EDI Cloud Operations Support Concepts and Procedures

EDI Cloud Operations Support Guide

EDI Cloud Operations Support Guide: EDI Cloud Operations Support Concepts and Procedures

Table of Contents

What is EDI Cloud Operations?

Energy Data Insights on AWS (EDI) managed by AWS Managed Services (AMS) helps you to easily deploy, manage, and operate your subsurface data management platform on AWS, in compliance with the Open Subsurface Data Universe (OSDU®) technical standards. For information, see AWS Announces Managed Support for Energy Data Insights.

EDI Cloud Operations (ECO), provides operational solutions and support for EDI on AWS. The ECO team of AMS operations uses a suite of native AWS services to provide a comprehensive set of operational management capabilities. With these capabilities, the ECO team creates and maintains curated sets of monitoring controls, detection guardrails, automations, and runbooks to support EDI on AWS operations in a compliant and secure way.

> **Note**
>
> ECO uses the AMS Accelerate operations plan that's referenced in this support guide. However, the scope, entitlements, and capabilities of ECO are limited to your EDI environment. Don't deploy other workloads in your EDI environment.

ECO service description

EDI Cloud Operations (ECO) provides operational solutions and support for EDI on AWS.

EDI Cloud Operations features and entitlements

ECO offers the following features:

- **Deployment and upgrades** – ECO deploys EDI on AWS instances in your AWS accounts, provides initial setup and configuration support, and deploys maintenance and feature upgrades as necessary.
- **Observability** – ECO monitors the health of your EDI environment. ECO proactively detects and responds to alerts and resolves issues in the EDI environment to maintain availability of the data platform and APIs.
- **Incident management** – ECO responds to incidents and resolves issues. You can contact ECO engineers 24x7 using the AWS Support Center Console, with response times as defined in Incident management response time.

- **Security** – ECO uses Amazon GuardDuty to identify potentially unauthorized or malicious activity in your EDI environment. The ECO team monitors GuardDuty findings 24x7. ECO also supports Amazon Macie to protect your sensitive data, such as personally identifiable information (PII) and financial data. ECO also monitors and triages all Amazon Route 53 Resolver ALERT and BLOCK events generated in EDI accounts to further inspect network traffic and augment its detective capabilities.
- **Backup management** – ECO uses backup management to take snapshots of your resources and data. ECO creates, monitors, and stores snapshots for AWS services that AWS Backup supports. The ECO team creates AWS Backup plans during EDI deployment and onboarding that define the backup schedules, frequency, and retention period. ECO tracks all backup jobs and alerts our team to run remediation when a backup job fails. If needed, ECO uses your snapshots to perform restoration actions during incidents. ECO provides you with a backup coverage report and a backup status report.
- **Problem management** – ECO performs trend analyses to identify and investigate problems. Problems are remediated either with a workaround or a permanent solution that prevents the recurrence of similar future service incidents. After the incident is resolved, you can request a post incident report (PIR). The PIR captures the root cause and actions taken, including preventative measures.
- **Designated experts** – ECO designates an EDI Solutions Delivery Manager (E-SDM) to partner with your organization and drive operational and security excellence. Your E-SDM provides you with guidance during and after configuration and onboarding. The E-SDM is your point of contact for EDI operational needs and collaborates with your AWS account team to deliver a monthly report of your operational metrics.
- **Logging and reporting** – ECO aggregates and stores logs that are generated because of operations in Amazon CloudWatch, AWS CloudTrail, and Amazon Virtual Private Cloud (Amazon VPC) Flow Logs. Logging helps the ECO team more quickly resolve incidents and audit systems. Your designated E-SDM provides you with a monthly service report that summarizes key performance metrics of EDI. The service report includes an executive summary and insights, operational metrics, EDI API service level agreement (SLA) adherence, and spending and savings metrics.
- **Service request management** – Use the AWS Support Center Console to request information about your EDI instances. You can submit a service request for "How to" questions about EDI features or to request additional EDI support.
- **Application management** – ECO performs EDI deployment on your behalf, updates and upgrades your EDI instances, and supports EDI instance deletion and offboarding.

