gives you the opportunity to customize your blueprints before making the project profile available.
9. Choose **Create project profile**.

> **Important**
>
> After you complete this procedure, your All capabilities project profile will only include the capabilities defined in the Tooling blueprint. You can further customize this project profile and configure it to include all capabilities by using the **Blueprints** tab to enable the rest of its required blueprints. They are the following:
>
> - MLExperiments
> - Workflows
> - LakehouseCatalog
> - EmrOnEc2
> - RedshiftServerless
> - LakeHouseDatabase
> - EmrServerless
> - AmazonBedrockGenerativeAI

Generative AI application development project profile

A Generative AI application development project profile enables generative AI solutions from Amazon Bedrock for your Amazon SageMaker unified domains. It provides project users in Amazon SageMaker Unified Studio with the access to the following generative AI tools: Bedrock Chat Agents, Bedrock Knowledge Bases, Bedrock Guardrails, Bedrock Functions, Bedrock Flows, Bedrock Prompts, and Bedrock Evaluations.

You can complete either of the following procedures to create a Generative API application development project profile in an Amazon Sagemaker unified domain.

Topics

- Configure Amazon Bedrock in SageMaker Unified Studio for your domain
- Create a generative AI application development project profile

Configure Amazon Bedrock in SageMaker Unified Studio for your domain

Complete the following procedure to configure Amazon Bedrock in SageMaker Unified Studio for your domain.

> **Important**
>
> In the current release of Amazon SageMaker Unified Studio, project profiles for the domain can be created only by a domain administrator from the AWS account that owns the domain. Completing this procedure as a user from an associated account only enables the generative AI blueprints but it doesn't create the Generative AI application development project profile. A domain administrator from the AWS account that owns the domain must create the Generative AI application development project profile in the domain for the associated accounts.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Either create a new domain or choose an existing domain where you want to configure Amazon Bedrock in SageMaker Unified Studio.

3. On the domain's details page, under the **Next steps for your domain** section, choose the **Configure** button next to the **Generative AI** domain capability.
4. On the **Create project profile: Amazon Bedrock generative AI** page, locate the **Generative AI blueprints** section and review the settings.

   As part of configuring Amazon Bedrock in SageMaker Unified Studio for your domain (this procedure) you are creating the Generative AI application development project profile and therefore you must enable the blueprints that contain the tools, resources, and parameters that this project profile requires. The following blueprints are enabled when you create this project profile as part of this procedure:

   - AmazonBedrockChatAgent
   - AmazonBedrockKnowledgeBase
   - AmazonBedrockGuardrail
   - AmazonBedrockFunction
   - AmazonBedrockFlow
   - AmazonBedrockPrompt
   - AmazonBedrockEvaluation

   > **Important**
   >
   > Note that by configuring Amazon Bedrock in SageMaker Unified Studio for your domain (this procedure), you can only enable the generative AI blueprints for this project profile in this domain's AWS account and Region. To enable these blueprints in an associated account, see Configure Amazon Bedrock in SageMaker Unified Studio in an associated account.

   Under **Provisioning role**, specify a new or existing service role that is to be used by Amazon SageMaker Unified Studio to provision and manage resources defined in the selected blueprints in your account.
5. On the **Create project profile: Amazon Bedrock generative AI** page, locate the **Default tooling blueprint deployment settings** section that contains the Tooling blueprint deployment settings used to create projects from this project profile and review them and

modify the following as needed. Note that if you have already enabled the Tooling blueprint, you cannot use this procedure to modify any of the Tooling blueprint settings.

- Under **Manage access** role, specify a service role that gives Amazon SageMaker Unified Studio the authorization to create and configure project resources using AWS CloudFormation in the project account and region. If this service role already exists in this AWS account, it is selected by default.
- For the Tooling blueprint deployment account and region, note that by configuring Amazon Bedrock in SageMaker Unified Studio capability for your domain (this procedure), you can only enable the Tooling blueprint in the same AWS account and region as your domain. To enable the Tooling blueprint in an associated account, see Configure Amazon Bedrock in SageMaker Unified Studio in an associated account.
- In the **Amazon S3 bucket for blueprints** section, specify an Amazon S3 bucket for blueprints in your AWS account.
- In the **Networking** section, in the **Virtual private cloud (VPC) setting**, choose a VPC in which to provision your Amazon SageManker unified domain. VPCs tagged with Amazon SageMaker Unified Studio should be correctly configured.

  In the **Subnets** section, select at least 3 subnets in different **Availability Zones** that contain required VPC Endpoints. Private subnets are recommended, not all functionality is available when selecting public subnets.
- In the **Data encryption** section, your data is encrypted by default with a key that AWS owns and manages for you. Encryption cannot be changed after the domain is created. Choose either **Use AWS owned key** (a key that AWS owns and manages for you) or the **Choose a different AWS KMS key (advanced)** (a key that you have permissions to use, or create a new one) and then specify an existing or create a new AWS KMS key.
- In the **User role policy** section, you have the option to specify your own user role policy. Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, AI, and ML actions. You can attach your own AWS IAM policies to the role rather than using the default system-managed policy. This provides more granular control over permissions but requires knowledge of IAM policy configuration. The IAM policy must include all necessary permissions required for the service to function properly.

6. On the **Create project profile: Amazon Bedrock generative AI** page, in the **Authorization - optional** section, specify who can use this project profile to create projects in all domain units. This can also be done per domain unit in the Amazon SageMaker Unified Studio. Choose either

Selected users and groups (select which users and groups are authorized to use this project profile) or **Allow all users and groups** (allow any user to use this project profile).

> **Note**
>
> Projects do not provide strong security isolation. To limit cross-domain and cross-project resource discovery you can consider creating projects in separate accounts.

7. On the **Create project profile: Amazon Bedrock generative AI** page, in the **Permissions for Bedrock model access** section, specify the permissions for users to interact with the enabled Amazon Bedrock models. The system can automatically create roles to control user access and interactions with these models or you can specify existing roles.

   For the **Model provisioning** role, you can create a new or use an existing role. The system uses the role you specify as the provisioning role to create an inference profile that has access to an Amazon Bedrock model in a project. The role you specify here is used as the provisioning role for all the Amazon Bedrock models enabled for this domain.

   For the **Model consumption** role, you can create a new or use an existing role. The system uses a consumption role to grant users access to Amazon Bedrock models in the playground in Amazon SageMaker Unified Studio.
8. Choose **Next** to advance to the **Configure model access** page.
9. On the **Configure model access** page, in the **Models** section, you can configure access to your Amazon Bedrock serverless models by enabling or disabling them for this domain.

   The system queries Amazon Bedrock and displays a list of Amazon Bedrock serverless models to which you have access. If no models are listed or if a specific model is missing, visit the Amazon Bedrock management console for the appropriate account and Region to grant access. If you have updated model access in Amazon Bedrock, choose the refresh icon in the **Amazon Bedrock Models** tab to refresh the updated list of accessible models

   The following are important elements to consider as you review the generated list of models:

   - Every model in the list is prepopulated with certain details, including modality, inference type, whether it's enabled in projects and playground, and roles for model access. A model's modality indicates the type of output data it can generate. Amazon Bedrock in SageMaker Unified Studio supports Amazon Bedrock foundation models with on-demand throughput and on-demand cross-region inference. If a model supports both on-demand and on-

demand cross-region inference, it appears in the list twice with the appropriate value listed in the **Inference** column. Amazon Bedrock in SageMaker Unified Studio does NOT support provisioned throughput, custom models, or imported models.

- For easy setup, the system pre-selects accessible models that support on-demand throughput, excluding legacy models, to enable in projects and playground. Review and adjust the list to enable models for projects and playgrounds based on your specific requirements.
- If the model that you want to manage for your Amazon SageMaker Unified Studio users is not present in the list, make sure that it has been enabled for access in Amazon SageMaker Unified Studio. This is done in the Amazon Bedrock management console. For more information, see Amazon Bedrock Documentation.

10. On the **Configure model access** page, in the **Default models - optional** section, you can set default models for the generative AI playgrounds in Amazon SageMaker Unified Studio.

    Amazon Bedrock in SageMaker Unified Studio supports generative AI playgrounds that enable Amazon SageMaker unified domain users to easily experiment with Amazon Bedrock models. Users can send prompt requests to various models and view the responses. There are two types of playgrounds in the Amazon Bedrock in SageMaker Unified Studio: the chat playground and the image and video playground.

    For the **Chat playground - optional**, select a default model from the drop-down menu. The drop-down menu includes only the models that support **Text** as the output modality and are enabled for playground use.

    For the **Image and video playground - optional**, select a default model from the drop-down menu. The drop-down menu will include only the models that support either **Image** or **Video** as the output modality and are enabled for playground use.

11. Choose **Finish** to complete configuring Amazon Bedrock in SageMaker Unified Studio for this domain.

Once the action is successfully completed and you've finished configuring Amazon Bedrock in SageMaker Unified Studio for this domain, you are redirected to the domain's details page where you can find the enabled generative AI blueprints under the **Blueprints** tab, a Generative AI project profile under the **Project profiles** tab, and the enabled models listed in the **Amazon Bedrock models** tab. Note, that you can manage model access directly from **Amazon Bedrock models** tab. For more information, see Amazon Bedrock in SageMaker Unified Studio

Create a generative AI application development project profile

Complete the following procedure to create a Generative AI application development project profile for your Amazon SageMaker unified domain. Once this procedure is complete, your Generative AI application development project profile will only include the capabilities defined in the Tooling blueprint. To configure the full generative AI application development capability for your Amazon SageMaker unified domain, you must then use the **Blueprints** tab and configure the **AmazonBedrockGenerativeAI** blueprint for this project profile. The **AmazonBedrockGenerativeAI** blueprint contains the following generative AI blueprints:

- AmazonBedrockChatAgent
- AmazonBedrockKnowledgeBase
- AmazonBedrockGuardrail
- AmazonBedrockFunction
- AmazonBedrockFlow
- AmazonBedrockPrompt
- AmazonBedrockEvaluation

> **Important**
>
> Note that when you enable a blueprint, by default, you are enabling it in the same region as your domain. When you are enabling blueprints for a project profile that is created and enabled in a different region from your domain, you must enable these blueprints in same region where this project profile is enabled (in addition to enabling this blueprint in the same region as your domain). You can do this via the **Regions** tab in the blueprint details page. This applies to all blueprints, including the Tooling blueprint.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Either create a new domain or choose an existing domain where you want to create a generative AI application development project profile.
3. On the domain's details page, choose the **Project profiles tab** and then choose **Create**.

4. On the **Create project profile** page, in the **Project profile name and description** section, specify the name of the project profile and the description.
5. On the **Create project profile** page, in the **Project profile creation options** section, choose **Create from a template**, and then under **Project profile templates**, choose **Generative AI application development**.
6. On the **Create project profile** page, in the **Default tooling blueprint deployment settings** section, review the selections for the default deployment settings for the Tooling blueprint.
   - On the **Create project profile** page, in the **Project files storage** section, choose a storage configuration type from Amazon S3 - new and Git repository. For more information on storage types, see ._unified-storage.xml

   > **Important**
   >
   > Note that by creating this project profile from a template, you can either enable the Tooling blueprint in the same AWS account and region as your domain (prepopulated by default) or you can enable the Tooling blueprint in a different AWS account and region from this domain (an associated account).

7. On the **Create project profile** page, in the **Authorization - optional** section, specify who can use this project profile to create projects in all domain units. This can also be done per domain unit in the Amazon SageMaker Unified Studio. You can specify **Selected users and groups** or **Allow all users and groups** options.

   > **Note**
   >
   > Projects do not provide strong security isolation. To limit cross-domain and cross-project resource discovery you can consider creating projects in separate accounts.

8. On the **Create project profile** page, in the **Project profile readiness** section, specify whether you want to enable this project profile on creation. Unless you check the **Enable project profile on creation** checkbox, your project profile is disabled and not available to use for Amazon SageMaker Unified Studio projects after its creation. Leaving a project profile in a disabled state upon creation gives you the opportunity to customize your blueprints before making the project profile available.
9. Choose **Create project profile**.

SQL analytics project profile

The SQL analytics project profiles enables your users to query Amazon SageMaker Lakehouse, Amazon Redshift and Amazon Athena data in their Amazon SageMaker Unified Studio projects. Amazon SageMaker Unified Studio project members can analyze their data in Amazon SageMaker Lakehouse using SQL.

You can complete the following procedures to create a SQL analytics project profile for your Amazon SageMaker unified domain.

Topics

- Configure SQL analytics for your Amazon SageMaker unified domain
- Create a SQL analytics project profile

Configure SQL analytics for your Amazon SageMaker unified domain

Complete the following procedure to configure SQL analytics capability for your Amazon SageMaker unified domain.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Either create a new domain or choose an existing domain where you want to configure SQL analytics.
3. On the domain's details page, under the **Next steps for your domain** section, choose the **Configure** button next to the **SQL** capability.
4. On the **Create project profile - SQL analytics** page, in the **SQL analytics** section, review the capabilities, tools, and functionalities that are enabled for this project profile.
5. On the **Create project profile: SQL analytics**, expand the **Default tooling blueprint deployment settings** section and review the settings, including the Tooling blueprint deployment account and region.

> **Important**
>
> Note that by configuring the SQL analytics capability for your domain (this procedure), you can only enable the Tooling blueprint in the same AWS account and region as your

domain. To enable the Tooling blueprint in an account or region that's different from that of your domain's, see Create a SQL analytics project profile or Custom project profile.

6. On the **Create project profile: SQL analytics** page, in the **Enable blueprints** section, review the following blueprints that will be enabled for this project profile.

> **Important**
>
> Note that by configuring SQL analytics for your domain (this procedure), you can only enable these blueprints in the same AWS account and region as your domain. To enable these blueprints in an account or region that's different from that of your domain's, see Create a SQL analytics project profile and Custom project profile.

   - LakehouseCatalog
   - RedshiftServerless
   - DataLake
7. On the **Create project profile: SQL analytics** page, in the **Manage access role** section, specify a service role that gives Amazon SageMaker Unified Studio authorization to ingest and manage access to datashares, tables and views in Amazon Redshift. You can create a new or using an existing role.
8. On the **Create project profil: SQL analytics** page, in the **Provisioning role** section, specify a service role that gives Amazon SageMaker Unified Studio authorization to ingest and manage access to datashares, tables and views in Amazon Redshift.
9. On the **Create project profile: SQL analytics** page, in the **Amazon S3 bucket for blueprints** section, specify an Amazon S3 bucket for blueprints in your AWS account.
10. On the **Create project profile: SQL analytics** page, in the **Networking** section, specify a VPC in which to provision your Amazon SageMaker unified domain. VPCs tagged with Amazon SageMaker Unified Studio should be correctly configured. In the **Subnets** section, select at least 3 subnets in different **Availability Zones** that contain required VPC Endpoints. Private subnets are recommended, not all functionality is available when selecting public subnets.
11. In the **Data encryption** section, specify the encryption settings. Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

12. In the **User role policy** section, you have the option to specify your own user role policy. Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, AI, and ML actions. You can attach your own AWS IAM policies to the role rather than using the default system-managed policy. This provides more granular control over permissions but requires knowledge of IAM policy configuration. The IAM policy must include all necessary permissions required for the service to function properly.
13. On the **Create project profile: SQL analytics** page, in the **Authorization - optional** section, specify who can use this project profile to create projects in all domain units. This can also be done per domain unit in the Amazon SageMaker Unified Studio. Choose either **Selected users and groups** (select which users and groups are authorized to use this project profile) or **Allow all users and groups** (allow any user to use this project profile).

> **Note**
>
> Projects do not provide strong security isolation. To limit cross-domain and cross-project resource discovery you can consider creating projects in separate accounts.

14. Choose **Create project profile**.

Create a SQL analytics project profile

Complete the following procedure to create a SQL analytics project profile for your Amazon SageMaker unified domain. Once this procedure is complete, your SQL analytics project profile will only include the capabilities defined in the Tooling blueprint. To configure the full data analytics and SQL analytics capability for your Amazon SageMaker unified domain, you must then use the **Blueprints** tab and configure the following blueprints for this project profile:

- LakehouseCatalog
- RedshiftServerless
- DataLake

> **Important**
>
> Note that when you enable a blueprint, by default, you are enabling it in the same region as your domain. When you are enabling blueprints for a project profile that is created and enabled in a different region from your domain, you must enable these blueprints in same

region where this project profile is enabled (in addition to enabling this blueprint in the same region as your domain). You can do this via the **Regions** tab in the blueprint details page. This applies to all blueprints, including the Tooling blueprint.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Either create a new domain or choose an existing domain where you want to create a SQL analytics project profile.
3. On the domain's details page, choose the **Project profiles** tab and then choose **Create**.
4. On the **Create project profile** page, in the **Project profile name and description** section, specify the name of the project profile and the description.
5. On the **Create project profile** page, in the **Project profile creation options** section, choose **Create from a template**, and then under **Project profile templates**, choose **SQL analytics**.
6. On the **Create project profile** page, in the **Default tooling blueprint deployment settings** section, review the selections for the default deployment settings for the Tooling blueprint and update them as needed.
   - On the **Create project profile** page, in the **Project files storage** section, choose a storage configuration type from Amazon S3 - new and Git repository. For more information on storage types, see ._unified-storage.xml

   Important

   Note that by creating this project profile from a template, you can either enable the Tooling blueprint in the same AWS account and region as your domain (prepopulated by default) or you can enable the Tooling blueprint in a different AWS account and region from this domain (an associated account).
7. On the **Create project profile** page, in the **Authorization - optional** section, specify who can use this project profile to create projects in all domain units. This can also be done per domain unit in Amazon SageMaker Unified Studio. You can specify **Selected users and groups** or **Allow all users and groups** options.

> **Note**
>
> Projects do not provide strong security isolation. To limit cross-domain and cross-project resource discovery you can consider creating projects in separate accounts.

8. On the **Create project profile** page, in the **Project profile readiness** section, specify whether you want to enable this project profile on creation. Unless you check the **Enable project profile on creation** checkbox, your project profile is disabled and not available to use for Amazon SageMaker Unified Studio projects after its creation. Leaving a project profile in a disabled state upon creation gives you the opportunity to customize your blueprints before making the project profile available.
9. Choose **Create project profile**.

> **Important**
>
> After you complete this procedure, your SQL project profile will only include the capabilities defined in the Tooling blueprint. You can further customize this project profile and configure it to include the full supported SQL analytics capability by using the **Bluerpints** tab to enable the rest of its required bluerpints. They are the following:
>
> - LakehouseCatalog
> - RedshiftServerless
> - DataLake

Custom project profile

Complete the following procedure to create a custom project profile for your Amazon SageMaker unified domain. With the Custom creation option, you can create a project profile from scratch with your own profile settings and a selection of blueprints.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Either create a new domain or choose an existing domain where you want to create a custom project profile.

3. On the domain's details page, choose the **Project profiles** tab and then choose **Create**.
4. On the **Create project profile** page, in the **Project profile name and description** section, specify the name of the project profile and the description.
5. On the **Create project profile** page, in the **Project profile creation options** section, choose **Custom create**.
6. On the **Create project profile** page, in **Blueprints**, specify the Amazon SageMaker Unified Studio blueprints to use in your project. You can customize each blueprint configuration after this custom project profile is created. This is where you can choose built-in blueprints or your own custom blueprints.
7. To configure the project account and Region information you want the profile to use, you can either provide account and Region information that projects will use each time, or you can configure your project profile to allow specifying accounts during project creation. Under **Account and region**, choose one of the following.
   - To create a project profile that will use the same account and region for each project created, select **Choose account and region**. Projects created with this profile will use the specified account and region and cannot specify otherwise at project creation.
   - To create a project profile that will choose from accounts available at project creation, select **Choose account and region during project creation**.
     - Under **Accounts available during project creation**, you can choose to create a project profile that will provide a list of all AWS accounts associated to the domain for selection at project creation. To choose this option, choose **All associated accounts**. For more information about associated accounts in Amazon SageMaker Unified Studio, see Associated accounts in Amazon SageMaker Unified Studio.
     - Under **Accounts available during project creation**, you can choose to create a project profile that will provide account pools to be selected at project creation. An account pool is a list of authorized associated accounts and regions. To choose this option, select **Choose account pool(s)**. Next, under **Account pools**, choose the account pool or pools that you want to be available for the project profile to use at project creation. For information about creating and updating account pools, see Account pools in Amazon SageMaker Unified Studio.
8. On the **Create project profile** page, in the **Default tooling blueprint deployment settings** section, review the selections for the default deployment settings for the Tooling blueprint.
9. On the **Create project profile** page, in the **Project files storage** section, specify the storage configuration for project code artifacts. You can choose one of the following:

- Amazon S3
- Git repository

For more information, see Source control and file storage in Amazon SageMaker Unified Studio.

10. On the **Create project profile** page, in the **Authorization - optional** section, specify who can use this project profile to create projects in all domain units. This can also be done per domain unit in Amazon SageMaker Unified Studio. You can specify **Selected users and groups** or **Allow all users and groups** options.

    > **Note**
    >
    > Projects do not provide strong security isolation. To limit cross-domain and cross-project resource discovery you can consider creating projects in separate accounts.

11. On the **Create project profile** page, in the **Project profile readiness** section, specify whether you want to enable this project profile on creation. Unless you check the **Enable project profile on creation** checkbox, your project profile is disabled and not available to use for Amazon SageMaker Unified Studio projects after its creation. Leaving a project profile in a disabled state upon creation gives you the opportunity to customize your blueprints before making the project profile available.
12. Choose **Create project profile**.

Update project profiles

Complete the following procedure to update a project profile for your domain.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose an existing domain where you want to update a project profile.
3. Choose the **Project profiles** tab and then choose the project profile that you want to update. You can choose the All capabilities project profile, the Generative AI application development project profile, the SQL analytics project profile, or your custom project profile.
4. In the project profile details page, choose **Edit**.

5. You can make changes to the project profile description, default Tooling blueprint deployment settings, including systems manager configuration parameters, the Tooling blueprint parameters, and notes for project owners. Here you can also choose between default storage and Git storage.

   Once you're done making updates, choose **Save**.

Disable or enable project profiles

Complete the following procedure to disable or enable a project profile for your domain.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose an existing domain where you want to disable or enable a project profile.
3. Choose the **Project profiles** tab and then choose a project profile. You can choose the All capabilities project profile, the Generative AI application development project profile, the SQL analytics project profile, or your custom project profile.
4. In the project profile details page, choose either **Disable** or **Enable**.

   When enabling a project profile, confirm the action in the pop up window by choosing **Enable**.

Delete project profiles

Complete the following procedure to delete a project profile for your domain.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose an existing domain where you want to delete a project profile.
3. Choose the **Project profiles** tab and then choose the project profile that you want to delete. You can choose the All capabilities project profile, the Generative AI application development project profile, the SQL analytics project profile, or your custom project profile.
4. In the project profile details page, choose **Delete**.

Confirm the action in the D**elete project profile** pop up window by typing the project profile name in the text field and choosing **Delete**.

> **Note**
>
> Deleting a project profile is final. Deletion removes the project profile and its blueprint deployment settings from Amazon SageMaker Unified Studio. It does not delete the blueprints used to create the blueprint deployment settings which make up this project profile.

Edit blueprint deployment settings

Blueprint deployment settings contain parameters used to create project profiles for Amazon SageMaker Unified Studio projects. Complete the following procedure to edit deployment settings for any of the supported blueprints.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose the domain's name from the list. The name is a hyperlink.
3. Choose the **Project profiles** tab and then choose the project profile that contains the blueprint the deployment settings of which you want to modify.
4. From the **Blueprint deployment settings** list, choose the blueprint the deployment settings of which you want to modify. The blueprint name is a hyperlink.
5. On the chose blueprint's **Blueprint deployment settings summary** page, choose **Edit**.

   You can make changes to the following:

   - The blueprint deployment settings description.
   - The AWS SSM Parameter Store path that contains parameters definition.
   - The blueprint parameters. You can use the table on this page to inspect and edit parameter values that will be used during project creation. To edit a parameter value, choose the parameter's radio button and choose **Edit**. You can override values that are set as blueprint or SSM values and check the **Editable** box if you want the values to be provided during project creation.

- Notes for project owners - let project owners know why you made these changes and anything else they need to know about how this will impact their projects that use this project profile.

Add blueprint deployment settings

Blueprint deployment settings contain parameters used to create project profiles for Amazon SageMaker Unified Studio projects. Complete the following procedure to add deployment settings for any of the supported blueprints.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose the domain's name from the list. The name is a hyperlink.
3. Choose the **Project profiles** tab and then choose the project profile that contains the blueprint to which you want to add a new deployment setting.
4. Choose the **Blueprints Deployment Settings** tab, and choose Add blueprint deployment settings.
5. On the **Add blueprint deployment settings** page, specify the following:
   - Blueprint deployment settings name.
   - The blueprint deployment settings description.
   - The blueprint to which these deployment settings will apply.
   - Deployment properties - the account and region where you want this blueprint deployment settings to be created. Note that the corresponding blueprint should be enabled in this account and region so that the blueprint deployment settings could be created successfully.
   - AWS SSM Parameter Store path in AWS Systems Manager Parameters Store that contains parameters definition.
   - Blueprint parameters - these parameter values that will be used during project creation. You can override values that are set as blueprint or SSM values and check the Editable box if you want the values to be provided during project creation.
   - Notes for project owners - let project owners know why you made these changes and anything else they need to know about how this will impact their projects that use this project profile.

Project resource tags

Project resource tags in Amazon SageMaker Unified Studio are custom key-value pairs that you assign to projects to help organize, categorize, and manage your resources. You can use tags for cost allocation, access control, and resource organization across your Amazon SageMaker Unified Studio projects.

Tags are configured through a Project Profile, applied at the project level and inherited by resources created through the create project and update project actions.

The following considerations apply for project resource tags in Amazon SageMaker Unified Studio:

- Configure project profiles with project resource tags using AWS CLI or API only.
- You can add up to 25 tags per project profile.
- Tag keys must conform to the IAM policy permissions of the domain provisioning role.
- Tag keys must be unique within a project and can contain up to 128 characters.
- Tag values are optional and can contain up to 256 characters.
- Tag keys and values can contain letters, numbers, spaces, and the following characters: + - = . _ : / @
- Tag keys and values are case-sensitive.

IAM permissions for project resource tags

By default, the tag Key must begin with the string "AmazonDataZone". This condition is set in the domain provisioning role. If Amazon SageMaker Unified Studio created the provisioning role for you it will be the AmazonSageMakerProvisioning-AccountId role. To create tags with a different string pattern (i.e. begins with, contains, etc.), a policy with appropriate permissions must be attached to the domain provisioning role.

To configure IAM policy for project resource tags

1. Navigate to the Identity and Access Management (IAM) console.
2. In the navigation pane, choose **Roles**.
3. In the list, search for AmazonSageMakerProvisioning-accountId or your custom domain provisioning role.

4. Choose the **Permissions** tab.
5. Choose **Add permissions**, and then choose **Create inline policy**.
6. Under **Policy editor**, choose **JSON**.
7. Enter the policy.
8. Save to attach the policy to the role.

The following is an example policy allowing tag Keys to begin with "AmazonDataZone" or "SageMaker". Modify aws:TagKeys within the condition to meet your tag Key name requirements.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CustomTagsUnTagPermissions",
            "Effect": "Allow",
            "Action": [
                "codecommit:UntagResource",
                "iam:UntagRole",
                "logs:UntagResource",
                "athena:UntagResource",
                "redshift-serverless:UntagResource",
                "scheduler:UntagResource",
                "bedrock:UntagResource",
                "neptune-graph:UntagResource",
                "quicksight:UntagResource",
                "glue:UntagResource",
                "airflow:UntagResource",
                "secretsmanager:UntagResource",
                "lambda:UntagResource",
                "emr-serverless:UntagResource",
                "elasticmapreduce:RemoveTags",
                "sagemaker:DeleteTags",
                "ec2:DeleteTags"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                },
                "ForAllValues:StringLike": {
```

```
                    "aws:TagKeys": [
                        "AmazonDataZone*",
                        "SageMaker*"
                    ]
                },
                "Null": {
                    "aws:ResourceTag/AmazonDataZoneProject": "false"
                }
            }
        },
        {
            "Sid": "CustomTagsTaggingPermissions",
            "Effect": "Allow",
            "Action": [
                "cloudformation:TagResource",
                "codecommit:TagResource",
                "iam:TagRole",
                "glue:TagResource",
                "athena:TagResource",
                "lambda:TagResource",
                "redshift-serverless:TagResource",
                "logs:TagResource",
                "secretsmanager:TagResource",
                "sagemaker:AddTags",
                "emr-serverless:TagResource",
                "neptune-graph:TagResource",
                "bedrock:TagResource",
                "elasticmapreduce:AddTags",
                "airflow:TagResource",
                "scheduler:TagResource",
                "quicksight:TagResource",
                "emr-containers:TagResource",
                "logs:CreateLogGroup",
                "athena:CreateWorkGroup",
                "scheduler:CreateScheduleGroup",
                "cloudformation:CreateStack",
                "ec2:*"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "aws:TagKeys": [
                        "AmazonDataZone*",
                        "SageMaker*"
```

```
                    ]
                },
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
}
```

> **Note**
>
> it is possible to scope down the specific AWS service tag and un-tag permissions based on which blueprints / capabilities are used.

Configure project resource tags

Project resource tags are configured in the project profile. The project profile sets the key/value tag pairs, whether the value can be modified by the project creator, and whether projects using the project profile can create their own project resource tags at the time of project creation. Once configured, project resource tags will be applied to all projects using the project profile.

To use the AWS CLI to create a project profile with project resource tags, use the create-project-profile command.

Parameter --project-resource-tags sets tags within the project profile. Each tag is composed of a key (string), value (string), and isValueEditable (boolean). IsValueEditable set to true means the value can be changed during project creation or update.

The following example shows the parameter project-resource-tags with tags configured.

```
--project-resource-tags '[
 {
  "key": "SageMaker",
  "value": "application",
  "isValueEditable": false
 },
 {
```

```
  "key": "AmazonDataZone-CostCenter",
  "value": "123",
  "isValueEditable": true
 }
]'
```

Parameter --allow-custom-project-resource-tags true | false permits the project creator to create additional key/value pairings. The key needs to conform to the policy of the domain provisioning role.

Parameter --project-resource-tags-description is a description field for project resource tags. The max character limit is 2048. The description needs to be passed in every time create-project-profile or update-project-profile is called.

Update project resource tags

Updates to project resource tags in the project profile apply automatically to new projects created from that point forward. For existing projects using the project profile, an update notification will be triggered in the project and the changes will be applied when the project is updated. Existing resources retain their current tags until they are recreated or manually updated.

To use the AWS CLI to update a project profile with project resource tags, use the update-project-profile command. Parameters --project-resource-tags and --allow-custom-project-resource-tags can be updated.

There are three ways to work with the project-resource-tags parameter when updating the project profile.

- Passing a non-empty list of project resource tags will replace the tags currently configured on the project profile. Updating project resource tags in the project profile is not an additive action - include the exhaustive set of tags.
- Passing an empty list of project resource tags will clear out all previously configured tags:

  --project-resource-tags '[]'
- Not including the project resource tag parameter will keep previously configured tags as-is.

Update the project

Projects need to be updated when:

1. Project resource tags are updated in the project profile.
2. The project, when permitted by the project profile, updates existing tag values or adds new tags.

To use the AWS CLI to update a project with project resource tags, use the update-project command.

Parameter --resource-tags updates tags in the project. Tag values can be updated when their property isValueEditable is set to true. New tags can be added if parameter --allow-custom-project-resource-tags from the project profile is set to true.

The following example shows the parameter --resource-tags in the update project call.

```
  --resource-tags '[
 {
  "key": "AmazonDataZone-CostCenter ",
  "value": "456"

]'
```

Project level tags (those not configured from the project profile) need to be passed during project update in order to be preserved. For tags with isValueEditable = true configured from the project profile, any override previously set needs to be applied or the value will revert to the default from the project profile.

Delete project resource tags

To delete project resource tags set from the project profile use the update-project-profile command followed by the update-project command.

1. Call the update-project-profile command with an empty list for parameter --project-resource-tags to remove project resource tags from the project profile. Existing project resources that already have these tags will retain them. New projects created using this project profile will not inherit the deleted tags.

   --project-resource-tags '[]'
2. Call the update-project command to remove project resource tags from the project resources. This removes the project resource tags set from the project profile. This will not remove the project resource tags set directly from the project.

To delete project resource tags set from the project use the update-project command with an empty list for parameter --resource-tags.

```
--resource-tags '[]'
```

Blueprints in Amazon SageMaker Unified Studio

A blueprint with which the project profile is created defines what AWS tools and services members of the project to which the project profile belongs can use as they work with data in the Amazon SageMaker catalog.

Topics

- Supported blueprints
- Custom blueprints
- Enable or disable blueprints
- Specify PEM certificate for EmrOnEc2 blueprint
- Getting started with Amazon EMR on EKS in Amazon SageMaker Unified Studio
- Manage blueprint authorization
- Tooling blueprints in Amazon SageMaker Unified Studio
- Enable Tooling blueprint
- Manage Tooling blueprint parameters
- Modify the OnDemandWorkflows blueprint for creating workflow environments in a shared VPC

Supported blueprints

In the current release of Amazon SageMaker Unified Studio, the following default blueprints are supported:

Blueprint name	Description	Resources created
AmazonBedrockGenerativeAI	This is the combined Amazon Bedrock blueprint which contains seven sub-Amazon Bedrock blueprints. It enables users to build generative AI applications using tools such as Agents, Knowledge Bases, Guardrails, Flows, Functions, and Model Evaluation.	

Blueprint name	Description	Resources created
AmazonBedrockChatAgent	Provides a reusable AWS CloudFormation template to create an Amazon Bedrock Agent and supportin g resources, including an execution role and a consumption role.	Bedrock Agent, Bedrock Agent Execution role, Bedrock Agent Consumption role
AmazonBedrockEvaluation	Creates one IAM role as the service role for an Amazon Bedrock evaluation job.	Bedrock Evaluation job execution role
AmazonBedrockFlow	Provides a reusable AWS CloudFormation template to create an Amazon Bedrock Prompt Flow and supportin g resources such as an execution role.	Amazon Bedrock Flow, Amazon Bedrock Flow Execution role
AmazonBedrockFunction	Provides a reusable AWS CloudFormation template to create an AWS Lamda function and supportin g resources, such as an execution role, and a secret manager.	Secrets Manager secret, AWS Lambda function, AWS Lambda function execution role, Log group
AmazonBedrockGuardrail	Provides an AWS CloudForm ation template to create an Amazon Bedrock Guardrail and supporting resources such as an execution role.	Amazon Bedrock Guardrail

Blueprint name	Description	Resources created
AmazonBedrockKnowledgeBase	Provides an AWS CloudFormation template to create a reusable Amazon Bedrock Knowledge Base and supporting resources such as an execution role.	Amazon Bedrock Knowledge Base, OpenSearch Serverless collection, Amazon Bedrock Knowledge Base Execution role, AWS Lambdas, including OpenSearch Index Lambda and KB Ingestion Trigger Lambda, AWS Lambda Execution role, Amazon Bedrock Knowledge Base data source
AmazonBedrockPrompt	Provides a reusable AWS CloudFormation template to create an Amazon Bedrock Prompt and supporting resources, such as an execution role, and a consumption role.	Amazon Bedrock Prompt, Amazon Bedrock Prompt Consumption role
LakeHouseDatabase Note: If you search using API/CLI, the blueprint name is DataLake.	Provides a reusable AWS CloudFormation template to create a data lake environment with a AWS Glue database for data management and an Amazon Athena workgroup for querying data.	AWS Glue databases, lake formation permissions, Amazon Athena workgroups

Blueprint name	Description	Resources created
EMRonEC2	Provides a reusable AWS CloudFormation template to create an Amazon EMR on EC2 cluster to run and scale Apache Spark, Hive, and other big data workloads. For more information about enabling this blueprint see, Specify PEM certificate for EmrOnEc2 blueprint	EMR on EC2 clusters
EMRServerless	Provides a reusable AWS CloudFormation template to create an Amazon EMR Serverless application that is ready to serve Apache Spark batch jobs and interactive sessions.	EMR on Serverless applicati ons
LakehouseCatalog	Provisions a new catalog in the Amazon SageMaker Lakehouse that is backed by Amazon Redshift Managed Storage	
MLExperiments	Provides OnDemand blueprint to enable MLflow tracking server for the experimentation inside a project.	MLflow tracking server (on demand)

Blueprint name	Description	Resources created
PartnerApps	Creates an IAM role and a Connection that enables access to Partner AI Apps. Through Partner AI Apps you can leverage integrate d and fully-managed thrid-party solutions for AI/Ml development.	Amazon SageMaker Partner AI Apps IAM role, Amazon SageMaker Partner AI Apps Connection
RedshiftServerless	Provides a reusable AWS CloudFormation template to create an Amazon Redshift Serverless environment to get insights from data without managing infrastructure.	Amazon Redshift Serverless warehouses
Tooling	Creates resources for the project, including IAM user roles, security groups, and Amazon SageMaker Unified Studio domains.	IAM user roles, Amazon SageMaker Unified Studio domains, security groups
Workflows	Provides an AWS CloudForm ation template to create the MWAA environment for Airflow based Workflows	Enables project workflows on MWAA

Blueprint name	Description	Resources created
Quicksight	Enables visualization of data within an Amazon SageMaker Unified Studio project using Amazon QuickSight.	For each project with the QuickSight blueprint, Amazon SageMaker Unified Studio creates a restricted folder in Amazon QuickSight. Additionally, it creates Amazon Athena and Amazon Redshift data sources in the restricted folder depending on other blueprints in the project. For more informati on, see Amazon QuickSight in Amazon SageMaker Unified Studio.

Custom blueprints

Custom blueprints in Amazon SageMaker Unified Studio enable organizations to standardize and accelerate how data projects get set up. They are administrator-defined templates, powered by AWS CloudFormation, that give teams a ready-made starting point for analytics and machine learning environments.

In addition to the blueprints that Amazon SageMaker Unified Studio provides, you can also design your own. For more information, see Supported blueprints. With custom blueprints, organizations can include their specific dependencies, security controls, and best practices to allow for new projects to align with internal standards. Since they're defined through infrastructure-as-code, custom blueprints are easy to version control, share across teams, and evolve over time. This not only speeds up onboarding but also keeps projects consistent and governed, no matter how big or distributed your data science organization becomes.

Topics

- Register a custom blueprint in the console
- Register a custom blueprint with the API
- Reserved parameters

- Trust policy for the provisioning role
- Sample custom blueprint template

Register a custom blueprint in the console

Have your AWS CloudFormation template ready before you start. The Amazon SageMaker Unified Studio console accepts either an Amazon S3 URL or a file that you upload.

1. Open the Amazon SageMaker Unified Studio console, and then use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains**, and then choose the domain's name (shown as a hyperlink) from the list.
3. On the domain's details page, navigate to the **Blueprints** tab.
4. In the **Blueprints** tab, in the **Blueprints** section, choose **Create**. This brings up the **Create custom blueprint** page.
5. In the **Create custom blueprint** page, specify the following and then choose **Next**:
   - **Name** - the name for your custom blueprint. This blueprint name cannot be changed after the blueprint is created.
   - **Description** - optional - the description for your custom blueprint.
   - In the **Upload CloudFormation template** section, specify the Amazon S3 file path where the custom AWS CloudFormation template for your blueprint is stored. You can choose to either specify the Amazon S3 URL for your template or you can choose to upload your own template file.

   > **Note**
   >
   > Choose **View templates** on the **Blueprints** page to open the sample template in the console, where you can modify it. For the same template with an explanation of what it creates, see Sample custom blueprint template.

6. In the **Configure editable parameters** page, you can choose the parameters for your custom blueprint. Editable parameters are values that are visible and editable when this blueprint is used in project profiles. On this page, you can remove parameters that you don't want to be editable in project profiles, or edit their default values. Then choose **Next**.

7. In the **Enable blueprint - optional** page, you can enable your custom blueprint so that it can be used in project profiles and projects.

   If you choose to enable your custom blueprint at this point, in the **Provisioning role**, you must specify the role that Amazon SageMaker Unified Studio can use to provision and manage resources defined in this blueprint in your account.

   Also, in the **Authorized domain units** section, you must specify the domain units where projects can access resources defined by this custom blueprint.

   Then choose **Next**.
8. Review your selections in the **Review and create** page, and then choose **Create blueprint**.

Now that your custom blueprint is created, you can use it when creating custom project profiles. For more information, see Custom project profile.

Register a custom blueprint with the API

The `CreateEnvironmentBlueprint` API requires an Amazon S3 URL for the AWS CloudFormation template. The blueprint's provisioning role must have access to that Amazon S3 object. The `SageMakerStudioProjectProvisioningRolePolicy` managed policy grants `s3:GetObject` on buckets whose names begin with `amazon-sagemaker-cf-templates`. The console creates such a bucket when you upload a template there.

```
aws datazone create-environment-blueprint \
  --domain-identifier domain-id \
  --name blueprint-name \
  --provisioning-properties '{
    "cloudFormation": {
      "templateUrl": "https://amazon-sagemaker-cf-
templates-region-suffix.s3.region.amazonaws.com/my-template.yaml"
    }
  }'
```

> **Note**
>
> You can categorize a custom blueprint as Tooling by setting `blueprintCategory` to `TOOLING`, so it serves as a project's Tooling environment in place of the one Amazon

SageMaker Unified Studio provides. For more information about what a Tooling template must declare and how to register one, see Custom blueprints as Tooling.

After you create the blueprint, Amazon SageMaker Unified Studio disables it by default. To enable a blueprint in an AWS Region, you must supply a provisioning role with permissions for all resources in the template.