EDI Cloud Operations terminology

ECO uses the following general terms:

- Managed environment or EDI environment: The AWS accounts where EDI on AWS is deployed (only EDI resources).
- Billing start date: The next business day after AWS receives the information that's requested in your EDI onboarding email. The EDI onboarding email is the email that AWS sends to you to collect the necessary information to activate EDI.
- Service termination: The process of cancelling EDI on AWS, which permanently removes all EDI-related services, OSDU® instances, and associated data from your account. This action is irreversible but doesn't affect account ownership.
- Event: A change in your EDI environment.
- Alert: When an event from a supported AWS service within your EDI environment exceeds a threshold and triggers an alarm, an alert is created. A notice is then sent to the ECO team, and an incident is added to your incident list.
- Incident: An unplanned interruption or performance degradation that affects your EDI environment and is reported by ECO or you.
- Problem: A shared underlying root cause of one or more incidents.
- Incident resolution:
  - ECO has restored all unavailable EDI services or resources that pertain to the incident to an available state.
  - Or ECO has determined that they can't restore unavailable stacks or resources to an available state.
- Incident response time: The difference in time between when you create an incident, and when ECO provides an initial response through the console, email, Support Center, or telephone.
- Incident resolution time: The difference in time between when either ECO or you create an incident and when the incident is resolved.
- Incident priority: How you or ECO prioritizes incidents as either Low, Medium, or High. For definitions, see Incident priority.

  ECO might recategorize incidents in accordance with the guidelines.
- Infrastructure restore: When an incident resolution isn't possible, ECO initiates a data restore based on the last known restore point, unless you specify otherwise.

- CSAT: EDI customer satisfaction (CSAT) is based on deep analytics that include quarterly surveys, Case Correspondence Ratings (CCR) on every case, and case correspondence when given.
- ITIL: Information Technology Infrastructure Library (ITIL) is an IT service management (ITSM) framework that's designed to standardize the lifecycle of IT services. ITIL is arranged in five stages of the IT service lifecycle: service strategy, service design, service transition, service operation, and service improvement.
- ITSM: A set of practices that align IT services with the needs of your business.
- MMS: Managed Monitoring Services (MMS) is a monitoring system that ECO operates that consumes AWS Health events and aggregates data from CloudWatch and other AWS services. Then, MMS uses an Amazon Simple Notification Service (Amazon SNS) topic to notify ECO operators (online 24x7) of alarms.

ECO uses the following infrastructure terms:

- Managed production environment: The account where your production applications are.
- Managed non-production environment: The account that contains only non-production applications, such as applications for development and testing.
- EDI stack: A group of AWS resources that ECO manages as a single unit.
- SLAs: The service-level agreement (SLA) defines the level of service you can expect from EDI.

ECO uses the following security terms:

- Detective controls: A library of EDI-created or enabled monitors that provides ongoing oversight of your EDI environment that doesn't align with security, operational, or customer controls. Detective controls notify owners and proactively modify or terminate resources.
- Service request: A request by you for an action that you want ECO to take on your behalf.
- Alert notification: A notice that ECO posts to your service requests list page when an EDI alert is initiated.

EDI on AWS supported configurations

For a list of configurations that ECO supports, see Supported configurations in the *AMS Accelerate User Guide*.

EDI on AWS supports the following AWS Regions, languages, and operating systems:

- **AWS Regions:**
  - US East (N. Virginia)
  - US West (Oregon)
  - Asia Pacific (Singapore)
  - Europe (Ireland)
  - Europe (Paris)
  - South America (São Paulo)
  - Asia Pacific (Mumbai)
  - Asia Pacific (Sydney)
- **Language** – English.
- **Operating systems** – See the AMS Accelerate Service description documentation.

EDI version support policy for Amazon EKS versions

To keep your EDI environment up to date and secure, it's important to understand the EDI support policy as it relates to Amazon Elastic Kubernetes Service (Amazon EKS) versions.

EDI on AWS uses Amazon EKS to facilitate core functions of the data platform. Given this dependency, we recommend that you upgrade to the latest EDI version as soon as it becomes available to enable standard support on Amazon EKS. If you stay on a previous EDI version and exceed the standard Amazon EKS support window, Amazon EKS offers an extended support option that provides an additional year of support. To learn more and estimate future Amazon EKS costs, see Amazon EKS extended support for Kubernetes versions pricing.

Your Amazon EKS clusters are automatically transitioned from standard support to extended support, with no further actions for you. If you remain on extended support, AWS continues to support your EDI version up to the previous two EDI versions. AWS also supports up to the last day of the extended Amazon EKS support version.

For example, if the latest EDI version is M24, then AWS supports M23 up to March 2026. When Amazon EKS versions reach the end of extended support, AWS force-upgrades the Amazon EKS service. Adhering to the policy helps maintain support for your EDI instance and provides you with access to the latest features and security updates.

For a list of end of support dates for Kubernetes, see the Amazon EKS Kubernetes release calendar in the *Amazon EKS User Guide*.

The following table provides an example summary of supported EDI versions. You can get the latest information from your E-SDM.

EDI versio	OSDU Forum Releas Date	EDI Soluti Releas Date	End of Amazon EKS standard support	End of extended support
M24(E 1.32)	Octob 2024	July 2025	March 2026	March 2027
M23(E 1.29)	May 2024	Augus 2024	March 2025	March 2026

EDI Cloud Operations supported services

ECO provides operational management support services only for EDI on AWS.

EDI Cloud Operations roles and responsibilities

The ECO responsible, accountable, consulted, and informed, or RACI, matrix assigns primary responsibility either to you or ECO for a variety of activities.

Each letter in RACI represents a different party that's involved in the matrix:

- **R** is the responsible party that does the work to achieve the task.
- **A** is the accountable party that gets the work done to complete the task.
- **C** is the consulted party whose opinions are sought, typically as subject matter experts (SMEs); and with whom there's bilateral communication.
- **I** is the informed party who's notified about the progress of a task, usually only on task completion.

ECO manages your EDI on AWS environment. The following table provides an overview of the activities in the lifecycle of an EDI application that runs within the managed environment. The "Customer" column represents your roles and responsibilities, and the "AWS" column represents the roles and responsibilities of ECO.

Activity	Customer	AWS
Provisioning		
EDI solution (Operations, Data Platform, and EDI IQ) deployment in the customer's account	C, I	R, A
EDI Data Portal initial admin user creation	C, I	R, A
EDI Data Portal user creation and management	R, A	C
EDI hosted zone creation and management for Data Portal	R	I
Monitoring and Logging		
EDI solution monitoring	I	R, A
AWS infrastructure monitoring	C, I	R, A
Recording AWS infrastructure change logs	I	R, A
Deploying and managing third-party monitoring tools, such as Dynatrace and New Relic	R, A	C
Data load and ingestion		
Data ingestion and reingestion from the application, the EDI IQ and custom sources—such as CSV, WITSML, Manifest, and Code Pipeline— into the EDI cluster	R, A	C
Missing or incorrect data validation and indexing issues	R	C
Disaster recovery		
Performing point-in-time backup restoration activities through AWS managed services, such as Amazon Relational Database Service (Amazon RDS), and Amazon DynamoDB	C	R, A
Backup and restore for EDI entitlement through Amazon OpenSearch Service	C	R, A

Activity	Customer	AWS
Deploying and reviewing backup plans	C	R, A
Deploying and managing third-party backup tools, such as Commvault	R, A	C
Migration		
Migrating data from the existing OSDU® to the EDI environment	R, A	C
Data snapshot backup and restore through AWS Disaster Recovery	R, A	C
Upgrades and patching		
Upgrading the EDI environment	I	R
Patching the EDI environment and AWS infrastructure for hotfixes or security vulnerabilities	I	R
Notification for EDI end of life support	I	R
Approval for EDI environment upgrade	R	I
Incident management		
Proactively notifying incidents on the EDI environment and AWS infrastructure that are based on monitoring	I	R
Categorizing incident priority	I	R
Providing incident response	I	R
Providing incident resolution and infrastructure restore	C, I	R
Documentation and training		
Providing customer documentation about the EDI architecture and EDI on AWS operations	I	R
Leading and conducting incident response processes through game days with the customer	C, I	R, A

Activity	Customer	AWS
Participating in incident response processes through game days	R	A, C
Troubleshooting		
EDI deployment issues	I	R
API endpoint connection failures	I	R
Data ingestion failures	R	C
EDI environment functionality issues and outages	C	R

ECO SIR roles and responsibilities

The following tables describe your (the "Customer") responsibilities compared with our ("AWS") responsibilities for the phases of security incident response (SIR).

Security incident response – Detect Phase

Activity	Customer	AWS
Logging, indicators, and monitors		
Configuring logs and monitors to enable event management for instances and accounts	C, I	R
Monitoring supported AWS services for security alerts	I	R
Deploying and managing endpoint security tools	R	I
Monitoring for malware on instances using endpoint security	R	I
Notifying customers of detected events through outbound messaging	I	R
Routing notification and subsequent updates to the decision makers for specific accounts and workloads to improve incident response time	C, I	R

Activity	Customer	AWS
Defining, deploying, and maintaining ECO standard detection services such as Amazon GuardDuty and AWS Config	C, I	R
Recording AWS infrastructure change logs	C	R
Implementing and maintaining an allowlist, denylist, and custom detections on supported AWS security services, such as Amazon GuardDuty	R	C

Security incident response – Analyze Phase

Activity	Customer	AWS
Investigation and analysis		
Performing an initial response for supported security alerts that a supported detection source generated	I	R, C
Using available data to assess false and true positives	C, I	R
Reviewing ECO assessments for false and true positives that ECO shares	R	C
Generating a snapshot of affected instances that ECO shares with the customer, if needed	I	R
Performing forensics tasks such as chain of custody, file system analysis, memory forensics, and binary analysis	R	C, I
Collecting application logs to help with troubleshooting	C	R
Collecting data and logs that are accessible to ECO to help investigate security alerts	C, I	R
Responding to the alerts to help ECO investigate	R	C, I
Engaging SMEs within ECO services on security investigations	C, I	R