```
aws datazone put-environment-blueprint-configuration \
  --domain-identifier domain-id \
  --environment-blueprint-identifier blueprint-id \
  --enabled-regions region \
  --provisioning-role-arn provisioning-role-arn
```

Reserved parameters

Reserved parameters are AWS CloudFormation parameters whose values Amazon SageMaker Unified Studio supplies when it deploys your template. The names are case-sensitive.
When Amazon SageMaker Unified Studio cannot find a value for an optional parameter, an empty string is injected, which overrides any `Default` you declared. The one exception is `sagemakerUnifiedStudioNetworkGlueConnectionNames`, which Amazon SageMaker Unified Studio omits instead, leaving your `Default` in place.

The prefixes `amazon`, `aws`, `datazone`, and `sagemaker` are reserved. When you register a blueprint, Amazon SageMaker Unified Studio rejects any name in `userParameters` that begins with one of them, whether or not it appears in the table.

Parameter name	Optional	Description
`awsDefaultGlueCataloglogKmsKeyArn`	Yes	The ARN of the AWS KMS key for the default AWS Glue Data Catalog.
`datazoneEnvironmentDomainArn`	No	The ARN of the Amazon SageMaker Unified Studio domain.

Parameter name	Optional	Description
`datazoneEnvironmentDomainId`	No	The ID of the Amazon SageMaker Unified Studio domain.
`datazoneEnvironmentDomainKmsKeyArn`	Yes	The ARN of the AWS KMS key for the Amazon SageMaker Unified Studio domain.
`datazoneEnvironmentEnvironmentId`	No	The ID of the environment.
`datazoneEnvironmentIdentityCenterInstanceArn`	Yes	The ARN of the AWS IAM Identity Center instance for the Amazon SageMaker Unified Studio domain.
`datazoneEnvironmentProjectExecutionRoleArn`	Yes	The ARN of the project execution role that you supply when you create the project. IAM-based domains only.
`datazoneEnvironmentProjectId`	No	The ID of the project.
`datazoneEnvironmentProjectName`	No	The name of the project.
`datazoneEnvironmentProvisioningRoleArn`	No	The ARN of the provisioning role for the blueprint.
`sagemakerUnifiedStudioKmsKeyArn`	Yes	The ARN of the AWS KMS key that you set on the blueprint configuration for the AWS Region.

Parameter name	Optional	Description
`sagemakerUnifiedStudioNetworkGlueConnectionNames`	Yes	The names of the AWS Glue connections for the VPC, as a comma-separated list. We omit this parameter entirely rather than sending an empty value, which leaves your `Default` in place.
`sagemakerUnifiedStudioNetworkSecurityGroupId`	Yes	The ID of the security group for the VPC.
`sagemakerUnifiedStudioNetworkSubnets`	Yes	The IDs of the subnets in the VPC, as a comma-separated list.
`sagemakerUnifiedStudioNetworkVpcId`	Yes	The ID of the VPC for the Amazon SageMaker Unified Studio domain.
`sagemakerUnifiedStudioToolingEnvironmentId`	Yes	The ID of the project's Tooling environment.
`sagemakerUnifiedStudioToolingIamConnectionId`	Yes	The ID of the IAM connection for the project.
`sagemakerUnifiedStudioToolingKmsKeyArn`	Yes	The ARN of the AWS KMS key for the project.
`sagemakerUnifiedStudioToolingS3BucketArn`	Yes	The ARN of the Amazon S3 bucket for the project.

Parameter name	Optional	Description
`sagemakerUnifiedStudioToolingUserRoleArn`	Yes	The ARN of the project user role. Use it as the principal when your template grants project members access to a resource.

> **Important**
>
> Reserved parameter names are case-sensitive. If your template declares a parameter that begins with a reserved prefix (`amazon`, `aws`, `datazone`, or `sagemaker`) but doesn't match a reserved name exactly, Amazon SageMaker Unified Studio doesn't supply a value for it. Deployment then fails, because CloudFormation rejects a parameter it received no value for:
>
> ```
> Parameters: [parameterName] must have values
> ```
>
> Review the parameters that your template declares and confirm that each name matches the preceding table exactly, including case.

Trust policy for the provisioning role

Amazon SageMaker Unified Studio assumes the blueprint's provisioning role with `sts:AssumeRole` to deploy your AWS CloudFormation template. It also attaches your user context to that session as tags with `sts:TagSession`. Amazon SageMaker Unified Studio resources such as connections and data sources require this user context to provision. Therefore, the trust policy of the provisioning role must allow both actions for the `datazone.amazonaws.com` service principal, as shown in the following example. The `aws:SourceAccount` condition restricts the role to your own AWS account, which guards against the cross-service confused deputy problem.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "datazone.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:TagSession"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                }
            }
        }
    ]
}
```

Sample custom blueprint template

The following template creates an AWS Glue database in your SageMaker Lakehouse catalog, grants the project's users access to it through AWS Lake Formation, and attaches a managed policy to the project's role. It is the same template that the **View templates** button on the **Blueprints** page shows.

```
{
  "Parameters": {
    "datazoneEnvironmentEnvironmentId": {
      "Type": "String",
      "Description": "EnvironmentId for which the resource will be created for."
    },
    "datazoneEnvironmentProjectId": {
      "Type": "String",
      "Description": "DZ projectId for which project the resource will be created for."
    },
    "userRoleArn": {
      "Type": "String",
      "Description": "Project Role ARN"
    },
    "glueDbName": {
      "Type": "String",
      "Default": "gluedb",
      "Description": "Glue DB name"
    }
```

```
  },
  "Resources": {
    "GlueDatabase": {
      "Type": "AWS::Glue::Database",
      "Properties": {
        "CatalogId": {
          "Ref": "AWS::AccountId"
        },
        "DatabaseInput": {
          "CreateTableDefaultPermissions": [],
          "Description": {
            "Fn::Join": [
              "",
              [
                "Created by DataZone for project ",
                {
                  "Ref": "datazoneEnvironmentProjectId"
                }
              ]
            ]
          },
          "LocationUri": {
            "Fn::Join": [
              "",
              [
                {
                  "Fn::ImportValue": {
                    "Fn::Join": [
                      "",
                      [
                        "s3BucketPath-",
                        {
                          "Ref": "datazoneEnvironmentProjectId"
                        },
                        "-dev"
                      ]
                    ]
                  }
                },
                "/data/catalogs/"
              ]
            ]
          },
          "Name": {
```

```
            "Fn::Sub": "${glueDbName}-${datazoneEnvironmentEnvironmentId}"
          }
        }
      }
    },
    "GlueAccessManagedPolicy": {
      "Type": "AWS::IAM::ManagedPolicy",
      "Properties": {
        "ManagedPolicyName": {
          "Fn::Sub": "GlueAccess-${glueDbName}-${datazoneEnvironmentEnvironmentId}-
Policy"
        },
        "PolicyDocument": {
          "Version": "2012-10-17",
          "Statement": [
            {
              "Effect": "Allow",
              "Action": [
                "glue:GetDatabase",
                "glue:GetTables",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:UpdateTable",
                "glue:DeleteTable",
                "glue:BatchDeleteTable",
                "glue:GetPartitions",
                "glue:GetPartition",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
              ],
              "Resource": [
                {
                  "Fn::Sub": "arn:aws:glue:${AWS::Region}:${AWS::AccountId}:catalog"
                },
                {
                  "Fn::Sub": "arn:aws:glue:${AWS::Region}:${AWS::AccountId}:database/
${glueDbName}-${datazoneEnvironmentEnvironmentId}"
                },
                {
                  "Fn::Sub": "arn:aws:glue:${AWS::Region}:${AWS::AccountId}:table/
${glueDbName}-${datazoneEnvironmentEnvironmentId}/*"
                }
              ]
            }
```

```
          ]
        }
      }
    },
    "LakeFormationDbPermissions": {
      "Type": "AWS::LakeFormation::Permissions",
      "Properties": {
        "DataLakePrincipal": {
          "DataLakePrincipalIdentifier": {
            "Ref": "userRoleArn"
          }
        },
        "Resource": {
          "DatabaseResource": {
            "CatalogId": {
              "Ref": "AWS::AccountId"
            },
            "Name": {
              "Fn::Sub": "${glueDbName}-${datazoneEnvironmentEnvironmentId}"
            }
          }
        },
        "Permissions": [
          "DESCRIBE",
          "CREATE_TABLE"
        ]
      },
      "DependsOn": [
        "GlueDatabase"
      ]
    },
    "LakeFormationTablePermissions": {
      "Type": "AWS::LakeFormation::Permissions",
      "Properties": {
        "DataLakePrincipal": {
          "DataLakePrincipalIdentifier": {
            "Ref": "userRoleArn"
          }
        },
        "Resource": {
          "TableResource": {
            "CatalogId": {
              "Ref": "AWS::AccountId"
            },
```

```
            "DatabaseName": {
              "Fn::Sub": "${glueDbName}-${datazoneEnvironmentEnvironmentId}"
            },
            "TableWildcard": {}
          }
        },
        "Permissions": [
          "ALL"
        ]
      },
      "DependsOn": [
        "GlueDatabase"
      ]
    }
  },
  "Outputs": {
    "GlueDatabaseName": {
      "Value": {
        "Fn::Sub": "${glueDbName}-${datazoneEnvironmentEnvironmentId}"
      },
      "Export": {
        "Name": {
          "Fn::Sub": "${glueDbName}-${datazoneEnvironmentEnvironmentId}"
        }
      }
    },
    "GlueAccessManagedPolicy": {
      "Description": "ARN of the created managed policy",
      "Value": {
        "Ref": "GlueAccessManagedPolicy"
      },
      "Export": {
        "Name": {
          "Fn::Sub": "datazone-managed-policy-glue-${glueDbName}-
${datazoneEnvironmentEnvironmentId}"
        }
      }
    }
  }
}
```

Enable or disable blueprints

You can complete the following procedure to enable or disable blueprints in the Amazon SageMaker management console:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose the domain's name from the list. The name is a hyperlink.
3. On the domain's details page, navigate to the **Blueprints** tab.
4. In the **Blueprints** tab, use the radio buttons to select the blueprints that you want to enable or disable and then choose the **Enable** or **Disable** buttons to perform the action.

> **Important**
>
> When you enable a blueprint, by default, you are enabling it in the same region as your domain. When you are enabling blueprints for a project profile that is created and enabled in a different region from your domain, you must enable these blueprints in same region where this project profile is enabled (in addition to enabling this blueprint in the same region as your domain). You can do this via the **Regions** tab in the blueprint details page. This applies to all blueprints, including the Tooling blueprint.

Specify PEM certificate for EmrOnEc2 blueprint

In order to successfully enable the EmrOnEc2 blueprint, you must specify the location of your PEM certificate. To do this, complete the following procedure:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose the domain's name from the list. The name is a hyperlink.
3. Choose the **Project profiles** tab and then choose **All capabilities**.
4. Choose one of the following instance type configurations:

- OnDemand Amazon EMR on EC2 General Purpose: this configuration uses Amazon EC2 instances (like m5.xlarge) to provide balanced compute, memory, and network resources. Choose this option for standard data processing workloads.
- OnDemand Amazon EMR on EC2 Memory-Optimized: this configuration uses Amazon EC2 instances (like r5.xlarge) to provide more memory per vCPU. Choose this option for memory-intensive workloads such as in-memory databases or real-time analytics.

5. Choose the corresponding radio button for the EmrOnEc2 blueprint deployment setting and choose **Edit**.
6. Under the **Blueprint parameters** section, edit the **certificateLocation** parameter. Enter the S3 location of the ZIP file that contains PEM certificate file(s). You must enter the S3 location URL using the correct format of `s3://<DomainBucketName>/<AmazonDataZoneDomainID>/certificate_location/` Make sure to replace <DomainBucketName>/<AmazonDataZoneDomainID> with the correct values for those for your domain.

   For more information about PEM certificates, see Using PEM certificates.

Getting started with Amazon EMR on EKS in Amazon SageMaker Unified Studio

Before you begin with Amazon EMR on EKS, you must have a compatible Amazon EKS cluster. If you do not have an existing Amazon EKS cluster, see Get started with Amazon EKS for more information regarding cost, installation and management of an Amazon EKS cluster.

Amazon EMR on EKS and Amazon SageMaker Unified Studio require additional Amazon EKS cluster configurations granting minimum access controls and connectivity. Review your Amazon EKS cluster configuration and ensure all requirements are fulfilled:

1. Install and configure the Load Balancer Controller for your Amazon EKS cluster
2. Tag exactly one security group for each Amazon EC2 node ENI with `kubernetes.io/cluster/{eks-cluster-name}`.

   - Amazon EMR on EKS routes the connection from Amazon SageMaker Unified Studio notebooks to Apache Livy on your Amazon EKS cluster through a Network Load Balancer, and the AWS Load Balancer Controller discovers the cluster security group by looking for a single security group that carries this tag on each node ENI. If the same ENI

has more than one security group with this tag, the controller cannot reconcile the `TargetGroupBinding`, no targets register in the load balancer target group, and notebook connections fail (for example, with RemoteDisconnected errors). If you use Karpenter to provision nodes, confirm that your `securityGroupSelectorTerms` configuration does not attach multiple cluster-tagged security groups to a node ENI.

3. Enable Amazon EKS cluster access for Amazon EMR on EKS and Amazon SageMaker Unified Studio

Additionally, Amazon EKS clusters in a different account or Amazon VPC network than your Amazon SageMaker Unified Studio domain require additional configuration. Review your Amazon EKS cluster configuration and ensure all requirements are fulfilled:

1. Enable cross-account access for Amazon EMR on EKS using Amazon SageMaker Unified Studio associated domains
2. Enable cross-network access for Amazon SageMaker Unified Studio using VPC peering connections

Configure project profiles in Amazon SageMaker Unified Studio for Amazon EMR on EKS

For data workers to use Amazon EMR on EKS in Amazon SageMaker Unified Studio, administrators must configure project profiles with Amazon EMR on EKS environment blueprint configurations.

> **Note**
>
> Administrators can configure multiple environment blueprint configurations using different Amazon EKS clusters in the same project profile. Data workers can view environment blueprint configurations and select a specific Amazon EKS cluster when creating Amazon EMR on EKS resources in a Amazon SageMaker Unified Studio project.

1. Navigate to the Amazon SageMaker Unified Studio management console.
2. From the navigation bar, select **Domains**. For cross-account Amazon EKS clusters, select **Associated domains**.
3. Select the name of the domain you want to configure Amazon EMR on EKS for.
4. In the domain management view, navigate to **Project profiles**.

5. Search for and select your target project profile.
6. In the project profile management view, navigate to the **Blueprint deployment settings** view and select **Blueprint deployment settings**.
7. In the **Blueprint** section, select **EmrOnEks** from the dropdown.
8. In the **Account and region** section, specify the same AWS account and AWS region as your Amazon EKS cluster.
9. In the **Blueprint parameters** section, specify the Amazon EKS cluster ARN as the `eksClusterArn` user parameter value.
10. At the bottom of the page, select **Add blueprint deployment settings** to create your Amazon EMR on EKS environment blueprint configuration.

Enable Amazon EKS cluster access for Amazon EMR on EKS and Amazon SageMaker Unified Studio

Amazon EMR on EKS and Amazon SageMaker Unified Studio require access to the Kubernetes service running on the Amazon EKS cluster.

Amazon EKS cluster access for Amazon EMR on EKS

1. Create a Kubernetes cluster role for Amazon EMR on EKS.

```
kubectl apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: emr-containers
rules:
  - apiGroups: [""]
    resources: ["namespaces"]
    verbs: ["get"]
  - apiGroups: [""]
    resources: ["statefulsets", "event", "serviceaccounts", "services",
 "configmaps", "events", "pods", "pods/log", "pods/exec", "pods/portforward",
 "pods/secrets"]
    verbs: ["update", "get", "list", "watch", "describe", "create", "edit",
 "delete", "deletecollection", "annotate", "patch", "label"]
  - apiGroups: [""]
    resources: ["secrets"]
    verbs: ["list", "get", "create", "patch", "delete", "watch"]
```

```
  - apiGroups: ["apps"]
    resources: ["statefulsets", "deployments", "configmaps", "events",
 "persistentvolumeclaims", "pods", "pods/exec", "pods/log", "pods/portforward",
 "pods/secrets", "serviceaccounts", "services"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "annotate", "patch", "update", "label", "deletecollection"]
  - apiGroups: ["batch", "extensions"]
    resources: ["jobs", "configmaps", "events", "persistentvolumeclaims", "pods",
 "pods/exec", "pods/log", "pods/portforward", "pods/secrets", "serviceaccounts",
 "services", "statefulsets"]
    verbs: ["get", "describe", "create", "delete", "watch", "list", "patch",
 "update", "edit", "deletecollection", "label"]
  - apiGroups: ["extensions", "networking.k8s.io"]
    resources: ["ingresses"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "annotate", "patch", "label"]
  - apiGroups: ["rbac.authorization.k8s.io"]
    resources: ["clusterroles","clusterrolebindings","roles", "rolebindings"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "deletecollection", "annotate", "patch", "label"]
  - apiGroups: [""]
    resources: ["persistentvolumeclaims"]
    verbs: ["update", "get", "list", "watch", "describe", "create", "edit",
 "delete",  "deletecollection", "annotate", "patch", "label"]
EOF
```

2. Create a Kubernetes cluster role binding for Amazon EMR on EKS.

```
kubectl apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: emr-containers
subjects:
- kind: User
  name: emr-containers
  apiGroup: rbac.authorization.k8s.io
- kind: User
  name: EmrContainersUser
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: emr-containers
  apiGroup: rbac.authorization.k8s.io
```

```
EOF
```

3. Create a Amazon EKS IAM identity mapping binding the Kubernetes user "emr-containers" to the service-linked IAM role for EMR on EKS.

```
eksctl create iamidentitymapping \
    --cluster {eks-cluster-name} \
    --arn "arn:aws:iam::{aws-account-id}:role/AWSServiceRoleForAmazonEMRContainers"
 \
    --username emr-containers
```

> **Note**
>
> `AWSServiceRoleForAmazonEMRContainers` is a service-linked role managed by Amazon EMR on EKS. For more information, see Using service-linked roles for Amazon EMR on EKS.

Amazon EKS cluster access for Amazon SageMaker Unified Studio

1. Create a Kubernetes cluster role for Amazon SageMaker Unified Studio.

```
kubectl apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: sagemaker-provisioning
rules:
  - apiGroups: [""]
    resources: ["namespaces"]
    verbs: ["create", "delete"]
EOF
```

2. Create a Kubernetes cluster role binding for Amazon SageMaker Unified Studio.

```
kubectl apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: sagemaker-provisioning
```

```
subjects:
- kind: Group
  name: sagemaker-provisioning
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: sagemaker-provisioning
  apiGroup: rbac.authorization.k8s.io
EOF
```

3. Create a Amazon EKS access entry binding the Kubernetes group "sagemaker-provisioning" to the IAM role designated as the provisioning role for your target domain.

```
aws eks create-access-entry \
    --cluster-name {eks-cluster-name} \
    --region {aws-region-code} \
    --principal-arn {iam-provisioning-role-arn} \
    --kubernetes-groups sagemaker-provisioning \
    --type STANDARD
```

Enable cross-account access for Amazon EMR on EKS using Amazon SageMaker Unified Studio associated domains

Amazon EMR on EKS virtual clusters require an Amazon EKS cluster residing in the same account. As an admin, you can make use of Amazon SageMaker Unified Studio associated domains to bring Amazon EKS clusters from any account and use with any Amazon SageMaker Unified Studio domain.

Enabling cross-account access for Amazon EMR on EKS using Amazon SageMaker Unified Studio associated domains requires high privilege access to both Amazon EKS cluster account and Amazon SageMaker Unified Studio domain account.

Step 1: Submit associated domain request from the Amazon SageMaker Unified Studio domain account

1. Navigate to the Amazon SageMaker Unified Studio management console.
2. From the navigation bar, select **Domains**.
3. Select the name of the domain you want to configure Amazon EMR on EKS for.
4. In the domain management view, navigate to **Account associations**.

5. Select the **Request association** button.
6. In the request domain association view, under accounts, provide the Amazon EKS cluster account.
7. Select the **Request assocation** button to submit.

Step 2: Accept and configure associated domain in the Amazon EKS cluster account

1. Navigate to the Amazon SageMaker Unified Studio management console.
2. Select **Associated domains**.
3. Under **Requests**, select the name of the domain you requested domain association for.
4. In the domain association request view, select **Accept association**.
5. After domain association succeeds, select the domain name to navigate the domain management view.
6. In the domain management view, select **Blueprints**.
7. In the Tooling section, select **Enable** and configure the associated Tooling environment.
8. In the Blueprints section, select **EmrOnEks**, enable and configure the associated EmrOnEks environment.

> **Note**
>
> The IAM role designated as the provisioning role must have access to the Amazon EKS cluster. See Enable Amazon EKS cluster access for Amazon EMR on EKS and Amazon SageMaker Unified Studio

Enable cross-network access for Amazon SageMaker Unified Studio using VPC peering connections

> **Note**
>
> If your Amazon SageMaker Unified Studio domain and your Amazon EKS cluster are configured with the same Amazon VPC, you can skip the steps in this section.

Amazon SageMaker Unified Studio requires network connectivity between your Amazon SageMaker Unified Studio domain and your Amazon EKS cluster in order to maintain interactive sessions. See What is VPC peering? and Update your route tables for a VPC peering connection for more information regarding cross-network connectivity with Amazon VPC.

Configuring monitoring with Spark History Server for Amazon EMR on EKS

Amazon EMR on EKS requires additional IAM permissions to enable monitoring with Spark History Server. You must attach the following inline IAM role policy to the IAM role created as the project user role.

> **Note**
>
> The project user role for an Amazon SageMaker Unified Studio project is named `datazone_usr_role_{project_id}`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SparkHistoryServer",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl"
            ],
            "Resource": "arn:aws:sagemaker:*:*:user-profile/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonDataZoneProject": "${aws:PrincipalTag/
AmazonDataZoneProject}"
                }
            }
        }
    ]
}
```

Configuring fine-grained access controls for Amazon EMR on EKS

Amazon EMR on EKS requires additional IAM permissions to enable fine-grained access controls. You must attach the following inline IAM role policy to the IAM role created as the project user role.

> **Note**
>
> The project user role for an Amazon SageMaker Unified Studio project is named `datazone_usr_role_{project_id}`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "FineGrainedAccessControls",
            "Effect": "Allow",
            "Action": [
                "emr-containers:CreateCertificate"
            ],
            "Resource": "*"
        }
    ]
}
```

Configuring trusted identity propagation for Amazon EMR on EKS

Amazon EMR on EKS requires additional IAM permissions to enable trusted identity propagation. You must attach the following inline IAM role policy to the IAM role created as the Amazon EMR on EKS system namespace role.

> **Note**
>
> The Amazon EMR on EKS system namespace role for an Amazon SageMaker Unified Studio project is named `datazone_emr_containers_system_namespace_role_{project_id}`.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TrustedIdentityPropagation",
            "Effect": "Allow",
            "Action": [
                "sso-oauth:CreateTokenWithIAM",
                "sso-oauth:IntrospectTokenWithIAM",
                "sso-oauth:RevokeTokenWithIAM"
            ],
            "Resource": "*"
        }
    ]
}
```

Configuring user background sessions for Amazon EMR on EKS

> **Warning**
>
> When user background sessions is enabled for Amazon EMR on EKS, Amazon SageMaker Unified Studio will not terminate interactive sessions. All interactive sessions will be only terminated once all queries are completed and the compute session has timed out.

Amazon EMR on EKS requires additional IAM permissions to enable user background sessions. You must attach the following inline IAM role policy to the IAM role created as the Amazon EMR on EKS system namespace role.

> **Note**
>
> The Amazon EMR on EKS system namespace role for an Amazon SageMaker Unified Studio project is named `datazone_emr_containers_system_namespace_role_{project_id}`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "UserBackgroundSessions",
```

```
            "Effect": "Allow",
            "Action": [
                "sso:GetApplicationSessionConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

Manage blueprint authorization

You can perform the following procedure to manage the authorization configuration of a blueprint.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose the domain's name from the list. The name is a hyperlink.
3. On the domain's details page, navigate to the **Blueprints** tab.
4. In the **Blueprints** tab, choose the blueprint the authorization configuration of which you'd like to change. The name of the blueprint is a hyperlink.
5. On the bluprint's details page, navigate to the **Authorization** tab.
6. In the Authorization tab, you can use the Add and Remove buttons to add or remove domain units. By adding a domain unit, you're allowing projects that belong to this domain unit to use this blueprint. By removing a domain unit, you're removing the ability to use this blueprint from projects that belong to this domain unit.

   You can use the **Cascade to all child domain units** toggle to apply the authorization setting that you're configuring to all the child domain units of the domain unit that you're adding or removing.

Tooling blueprints in Amazon SageMaker Unified Studio

Every Amazon SageMaker Unified Studio project deploys a Tooling environment first. Tooling provisions the project's Amazon S3 storage, the IAM role for project execution, and a collection of default Amazon DataZone connections. Tooling also provisions AWS resources commonly used within projects, such as Amazon Athena workgroups and AWS Lake Formation permissions.

All blueprints in Amazon SageMaker Unified Studio provision an AWS CloudFormation template using an IAM role designated as the provisioning role. After a project becomes active, you need an IAM role designated as the project user role to run the project. The following table gives the name of each role in an IAM-based domain and in an Identity Center-based domain.

IAM role	IAM-based domain	Identity Center-based domain
Provisioning	`AmazonSageMakerAdminIAMExecutionRole`	`AmazonSageMakerProvisioning-` *`accountId`*
Project user	`AmazonSageMakerUserIAMExecutionRole`	`datazone_usr_role_` *`projectId`* `_` *`environmentId`*

Depending on the type of domain, Amazon SageMaker Unified Studio provides AWS managed policies that can be attached to the provisioning or project user roles to grant full permissions. The following table gives the managed policy for each role in an IAM-based domain and in an Identity Center-based domain.

IAM role	IAM-based domain	Identity Center-based domain
Provisioning	AWS policy: SageMakerStudioAdminIAMPermissiveExecutionPolicy	AWS policy: SageMakerStudioProjectProvisioningRolePolicy
Project user	AWS policy: SageMakerStudioUserIAMPermissiveExecutionPolicy	AWS policy: SageMakerStudioProjectUserRolePolicy

Tooling provisions the default connections that every project requires. The set of connections differs between an IAM-based domain and an Identity Center-based domain. The name of each connection differs too.

Default connection	IAM-based domain	Identity Center-based domain
Amazon Athena (Spark)	`serverless.spark`	`serverless.spark`
Amazon Athena (SQL)	`default.sql`	`project.athena`
Amazon S3, default folder	`default.s3_project`	`project.s3_default_folder`
Amazon S3, root	`default.s3`	—
Amazon S3, shared folder	`default.s3_shared`	`default.s3_shared`
AWS Glue (Spark)	`default.spark`	`project.spark.compatibility` , `project.spark.fineGrained`
AWS IAM	`default.iam`	`project.iam`
Data catalog	`default.catalog`	`project.default_lakehouse`
Workflows	`default.workflow_serverless`	`default.workflow_serverless`

Enable the managed Tooling blueprint for your domain on the Blueprints page. Tooling has parameters you can set, and a permissions boundary you can apply to the roles it creates. For both, see Manage Tooling blueprint parameters.

Topics

- Custom blueprints as Tooling
- Tooling capabilities
- Compatibility with managed blueprints

Custom blueprints as Tooling

In Amazon SageMaker Unified Studio, the managed Tooling blueprint provisions a fixed set of resources for every project. When your organization requires a different foundation, you can use a custom blueprint as a project's Tooling environment instead. Assign the `TOOLING` category when you create a custom blueprint, or update an existing custom blueprint to comply with the minimum Tooling requirements in Template requirements. Amazon SageMaker Unified Studio accepts custom blueprints categorized as `TOOLING` as the first environment deployed in a project profile.

For information that applies to all custom blueprints, including the reserved parameters that Amazon SageMaker Unified Studio populates and the trust policy that the provisioning role requires, see Custom blueprints.

Topics

- Template requirements
- Minimum Tooling template
- Usage

Template requirements

When a blueprint is categorized as `TOOLING`, Amazon SageMaker Unified Studio validates your template by calling `cloudformation:GetTemplateSummary`. The summary of your template must adhere to the minimum Tooling requirements captured in this section, including required AWS CloudFormation parameters, required AWS CloudFormation resources, and required AWS CloudFormation exports.

Parameters

Amazon SageMaker Unified Studio requires your template to declare the following three parameters so that it can supply their values at deployment time.

`datazoneEnvironmentDomainId`

The domain ID.

`datazoneEnvironmentEnvironmentId`

The environment ID.

`datazoneEnvironmentProjectId`

The project ID.

Resources

`DefaultIAMConnection`

The IAM connection that tools use to authenticate. Its name determines which project experience your users see. For more information about project permission sets, see Tooling blueprints in Amazon SageMaker Unified Studio.

`DefaultS3Connection`

The project's primary Amazon S3 connection.

`DefaultS3SharedConnection`

The project's shared Amazon S3 connection, at the `/shared/` prefix of project storage.

Exports

`s3BucketArn`

The ARN of the project's Amazon S3 bucket. A key prefix after the bucket name is allowed.

`s3BucketPath`

The `s3://` URI that other environments in the project resolve their own paths against. A trailing forward slash is optional.

Suffix each export name with the project ID and the scope name, which keeps the name unique within an AWS account and AWS Region and matches the name that other blueprints import. Declare `datazoneScopeName` with a default of `dev`.

```
Outputs:
  S3BucketArn:
    Value: !Sub '${ProjectBucket.Arn}/'
    Export:
      Name: !Sub 's3BucketArn-${datazoneEnvironmentProjectId}-${datazoneScopeName}'
  S3BucketPath:
    Value: !Sub 's3://${ProjectBucket}/shared'
    Export:
```

```
      Name: !Sub 's3BucketPath-${datazoneEnvironmentProjectId}-${datazoneScopeName}'
```

> **Important**
>
> The AWS CloudFormation export `userRoleArn` is not allowed. Amazon SageMaker Unified Studio resolves the project role itself, from the `RoleArn` you bind on the IAM connection, and rejects a template that exports the role again.

Minimum Tooling template

Use one of the templates below to create a minimum Tooling template. Choose the template that matches your domain type, and add capabilities from Tooling capabilities.

> **Note**
>
> The name of the default IAM connection sets the project's experience. The name must match the permission set that project members authenticate with: `default.iam` for IAM permissions, or `project.iam` for IAM Identity Center permissions. No other name is accepted. For more information about project permission sets, see Tooling blueprints in Amazon SageMaker Unified Studio.

The `CreateEnvironmentBlueprint` API requires an Amazon S3 URL for the AWS CloudFormation template. The blueprint's provisioning role must have access to that Amazon S3 object. The `SageMakerStudioProjectProvisioningRolePolicy` managed policy grants `s3:GetObject` on buckets whose names begin with `amazon-sagemaker-cf-templates`. The console creates such a bucket when you upload a template there.

Register the template as a blueprint with `CreateEnvironmentBlueprint`, passing `TOOLING` as the `blueprintCategory`. Optionally, you can declare additional CloudFormation parameters mapped to user parameters when you create a blueprint.

```
aws datazone create-environment-blueprint \
  --domain-identifier domain-id \
  --name blueprint-name \
  --blueprint-category TOOLING \
  --provisioning-properties '{
    "cloudFormation": {
```

```
      "templateUrl": "https://amazon-sagemaker-cf-
templates-region-suffix.s3.region.amazonaws.com/tooling-template.yaml"
    }
  }' \
  --user-parameters '[
    {
      "keyName": "key",
      "fieldType": "String",
      "defaultValue": "value",
      "isEditable": true,
      "isOptional": true
    }
  ]'
```

By default, the blueprint is disabled after it is created. To enable the blueprint in an AWS account and AWS Region, you must provide a provisioning role.

> **Note**
>
> Amazon SageMaker Unified Studio deploys your template under the blueprint's provisioning role, so that role's trust policy must let Amazon SageMaker Unified Studio assume it with `sts:AssumeRole` and pass your user context with `sts:TagSession` for the `datazone.amazonaws.com` service principal. For the policy, see Trust policy for the provisioning role.

```
aws datazone put-environment-blueprint-configuration \
  --domain-identifier domain-id \
  --environment-blueprint-identifier blueprint-id \
  --enabled-regions region \
  --provisioning-role-arn provisioning-role-arn \
  --regional-parameters '{
    "region": {
      "kmsKeyArn": "kms-key-arn"
    }
  }'
```

IAM-based domain

```
AWSTemplateFormatVersion: '2010-09-09'
```

```
Parameters:
  datazoneEnvironmentDomainId:                { Type: String }
  datazoneEnvironmentEnvironmentId:           { Type: String }
  datazoneEnvironmentProjectExecutionRoleArn: { Type: String }
  datazoneEnvironmentProjectId:               { Type: String }
  datazoneScopeName:                          { Type: String, Default: 'dev' }
  sagemakerUnifiedStudioKmsKeyArn:            { Type: String, Default: '' }

Conditions:
  kmsKeyArnExist: !Not [!Equals [!Ref sagemakerUnifiedStudioKmsKeyArn, '']]

Resources:
  ProjectBucket:
    Type: AWS::S3::Bucket
    DeletionPolicy: Retain
    UpdateReplacePolicy: Retain
    Properties:
      BucketName: !Sub 'amazon-sagemaker-${AWS::AccountId}-${AWS::Region}-
${datazoneEnvironmentProjectId}'
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:
              SSEAlgorithm:   !If [kmsKeyArnExist, 'aws:kms', 'AES256']
              KMSMasterKeyID: !If [kmsKeyArnExist, !Ref
 sagemakerUnifiedStudioKmsKeyArn, !Ref 'AWS::NoValue']
      PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
      CorsConfiguration:
        CorsRules:
          - AllowedHeaders: ['*']
            AllowedMethods: [PUT, GET, POST, DELETE, HEAD]
            AllowedOrigins: ['*']
            ExposedHeaders: [x-amz-version-id, ETag, x-amz-checksum-crc32]

  ProjectBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref ProjectBucket
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
```

```
          - Sid: EnforceSSL
            Effect: Deny
            Principal: '*'
            Action: 's3:*'
            Resource: [!GetAtt ProjectBucket.Arn, !Sub '${ProjectBucket.Arn}/*']
            Condition: { Bool: { 'aws:SecureTransport': 'false' } }
          - Sid: ProjectUserRoleAccess
            Effect: Allow
            Principal: '*'
            Action:
              - s3:GetObject*
              - s3:GetBucket*
              - s3:PutObject*
              - s3:ListBucket*
              - s3:RestoreObject
              - s3:ReplicateObject
              - s3:DeleteObject
              - s3:DeleteObjectVersion
              - s3:ListMultipartUploadParts
              - s3:AbortMultipartUpload
              - s3:GetEncryptionConfiguration
            Resource: [!GetAtt ProjectBucket.Arn, !Sub '${ProjectBucket.Arn}/*']
            Condition: { ArnEquals: { 'aws:PrincipalArn': !Ref
datazoneEnvironmentProjectExecutionRoleArn } }
          - Sid: DenyDeleteOfShared
            Effect: Deny
            Principal: '*'
            Action: s3:DeleteObject
            Resource:
              - !Sub '${ProjectBucket.Arn}/shared/'
              - !Sub '${ProjectBucket.Arn}/shared/*'
            Condition: { ArnEquals: { 'aws:PrincipalArn': !Ref
datazoneEnvironmentProjectExecutionRoleArn } }

 DefaultIAMConnection:
   Type: AWS::DataZone::Connection
   Properties:
     Name: default.iam
     DomainIdentifier: !Ref datazoneEnvironmentDomainId
     EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
     ProjectIdentifier: !Ref datazoneEnvironmentProjectId
     AwsLocation: { AwsAccountId: !Ref 'AWS::AccountId', AwsRegion: !Ref
'AWS::Region' }
     Props:
```

```
        IamProperties:
          GlueLineageSyncEnabled: true
          RoleArn: !Ref datazoneEnvironmentProjectExecutionRoleArn

  DefaultS3Connection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: default.s3
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref 'AWS::AccountId'
        AwsRegion: !Ref 'AWS::Region'
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        S3Properties: { S3Uri: !Sub 's3://${ProjectBucket}/',
 RegisterS3AccessGrantLocation: false }

  DefaultS3SharedConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: default.s3_shared
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref 'AWS::AccountId'
        AwsRegion: !Ref 'AWS::Region'
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        S3Properties: { S3Uri: !Sub 's3://${ProjectBucket}/shared/',
 RegisterS3AccessGrantLocation: false }

Outputs:
  S3BucketArn:
    Value: !Sub '${ProjectBucket.Arn}/'
    Export: { Name: !Sub 's3BucketArn-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
  S3BucketPath:
    Value: !Sub 's3://${ProjectBucket}/shared'
    Export: { Name: !Sub 's3BucketPath-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
```

Identity Center-based domain

```
AWSTemplateFormatVersion: '2010-09-09'

Parameters:
  awsDefaultGlueCatalogKmsKeyArn:         { Type: String, Default: '' }
  datazoneEnvironmentDomainArn:           { Type: String }
  datazoneEnvironmentDomainId:            { Type: String }
  datazoneEnvironmentDomainKmsKeyArn:     { Type: String, Default: '' }
  datazoneEnvironmentEnvironmentId:       { Type: String }
  datazoneEnvironmentProjectId:           { Type: String }
  datazoneEnvironmentProvisioningRoleArn: { Type: String }
  datazoneScopeName:                      { Type: String, Default: 'dev' }
  sagemakerUnifiedStudioKmsKeyArn:        { Type: String, Default: '' }
  sagemakerUnifiedStudioNetworkVpcId:     { Type: String, Default: '' }

Conditions:
  defaultGlueCatalogKmsKeyArnExist: !Not [!Equals [!Ref
 awsDefaultGlueCatalogKmsKeyArn, '']]
  domainKmsKeyArnExist:             !Not [!Equals [!Ref
 datazoneEnvironmentDomainKmsKeyArn, '']]
  kmsKeyArnExist:                   !Not [!Equals [!Ref
 sagemakerUnifiedStudioKmsKeyArn, '']]

Resources:
  ProjectBucket:
    Type: AWS::S3::Bucket
    DeletionPolicy: Retain
    UpdateReplacePolicy: Retain
    Properties:
      BucketName: !Sub 'sagemaker-${AWS::AccountId}-${AWS::Region}-
${datazoneEnvironmentProjectId}'
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:
              SSEAlgorithm:   !If [kmsKeyArnExist, 'aws:kms', 'AES256']
              KMSMasterKeyID: !If [kmsKeyArnExist, !Ref
 sagemakerUnifiedStudioKmsKeyArn, !Ref 'AWS::NoValue']
      PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
      CorsConfiguration:
```

```
        CorsRules:
          - AllowedHeaders: ['*']
            AllowedMethods: [PUT, GET, POST, DELETE, HEAD]
            AllowedOrigins: ['*']
            ExposedHeaders: [x-amz-version-id, ETag, x-amz-checksum-crc32]

  ToolingLogGroup:
    Type: AWS::Logs::LogGroup
    DeletionPolicy: Delete
    Properties:
      LogGroupName: !Sub 'datazone-${datazoneEnvironmentProjectId}-
${datazoneScopeName}'
      RetentionInDays: 30

  ProjectUserRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: !Sub 'datazone_usr_role_${datazoneEnvironmentProjectId}_
${datazoneEnvironmentEnvironmentId}'
      Description: User role for all environments and tools.
      Path: /
      ManagedPolicyArns:
        - !Sub 'arn:${AWS::Partition}:iam::aws:policy/
SageMakerStudioProjectUserRolePolicy'
        - !Sub 'arn:${AWS::Partition}:iam::aws:policy/
SageMakerStudioProjectRoleMachineLearningPolicy'
        - !Sub 'arn:${AWS::Partition}:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy'
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service: [datazone.amazonaws.com, auth.datazone.amazonaws.com]
            Action: [sts:AssumeRole, sts:TagSession, sts:SetContext,
 sts:SetSourceIdentity]
            Condition:
              StringEquals:
                aws:SourceAccount: !Select [4, !Split [':', !Ref
 datazoneEnvironmentDomainArn]]
          - Effect: Allow
            Principal:
              Service:
                - glue.amazonaws.com
```

```
                - lakeformation.amazonaws.com
                - sagemaker.amazonaws.com
                - emr-serverless.amazonaws.com
                - elasticmapreduce.amazonaws.com
                - airflow.amazonaws.com
                - airflow-env.amazonaws.com
                - lambda.amazonaws.com
                - scheduler.amazonaws.com
                - quicksight.amazonaws.com
                - access-grants.s3.amazonaws.com
                - athena.amazonaws.com
                - airflow-serverless.amazonaws.com
                - bedrock.amazonaws.com
            Action: [sts:AssumeRole, sts:TagSession, sts:SetContext,
 sts:SetSourceIdentity]
            Condition:
              StringEquals: { aws:SourceAccount: !Ref 'AWS::AccountId' }
          - Effect: Allow
            Principal:
              Service: [redshift-serverless.amazonaws.com, redshift.amazonaws.com]
            Action: sts:AssumeRole
            Condition:
              StringLike:
                sts:ExternalId: !Sub 'arn:${AWS::Partition}:redshift:*:
${AWS::AccountId}:dbuser:*/*'
          - Effect: Allow
            Principal:
              Service: [redshift-serverless.amazonaws.com, redshift.amazonaws.com]
            Action: [sts:TagSession, sts:SetContext, sts:SetSourceIdentity]
          - Effect: Allow
            Principal:
              AWS: !Ref datazoneEnvironmentProvisioningRoleArn
            Action: [sts:AssumeRole, sts:TagSession, sts:SetContext,
 sts:SetSourceIdentity]
      Tags:
        - { Key: AmazonDataZoneScopeName,               Value: !Ref
 datazoneScopeName }
        - { Key: RedshiftDbUser,                        Value: !Sub 'user-project@
${datazoneEnvironmentProjectId}' }
        - { Key: DomainBucketName,                      Value: !Ref ProjectBucket }
        - { Key: EnableAmazonBedrockPermissions,        Value: 'true' }
        - { Key: EnableGlueWorkloadsPermissions,        Value: 'true' }
        - { Key: EnableSageMakerMLWorkloadsPermissions, Value: 'true' }
```

```
        - { Key: KmsKeyId,                   Value: !If [kmsKeyArnExist,
       !Select [1, !Split ['/', !Ref sagemakerUnifiedStudioKmsKeyArn]],    ''] }
        - { Key: DomainKmsKeyId,             Value: !If [domainKmsKeyArnExist,
       !Select [1, !Split ['/', !Ref datazoneEnvironmentDomainKmsKeyArn]], ''] }
        - { Key: DefaultGlueCatalogKmsKeyId, Value: !If
 [defaultGlueCatalogKmsKeyArnExist, !Select [1, !Split ['/', !Ref
 awsDefaultGlueCatalogKmsKeyArn]],     ''] }
        - { Key: LogGroupName,                         Value: !Ref
 ToolingLogGroup }
        - { Key: RoleName,  Value: !Sub 'datazone_usr_role_
${datazoneEnvironmentProjectId}_${datazoneEnvironmentEnvironmentId}' }
        - { Key: vpcArn,    Value: !Sub 'arn:${AWS::Partition}:ec2:${AWS::Region}:
${AWS::AccountId}:vpc/${sagemakerUnifiedStudioNetworkVpcId}' }
        - { Key: VpcId,     Value: !Ref sagemakerUnifiedStudioNetworkVpcId }

  ProjectBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref ProjectBucket
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Sid: DenyInsecureConnections
            Effect: Deny
            Principal: '*'
            Action: 's3:*'
            Resource: [!GetAtt ProjectBucket.Arn, !Sub '${ProjectBucket.Arn}/*']
            Condition: { Bool: { 'aws:SecureTransport': 'false' } }
          - Sid: AllowToolingUserAccess
            Effect: Allow
            Principal: '*'
            Action: [s3:GetObject*, s3:GetBucket*, s3:PutObject*, s3:ListBucket*,
 s3:RestoreObject, s3:ReplicateObject,
                     s3:DeleteObject, s3:DeleteObjectVersion,
 s3:ListMultipartUploadParts, s3:AbortMultipartUpload,
                     s3:GetEncryptionConfiguration]
            Resource: [!GetAtt ProjectBucket.Arn, !Sub '${ProjectBucket.Arn}/*']
            Condition: { ArnEquals: { 'aws:PrincipalArn': !GetAtt
 ProjectUserRole.Arn } }

  DefaultIAMConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: project.iam
```

```
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation: { AwsAccountId: !Ref 'AWS::AccountId', AwsRegion: !Ref
 'AWS::Region' }
      Props:
        IamProperties:
          GlueLineageSyncEnabled: true
          RoleArn: !GetAtt ProjectUserRole.Arn

  DefaultS3Connection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: default.s3
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref 'AWS::AccountId'
        AwsRegion: !Ref 'AWS::Region'
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        S3Properties: { S3Uri: !Sub 's3://${ProjectBucket}/',
 RegisterS3AccessGrantLocation: false }

  DefaultS3SharedConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: default.s3_shared
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref 'AWS::AccountId'
        AwsRegion: !Ref 'AWS::Region'
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        S3Properties: { S3Uri: !Sub 's3://${ProjectBucket}/shared/',
 RegisterS3AccessGrantLocation: false }

Outputs:
  S3BucketArn:
    Value: !Sub '${ProjectBucket.Arn}/'
```

```
    Export: { Name: !Sub 's3BucketArn-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
  S3BucketPath:
    Value: !Sub 's3://${ProjectBucket}/shared'
    Export: { Name: !Sub 's3BucketPath-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
```

Usage

After your blueprint is created and enabled, you use it by composing it into a project profile and then creating a project from that profile.

Project profile

A project profile names the blueprint that fills the Tooling slot and declares which parameters a project creator can set. Call `CreateProjectProfile`.

Give the Tooling environment a `deploymentMode` of `ON_CREATE` and a `deploymentOrder` of `0`, so that it deploys before anything else in the profile.

> **Note**
>
> A profile can target an account pool instead of a named account. For how account pools work and how to create one, see Account pools in Amazon SageMaker Unified Studio.