Activity	Customer	AWS
Engaging third-party vendors during investigation such as for EPS anti-malware	R, C, I	I
Sharing investigation logs from supported AWS services to customers during an investigation	I	R
Communication		
Sending alerts and notifications from ECO detection sources for managed resources	I	R
Managing alerts and notifications for application security events	C	R
Engaging the customer security point of contact during a security incident investigation	R	I

Security incident response – Contain Phase

Activity	Customer	AWS
Containment strategy and execution		
Deciding on the execution of the agreed containment strategy and agreeing with the consequences that might affect the availability of services during the containment window	R	C, I
Backing up affected systems for further analysis	C, I	R
Containing applications and workloads through application-specific configuration or response activity	C, I	R
Defining the containment strategy based on the security incident and the affected resource	C, I	R
Enabling encryption and secure storage of point-in-time backups of affected systems	R, C, I	C

Activity	Customer	AWS
Executing supported containment actions for AWS resources, including Amazon Elastic Compute Cloud (Amazon EC2) instances, network, and AWS Identity and Access Management (IAM)	C, I	R

Security incident response – Eradicate Phase

Activity	Customer	AWS
Eradication strategy and execution		
Defining eradication options based on the security incident and the affected resource on customer application workloads	R	C, I
Deciding on the agreed eradication strategy, timing of eradication execution and the consequences	R	C, I
Defining eradication steps based on the security incident and the affected resource on ECO managed workloads	C, I	R
Eradicating and hardening AWS resources including Amazon EC2 instances, network, and IAM	C, I	R
Eradicating and hardening applications and workloads through application-specific configuration or response activity	R	I

Security incident response – Recover Phase

Activity	Customer	AWS
Recovery preparation and execution		
Configuring backup plans and targets as requested by the customer	C	R
Reviewing backup plans to restore ECO managed workloads	C	R

Activity	Customer	AWS
Performing backup restoration activities for resources of supported AWS services	I	R
Reviewing and confirming backup plans to restore customer applicati ons and workloads post-incident	R, A	C, I
Backing up customer applications, application configurations, and deployment settings to restore customer applications and workloads post-incident	C, I	R, A
Restoring applications and customer workloads through application-specific restoration steps	R, C	R, C

Security incident response – PIR Phase

Activity	Customer	AWS
Post incident reporting		
Sharing appropriate lessons learned and action items with customer as required	I	R, A

Incident management response time

Incidents that you create in the AWS Support Center or AWS Support API have different classifications from incidents that you create in the AMS console.

Incident priority	Response time
Priority 1 Incident (High)	<= 15 mins
Priority 2 Incident (Medium)	<= 4 hours
Priority 3 Incident (Low)	<= 12 hours

Scope of changes performed by EDI Cloud Operations

ECO deploys or updates AWS resources only in the following situations through a predefined access model:

- To deploy and update tools and resources required by ECO to service EDI.
- As part of EDI monitoring in response to events and alarms.
- To remediate security issues as part of responses to violations in EDI such as making noncompliant resources conform to security best practices.
- During remediation and restoration as part of an incident response.
- During deployment, application patching, and updates for major and minor releases of EDI.
- When configuring the following ECO features:
  - Alarm manager
  - Resource tagger
  - Resource scheduler
  - Backup plans

ECO doesn't deploy or update resources outside the preceding situations.

Contacting EDI Cloud Operations

Your designated E-SDM provides advisory assistance across EDI and has a detailed understanding of your use case and technology architecture for your managed environment. Your E-SDM works with account managers, technical account managers (TAMs), cloud architects (CAs), and AWS solutions architects (SAs), as applicable. The E-SDM is your primary point of contact for EDI.

The following are the primary responsibilities of your E-SDM:

- Organize and lead monthly service review meetings with you.
- Provide details on security, software updates for your EDI environment, and opportunities for optimization.
- Champion your requirements, including feature requests for EDI on AWS.
- Respond to and resolve billing and service reporting requests.

EDI Cloud Operations contact hours

The following table lists the ECO contact hours:

Feature	ECO team
Service request	24 hours a day, 7 days a week
Incident management	24 hours a day, 7 days a week
Backup and recovery	24 hours a day, 7 days a week
Patch management	24 hours a day, 7 days a week
Monitoring and alerting	24 hours a day, 7 days a week
E-SDM	Monday to Friday: 08:00 – 17:00, local business hours

EDI Cloud Operations escalation path

ECO supports customers with incident management and service request management, 24 hours a day, 7 days a week, 365 days a year in accordance with the Incident management response time.

To report an EDI service performance issue, use the AWS Support Center and submit an incident case. For details, see Submitting EDI incidents. For general information about ECO incident management, see Incident management in ECO.

To request information, advice, or additional services from ECO, use the AWS Support Center and submit a service request. For details, see Creating EDI service requests.

Onboarding to EDI Cloud Operations

After you sign up for EDI and accept the terms of agreement, your E-SDM guides you through the onboarding process and checklist.

The initial steps to onboarding EDI are as follows:

1. On the EDI on AWS – OSDU® Data Platform product page, choose **Contact an Industry Expert** to open a contact form.
2. Provide the requested information, and then choose **Submit**.

   An EDI representative will contact you with EDI usage terms.
3. Review and accept the EDI usage terms and sign a contract with AWS for an EDI subscription. The EDI Cloud Operations team then initiates the onboarding process for your organization, including sending an onboarding email and assisting you with following actions:
   a. Accept the onboarding email and provide the requested EDI deployment parameters.
   b. Create new EDI on AWS accounts, one account for user management and a separate account for EDI IQ.

ECO notifies you when the deployment is successful and provides a URL for you to start using EDI.

Using the AMS console

The AMS console is available for you to interact with ECO. The console behaves similarly to other AWS consoles. However, only EDI on AWS enabled accounts can access the AMS console for EDI. After EDI is deployed in your account, you can search for **Managed Services** in the unified search bar to access the AMS console.

The console is account specific. So, if you're in a "Test" account for your organization, you can't see resources in the "Prod" account for the organization.

When you authenticate, the console applies an IAM policy that determines which console you can access and what you can do there. Your administrator might apply additional statements to the default policy to restrict what you can see and do in the console.

The console has the following features:

- Opening page – Has information and a **Get started** text box with a link to the **Dashboard** that includes the following information:
  - **Incidents on your resources** – Has a button to open an incident case in AWS Support Center, and shows how many incident cases are open, waiting for approval and require your attention
  - **Compliance status** – Links to the **Rules and Resources** page that shows are noncompliant and compliant rules and resources
  - **Service requests** – Has a button to open a service request case in AWS Support Center, and shows how many cases are open, waiting for approval and require your attention
  - **Account-level security** – Links to details on real-time threat detection findings from GuardDuty and data security and privacy findings from Macie
  - **Quick actions** – Links to **Go to backup vaults** and **Create patch maintenance window**
- Feature pages in the left-hand navigation pane:
  - **Dashboard** – Includes the preceding information
  - **Reports** – Opens a page with links to your current ECO reports
  - **Configuration** – Opens a page with links to common AMS configuration tasks
  - **Documentation** – Opens the AWS Managed Services Documentation landing page

Setting up notifications

Communication between you and your ECO team occurs for the following reasons:

- Events that monitoring alerts create
- Service requests and incident reports
- Occasional important EDI Cloud Operations announcements. Your E-SDM contacts you when action is required on your part

ECO or your E-SDM sends all notifications to the email address that you provided when you were onboarded. We recommend that you use a group email address that you can easily update rather than individual email addresses. You can use named lists of contacts for non-resource based notifications, such as alerts based on GuardDuty or AWS Config. For example, you might have a list that's named SecurityContacts for security alarms and notifications.

Offboarding an EDI account

After you send an EDI Service Termination Request with at least a 30-day notice, ECO offboards your account. The Service Termination Date is the last day of the calendar month following the end of the required 30-day termination notice period. If the end of the termination notice period is after the 20th day of the calendar month, then the Service Termination Date is the last day of the following calendar month.

To request offboarding an account you must take the following actions:

1. Submit a formal service request to offboard the account. The request must include all the EDI instances that you want to offboard.
2. Inform your E-SDM about the EDI instances that you want to offboard and request their help with the offboarding process.

Incident reports, service requests, and billing questions in EDI Cloud Operations

You can get help with EDI on AWS at any time through the AWS Support Center. ECO operations engineers are available to respond to your incidents and service requests all day and night, and all week, within response times as defined in Incident management response time.

Incident management in ECO

In ECO, you can use the AWS Support Center Console to create incidents. Incidents are EDI performance issues that affect your managed environment, as determined by ECO or you. An incident that the ECO team identifies is first received as an "event," which is a change in the system state that monitoring captures. If a configured threshold is exceeded, then the event initiates an alarm, also called an alert. The ECO team determines if the event is non-impacting, an incident, or a problem. The ECO team also receives incidents that you programmatically create using the AWS Support API with the `service-ams-operations-report-incident` service code.