```
aws datazone create-project-profile \
  --domain-identifier domain-id \
  --name profile-name \
  --status ENABLED \
  --environment-configurations '[
    {
      "name": "CustomTooling",
      "environmentBlueprintId": "blueprint-id",
      "deploymentMode": "ON_CREATE",
      "deploymentOrder": 0,
      "awsAccount": { "awsAccountId": "account-id" },
      "awsRegion": { "regionName": "region" },
      "configurationParameters": {
        "parameterOverrides": [
          { "name": "parameter-name", "value": "" }
```

```
        ]
      }
    }
  ]'
```

> **Important**
>
> Pass `--status ENABLED`. A profile is created `DISABLED`, and a disabled profile can't be used to create a project.

Project

Create a project

Call `CreateProject` and reference the profile. Supply user parameter values under `--user-parameters`. The `environmentConfigurationName` value must match the name in the profile exactly.

```
aws datazone create-project \
  --domain-identifier domain-id \
  --name project-name \
  --project-profile-id profile-id \
  --user-parameters '[
    {
      "environmentConfigurationName": "CustomTooling",
      "environmentParameters": [
        { "name": "parameter-name", "value": "value" }
      ]
    }
  ]'
```

In an IAM-based domain, also pass the role that becomes the project role. Your template receives this ARN through the reserved parameter `datazoneEnvironmentProjectExecutionRoleArn`. In an Identity Center-based domain, omit it, because your template creates the project role itself.

```
aws datazone create-project \
  --domain-identifier domain-id \
  --name project-name \
  --project-profile-id profile-id \
  --project-execution-role project-role-arn
```

Tooling capabilities

A service-managed Tooling environment already provisions a broad set of capabilities. With a custom Tooling blueprint you decide which of them your template provisions, subject only to the minimum in Template requirements.

Each module is a partial AWS CloudFormation fragment, not a template on its own. Combine one, several, or all of them into a template from Minimum Tooling template. For the IAM roles that Tooling requires and the AWS managed policies that grant their permissions, see Tooling blueprints in Amazon SageMaker Unified Studio.

Topics

- Amazon Athena
- Amazon Athena (Spark)
- Data catalog
- Amazon EventBridge Scheduler
- AWS Glue (Spark)
- AWS Lake Formation
- Amazon Managed Workflows for Apache Airflow
- Amazon SageMaker AI
- Trusted identity propagation

Amazon Athena

Provisions an Amazon Athena workgroup and a connection to it, so project members can run SQL against the project's data. The workgroup writes its results under the project's Amazon S3 storage, encrypted with the project's AWS KMS key when the domain has one.

IAM-based domain

```
Resources:
  AthenaWorkGroup:
    Type: AWS::Athena::WorkGroup
    Properties:
      Name: !Sub 'sagemaker-studio-workgroup-${datazoneEnvironmentProjectId}'
      Description: SageMaker Unified Studio project Workgroup
      RecursiveDeleteOption: true
```

```
      Tags:
        - { Key: AmazonDataZoneScopeName, Value: !Ref datazoneScopeName }
      WorkGroupConfiguration:
        EnforceWorkGroupConfiguration: true
        CustomerContentEncryptionConfiguration:
          Fn::If:
            - kmsKeyArnExist
            - KmsKey: !Ref sagemakerUnifiedStudioKmsKeyArn
            - !Ref 'AWS::NoValue'
        ResultConfiguration:
          EncryptionConfiguration:
            Fn::If:
              - kmsKeyArnExist
              - EncryptionOption: SSE_KMS
                KmsKey: !Ref sagemakerUnifiedStudioKmsKeyArn
              - EncryptionOption: SSE_S3
          OutputLocation: !Sub 's3://${ProjectBucket}/sys/athena/'

  AthenaConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: default.sql
      Description: Default connection to Amazon Athena SQL for interactive queries
 on your data.
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        AthenaProperties:
          WorkgroupName: !Ref AthenaWorkGroup

Outputs:
  AthenaWorkGroupName:
    Value: !Ref AthenaWorkGroup
    Export:
      Name: !Sub 'athenaWorkGroupName-${datazoneEnvironmentEnvironmentId}'
  AthenaOutputUri:
    Value: !Sub 's3://${ProjectBucket}/sys/athena/'
    Export:
```

```
      Name: !Sub 'athenaOutputUri-${datazoneEnvironmentEnvironmentId}'
```

Identity Center-based domain

```
Resources:
  AthenaWorkGroup:
    Type: AWS::Athena::WorkGroup
    Properties:
      Name: !Sub 'workgroup-${datazoneEnvironmentProjectId}-
${datazoneEnvironmentEnvironmentId}'
      Description: DataZone Workgroup
      RecursiveDeleteOption: true
      Tags:
        - { Key: AmazonDataZoneScopeName, Value: !Ref datazoneScopeName }
      WorkGroupConfiguration:
        EnforceWorkGroupConfiguration: true
        CustomerContentEncryptionConfiguration:
          Fn::If:
            - kmsKeyArnExist
            - KmsKey: !Ref sagemakerUnifiedStudioKmsKeyArn
            - !Ref 'AWS::NoValue'
        ResultConfiguration:
          EncryptionConfiguration:
            Fn::If:
              - kmsKeyArnExist
              - EncryptionOption: SSE_KMS
                KmsKey: !Ref sagemakerUnifiedStudioKmsKeyArn
              - EncryptionOption: SSE_S3
          OutputLocation: !Sub 's3://${ProjectBucket}/dev/sys/athena/'

  AthenaConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: project.athena
      Description: Default connection to Amazon Athena SQL for interactive queries
 on your data.
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
```

```
      Props:
        AthenaProperties:
          WorkgroupName: !Ref AthenaWorkGroup

Outputs:
  AthenaWorkGroupName:
    Value: !Ref AthenaWorkGroup
    Export:
      Name: !Sub 'athenaWorkGroupName-${datazoneEnvironmentEnvironmentId}'
  AthenaOutputUri:
    Value: !Sub 's3://${ProjectBucket}/dev/sys/athena/'
    Export:
      Name: !Sub 'athenaOutputUri-${datazoneEnvironmentEnvironmentId}'
```

Amazon Athena (Spark)

Provisions an Amazon Athena Spark workgroup and a connection to it, which gives members Spark without a VPC or a cluster. The workgroup runs calculations as the project user role and writes its logs under the project's Amazon S3 storage.

IAM-based domain

```
Resources:
  AthenaSparkWorkGroup:
    Type: AWS::Athena::WorkGroup
    Properties:
      Name: !Sub 'sagemaker-studio-spark-workgroup-${datazoneEnvironmentProjectId}'
      Description: SageMaker Unified Studio project Athena Spark Workgroup
      WorkGroupConfiguration:
        EnforceWorkGroupConfiguration: false
        PublishCloudWatchMetricsEnabled: true
        EngineVersion:
          SelectedEngineVersion: Apache Spark version 3.5
        ExecutionRole: !Ref datazoneEnvironmentProjectExecutionRoleArn
        MonitoringConfiguration:
          ManagedLoggingConfiguration:
            Enabled: true
            KmsKey: !If [kmsKeyArnExist, !Ref sagemakerUnifiedStudioKmsKeyArn, !Ref
 'AWS::NoValue']
          S3LoggingConfiguration:
            Enabled: true
```

```
            KmsKey: !If [kmsKeyArnExist, !Ref sagemakerUnifiedStudioKmsKeyArn, !Ref
 'AWS::NoValue']
            LogLocation: !Sub 's3://${ProjectBucket}/sys/athena-spark/'

  ServerlessSparkConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: serverless.spark
      Description: Default connection to Amazon Athena for Apache Spark, designed
 for interactive data analysis.
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        AthenaProperties:
          WorkgroupName: !Ref AthenaSparkWorkGroup

Outputs:
  AthenaSparkWorkGroupName:
    Value: !Ref AthenaSparkWorkGroup
    Export:
      Name: !Sub 'athenaSparkWorkGroupName-${datazoneEnvironmentEnvironmentId}'
```

Identity Center-based domain

```
Resources:
  AthenaSparkWorkGroup:
    Type: AWS::Athena::WorkGroup
    Properties:
      Name: !Sub 'sagemaker-studio-spark-workgroup-${datazoneEnvironmentProjectId}'
      Description: SageMaker Unified Studio project Athena Spark Workgroup
      WorkGroupConfiguration:
        EnforceWorkGroupConfiguration: true
        PublishCloudWatchMetricsEnabled: true
        EngineVersion:
          SelectedEngineVersion: Apache Spark version 3.5
        ExecutionRole: !GetAtt ProjectUserRole.Arn
        MonitoringConfiguration:
          ManagedLoggingConfiguration:
```

```
            Enabled: true
            KmsKey: !If [kmsKeyArnExist, !Ref sagemakerUnifiedStudioKmsKeyArn, !Ref
 'AWS::NoValue']
          S3LoggingConfiguration:
            Enabled: true
            KmsKey: !If [kmsKeyArnExist, !Ref sagemakerUnifiedStudioKmsKeyArn, !Ref
 'AWS::NoValue']
            LogLocation: !Sub 's3://${ProjectBucket}/dev/sys/athena-spark-logs/'

  ServerlessSparkConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: serverless.spark
      Description: Default connection to Amazon Athena for Apache Spark, designed
 for interactive data analysis.
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        AthenaProperties:
          WorkgroupName: !Ref AthenaSparkWorkGroup

Outputs:
  AthenaSparkWorkGroupName:
    Value: !Ref AthenaSparkWorkGroup
    Export:
      Name: !Sub 'athenaSparkWorkGroupName-${datazoneEnvironmentEnvironmentId}'
```

Data catalog

Declares the connection that gives project members the catalogs available in AWS Glue, which is what populates the catalog browser in the project. The connection carries no configuration of its own: it resolves the account's catalogs through the project user role, so a project gets exactly the catalogs that role can reach.

IAM-based domain

```
Resources:
```

```
  DefaultCatalogConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: default.catalog
      Description: This is the default connection to all catalogs available in your
 AWS Glue.
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        LakehouseProperties: {}
```

Identity Center-based domain

```
Resources:
  DefaultCatalogConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: project.default_lakehouse
      Description: This is the default connection to interact with project
 Lakehouse.
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        LakehouseProperties:
          GlueLineageSyncEnabled: true
```

Amazon EventBridge Scheduler

Declares the schedule group that holds a project's schedules. Project members who schedule a notebook or a query create schedules inside this group, and a project without one cannot schedule work.

```
Resources:
  EventBridgeScheduleGroup:
    Type: AWS::Scheduler::ScheduleGroup
    Properties:
      Name: !Sub 'SageMakerUnifiedStudio-${datazoneEnvironmentProjectId}-
${datazoneScopeName}'
      Tags:
        - { Key: AmazonDataZoneScopeName, Value: !Ref datazoneScopeName }

Outputs:
  ScheduleGroupName:
    Value: !Ref EventBridgeScheduleGroup
    Export:
      Name: !Sub 'ScheduleGroupName-${datazoneEnvironmentProjectId}-
${datazoneScopeName}'
```

AWS Glue (Spark)

Declares the Spark connections that run AWS Glue ETL sessions. An IAM-based domain uses a single compatibility connection. An Identity Center-based domain uses two, differing only in AWS Lake Formation permission mode. Each connection takes the project's Glue network connection when the domain has one, and omits it otherwise.

IAM-based domain

```
Parameters:
  sagemakerUnifiedStudioNetworkGlueConnectionNames:
    Type: String
    Default: ''

Conditions:
  NetworkGlueConnectionsExist: !Not [!Equals [!Ref
 sagemakerUnifiedStudioNetworkGlueConnectionNames, '']]

Resources:
  SparkGlueCompatibilityConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: default.spark
      Description: Default connection to Spark compute from AWS Glue for visual ETL,
 interactive analysis and batch jobs.
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
```

```
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        SparkGlueProperties:
          GlueConnectionName: !If
            - NetworkGlueConnectionsExist
            - !Select [0, !Split [',', !Ref
 sagemakerUnifiedStudioNetworkGlueConnectionNames]]
            - !Ref 'AWS::NoValue'
          GlueVersion: '5.0'
          IdleTimeout: 60
          NumberOfWorkers: 10
          WorkerType: G.1X
      Configurations:
        - Classification: GlueDefaultArgument
          Properties:
            '--enable-lakeformation-fine-grained-access': 'false'
```

Identity Center-based domain

```
Parameters:
  sagemakerUnifiedStudioNetworkSecurityGroupId:
    Type: String
  sagemakerUnifiedStudioNetworkSubnets:
    Type: String

Resources:
  ProjectGlueNetworkConnection:
    Type: AWS::Glue::Connection
    Properties:
      CatalogId: !Ref AWS::AccountId
      ConnectionInput:
        ConnectionType: NETWORK
        Description: Connection between Glue and VPC
        Name: !Sub 'datazone-glue-network-connection-
${datazoneEnvironmentProjectId}-${datazoneScopeName}'
        PhysicalConnectionRequirements:
          SecurityGroupIdList:
            - !Ref sagemakerUnifiedStudioNetworkSecurityGroupId
```

```
          SubnetId: !Select [0, !Split [',', !Ref
 sagemakerUnifiedStudioNetworkSubnets]]

  SparkGlueCompatibilityConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: project.spark.compatibility
      Description: Glue-ETL compute with Permission Mode set to compatibility.
 (Auto-created by project).
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        SparkGlueProperties:
          GlueConnectionName: !Ref ProjectGlueNetworkConnection
          GlueVersion: '5.0'
          IdleTimeout: 60
          NumberOfWorkers: 10
          WorkerType: G.1X
      Configurations:
        - Classification: GlueDefaultArgument
          Properties:
            '--enable-lakeformation-fine-grained-access': 'false'

  SparkGlueFineGrainedConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: project.spark.fineGrained
      Description: Glue-ETL compute with Permission Mode set to fine-grained. (Auto-
created by project).
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        SparkGlueProperties:
          GlueConnectionName: !Ref ProjectGlueNetworkConnection
```

```
          GlueVersion: '5.0'
          IdleTimeout: 60
          NumberOfWorkers: 10
          WorkerType: G.1X
      Configurations:
        - Classification: GlueDefaultArgument
          Properties:
            '--enable-lakeformation-fine-grained-access': 'true'
```

AWS Lake Formation

Grants the project user role the AWS Lake Formation permissions it needs to work with the project's data. With an Identity Center-based domain, your project's Amazon S3 location is also registered with AWS Lake Formation, so AWS Lake Formation governs data written there. With an IAM-based domain, you rely on account-level full table access instead; no location is registered and no data location permission is granted.

With an IAM-based domain, you don't add this capability to your template. The project role is the role that you pass at project creation, and the grant belongs to that role rather than to a project. As a result, you make the grant once per role with the AWS CLI instead of once per project in a template.

> **Important**
>
> Amazon SageMaker Unified Studio performs two account-level AWS Lake Formation actions for a service-managed environment that a template can't express. You are responsible for both, once per account, before you deploy a custom blueprint that includes this capability:
>
> - Register the blueprint's provisioning role as an AWS Lake Formation data lake administrator. Creating an AWS Lake Formation permission fails without it.
> - In an IAM-based domain, enable full table access for the account. This is an account-level setting, and it stays in effect after you delete the project.

IAM-based domain

Don't put this grant in your template. The project role in an IAM-based domain is the role that you pass at project creation, and an AWS Lake Formation permission is held by a principal,

not by a project. A template that grants it fails on the second project that passes the same role, with `Resource of type 'AWS::LakeFormation::PrincipalPermissions' ... already exists.`

Grant it yourself instead, once per project role.

```
aws lakeformation grant-permissions \
  --catalog-id account-id \
  --principal DataLakePrincipalIdentifier=project-role-arn \
  --resource '{
    "Database": { "CatalogId": "account-id", "Name": "default" }
  }' \
  --permissions DESCRIBE
```

An IAM-based domain registers no Amazon S3 location and grants no data location permission, so this AWS Lake Formation DESCRIBE grant is the whole of the capability for this domain type.

Identity Center-based domain

```
Resources:
  ProjectS3LakeFormationResource:
    Type: AWS::LakeFormation::Resource
    Properties:
      ResourceArn: !Sub '${ProjectBucket.Arn}/${datazoneScopeName}'
      RoleArn: !GetAtt ProjectUserRole.Arn
      UseServiceLinkedRole: false

  DefaultDatabaseDescribePermission:
    Type: AWS::LakeFormation::PrincipalPermissions
    Properties:
      Catalog: !Ref AWS::AccountId
      Principal:
        DataLakePrincipalIdentifier: !GetAtt ProjectUserRole.Arn
      Resource:
        Database:
          CatalogId: !Ref AWS::AccountId
          Name: default
      Permissions:
        - DESCRIBE
      PermissionsWithGrantOption: []

  ProjectS3DataLocationPermission:
    Type: AWS::LakeFormation::PrincipalPermissions
```

```
    DependsOn: ProjectS3LakeFormationResource
    Properties:
      Catalog: !Ref AWS::AccountId
      Principal:
        DataLakePrincipalIdentifier: !GetAtt ProjectUserRole.Arn
      Resource:
        DataLocation:
          CatalogId: !Ref AWS::AccountId
          ResourceArn: !Sub '${ProjectBucket.Arn}/${datazoneScopeName}'
      Permissions:
        - DATA_LOCATION_ACCESS
      PermissionsWithGrantOption: []
```

Amazon Managed Workflows for Apache Airflow

Declares the connection that runs a project's workflows on serverless Amazon Managed Workflows for Apache Airflow compute. Project members author and run workflows through this connection, and a project without it cannot run them. The connection carries no configuration of its own.

IAM-based domain

```
Resources:
  WorkflowsServerlessConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: default.workflow_serverless
      Description: Default connection to Amazon Managed Workflows for Apache Airflow
 (MWAA) serverless compute.
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        WorkflowsServerlessProperties: {}
```

Identity Center-based domain

```
Resources:
  WorkflowsServerlessConnection:
```

```
    Type: AWS::DataZone::Connection
    Properties:
      Name: default.workflow_serverless
      Description: Default connection to Amazon Managed Workflows for Apache Airflow
 (MWAA) serverless compute.
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      Props:
        WorkflowsServerlessProperties: {}
```

Amazon SageMaker AI

Provisions an Amazon SageMaker AI domain, which backs the JupyterLab and Code Editor spaces that members open from the project. The domain runs spaces as the project user role. When the Amazon SageMaker Unified Studio domain is configured with a VPC, the Amazon SageMaker AI domain confines space traffic to it; otherwise spaces reach the internet through an Amazon SageMaker AI managed VPC.

IAM-based domain

```
Parameters:
  datazoneEnvironmentDomainArn:
    Type: String
  sagemakerUnifiedStudioNetworkVpcId:
    Type: String
    Default: ''
  sagemakerUnifiedStudioNetworkSubnets:
    Type: String
    Default: ''
  sagemakerUnifiedStudioNetworkSecurityGroupId:
    Type: String
    Default: ''

Conditions:
  VpcIdExists: !Not [!Equals [!Ref sagemakerUnifiedStudioNetworkVpcId, '']]

Resources:
```

```
  SageMakerSpacesDefaultDomain:
    Type: AWS::SageMaker::Domain
    Properties:
      DomainName: !Sub 'SageMakerUnifiedStudio-${datazoneEnvironmentProjectId}-
${datazoneEnvironmentEnvironmentId}-${datazoneScopeName}'
      AuthMode: IAM
      AppNetworkAccessType: !If [VpcIdExists, VpcOnly, PublicInternetOnly]
      VpcId: !If [VpcIdExists, !Ref sagemakerUnifiedStudioNetworkVpcId, !Ref
 'AWS::NoValue']
      SubnetIds: !If [VpcIdExists, !Split [',', !Ref
 sagemakerUnifiedStudioNetworkSubnets], !Ref 'AWS::NoValue']
      KmsKeyId: !If [kmsKeyArnExist, !Ref sagemakerUnifiedStudioKmsKeyArn, !Ref
 'AWS::NoValue']
      DomainSettings:
        DockerSettings:
          EnableDockerAccess: ENABLED
        ExecutionRoleIdentityConfig: USER_PROFILE_NAME
      DefaultSpaceSettings:
        ExecutionRole: !Ref datazoneEnvironmentProjectExecutionRoleArn
        JupyterLabAppSettings:
          AppLifecycleManagement:
            IdleSettings:
              IdleTimeoutInMinutes: 60
              LifecycleManagement: ENABLED
              MaxIdleTimeoutInMinutes: 525600
              MinIdleTimeoutInMinutes: 60
      DefaultUserSettings:
        ExecutionRole: !Ref datazoneEnvironmentProjectExecutionRoleArn
        SecurityGroups: !If [VpcIdExists, !Split [',', !Ref
 sagemakerUnifiedStudioNetworkSecurityGroupId], !Ref 'AWS::NoValue']
        JupyterLabAppSettings:
          AppLifecycleManagement:
            IdleSettings:
              IdleTimeoutInMinutes: 60
              LifecycleManagement: ENABLED
              MaxIdleTimeoutInMinutes: 525600
              MinIdleTimeoutInMinutes: 60
        CodeEditorAppSettings:
          AppLifecycleManagement:
            IdleSettings:
              IdleTimeoutInMinutes: 60
              LifecycleManagement: ENABLED
              MaxIdleTimeoutInMinutes: 525600
              MinIdleTimeoutInMinutes: 60
```

```
        SpaceStorageSettings:
          DefaultEbsStorageSettings:
            DefaultEbsVolumeSizeInGb: 16
            MaximumEbsVolumeSizeInGb: 100
        CustomFileSystemConfigs:
          - S3FileSystemConfig:
              S3Uri: !Sub 's3://${ProjectBucket}/shared/'
              MountPath: shared
      Tags:
        - { Key: AmazonDataZoneDomainAccount, Value: !Select [4, !Split [':', !Ref
 datazoneEnvironmentDomainArn]] }
        - { Key: AmazonDataZoneDomainRegion,  Value: !Select [3, !Split [':', !Ref
 datazoneEnvironmentDomainArn]] }
        - { Key: AmazonDataZoneDomain,        Value: !Ref
 datazoneEnvironmentDomainId }
        - { Key: AmazonDataZoneProject,       Value: !Ref
 datazoneEnvironmentProjectId }
        - { Key: AmazonDataZoneEnvironment,   Value: !Ref
 datazoneEnvironmentEnvironmentId }
        - { Key: AmazonDataZoneStage,         Value: prod }
        - { Key: AmazonDataZoneScopeName,     Value: !Ref datazoneScopeName }
        - { Key: ProjectS3Path,               Value: !Sub 's3://${ProjectBucket}/
shared/' }

Outputs:
  SageMakerSpacesDomain:
    Value: !GetAtt SageMakerSpacesDefaultDomain.DomainId
    Export:
      Name: !Sub 'SageMakerSpacesDomain-${datazoneEnvironmentEnvironmentId}-
${datazoneScopeName}'
  SageMakerDomainId:
    Value: !GetAtt SageMakerSpacesDefaultDomain.DomainId
    Export:
      Name: !Sub 'sageMakerDomainId-${datazoneEnvironmentEnvironmentId}-
${datazoneScopeName}'
```

Identity Center-based domain

> **Note**
>
> Replace *minute* and *hour* on the data source schedule with a daily time of your choosing. A service-managed environment picks this time per data source so that scans don't all run at once. Avoid giving every project the same value. Copying the

listing without substituting them leaves an invalid cron expression. The stack then fails validation before any resource is created.

```
Parameters:
  datazoneEnvironmentDomainArn:
    Type: String
  sagemakerUnifiedStudioNetworkVpcId:
    Type: String
    Default: ''
  sagemakerUnifiedStudioNetworkSubnets:
    Type: String
    Default: ''
  sagemakerUnifiedStudioNetworkSecurityGroupId:
    Type: String
    Default: ''

Conditions:
  VpcIdExists: !Not [!Equals [!Ref sagemakerUnifiedStudioNetworkVpcId, '']]

Resources:
  SageMakerSpacesDefaultDomain:
    Type: AWS::SageMaker::Domain
    Properties:
      DomainName: !Sub 'SageMakerUnifiedStudio-${datazoneEnvironmentProjectId}-
${datazoneEnvironmentEnvironmentId}-${datazoneScopeName}'
      AuthMode: IAM
      AppNetworkAccessType: !If [VpcIdExists, VpcOnly, PublicInternetOnly]
      VpcId: !If [VpcIdExists, !Ref sagemakerUnifiedStudioNetworkVpcId, !Ref
 'AWS::NoValue']
      SubnetIds: !If [VpcIdExists, !Split [',', !Ref
 sagemakerUnifiedStudioNetworkSubnets], !Ref 'AWS::NoValue']
      KmsKeyId: !If [kmsKeyArnExist, !Ref sagemakerUnifiedStudioKmsKeyArn, !Ref
 'AWS::NoValue']
      DomainSettings:
        DockerSettings:
          EnableDockerAccess: ENABLED
        ExecutionRoleIdentityConfig: USER_PROFILE_NAME
      DefaultSpaceSettings:
        ExecutionRole: !GetAtt ProjectUserRole.Arn
        JupyterLabAppSettings:
          AppLifecycleManagement:
            IdleSettings:
```

```
              IdleTimeoutInMinutes: 60
              LifecycleManagement: ENABLED
              MaxIdleTimeoutInMinutes: 525600
              MinIdleTimeoutInMinutes: 60
      DefaultUserSettings:
        ExecutionRole: !GetAtt ProjectUserRole.Arn
        SecurityGroups: !If [VpcIdExists, !Split [',', !Ref
sagemakerUnifiedStudioNetworkSecurityGroupId], !Ref 'AWS::NoValue']
        JupyterLabAppSettings:
          AppLifecycleManagement:
            IdleSettings:
              IdleTimeoutInMinutes: 60
              LifecycleManagement: ENABLED
              MaxIdleTimeoutInMinutes: 525600
              MinIdleTimeoutInMinutes: 60
        CodeEditorAppSettings:
          AppLifecycleManagement:
            IdleSettings:
              IdleTimeoutInMinutes: 60
              LifecycleManagement: ENABLED
              MaxIdleTimeoutInMinutes: 525600
              MinIdleTimeoutInMinutes: 60
        SpaceStorageSettings:
          DefaultEbsStorageSettings:
            DefaultEbsVolumeSizeInGb: 16
            MaximumEbsVolumeSizeInGb: 100
        CustomFileSystemConfigs:
          - S3FileSystemConfig:
              S3Uri: !Sub 's3://${ProjectBucket}/shared'
              MountPath: shared
      Tags:
        - { Key: AmazonDataZoneDomainAccount, Value: !Select [4, !Split [':', !Ref
datazoneEnvironmentDomainArn]] }
        - { Key: AmazonDataZoneDomainRegion,  Value: !Select [3, !Split [':', !Ref
datazoneEnvironmentDomainArn]] }
        - { Key: AmazonDataZoneDomain,        Value: !Ref
datazoneEnvironmentDomainId }
        - { Key: AmazonDataZoneProject,       Value: !Ref
datazoneEnvironmentProjectId }
        - { Key: AmazonDataZoneEnvironment,   Value: !Ref
datazoneEnvironmentEnvironmentId }
        - { Key: AmazonDataZoneStage,         Value: prod }
        - { Key: AmazonDataZoneScopeName,     Value: !Ref datazoneScopeName }
```

```
        - { Key: ProjectS3Path,              Value: !Sub 's3://${ProjectBucket}/
${datazoneScopeName}' }

  SageMakerSubscriptionTarget:
    Type: AWS::DataZone::SubscriptionTarget
    Properties:
      Name: 'Tooling-default-target'
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      Type: BaseSubscriptionTargetType
      Provider: Amazon SageMaker
      ApplicableAssetTypes:
        - SageMakerFeatureGroupAssetType
        - SageMakerModelPackageGroupAssetType
      AuthorizedPrincipals:
        - !GetAtt ProjectUserRole.Arn
      SubscriptionTargetConfig: []

  SageMakerDataSource:
    Type: AWS::DataZone::DataSource
    Properties:
      Name: 'Tooling-default-sagemaker-modelpackagegroup-datasource'
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      ConnectionIdentifier: !GetAtt DefaultIAMConnection.ConnectionId
      Type: SAGEMAKER
      EnableSetting: ENABLED
      PublishOnImport: false
      Schedule:
        Schedule: 'cron(minute hour * * ? *)'
      Recommendation:
        EnableBusinessNameGeneration: false
      Configuration:
        SageMakerRunConfiguration:
          TrackingAssets:
            SageMakerModelPackageGroupAssetType: []

Outputs:
  SageMakerSpacesDomain:
    Value: !GetAtt SageMakerSpacesDefaultDomain.DomainId
    Export:
      Name: !Sub 'SageMakerSpacesDomain-${datazoneEnvironmentEnvironmentId}-
${datazoneScopeName}'
  SageMakerDomainId:
```

```
    Value: !GetAtt SageMakerSpacesDefaultDomain.DomainId
    Export:
      Name: !Sub 'sageMakerDomainId-${datazoneEnvironmentEnvironmentId}-
${datazoneScopeName}'
```

Trusted identity propagation

Declares the connections that support trusted identity propagation, and whether the project enables user background sessions. For more information, see Trusted identity propagation.

IAM-based domain

Trusted identity propagation requires an IAM Identity Center instance attached to your Amazon SageMaker Unified Studio domain.

Identity Center-based domain

```
Parameters:
  enableTrustedIdentityPropagation:
    Type: String
    Default: 'false'
    AllowedValues: ['true', 'false']
  enableUserBackgroundSessions:
    Type: String
    Default: 'false'
    AllowedValues: ['true', 'false']

Resources:
  AthenaConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: project.athena
      Description: Default connection to Amazon Athena SQL for interactive queries
 on your data.
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      EnableTrustedIdentityPropagation: !Ref enableTrustedIdentityPropagation
      Props:
```

```
        AthenaProperties:
          WorkgroupName: !Ref AthenaWorkGroup

  DefaultCatalogConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: project.default_lakehouse
      Description: This is the default connection to interact with project
 Lakehouse.
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      EnableTrustedIdentityPropagation: !Ref enableTrustedIdentityPropagation
      Props:
        LakehouseProperties:

  SparkGlueCompatibilityConnection:
    Type: AWS::DataZone::Connection
    Properties:
      Name: project.spark.compatibility
      Description: Glue-ETL compute with Permission Mode set to compatibility.
 (Auto-created by project).
      DomainIdentifier: !Ref datazoneEnvironmentDomainId
      EnvironmentIdentifier: !Ref datazoneEnvironmentEnvironmentId
      ProjectIdentifier: !Ref datazoneEnvironmentProjectId
      AwsLocation:
        AwsAccountId: !Ref AWS::AccountId
        AwsRegion: !Ref AWS::Region
        IamConnectionId: !GetAtt DefaultIAMConnection.ConnectionId
      EnableTrustedIdentityPropagation: !Ref enableTrustedIdentityPropagation
      Props:
        SparkGlueProperties:
          GlueConnectionName: !Ref ProjectGlueNetworkConnection
          GlueVersion: '5.0'
          IdleTimeout: 60
          NumberOfWorkers: 10
          WorkerType: G.1X

Outputs:
  EnableTrustedIdentityPropagationPermissions:
```

```
    Value: !Ref enableTrustedIdentityPropagation
    Export:
      Name: !Sub 'enableTrustedIdentityPropagationPermissions-
${datazoneEnvironmentProjectId}-${datazoneScopeName}'
  EnableUserBackgroundSessions:
    Value: !Ref enableUserBackgroundSessions
    Export:
      Name: !Sub 'enableUserBackgroundSessions-${datazoneEnvironmentProjectId}-
${datazoneScopeName}'
```

Compatibility with managed blueprints

In Amazon SageMaker Unified Studio, service-managed blueprints provide a wide variety of resource provisioning capabilities, such as Amazon EMR and Amazon Redshift Serverless. For more information, see Supported blueprints. Service-managed blueprints require metadata populated by AWS CloudFormation exports from the project's Tooling environment. When you use a custom blueprint categorized as `TOOLING` in a project with a service-managed blueprint, ensure that your custom blueprint contains the following AWS CloudFormation exports.

IAM-based domain

```
Parameters:
  sagemakerUnifiedStudioNetworkSecurityGroupId: { Type: String, Default: '' }
  sagemakerUnifiedStudioNetworkSubnets:         { Type: String, Default: '' }
  sagemakerUnifiedStudioNetworkVpcId:           { Type: String, Default: '' }

Outputs:
  KmsKeyArn:
    Condition: kmsKeyArnExist
    Value: !Ref sagemakerUnifiedStudioKmsKeyArn
    Export: { Name: !Sub 'kmsKeyArn-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
  PrivateSubnets:
    Value: !Ref sagemakerUnifiedStudioNetworkSubnets
    Export: { Name: !Sub 'privateSubnets-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
  SecurityGroup:
    Value: !Ref sagemakerUnifiedStudioNetworkSecurityGroupId
    Export: { Name: !Sub 'securityGroup-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
  VpcId:
```

```
    Value: !Ref sagemakerUnifiedStudioNetworkVpcId
    Export: { Name: !Sub 'vpcId-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
```

Identity Center-based domain

```
Parameters:
  sagemakerUnifiedStudioNetworkSecurityGroupId: { Type: String, Default: '' }
  sagemakerUnifiedStudioNetworkSubnets:         { Type: String, Default: '' }

Outputs:
  KmsKeyArn:
    Condition: kmsKeyArnExist
    Value: !Ref sagemakerUnifiedStudioKmsKeyArn
    Export: { Name: !Sub 'kmsKeyArn-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
  LogGroupName:
    Value: !Ref ToolingLogGroup
    Export: { Name: !Sub 'logGroupName-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
  PrivateSubnets:
    Value: !Ref sagemakerUnifiedStudioNetworkSubnets
    Export: { Name: !Sub 'privateSubnets-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
  SecurityGroup:
    Value: !Ref sagemakerUnifiedStudioNetworkSecurityGroupId
    Export: { Name: !Sub 'securityGroup-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
  VpcId:
    Value: !Ref sagemakerUnifiedStudioNetworkVpcId
    Export: { Name: !Sub 'vpcId-${datazoneEnvironmentProjectId}-
${datazoneScopeName}' }
```

Enable Tooling blueprint

Before you can create projects with compute capabilities, you must enable the Tooling blueprint and configure its provisioning settings. The Tooling blueprint provisions IAM roles, security groups, and an Amazon SageMaker Unified Studio domain for each project.

This section enables the managed Tooling blueprint in the console. For more information, see Tooling blueprints in Amazon SageMaker Unified Studio. For more information about using your own template as a project's Tooling environment instead, see Custom blueprints as Tooling.

To enable the Tooling blueprint, complete the following steps.

Before you begin, verify that you have the following:

- Domain administrator access to the Amazon SageMaker Unified Studio domain
- An AWS account with permissions to create IAM roles and manage resources

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose the domain's name from the list. The name is a hyperlink.
3. On the domain's details page, navigate to the **Blueprints** tab.
4. In the Tooling blueprint section, choose **Enable** and then specify the following configurations:
   - **Provisioning role** — Amazon SageMaker Unified Studio uses this role to provision and manage resources defined in the selected blueprints in your account. Amazon SageMaker Unified Studio can auto-create this role or you can provide your own.
   - **Manage access role** — This role grants Amazon SageMaker Unified Studio permissions to publish, grant access, and revoke access to Amazon SageMaker Lakehouse, AWS Glue Data Catalog, and Amazon Redshift data. It also grants Amazon SageMaker Unified Studio permissions to publish and manage subscriptions on Amazon SageMaker Catalog data and AI assets.
   - **Query execution role** — This role is used while running a query execution. AWS Lake Formation assumes this role to vend credentials needed by Amazon Athena during query execution.
   - **Amazon S3 bucket for projects** — Amazon SageMaker Unified Studio requires an S3 bucket in your AWS account for storing project artifacts and data.
   - **Virtual private cloud (VPC)** — Select a VPC configured for use with Amazon SageMaker Unified Studio. For more information, see *VPC networking*.
   - **Data encryption** — This setting is optional. By default, your data is encrypted with an AWS managed key. To choose a different key, customize your encryption settings.

- **User role policy** — This is an optional advanced configuration. Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, AI, and ML actions. You can attach your own AWS IAM policies to the role rather than using the default system-managed policy. The IAM policy must include all necessary permissions required for the service to function properly.
- **Authorized domain units** — Domain units where projects can access resources defined by the blueprints.

5. After you specify all configuration settings, choose **Enable blueprint**.

After you enable the Tooling blueprint, you can create projects that use compute capabilities. To configure blueprint parameters such as idle timeout settings and permissions boundaries, see the section called “Manage Tooling blueprint parameters”.

Manage Tooling blueprint parameters

The Tooling blueprint provisions infrastructure for each project, including IAM roles, security groups, and an Amazon SageMaker Unified Studio domain. You can customize the blueprint's behavior by modifying its parameters, such as idle timeout settings, EBS volume sizes, network isolation, and permissions boundaries. Changes to blueprint parameters apply to all new projects created under the blueprint.

These parameters belong to the managed Tooling blueprint. A custom blueprint used as Tooling takes its values from reserved parameters and from the project profile instead.

This topic covers the following tasks:

- Configure Tooling blueprint parameters through the console
- Configure IAM permissions boundaries for roles created by the Tooling blueprint

Configure Tooling blueprint parameters

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose the domain's name from the list. The name is a hyperlink.
3. On the domain's details page, navigate to the **Project profiles** tab.

4. In the **Project profiles** tab, choose a project profile, for example, **All capabilities**. The name of the project profile is a hyperlink.
5. On the project profile details page, choose **Tooling configuration**.
6. In the **Blueprint parameters** section, review the parameter values used during project creation.
7. To modify a parameter, choose **Edit** on the **Tooling configuration** tab.
8. Select the radio button next to the parameter you want to modify, then choose **Edit**.
9. In the **Edit blueprint parameter** dialog, update the value. Select **Editable** if you want the value to be configurable during project creation. Choose **Save**.

The following parameters are available for the Tooling blueprint:

- `minIdleTimeoutInMinutes` — The minimum time (in minutes) that Amazon SageMaker waits after the application becomes idle before shutting down the user's space.
- `maxEbsVolumeSize` — The maximum EBS storage volume size (in GB) for the user's private spaces.
- `idleTimeoutInMinutes` — The time (in minutes) that Amazon SageMaker waits after the application becomes idle before shutting down the user's space.
- `enableNetworkIsolation` — Enables network isolation for training and deployed inference containers.
- `lifecycleManagement` — Indicates whether idle shutdown is activated for this project's Amazon SageMaker Unified Studio domain.
- `sagemakerDomainNetworkType` — The network type for this project's Amazon SageMaker Unified Studio domain.
- `maxIdleTimeoutInMinutes` — The maximum time (in minutes) that Amazon SageMaker waits after the application becomes idle before shutting down this project's Amazon SageMaker Unified Studio domain.
- `allowConnectionToUserGovernedEmrClusters` — Allows connection creation to existing user-governed EMR clusters.
- `enableSpaces` — Enables creation of private compute spaces for development tools.
- `enableProjectRepositoryAutoSync` — Synchronizes your Git repository code artifacts to your project's S3 bucket at `s3://{bucket}/{domain_id}/{project_id}/sys/code/dev/{repository_id}/{branch}/`. Synchronization is triggered by Git push events.

> **Note**
>
> Enabling `maxEbsVolumeSize`, `enableSpaces`, or `enableProjectRepositoryAutoSync` parameters might result in incurring additional costs. For more information, see Amazon SageMaker pricing.

Configure IAM permissions boundaries

Amazon SageMaker Unified Studio supports custom permissions boundaries for IAM roles created by the Tooling blueprint. Organizations that enforce Service Control Policies requiring permissions boundaries on all IAM roles can configure a permission boundary on the Tooling blueprint.

When configured, the service attaches the boundary to all IAM roles provisioned by the Tooling blueprint during project creation, including the `datazone_usr_role`, `AmazonBedrockServiceRole`, and `AmazonBedrockLambdaExecutionRole`. To learn more about permission boundaries, see Permissions boundaries for IAM entities in the *AWS Identity and Access Management User Guide*.

You set the permissions boundary at the blueprint configuration level using the `PermissionsBoundaryArn` regional parameter. When a user creates a new project that includes the Tooling blueprint, the CloudFormation stack creates IAM roles with the specified boundary attached. Because you set the boundary at the blueprint level, it applies to every project created under that blueprint.

Before you configure a permissions boundary, verify that you have the following:

- An Identity Center-based domain with the Tooling blueprint enabled
- AWS CLI configured with permissions to manage domain configurations
- An existing IAM managed policy to use as the permissions boundary

To configure a permissions boundary on the Tooling blueprint

1. Retrieve your domain ID by running the following command:

```
aws datazone list-domains \
    --region region \
    --query "items[?name=='domain-name'].id | [0]" \
```

```
    --output text
```

2. Retrieve the Tooling blueprint ID by running the following command:

```
aws datazone list-environment-blueprints \
    --domain-identifier domain-id \
    --managed \
    --region region \
    --query "items[?name=='Tooling'].id | [0]" \
    --output text
```

3. Retrieve the current blueprint configuration by running the following command:

```
aws datazone get-environment-blueprint-configuration \
    --domain-identifier domain-id \
    --environment-blueprint-identifier tooling-bp-id \
    --region region
```

Record the following values from the output. You need these values in the next step:

- `provisioningRoleArn`
- `manageAccessRoleArn`
- `enabledRegions`
- All fields inside `regionalParameters`

4. Update the blueprint configuration to include `PermissionsBoundaryArn` in the regional parameters by running the following command:

```
aws datazone put-environment-blueprint-configuration \
    --domain-identifier domain-id \
    --environment-blueprint-identifier tooling-bp-id \
    --enabled-regions 'enabledRegions' \
    --provisioning-role-arn "provisioningRoleArn" \
    --manage-access-role-arn "manageAccessRoleArn" \
    --regional-parameters '{
        "region": {
            "AZs": "AZs",
            "S3Location": "S3Location",
            "Subnets": "Subnets",
            "VpcId": "VpcId",
            "PermissionsBoundaryArn": "arn:aws:iam::account-id:policy/policy-name"
        }
```

```
    }' \
    --region region
```

> **Important**
>
> The `put-environment-blueprint-configuration` API operates in overwrite mode. It replaces the entire configuration. You must include all existing values from the preceding step. The only new field is `PermissionsBoundaryArn`. Omitting any existing parameter removes it.

5. Verify the configuration by running the following command:

```
aws datazone get-environment-blueprint-configuration \
    --domain-identifier domain-id \
    --environment-blueprint-identifier tooling-bp-id \
    --region region \
    --query "regionalParameters.\"region\".PermissionsBoundaryArn"
```

> **Important considerations**
>
> - The permissions boundary only affects new projects. Existing projects retain their original configuration.
> - The boundary applies to all three IAM roles created by the Tooling blueprint. You cannot selectively apply it to individual roles.
> - The IAM policy referenced by `PermissionsBoundaryArn` must exist in the account before project creation. If the policy is deleted or the ARN is invalid, provisioning fails.
> - To remove the boundary from future projects, run `put-environment-blueprint-configuration` again without the `PermissionsBoundaryArn` parameter.

Modify the OnDemandWorkflows blueprint for creating workflow environments in a shared VPC

In order to support creating workflow environments in a shared VPC setup, where the VPC is in one AWS account and the project and the Amazon Managed Workflows for Apache Airflow (Amazon

MWAA) environment are in another AWS account, the domain administrator must complete the following procedure to modify the endpointManagement parameter of the OnDemand Workflows blueprint.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose the domain's name from the list. The name is a hyperlink.
3. On the domain's details page, navigate to the **Project profiles** tab.
4. In the **Project profiles** tab, choose a project profile, for example, **All capabilities**. The name of the project profile is a hyperlink.
5. On the project profile details page, choose **OnDemand Workflows** blueprint.
6. In the **OnDemand Workflows** details page, choose **Edit**.
7. In the **Blueprint parameters** section, choose **endpointManagement** and then choose **Edit**.
8. In the **Edit blueprint parameter** pop up window, choose **Customer** in the **Value** drop-down.

   This value defines whether the VPC endpoints configured for the environment are created and managed by the customer or by Amazon MWAA. If **Value** is set to **SERVICE**, Amazon MWAA creates and manages the required VPC endpoints in your VPC. If **Value** is set to **CUSTOMER**, you must create and manage the VPC endpoints for your VPC. If you choose to create an environment in a shared VPC, you must set this value to **CUSTOMER**.

The domain users can then create workflow environments and the domain administrators then can follow the steps and procedures described here to automate deployment of Amazon Amazon MWAA environments using customer-managed endpoints in a VPC.

Account pools in Amazon SageMaker Unified Studio

In Amazon SageMaker Unified Studio, you can configure your domain to create project profiles where an account pool provides AWS account and AWS Region information. An account pool is a list of authorized associated accounts and regions. This allows you to create project profiles that can be used to create projects across multiple accounts and regions, while controlling which accounts and regions are available for use.

There are two ways to create project profiles with account pools that you configure for validation of authorized accounts at the time of project creation.

- Static list of account and region pairs
- Custom Lambda handler to authorize account and region pair information

The custom handler accesses customer information and then dynamically generates a list of authorized associated account and region pairs based on a set of rules in the Lambda function. Amazon SageMaker Unified Studio then resolves the list of account and region pairs in the account pool at project creation time.

For more information about associated accounts in Amazon SageMaker Unified Studio, see Associated accounts in Amazon SageMaker Unified Studio.

Topics

- Considerations
- Use cases
- Create an account pool
- View an account pool
- List account pools for a domain
- View the list of accounts in an account pool
- Delete an account pool
- Create a project profile with an account pool

Considerations

The following considerations apply for account pools in Amazon SageMaker Unified Studio.

- Account pools contain a list of accounts where each account has an associated region.
- You can have up to 100 account pools per domain. For details, see Quotas and limits for Amazon SageMaker Unified Studio.
- Account pools are not supported by Amazon Datazone domains.
- You can configure custom project profiles to use account pools using either the console or the CLI. Steps for the creation, update, and deletion of account pools are only supported in the AWS CLI.

For more information about creating a custom project profile with an account pool, see Project profiles in Amazon SageMaker Unified Studio.

Use cases

Account pools allow administrators to perform the following tasks.

- Create project profiles that are agnostic of AWS account and AWS Region information.
- Define a subset of associated account and region pairs that the profile can use (compared with specifying all accounts)

Create an account pool

To use the AWS CLI to create an account pool, you run the **create-account-pool** command and provide the source.

- **For Lambda handler sources**: Provide the Lambda function and an IAM role with permissions to invoke the lambda, and trusts the `datazone.amazonaws.com` service principal.
- **For static account sources**: Provide a list of account and region pairs as key-value pairs in the command.

Once configured in your domain, account pools automatically provide account and region information when creating new projects.

Topics

- Create an account pool with a custom handler source
- Create an account pool with a static list of account and region pairs

Create an account pool with a custom handler source

You can create an account pool where the account authentication is provided by a custom Lambda handler. Use these steps to create a sample custom handler and provide it when creating the account pool.

To create example custom Lambda handler

- Create a function in Lambda that provides authorization for Amazon SageMaker Unified Studio to use when authenticating accounts for the account pool.

  The following example provides sample handler code for a python function.