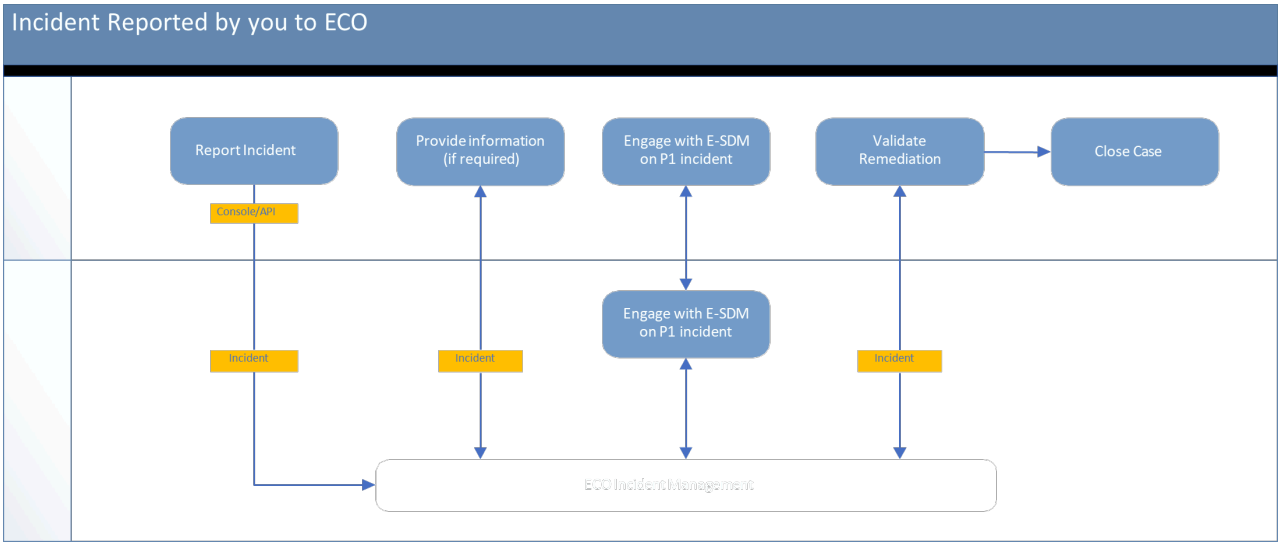
What is incident management?

Incident management is the process that ECO uses to record, act on, communicate the progress of, and provide notification of active incidents. The incident management process quickly restores operations for EDI on AWS, minimizes business impact, and keeps concerned parties informed.

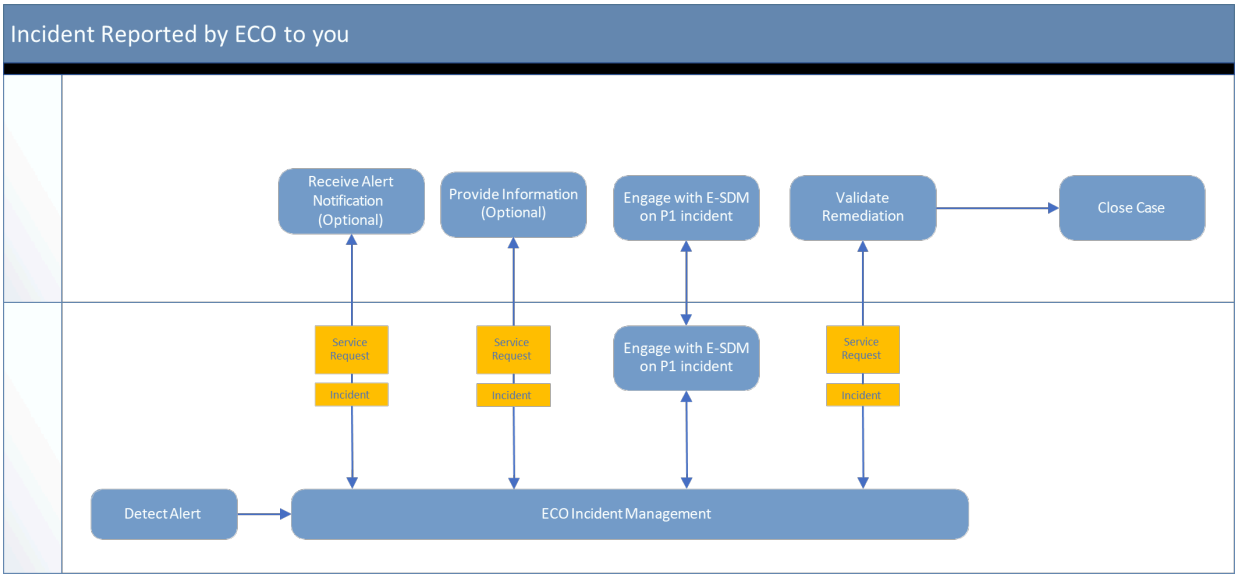
The following issues are examples of incidents that ECO manages:

- Loss or degradation of network connectivity
- An unresponsive process or API
- A scheduled task that isn't being performed, such as a failed backup

The following graphic shows the workflow of an incident reported by you to ECO.