```
import json

def lambda_handler(event, context):
    print(f'Received Event {event}')
    if event['operationRequest']['listAuthorizedAccountsRequest'] is not None:
        print("ListAuthorizedAccountsRequest Received...")
        return list_authorized_accounts()
    elif event['operationRequest']['validateAccountAuthorizationRequest'] is not
 None:
        print("ValidateAccountAuthorizationRequest Received...")
        return validate_account_authorization()
    else:
        raise Exception(f'Operation type {operation_type} not supported')

def list_authorized_accounts():
    account1 = {"awsAccountId": "111122223333", "awsAccountName": "Acct1",
 "supportedRegions": ["us-east-1", "us-west-2", "eu-west-1"]}
    account2 = {"awsAccountId": "892325846722", "awsAccountName": "Acct2",
 "supportedRegions": ["us-east-1", "us-west-2", "us-east-2"]}
    return {
        'operationResponse': {
            'listAuthorizedAccountsResponse': {
                'items': [account1, account2]
            }
        }
    }

def validate_account_authorization():
    return {
        'operationResponse': {
```

```
            'validateAccountAuthorizationResponse': {
                'authResult': 'GRANT'
            }
        }
    }
```

After you create your account pool, you can create a project in your domain that uses the account pool. For more information about associated accounts, see Associated accounts in Amazon SageMaker Unified Studio.

To create an account pool with a custom handler source (CLI)

- Open a terminal (Linux, macOS, or Unix) or command prompt (Windows) and use the AWS CLI to run the `create-account-pool` command with the following format, where the following are required arguments:
  - `--domain-identifier` - the domain ID in SageMaker Unified Studio
  - `--name` - the account pool name
  - `--account-source` - the method for providing account information (custom handler or static list)
  - `--resolution-strategy` - the manual option is shown in this example

  domain ID, account pool name, and the Lambda handler ARN and IAM role ARN are required arguments.

```
aws datazone create-account-pool --domain-identifier DOMAIN_ID --
name ACCOUNT_POOL_ID --resolution-strategy MANUAL --account-source <source>
```

  Example command:

```
aws datazone create-account-pool --domain-identifier dzd_dkqsou2EXAMPLE
 --name my-accountpool --resolution-strategy MANUAL --account-source
 '{"customAccountPoolHandler": {"lambdaFunctionArn": "arn:aws:lambda:us-
east-1:111122223333:function:MyAccountPoolResolver", "lambdaExecutionRoleArn":
 "arn:aws:iam::111122223333:role/AccountResolutionRole"}}'
```

  This command returns output with the account pool details.

```
{
    "domainId": "dzd_dkqsou2EXAMPLE",
    "name": "my-accountpool",
    "id": "cln5qjqEXAMPLE",
    "resolutionStrategy": "MANUAL",
    "accountSource": {
        "customAccountPoolHandler": {
            "lambdaFunctionArn": "arn:aws:lambda:us-
east-1:111122223333:function:MyAccountPoolResolver",
            "lambdaExecutionRoleArn": "arn:aws:iam::111122223333:role/
AccountResolutionRole"
        }
    },
    "createdAt": "2025-08-12T00:26:27.017118+00:00",
    "lastUpdatedAt": "2025-08-12T00:26:27.017118+00:00",
    "domainUnitId": "4njnngous3oyw7"
}
```

Create an account pool with a static list of account and region pairs

You can create an account pool where the accounts are provided as a list of static accounts. Use these steps when your account pool source is a static list and not provided by the custom Lambda function.

- Open a terminal (Linux, macOS, or Unix) or command prompt (Windows) and use the AWS CLI to run the `get-account-pool` command with the following format, where the domain ID, account pool name, and source of accounts are required arguments.

  ```
  aws datazone create-account-pool --domain-identifier DOMAIN_ID --
  name ACCOUNT_POOL_ID --resolution-strategy MANUAL --account-source <source>
  ```

  Example command:

  ```
  aws datazone create-account-pool --domain-identifier dzd_dkqsou2EXAMPLE --name
   my-accountpool --resolution-strategy MANUAL --account-source '{"accounts":
   [{"awsAccountId": "111122223333", "supportedRegions": ["us-east-1"],
   "awsAccountName": "ExampleAccount"}]}'
  ```

  This command returns output with the account pool details.

```
{
    "domainId": "dzd_dkqsou2EXAMPLE",
    "name": "my-accountpool",
    "id": "cln5qjqEXAMPLE",
    "resolutionStrategy": "MANUAL",
    "accountSource": {
        "accounts": [
            {
                "awsAccountId": "111122223333",
                "supportedRegions": [
                    "us-east-1"
                ],
                "awsAccountName": "ExampleAccount"
            }
        ]
    },
    "createdAt": "2025-08-08T00:34:48.946606+00:00",
    "lastUpdatedAt": "2025-08-08T00:34:48.946606+00:00",
    "domainUnitId": "4njnngous3oyw7"
}
```

View an account pool

To use the AWS CLI to view the accounts in an account pool, use the `get-account-pool` command.

- Open a terminal (Linux, macOS, or Unix) or command prompt (Windows) and use the AWS CLI to run the `get-account-pool` command with the following format, where the domain ID and account pool ID are required arguments.

  ```
  aws datazone get-account-pool --domain-identifier DOMAIN_ID --
  identifier ACCOUNT_POOL_ID
  ```

  Example command:

  ```
  aws datazone get-account-pool --domain-identifier dzd_dkqsou2EXAMPLE --
  identifier cln5qjqEXAMPLE
  ```

  This command returns output with the account pool details.

```
{
    "domainId": "dzd_dkqsou2EXAMPLE",
    "name": "my-accountpool",
    "id": "cln5qjqEXAMPLE",
    "resolutionStrategy": "MANUAL",
    "accountSource": {
        "accounts": [
            {
                "awsAccountId": "111122223333",
                "supportedRegions": [
                    "us-east-1"
                ],
                "awsAccountName": "ExampleAccount"
            }
        ]
    },
    "createdBy": "",
    "createdAt": "2025-08-08T00:34:48.946606+00:00",
    "lastUpdatedAt": "2025-08-08T00:34:48.946606+00:00",
    "updatedBy": "",
    "domainUnitId": "4njnngous3oyw7"
}
```

List account pools for a domain

To use the AWS CLI to view the account pools in a domain, use the `list-account-pools` command.

- Open a terminal (Linux, macOS, or Unix) or command prompt (Windows) and use the AWS CLI to run the `list-account-pools` command with the following format, where the domain ID is a required argument.

  ```
  aws datazone list-account-pools --domain-identifier DOMAIN_ID
  ```

  Example command:

  ```
  aws datazone list-account-pools --domain-identifier dzd_dkqsou2EXAMPLE
  ```

  This command returns output with the account pool details.

```
{
    "items": [
        {
            "domainId": "dzd_dkqsou2EXAMPLE",
            "id": "5htvndro7wd89z",
            "name": "my-accountpool",
            "resolutionStrategy": "MANUAL",
            "domainUnitId": "4njnngous3oyw7",
            "createdBy": "",
            "updatedBy": ""
        }
    ]
}
```

View the list of accounts in an account pool

To use the AWS CLI to view the accounts in an account pool where the source is a list of static accounts, use the `list-accounts-in-account-pool` command.

- Open a terminal (Linux, macOS, or Unix) or command prompt (Windows) and use the AWS CLI to run the `list-accounts-in-account-pool` command with the following format, where the domain ID is a required argument.

  ```
  aws datazone list-accounts-in-account-pool --domain-identifier DOMAIN_ID --
  identifier ACCOUNT_POOL_ID
  ```

  Example command:

  ```
  aws datazone list-accounts-in-account-pool --domain-identifier dzd_dkqsou2EXAMPLE
   --identifier cln5qjqEXAMPLE
  ```

  This command returns output with the account pool account list details.

  ```
  {
      "items": [
          {
              "awsAccountId": "111122223333",
              "supportedRegions": [
  ```

```
                "us-east-1"
            ],
            "awsAccountName": "ExampleAccount"
        }
    ]
}
```

Delete an account pool

To use the AWS CLI to delete an account pool, use the `delete-account-pool` command.

> **Important**
>
> This operation will delete the account pool for the domain. This operation cannot be undone.

- Open a terminal (Linux, macOS, or Unix) or command prompt (Windows) and use the AWS CLI to run the `delete-account-pool` command with the following format, where the domain ID and account pool ID are required arguments.

  ```
  aws datazone delete-account-pool --domain-identifier DOMAIN_ID --
  identifier ACCOUNT_POOL_ID
  ```

  Example command:

  ```
  aws datazone delete-account-pool --domain-identifier dzd_dkqsou2EXAMPLE --
  identifier 5htvndro7wd89z
  ```

  This command performs the deletion and does not return any output.

Create a project profile with an account pool

You can create a project profile that has your account pool associated such that you can choose accounts and regions from it when creating a project with the profile.

Use the console or the CLI to set up your account pool-associated project profile.

Create a project profile with an account pool (Console)

To configure a custom project profile using the console, see the steps in Custom project profile.

Create a project profile with an account pool (CLI)

Use the `create-project-profile` command to set up your account pool-associated project profile.

- Open a terminal (Linux, macOS, or Unix) or command prompt (Windows) and use the AWS CLI to run the `create-project-profile` command with the following format, where the domain ID and name of the project profile are required arguments, along with the environment configuration for blueprints, which is provided as JSON with account pool details. The status is disabled by default, so the following command also enables the environment configuration.

```
aws datazone create-project-profile --domain-identifier DOMAIN_ID
 --name PROFILE_NAME --status ENABLED --environment-configuration
 <environment_configuration>
```

Example command:

```
aws datazone create-project-profile --domain-identifier dzd_dkqsou2EXAMPLE --
name NAME --status ENABLED --environment-configuration '[{"name": "Tooling",
 "environmentBlueprintId": "4son14jdv5dq7b", "deploymentOrder": 0, "accountPools":
 ["cln5qjqEXAMPLE"]}, {"name": "DataLake", "environmentBlueprintId":
 "BLUEPRINT_ID", "accountPools": ["cln5qjqEXAMPLE"]}]'
```

This command returns output with the project profile details.

```
{
    "domainId": "dzd_dkqsou2EXAMPLE",
    "id": "aipopwr7db0rzb",
    "name": "NAME",
    "status": "ENABLED",
    "allowCustomProjectResourceTags": false,
    "environmentConfigurations": [
        {
            "name": "Tooling",
            "id": "948f994d-ed81-496a-8e1f-2f0e1288dcec",
```

```
            "environmentBlueprintId": "4son14jdv5dq7b",
            "deploymentMode": "ON_CREATE",
            "accountPools": [
                "cln5qjqEXAMPLE"
            ],
            "deploymentOrder": 0
        },
        {
            "name": "DataLake",
            "id": "3210351a-111c-476b-a66d-64d88a99a567",
            "environmentBlueprintId": "BLUEPRINT_ID",
            "deploymentMode": "ON_CREATE",
            "accountPools": [
                "cln5qjqEXAMPLE"
            ]
        }
    ],
    "createdAt": "2025-08-08T00:57:39.358016+00:00",
    "lastUpdatedAt": "2025-08-08T00:57:39.358016+00:00",
    "domainUnitId": "4njnngous3oyw7"
}
```

Onboarding data in Amazon SageMaker Unified Studio

Amazon SageMaker Unified Studio supports the following key capabilities for Amazon SageMaker Lakehouse data management and governance.

- Automated onboarding of Amazon SageMaker Lakehouse: you can automatically ingest the metadata of all datasets in your Amazon SageMaker Lakehouse into the catalog. This removes the need for manually granting permissions, creating metadata ingestion jobs, or configuring scripts. By onboarding assets in a single step, administrators can immediately make this data discoverable and ready for governance, analysis, and collaboration within Amazon SageMaker Unified Studio.
- Continuous real-time metadata ingestion: After onboarding existing Amazon SageMaker datasets, the catalog continuously keeps metadata current via real-time streaming. Any changes, such as new tables or schema updates, are automatically reflected in the catalog. This eliminates the need for periodic ingestion jobs, reduces stale metadata risk, and lowers your operational costs while ensuring your teams have access to the freshest metadata.
- Continuous Real-time data quality sync: After onboarding existing Amazon SageMaker datasets, the catalog continuously keeps data quality results current via real-time streaming. Metrics such as completeness, timeliness, and accuracy are automatically synchronized, enabling data consumers to visualize quality scores and track changes over time. This eliminates manual dataSourceRuns and ensures immediate visibility into data health status.
- Direct sharing: data owners can now proactively grant access to their assets without waiting for data access requests. This enables smoother cross-team collaboration, helping accelerate projects and reduce handoffs while maintaining strong governance.

You can onboard your Amazon SageMaker Lakehouse data as part of creating a new Amazon SageMaker unified domain or for an existing domain.

- If you create your new domain using the quick set up option, data onboarding is supported as part of domain creation. For more information, see Create a Amazon SageMaker Unified Studio domain - quick setup.
- If you create your new domain using the manual setup option, once the domain is created you must first enable the Tooling blueprint before you can onboard your data. To do this, complete the steps in Enable or disable blueprints (choose the Tooling blueprint in the **Blueprints** tab). You can also get to the **Enable Tooling** blueprint page by first navigating to the **Onboarded data**

tab, then attempting to onboard your data by choosing **Onboard data**. This displays the **Tooling blueprint not enabled** notification and the **Enable Tooling** button opens the **Enable Tooling** page where you can complete this task.

To onboard your data in an existing Amazon SageMaker unified domain, complete the following procedure.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and choose the domain's name from the list. The name is a hyperlink.
3. On the domain's details page, navigate to the **Onboarded data** tab and choose **Onboard data**.
4. On the **Onboard your data** page, do the following and then choose **Onboard data**.
   - Check the AWS Glue (SageMaker Lakehouse) checkbox.
   - Optional - check the **Make your data discoverable** checkbox - other users in the domain will be able to find your data in the catalog. This setting can only be reverted later in Amazon SageMaker Unified Studio by un-publishing each dataset individually.
   - Under **Permissions and resources**, specify the provisioning role. Amazon SageMaker Unified Studio uses this role to provision and manage resources required to onboard the account data.
   - Under **Owning project** specify the owning project. Your data will be accessible in this project that is auto-created in Amazon SageMaker Unified Studio. Once created, you cannot rename the project.
   - Under **Add project owner**, add the project owner for the owning project.

Generative AI assistance in Amazon SageMaker Unified Studio

Amazon SageMaker Unified Studio provides generative AI assistance through Amazon Q and the SageMaker Data Agent. Amazon Q provides conversational AI chat and command line tools in JupyterLab and Code Editor. The SageMaker Data Agent provides intelligent assistance for code generation, error diagnosis, and data analysis recommendations in Notebooks and Query Editor.

Amazon Q

In the current release of Amazon SageMaker Unified Studio, by default, all users of an Amazon SageMaker unified domain have access to the Free Tier release of Amazon Q.

Disable Amazon Q

To disable Amazon Q in your domain, you must update your permissions to use deny statements and update your domain level configuration. Complete the following steps:

1. Update your permissions in the AWS policy: SageMakerStudioDomainExecutionRolePolicy to Deny "q:*".

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "q:*",
                "glue:StartCompletion",
                "glue:GetCompletion"
            ],
            "Resource": "*"
        }
    ]
}
```

2. Update your permissions in the AWS policy: SageMakerStudioProjectUserRolePolicy to Deny "q:*". The following policy statement denies the required actions:

```
{
        "Sid": "AmazonQChatPermissions",
        "Effect": "Deny",
        "Action": [
            "q:*",
            "glue:StartCompletion",
           "glue:GetCompletion",
           "codewhisperer:GenerateRecommendations",
           "sqlworkbench:PutQCustomContext",
           "sqlworkbench:GetQCustomContext",
           "sqlworkbench:DeleteQCustomContext",
           "sqlworkbench:GetQSqlRecommendations",
           "sqlworkbench:GetQSqlPromptQuotas"
        ],
        "Resource": "*"
    },
```

3. Update the Amazon Q parameter value through AWS Systems Manager. Set the following parameters to disable Amazon Q:

```
arn:aws:ssm:<region>:<account-id>:parameter/amazon/datazone/q/<domain-id> to empty
arn:aws:ssm:<region>:<account-id>:parameter/amazon/datazone/q/<domain-id>/q-enabled
 to false
```

SageMaker Data Agent

The SageMaker Data Agent provides intelligent assistance for code generation, error diagnosis, and data analysis recommendations in Notebooks and Query Editor. The SageMaker Data Agent is available in both IAM and IAM Identity Center (IdC) domains.

Disable the SageMaker Data Agent

To disable the SageMaker Data Agent in your domain, use IAM permissions to deny the required API actions. The following IAM policy statement denies the Amazon DataZone API actions that the SageMaker Data Agent requires. Add this statement to your project role policy.

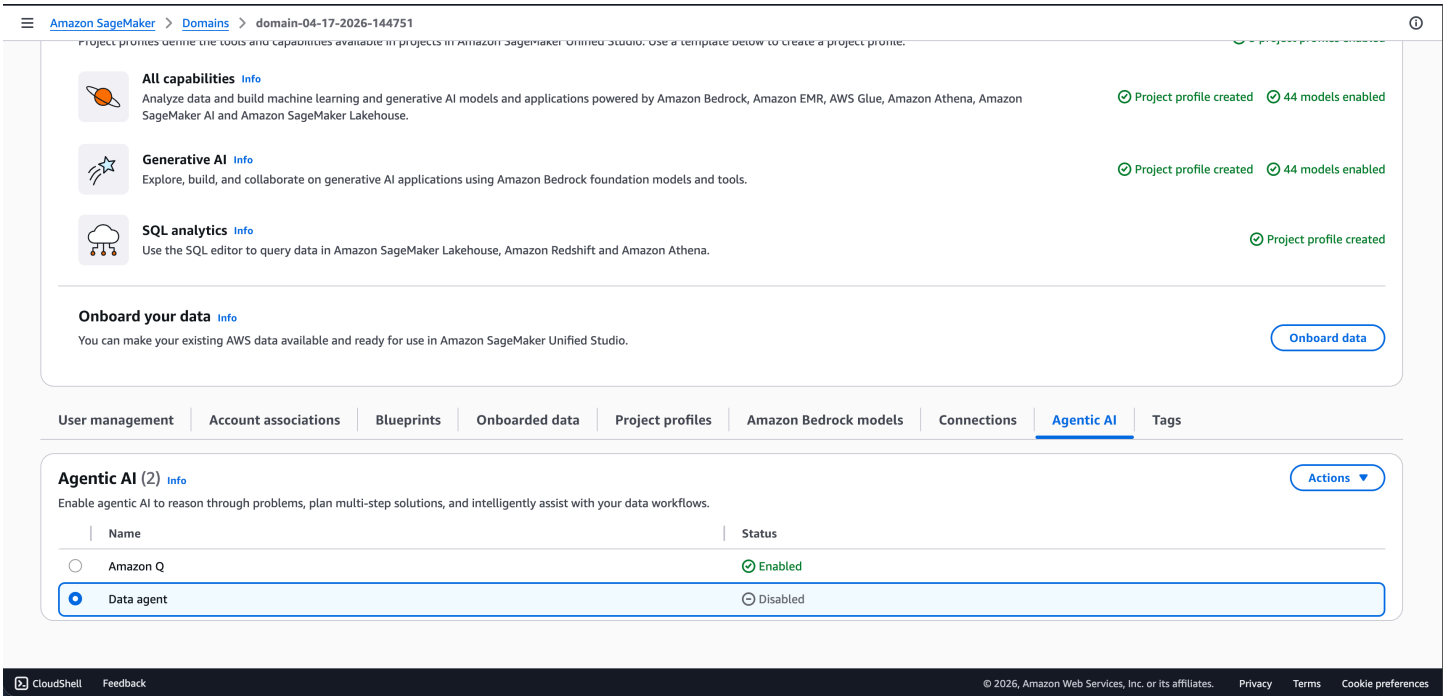
```
{
    "Sid": "SageMakerDataAgentDeny",
    "Effect": "Deny",
    "Action": [
        "datazone:SendMessage",
        "datazone:GenerateCode",
        "datazone:StartConversation",
        "datazone:GetConversation",
        "datazone:ListConversations"
    ],
    "Resource": "*"
}
```

The following list describes the denied actions:

- `datazone:SendMessage` – Prevents sending messages to the SageMaker Data Agent.
- `datazone:GenerateCode` – Prevents the SageMaker Data Agent from generating code suggestions.
- `datazone:StartConversation`, `datazone:GetConversation`, `datazone:ListConversations` – Prevents users from starting, retrieving, or listing SageMaker Data Agent conversations.

In IAM Identity Center (IdC) domains, you can also disable the SageMaker Data Agent through the domain configuration page. This option provides a domain-level control to turn off the SageMaker Data Agent for all users in the domain.

The following image shows the domain configuration option for disabling the SageMaker Data Agent.


Amazon SageMaker > Domains > domain-04-17-2026-144751
All capabilities Info
Analyze data and build machine learning and generative AI models and applications powered by Amazon Bedrock, Amazon EMR, AWS Glue, Amazon Athena, Amazon SageMaker AI and Amazon SageMaker Lakehouse.
Project profile created
44 models enabled
Generative AI Info
Explore, build, and collaborate on generative AI applications using Amazon Bedrock foundation models and tools.
Project profile created
44 models enabled
SQL analytics Info
Use the SQL editor to query data in Amazon SageMaker Lakehouse, Amazon Redshift and Amazon Athena.
Project profile created
Onboard your data Info
You can make your existing AWS data available and ready for use in Amazon SageMaker Unified Studio.
Onboard data
User management
Account associations
Blueprints
Onboarded data
Project profiles
Amazon Bedrock models
Connections
Agentic AI
Tags
Agentic AI (2) Info
Actions
Enable agentic AI to reason through problems, plan multi-step solutions, and intelligently assist with your data workflows.
Name
Status
Amazon Q
Enabled
Data agent
Disabled
CloudShell
Feedback
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Amazon Bedrock in SageMaker Unified Studio

Amazon Bedrock in SageMaker Unified Studio enables you to easily build and scale generative AI applications. Amazon Bedrock in SageMaker Unified Studio provides a web interface that allow users to interact with Amazon Bedrock foundation models and use Amazon Bedrock tools, such as Agents, Guardrails, Prompts, Flows, Evaluation, and Functions in a seamless unified fashion. Users can interact with models in a generative AI playground or collaborate on developing generative AI applications in projects.

Amazon Bedrock in SageMaker Unified Studio can be only used by the members of the Amazon SageMaker unified domains. For more information, see Amazon Bedrock in SageMaker Unified Studio.

In the current release of Amazon SageMaker Unified Studio, there are the following configuration paths available for setting up Amazon Bedrock in SageMaker Unified Studio in your domain, each offering a different level of customization:

- **Quick setup** - you can use this option as part of creating an Amazon SageMaker unified domain. Quick setup option simplifies the process of setting up Amazon Bedrock in SageMaker Unified Studio by automating key steps without requiring user input. When selected during domain creation, the **Quick setup** performs the following:
  - Creates the **Generative AI application development project profile** that the Amazon SageMaker Unified Studio user then uses to create Amazon SageMaker in SageMaker Unified Studio projects.
  - Activates all generative AI blueprints and the default Tooling blueprint needed to provision resources for the Amazon Bedrock capabilities.
  - Configures permissions for all enabled Amazon Bedrock serverless models accessible in the AWS account and Region, enabling their use in the generative AI projects and playgrounds.

  For more informaiton about creating an Amazon SageMaker unified domain with **Quick setup**, see Create a Amazon SageMaker Unified Studio domain - quick setup.
- **Guided setup** - this is the guided setup with a step-by-step walkthrough of configuring Generative AI capabilities for your Amazon SageMaker unified domains. You can use this option only after you've created your Amazon SageMaker unified domain by navigating to the domain details page and using the **Next steps for your domain** section. It pre-populates system-recommended configurations which you can review and modify. Key steps include:

- Creating the **Generative AI application development project profile** - the system generates a project profile specific to the domain's AWS account and Region. This step also automatically enables the generative AI blueprints if they are not already enabled. If the Tooling blueprint is not yet enabled in the domain, the system augments steps to enable it as well.
- Configuring model access - the system identifies all Amazon Bedrock serverless models available in the account and Region, then configures access permissions for these models. You can review the model list and selectively enable models for use in Amazon Bedrock in SageMaker Unified Studio projects and domain playgrounds.

For detailed steps of using the guided setup of Generative AI capabilities for your Amazon SageMaker unified domain, see Configure Amazon Bedrock in SageMaker Unified Studio for your domain.

- **Manual setup** - this is a step-by-step configuration of project profiles, blueprints, and model access with granular control over configurations. You can use this option only after you've created your Amazon SageMaker unified domain by navigating to the domain details page and using the configuration settings under the **Project profiles**, **Blueprints**, and **Amazon Bedrock models** tabs. Manual setup is recommended for advanced scenarios, such as enabling generative AI in a different Region or account from the domain. Manual setup includes:
  - Manually creating custom project profiles
  - Enabling specific blueprints
  - Configuring access to your Amazon Bedrock serverless models for the selected AWS accounts and regions

Once Amazon Bedrock in SageMaker Unified Studio for a domain is set up, you can perform the following procedures to further customize and configure it.

Topics

- Configure access to your Amazon Bedrock serverless models for the selected AWS accounts and regions
- Set default models for the generative AI playgrounds in Amazon SageMaker Unified Studio
- Publishing models from associated accounts

Configure access to your Amazon Bedrock serverless models for the selected AWS accounts and regions

You can configure access to your Amazon Bedrock serverless models for Amazon Bedrock in SageMaker Unified Studio projects and playgrounds by enabling or disabling access in the **Amazon Bedrock models** tab. To configure access, follow these steps:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to manage your Amazon Bedrock serverless models.
3. Choose the **Amazon Bedrock models** tab.
4. Amazon Bedrock in SageMaker Unified Studio uses the Amazon Bedrock to enable model interaction. The in SageMaker Unified Studio allows you to use the model that you have granted access in Amazon Bedrock. An Amazon Bedrock in SageMaker Unified Studio project can only access models from the project's AWS account and AWS Region. A playground can access models from any account and region. On the **Amazon Bedrock models** page, under the **Select account and region** section, choose the AWS account and Region where you want to manage your serverless models.
5. On the **Amazon Bedrock models** page, under the **Models enabled for the selected account and region** section, choose the refresh icon.

   The system queries Amazon Bedrock and displays a list of Amazon Bedrock serverless models to which you have access. If no models are listed or if a specific model is missing, visit the Amazon Bedrock management console for the appropriate account and Region to grant access. If you have updated model access in Amazon Bedrock, choose the refresh icon in the **Amazon Bedrock Models** tab to refresh the updated list of accessible models

   The following are important elements to consider as you review the generated list of models:

   - Every model in the list is prepopulated with certain details, including modality, inference type, whether it's enabled in projects and playground, and roles for model access. A model's modality indicates the type of output data it can generate. Amazon Bedrock in SageMaker Unified Studio supports Amazon Bedrock foundation models with on-demand throughput and on-demand cross-region inference. If a model supports both on-demand and on-

demand cross-region inference, it appears in the list twice with the appropraite value listed in the **Inference** column. You have the flexibility to enable your preferred inference type for use in projects and playgrounds. Amazon Bedrock in SageMaker Unified Studio does NOT support provisioned throughput, custom models, or imported models.

- For easy setup, the system pre-selects accessible models that support on-demand throughput, excluding legacy models, to enable in projects and playground. Review and adjust the list to enable models for projects and playgrounds based on your specific requirements.
- The models that you have not yet enabled for projects and playground access are grayed out in the list. To enable or disable access, choose **Manage** and then use the checkboxes in the **Enable in project** and **Enable in playground** columns. If you choose to disable project access of a model, confirm the disable action in the pop up window that appears.

6. To enable or disable your models in the Amazon SageMaker Unified Studio projects and playgrounds, choose **Manage** and then use the checkboxes in the **Enable in project** and **Enable in playground** columns to enable or disable your models. If you choose to disable a model in a project, confirm the disable action in the pop up window that appears.

Set default models for the generative AI playgrounds in Amazon SageMaker Unified Studio

Amazon Bedrock in SageMaker Unified Studio supports generative AI playgrounds that enable the Amazon SageMaker unified domain users to easily experiment with Amazon Bedrock models. Users can send prompt requests to various models and view the responses. There are two types of playgrounds in the Amazon Bedrock in SageMaker Unified Studio: the chat playground and the image and video playground.

As the administrator of an Amazon SageMaker unified domain, you can complete the following procedure to set default chat and video and image generative AI playgrounds in the Amazon SageMaker Unified Studio for your domain and their respective default models. When users access the playground, the default model is preselected for them to begin interacting.

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to configure the detaul playgrounds and models.

3. Choose the **Amazon Bedrock models** tab.
4. In the **Default models** section, choose **Manage**.
5. On the **Default models - optional** page:
   - For the **Chat playground - optional**, select a default model from the drop-down menu. The drop-down menu includes only the models that support **Text** as the output modality and are enabled for playground use.
   - For the **Image and video playground - optional**, select a default model from the drop-down menu. The drop-down menu will include only the models that support either **Image** or **Video** as the output modality and are enabled for playground use.
   - Choose **Save** to save your choices for the default playgrounds and their respective default models.

Publishing models from associated accounts

Amazon Bedrock models are published to the domain as model assets through the **GenerativeAIModelGovernanceProject** project. This project is is created by Amazon SageMaker Unified Studio automatically and by default, the IAM identity (IAM user or role) who configures Amazon Bedrock in SageMaker Unified Studio for the domain is the owner of this project. If the domain was created via Quick setup, SSO users that were configured during Quick setup are also owners of the **GenerativeAIModelGovernanceProject** project.

If you want to publish models from your associated account, the IAM identity of the associated account must be added to the **GenerativeAIModelGovernanceProject** project. In the current release of Amazon SageMaker Unified Studio, you must complete the following procedure to do this:

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain where you want to add an associated account user to the model governance project.
3. Choose the **Amazon Bedrock models** tab and locate the **Model governance project section**.
4. In the **Model governance project section**, choose **Add IAM users or roles**, then choose **Associated account**, specify the ARN of the user that you want to add from the associated account, then choose **Add**, and then choose **Add user(s)**.

Amazon Quicksight in SageMaker Unified Studio

Enabling Amazon QuickSight integration in Amazon SageMaker Unified Studio allows data consumers to directly visualize and analyze data from the SageMaker Catalog using QuickSight. With QuickSight in Amazon SageMaker Unified Studio, users can access their data and employ the built-in business intelligence visualization capabilities reaching a seamless data analysis workflow.

With this integration, users can go from exploring data in Amazon SageMaker Unified Studio to visualizing it in QuickSight with a single click. Behind the scenes, Amazon SageMaker Unified Studio creates a QuickSight dataset and organizes it in a secured folder accessible only to members within the project. Any dashboards you build in QuickSight stay within this folder and are automatically added as assets to your Amazon SageMaker Unified Studio project, where you can publish them to the SageMaker Catalog. From there, you can share them with users or groups in your corporate directory for broader access—all within Amazon SageMaker Unified Studio. This keeps your dashboards organized, discoverable, shareable, and governed, making cross-team collaboration and asset reuse much easier.

Important

To enable the QuickSight blueprint in an AWS account, you must meet the following required conditions:

- Your Amazon SageMaker unified domain and QuickSight account both must be integrated with AWS IAM Identity Center using the same Identity Center instance.
- Your QuickSight account must exist in the same AWS Account where you are looking to enable the QuickSight blueprint.
- The QuickSight blueprint is available only in Identity Center-based domains. IAM-based domains and projects do not display the **Blueprints** tab.
- If your QuickSight account uses QuickSight-managed users or IAM federation, you cannot switch it to IAM Identity Center in place. You must sign up for a new QuickSight subscription instead. For more information, see Using IAM Identity Center in the *Amazon QuickSight User Guide*.

Enable the QuickSight blueprint

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** or **View associated domains** depending on whether you want to enable the Quicksight blueprint in the domain owner AWS account or the associated AWS account and then choose that domain by choosing its name from the list. The name is a hyperlink.
3. On the domain's details page, navigate to the **Blueprints** tab.
4. In the **Blueprints** tab, locate the **QuickSight** blueprint. You can either choose the radio button next to the QuickSight blueprint and then choose the **Enable** button. Or you can choose the **QuickSight** blueprint (the name is a hyperlink) and then on the blueprint details page, choose **Enable in this account**.
5. On the **Enable QuickSight** page, specify the following and then choose **Enable blueprint**:
   - **Provisioning role** - Amazon SageMaker Unified Studio uses this role to provision and manage resources defined in the selected blueprints in your account. You can either choose the existing or create a new role. For more information, see AmazonSageMakerProvisioning role.
   - **QuickSight VPC manager role** - Amazon SageMaker Unified Studio provisions QuickSight to create and manage VPCs in your account using this role. You can either choose the existing or create a new role. For more information, see AmazonSageMakerQuickSightVPCTRole.
   - **Authorized domain units** - these are domain units where projects can access resources defined by this blueprint. You can use the text field to search for the domain units and then the **Add** button to add them to the list of authorized domain units.

Complete the following steps to add the Quicksight blueprint to an existing project profile. You can only do this in the domain owner AWS account.

Add the QuickSight blueprint to an existing project profile

1. Navigate to the Amazon SageMaker management console at https://console.aws.amazon.com/datazone and use the region selector in the top navigation bar to choose the appropriate AWS Region.
2. Choose **View domains** and then choose the domain that you're working with by choosing its name from the list. The name is a hyperlink.

3. On the domain's details page, navigate to the **Project profiles** tab and then choose the project profile to which you want to add the Quicksight blueprint. It can be either the All capabilities project profile, or the Generative AI application development project profile, or the SQL analytics project profile, or an existing custom project profile.
4. On the chosen project profile's details page, choose **Add blueprint deployment settings**.
5. On the Add blueprint deployment settings page, specify the following and then choose Add blueprint deployment settings.
   - Blueprint deployment settings name
   - Blueprint deployment settings description - optional
   - Under **Blueprint**, use the drop-down menu to choose **Quicksight**.
   - Deployment properties - the account and region where you want this blueprint deployment settings to be created. Note that the corresponding blueprint should be enabled in this account and region so that the blueprint deployment settings could be created successfully. This is also where you can specify the **Mode**, choosing between **On create** (deploy the blueprint deployment settings as soon as the project is created) or **On demand** (deploy blueprint deployment settings when users need it) and the deployment order.
   - AWS SSM Parameter Store path in AWS Systems Manager Parameters Store that contains parameters definition.
   - Blueprint parameters - these parameter values that will be used during project creation. You can override values that are set as blueprint or SSM values and check the Editable box if you want the values to be provided during project creation.

> **Note**
>
> It is recommend when you add the Quicksight blueprint to a project profile together with at least one of the following blueprints - LakehouseDatabase, LakehouseCatalog, RedshiftServerless. For more information, see Blueprints in Amazon SageMaker Unified Studio.
>
> If you include the above blueprint(s), it is also recommended that in the blueprint deployment configuration, you keep the order of the Quicksight blueprint after the LakehouseDatabase, LakehouseCatalog, RedshiftServerless blueprints.

You can also add the Quicksight blueprint to a new custom project profile. For more information on creating custom project profiles, see Custom project profile.

For information on the user flow for Quicksight in Amazon SageMaker Unified Studio, see Amazon QuickSight in Amazon SageMaker Unified Studio.

Security in Amazon SageMaker Unified Studio

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to Amazon SageMaker Unified Studio, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon SageMaker Unified Studio. The following topics show you how to configure Amazon SageMaker Unified Studio to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon SageMaker Unified Studio resources.

Topics

- Identity and access management for Amazon SageMaker Unified Studio
- Data protection in Amazon SageMaker Unified Studio
- Authorization in Amazon SageMaker Unified Studio
- Compliance validation for Amazon SageMaker Unified Studio
- Security Best Practices for Amazon SageMaker Unified Studio
- Resilience in Amazon SageMaker Unified Studio
- Infrastructure Security in Amazon SageMaker Unified Studio
- Network isolation in Amazon SageMaker Unified Studio
- Configuration and vulnerability analysis for Amazon SageMaker Unified Studio

- Cross-service confused deputy prevention

Identity and access management for Amazon SageMaker Unified Studio

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Amazon SageMaker Unified Studio resources. IAM is an AWS service that you can use with no additional charge.

> **Note**
>
> Certain features in Amazon SageMaker Unified Studio may maintain active sessions even after you log out of your IAM Identity Center/SSO session. Sometimes, these disconnected sessions can persist for up to 12 hours. Affected features include:
>
> - Spaces
> - Local IDE (Visual Studio Code) Support
> - Workflows
> - ML Experiments (MLFlow)
> - Connections
> - Hyperpod
> - Amazon SageMaker partner applications
>
> To ensure the security of your environment, administrators must review and adjust session duration settings where possible and be cautious when using shared workstations or public networks.

Topics

- Audience
- Authenticating with identities
- Managing access using policies
- How Amazon SageMaker Unified Studio works with IAM

- Identity-based policy examples for Amazon SageMaker Unified Studio
- AWS managed policies for Amazon SageMaker Unified Studio
- IAM roles for Amazon SageMaker Unified Studio
- Access control patterns Amazon SageMaker Unified Studio
- Troubleshooting Amazon SageMaker Unified Studio identity and access

Audience

How you use AWS Identity and Access Management (IAM) differs based on your role:

- **Service user** - request permissions from your administrator if you cannot access features (see Troubleshooting Amazon SageMaker Unified Studio identity and access)
- **Service administrator** - determine user access and submit permission requests (see How Amazon SageMaker Unified Studio works with IAM)
- **IAM administrator** - write policies to manage access (see Identity-based policy examples for Amazon SageMaker Unified Studio)

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be authenticated as the AWS account root user, an IAM user, or by assuming an IAM role.

You can sign in as a federated identity using credentials from an identity source like AWS IAM Identity Center (IAM Identity Center), single sign-on authentication, or Google/Facebook credentials. For more information about signing in, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

For programmatic access, AWS provides an SDK and CLI to cryptographically sign requests. For more information, see AWS Signature Version 4 for API requests in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity called the AWS account *root user* that has complete access to all AWS services and resources. We strongly recommend that you don't use the root user for everyday tasks. For tasks that require root user credentials, see Tasks that require root user credentials in the *IAM User Guide*.

Federated identity

As a best practice, require human users to use federation with an identity provider to access AWS services using temporary credentials.

A *federated identity* is a user from your enterprise directory, web identity provider, or Directory Service that accesses AWS services using credentials from an identity source. Federated identities assume roles that provide temporary credentials.

For centralized access management, we recommend AWS IAM Identity Center. For more information, see What is IAM Identity Center? in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An *IAM user* is an identity with specific permissions for a single person or application. We recommend using temporary credentials instead of IAM users with long-term credentials. For more information, see Require human users to use federation with an identity provider to access AWS using temporary credentials in the *IAM User Guide*.

An *IAM group* specifies a collection of IAM users and makes permissions easier to manage for large sets of users. For more information, see Use cases for IAM users in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity with specific permissions that provides temporary credentials. You can assume a role by switching from a user to an IAM role (console) or by calling an AWS CLI or AWS API operation. For more information, see Methods to assume a role in the *IAM User Guide*.

IAM roles are useful for federated user access, temporary IAM user permissions, cross-account access, cross-service access, and applications running on Amazon EC2. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy defines permissions when associated with an identity or resource. AWS evaluates these policies when a principal makes a request. Most policies are stored in AWS as JSON documents. For more information about JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Using policies, administrators specify who has access to what by defining which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. An IAM administrator creates IAM policies and adds them to roles, which users can then assume. IAM policies define permissions regardless of the method used to perform the operation.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you attach to an identity (user, group, or role). These policies control what actions identities can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

Identity-based policies can be *inline policies* (embedded directly into a single identity) or *managed policies* (standalone policies attached to multiple identities). To learn how to choose between managed and inline policies, see Choose between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples include IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. You must specify a principal in a resource-based policy.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Other policy types

AWS supports additional policy types that can set the maximum permissions granted by more common policy types:

- **Permissions boundaries** – Set the maximum permissions that an identity-based policy can grant to an IAM entity. For more information, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – Specify the maximum permissions for an organization or organizational unit in AWS Organizations. For more information, see Service control policies in the *AWS Organizations User Guide*.

- **Resource control policies (RCPs)** – Set the maximum available permissions for resources in your accounts. For more information, see Resource control policies (RCPs) in the *AWS Organizations User Guide*.
- **Session policies** – Advanced policies passed as a parameter when creating a temporary session for a role or federated user. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

How Amazon SageMaker Unified Studio works with IAM

Before you use IAM to manage access to Amazon SageMaker Unified Studio, learn what IAM features are available to use with Amazon SageMaker Unified Studio.

IAM features you can use with Amazon SageMaker Unified Studio

IAM feature	Amazon SageMaker Unified Studio support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes
Policy resources	Yes
Policy condition keys	Yes
ACLs	No
ABAC (tags in policies)	Partial
Temporary credentials	Yes
Principal permissions	Yes

IAM feature	Amazon SageMaker Unified Studio support
Service roles	Yes
Service-linked roles	No

To get a high-level view of how Amazon SageMaker Unified Studio and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

Identity-based policies for Amazon SageMaker Unified Studio

Supports identity-based policies: Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Identity-based policy examples for Amazon SageMaker Unified Studio

To view examples of Amazon SageMaker Unified Studio identity-based policies, see Identity-based policy examples for Amazon SageMaker Unified Studio.

Resource-based policies within Amazon SageMaker Unified Studio

Supports resource-based policies: No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Policy actions for Amazon SageMaker Unified Studio

Supports policy actions: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Include actions in a policy to grant permissions to perform the associated operation.

To see a list of Amazon SageMaker Unified Studio actions, see Actions Defined by Amazon SageMaker Unified Studio in the *Service Authorization Reference*.

Policy actions in Amazon SageMaker Unified Studio use the following prefix before the action:

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      ":action1",
      ":action2"
         ]
```

To view examples of Amazon SageMaker Unified Studio identity-based policies, see Identity-based policy examples for Amazon SageMaker Unified Studio.

Policy resources for Amazon SageMaker Unified Studio

Supports policy resources: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. As a best practice, specify a resource using its Amazon Resource Name (ARN). For actions that don't

support resource-level permissions, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To see a list of Amazon SageMaker Unified Studio resource types and their ARNs, see Resources Defined by Amazon SageMaker Unified Studio in the *Service Authorization Reference*. To learn with which actions you can specify the ARN of each resource, see Actions Defined by Amazon SageMaker Unified Studio .

To view examples of Amazon SageMaker Unified Studio identity-based policies, see Identity-based policy examples for Amazon SageMaker Unified Studio.

Policy condition keys for Amazon SageMaker Unified Studio

Supports service-specific policy condition keys: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element specifies when statements execute based on defined criteria. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

To see a list of Amazon SageMaker Unified Studio condition keys, see Condition Keys for Amazon SageMaker Unified Studio in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see Actions Defined by Amazon SageMaker Unified Studio .

To view examples of Amazon SageMaker Unified Studio identity-based policies, see Identity-based policy examples for Amazon SageMaker Unified Studio.

ACLs in Amazon SageMaker Unified Studio

Supports ACLs: No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

ABAC with Amazon SageMaker Unified Studio

Supports ABAC (tags in policies): Partial

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes called tags. You can attach tags to IAM entities and AWS resources, then design ABAC policies to allow operations when the principal's tag matches the tag on the resource.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see Define permissions with ABAC authorization in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

Using temporary credentials with Amazon SageMaker Unified Studio

Supports temporary credentials: Yes

Temporary credentials provide short-term access to AWS resources and are automatically created when you use federation or switch roles. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM and AWS services that work with IAM in the *IAM User Guide*.

Cross-service principal permissions for Amazon SageMaker Unified Studio

Supports forward access sessions (FAS): Yes

Forward access sessions (FAS) use the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. For policy details when making FAS requests, see Forward access sessions.

Service roles for Amazon SageMaker Unified Studio

Supports service roles: Yes

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an AWS service in the *IAM User Guide*.

> **Warning**
>
> Changing the permissions for a service role might break Amazon SageMaker Unified Studio functionality. Edit service roles only when Amazon SageMaker Unified Studio provides guidance to do so.

Service-linked roles for Amazon SageMaker Unified Studio

Supports service-linked roles: No

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing service-linked roles, see AWS services that work with IAM. Find a service in the table that includes a `Yes` in the **Service-linked role** column. Choose the **Yes** link to view the service-linked role documentation for that service.

Identity-based policy examples for Amazon SageMaker Unified Studio

By default, users and roles don't have permission to create or modify Amazon SageMaker Unified Studio resources. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Create IAM policies (console) in the *IAM User Guide*.

For details about actions and resource types defined by Amazon SageMaker Unified Studio, including the format of the ARNs for each of the resource types, see Actions, Resources, and Condition Keys for Amazon SageMaker Unified Studio in the *Service Authorization Reference*.

Topics

- Policy best practices

- Using the Amazon SageMaker Unified Studio console
- Allow users to view their own permissions

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon SageMaker Unified Studio resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see Validate policies with IAM Access Analyzer in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Secure API access with MFA in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

Using the Amazon SageMaker Unified Studio console

To access the Amazon SageMaker Unified Studio console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon SageMaker Unified Studio resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that they're trying to perform.

To ensure that users and roles can still use the Amazon SageMaker Unified Studio console, also attach the Amazon SageMaker Unified Studio `ConsoleAccess` or `ReadOnly` AWS managed policy to the entities. For more information, see Adding permissions to a user in the *IAM User Guide*.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
```

```
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS managed policies for Amazon SageMaker Unified Studio

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ReadOnlyAccess** AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the *IAM User Guide*.

Topics

- AWS policy: SageMakerStudioFullAccess
- AWS policy: SageMakerStudioProjectUserRolePermissionsBoundary
- AWS policy: SageMakerStudioDomainExecutionRolePolicy
- AWS policy: SageMakerStudioProjectUserRolePolicy
- AWS policy: SageMakerStudioProjectRoleMachineLearningPolicy
- AWS policy: SageMakerStudioDomainServiceRolePolicy
- AWS policy: SageMakerStudioProjectProvisioningRolePolicy
- AWS policy: AmazonDataZoneBedrockModelManagementPolicy
- AWS policy: SageMakerStudioQueryExecutionRolePolicy
- AWS policy: SageMakerStudioEMRServiceRolePolicy
- AWS policy: AmazonDataZoneBedrockModelConsumptionPolicy
- AWS policy: SageMakerStudioEMRInstanceRolePolicy
- AWS policy: SageMakerStudioBedrockAgentServiceRolePolicy
- AWS policy: SageMakerStudioBedrockChatAgentUserRolePolicy
- AWS policy: SageMakerStudioBedrockPromptUserRolePolicy
- AWS policy: SageMakerStudioBedrockFlowServiceRolePolicy
- AWS policy: SageMakerStudioBedrockEvaluationJobServiceRolePolicy
- AWS policy: SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy
- AWS policy: SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy
- AWS policy: SageMakerStudioBedrockFunctionExecutionRolePolicy
- AWS policy: SageMakerStudioUserIAMConsolePolicy
- AWS policy: SageMakerStudioUserIAMDefaultExecutionPolicy
- AWS policy: SageMakerStudioUserIAMPermissiveExecutionPolicy
- AWS policy: SageMakerStudioAdminIAMConsolePolicy
- AWS policy: SageMakerStudioAdminIAMDefaultExecutionPolicy
- AWS policy: SageMakerStudioAdminIAMPermissiveExecutionPolicy
- AWS policy: SageMakerStudioAdminProjectUserRolePolicy

- Amazon SageMaker Unified Studio updates to AWS managed policies

AWS policy: SageMakerStudioFullAccess

This policy provides full access to Amazon SageMaker Unified Studio via the Amazon SageMaker management console.

To view the permissions for this policy, see SageMakerStudioFullAccess in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioProjectUserRolePermissionsBoundary

Amazon SageMaker Unified Studio creates IAM roles for Projects users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the boundary of their permissions.

This policy is a permissions boundary. A permissions boundary sets the maximum permissions that an identity-based policy can grant to an IAM entity. You should not use and attach Amazon SageMaker Unified Studio permissions boundary policies on your own. Amazon SageMaker Unified Studio permissions boundary policies should only be attached to Amazon SageMaker Unified Studio managed roles.

When you create a project via the Amazon SageMaker Unified Studio, it applies this permissions boundary to the IAM roles that are provisioned during project creation. The permissions boundary limits the scope of the roles that Amazon SageMaker Unified Studio creates and any roles that you add.

Amazon SageMaker Unified Studio uses the SageMakerStudioProjectUserRolePermissionsBoundary managed policy to limit the provisioned IAM principal to which it is attached. The principals might take the form of the user roles that Amazon SageMaker Unified Studiocan assume on behalf of interactive enterprise users or analytic services (AWS Glue, for example), and then conduct actions to process data such as reading and writing from Amazon S3 or running AWS Glue crawler.

The SageMakerStudioProjectUserRolePermissionsBoundary policy grants read and write access for Amazon SageMaker Unified Studioto services such as Amazon SageMaker, AWS Glue, Amazon S3, AWS Lake Formation, Amazon Redshift, Amazon Athena, Amazon Q, Amazon EMR. The policy also gives read and write permissions to some infrastructure resources that are required to use these services such as network interfaces, AWS KMS keys, AWS CodeCommit, and AWS Secrets Manager.

> **Note**
>
> You can't create new projects with AWS CodeCommit. Existing projects that were created using CodeCommit will continue to work.

- Amazon SageMaker permissions are required for users to use the Amazon SageMaker Domain and Spaces provisioned by default by the Tooling blueprint.
- AWS Glue permissions are required for users to use the default AWS Glue Connection and create AWS Glue Sessions.
- Amazon S3 permissions are required for users to access the project's Amazon S3 bucket.
- AWS Lake Formation permissions are required for users to access underlying data in Amazon S3.
- Amazon Redshift permissions are required for users to perform SQL queries against Amazon Redshift, and to allow access to the project's Amazon Redshift clusters.
- Amazon Athena permissions are required for users to use the provisioned Amazon Athena workgroup and to perform SQL queries.
- Amazon Q permissions are required for users to interact with Amazon Q within Amazon SageMaker Unified Studio.
- Amazon EMR permissions are required for users to create and access EMR clusters. AWS KMS permissions are required to use CMK in the various services integrated with Amazon SageMaker Unified Studio.
- AWS CodeCommit permissions are required for users to use the default Git repository, and perform operations such as committing changes.
- AWS Secrets Manager permissions are required for accessing the secret for various services, such as Amazon Redshift, AWS Glue federated data connections, and Amazon Bedrock.
- Amazon Bedrock permissions are required to allow users access to Amazon Bedrock IDE, a development experience in Amazon SageMaker Unified Studio that lets you easily discover Amazon Bedrock models and build generative AI apps that use Amazon Bedrock models and features.

To view the permissions for this policy, see SageMakerStudioProjectUserRolePermissionsBoundary in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioDomainExecutionRolePolicy

Default policy for the SageMakerUnifiedStudioDomainExecutionRole service role. This role is used by Amazon SageMaker Unified Studio to catalog, discover, govern, share, and analyze data in the Amazon SageMaker Unified Studio domain.

This role provides access to all Amazon SageMaker Unified Studio APIs that are required for Amazon SageMaker Unified Studio use, as well as RAM permissions to support usage of associated accounts in a Amazon SageMaker Unified Studio domain. It also provides access to services used outside of a project scope, including AWS CodeConnections, Amazon Q, AWS Systems Manager, and Amazon Bedrock.

To view the permissions for this policy, see SageMakerStudioDomainExecutionRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioProjectUserRolePolicy

Amazon SageMaker Unified Studio creates IAM roles for projects users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the permissions.

This is the main policy for the SageMakerUnifiedStudioProjectRole role. The SageMakerStudioProjectUserRolePolicy policy is created as part of the Tooling environment blueprint. This policy grants read and write access for Amazon SageMaker Unified Studio users to services such as Amazon SageMaker, AWS Glue, Amazon S3, AWS Lake Formation, Amazon Redshift, Amazon Athena, Amazon Q, Amazon EMR. The policy also gives read and write permissions to some infrastructure resources that are required to use these services such as network interfaces, AWS KMS keys, AWS CodeCommit, and AWS Secrets Manager.

An administrator can control certain permissions in this policy by tagging the role to which the policy is attached. The following tags control permission scoping:

- EnableGlueWorkloadsPermissions — When set to "true" (default), grants permissions for AWS Glue workloads including creating and managing Glue Sessions, Blueprints, Jobs, Data Quality Rulesets, and Workflows. When not set to "true", these Glue workload permissions are not granted. Glue Data Catalog permissions (such as GetCatalogs, GetDatabases, GetTables) are not affected by this tag and remain available regardless of this setting.
- EnableAmazonBedrockPermissions — When set to "true" (default), grants permissions for Amazon Bedrock including foundation model access and Bedrock agent operations. When not set to "true", these Bedrock permissions are not granted.

> **Note**
>
> You can't create new projects with AWS CodeCommit. Existing projects that were created using CodeCommit will continue to work.

- Amazon SageMaker permissions are required for users to use the Amazon SageMaker Domain and Spaces provisioned by default by the Tooling blueprint.
- AWS Glue permissions are required for users to use the default AWS Glue Connection and create AWS Glue Sessions.
- Amazon S3 permissions are required for users to access the project's Amazon S3 bucket.
- AWS Lake Formation permissions are required for users to access underlying data in Amazon S3.
- Amazon Redshift permissions are required for users to perform SQL queries against Amazon Redshift, and to allow access to the project's Amazon Redshift clusters.
- Amazon Athena permissions are required for users to use the provisioned Amazon Athena workgroup and to perform SQL queries.
- Amazon Q permissions are required for users to interact with Amazon Q within Amazon SageMaker Unified Studio.
- Amazon EMR permissions are required for users to create and access Amazon EMR clusters.
- AWS CodeCommit permissions are required for users to use the default Git repository, and perform operations such as committing changes.
- AWS Secrets Manager permissions are required for accessing the secret for various services, such as Amazon Redshift, AWS Glue federated data connections, and Amazon Bedrock.
- Amazon Bedrock permissions are required to allow users access to Amazon Bedrock IDE, a development experience in Amazon SageMaker Unified Studio that lets you easily discover Amazon Bedrock models and build generative AI apps that use Amazon Bedrock models and features.
- AWS KMS permissions are required to support customer managed keys. Resources provisioned by Amazon SageMaker Unified Studio can be encrypted with your customer managed key.

To view the permissions for this policy, see SageMakerStudioProjectUserRolePolicy in the *AWS Managed Policy Reference*.

> **Note**
>
> Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, AI, and ML actions. You can attach the SageMakerStudioProjectUserRolePolicy managed policy as your user role policy or you can create and attach your own user role policy. Using your own policy provides more granular control over permissions but requires knowledge of IAM policy configuration. The IAM policy must include all necessary permissions required for the service to function properly.

Role assumption permissions in this policy

This policy lets the project user role assume other IAM roles. Amazon SageMaker Unified Studio projects can use compute resources that you provide, such as an Amazon EMR on EC2 cluster, through an access role. Because you define the access role name, the policy can't predict it in advance. For this reason, the AllowAssumeAccessRole statement grants `sts:AssumeRole` on `Resource: "*"`, so the project user role can assume the access role at runtime. The policy also includes a SetSourceIdentityForAssumeAccessRole statement that requires `sts:SetSourceIdentity` on every assume-role call the project user role makes. For more information about roles and trust policies, see Roles terms and concepts in the *IAM User Guide*.

Because of these two statements, the project user role can assume another IAM role in the account *only if* that target role's trust policy explicitly allows both `sts:AssumeRole` and `sts:SetSourceIdentity`. A role whose trust policy allows only `sts:AssumeRole` can't be assumed by the project user role. For example, a role that trusts the account root but doesn't grant `sts:SetSourceIdentity` fails the assume-role call with an `AccessDenied` error.

> **Audit trust policies for broad role assumption**
>
> If you administer an account that hosts Amazon SageMaker Unified Studio projects, audit the trust policies of privileged IAM roles in the account. This helps you avoid unintended role assumption from a project identity. Confirm that no privileged role grants `sts:SetSourceIdentity` to a broad principal, such as the account root, using an unrestricted or wildcard source-identity condition (for example, `"Condition": {"StringLike": {"sts:SourceIdentity": "*"}}`). An exception applies only if the role is intended to be assumable by Amazon SageMaker Unified Studio project roles.

When you register an access or compute role for a project, scope the role's trust policy to the specific project user role. Where possible, use an `sts:ExternalId` condition that matches the project ID, instead of trusting the account root broadly.

AWS policy: SageMakerStudioProjectRoleMachineLearningPolicy

Amazon SageMaker Unified Studio creates IAM roles for projects users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the permissions related to Amazon SageMaker.

This is the SageMaker policy for the SageMakerUnifiedStudioProjectRole role. This policy grants read and write access for Amazon SageMaker Unified Studio users to services such as Amazon SageMaker, Amazon CloudWatch, and AWS Resource Groups. The policy also gives read and write permissions to some infrastructure resources that are required to use these services such as network interfaces and AWS KMS keys.

An administrator can control certain permissions in this policy by tagging the role to which the policy is attached. The tag EnableSageMakerMLWorkloadsPermissions — when set to "true" (default), grants permissions for SageMaker ML workloads including training jobs, processing jobs, and model deployment. When not set to "true", these SageMaker ML workload permissions are not granted.

To view the permissions for this policy, see SageMakerStudioProjectRoleMachineLearningPolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioDomainServiceRolePolicy

This is the default policy for the SageMakerUnifiedStudioDomainServiceRole service role. This policy is used by Amazon SageMaker Unified Studio to access the SSM parameters in the user's account. Those parameters are set by the administrator in the Amazon SageMaker Unified Studio project profiles. This policy also has permissions to AWS KMS for encrypted SSM parameters. The KMS key must be tagged with EnableKeyForAmazonDataZone to allow decrypting the SSM parameters.

To view the permissions for this policy, see SageMakerStudioDomainServiceRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioProjectProvisioningRolePolicy

Amazon SageMaker Unified Studio uses this policy to provision and manage resources in your account.

This is the default policy for the AmazonSageMakerProvisioning-<domainAccountId> service role. This role is used by Amazon SageMaker Unified Studio to manage resources in your account created as part of projects lifecycle. This role provides access to manage resources for all services used in Amazon SageMaker Unified Studio, including Amazon SageMaker, AWS Glue, Amazon S3, AWS Lake Formation, Amazon Redshift, Amazon Athena, Amazon Q, Amazon EMR, Amazon Bedrock, AWS CodeCommit, and AWS IAM.

> **Note**
>
> You can't create new projects with AWS CodeCommit. Existing projects that were created using CodeCommit will continue to work.

- Amazon SageMaker permissions are required to manage the SageMaker Domain and Spaces provisioned by default by the Tooling blueprint.
- AWS Glue permissions are required to manage AWS Glue Connections, AWS Glue Catalog, and AWS Glue Databases.
- Amazon S3 permissions are required to access S3 objects to provision Amazon Bedrock resources, federated AWS Glue connection, and to create the staging bucket for Amazon Redshift.
- AWS Lake Formation permissions are required to manage grants on AWS Glue Data Catalog.
- Amazon Redshift permissions are required to provision Amazon Redshift Serverless workgroup and namespace.
- Amazon Athena permissions are required to provision Amazon Athena workgroup and Amazon Athena data catalog for federated connection.
- Amazon EMR permissions are required to provision Amazon EMR on EC2 clusters.
- AWS KMS permissions are required to use CMK in the various services integrated with Amazon SageMaker Unified Studio.
- AWS CodeCommit permissions are required to provision the default Git repository.
- AWS Secrets Manager permissions are required to provision the secret for various services, such as Amazon Redshift, AWS Glue federated data connections, and Amazon Bedrock.

- AWS IAM permissions are required to provision the roles that will be used by users of Amazon SageMaker Unified Studio.
- Amazon Bedrock permissions are required to provision Amazon Bedrock IDE related resources to enable discovery of Amazon Bedrock models and build generative AI apps that use Amazon Bedrock models and features.

To view the permissions for this policy, see SageMakerStudioProjectProvisioningRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: AmazonDataZoneBedrockModelManagementPolicy

Provides permissions to manage Amazon Bedrock model access, including creating, tagging and deleting application inference profiles.

To view the permissions for this policy, see AmazonDataZoneBedrockModelManagementPolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioQueryExecutionRolePolicy

This is the default policy for the SageMakerQueryExecutionRole role. This policy provides permissions to run query executions on federated connections.

To view the permissions for this policy, see SageMakerStudioQueryExecutionRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioEMRServiceRolePolicy

Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the permissions related to EMR.

To view the permissions for this policy, see SageMakerStudioEMRServiceRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: AmazonDataZoneBedrockModelConsumptionPolicy

Provides permissions to consume Amazon Bedrock models, including invoking Amazon Bedrock application inference profile created for particular Amazon DataZone domain.

To view the permissions for this policy, see AmazonDataZoneBedrockModelConsumptionPolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioEMRInstanceRolePolicy

Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, artificial intelligence, and machine learning actions and uses this policy when creating these roles to define the permissions related to EMR.

To view the permissions for this policy, see SageMakerStudioEMRInstanceRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioBedrockAgentServiceRolePolicy

This policy allows Amazon Bedrock Agents to access Amazon Bedrock models and other resources attached to an agent in Amazon SageMaker Unified Studio.

This is the main policy for the Amazon Bedrock IDE agent service role. This role is part of the AmazonBedrockChatAgent environment blueprint.

This policy grants the Amazon Bedrock service access to resources attached to a Amazon Bedrock IDE chat agent app, including Amazon Bedrock models, guardrails, knowledge bases; AWS Lambda functions; Amazon S3 objects; and an AWS KMS key.

- Amazon Bedrock permissions are required for Amazon Bedrock agents to invoke Amazon Bedrock models enabled at the project level. This policy also grants access to Amazon Bedrock resources managed within Amazon SageMaker Unified Studio.
- AWS Lambda permissions are required for Amazon Bedrock agents to run functions attached to an Amazon Bedrock IDE chat agent app.
- Amazon S3 permissions are required for Amazon Bedrock agents to access the project's Amazon S3 bucket.
- AWS KMS permissions are required to access Amazon Bedrock and Amazon S3 data encrypted with a customer managed key.

This policy allows the Amazon Bedrock service to access specific resources tagged with the same project ID as the service role. This tag restriction effectively only permits access to resources in the same project. By default, project users are not allowed to change service role tags.

To view the permissions for this policy, see SageMakerStudioBedrockAgentServiceRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioBedrockChatAgentUserRolePolicy

This policy provides access to an Amazon Bedrock chat agent app's configuration and Amazon Bedrock agent in Amazon SageMaker Unified Studio.

This is the main policy for the Amazon Bedrock IDE chat agent user role. This role is part of the AmazonBedrockChatAgent environment blueprint.

This policy grants users access to a shared Amazon Bedrock IDE chat agent app, including the permission to invoke an Amazon Bedrock agent, get its configuration from Amazon S3, and use an AWS KMS key.

- Amazon Bedrock permissions are required for app users to read and invoke an Amazon Bedrock agent.
- Amazon S3 permissions are required for app users to read an object in the project's Amazon S3 bucket.
- AWS KMS permissions are required to access Amazon Bedrock and Amazon S3 data encrypted with a customer managed key.

This policy allows users to access individually shared Amazon Bedrock IDE chat agent apps. By default, domain users and project users are not allowed to change user role tags.

To view the permissions for this policy, see SageMakerStudioBedrockChatAgentUserRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioBedrockPromptUserRolePolicy

This policy provides access to an Amazon Bedrock prompt and its configuration in Amazon SageMaker Unified Studio.

This is the main policy for the Amazon Bedrock IDE prompt user role. This role is part of the AmazonBedrockPrompt environment blueprint.

This policy grants users access to a shared Amazon Bedrock IDE prompt, including the Amazon Bedrock prompt, its configuration in Amazon S3, and an AWS KMS key.

- Amazon Bedrock permissions are required for prompt users to read Amazon Bedrock prompts.
- Amazon S3 permissions are required for prompt users to read an object in the project's Amazon S3 bucket.

- AWS KMS permissions are required to access Amazon Bedrock and Amazon S3 data encrypted with a customer managed key.

This policy allows users to access individually shared Amazon Bedrock IDE prompts. By default, domain users and project users are not allowed to change user role tags.

To view the permissions for this policy, see SageMakerStudioBedrockPromptUserRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioBedrockFlowServiceRolePolicy

This policy allows Amazon Bedrock Flows to access Amazon Bedrock models and other resources attached to a flow in Amazon SageMaker Unified Studio.

This is the main policy for the Amazon Bedrock IDE prompt flow service role. This role is part of the AmazonBedrockFlow environment blueprint.

This policy grants the Amazon Bedrock service access to resources attached to a Amazon Bedrock IDE flow app, including Amazon Bedrock models, guardrails, knowledge bases, prompts; AWS Lambda functions; and an AWS KMS key.

- Amazon Bedrock permissions are required for Amazon Bedrock prompt flows to invoke Amazon Bedrock models enabled at the project level. This policy also grants access to Amazon Bedrock resources managed within Amazon SageMaker Unified Studio.
- AWS Lambda permissions are required for Amazon Bedrock prompt flows to run functions attached to an Amazon Bedrock IDE flow app.
- AWS KMS permissions are required to access Amazon Bedrock and Amazon S3 data encrypted with a customer managed key.

This policy allows the Amazon Bedrock service to access specific resources tagged with the same project ID as the service role. This tag restriction effectively only permits access to resources in the same project. By default, project users are not allowed to change service role tags.

To view the permissions for this policy, see SageMakerStudioBedrockFlowServiceRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioBedrockEvaluationJobServiceRolePolicy

This policy allows Amazon Bedrock to access Amazon Bedrock models and datasets for evaluation jobs in Amazon SageMaker Unified Studio.

This is the main policy for the Amazon Bedrock IDE evaluation job service role. This role is part of the AmazonBedrockEvaluation environment blueprint.

This policy grants the Amazon Bedrock service access to resources for an Amazon Bedrock model evaluation job, including Amazon Bedrock models, Amazon S3 objects, and an AWS KMS key.

- Amazon Bedrock permissions are required for Amazon Bedrock evaluation jobs to invoke Amazon Bedrock models enabled at the project level. This policy also grants access to Amazon Bedrock resources managed within Amazon SageMaker Unified Studio.
- Amazon S3 permissions are required for Amazon Bedrock evaluation jobs to access the project's Amazon S3 bucket.
- AWS KMS permissions are required to access Amazon S3 data encrypted with a customer managed key.

This policy allows the Amazon Bedrock service to access specific resources tagged with the same project ID as the service role. This tag restriction effectively only permits access to resources in the same project. By default, project users are not allowed to change service role tags.

To view the permissions for this policy, see SageMakerStudioBedrockEvaluationJobServiceRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

This policy provides access to configure vector stores and Amazon Bedrock knowledge bases in Amazon SageMaker Unified Studio.

This is the main policy for the Amazon Bedrock IDE knowledge base custom resource service role. This role is part of the AmazonBedrockKnowledgeBase environment blueprint.

This policy grants AWS Lambda-backed CloudFormation custom resources access to Amazon Bedrock IDE knowledge bases and their Amazon OpenSearch Serverless collections.

- Amazon Bedrock permissions are required for the custom resource to start and query Amazon Bedrock knowledge base ingestion jobs.

- Amazon OpenSearch Serverless permissions for the custom resource to prepare Amazon OpenSearch Serverless collections for use with Amazon Bedrock knowledge bases.

This policy allows the Amazon Bedrock service to access specific resources tagged with the same project ID as the service role. This tag restriction effectively only permits access to resources in the same project. By default, project users are not allowed to change service role tags.

To view the permissions for this policy, see SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

This policy allows Amazon Bedrock Knowledge Bases to access Amazon Bedrock models and data sources in Amazon SageMaker Unified Studio.

This is the main policy for the Amazon Bedrock IDE knowledge base service role. This role is part of the AmazonBedrockKnowledgeBase environment blueprint.

This policy grants the Amazon Bedrock service access to resources attached to Amazon Bedrock IDE knowledge bases, including Amazon Bedrock models, Amazon OpenSearch Serverless collections, Amazon S3 objects, and an AWS KMS key.

- Amazon Bedrock permissions are required for Amazon Bedrock knowledge bases to invoke Amazon Bedrock models enabled at the project level and generate queries.
- AWS SQL Workbench permissions are required to generate SQL recommendations for querying structured data sources.
- Amazon OpenSearch Serverless permissions are required for Amazon Bedrock knowledge bases to access the vector search collections that store knowledge base embeddings.
- Amazon S3 permissions are required for Amazon Bedrock agents to access the project's Amazon S3 bucket.
- AWS KMS permissions are required to access Amazon Bedrock and Amazon S3 data encrypted with a customer managed key.

This policy allows the Amazon Bedrock service to access specific resources tagged with the same project ID as the service role. This tag restriction effectively only permits access to resources in the same project. By default, project users are not allowed to change service role tags.

To view the permissions for this policy, see SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioBedrockFunctionExecutionRolePolicy

This policy allows AWS Lambda to access an Amazon Bedrock function component's configuration in Amazon SageMaker Unified Studio.

This is the main policy for the Amazon Bedrock IDE function execution role. This role is part of the AmazonBedrockFunction environment blueprint.

This policy grants the AWS Lambda service access to an Amazon Bedrock IDE function's configuration, including AWS Secrets Manager secrets and an AWS KMS key.

- AWS Secrets Manager permissions are required for AWS Lambda to access the Amazon Bedrock IDE function's API keys while fulfilling API requests.
- AWS KMS permissions are required to access AWS Secrets Manager secrets encrypted with a customer managed key.

This policy allows the AWS Lambda service to access specific resources tagged with the same project ID as the service role. This tag restriction effectively only permits access to resources in the same project. By default, project users are not allowed to change service role tags.

To view the permissions for this policy, see SageMakerStudioBedrockFunctionExecutionRolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioUserIAMConsolePolicy

This policy provides individual setup privileges for Amazon SageMaker Unified Studio using the AWS Management Console and SDK. It grants permissions for launching Amazon SageMaker Unified Studio.

- Amazon DataZone permissions are required to allow principals access to Amazon DataZone actions to create a project, and to log in to Amazon SageMaker Unified Studio.
- AWS Identity and Access Management permissions are required to allow principals to list and get IAM roles, get IAM users.

To view the permissions for this policy, see SageMakerStudioUserIAMConsolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioUserIAMDefaultExecutionPolicy

This is the default execution policy for using IAM roles with Amazon SageMaker Unified Studio. This policy grants access to users to access resources. This does not grant access to data resources.

- Amazon DataZone permissions are required to access DataZone resources such as Project and Asset.
- AWS Identity and Access Management permissions are required to list IAM roles, create service-linked roles, and pass roles when provisioning resources.
- AWS STS permissions are required to assume other roles for accessing resources in cross-account.
- Amazon S3 permissions are required to list S3 buckets, allow cross-account object read, and register Amazon S3 Access Grants locations and manage the grants that share project data.
- AWS Lake Formation permissions are required to describe AWS Lake Formation resources.
- Amazon Redshift Query Editor permissions are required to interact with the query editor in Amazon SageMaker Unified Studio.
- Amazon Redshift Data API API permissions are required to run SQL statements using the Data API.
- Amazon Redshift Serverless permissions are required for discovery of Redshift Serverless.
- Amazon Redshift permissions are required for discovery of Redshift clusters.
- Amazon Bedrock permissions are required to interact with Bedrock APIs in Amazon SageMaker Unified Studio.
- Amazon EventBridge Scheduler permissions are required to interact with one-click scheduling in Amazon SageMaker Unified Studio.
- Amazon DynamoDB permissions are required to enable federated connections to external data.
- Amazon Athena permissions are required to interact with Query Editor in Amazon SageMaker Unified Studio.
- AWS Secrets Manager permissions are required to access secrets for connections.
- Amazon CodeWhisperer permissions are required to generate code recommendation.
- Amazon ECR permissions are required to run SageMaker training jobs.
- Amazon MWAA permissions are required to manage and schedule workflows.
- AWS KMS permissions are required to support customer managed key. Resources provisioned by Amazon SageMaker Unified Studio can be encrypted with your customer managed key.
- AWS IAM Identity Center permissions are required to look up the users and groups that Amazon S3 Access Grants are issued to.

To view the permissions for this policy, see SageMakerStudioUserIAMDefaultExecutionPolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioUserIAMPermissiveExecutionPolicy

This is an execution policy for using IAM roles with Amazon SageMaker Unified Studio. This policy grants access to users to access resources in your account, including broad access to data resources.

This policy provides full access to all APIs and resources for services used in Amazon SageMaker Unified Studio, such as Amazon CloudWatch Logs AWS Glue, Amazon Redshift, Amazon Redshift Data API, Amazon Redshift Serverless, Amazon S3, Amazon Athena, Amazon Bedrock, Amazon CodeWhisperer, Amazon DataZone, Amazon Q, Amazon SageMaker AI, AWS SQL Workbench, Amazon EventBridge Scheduler, and CloudFormation.

Additional access is provided for the following services:

- Amazon DataZone permissions are required to access Amazon DataZone resources such as Project and Asset.
- AWS Identity and Access Management permissions are required to list IAM roles, create service-linked roles, and pass roles when provisioning resources.
- AWS Security Token Service permissions are required to assume other roles for accessing cross-account resources.
- AWS Systems Manager permissions are required to access parameters for Amazon Q and Amazon SageMaker AI distribution.
- AWS Lake Formation permissions are required to describe AWS Lake Formation Resources.
- Amazon DynamoDB permissions are required to enable federated connections to external data.
- AWS Secrets Manager permissions are required to access secrets for connections.
- Amazon ECR permissions are required to run Amazon SageMaker AI training jobs.
- Amazon MWAA permissions are required to manage and schedule workflows.
- AWS KMS permissions are required to support customer managed key. Resources provisioned by Amazon SageMaker Unified Studio can be encrypted with your customer managed key.
- AWS IAM Identity Center permissions are required to look up the users and groups that Amazon S3 Access Grants are issued to.

To view the permissions for this policy, see SageMakerStudioUserIAMPermissiveExecutionPolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioAdminIAMConsolePolicy

This policy provides initial administrative and individual setup privileges for Amazon SageMaker Unified Studio via the AWS Management Console and SDK. It grants permissions for launching Amazon SageMaker Unified Studio.

- Amazon DataZone permissions are required to allow principals full access to all Amazon DataZone actions.
- AWS Identity and Access Management permissions are required to allow principals to list and get IAM roles, get IAM users and pass roles when creating Amazon DataZone resources.
- AWS Systems Manager permissions are required to manage parameters to enable Amazon Q.
- Amazon EC2 permissions are required to describe, create, modify, and delete VPC infrastructure including VPCs, subnets, security groups, internet gateways, NAT gateways, route tables, VPC endpoints, and elastic IP addresses for Amazon SageMaker Unified Studio environments.
- CloudFormation permissions are required to create and manage infrastructure stacks for Amazon SageMaker Unified Studio deployment.
- Amazon S3 permissions are required to allow CloudFormation to access template files from S3 buckets, including cross-account scenarios.
- AWS KMS permissions are required to manage encryption keys, perform encrypt/decrypt operations, and create grants for Amazon DataZone resources.

All EC2 resources must be tagged with `CreatedForUseWithSageMakerUnifiedStudio: true` for creation, modification, and deletion operations to ensure proper resource governance and lifecycle management.

To view the permissions for this policy, see SageMakerStudioAdminIAMConsolePolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioAdminIAMDefaultExecutionPolicy

This is the administrative execution policy for using IAM roles with Amazon SageMaker Unified Studio. This policy grants administrative access to provision, manage, and access resources in your account. This does not grant access to data resources.

- Amazon DataZone permissions are required to manage Amazon DataZone resources such as Domain and Project.

- AWS Identity and Access Management permissions are required to list IAM roles, create service-linked roles, and pass roles when provisioning resources.
- AWS STS permissions are required to assume other roles for accessing resources in cross-account.
- Amazon Q permissions are required to interact with Amazon Q within Amazon SageMaker Unified Studio.
- AWS Glue permissions are required to access data in Glue and allow usage of Glue Sessions.
- AWS Systems Manager permissions are required to manage parameters to enable Q and access SageMaker distribution.
- Amazon SageMaker AI permissions are required to manage SageMaker Space and allow SageMaker ML workloads.
- Amazon S3 permissions are required to create S3 buckets, access service CloudFormation templates in S3, delete S3 bucket policies, and register Amazon S3 Access Grants locations and manage the grants that share project data.
- CloudFormation permissions are required to manage CloudFormation stack for managing resources of other services.
- Amazon CloudWatch Logs permissions are required to access logs from workloads in Amazon SageMaker Unified Studio.
- AWS Lake Formation permissions are required to manage Lake Formation grants to access data.
- Amazon Redshift Query Editor permissions are required to interact with Query Editor in Amazon SageMaker Unified Studio.
- Amazon Redshift Data API API permissions are required to run SQL statements using the Data API.
- Amazon Redshift Serverless permissions are required for discovery of Redshift Serverless.
- Amazon Redshift permissions are required for discovery of Redshift clusters.
- Amazon Bedrock permissions are required to interact with Bedrock APIs in Amazon SageMaker Unified Studio.
- Amazon DynamoDB permissions are required to enable federated connections to external data.
- AWS Secrets Manager permissions are required to manage secrets for connections.
- Amazon Athena permissions are required to interact with Query Editor in Amazon SageMaker Unified Studio.
- Amazon CodeWhisperer permissions are required to generate code recommendations.
- Amazon EventBridge Scheduler permissions are required to interact with one-click scheduling in Amazon SageMaker Unified Studio.

- Amazon ECR permissions are required to run SageMaker training jobs.
- Amazon MWAA permissions are required to manage and schedule workflows.
- AWS KMS permissions are required to support customer managed key. Resources provisioned by Amazon SageMaker Unified Studio can be encrypted with your customer managed key.
- AWS IAM Identity Center permissions are required to look up the users and groups that Amazon S3 Access Grants are issued to.

To view the permissions for this policy, see SageMakerStudioAdminIAMDefaultExecutionPolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioAdminIAMPermissiveExecutionPolicy

This is an administrative execution policy for using IAM roles with Amazon SageMaker Unified Studio. This policy grants administrative access to provision, manage, and access resources in your account. This includes broad access to data resources.

This policy provides full access to all APIs and resources for services used in Amazon SageMaker Unified Studio, such as Amazon CloudWatch Logs AWS Glue, Amazon Redshift, Amazon Redshift Data API, Amazon Redshift Serverless, Amazon S3, Amazon Athena, Amazon Bedrock, Amazon CodeWhisperer, Amazon DataZone, Amazon Q, Amazon SageMaker AI, AWS SQL Workbench, Amazon EventBridge Scheduler, and CloudFormation.

Additional access is provided for the following services:

- AWS Identity and Access Management permissions are required to list IAM roles, create service-linked roles, and pass roles when provisioning resources.
- AWS Security Token Service permissions are required to assume other roles for accessing resources in cross-account.
- AWS Systems Manager permissions are required to manage parameters to enable Amazon Q and access SageMaker distribution.
- AWS Lake Formation permissions are required to manage AWS Lake Formation grants to access data.
- Amazon DynamoDB permissions are required to enable federated connections to external data.
- AWS Secrets Manager permissions are required to manage secrets for connections.
- Amazon ECR permissions are required to run SageMaker training jobs.
- Amazon MWAA permissions are required to manage and schedule workflows.

- AWS KMS permissions are required to support customer managed key. Resources provisioned by Amazon SageMaker Unified Studio can be encrypted with your customer managed key.
- AWS IAM Identity Center permissions are required to look up the users and groups that Amazon S3 Access Grants are issued to.

To view the permissions for this policy, see SageMakerStudioAdminIAMPermissiveExecutionPolicy in the *AWS Managed Policy Reference*.

AWS policy: SageMakerStudioAdminProjectUserRolePolicy

This IAM policy grants an IAM role full access to AWS Glue Data Catalog (metadata) and Amazon S3 (actual data) for data lake operations, with access scoped by account, and role tags. You can attach SageMakerStudioAdminProjectUserRolePolicy to your users, groups, and roles.

To view the permissions for this policy, see SageMakerStudioAdminProjectUserRolePolicy in the *AWS Managed Policy Reference*.

Amazon SageMaker Unified Studio updates to AWS managed policies

View details about updates to AWS managed policies for Amazon SageMaker Unified Studio since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Amazon SageMaker Unified Studio Document history page.

Change	Description	Date
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding Amazon S3 Access Grants permissions to register Access Grants locations and manage grants for project data, and read-only AWS IAM Identity Center and Identity Store permissions to resolve users and groups.	10/08/2026

Change	Description	Date
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adding `access-grants.s3.amazonaws.com` as a target for `iam:PassRole`, and read-only AWS IAM Identity Center and Identity Store permissions to resolve users and groups.	10/08/2026
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding Amazon S3 Access Grants permissions to register Access Grants locations and manage grants for project data, and read-only AWS IAM Identity Center and Identity Store permissions to resolve users and groups.	10/08/2026
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding `access-grants.s3.amazonaws.com` as a target for `iam:PassRole`, and read-only AWS IAM Identity Center and Identity Store permissions to resolve users and groups.	10/08/2026

Change	Description	Date
Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to SageMakerStudioProjectRoleMachineLearningPolicy - adding `sagemaker:UpdateUserProfile` to support per-user application settings management for project members.	09/14/2026
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding `cloudformation:UntagResource` to comply with upcoming CloudFormation tag authorization enforcement.	08/24/2026
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding SageMaker app lifecycle permissions to support managed app creation and deletion, including RStudio apps.	08/24/2026

Change	Description	Date
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding permissions to support Amazon SageMaker Canvas integration including Amazon Redshift, Amazon S3, Amazon Comprehend, Amazon Textract, Amazon Rekognition, Amazon EventBridge, and Amazon EMR.	06/29/2026
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adding permissions to support Amazon SageMaker Canvas integration including Amazon Redshift, Amazon S3, Amazon Comprehend, Amazon Textract, Amazon Rekognition, Amazon EventBridge, and Amazon EMR.	06/29/2026
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions to support Amazon SageMaker Canvas integration including Amazon Redshift, Amazon S3, Amazon Comprehend, Amazon Textract, Amazon Rekognition, Amazon EventBridge, and Amazon EMR.	06/29/2026

Change	Description	Date
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding permissions to support Amazon SageMaker Canvas integration including Amazon Redshift, Amazon S3, Amazon Comprehend, Amazon Textract, Amazon Rekognition, Amazon EventBridge, and Amazon EMR.	06/29/2026
Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to SageMakerStudioProjectRoleMachineLearningPolicy. The updates add permissions for Amazon SageMaker Feature Store, including create, describe, update, and delete feature groups and manage records. The updates also add read-only access to the SageMaker public model hub and permissions to list schedules for pipeline import.	06/25/2026
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions and AWS Glue session endpoints.	06/04/2026

Change	Description	Date
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions and AWS Glue session endpoints.	06/04/2026
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions and AWS Glue session endpoints.	06/04/2026
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions and AWS Glue session endpoints.	06/04/2026
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to SageMakerStudioProjectUserRolePolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions.	06/04/2026
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions.	06/04/2026

Change	Description	Date
Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to SageMakerStudioProjectRoleMachineLearningPolicy - adding `datazone:CreateAsset*` permissions to the DataZoneUserPermissions statement to support scheduling notebook runs using the Data Agent.	05/21/2026
Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to SageMakerStudioProjectRoleMachineLearningPolicy - updating the DataZoneUserPermissions statement to support the Business Data Catalog within Data Agent. Adding `datazone:List*` and `datazone:Search*` permissions for catalog discovery, and replacing `datazone:SendMessage` with `datazone:*Message*` to support conversation management.	05/13/2026
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to SageMakerStudioProjectUserRolePolicy - adding permissions to support integration with AWS Glue Data Quality.	05/11/2026

Change	Description	Date
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions to support integration with multiple services. These services include Amazon EMR Serverless Spark Connect in DataZone Data Notebook, Amazon Managed Workflows for Apache Airflow (MWAA) environments, and AWS Glue Data Quality.	05/11/2026
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding permissions to support integration with Amazon EMR Serverless Spark Connect in DataZone Data Notebook.	05/11/2026
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding permissions to support integration with multiple services. These services include Amazon EMR Serverless Spark Connect in DataZone Data Notebook, Amazon Managed Workflows for Apache Airflow (MWAA) environments, AWS Glue Data Quality, and AWS Resource Access Manager.	05/11/2026

Change	Description	Date
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adding permissions to support integration with multiple services. These services include Amazon EMR Serverless Spark Connect in DataZone Data Notebook, Amazon Managed Workflows for Apache Airflow (MWAA) environments, and AWS Resource Access Manager.	05/11/2026
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding permissions to support integration of CloudFormation LanguageExtensions transform and admin project IAM policy attachment.	05/06/2026
Policy update - SageMakerStudioUserIAMConsolePolicy	Policy updates to SageMakerStudioUserIAMConsolePolicy - adding permissions for `datazone:GetConnection` and `datazone:ListConnections` to support IAM role federation in Local IDE.	03/31/2026

Change	Description	Date
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to SageMakerStudioProjectUserRolePolicy - adding AWS Glue permissions scoped to S3 Tables catalog resource to support querying S3 Tables from SageMaker Unified Studio IdC domains.	03/24/2026
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding cloudwatch:GetMetricData, SageMaker Feature store, LakeFormation data filter, SSO and Admin UI permission to SageMaker Unified Studio.	03/30/2026
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding cloudwatch:GetMetricData, notebook import and export functionality for permissive users SageMaker Feature store, and LakeFormation data filter for SageMaker Unified Studio. These permissions are applied to default IAM users.	03/30/2026

Change	Description	Date
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adds notebook import and export functionality for permissive users. These permissions are applied to default IAM users when using the permissive role.	03/30/2026
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adds SSO permissions for permissive admin policies. Also adds Admin and LakeFormation data filter permissions to permissive admin roles.	03/30/2026
Policy update - SageMakerStudioAdminIAMConsolePolicy	Policy updates to SageMakerStudioAdminIAMConsolePolicy - adding sso:DeleteApplication permission to allow deleting DataZone domain integrated with AWS IAM Identity Center. Adding KMS permissions required for IAM Identity Center instances that use customer managed keys for encryption.	03/30/2026

Change	Description	Date
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding iam:CreateServiceLinkedRole permission to allow creating the Amazon Athena service-linked role for Athena Spark workgroup provisioning.	03/09/2026
Policy update - SageMakerStudioDomainExecutionRolePolicy	Policy updates to SageMakerStudioDomainExecutionRolePolicy - adding support for the new API action - `QueryGraph` to enable graph-based entity search capabilities.	02/25/2026
Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to SageMakerStudioProjectRoleMachineLearningPolicy - adding permissions to support SageMaker Notebooks, Data Agent, and Airflow Serverless workflows	02/26/2026
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding permissions to pass roles to Amazon Athena for Athena Spark workgroup support	03/02/2026

Change	Description	Date
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to SageMakerStudioProjectUserRolePolicy - adding permissions to support Airflow Serverless	03/02/2026
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adding Amazon S3 Tables permissions to support integration with S3 table buckets IAM mode.	02/27/2026
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding Amazon S3 Tables permissions to support integration with S3 table buckets IAM mode.	02/27/2026
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding permissions to support integration with encrypted Identity Center instances	02/05/2026
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding permissions to support integration with MLflow App to track runs and experiments	01/27/2026

Change	Description	Date
Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to SageMakerStudioProjectRoleMachineLearningPolicy - adding permissions to support integration with MLflow App to track runs and experiments	01/27/2026
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions to support integration with MLflow App to track runs and experiments	01/27/2026
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding permissions to support integration with MLflow App to track runs and experiments	01/27/2026
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to SageMakerStudioProjectUserRolePolicy - adding permissions to support integration with SageMaker Unified Studio MCP.	11/21/2025
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to SageMakerStudioProjectUserRolePolicy - fix KMS permissions for integration with Scheduler.	11/20/2025

Change	Description	Date
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - fix KMS permissions for integration with Workflows, Scheduler, and DataZone Data Notebook.	11/18/2025
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - fix KMS permissions for integration with Workflows, Scheduler, and DataZone Data Notebook.	11/18/2025
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - fix KMS permissions for integration with Workflows, Scheduler, and DataZone Data Notebook.	11/18/2025
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - fix KMS permissions for integration with Workflows, Scheduler, and DataZone Data Notebook.	11/18/2025

Change	Description	Date
Policy update - SageMakerStudioAdminIAMConsolePolicy	Policy updates to SageMakerStudioAdminIAMConsolePolicy - adding KMS, CloudFormation and EC2 permissions for Amazon SageMaker Unified Studio.	11/14/2025
Policy update - SageMakerStudioUserIAMConsolePolicy	Policy updates to SageMakerStudioUserIAMConsolePolicy - removing pass role permissions.	11/14/2025
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding permissions for new APIs for SageMaker Unified Studio MCP, Airflow Serverless, and Athena sessions. Improve isolation for Glue and Athena sessions by making sure users can only access their own sessions.	11/14/2025
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adding permissions for new APIs for SageMaker Unified Studio MCP, Airflow Serverless, and Athena sessions. Improve isolation for Glue and Athena sessions by making sure users can only access their own sessions.	11/14/2025

Change	Description	Date
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions for new APIs for SageMaker Unified Studio MCP, Airflow Serverless, and Athena sessions. Improve isolation for Glue and Athena sessions by making sure users can only access their own sessions.	11/14/2025
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding permissions for new APIs for SageMaker Unified Studio MCP, Airflow Serverless, and Athena sessions. Improve isolation for Glue and Athena sessions by making sure users can only access their own sessions.	11/14/2025

Change	Description	Date
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding permissions to support integration with multiple services including Amazon EMR Serverless, Amazon Redshift, AWS Secrets Manager, AWS Lake Formation, Amazon SageMaker AI, Amazon S3, AWS CodeConnections, and AWS Glue. Adding KMS permissions to manage resources encrypted with CMK. Adding IAM CreateRole permission to allow creating new execution roles.	11/11/2025

Change	Description	Date
Policy update - SageMaker StudioAdminIAMPerm issiveExecutionPolicy	Policy updates to SageMaker StudioAdminIAMPerm issiveExecutionPolicy - adding permissions to support integration with multiple services including Amazon EMR Serverles s, Amazon Redshift, AWS Secrets Manager, AWS Lake Formation, Amazon SageMaker AI, Amazon S3, AWS CodeConnections, and AWS Glue. Adding KMS permissions to manage resources encrypted with CMK. Adding IAM CreateRole permission to allow creating new execution roles.	11/10/2025

Change	Description	Date
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions to support integration with multiple services including Amazon EMR Serverless, Amazon Redshift, AWS Secrets Manager, AWS Lake Formation, Amazon SageMaker AI, Amazon S3, AWS CodeConnections, and AWS Glue. Adding KMS permissions to manage resources encrypted with CMK. Adding IAM CreateRole permission to allow creating new execution roles.	11/10/2025

Change	Description	Date
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding permissions to support integration with multiple services including Amazon EMR Serverless, Amazon Redshift, AWS Secrets Manager, AWS Lake Formation, Amazon SageMaker AI, Amazon S3, AWS CodeConnections, and AWS Glue. Adding KMS permissions to manage resources encrypted with CMK. Adding IAM CreateRole permission to allow creating new execution roles.	11/10/2025
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - permissions updates for the following features: EMR on EKS compute capabilities, trusted identity propagation with user background sessions, AWS resource custom tags support, support default AWS Glue catalog encryption, Amazon SageMaker Unified Studio per project S3 bucket.	10/31/2025

Change	Description	Date
Policy update - SageMakerStudioEMRContainersSystemNamespaceRolePolicy	Policy updates to SageMakerStudioEMRContainersSystemNamespaceRolePolicy this revision refactors the scope of STS actions required for the EMR Containers service.	10/31/2025
New policy - SageMakerStudioEMRContainersSystemNamespaceRolePolicy	New policy - SageMakerStudioEMRContainersSystemNamespaceRolePolicy - Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the permissions related to Amazon EMR.	10/24/2025
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding `sagemaker:StartSession` to allow users to connect to a space from the local IDE. Also adding `glue:UntagResource` permission.	10/10/2025

Change	Description	Date
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding support for customers who opt-in to the Trusted Identity Propagation (TIP) feature, additional resources and configurations are required which require additional permissions, including LakeFormation IdentityCenterConfiguration resource permissions, AWS Glue IdentityCenterConfiguration resource permissions, EMR SecurityConfiguration `Describe` permission SSO resource permissions.	9/26/2025
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to SageMakerStudioProjectUserRolePolicy - restoring table tag visibility in the asset page of Amazon SageMaker Unified Studio for Amazon SageMaker unified domains.	9/18/2025
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to SageMakerStudioProjectUserRolePolicy - adding AWS Glue permissions to enable users to delete AWS Glue databases in their Amazon SageMaker Unified Studio projects.	9/12/2025

Change	Description	Date
Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to SageMakerStudioProjectRoleMachineLearningPolicy - adding support for the SageMaker:StartSession permission to enable remote connections to Amazon SageMaker spaces.	9/08/2025
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adding iam:CreateServiceLinkedRole permissions for resource management.	8/29/2025
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding iam:CreateServiceLinkedRole permissions for resource management.	8/29/2025
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding iam:CreateServiceLinkedRole permissions for resource management.	8/29/2025

Change	Description	Date
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding permissions iam:CreateServiceLinkedRole and s3:DeleteBucketPolicy for resource management.	8/29/2025
Policy update - SageMakerStudioDomainExecutionRolePolicy	Policy updates to SageMakerStudioDomainExecutionRolePolicy - adding support for the new API actions - AssociateGovernedTerms and DisassociateGovernedTerms for the asset classification using restricted glossary terms feature in the catalog where users can associate or disassociate restricted glossary terms to an asset.	8/20/2025
New policy - SageMakerStudioUserIAMPermissiveExecutionPolicy	This is an execution policy for using IAM roles with Amazon SageMaker Unified Studio. It grants access to users to access resources, including broad access to data resources.	8/20/2025

Change	Description	Date
New policy - SageMakerStudioAdminIAMPermissiveExecutionPolicy	This is an administrative execution policy for using IAM roles with Amazon SageMaker Unified Studio. It grants administrative access to provision, manage and access resources, including broad access to data resources.	8/20/2025
New policy - SageMakerStudioUserIAMDefaultExecutionPolicy	This is an execution policy for using IAM roles with Amazon SageMaker Unified Studio. It grants access to users to access resources, excluding access to data resources.	8/20/2025
New policy - SageMakerStudioAdminIAMDefaultExecutionPolicy	This is an administrative execution policy for using IAM roles with Amazon SageMaker Unified Studio. It grants administrative access to provision, manage and access resources in your account, excluding access to data resources.	8/20/2025

Change	Description	Date
New policy - SageMakerStudioAdminIAMConsolePolicy	This policy provides administrative and individual setup privileges for Amazon SageMaker Unified Studio using the AWS Management Console and SDK. It grants permissions for launching Amazon SageMaker Unified Studio.	8/20/2025
New policy - SageMakerStudioUserIAMConsolePolicy	This policy provides individual setup privileges for Amazon SageMaker Unified Studio using the AWS Management Console and SDK. It grants permissions for launching Amazon SageMaker Unified Studio.	8/20/2025
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding permissions to untag Amazon Athena, AWS CodeCommit, logs, scheduler, and Amazon EC2 resources. Also adding permissions to update Amazon Athena workgroups and delete the IAM role policy for Amazon SageMaker Unified Studio projects.	8/15/2025

Change	Description	Date
Policy update - SageMakerStudioDomainExecutionRolePolicy	Policy updates to SageMakerStudioDomainExecutionRolePolicy - adding support for the new API actions - AssociateGovernedTerms and DisassociateGovernedTerms for the asset classification via restricted glossary terms feature in the catalog where users can associate or disassociate restricted glossary terms to an asset.	8/11/2025
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - adding permissions to support Amazon SageMaker Unified Studio seamlessly for customers with Data Catalog Encryption. Also adding `STS:SetContext` permission to support trusted identity propagation for external computes. Also updaing CloudWatch log groups to be more specific.	7/30/2025

Change	Description	Date
Policy update - SageMaker StudioFullAccess	Policy update - generalizing the scope for SecretsManager `create` and `tag` permissio ns for new domains that will have the format of `dzd-` instead of `dzd_...` Also adding permissions to allow users to use custom blueprint templates from Amazon S3 as well as upload their own template files to Amazon S3.	7/23/2025
Policy update - SageMaker StudioEMRServiceRolePolicy	Policy update - removing unwanted KMS permissio ns for EMR cluster At RestEncryption in the Amazon SageMaker Unified Studio EmrOnEc2 blueprint and adding permissions for EMR clsuter to encrypt customer data using customer m anaged KMS for logs pushed to Amazon S3 bucket in Amazon SageMaker Unified Studio when using EmrOnEc2 blueprint with customer managed encryption.	7/23/2025
Policy update - SageMaker StudioProjectRoleMachineLea rningPolicy	Policy updates to the SageMa kerStudioProjectRoleMachine LearningPolicy - adding permissions to support cross-account Amazon S3 asset subscription fulfillment using Amazon S3 access grants.	7/23/2025

Change	Description	Date
Policy update - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding permissions to create and manage Amazon S3 table buckets and also adding permissions to automate S3 table analytics integration flow within Amazon SageMaker Unified Studio. Also adding permissions to read templates from users' S3 buckets and permissions to validate the template using AWS Cloud Formation. Also adding permissions to get and create an S3 access grant instance in the project account to support managing subscriptions for S3 asset types. Also adding `neptune-graph:*` and `s3vectors:*` permissions to support Knowledge Base vector store management of two new vector store services in Amazon SageMaker Unified Studio: S3Vectors vector buckets and Neptune Analytics graphs. Also adding permissions to allow cross-account project access for encrypted domains. And adding support for the	7/15/2025

Change	Description	Date
	data onboarding in Amazon SageMaker Unified Studio.	
Policy update - SageMaker StudioProjectUserRolePolicy	Policy update - adding permissions to allow deletion of AWS Glue databases in Amazon Datalake, adding `sqlworkbench` service principals for the `redshift-serverless:GetCredentials` action, adding permissions to fetch jobs based on tags and resources, adding permissions to update Amazon CloudWatch metrics from job runs and read/write job logs, and adding permissions to support Amazon S3 access grants. Also adding permissions to allow cross-account project access for encrypted domains and adding support for `ProjectRole` and `DescribeResource` actions in order to check for the Amazon S3 tables' Lake Formation registration.	7/15/2025

Change	Description	Date
New policy - SageMakerStudioAdminProjectUserRolePolicy	New policy - This IAM policy grants an IAM role full access to the AWS Glue Data Catalog (metadata) and Amazon S3 (actual data) for the data lake operations, with access scoped by region, account, and role tags.	7/15/2025
Policy update - SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy	Policy updates to the SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy - adding `neptune-graph:*` and `s3vectors:*` permissions to support vector read/write on vector stores for two new vector store services: S3Vectors vector buckets and Neptune Analytics graphs.	7/15/2025
Policy update - SageMakerStudioProjectUserRolePolicy	Policy update - adding permissions to access Amazon Athena default catalog resource.	6/25/2025

Change	Description	Date
Policy update - SageMakerStudioDomainExecutionRolePolicy	Policy updates to the SageMakerStudioDomainExecutionRolePolicy - adding support for the Amazon Q `GetIdentityMetadata` API action in order to obtain user's Q subscription information to set an appropriate subscription tier badge.	6/18/2025
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - bring back previously removed permission to `ListBucket` to fix issues in AWS Glue sessions and connections.	6/13/2025
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - adding permissions to list Amazon Bedrock foundation models. Removing permissions to terminate EMR Cluster, change security group rules, Amazon Athena default catalog permissions, and list S3 buckets permissions at bucket level.	6/13/2025

Change	Description	Date
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding the untag role permission to fix project update failure. Also adding permissions to integrate with Amazon QuickSight. Also optimizing to reduce the policy size. And adding permissions to enable automatic sync of repositories.	6/04/2025
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - removing RedshiftDbUser format restriction. Adding KMS permissions required by dependent services for Federated Data Connection. Adding permissions to support Amazon QuickSight integration.	6/04/2025

Change	Description	Date
Policy update - AmazonDataZoneBedrockModelConsumptionPolicy	Policy updates to the AmazonDataZoneBedrockModelConsumptionPolicy - adding permissions to call the `ListFoundationModels` action. This permission is added to help get model metadata more programmatically when the user is selecting which models to invoke.	5/28/2025
Policy update - SageMakerStudioFullAccess	Policy updates to the SageMakerStudioFullAccess - adding permissions to support attaching or updating AWS managed permissions in AWS RAM resource shares in the Amazon SageMaker console.	5/22/2025
Policy update - AmazonDataZoneBedrockModelConsumptionPolicy	Policy updates to the AmazonDataZoneBedrockModelConsumptionPolicy - adding support for the conversation history feature powered by Amazon Bedrock session management in generative AI playgrounds.	5/13/2025

Change	Description	Date
Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to the SageMakerStudioProjectRoleMachineLearningPolicy - as CodeEditor (VS Code) is introduced into Amazon SageMaker Unified Studio, users need the ability to create/delete CodeEditor space applications in Amazon SageMaker. Currently, only Amazon SageMaker space apps are allowed to be created with the JupyterLab app type. This change extends the current capability of creating/deleting JupyterLab space applications to CodeEditor (VS Code).	5/01/2025

Change	Description	Date
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding IAM permissions for the AmazonSageMakerQueryExecution role to support query execution role creation during enabling of the Toolin g blueprint. Adding the DeleteSchedule permissio n so that when projects are deleted, the Schedule Group can be deleted. EventBrid ge runs DeleteSchedule automatically on Schedule Groups when it attempts to delete them, regardles s of whether the Schedule Group actually has schedules in it. This permission allows for that deleteSchedule call to be made during project deletion.	4/28/2025

Change	Description	Date
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - adding permissions for integration with Amazon Bedrock Data Automation. Adding permissions to show Amazon Bedrock agent versions and their details to users. Adding permission to support Trusted Identity Propagation in QEv2. Ensuring project isolation for Amazon Bedrock Inline Agents.	4/28/2025
Policy update - SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy	Policy updates to the SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy - adding support for structured data sources in Amazon Bedrock knowledge bases for generative AI app development projects.	4/16/2025
Policy update - SageMakerStudioBedrockFlowServiceRolePolicy	Policy updates to the SageMakerStudioBedrockFlowServiceRolePolicy - adding support for using Amazon Bedrock agent nodes in Amazon Bedrock flows for generative AI app development projects.	4/09/2025

Change	Description	Date
Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - preventing sharing provisioned Amazon Redshift-Serverless across all projects. Adding EventBridge Scheduler permissions for users to create schedules in the project schedule group. Adding permissions to handle Amazon SageMaker Studio migration to Amazon SageMaker Unified Studio. Adding support for the Amazon SageMaker App type CodeEditor.	4/09/2025

Change	Description	Date
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding `lakeformation:DescribeResource` to improve deregistering of federated connections. Adding EventBridge Scheduler permissions to manage a schedule group for each project. Adding permission to manage Amazon Bedrock resources directly from the Amazon DataZone service. Add support for the Amazon SageMaker App type CodeEditor.	4/09/2025
Policy update - SageMakerStudioDomainExecutionRolePolicy	Policy updates to the SageMakerStudioDomainExecutionRolePolicy - adding support for the GetUpdateEligibility API required by Amazon SageMaker Unified Studio to fetch update comments and determine project's eligibility for the workflow of updating projects. Also adding support for the existing Amazon DataZone Rule APIs required by Amazon SageMaker Unified Studio to mange and enforce rules.	3/25/2025

Change	Description	Date
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - preventing default AWS Glue database from being listed as it causes issues with Spark SQL. Also adding permission to use new project-wide Amazon Bedrock service role for improved scalability.	3/21/2025
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding permission to describe stack event for better error reporting.	3/21/2025
Policy update - SageMakerStudioBedrockFlowServiceRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding KMS permissions to decrypt Amazon Bedrock guardrails attached to the Amazon Bedrock flows.	3/10/2025

Change	Description	Date
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding permission to change trust policy during project update to address confused deputy problem. Also adding permission to attach PartnerApps policy to the user role.	3/05/2025
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding support for ProjectUpdate for EMR Serverless blueprint to proactively notify users on invalid updates on EMR Serverless application.	3/04/2025
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - renaming Amazon Bedrock tag and adding permission to remove deprecated tag on roles.	2/28/2025
Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to the SageMakerStudioProjectRoleMachineLearningPolicy - adding support for the MLFlow Tracking Server for Shared VPC, applying visibility condition to Amazon SageMaker Search API.	2/28/2025

Change	Description	Date
Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - changes to support shared VPC by removing ResourceAccount condition on actions dependent on VPC/subnets. Moving permissions from inline to this AWS managed policy for Amazon EMR, EMR-Serverless, and federated connections. Adding support for buckets with public access blocked with permission `s3:GetBucketPublicAccessBlock` . Adding permission to support data lineage in Amazon DataZone. Supporting Amazon LakeFormation ABAC by adding session tag the access role. Supporting users operating on private ECR. Also adding support for managing AWS Glue subscriptions by the user.	2/28/2025
Policy update - SageMaker StudioEMRServiceRolePolicy	Policy updates to the SageMakerStudioEMRServiceRolePolicy - adding permissions to allow Amazon EMR to create network interfaces against Shared VPC.	2/28/2025

Change	Description	Date
New policy - SageMakerStudioEMRInstanceRolePolicy	Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, artificial intelligence, and machine learning actions and uses this policy when creating these roles to define the permissions related to EMR.	2/28/2025
New policy - SageMakerStudioBedrockFunctionExecutionRolePolicy	This policy allows AWS Lambda to access an Amazon Bedrock function component's configuration in Amazon SageMaker Unified Studio.	2/25/2025
New policy - SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy	This policy provides access to configure vector stores and Amazon Bedrock knowledge bases in Amazon SageMaker Unified Studio.	2/25/2025
New policy - SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy	This policy allows Amazon Bedrock Knowledge Bases to access Amazon Bedrock models and data sources in Amazon SageMaker Unified Studio.	2/25/2025

Change	Description	Date
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding permissions for batch grants in AWS LakeFormation to give grants to IDC users. Adding various `Update*` permissions to allow managing project resources . Removing `ResourceAccount` condition on resources depending on VPC to allow usage of shared VPC. Using new Amazon Bedrock managed policy name. Adding permissions to clean up Amazon EMR project level resources during project deletion.	2/24/2025
New policy - SageMakerStudioBedrockEvaluationJobServiceRolePolicy	This policy allows Amazon Bedrock to access Amazon Bedrock models and datasets for evaluation jobs in Amazon SageMaker Unified Studio.	2/14/2025
New policy - SageMakerStudioBedrockPromptUserRolePolicy	This policy provides access to an Amazon Bedrock prompt and its configuration in Amazon SageMaker Unified Studio.	2/14/2025

Change	Description	Date
New policy - SageMakerStudioBedrockFlowServiceRolePolicy	This policy allows Amazon Bedrock Flows to access Amazon Bedrock models and other resources attached to a flow in Amazon SageMaker Unified Studio.	2/14/2025
New policy - SageMakerStudioBedrockChatAgentUserRolePolicy	This policy provides access to an Amazon Bedrock chat agent app's configuration and Amazon Bedrock agent in Amazon SageMaker Unified Studio.	2/14/2025
New policy - SageMakerStudioBedrockAgentServiceRolePolicy	This policy allows Amazon Bedrock Agents to access Amazon Bedrock models and other resources attached to an agent in Amazon SageMaker Unified Studio.	2/14/2025
Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to the SageMakerStudioProjectRoleMachineLearningPolicy - adding permission for `DescribeAutoMLJobV2`, moving multiple Amazon SageMaker `List` operations to tag based authorization, adding CMK permissions for JupyterLab, add Amazon SageMaker `ListModelPackages` and `CreateModel` permissions for cross-account use case.	2/14/2025

Change	Description	Date
New Policy - SageMaker StudioEMRServiceRolePolicy	New policy SageMaker StudioEMRServiceRolePolicy - Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, artificial intellige nce, and machine learning actions and uses this policy when creating these roles to define the permissions related to Amazon EMR.	1/31/2025
New Policy - SageMaker StudioQueryExecutionRolePol icy	New policy SageMaker StudioQueryExecutionRolePol icy - this is the default policy for the SageMakerQueryExec utionRole role. This policy provides permissions to run query executions on federated connections.	1/31/2025
Policy update - SageMaker StudioProjectProvisioningRo lePolicy	Policy updates to SageMaker StudioProjectProvisioningRo lePolicy - adding permissio ns to manage IAM roles with only AWS managed policies attached to them and no permissions boundary. Also adding permissions to update the AWS Lambda function for Amazon Athena federated connections.	1/31/2025

Change	Description	Date
Policy update - SageMaker StudioFullAccess	Policy updates to SageMaker StudioFullAccess - updating the CodeConnections tagging permissions to support tagging for CodeConnections host resources in the Amazon SageMaker console.	1/24/2025
Policy update - SageMaker StudioDomainExecutionRolePolicy	Policy updates to SageMaker StudioDomainExecutionRolePolicy - adding support for the AWS CodeConnections APIs in order to make the Copy button available for self-managed Git providers.	1/24/2025
Policy updates to SageMaker StudioProjectProvisioningRolePolicy	Policy updates to SageMaker StudioProjectProvisioningRolePolicy - adding permissions to support CMK in CodeCommit, AWS Glue Catalog, and Amazon Redshift Serverless.	12/18/2024
Policy updates to SageMaker StudioProjectUserRolePolicy.	Policy updates to SageMaker StudioProjectUserRolePolicy - adding permissions to support CMK in CodeCommit, and AWS Glue Catalog.	12/18/2024

Change	Description	Date
Policy updates to SageMakerStudioProjectUserRolePermissionsBoundary	Policy updates to SageMakerStudioProjectUserRolePermissionsBoundary - adding permissions to support CMK in CodeCommit, AWS Glue Catalog, Amazon Redshift Serverless, and EMR on EC2.	12/18/2024
New policy - SageMakerStudioFullAccess	Adding a new managed policy - this policy provides full access to Amazon SageMaker Unified Studio via the Amazon SageMaker management console.	12/02/2024
New policy - SageMakerStudioProjectUserRolePermissionsBoundary	Adding a new managed policy - SageMakerStudioProjectUserRolePermissionsBoundary. Amazon SageMaker Unified Studio creates IAM roles for Projects users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the boundary of their permissions.	12/02/2024

Change	Description	Date
New policy - SageMakerStudioProjectProvisioningRolePolicy	Adding a new managed policy - SageMakerStudioProjectProvisioningRolePolicy. Amazon SageMaker Unified Studio uses this policy to provision and manage resources in your account.	12/02/2024
New policy - SageMakerStudioDomainExecutionRolePolicy	Adding a new managed policy - SageMakerStudioDomainExecutionRolePolicy - Default policy for the SageMakerUnifiedStudioDomainExecutionRole service role. This role is used by Amazon SageMaker Unified Studio to catalog, discover, govern, share, and analyze data in the Amazon SageMaker Unified Studio domain.	12/02/2024

Change	Description	Date
New policy - SageMaker StudioDomainServiceRolePolicy	Adding a new managed policy - SageMakerStudioDomainServiceRolePolic. This is the default policy for the SageMakerUnifiedStudioDomainServiceRole service role. This policy is used by Amazon SageMaker Unified Studio to access the SSM parameters in the user's account. Those parameters are set by the administrator in the Amazon SageMaker Unified Studio project profiles. This policy also has permissions to AWS KMS for encrypted SSM parameters. The KMS key must be tagged with EnableKeyForAmazonDataZone to allow decrypting the SSM parameters.	12/02/2024
New policy - SageMaker StudioProjectUserRolePolicy	Adding a new managed policy - SageMakerStudioProjectUserRolePolicy. Amazon SageMaker Unified Studio creates IAM roles for projects users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the permissions.	12/02/2024

Change	Description	Date
New policy - SageMakerStudioProjectRoleMachineLearningPolicy	Adding a new managed policy - SageMakerStudioProjectRoleMachineLearningPolicy. Amazon SageMaker Unified Studio creates IAM roles for projects users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the permissions.	12/02/2024
New policy - AmazonDataZoneBedrockModelManagementPolicy	Adding a new managed policy - AmazonDataZoneBedrockModelManagementPolicy - that provides permissions to manage Amazon Bedrock model access, including creating, tagging and deleting application inference profiles.	12/02/2024
New policy - AmazonDataZoneBedrockModelConsumptionPolicy	Adding a new managed policy - AmazonDataZoneBedrockModelConsumptionPolicy - that provides permissions to consume Amazon Bedrock models, including invoking Amazon Bedrock application inference profile created for particular Amazon DataZone domain.	12/02/2024

Change	Description	Date
Amazon SageMaker Unified Studio started tracking changes	Amazon SageMaker Unified Studio started tracking changes for its AWS managed policies.	December 2nd, 2024

IAM roles for Amazon SageMaker Unified Studio

Topics

- AmazonSageMakerDomainExecution role
- AmazonSageMakerDomainService role
- AmazonSageMakerManageAccess-<region>-<domainId> role
- AmazonSageMakerProvisioning-<domainAccountId> role
- AmazonDataZoneBedrockModelManagementRole
- AmazonDataZoneBedrockFMConsumptionRole
- AmazonSageMakerQueryExecution

AmazonSageMakerDomainExecution role

The AmazonSageMakerDomainExecution role has the AWS policy: SageMakerStudioDomainExecutionRolePolicy attached. This is an IAM role that Amazon SageMaker Unified Studio requires to call APIs on behalf of authorized users, including those logged in to Amazon SageMaker Unified Studio.

The default `AmazonSageMakerDomainExecution` role has the following trust policy attached:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Principal": {
```

```
                "Service": "datazone.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:TagSession",
                "sts:SetContext"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{{source_account_id}}"
                },
                "ForAllValues:StringLike": {
                    "aws:TagKeys": "datazone*"
                }
            }
        }
    ]
}
```