The following graphic shows the workflow of an incident reported by ECO to you.



Incident priority

Incidents that you create in AWS Support Center or AWS Support API have different classifications from incidents that you create in the AMS console.

The following classifications define the priority level for AWS or EDI related services and applications:

- **Low** – Non-critical functions of your business service or application are impacted.
- **Medium** – A business service or application is available but isn't performing according to the applicable service description.

- **High** – Your business is significantly impacted. Critical functions of your application or resources are unavailable. The **High** priority level is reserved for the most critical outages that affect production systems.

> **Note**
>
> The AWS Support Center Console offers five levels of incident priority that we modified to the preceding three levels of priority.

Incident resolution

ECO uses IT service management (ITSM) incident management best practices to restore service as quickly as possible. We provide all day and night, all week, all year, follow-the-sun support through operations centers around the world with dedicated operators that actively watch monitoring dashboards and incident queues.

> **Note**
>
> For incident response times, see Incident management response time

Our operations engineers use internal incident tracking tools to identify, log, categorize, prioritize, diagnose, resolve, and close incidents. We provide you with updates on all the activities through the AWS Support Center and the AWS Support API. Our operators are deeply familiar with EDI supported infrastructure and have expert-level technical skills to address identified issues. If ECO operators need assistance, they contact the AWS Support and AWS service teams.

After the ECO team receives your incident, they validate the priority and classification and work with you if they require clarifications. For example, if the incident report is better classified as a service request, they reclassify it, the ECO service request team takes over, and you're notified. ECO operators consult internal documentation to quickly resolve the incident. If an operator can't resolve the incident, they escalate it to other support teams. After it's resolved, the ECO team documents the incident and resolution for future use.

In cases where critical severity incidents are impacting your crucial workloads, ECO might recommend a restore. The risks of a restore and the impact from the required service downtime

help determine whether the ECO team restores from a known functional backup. If the issue is urgent, then ECO can initiate a restore. If a restore is too risky, then ECO will help you troubleshoot the issue.

Working with incidents in the Support Center

You can perform the following tasks in the AWS Support Center:

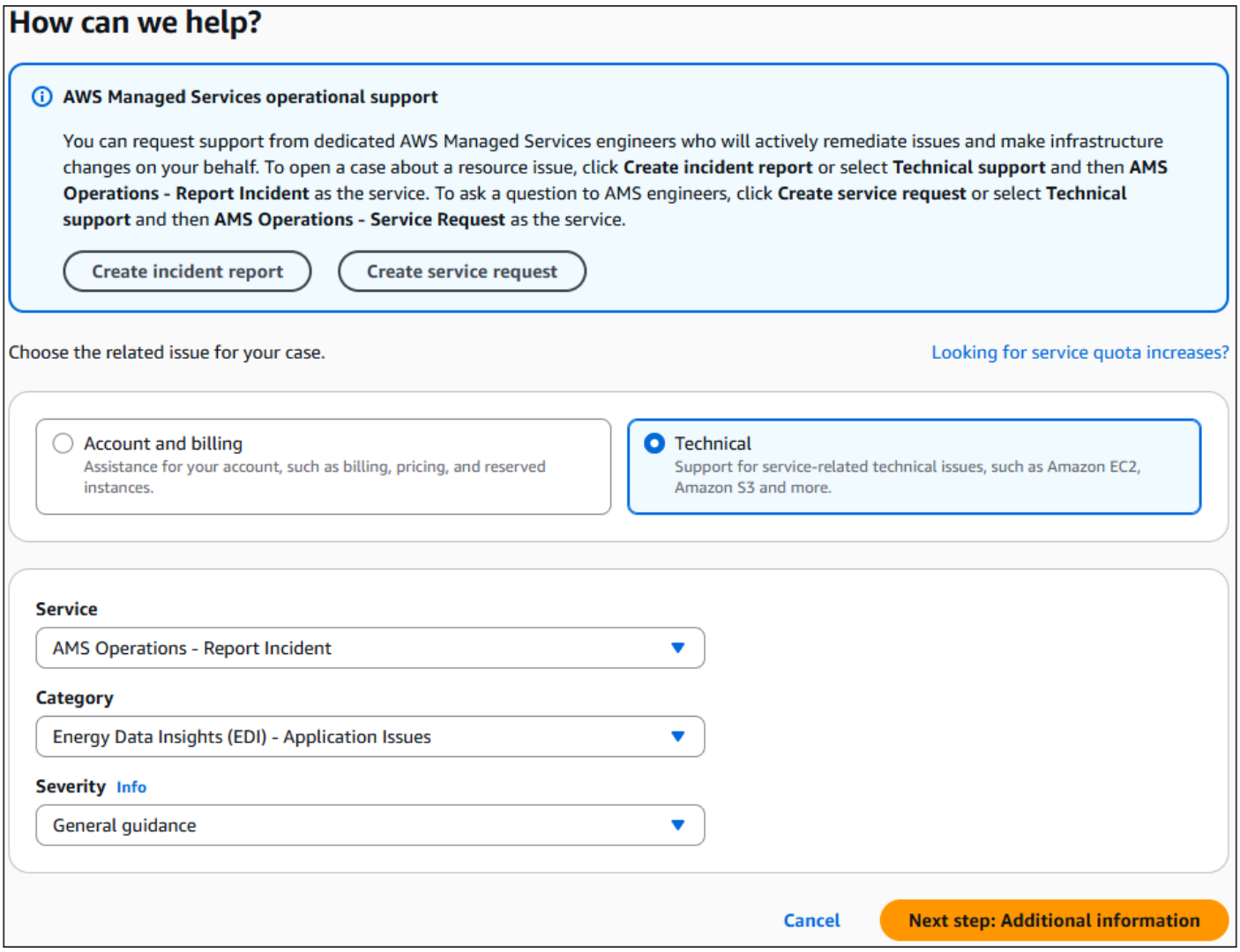
- Report and update an incident.
- Get a list of and detailed information about your submitted incidents.
- Narrow your search for incidents by status and other filters.
- Add communications and file attachments to your incidents and add email recipients for case correspondence.
- Initiate a live chat or request a callback on your incident.
- Resolve incidents.
- Rate incident communications.