AmazonSageMakerDomainService role

The AmazonSageMakerDomainService role has the AWS policy: SageMakerStudioDomainServiceRolePolicy attached. This is a service role for domain level actions performed by Amazon SageMaker Unified Studio.

The default `AmazonSageMakerDomainService` role has the following trust policy attached:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

AmazonSageMakerManageAccess-<region>-<domainId> role

AmazonSageMakerManageAccess-<region>-<domainId> role grants Amazon SageMaker Unified Studio permissions to publish, grant access, and revoke access to Amazon SageMaker Lakehouse, AWS Glue Data Catalog and Amazon Redshift data. It also grants Amazon SageMaker Unified Studio access to publish and manage subscriptions on Amazon SageMaker Catalog data and AI assets.

AmazonSageMakerManageAccess-<region>-<domainId> role has the following Amazon DataZone managed policies attached:

- AmazonDataZoneGlueManageAccessRolePolicy
- AmazonDataZoneRedshiftManageAccessRolePolicy
- AmazonDataZoneSageMakerAccess

The default `AmazonSageMakerManageAccess-<region>-<domainId>` role has the following inline policy attached:

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
```

```
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

The default `AmazonSageMakerManageAccess-<region>-<domainId>` role has the following trust policy attached:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "datazone.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": "111122223333"
                },
                "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:us-east-1:111122223333:domain/
dzd-12345"
                }
            }
        }
    ]
}
```

AmazonSageMakerProvisioning-<domainAccountId> role

AmazonSageMakerProvisioning-<domainAccountId> role is used by Amazon SageMaker Unified Studio to provision and manage resources defined in the selected blueprints in your account.

AmazonSageMakerProvisioning-<domainAccountId> role has the AWS policy: SageMakerStudioProjectProvisioningRolePolicy attached.

The default `AmazonSageMakerProvisioning-<domainAccountId>` role has the following trust policy attached:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

Important

If you are using your own query execution role (instead of the default AmazonSageMakerQueryExecution role), then you must modify the permissions of your provisioning role (whether you're using this default AmazonSageMakerProvisioning role or your own custom provisioning role) to include `iam:PassRole` and `iam:GetRole` permissions. These permissions enable your provisioning role to pass the query execution role to AWS LakeFormation during creation of federated connections. You can include these permissions by attaching the following inline policy to your provisioning role:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "IamRolePermissionsForQueryExecution",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/{your-role}"
    }
  ]
}
```

AmazonDataZoneBedrockModelManagementRole

Amazon SageMaker Unified Studio uses this role to create an inference profile for an Amazon Bedrock model in a project. The inference profile is required for the project to interact with the model. You can either let Amazon SageMaker Unified Studio automatically create a unique provisioning role, or you can provide a custom provisioning role.

The AmazonDataZoneBedrockModelManagementRole has the AWS policy: AmazonDataZoneBedrockModelManagementPolicy attached.

The default `AmazonDataZoneBedrockModelManagementRole` has the following trust policy attached:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
          "Service": "datazone.amazonaws.com"
      },
      "Action": [
           "sts:AssumeRole",
           "sts:SetContext"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{accountId}}"
        }
      }
    }
  ]
}
```

AmazonDataZoneBedrockFMConsumptionRole

A consumption role is required for each Amazon Bedrock model that you want to enable in the playground for non-builders. Amazon SageMaker Unified Studio can create a consumption role per model by default or you have the option to configure a single existing consumption role for all models.

The AmazonDataZoneBedrockFMConsumptionRole has the AWS policy: AmazonDataZoneBedrockModelConsumptionPolicy attached.

The default `AmazonDataZoneBedrockFMConsumptionRole` has the following inline policy attached:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowInferenceProfileToInvokeFoundationModels",
            "Effect": "Allow",
            "Action": [
```

```
                "bedrock:InvokeModel",
                "bedrock:InvokeModelWithResponseStream"
            ],
            "Resource": [
                "arn:aws:bedrock:us-east-1::foundation-model/{{modelId}}"
            ],
            "Condition": {
                "ArnLike": {
                    "bedrock:InferenceProfileArn":
 "arn:aws:bedrock:*:111122223333:application-inference-profile/*"
                }
            }
        }
    ]
}
```

The default `AmazonDataZoneBedrockFMConsumptionRole` has the following trust policy attached:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "Service": "datazone.amazonaws.com"
      },
      "Action": [
           "sts:AssumeRole",
           "sts:SetContext"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{accountId}}"
        }
      }
    }
  ]
```

```
}
```

AmazonSageMakerQueryExecution

This role is used while running a query execution. AWS LakeFormation assumes this role to vend credentials needed by Amazon Athena during query execution.

The AmazonSageMakerQueryExecution role has the AWS policy: SageMakerStudioQueryExecutionRolePolicy attached.

The default `AmazonSageMakerQueryExecution` role has the following trust policy attached:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
                    "lakeformation.amazonaws.com",
                    "glue.amazonaws.com"
                ]
      },
      "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{source_account}}"
        }
      }
    }
  ]
}
```

Important

If you are using your own query execution role (instead of this default AmazonSageMakerQueryExecution role), then you must modify the permissions of your provisioning role (whether you're using this default AmazonSageMakerProvisioning-<domainAccountId> role role or your own custom provisioning role) to include `iam:PassRole` and `iam:GetRole` permissions. These permissions enable your provisioning role to pass the query execution role to AWS LakeFormation during creation of federated connections. You can include these permissions by attaching the following inline policy to your provisioning role:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "IamRolePermissionsForQueryExecution",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/{your-role}"
    }
  ]
}
```

Access control patterns Amazon SageMaker Unified Studio

Effective data management and governance are crucial to deriving value from data assets while maintaining compliance and security. In Amazon SageMaker Unified Studio, you can use projects to simplify development and collaboration. Projects contain one or more IAM roles, and there is at least one project role for each account in which the project has resources. You have access to all the tools, compute, data, and AIML assets this role has access to. When you access a project from Amazon SageMaker Unified Studio, it is equivalent to logging into an account in a specific

region and assuming one of the project's roles. There are two ways to manage what these roles have access to. First, you can simply add the IAM permissions directly to the project's IAM role. Second, you can publish data and AI/ML assets to the Amazon SageMaker catalog and enable project members to subscribe to those assets. Both of these approaches are covered in this section.

Topics

- Using IAM to configure access in Amazon SageMaker Unified Studio
- Data access and subscription workflows using Amazon SageMaker catalog

Using IAM to configure access in Amazon SageMaker Unified Studio

In Amazon SageMaker Unified Studio, a domain is the fundamental organizational unit that enables you to manage multiple AWS Regions, accounts, and workloads through a single interface. Each domain has its own unique URL and provides centralized management of studio settings, accounts, users, and network configurations.

Within domains, projects streamline and enable collaboration. Projects can be located in different regions or in different accounts within a given region. Project metadata contains information about the project's git repository, members, and their permissions. There is at least one project role for each account in which the project has resources. The project IAM role defines what tools, compute resources, data, and AI/ML assets project members can access. You can think of entering a project in Amazon SageMaker Unified Studio as logging into a regional account where you take on a designated role. To manage access to data, you can simply modify the IAM permissions to the project's IAM role.

It is important that you understand the different IAM roles used in Amazon SageMaker Unified Studio and their functions in detail. This section covers those details. When you modify an IAM role to manage data access, you must factor in the region, account, and role you need to give permissions to. For more information on simplifying configuring permissions and customizing role assignments, see the AWS IAM Roles section in "Bringing existing resources into Amazon SageMaker Unified Studio".

Domain execution role - the AmazonSageMakerDomainExecution role is an IAM role that enables Amazon SageMaker Unified Studio to execute API calls on behalf of authorized users. It provides access to all APIs that are required for Amazon SageMaker Unified Studio to use, as well as RAM permissions to support usage of associated accounts in an Amazon SageMaker unified domain. It also provides access to services used outside of a project scope, including AWS CodeConnections, Amazon Q, AWS Systems Manager, and Amazon Bedrock.

Service role - the AmazonSageMakerDomainService role is a specialized service role that enables domain-level actions in Amazon SageMaker Unified Studio. It is responsible for managing critical operations within the domain, particularly the handling of blueprint parameters in Systems Manager (SSM). These parameters are essential for executing privileged calls, ensuring secure and controlled access to domain-level functionalities.

Provisioning Role - Amazon SageMaker Unified Studio employs an IAM policy to manage and provision resources across various AWS services within an AWS account. This policy, associated with the AmazonSageMakerProvisioning role, grants access to essential services such as Amazon SageMaker, AWS Glue, Amazon S3, AWS Lake Formation, Amazon Redshift, Amazon Athena, Amazon Q, Amazon EMR, AWS CodeCommit, Amazon Bedrock, and AWS IAM. The policy enables management of SageMaker Domains and Spaces, AWS Glue components, S3 objects, Lake Formation grants, Redshift workgroups, Athena workgroups and catalogs, EMR clusters, KMS keys, CodeCommit repositories, Secrets Manager secrets, IAM roles, and Amazon Bedrock in SageMaker Unified Studio resources. This access allows Amazon SageMaker Unified Studio to effectively orchestrate and manage the lifecycle of projects and resources across the AWS ecosystem, providing users with a seamless and integrated experience for data science and machine learning tasks.

Manage Access Role - the AmazonSageMakerManageAccess role is designed to manage access and permissions across various data services. This role enables Amazon SageMaker Unified Studio to publish, grant, and revoke access to data within Amazon SageMaker Lakehouse, AWS Glue Data Catalog, and Amazon Redshift. Additionally, it facilitates the management of subscriptions for data and AI assets in the Amazon SageMaker catalog. To achieve these functionalities, the role incorporates three Amazon DataZone managed policies: AmazonDataZoneGlueManageAccessRolePolicy, AmazonDataZoneRedshiftManageAccessRolePolicy, and AmazonDataZoneSageMakerAccess. These policies collectively provide the necessary permissions for seamless data management and access control, ensuring efficient collaboration and resource utilization across different AWS services.

Project role - Amazon SageMaker Unified Studio creates IAM roles that enable project users to perform data analytics, AI, and machine learning tasks. There are two IAM policies governing these permissions: SageMakerStudioProjectUserRolePolicy and SageMakerStudioProjectRoleMachineLearningPolicy. This role grants users read and write access to relevant AWS services including Amazon SageMaker, AWS Glue, Amazon S3, AWS Lake Formation, Amazon Redshift, Amazon Athena, Amazon Q, and Amazon EMR. Additionally, it provides necessary permissions for infrastructure resources such as network interfaces, AWS KMS keys, AWS CodeCommit, and AWS Secrets Manager. Administrators maintain granular control over

these permissions through role tagging. The tag 'EnableGlueWorkloadsPermissions' controls AWS Glue workload permissions (Sessions, Blueprints, Jobs, Data Quality Rulesets, and Workflows), the tag 'EnableAmazonBedrockPermissions' controls Amazon Bedrock permissions, and the tag 'EnableSageMakerMLWorkloadsPermissions' controls SageMaker ML workload permissions (training jobs, processing jobs, and model deployment).

> **Note**
>
> You can't create new projects with AWS CodeCommit. Existing projects that were created using CodeCommit will continue to work.

Amazon Bedrock service role - in each Generative AI app development project, Amazon SageMaker Unified Studio creates an IAM role that allows the Amazon Bedrock service to access generative AI application resources in the project. This role governs the access and permissions for various Amazon Bedrock components within Amazon SageMaker Unified Studio. It encompasses four main service roles: Amazon Bedrock Agent, Amazon Bedrock Knowledge Base, Amazon Bedrock Flows, and Amazon Bedrock Evaluation. Each role is designed to grant specific permissions to Amazon Bedrock services, allowing them to interact with relevant resources such as Amazon Bedrock models, AWS Lambda functions, Amazon S3 buckets, AWS KMS keys, and OpenSearch Serverless collections. The policies ensure that Amazon Bedrock Agents, Knowledge Bases, Flows, and Evaluations can access necessary resources while maintaining security through project-specific tag restrictions. These roles enable seamless integration of Amazon Bedrock capabilities with Amazon SageMaker Unified Studio, facilitating tasks like model invocation, data access, encryption, and resource management within the confines of each project's scope. This structured approach ensures efficient operation of Amazon Bedrock services while maintaining appropriate access controls and resource isolation. This role is attached with the following AWS managed policies:

- AWS policy: SageMakerStudioBedrockAgentServiceRolePolicy
- AWS policy: SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy
- AWS policy: SageMakerStudioBedrockFlowServiceRolePolicy
- AWS policy: SageMakerStudioBedrockEvaluationJobServiceRolePolicy

Amazon Bedrock Lambda execution role - in each Generative AI app development project, Amazon SageMaker Unified Studio creates an IAM role that allows the AWS Lambda service to access generative AI application resources in the project. This role encompasses two key roles

within Amazon SageMaker Unified Studio: the Amazon Bedrock Knowledge Base custom resource service role and the Amazon Bedrock function execution role. The knowledge base custom resource role enables configuration of vector stores and Amazon Bedrock knowledge bases, granting AWS Lambda-backed CloudFormation custom resources access to Amazon Bedrock knowledge bases and OpenSearch Serverless collections. It allows for starting and querying knowledge base ingestion jobs and preparing OpenSearch collections. It permits AWS Lambda to access Amazon Bedrock function component configurations, including Secrets Manager secrets and KMS keys, which are necessary for handling API requests. Additionally, this role provides write permissions to CloudWatch Logs for monitoring and logging purposes. This facilitates the seamless integration and management of Amazon Bedrock components within the Amazon SageMaker Unified Studio while maintaining appropriate access controls. This role is attached with the following AWS managed policies:

- AWSLambdaBasicExecutionRole
- AWS policy: SageMakerStudioBedrockFunctionExecutionRolePolicy
- AWS policy: SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

Amazon Bedrock chat agent user role - in each Amazon Bedrock chat agent, Amazon SageMaker Unified Studio creates an IAM role that allows the Amazon DataZone service to provide shared users access to an Amazon Bedrock chat agent app's configuration and Amazon Bedrock chat agent. As part of the AmazonBedrockChatAgent blueprint, it defines the main policy for the Amazon Bedrock chat agent user role. It grants users the ability to interact with shared Amazon Bedrock chat agent apps, including invoking Amazon Bedrock chat agents, retrieving configurations from Amazon S3, and utilizing AWS KMS keys for encryption. It provides necessary permissions for users to read and invoke Amazon Bedrock chat agents, access specific S3 objects within the project's bucket, and use KMS keys for encrypted data access. The role is designed to allow access only to individually shared Amazon Bedrock chat agent apps, maintaining security by restricting domain and project users from modifying user role tags. It ensures that users can effectively utilize Amazon Bedrock chat agent applications while adhering to appropriate access controls and data protection measures. This role is attached with the following AWS managed policies:

Amazon Bedrock prompt user role - in each Amazon Bedrock prompt, Amazon SageMaker Unified Studio creates an IAM role that allows the Amazon DataZone service to provide shared users access to an Amazon Bedrock prompt and its configuration. It defines the access permissions for users of Amazon Bedrock prompts within Amazon SageMaker Unified Studio. As part of the AmazonBedrockPrompt blueprint, it serves as the main policy for the Amazon Bedrock prompt

user role. It grants users access to shared Amazon Bedrock prompts, including the ability to read Amazon Bedrock prompts, access their configurations stored in Amazon S3, and use AWS KMS keys for encryption. It provides necessary permissions for users to interact with Amazon Bedrock prompts, retrieve specific objects from the project's S3 bucket, and utilize KMS keys for encrypted data access. It is designed to allow access only to individually shared Amazon Bedrock prompts, maintaining security by restricting domain and project users from modifying user role tags. This ensures that users can effectively work with Amazon Bedrock prompts while adhering to appropriate access controls and data protection measures within Amazon SageMaker Unified Studio.

Query execution role for federated connection - this role is used when executing a query using Amazon Athena. AWS LakeFormation assumes this role to vend credentials needed by Amazon Athena during query execution. The SageMakerQueryExecutionRole has the AWS policy: SageMakerStudioQueryExecutionRolePolicy attached.

EMR Service role - this role defines the necessary permissions for Amazon EMR instances running on EC2, ensuring secure and controlled access to EC2 networking, IAM roles, and AWS KMS for encryption. It grants permissions to create network interfaces and launch instances, restricting these actions to VPCs that match the principal’s VPC ID tag. To support secure data handling, it provides AWS KMS encryption and decryption permissions for a specified KMS key, allowing EMR instances to manage encrypted data and EBS volumes. It also enables EMR to manage KMS grants, including listing, revoking, and describing keys, specifically for EC2 services within the same AWS account. Furthermore, the policy permits EMR to list KMS key aliases, ensuring seamless access to encryption keys. This policy ensures that EMR instances operate within a well-defined network, securely handle encrypted data, and adhere to account-specific security constraints.

EMR Instance Profile role - this role grants permissions necessary for Amazon EMR instances operating within Amazon SageMaker Unified Studio, ensuring secure access to S3, IAM, and KMS resources. It allows EMR instances to retrieve SSL certificates from an S3 bucket, ensuring secure communication, and access patching RPMs stored in a predefined S3 location. Additionally, it permits retrieval of bootstrap action scripts from S3, enabling customized EMR cluster configurations, and allows the uploading of EMR cluster logs to a designated S3 location for monitoring and debugging purposes. The role also enables EMR instances to assume runtime roles with specific session tags, ensuring authorized access to Lake Formation resources. Furthermore, it grants permissions for AWS KMS operations, including encryption, decryption, and key generation, allowing secure handling of sensitive data and EBS volume encryption. By enforcing conditions based on resource ownership, principal tags, and account constraints, this IAM role ensures that

EMR clusters operate securely within a well-defined Amazon DataZone framework, maintaining compliance and access control best practices.

Partner Apps IAM role - this role enables Amazon SageMaker partner app users to access applications, list available applications, launch application web UIs, and connect via the application SDK. Access is restricted to partner apps owned by the same AWS account as the requesting principal (enforced by the aws:ResourceAccount condition). This ensures that the user can only interact with partner apps within their own AWS account, preventing cross-account access.

Data access and subscription workflows using Amazon SageMaker catalog

You get a comprehensive framework for data discovery, subscription, and consumption through the Amazon SageMaker catalog. It enables seamless collaboration between data publishers and subscribers, facilitating controlled access to valuable data assets across an organization. By implementing a structured process for asset discovery, subscription requests, and approval workflows, Amazon SageMaker Unified Studio ensures that data access is granted based on justified needs and adheres to organizational policies.

Once an asset is published to a domain, subscribers can discover and request a subscription to this asset. The subscription process begins with a subscriber searching for and browsing the catalog to discover an asset they want. From Amazon SageMaker Unified Studio, they choose to subscribe to the asset by submitting a subscription request that includes justification and the reason for the request. The subscription approver then reviews the access request. They can either approve or reject the request. After a subscription is granted, a fulfillment process starts to facilitate access to the asset for the subscriber. For more information, see Request subscription to assets in Amazon DataZone.

In Amazon SageMaker catalog, subscription requests to assets are managed by subscription approvers. A subscription approver for an asset is determined by the publishing agreement with which this asset was published into the Amazon SageMaker catalog. For some assets, Amazon SageMaker catalog can manage access grants and auto-approve subscription requests. These assets are called managed assets and include Lake Formation-managed AWS Glue Data Catalog tables and Amazon Redshift tables and views. Alternatively, for manual approvals, Amazon SageMaker catalog kicks of a workflow via an EventBridge integration so the subscription approver can review and approve/reject the request. After a subscription is granted, Amazon SageMaker catalog starts a fulfillment process starts to facilitate access to the asset for the subscriber and takes care of managing and orchestrating the permissions setup across regions and accounts. To learn more about how Amazon SageMaker catalog facilitates asset discovery, subscription requests,

approval processes, and access controls, see Amazon DataZone data discovery, subscription, and consumption.

Troubleshooting Amazon SageMaker Unified Studio identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon SageMaker Unified Studio and IAM.

Topics

- I am not authorized to perform an action in Amazon SageMaker Unified Studio
- I am not authorized to perform iam:PassRole
- I want to allow people outside of my AWS account to access my Amazon SageMaker Unified Studio resources

I am not authorized to perform an action in Amazon SageMaker Unified Studio

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional *`my-example-widget`* resource but doesn't have the fictional `:`*`GetWidget`* permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: :GetWidget on resource: my-example-widget
```

In this case, the policy for the `mateojackson` user must be updated to allow access to the *`my-example-widget`* resource by using the `:`*`GetWidget`* action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Amazon SageMaker Unified Studio.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Amazon SageMaker Unified Studio. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my Amazon SageMaker Unified Studio resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon SageMaker Unified Studio supports these features, see How Amazon SageMaker Unified Studio works with IAM.
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

Data protection in Amazon SageMaker Unified Studio

The AWS shared responsibility model applies to data protection in Amazon SageMaker Unified Studio. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see Data Privacy FAQ. For information about data protection in Europe, see the General Data Protection Regulation (GDPR) Center.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail. For information about using CloudTrail trails to capture AWS activities, see Working with CloudTrail trails in the *AWS CloudTrail User Guide*.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Amazon SageMaker Unified Studio or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

For more information about data protection, inluding data encryption, encryption at rest, encryption in transit, key management, and inter-network traffic privacy for various AWS services that inter-operate with Amazon SageMaker Unified Studio, see the following:

- Data Protection in Amazon SageMaker
- Data Protection in Amazon Managed Workflows for Apache Airflow
- Data protection in Amazon Redshift
- Data protection in Amazon EMR
- Data protection in Amazon DataZone
- Data protection in Amazon Q Business and Data protection in Amazon Q Developer
- Data protection in Athena
- Data protection in Amazon Bedrock
- Data protection in AWS Glue

KMS Permissions for resources provisioned by Amazon SageMaker Unified Studio

You can encrypt the resources provisioned by Amazon SageMaker Unified Studio with your customer managed AWS KMS keys. You can do this by adding to your default KMS key policy the permissions that you can find in the following policy for the Tooling blueprint config.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-policy-for-smus",
    "Statement": [
        {
            "Sid": "AllowKmsPermissionsForCloudWatch",
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.us-east-1.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt*",
                "kms:Decrypt*",
```

```
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:Describe*"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "kms:EncryptionContext:aws:logs:arn": [
                        "arn:aws:logs:us-east-1:111122223333:log-group:datazone-
*",
                        "arn:aws:logs:us-east-1:111122223333:log-group:airflow-
*",
                        "arn:aws:logs:us-east-1:111122223333:log-group:/aws/mwaa-
serverless*"
                    ]
                }
            }
        },
        {
            "Sid": "RedshiftCreateGrantKmsPermissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/service-role/
AmazonSageMakerProvisioning-111122223333"
            },
            "Action": "kms:CreateGrant",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                },
                "StringLike": {
                    "kms:ViaService": [
                        "redshift-serverless.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AthenaKmsPermissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/service-role/
AmazonSageMakerProvisioning-111122223333"
```

```
            },
            "Action": "kms:GenerateDataKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "athena.amazonaws.com",
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "EmrServerlessKmsPermissions",
            "Effect": "Allow",
            "Principal": {
                "Service": "emr-serverless.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:emr-serverless:us-
east-1:111122223333:/applications/*"
                }
            }
        },
        {
            "Sid": "EmrServerlessKmsPermissionsForProvisioning",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/service-role/
AmazonSageMakerProvisioning-111122223333"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AirflowCreateGrantKmsPermissions",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/service-role/
AmazonSageMakerProvisioning-111122223333"
            },
            "Action": "kms:CreateGrant",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                },
                "StringLike": {
                    "kms:ViaService": [
                        "airflow.*.amazonaws.com",
                        "airflow-serverless.*.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowKmsKeyUsageForSageMakerDomain",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "datazone.amazonaws.com"
                ],
                "AWS": [
                    "arn:aws:iam::111122223333:role/service-role/
AmazonSageMakerDomainExecution"
                ]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:CreateGrant"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowSageMakerDomainKmsGrantPermissions",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": [
                    "datazone.amazonaws.com"
                ],
                "AWS": [
                    "arn:aws:iam::111122223333:role/service-role/
AmazonSageMakerDomainExecution"
                ]
            },
            "Action": [
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GrantKMSPermissionsForAllProjectRoles",
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalTag/AmazonDataZoneDomain": "dzd_0123456789",
                    "kms:EncryptionContext:aws:datazone:domainId":
 "dzd_0123456789",
                    "kms:ViaService": [
                        "datazone.us-east-1.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowCreateGrantForProjectRoles",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": "kms:CreateGrant",
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:aws:datazone:domainId":
 "dzd_0123456789"
                },
                "StringLike": {
                    "kms:GrantConstraintType": "EncryptionContextSubset"
                },
                "Null": {
                    "kms:GrantOperations": "false"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Encrypt",
                        "Decrypt",
                        "ReEncryptFrom",
                        "ReEncryptTo",
                        "GenerateDataKey",
                        "GenerateDataKeyWithoutPlaintext",
                        "DescribeKey",
                        "RetireGrant",
                        "CreateGrant"
                    ]
                }
            }
        }
    ]
}
```

KMS permissions for exporting asset metadata in Amazon SageMaker Unified Studio

Topics

- Granting the Amazon SageMaker Catalog export service principal and S3 Tables maintenance service principal permissions to your KMS key
- IAM permissions required for the principal for exporting

Granting the Amazon SageMaker Catalog export service principal and S3 Tables maintenance service principal permissions to your KMS key

All data in S3 tables are encrypted with SSE-S3 encryption by default. You can choose to encrypt your data with AWS Key Management Service (AWS KMS) keys (SSE-KMS). If you choose to encrypt your data with KMS keys, you must have additional permissions.

For Amazon SageMaker Catalog, these permissions are required so that your data can be encrypted when exporting the data into the S3 tables. Note that the KMS key used for export feature can be same or different than the one used for Amazon SageMaker Catalog domain. To read more about how Amazon SageMaker Catalog domain data encryption works at rest, see Data encryption at rest for Amazon DataZone.

To allow Amazon SageMaker Catalog access on SSE-KMS encrypted tables, you can use the following example key policy. The policy allows `maintenance.s3tables.amazonaws.com` service principal to use a specific KMS key for encrypting and decrypting tables in a specific table bucket. To use the policy, replace the user input placeholders with your own information:

To read more about the S3 maintenance service principal, see Permissions required for S3 Tables SSE-KMS encryption.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableSystemTablesKeyUsage",
            "Effect": "Allow",
            "Principal": {
                "Service": "systemtables.sagemaker-catalog.amazonaws.com"
            },
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                }
```

```
            }
        },
        {
            "Sid": "EnableKeyUsage",
            "Effect": "Allow",
            "Principal": {
                "Service": "maintenance.s3tables.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id",
            "Condition": {
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3tables:us-
east-1:111122223333:bucket/*"
                }
            }
        }
    ]
}
```

Replace the following placeholder values with your own:

us-east-1

The AWS Region of your AWS KMS key.

key-id

The ID of your AWS KMS key.

IAM permissions required for the principal for exporting

When your Amazon SageMaker Catalog domain is encrypted using AWS Key Management Service (AWS KMS) keys, you need to grant permissions to the principals that will allow them to enable exporting the asset metadata. The policy below grants the IAM principal access to decrypt a specific Amazon SageMaker Catalog domain.

To read more about how Amazon SageMaker Catalog domain data encryption works at rest, see Data encryption at rest for Amazon DataZone.

```
{
    "Version": "2012-10-17",
    "Statement": [

        {
            "Sid": "Allow access to principal to manage an Amazon SageMaker catalog
 domain with the given domain id",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id",
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:aws:datazone:domainId": "dzd_sampleid"
                }
            }
        }
    ]
}
```

Replace the following placeholder values with your own:

ExampleRole

The IAM role granted access to decrypt the Amazon SageMaker Unified Studio domain.

us-east-1

The AWS Region of your AWS KMS key.

key-id

The ID of your AWS KMS key.

dzd_sampleid

Your Amazon SageMaker Unified Studio domain ID (begins with dzd_).

Amazon Bedrock in SageMaker Unified Studio KMS Permissions

- **KMS Key Policy — Amazon DataZone domain key and the Tooling blueprint Key**: manually set the following key policy to the domain key and the Tooling blueprint key.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Allow administrators to manage key",
            "Effect": "Allow",
            "Principal": {
            "AWS": "arn:aws:iam::444455556666:role/ExampleAdminRole"
            },
            "Action": [
                "kms:Create*",
                "kms:Describe*",
                "kms:Enable*",
                "kms:List*",
                "kms:Put*",
                "kms:Update*",
                "kms:Revoke*",
                "kms:Disable*",
                "kms:Get*",
                "kms:Delete*",
                "kms:TagResource",
                "kms:UntagResource",
                "kms:ScheduleKeyDeletion",
                "kms:CancelKeyDeletion",
                "kms:RotateKeyOnDemand"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow administrators and SageMaker domain execution role to
 encrypt and decrypt DataZone data",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                "arn:aws:iam::444455556666:role/ExampleAdminRole",
    "arn:aws:iam::444455556666:role/ExampleDomainUser",
```

```
    "arn:aws:iam::111122223333:role/service-role/
AmazonSageMakerDomainExecution"
                ]
            },
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                "kms:EncryptionContext:aws:datazone:DOMAIN_ID": "domain_id"
                }
            }
        },
        {
            "Sid": "Allow SageMaker provisioning role to encrypt and decrypt
 Amazon Bedrock resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/service-role/
AmazonSageMakerProvisioning-111122223333"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow SageMaker project roles to describe key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:DescribeKey",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:PrincipalTag/AmazonDataZoneProject": "false"
```

```
                }
            }
        },
        {
            "Sid": "Allow SageMaker project roles to encrypt and decrypt data
 in Tooling blueprint S3 bucket",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:PrincipalTag/AmazonDataZoneProject": "false"
                },
                "StringLike": {
                    "kms:ViaService": "s3.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "Allow SageMaker project roles to encrypt and decrypt Amazon
 Bedrock secrets",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:PrincipalTag/AmazonDataZoneProject": "false"
                },
                "StringLike": {
                    "kms:ViaService": "secretsmanager.*.amazonaws.com"
                },
```

```
                "ArnLike": {
                    "kms:EncryptionContext:SecretARN":
"arn:aws:secretsmanager:*:*:secret:amazon-bedrock*"
                }
            }
        },
        {
            "Sid": "Allow SageMaker project roles to encrypt and decrypt Amazon
Bedrock data",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:PrincipalTag/AmazonDataZoneProject": "false"
                },
                "ForAnyValue:StringLike": {
                    "kms:EncryptionContextKeys": [
                        "aws:bedrock*",
                        "evaluationJobArn"
                    ]
                }
            }
        },
        {
            "Sid": "Allow Amazon Bedrock to encrypt and decrypt Amazon Bedrock
data",
            "Effect": "Allow",
            "Principal": {
                "Service": "bedrock.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
```

```
                    "kms:EncryptionContextKeys": [
                        "aws:bedrock*",
                        "evaluationJobArn"
                    ]
                }
            }
        },
        {
            "Sid": "Allow Amazon Bedrock to create and revoke grants for Amazon
 Bedrock resources",
            "Effect": "Allow",
            "Principal": {
                "Service": "bedrock.amazonaws.com"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Sid": "Allow CloudWatch Logs to encrypt and decrypt Amazon Bedrock
 log groups",
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:Describe*",
                "kms:Encrypt*",
                "kms:GenerateDataKey*",
                "kms:ReEncrypt*"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
```

```
                    "kms:EncryptionContext:aws:logs:arn":
 "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock*"
                }
            }
        }
    ]
}
```

- **AmazonSageMakerDomainExecution role — inline Policy**: manually attach the following to the AmazonSageMakerDomainExecution role or any role that is used for domain execution role in IAM console.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "KmsDescribeKeyPermissions",
            "Effect": "Allow",
            "Action": "kms:DescribeKey",
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/dzd-12345"
        },
        {
            "Sid": "KmsPermissions",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/dzd-12345",
            "Condition": {
                "StringLike": {
                    "kms:EncryptionContext:aws:datazone:domainId": "dzd*"
                }
            }
        }
    ]
}
```

- **AmazonSageMakerProvisioning-<domainAccountId> role - inline Policy**: manually attach the following to the AmazonSageMakerProvisioning-<domainAccountId> role or the role that is used as the provisioning role in the IAM console.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "KmsDescribeKeyPermissions",
            "Effect": "Allow",
            "Action": "kms:DescribeKey",
            "Resource": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        },
        {
            "Sid": "ToolingBlueprintS3BucketKmsPermissions",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "s3.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "LambdaFunctionKmsPermissions",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:Encrypt"
            ],
            "Resource": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "Condition": {
                "StringLike": {
```

```
                    "kms:ViaService": "lambda.*.amazonaws.com"
                },
                "ArnLike": {
                    "kms:EncryptionContext:aws:lambda:FunctionArn":
 "arn:aws:lambda:*:*:function:amazon-bedrock*"
                }
            }
        },
        {
            "Sid": "SecretsManagerKmsPermissions",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "secretsmanager.*.amazonaws.com"
                },
                "ArnLike": {
                    "kms:EncryptionContext:SecretARN":
 "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*"
                }
            }
        },
        {
            "Sid": "BedrockKmsPermissions",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "bedrock.*.amazonaws.com"
                },
                "ForAnyValue:StringLike": {
                    "kms:EncryptionContextKeys": "aws:bedrock*:arn"
```

```
                }
            }
        }
    ]
}
```

Authorization in Amazon SageMaker Unified Studio

Amazon SageMaker Unified Studio's interface consists of a management console within AWS and an off-console web application.

The Amazon SageMaker Unified Studio management console can be used by AWS administrators for top-level-resource APIs, including creating and managing domains, AWS account associations for these domains, and data sources for which you want to delegate access management to Amazon SageMaker Unified Studio. You can use the Amazon SageMaker Unified Studio management console to manage all of the IAM roles and configuration needed to delegate access management control to the Amazon SageMaker Unified Studio service for their explicitly configured AWS accounts. The Amazon SageMaker Unified Studio is a first-party AWS Identity Center application for SSO users. If enabled, the console can also be used by authorized IAM principals to federate into the Amazon SageMaker Unified Studio instead of using an SSO identity.

Amazon SageMaker Unified Studio is designed to be used principally by AWS IAM Identity Center-authenticated users or third party Identity Providers who support SAML to manage access to data and perform data publishing, discovery, subscription, and analytics tasks.

Authorization in the Amazon SageMaker Unified Studio console

The Amazon SageMaker Unified Studio console authorization model uses IAM authorization. The console is used by administrators primarily for setup. Amazon SageMaker Unified Studio uses the concept of a domain administrator AWS account, and member AWS accounts, and the console is used from all of these accounts to build the trust relationships while respecting AWS Organization boundaries.

Authorization in Amazon SageMaker Unified Studio

The Amazon SageMaker Unified Studio authorization model is a hierarchical ACL with static role archetypes (profiles) that include administrators and viewers. For example, users can have a profile of administrator or user. At the level of a domain, they may have a domain user owner designation.

At the level of a project, a user can be an owner or contributor. These profiles can be configured as one of two types: users and groups.

Within this authorization model, Amazon SageMaker Unified Studio allows users to manage user and group permissions. Users manage project membership, request membership to projects, and approve memberships. Users publish data, define data subscription approvers, subscribe to data, and approve subscriptions.

Users perform data analytics in specific projects when their Amazon SageMaker Unified Studio client requests IAM session credentials that Amazon SageMaker Unified Studio generates based on the user's effective profile in the specific project context. This session is scoped both to the user's permissions and also the specific project's resources. Users then use the projects tools (i.e. Amazon Athena or Amazon Redshift) to query the relevant data, and all of the underlying IAM work is completely abstracted away.

Note that only IAM users and SSO users can access the Amazon SageMaker Unified Studio UI. IAM roles cannot access the Amazon SageMaker Unified Studio UI. But but IAM roles can interact with the Amazon SageMaker Unified Studio through APIs (searching assets, creating and managing projects, etc.)

Amazon SageMaker Unified Studio profiles and roles

Once a user is authenticated, the authenticated context maps to a user profile ID. This user profile can have multiple, different associations (project owner, domain owner etc.) which is used for authorizing users. Each association (for example, project owner, domain administrator, etc.) has permissions for certain activities based on the context. For example, a user that has a domain owner association can create additional domains andcan assign other domain owners to the domain. A project owner can add or remove project members for their project, they can create publishing agreements with a domain, and publish assets to a domain.

Compliance validation for Amazon SageMaker Unified Studio

Compliance programs for Amazon SageMaker

Amazon SageMaker Unified Studio and SageMaker Catalog are built on Amazon DataZone. These services use the same entity store, identity and access mechanisms, and APIs as Amazon DataZone. As a result, they are included in the scope of the same compliance programs as Amazon DataZone.

Amazon DataZone is in scope for the following programs:

- SOC
- Certain ISO certifications
- PCI DSS
- HITRUST CSF
- HIPAA eligible services

Our new AWS sign-up experience is not designed for regulated workloads. If you're using our new AWS sign-up experience, but you want to use AWS for regulated workloads, you can sign up for AWS (advanced) or activate advanced features for your AWS environment.

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. For more information about your compliance responsibility when using AWS services, see AWS Security Documentation.

Security Best Practices for Amazon SageMaker Unified Studio

Amazon SageMaker Unified Studio provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don’t represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

Implement least privilege access

When granting permissions, you decide who is getting what permissions to which Amazon SageMaker Unified Studio resources. You enable specific actions that you want to allow on those resources. Therefore you should grant only the permissions that are required to perform a task. Implementing least privilege access is fundamental in reducing security risk and the impact that could result from errors or malicious intent.

Use IAM roles

Producer and client applications must have valid credentials to access Amazon SageMaker Unified Studio resources. You should not store AWS credentials directly in a client application or in an Amazon S3 bucket. These are long-term credentials that are not automatically rotated and could have a significant business impact if they are compromised.

Instead, you should use an IAM role to manage temporary credentials for your producer and client applications to access Amazon SageMaker Unified Studio resources. When you use a role, you don't have to use long-term credentials (such as a user name and password or access keys) to access other resources.

For more information, see the following topics in the *IAM User Guide*:

- IAM Roles
- Common Scenarios for Roles: Users, Applications, and Services

Implement Server-Side Encryption in Dependent Resources

Data at rest and data in transit can be encrypted in Amazon SageMaker Unified Studio.

Use CloudTrail to Monitor API Calls

Amazon SageMaker Unified Studio is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon SageMaker Unified Studio.

Using the information collected by CloudTrail, you can determine the request that was made to Amazon SageMaker Unified Studio, the IP address from which the request was made, who made the request, when it was made, and additional details.

Resilience in Amazon SageMaker Unified Studio

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

In addition to the AWS global infrastructure, Amazon SageMaker Unified Studio offers several features to help support your data resiliency and backup needs.

Infrastructure Security in Amazon SageMaker Unified Studio

As a managed service, Amazon SageMaker Unified Studio is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access Amazon SageMaker Unified Studio through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Network isolation in Amazon SageMaker Unified Studio

Amazon SageMaker Unified Studio can be configured to limit from where your data is accessed and exposure of that data over the public internet. You can interact with Amazon SageMaker Unified Studio, and dependent AWS services, directly through interface endpoints in your Amazon VPC instead of connecting over the internet. When using Amazon VPC interface endpoints, communication between your Amazon VPC and Amazon SageMaker Unified Studio happens within the AWS network.

This topic discusses how customers can isolate their Amazon SageMaker Unified Studio portal experience by restricting Amazon SageMaker Unified Studio network traffic to stay within the AWS network.

Prerequisites

Before implementing these solutions, ensure you have:

- Working knowledge of Amazon SageMaker Unified Studio
- Experience with Amazon VPC and subnet configuration
- Administrator access to IAM
- Understanding of VPC interface and gateway endpoints
- Understanding of Security best practices for your Amazon VPC
- AWS CLI or AWS Console access with appropriate permissions

Restrict Amazon SageMaker Unified Studio network traffic to within the AWS network

Your Amazon SageMaker Unified Studio domain and the data within can be configured to limit all traffic to only use the AWS network - and not pass through the public internet. With AWS PrivateLink, AWS service endpoints can be provisioned within your Amazon VPC, keeping customer data within the AWS network.

This level of network isolation means:

- Customers can only use Amazon SageMaker Unified Studio within a configured Amazon VPC. AWS services, accessed through Amazon SageMaker Unified Studio, that support AWS PrivateLink do not send customer data over the public internet.
- Customer access to Amazon SageMaker Unified Studio and other AWS services from outside the Amazon VPC is denied. Customers cannot use Amazon SageMaker Unified Studio outside of the Amazon VPC. This includes denying access from the public internet.
- Access to the public internet is denied from the Amazon VPC. All network traffic must be served within the Amazon VPC, there is no access to the public internet. Access to public internet for non-customer data for items such as Amazon SageMaker Unified Studio web clients and client operations may be required.

> **Important**
>
> Amazon Athena for Apache Spark does not currently support Amazon VPC. If you require Amazon VPC connectivity for your Spark workloads, use Amazon EMR or AWS Glue instead.

Disable Amazon Athena Spark in Amazon VPC-enabled domains

If your organization requires all compute traffic to stay within the Amazon VPC, you can disable Amazon Athena Spark by using the following controls.

- **Account or organization-level SCP** — Apply a service control policy (SCP) that denies `athena:StartSession`.

  The following IAM policy denies this action for all Amazon Athena workgroups.

  ```
  {
      "Version": "2012-10-17",
      "Statement": [
          {
              "Sid": "DenyAthenaSparkStartSession",
              "Effect": "Deny",
              "Action": [
                  "athena:StartSession"
              ],
              "Resource": [
                  "arn:aws:athena:*:*:workgroup/*"
              ]
          }
      ]
  }
  ```

  The wildcard ARN `arn:aws:athena:*:*:workgroup/*` applies to all Regions and accounts. You can scope the policy to specific Regions, accounts, or workgroups by replacing the wildcards.
- **Tooling blueprint configuration** — Disable the Amazon Athena flag in tooling blueprints to prevent Amazon Athena (SQL) and Amazon Athena Spark from being provisioned in new projects.
- **Project-level policy updates** — Remove Amazon Athena Spark permissions from individual project IAM policies to restrict access at the project level.

If Amazon VPC endpoints are missing or misconfigured, network calls to Amazon SageMaker Unified Studio and other AWS services route over the public internet when that network path is available.

Step 1 - Deploy Amazon VPC endpoints

The Amazon SageMaker Unified Studio portal calls the following AWS services, each of which supports AWS PrivateLink Amazon VPC endpoints. The network traffic between the Amazon SageMaker Unified Studio portal and AWS services stays within the AWS network when the Amazon VPC endpoints are created in the Amazon VPC.

Create the Amazon VPC endpoint for each required AWS service API and any optional AWS service APIs from the tables below. To create a Amazon VPC endpoint see, Access an AWS service using an interface Amazon VPC endpoint.

For the list of AWS Services with support for AWS PrivateLink see, AWS services that integrate with AWS PrivateLink.

Amazon VPC endpoint considerations:

- For high availability it is recommended that Amazon VPC endpoints be deployed to multiple Availability Zones (AZ). The recommended minimum number of Availability Zones is two.
- Refer to AWS PrivateLink pricing to understand the costs associated with Amazon VPC endpoints across Availability Zones.

Required Amazon VPC endpoints

These Amazon VPC endpoints are required for Amazon SageMaker Unified Studio and supporting services to function correctly.

AWS service name	Amazon VPC endpoint service name (API endpoint)
Amazon Athena	com.amazonaws.<region>.athena
Amazon DataZone	com.amazonaws.<region>.datazone com.amazonaws.<region>.datazone-fips
Amazon EC2	com.amazonaws.<region>.ec2 com.amazonaws.<region>.ec2-fips com.amazonaws.<region>.ec2messages

AWS service name	Amazon VPC endpoint service name (API endpoint)
Amazon Q Developer	com.amazonaws.<region>.q com.amazonaws.us-east-1.codewhisperer **Note** Available only in us-east-1 region. Domains in different regions will use this endpoint.
Amazon Simple Storage Service	com.amazonaws.<region>.s3
Amazon SageMaker AI	com.amazonaws.<region>.sagemaker.api com.amazonaws.<region>.sagemaker.runtime com.amazonaws.<region>.sagemaker.api-fips com.amazonaws.<region>.sagemaker.runtime-fips
AWS Glue	com.amazonaws.<region>.glue
AWS KMS	com.amazonaws.<region>.kms com.amazonaws.<region>.kms-fips
AWS Secrets Manager	com.amazonaws.<region>.secretsmanager
AWS Security Token Service	com.amazonaws.<region>.sts com.amazonaws.<region>.sts-fips
AWS Systems Manager	com.amazonaws.<region>.ssm com.amazonaws.<region>.ssmmessages

Optional Amazon VPC endpoints

Create these Amazon VPC endpoints if you plan to deploy Amazon SageMaker Unified Studio projects that include blueprints using the services listed below.

AWS service name	Amazon VPC endpoint service name (API endpoint)
Amazon Bedrock	com.amazonaws.<region>.bedrock-agent com.amazonaws.<region>.bedrock-agent-runtime com.amazonaws.<region>.bedrock-runtime
Amazon Athena Spark	com.amazonaws.<region>.athena.sessions com.amazonaws.<region>.athena.dashboard com.amazonaws.<region>.athena.persistent-dashboard
AWS Glue Interactive Sessions	com.amazonaws.<region>.glue.sessions
Amazon CloudWatch	com.amazonaws.<region>.logs
Amazon EMR	com.amazonaws.<region>.elasticmapreduce com.amazonaws.<region>.elasticmapreduce-services com.amazonaws.<region>.emr-serverless com.amazonaws.<region>.emr-serverless-services.livy com.amazonaws.<region>.emr-serverless-services.sessions com.amazonaws.<region>.emr-serverless.dashboard com.amazonaws.<region>.emr-dashboard com.amazonaws.<region>.elasticmapreduce-fips
Amazon EMR on Amazon EKS	com.amazonaws.<region>.emr-containers
Amazon RDS	com.amazonaws.<region>.rds

AWS service name	Amazon VPC endpoint service name (API endpoint)
	com.amazonaws.<region>.rds-fips
Amazon Redshift	com.amazonaws.<region>.redshift com.amazonaws.<region>.redshift-data com.amazonaws.<region>.redshift-serverless com.amazonaws.<region>.redshift-fips com.amazonaws.<region>.redshift-data-fips com.amazonaws.<region>.redshift-serverless-fips
Portal Query Editors	com.amazonaws.<region>.sqlworkbench com.amazonaws.<region>.sqlworkbench-v2
AWS CodeCommit	com.amazonaws.<region>.codecommit com.amazonaws.<region>.git-codecommit com.amazonaws.<region>.codecommit-fips com.amazonaws.<region>.git-codecommit-fips
AWS CodeConnections	com.amazonaws.<region>.codeconnections.api com.amazonaws.<region>.codestar-connections.api

Step 2: Create an IAM policy

Create an IAM policy that only allows the Amazon SageMaker Unified Studio Portal web client to call AWS service APIs through VPC endpoints deployed in an allowed VPC(s). The global context condition key aws:SourceVpc in the IAM policy can be used to enforce this access for AWS service callers (Amazon SageMaker domain execution role, IAM user or role), and AWS Organizations service control policies.

This policy denies the Amazon SageMaker Unified Studio portal's access to all AWS service APIs when the API calls do not originate from within an allowed Amazon VPC. The `Deny` policy is applied when all of the three policy `Conditions` evaluate to `true`. You will need to replace the example VPC ID with your VPC ID or VPC ID list.

This policy may need to be modified if the domain execution role credentials are used in other contexts, or if this policy is applied to a role other than the domain execution role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyUserAccessFromUnauthorizedVPCs",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:SourceVpc": [
                        "vpc-1234567890abcdef0"
                    ]
                },
                "StringLike": {
                    "aws:userid": "*:user-*"
                },
                "BoolIfExists": {
                    "aws:ViaAWSService": "false"
                }
            }
        }
    ]
}
```

The following are details about the policy conditions:

```
"StringNotEquals": {
    "aws:SourceVpc": [
        "vpc-1234567890abcdef0"
    ]
}
```

This condition evaluates to `true` when the API call originates from a network location other than a VPC endpoint deployed in one of the allowed source Amazon VPC IDs.

```
"StringLike": { "aws:userid": "*:user-*" }
```

This condition evaluates to `true` for the domain execution role credentials issued to the Amazon SageMaker Unified Studio portal, so that the `Deny` policy is only applied for portal users. For example, the condition evaluates to `false` and the `Deny` policy is not applied when the Amazon SageMaker Unified Studio catalog service executes tasks that use the domain execution role.

```
"BoolIfExists": { "aws:ViaAWSService": "false" }
```

This condition evaluates to `true` when the API caller is not an AWS service (`aws:ViaAWSService` is `false`), which is the case for the Amazon SageMaker Unified Studio portal. When an AWS service calls another AWS service on behalf of the original caller, `aws:ViaAWSService` is `true` and the condition evaluates to `false` - allowing the AWS service call to another AWS service to succeed.

Step 3: Attach the custom policy

Attach the new custom policy to the SageMaker AI domain execution role. If SageMaker AI created this role for you it will be called AmazonSageMakerDomainExecution. The Amazon SageMaker Unified Studio portal uses the domain execution role for the Amazon SageMaker Unified Studio domain to call all AWS services. When a DENY by source Amazon VPC policy is added to the domain execution role, Amazon SageMaker Unified Studio portal calls to AWS service APIs from outside the allowed Amazon VPC will fail with `Access denied`. This policy can also be applied to an IAM user, IAM role or to an AWS Organizations service control policy.

Public internet access

Public internet access is required to load Amazon SageMaker Unified Studio clients and for client operations that do not handle customer data.

Public internet access for Amazon SageMaker Unified Studio portal

Running the Amazon SageMaker Unified Studio portal web client requires public internet access to download client assets (portal web application, plugins, and user interface components) and to call client management APIs. Customer data is not transmitted through these calls. These endpoints are used by the Amazon SageMaker Unified Studio portal.

Action	Endpoint
Portal asset delivery	https://<domain_id>.sagemaker.<region>.on.aws **Note** The Amazon SageMaker Unified Studio portal URL for your domain. https://*.cdn.console.awsstatic.com https://*.cdn.uis.awsstatic.com https://*.shortbread.aws.dev https://public.lotus.awt.aws.a2z.com
Portal client APIs (Cookie management, customer feedback, UI business and operational metrics, etc.)	https://*.console.api.aws https://*.console.aws.a2z.com https://*.execute-api.<region>.amazonaws.com https://*.sagemaker.aws https://*.sagemaker.aws.dev https://agent.datazone.<region>.api.aws https://monitoring.<region>.amazonaws.com https://sagemaker-unified-studio.<region>.api.aws

Public internet access for IAM Identity Center login to Amazon SageMaker Unified Studio portal

When the Amazon SageMaker Unified Studio portal web client logs into a domain using AWS Identity and Access Management Identity Center (IDC) Single Sign-On (IAM Identity Center), public

internet access is required. These endpoints are used by the Amazon SageMaker Unified Studio portal.

Action	Endpoint
AWS Identity and Access Management Identity Center (IDC), Single Sign-On (IAM Identity Center)	https://assets.sso-portal.<region>.amazonaws.com https://d35uxhjf90umnp.cloudfront.net https://oidc.<region>.amazonaws.com https://d-12345abcde.awsapps.com **Note** IDC IAM Identity Center application URL for the Amazon SageMaker Unified Studio domain https://portal.sso.<region>.amazonaws.com https://log.sso-portal.<region>.amazonaws.com https://<region>.signin.aws

Public internet access for Amazon SageMaker Unified Studio on AWS console

Running the Amazon SageMaker Unified Studio console web client requires public internet access to download client assets (console web application, plugins, and user interface components) and to call AWS console platform APIs. Customer data is not transmitted through these calls. These endpoints are used by the AWS console.

Action	Endpoint
Console asset delivery	https://console.aws.amazon.com https://*.console.aws.amazon.com https://*.cdn.console.awsstatic.com

Action	Endpoint
	https://cdn.1.as2.amazonaws.com https://cdn.2.as2.amazonaws.com https://cdn.assets.as2.amazonaws.com https://*.cloudfront.net **Note** One distribution endpoint needed for each region.
Sign-in	https://signin.aws.amazon.com https://*.signin.aws.amazon.com
Console Control Service (console management / settings)	https://*.ccs.amazonaws.com
AWS User Notifications - AWS Health category	https://health.aws.amazon.com https://phd.aws.amazon.com https://*.ctrl.prod.os.notifications.aws.dev
AWS User Experience Customization (UXC)	https://uxc.us-east-1.api.aws **Note** Endpoint is in us-east-1 only.
Amazon Q for console	https://conversational-experience-worker.widget.console.aws.amazon.com
Console unified search	https://unifiedsearch.amazonaws.com/ https://*.unifiedsearch.amazonaws.com

Action	Endpoint
Console platform APIs	https://account.*.api.aws https://*.console.api.aws https://*.console-api.aws.amazon.com https://*.console.aws.a2z.com https://freetier.us-east-1.api.aws **Note** Endpoint is in us-east-1 only. **Note** For regions in the AWS Regions (partition)

Public internet access for IAM login to Amazon SageMaker Unified Studio portal

Amazon SageMaker Unified Studio domains that use IAM login for the Portal web client require the Amazon SageMaker Unified Studio Console. See the public internet access requirements for the Amazon SageMaker Unified Studio on AWS console above.

Amazon VPC troubleshooting

This section helps you diagnose and resolve common Amazon VPC configuration issues that affect notebook connectivity in Amazon SageMaker Unified Studio. Use the following table to identify your subnet configuration and determine the appropriate recovery action.

Scenario (Subnet 1 type, Subnet 2 type)	Expected behavior	Recovery action
Private with NAT + Private with NAT	Works as expected	No action needed
Private no NAT + Private no NAT	Only local Python kernel works	Add NAT (the section called "Add a NAT gateway to a private subnet") or add Amazon VPC endpoints (the section called "Add Amazon VPC endpoints")
Public + Public	Only local Python kernel works	Convert to private (the section called "Convert a public subnet to a private subnet") or add Amazon VPC endpoints (the section called "Add Amazon VPC endpoints ")
Private with NAT + Public	Works as expected	No action needed
Private no NAT + Public	Only local Python kernel works	Convert to private (the section called "Convert a public subnet to a private subnet"), add NAT (the section called "Add a NAT gateway to a private subnet"), or add Amazon VPC endpoints (the section called "Add Amazon VPC endpoints ")

Convert a public subnet to a private subnet

A public subnet has a route to an internet gateway (IGW), which allows resources in the subnet to communicate directly with the internet. To convert a public subnet to a private subnet, remove the IGW route and disable auto-assign public IP.

> **Note**
>
> Existing instances in the subnet retain their public IP addresses after you make this change. Any services that rely on inbound internet access stop working. To maintain outbound access for package installations and AWS API calls, set up a NAT gateway or Amazon VPC endpoints before converting the subnet.

To convert a public subnet to a private subnet

1. Open the Amazon Virtual Private Cloud console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Route tables**.
3. Select the route table associated with your public subnet.
4. Choose the **Routes** tab.
5. Choose **Edit routes**.
6. Choose **Remove** for the route with destination `0.0.0.0/0` that targets an internet gateway (`igw-xxx`).
7. Choose **Save changes**.

To disable auto-assign public IP

1. In the navigation pane, choose **Subnets**.
2. Select your subnet.
3. Choose **Actions**, **Edit subnet settings**.
4. Clear the **Enable auto-assign public IPv4 address** checkbox.
5. Choose **Save**.

(Optional) If instances in the subnet need outbound internet access, add a NAT gateway route. For instructions, see the section called “Add a NAT gateway to a private subnet”.

To verify the conversion

1. In the navigation pane, choose **Subnets**.
2. Select your subnet and choose the **Route table** tab.
3. Confirm that no route with destination `0.0.0.0/0` targets an internet gateway.

Add a NAT gateway to a private subnet

A NAT gateway allows instances in a private subnet to connect to the internet for outbound traffic while preventing unsolicited inbound connections. You must have a public subnet with an internet gateway route before you create a NAT gateway.

To create a NAT gateway

1. Open the Amazon Virtual Private Cloud console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **NAT gateways**.
3. Choose **Create NAT gateway**.
4. For **Subnet**, select a public subnet that has a route to an internet gateway.
5. For **Connectivity type**, select **Public**.
6. Choose **Allocate Elastic IP** to assign a new Elastic IP address to the NAT gateway.
7. Choose **Create NAT gateway**.

To update the private subnet route table

1. In the navigation pane, choose **Route tables**.
2. Select the route table associated with your private subnet.
3. Choose the **Routes** tab.
4. Choose **Edit routes**.
5. Choose **Add route**. For **Destination**, enter `0.0.0.0/0`. For **Target**, select the NAT gateway that you created.
6. Choose **Save changes**.

To verify the NAT gateway

1. In the navigation pane, choose **NAT gateways**.

2. Confirm that the NAT gateway status is **Available**.
3. In the navigation pane, choose **Route tables** and select the private subnet route table.
4. Confirm that the `0.0.0.0/0` route targets the NAT gateway.

Add Amazon VPC endpoints

Amazon VPC endpoints allow resources in your private subnets to communicate with AWS services without requiring internet access. There are two types of Amazon VPC endpoints:

- **Gateway endpoints** – For Amazon Simple Storage Service and Amazon DynamoDB. Gateway endpoints are free of charge.
- **Interface endpoints** – For other AWS services such as AWS Security Token Service, Amazon CloudWatch, Amazon ECR, and AWS Systems Manager. Interface endpoints cost approximately $0.01 per hour per Availability Zone, plus data processing charges.

The following are common endpoints to add for Amazon SageMaker Unified Studio notebook connectivity:

- Amazon Simple Storage Service (gateway)
- Amazon DynamoDB (gateway)
- AWS Security Token Service (interface)
- Amazon ECR – `ecr.api` and `ecr.dkr` (interface)
- Amazon CloudWatch Logs (interface)
- AWS Systems Manager (interface)

To create a gateway endpoint

1. Open the Amazon Virtual Private Cloud console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Endpoints**.
3. Choose **Create endpoint**.
4. For **Service category**, select **AWS services**.
5. Search for and select the gateway service (for example, `com.amazonaws.<region>.s3` with type **Gateway**).
6. For **VPC**, select your Amazon VPC.

7. For **Route tables**, select the route tables associated with your private subnets.
8. Choose **Create endpoint**.

To create an interface endpoint

1. Open the Amazon Virtual Private Cloud console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Endpoints**.
3. Choose **Create endpoint**.
4. For **Service category**, select **AWS services**.
5. Search for and select the interface service (for example, `com.amazonaws.<region>.sts`).
6. For **VPC**, select your Amazon VPC.
7. For **Subnets**, select the subnets in your private subnet Availability Zones.
8. For **Security groups**, select a security group that allows inbound traffic on port 443 (HTTPS).
9. Select **Enable DNS name** to turn on private DNS for the endpoint.
10. Choose **Create endpoint**.

To verify Amazon VPC endpoints

1. In the navigation pane, choose **Endpoints**.
2. Confirm that each endpoint status is **Available**.
3. For gateway endpoints, choose **Route tables** in the navigation pane and confirm that the route table includes a route for the endpoint.

Configuration and vulnerability analysis for Amazon SageMaker Unified Studio

AWS handles basic security tasks like guest operating system (OS) and database patching, firewall configuration, and disaster recovery. These procedures have been reviewed and certified by the appropriate third parties. For more information, see the AWS shared responsibility model.

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource policies to limit the permissions that ServiceNameLongEntity gives another service to the resource. Use `aws:SourceArn` if you want only one resource to be associated with the cross-service access. Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. If you don't know the full ARN of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global context condition key with wildcard characters (*) for the unknown portions of the ARN. For example, `arn:aws:servicename:*:123456789012:*`.

If the `aws:SourceArn` value does not contain the account ID, such as an Amazon S3 bucket ARN, you must use both global condition context keys to limit permissions.

Quotas and limits for Amazon SageMaker Unified Studio

Your AWS account has default quotas, formerly referred to as limits, for each AWS service. Unless otherwise noted, each quota is account specific and region-specific.

Resource quotas

The resource quotas are applied at the account level, meaning the depletion of resource quotas in one project can affect all other projects within the account.

Amazon SageMaker Unified Studio has the following quotas and limits.

Resource	Default
Maximum number of account pools for your Amazon SageMaker unified domain	100
Maximum number of JupyterLab instances	4000
Maximum number of user type project members per project	100
Maximum number of group type project members per project	20
Maximum number of spaces	6000
Maximum number of projects	1000
Maximum number of environments	1000
Maximum number of Micro environments	200

Amazon DataZone quotas

The following table describes quotas for Amazon DataZone:

Resource	Description	Value
Data Asset Types	The maximum number of data asset types that can be created in a DataZone domain	1000
Data assets	The maximum number of data assets that can be created in an Amazon DataZone domain	1 million
Glossaries	The maximum number of business glossaries you can create in a domain	1000
Business glossary terms	The maximum number of total business glossary terms you can create in a domain	10000
Number of asset filters	The maximum number of asset filters per Amazon DataZone domain	100

Amazon DataZone API rate limits

The following table describes rate limits for the Amazon DataZone APIs. These limits apply per AWS account per Region.

API	API rate limit
CreateGlossary	5 transactions per second (TPS)
UpdateGlossary	20 TPS
GetGlossary	20 TPS
DeleteGlossary	20 TPS

API	API rate limit
UpdateGlossaryTerm	20 TPS
DeleteGlossaryTerm	20 TPS
CreateAsset	20 TPS
UpdateAsset	20 TPS

For more information about other AWS service quotas, see AWS service quotas.

For more quotas information, see the following:

- Amazon SageMaker Supported Regions and Quotas
- Amazon Managed Workflows for Apache Airflow endpoints and quotas
- Amazon Redshift endpoints and quotas
- Amazon EMR endpoints and quotas
- Amazon Q Business endpoints and quotas
- Amazon Athena endpoints and quotas
- Amazon Bedrock endpoints and quotas
- AWS Glue endpoints and quotas

Document history for the Amazon SageMaker Unified Studio Administrator Guide

The following table describes the documentation releases for Amazon SageMaker Unified Studio.

Change	Description	Date
Policy update - SageMaker StudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMaker StudioUserIAMPermissiveExecutionPolicy - adding `access-grants.s3.amazonaws.com` as a target for `iam:PassRole` , and read-only AWS IAM Identity Center permissions to resolve users and groups. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	October 8, 2026
Policy update - SageMaker StudioUserIAMDefaultExecutionPolicy	Policy updates to SageMaker StudioUserIAMDefaultExecutionPolicy - adding Amazon S3 Access Grants permissions to register Access Grants locations and manage grants for project data, and read-only AWS IAM Identity Center permissions to resolve users and groups. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	October 8, 2026

Policy update - SageMaker StudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMaker StudioAdminIAMPermissiveExecutionPolicy - adding `access-grants.s3.amazonaws.com` as a target for `iam:PassRole` , and read-only AWS IAM Identity Center permissions to resolve users and groups. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	October 8, 2026
Policy update - SageMaker StudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMaker StudioAdminIAMDefaultExecutionPolicy - adding Amazon S3 Access Grants permissions to register Access Grants locations and manage grants for project data, and read-only AWS IAM Identity Center permissions to resolve users and groups. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	October 8, 2026

Policy update - SageMaker StudioProjectRoleMachineLearningPolicy	Policy updates to SageMaker StudioProjectRoleMachineLearningPolicy - adding `sagemaker:UpdateUserProfile` to support per-user application settings management for project members. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	September 14, 2026
Policy update - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to SageMaker StudioProjectProvisioningRolePolicy - adding `cloudformation:UntagResource` to comply with upcoming CloudFormation tag authorization enforcement. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 24, 2026
Policy update - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to SageMaker StudioProjectProvisioningRolePolicy - adding SageMaker app lifecycle permissions to support managed app creation and deletion, including RStudio apps. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 24, 2026

Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding permissions to support Amazon SageMaker Canvas integration including Amazon Redshift, Amazon S3, Amazon Comprehend, Amazon Textract, Amazon Rekognition, Amazon EventBridge, and Amazon EMR. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 29, 2026
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions to support Amazon SageMaker Canvas integration including Amazon Redshift, Amazon S3, Amazon Comprehend, Amazon Textract, Amazon Rekognition, Amazon EventBridge, and Amazon EMR. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 29, 2026

Policy update - SageMaker StudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMaker StudioAdminIAMPermissiveExecutionPolicy - adding permissions to support Amazon SageMaker Canvas integration including Amazon Redshift, Amazon S3, Amazon Comprehend, Amazon Textract, Amazon Rekognition, Amazon EventBridge, and Amazon EMR. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 29, 2026
Policy update - SageMaker StudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMaker StudioAdminIAMDefaultExecutionPolicy - adding permissions to support Amazon SageMaker Canvas integration including Amazon Redshift, Amazon S3, Amazon Comprehend, Amazon Textract, Amazon Rekognition, Amazon EventBridge, and Amazon EMR. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 29, 2026

Policy update: SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to SageMakerStudioProjectRoleMachineLearningPolicy. The updates add permissions for Amazon SageMaker Feature Store, including create, describe, update, and delete feature groups and manage records. The updates also add read-only access to the SageMaker public model hub and permissions to list schedules for pipeline import. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 25, 2026
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions and AWS Glue session endpoints. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 4, 2026

Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions and AWS Glue session endpoints. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 4, 2026
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to SageMakerStudioProjectUserRolePolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 4, 2026
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 4, 2026

Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions and AWS Glue session endpoints. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 4, 2026
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding permissions to support Amazon EMR on EC2 Spark Connect sessions and AWS Glue session endpoints. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 4, 2026

Policy update - SageMaker StudioProjectRoleMachineLearningPolicy	Policy updates to SageMaker StudioProjectRoleMachineLearningPolicy - adding `datazone:CreateAsset*` permissions to the DataZoneUserPermissions statement to support scheduling notebook runs using the Data Agent. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 21, 2026
Policy update - SageMaker StudioProjectRoleMachineLearningPolicy	Policy updates to SageMaker StudioProjectRoleMachineLearningPolicy - updating the DataZoneUserPermissions statement to support the Business Data Catalog within Data Agent. Adding `datazone:List*` and `datazone:Search*` permissions for catalog discovery, and replacing `datazone:SendMessage` with `datazone:*Message*` to support conversation management. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 13, 2026

Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding permissions to support integration with Amazon EMR Serverless Spark Connect in DataZone Data Notebook. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 11, 2026
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions to support integration with multiple services including Amazon EMR Serverless Spark Connect in DataZone Data Notebook, Amazon Managed Workflows for Apache Airflow (MWAA) environments, and AWS Glue Data Quality. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 11, 2026
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to SageMakerStudioProjectUserRolePolicy - adding permissions to support integration with AWS Glue Data Quality. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 11, 2026

Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adding permissions to support integration with multiple services including Amazon EMR Serverless Spark Connect in DataZone Data Notebook, Amazon Managed Workflows for Apache Airflow (MWAA) environments, and AWS Resource Access Manager. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 11, 2026
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding permissions to support integration with multiple services including Amazon EMR Serverless Spark Connect in DataZone Data Notebook, Amazon Managed Workflows for Apache Airflow (MWAA) environments, AWS Glue Data Quality, and AWS Resource Access Manager. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 11, 2026

Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding permissions to support integration of CloudFormation LanguageExtensions transform and admin project IAM policy attachment. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 6, 2026
Policy update - SageMakerStudioUserIAMConsolePolicy	Policy updates to SageMakerStudioUserIAMConsolePolicy - adding permissions for `datazone:GetConnection` and `datazone:ListConnections` to support IAM role federation in Local IDE. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 31, 2026

Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adds notebook import and export functionality for permissive users. These permissions are applied to default IAM users when using the permissive role. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 30, 2026
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding cloudwatch:GetMetricData, notebook import and export functionality for permissive users, SageMaker Feature store, and LakeFormation data filter for SageMaker Unified Studio. These permissions are applied to default IAM users. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 30, 2026

Policy update - SageMaker StudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMaker StudioAdminIAMPermissiveExecutionPolicy - adds SSO permissions for permissive admin policies. Also adds Admin and LakeFormation data filter permissions to permissive admin roles. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 30, 2026
Policy update - SageMaker StudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMaker StudioAdminIAMDefaultExecutionPolicy - adding cloudwatch:GetMetricData, SageMaker Feature store, LakeFormation data filter, SSO and Admin UI permissions to SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 30, 2026

Policy update - SageMaker StudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMaker StudioAdminIAMDefaultExecutionPolicy - adding cloudwatch:GetMetricData, SageMaker Feature store, LakeFormation data filter, SSO and Admin UI permissions to SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 30, 2026
Policy update - SageMaker StudioAdminIAMConsolePolicy	Policy updates to SageMaker StudioAdminIAMConsolePolicy - adding sso:DeleteApplication permission to allow deleting DataZone domain integrated with AWS IAM Identity Center. Adding KMS permissions required for IAM Identity Center instances that use customer managed keys for encryption. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 30, 2026

Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to SageMaker StudioProjectUserRolePolicy - adding AWS Glue permissions scoped to S3 Tables catalog resource to support querying S3 Tables from SageMaker Unified Studio IdC domains. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 24, 2026
Policy update - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to SageMaker StudioProjectProvisioningRolePolicy - adding iam:CreateServiceLinkedRole permission to allow creating the Amazon Athena service-linked role for Athena Spark workgroup provisioning. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 9, 2026
Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to SageMaker StudioProjectUserRolePolicy - adding permissions to support Airflow Serverless. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 2, 2026

Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding permissions to pass roles to Amazon Athena for Athena Spark workgroup support. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 2, 2026
Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - adding Amazon S3 Tables permissions to support integration with S3 table buckets IAM mode. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 27, 2026
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adding Amazon S3 Tables permissions to support integration with S3 table buckets IAM mode. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 27, 2026

Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to SageMakerStudioProjectRoleMachineLearningPolicy - adding permissions to support SageMaker Notebooks, Data Agent, and Airflow Serverless workflows. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 26, 2026
Policy update - SageMakerStudioDomainExecutionRolePolicy	Policy updates to SageMakerStudioDomainExecutionRolePolicy - adding permissions to support graph-based entity search capabilities. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 25, 2026
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding permissions to support integration with encrypted Identity Center instances. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 5, 2026

Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions to support integration with MLflow App to track runs and experiments. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	January 27, 2026
Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to SageMakerStudioProjectRoleMachineLearningPolicy - adding permissions to support integration with MLflow App to track runs and experiments. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	January 27, 2026
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to SageMakerStudioProjectProvisioningRolePolicy - adding permissions to support integration with MLflow App to track runs and experiments. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	January 27, 2026

Policy update - SageMaker StudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMaker StudioAdminIAMDefaultExecutionPolicy - adding permissions to support integration with MLflow App to track runs and experiments. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	January 27, 2026
Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to SageMaker StudioProjectUserRolePolicy - adding permissions to support integration with SageMaker Unified Studio MCP. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 21, 2025
Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to SageMaker StudioProjectUserRolePolicy - fix KMS permissions for integration with Scheduler. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 20, 2025

Policy update - SageMakerStudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioUserIAMPermissiveExecutionPolicy - fix KMS permissions for integration with Workflows, Scheduler, and DataZone Data Notebook. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 18, 2025
Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - fix KMS permissions for integration with Workflows, Scheduler, and DataZone Data Notebook. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 18, 2025
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - fix KMS permissions for integration with Workflows, Scheduler, and DataZone Data Notebook. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 18, 2025

Policy update - SageMaker StudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMaker StudioAdminIAMDefaultExecutionPolicy - fix KMS permissions for integration with Workflows, Scheduler, and DataZone Data Notebook. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 18, 2025
Policy update - SageMaker StudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMaker StudioUserIAMPermissiveExecutionPolicy - adding permissions for new APIs for SageMaker Unified Studio MCP, Airflow Serverless, and Athena sessions. Improve isolation for Glue and Athena sessions by making sure users can only access their own sessions. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 14, 2025

Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions for new APIs for SageMaker Unified Studio MCP, Airflow Serverless, and Athena sessions. Improve isolation for Glue and Athena sessions by making sure users can only access their own sessions. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 14, 2025
Policy update - SageMakerStudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMakerStudioAdminIAMPermissiveExecutionPolicy - adding permissions for new APIs for SageMaker Unified Studio MCP, Airflow Serverless, and Athena sessions. Improve isolation for Glue and Athena sessions by making sure users can only access their own sessions. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 14, 2025

Policy update - SageMaker StudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMaker StudioAdminIAMDefaultExecutionPolicy - adding permissions for new APIs for SageMaker Unified Studio MCP, Airflow Serverless, and Athena sessions. Improve isolation for Glue and Athena sessions by making sure users can only access their own sessions. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 14, 2025
Policy update - SageMaker StudioUserIAMPermissiveExecutionPolicy	Policy updates to SageMaker StudioUserIAMPermissiveExecutionPolicy - adding permissions to support integration with multiple services including Amazon EMR Serverless, Amazon Redshift, AWS Secrets Manager, AWS Lake Formation, Amazon SageMaker AI, Amazon S3, AWS CodeConnections, and AWS Glue. Adding KMS permissions to manage resources encrypted with CMK. Adding IAM CreateRole permission to allow creating new execution roles.For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 10, 2025

Policy update - SageMakerStudioUserIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy - adding permissions to support integration with multiple services including Amazon EMR Serverless, Amazon Redshift, AWS Secrets Manager, AWS Lake Formation, Amazon SageMaker AI, Amazon S3, AWS CodeConnections, and AWS Glue. Adding KMS permissions to manage resources encrypted with CMK. Adding IAM CreateRole permission to allow creating new execution roles.For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 10, 2025

Policy update - SageMaker StudioAdminIAMPermissiveExecutionPolicy	Policy updates to SageMaker StudioAdminIAMPermissiveExecutionPolicy - adding permissions to support integration with multiple services including Amazon EMR Serverless, Amazon Redshift, AWS Secrets Manager, AWS Lake Formation, Amazon SageMaker AI, Amazon S3, AWS CodeConnections, and AWS Glue. Adding KMS permissions to manage resources encrypted with CMK. Adding IAM CreateRole permission to allow creating new execution roles.For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 10, 2025

Policy update - SageMaker StudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMaker StudioAdminIAMDefaultExecutionPolicy - adding permissions to support integration with multiple services including Amazon EMR Serverless, Amazon Redshift, AWS Secrets Manager, AWS Lake Formation, Amazon SageMaker AI, Amazon S3, AWS CodeConnections, and AWS Glue. Adding KMS permissions to manage resources encrypted with CMK. Adding IAM CreateRole permission to allow creating new execution roles.For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	November 10, 2025
Policy update - SageMaker StudioEMRContainersSystemNamespaceRolePolicy	Policy updates to SageMaker StudioEMRContainersSystemNamespaceRolePolicy - this revision refactors the scope of STS actions required for the EMR Containers service. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	October 31, 2025

Policy update - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to SageMaker StudioProjectProvisioningRolePolicy - permissions updates for the following features: EMR on EKS compute capabilities, trusted identity propagation with user background sessions, AWS resource custom tags support, support default AWS Glue catalog encryption, Amazon SageMaker Unified Studio per project S3 bucket. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	October 30, 2025
New policy - SageMaker StudioEMRContainersSystemNamespaceRolePolicy	New policy - SageMaker StudioEMRContainersSystemNamespaceRolePolicy - Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the permissions related to Amazon EMR. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	October 24, 2025

Policy updates	Policy updates to SageMaker StudioUserIAMDefaultExecutionPolicy - adding `sagemaker:StartSession` to allow users to connect to a space from the local IDE. Also adding `glue:UntagResource` permission. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	October 10, 2025
Policy update - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to SageMaker StudioProjectProvisioningRolePolicy - adding support for customers who opt-in to the Trusted Identity Propagation (TIP) feature, additional resources and configurations are required which require additional permissions, including LakeFormation IdentityCenterConfiguration resource permissions, AWS Glue IdentityCenterConfiguration resource permissions, EMR SecurityConfiguration `Describe` permission SSO resource permissions. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	September 26, 2025

Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to SageMaker StudioProjectUserRolePolicy - restoring table tag visibility in the asset page of Amazon SageMaker Unified Studio for Amazon SageMaker unified domains. For more informati on, see Amazon SageMaker Unified Studio updates to AWS managed policies.	September 18, 2025
Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to SageMaker StudioProjectUserRolePolicy - adding AWS Glue permissio ns to enable users to delete AWS Glue databases in their Amazon SageMaker Unified Studio projects. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	September 12, 2025
Policy update - SageMaker StudioProjectRoleMachineLea rningPolicy	Policy updates to SageMaker StudioProjectRoleMachineLea rningPolicy - adding support for the SageMaker:StartSes sion permission to enable remote connections to Amazon SageMaker spaces. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	September 8, 2025

Policy updates	Policy updates to SageMakerStudioUserIAMDefaultExecutionPolicy, SageMakerStudioAdminIAMPermissiveExecutionPolicy, and SageMakerStudioUserIAMPermissiveExecutionPolicy - adding additional permissions required to create service linked roles. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 29, 2025
Policy update - SageMakerStudioAdminIAMDefaultExecutionPolicy	Policy updates to SageMakerStudioAdminIAMDefaultExecutionPolicy - adding permissions iam:CreateServiceLinkedRole and s3:DeleteBucketPolicy for resource management. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 29, 2025
Support for account pools in Amazon SageMaker Unified Studio	You can configure your domain to create and manage account pools for your custom project profile. For more information, see Account pools in Amazon SageMaker Unified Studio and Custom project profile.	August 21, 2025

Policy update - SageMaker StudioDomainExecutionRolePolicy	Policy updates to SageMaker StudioDomainExecutionRolePolicy - adding support for the new API actions - AssociateGovernedTerms and DisassociateGovernedTerms for the asset classification using restricted glossary terms feature in the catalog where users can associate or disassociate restricted glossary terms to an asset. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 20, 2025
New policy - SageMaker StudioUserIAMPermissiveExecutionPolicy	New policy - This is an execution policy for using IAM roles with Amazon SageMaker Unified Studio. This policy grants access to users to access resources, including broad access to data resources. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 20, 2025

New policy - SageMaker StudioUserIAMDefaultExecutionPolicy	New policy - This is the execution policy for using IAM roles with Amazon SageMaker Unified Studio. This policy grants access to users to resources. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 20, 2025
New policy - SageMaker StudioUserIAMConsolePolicy	New policy - This policy provides individual setup privileges for Amazon SageMaker Unified Studio using the AWS Management Console and SDK. It grants permissions for launching Amazon SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 20, 2025
New policy - SageMaker StudioAdminIAMPermissiveExecutionPolicy	New policy - This is an administrative execution policy for using IAM roles with Amazon SageMaker Unified Studio. This policy grants administrative access to provision, manage, and access resources, including broad access to data resources. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 20, 2025

New policy - SageMakerStudioAdminIAMDefaultExecutionPolicy	New policy - This is the administrative execution policy for using IAM roles with Amazon SageMaker Unified Studio. This policy grants administrative access to provision, manage, and access resources (excluding data resources) in your account. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 20, 2025
New policy - SageMakerStudioAdminIAMConsolePolicy	New policy - This policy provides administrative and individual setup privileges for Amazon SageMaker Unified Studio using the AWS Management Console and SDK. It grants permissions for launching Amazon SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 20, 2025

Policy updates - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding permissions to untag Amazon Athena, AWS CodeCommit, logs, scheduler, and Amazon EC2 resources. Also adding permissions to update Amazon Athena workgroups and delete the IAM role policy for Amazon SageMaker Unified Studio projects. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 15, 2025
Policy updates - SageMaker StudioDomainExecutionRolePolicy	Policy updates to the SageMakerStudioDomainExecutionRolePolicy - adding support for the following APIs: `GetAccountPool` , `ListAccountPools` , `ListAccountsInAccountPool` . For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	August 11, 2025

Policy updates - SageMaker StudioProjectUserRolePolicy	Adding permissions to support Amazon SageMaker Unified Studio seamlessly for customers with Data Catalog Encryption. Also adding `STS:SetContext` permission to support trusted identity propagation for external computes. Also updaing CloudWatch log groups to be more specific. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	July 30, 2025
Policy updates - SageMaker StudioFullAccess	Policy updates to the SageMakerStudioFullAccess - generalizing the scope for SecretsManager `create` and `tag` permissions for new domains that will have the format of `dzd-` instead of `dzd_...` Also adding permissions to allow users to use custom blueprint templates from Amazon S3 as well as upload their own template files to Amazon S3. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	July 23, 2025

Policy updates - SageMaker StudioEMRServiceRolePolicy	Policy updates to SageMaker StudioEMRServiceRolePolicy - removing unwanted KMS permissions for EMR cluster AtRestEncryption in the Amazon SageMaker Unified Studio EmrOnEc2 blueprint and adding permissions for EMR clsuter to encrypt customer data using customer managed KMS for logs pushed to Amazon S3 bucket in Amazon SageMaker Unified Studio when using EmrOnEc2 blueprint with customer managed encryptio n. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	July 23, 2025

Policy updates - SageMaker StudioProjectUserRolePolicy	Policy update - adding permissions to allow deletion of AWS Glue databases in Amazon Datalake, adding `sqlworkbench` service principals for the `redshift-serverless:GetCredentials` action, adding permissions to fetch jobs based on tags and resources, adding permissions to update Amazon CloudWatch metrics from job runs and read/write job logs, and adding permissions to support Amazon S3 access grants. Also adding permissions to allow cross-account project access for encrypted domains and adding support for `ProjectRole` and `DescribeResource` actions in order to check for the Amazon S3 tables' Lake Formation registration. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	July 15, 2025

Policy updates - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to the SageMakerStudioProjectRoleMachineLearningPolicy - adding permissions to support cross-account Amazon S3 asset subscription fulfillment using Amazon S3 access grants. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	July 15, 2025

Policy updates - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding permissions to create and manage Amazon S3 table buckets and also adding permissions to automate S3 table analytics integration flow within Amazon SageMaker Unified Studio. Also adding permissions to read templates from users' S3 buckets and permissions to validate the template using AWS Cloud Formation. Also adding permissions to get and create an S3 access grant instance in the project account to support managing subscriptions for S3 asset types. Also adding `neptune-graph:*` and `s3vectors:*` permissions to support Knowledge Base vector store management of two new vector store services in Amazon SageMaker Unified Studio: S3Vectors vector buckets and Neptune Analytics graphs. Also adding permissions to allow cross-account project access for encrypted domains. And adding support for the data onboarding in Amazon SageMaker Unified Studio.	July 15, 2025

	For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	
Policy updates - SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy	Policy updates to the SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy - adding `neptune-graph:*` and `s3vectors:*` permissions to support vector read/write on vector stores for two new vector store services: S3Vectors vector buckets and Neptune Analytics graphs. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	July 15, 2025
New policy - SageMakerStudioAdminProjectUserRolePolicy	New policy - this IAM policy grants an IAM role full access to the AWS Glue Data Catalog (metadata) and Amazon S3 (actual data) for the data lake operations, with access scoped by region, account, and role tags. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	July 15, 2025

Automated onboarding of Amazon SageMaker Lakehouse	Adding support for automated onboarding of Amazon SageMaker Lakehouse. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	July 15, 2025
Amazon QuickSight integration	Enabling Amazon QuickSight integration in Amazon SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	July 15, 2025
Policy updates - SageMakerStudioProjectUserRolePolicy	Policy updates to SageMakerStudioProjectUserRolePolicy - adding permissions to access Amazon Athena default catalog resource. Amazon SageMaker Unified Studio updates to AWS managed policies.	June 25, 2025

Policy updates - SageMaker StudioDomainExecutionRolePolicy	Policy updates to the SageMakerStudioDomainExecutionRolePolicy - adding support for the Amazon Q `GetIdentityMetadata` API action in order to obtain user's Q subscription information to set an appropriate subscription tier badge. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 18, 2025
Policy updates - SageMaker StudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - adding permissions to list Amazon Bedrock foundation models. Removing permissions to terminate EMR Cluster, change security group rules, Amazon Athena default catalog permissions, and list S3 buckets permissions at bucket level. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 13, 2025

Policy updates - SageMaker StudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - bring back previously removed permission to `ListBucket` to fix issues in AWS Glue sessions and connections. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 13, 2025
Policy updates - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding the untag role permission to fix project update failure. Also adding permissions to integrate with Amazon QuickSight. Also optimizing to reduce the policy size. And adding permissions to enable automatic sync of repositories. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 4, 2025

Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - removing RedshiftDbUser format restriction. Adding KMS permissions required by dependent services for Federated Data Connection. Adding permissions to support Amazon QuickSight integration.For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	June 4, 2025
Policy updates - AmazonDataZoneBedrockModelConsumptionPolicy	Policy updates to the AmazonDataZoneBedrockModelConsumptionPolicy - adding permissions to call the `ListFoundationModels` action. This permission is added to help get model metadata more programmatically when the user is selecting which models to invoke.For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 28, 2025

Policy update - SageMaker StudioFullAccess	Policy updates to the SageMakerStudioFullAccess - adding permissions to support attaching or updating AWS managed permissions in AWS RAM resource shares in the Amazon SageMaker console. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 22, 2025
Policy update - AmazonDataZoneBedrockModelConsumptionPolicy	Policy updates to the AmazonDataZoneBedrockModelConsumptionPolicy - adding support for the conversation history feature powered by Amazon Bedrock session management in generative AI playgrounds. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 13, 2025

Policy update - SageMakerStudioProjectRoleMachineLearningPolicy	Policy updates to the SageMakerStudioProjectRoleMachineLearningPolicy - as CodeEditor (VS Code) is introduced into Amazon SageMaker Unified Studio, users need the ability to create/delete CodeEditor space applications in Amazon SageMaker. Currently, only Amazon SageMaker space apps are allowed to be created with the JupyterLab app type. This change extends the current capability of creating/deleting JupyterLab space applications to CodeEditor (VS Code). For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	May 1, 2025

Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - adding permissions for integration with Amazon Bedrock Data Automation. Adding permissions to show Amazon Bedrock agent versions and their details to users. Adding permission to support Trusted Identity Propagation in QEv2. Ensuring project isolation for Amazon Bedrock Inline Agents. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	April 28, 2025

Policy update - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding IAM permissions for the AmazonSageMakerQueryExecution role to support query execution role creation during enabling of the Tooling blueprint. Adding the DeleteSchedule permission so that when projects are deleted, the Schedule Group can be deleted. EventBridge runs DeleteSchedule automatically on Schedule Groups when it attempts to delete them, regardless of whether the Schedule Group actually has schedules in it. This permission allows for that deleteSchedule call to be made during project deletion. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	April 28, 2025

Policy update - SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy	Policy updates to the SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy - adding support for structured data sources in Amazon Bedrock knowledge bases for generative AI app development projects. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	April 16, 2025
Policy update - SageMakerStudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - preventing sharing provisioned Amazon Redshift-Serverless across all projects. Adding EventBridge Scheduler permissions for users to create schedules in the project schedule group. Adding permissions to handle Amazon SageMaker Studio migration to Amazon SageMaker Unified Studio. Adding support for the Amazon SageMaker App type CodeEditor. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	April 9, 2025

Policy update - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding `lakeformation:DescribeResource` to improve deregistering of federated connections. Adding EventBridge Scheduler permissions to manage a schedule group for each project. Adding permission to manage Amazon Bedrock resources directly from the Amazon DataZone service. Add support for the Amazon SageMaker App type CodeEditor. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	April 9, 2025
Policy update - SageMaker StudioBedrockFlowServiceRolePolicy	Policy updates to the SageMakerStudioBedrockFlowServiceRolePolicy - adding support for using Amazon Bedrock agent nodes in Amazon Bedrock flows for generative AI app development projects. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	April 9, 2025

Policy update - SageMaker StudioDomainExecutionRolePolicy	Policy updates to the SageMakerStudioDomainExecutionRolePolicy - adding support for the GetUpdateEligibility API required by Amazon SageMaker Unified Studio to fetch update comments and determine project's eligibility for the workflow of updating projects. Also adding support for the existing Amazon DataZone Rule APIs required by Amazon SageMaker Unified Studio to mange and enforce rules. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 25, 2025
Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - preventing default AWS Glue database from being listed as it causes issues with Spark SQL. Also adding permission to use new project-wide Amazon Bedrock service role for improved scalability.For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 21, 2025

Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding permission to describe stack event for better error reporting. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 21, 2025
Policy update - SageMakerStudioBedrockFlowServiceRolePolicy	Policy updates to the SageMakerStudioBedrockFlowServiceRolePolicy - adding KMS permissions to decrypt Amazon Bedrock guardrails attached to the Amazon Bedrock flows. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 10, 2025
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding permission to change trust policy during project update to address confused deputy problem. Also adding permission to attach PartnerApps policy to the user role. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 5, 2025

Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the - renaming Amazon Bedrock tag and adding permission to removeSageMakerStudioProjectProvisioningRolePolicy deprecated tag on roles. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	March 4, 2025

Policy update - SageMaker StudioProjectUserRolePolicy	Policy updates to the SageMakerStudioProjectUserRolePolicy - changes to support shared VPC by removing ResourceAccount condition on actions dependent on VPC/subnets. Moving permissions from inline to this AWS managed policy for Amazon EMR, EMR-Serverless, and federated connections. Adding support for buckets with public access blocked with permission `s3:GetBucketPublicAccessBlock` . Adding permission to support data lineage in Amazon DataZone. Supporting Amazon LakeFormation ABAC by adding session tag the access role. Supporting users operating on private ECR. Also adding support for managing AWS Glue subscriptions by the user. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 28, 2025

Policy update - SageMaker StudioProjectRoleMachineLearningPolicy	Policy updates to the SageMakerStudioProjectRoleMachineLearningPolicy - adding support for the MLFlow Tracking Server for Shared VPC, applying visibility condition to Amazon SageMaker Search API. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 28, 2025
Policy update - SageMaker StudioProjectProvisioningRolePolicy	Policy updates to the - renaming Amazon Bedrock tag and adding permission to removeSageMakerStudioProjectProvisioningRolePolicy deprecated tag on roles. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 28, 2025
Policy update - SageMaker StudioEMRServiceRolePolicy	Policy updates to the SageMakerStudioEMRServiceRolePolicy - adding permissions to allow Amazon EMR to create network interfaces against Shared VPC.For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 28, 2025

New policies - SageMaker StudioEMRInstanceRolePolicy	Amazon SageMaker Unified Studio creates IAM roles for projects users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the permissions related to EMR. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 28, 2025
New policy - SageMaker StudioBedrockKnowledgeBaseServiceRolePolicy	This policy allows Amazon Bedrock Knowledge Bases to access Amazon Bedrock models and data sources in Amazon SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 25, 2025
New policy - SageMaker StudioBedrockKnowledgeBaseCustomResourcePolicy	This policy provides access to configure vector stores and Amazon Bedrock knowledge bases in Amazon SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 25, 2025

New policy - SageMakerStudioBedrockFunctionExecutionRolePolicy	This policy allows AWS Lambda to access an Amazon Bedrock function component's configuration in Amazon SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 25, 2025
Policy update - SageMakerStudioProjectProvisioningRolePolicy	Policy updates to the SageMakerStudioProjectProvisioningRolePolicy - adding permissions for batch grants in AWS LakeFormation to give grants to IDC users. Adding various `Update*` permissions to allow managing project resources. Removing `ResourceAccount` condition on resources depending on VPC to allow usage of shared VPC. Using new Amazon Bedrock managed policy name. Adding permissions to clean up Amazon EMR project level resources during project deletion. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 24, 2025

Policy update - SageMaker StudioProjectRoleMachineLearningPolicy	Policy updates to the SageMakerStudioProjectRoleMachineLearningPolicy - adding permission for `DescribeAutoMLJobV2` , moving multiple Amazon SageMaker `List` operations to tag based authorization, adding CMK permissions for JupyterLab, add Amazon SageMaker `ListModelPackages` and `CreateModel` permissions for cross-account use case. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 14, 2025
New policy - SageMaker StudioBedrockPromptUserRolePolicy	This policy provides access to an Amazon Bedrock prompt and its configuration in Amazon SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 14, 2025

New policy - SageMaker StudioBedrockFlowServiceRolePolicy	This policy allows Amazon Bedrock Flows to access Amazon Bedrock models and other resources attached to a flow in Amazon SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 14, 2025
New policy - SageMaker StudioBedrockEvaluationJobServiceRolePolicy	This policy allows Amazon Bedrock to access Amazon Bedrock models and datasets for evaluation jobs in Amazon SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 14, 2025
New policy - SageMaker StudioBedrockChatAgentUserRolePolicy	This policy provides access to an Amazon Bedrock chat agent app's configuration and Amazon Bedrock agent in Amazon SageMaker Unified Studio. For more informati on, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 14, 2025

New policy - SageMaker StudioBedrockAgent ServiceRolePolicy	This policy allows Amazon Bedrock Agents to access Amazon Bedrock models and other resources attached to an agent in Amazon SageMaker Unified Studio. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	February 14, 2025
Policy updates to SageMaker StudioProjectProvisioningRolePolicy	Policy updates to SageMaker StudioProjectProvisioningRolePolicy - adding permissions to manage IAM roles with only AWS managed policies attached to them and no permissions boundary. Also adding permissions to update the AWS Lambda function for Amazon Athena federated connections.For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	January 31, 2025

New policy SageMaker StudioQueryExecutionRolePolicy	New policy SageMaker StudioQueryExecutionRolePolicy - this is the default policy for the SageMakerQueryExecutionRole role. This policy provides permissions to run query executions on federated connections. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	January 31, 2025
New policy SageMaker StudioEMRServiceRolePolicy	New policy SageMaker StudioEMRServiceRolePolicy - Amazon SageMaker Unified Studio creates IAM roles for project users to perform data analytics, artificial intelligence, and machine learning actions and uses this policy when creating these roles to define the permissions related to Amazon EMR. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	January 31, 2025

Policy update to SageMaker StudioFullAccess	Policy updates to SageMaker StudioFullAccess - updating the CodeConnections tagging permissions to support tagging for CodeConnections host resources in the Amazon SageMaker console. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	January 24, 2025
Policy update to SageMaker StudioDomainExecutionRolePolicy	Policy updates to SageMaker StudioDomainExecutionRolePolicy - adding support for the AWS CodeConnections APIs in order to make the Copy button available for self-managed Git providers. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	January 24, 2025

Policy updates to SageMakerStudioProjectProvisioningRolePolicy, SageMakerStudioProjectUserRolePolicy, and SageMakerStudioProjectUserRolePermissionsBoundary	Policy updates to SageMakerStudioProjectProvisioningRolePolicy (adding permissions to support CMK in CodeCommit, AWS Glue Catalog, and Amazon Redshift Serverless), SageMakerStudioProjectUserRolePolicy (adding permissions to support CMK in CodeCommit, and AWS Glue Catalog), and SageMakerStudioProjectUserRolePermissionsBoundary (adding permissions to support CMK in CodeCommit, AWS Glue Catalog, Amazon Redshift Serverless, and EMR on EC2.) For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	December 18, 2024

New policy - SageMaker StudioProjectUserRolePolicy	Adding a new managed policy - SageMakerStudioProjectUserRolePolicy. Amazon SageMaker Unified Studio creates IAM roles for projects users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the permissions. This is the main policy for the SageMakerUnifiedStudioProjectRole role. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	December 2, 2024
New policy - SageMaker StudioProjectUserRolePermissionsBoundary	Adding a new managed policy - SageMakerStudioProjectUserRolePermissionsBoundary. Amazon SageMaker Unified Studio creates IAM roles for Projects users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the boundary of their permissions. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	December 2, 2024

New policy - SageMaker StudioProjectRoleMachineLearningPolicy	Adding a new managed policy - SageMakerStudioProjectRoleMachineLearningPolicy. Amazon SageMaker Unified Studio creates IAM roles for projects users to perform data analytics, artificial intelligence, and machine learning actions, and uses this policy when creating these roles to define the permissions related to Amazon SageMaker. This is the SageMaker policy for the SageMakerUnifiedStudioProjectRole role. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	December 2, 2024
New policy - SageMaker StudioProjectProvisioningRolePolicy	Adding a new managed policy - SageMakerStudioProjectProvisioningRolePolicy. Amazon SageMaker Unified Studio uses this policy to provision and manage resources in your account.For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	December 2, 2024

New policy - SageMaker StudioFullAccess	Adding a new managed policy - SageMakerStudioFullAccess. This policy provides full access to Amazon SageMaker Unified Studio via the Amazon SageMaker management console. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	December 2, 2024

New policy - SageMaker StudioDomainServiceRolePolicy	Adding a new managed policy - SageMakerStudioDomainServiceRolePolicy. This is the default policy for the SageMakerUnifiedStudioDomainServiceRole service role. This policy is used by Amazon SageMaker Unified Studio to access the SSM parameters in the user's account. Those parameters are set by the administrator in the Amazon SageMaker Unified Studio project profiles. This policy also has permissions to AWS KMS for encrypted SSM parameters. The KMS key must be tagged with EnableKeyForAmazonDataZone to allow decrypting the SSM parameters. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	December 2, 2024

New policy - SageMakerStudioDomainExecutionRolePolicy	Adding a new managed policy - SageMakerStudioDomainExecutionRolePolicy - default policy for the SageMakerUnifiedStudioDomainExecutionRole service role. This role is used by Amazon SageMaker Unified Studio to catalog, discover, govern, share, and analyze data in the Amazon SageMaker Unified Studio domain. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	December 2, 2024
New policy - AmazonDataZoneBedrockModelManagementPolicy	Adding a new managed policy - AmazonDataZoneBedrockModelManagementPolicy - that provides permissions to manage Amazon Bedrock model access, including creating, tagging and deleting application inference profiles. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	December 2, 2024

New policy - AmazonDataZoneBedrockModelConsumptionPolicy	Adding a new managed policy - AmazonDataZoneBedrockModelConsumptionPolicy - that provides permissions to consume Amazon Bedrock models, including invoking Amazon Bedrock application inference profile created for particular Amazon DataZone domain. For more information, see Amazon SageMaker Unified Studio updates to AWS managed policies.	December 2, 2024
Initial release	Initial release of the Amazon SageMaker Unified Studio Administrator Guide	December 2, 2024