After you submit an incident, the ECO team works with you to resolve the incident according to the incident response time matrix.

Submitting EDI incidents

To report an incident, follow these steps:

1. Sign in to Support Center Console.
2. Choose **Create case** and then **Create incident report**. The **Technical** support issue type auto-selects.



3. Choose options from the following menus:

   a. **Service** – AMS Operations – Report Incident is selected by default

   b. For **Category** – select Energy Data Insights (EDI) – Application Issues

   c. **Severity** – as appropriate

   Choose **Next step: Additional information**. The **Additional information** page opens.

4. Include information about your incident and then choose **Next step: Solve now or contact us**. The **Solve now or contact us** page opens to the **Solve now** tab by default.

5. The **Solve now** tab offers AI generated suggestions for your incident. Choose **Next**. The **Contact us** tab opens.

6. On the **Contact us** tab, ensure that **English** is your preferred language because EDI supports only English for incident reports. Choose a contact method:

- **Web**, selected by default – An ECO representative emails your configured contact.
- **Phone** – An ECO representative calls you back. Enter your AWS Region, phone number, and extension if applicable.
- **Chat** – Chat online with an ECO representative. This option adds you to the chat queue.

Use the **Additional contacts** option to add email addresses you want copied on your incident report.

7. Choose **Submit**. A case details page opens with information on the incident and a **Correspondence** area that includes the description of the report that you created. To provide additional details or updates in status, choose **Reply**. For cases that include a lot of correspondence, choose **Load More** to view all communication.
8. After the incident has been resolved, choose **Resolve Case**. Be sure to rate the service through the 1-5 star rating to let the ECO team know how we're doing.

> **Note**
>
> Make your description as detailed as possible. Include relevant resource information, along with anything else that might help us understand your issue. For example, to troubleshoot performance, include timestamps and logs. For feature requests or general guidance questions, include a description of your environment and purpose. In all cases, follow the Description Guidance that appears on your case submission form. When you provide as much detail as possible, you increase the chances that ECO can quickly resolve your case. You can use the AWS Support API with the `service-ams-operations-report-incident` service code to report an incident.

For more information about how to use the AWS Support Center Console to report an incident, see Creating support cases and case management in the *AWS Support User Guide*.

Service request management in ECO

ECO uses service request management to record, act on, communicate the progress of, and provide notification of active service requests.

When to submit EDI service requests

The following are examples of when to submit a service request:

- EDI or AWS general guidance
- Questions about the functionality of EDI services
- Billing-related queries

Don't submit a service request for the following:

- Access issues
- Portal issues
- Backup failure

Instead, submit an incident report, see Working with incidents in the Support Center.

How service requests work

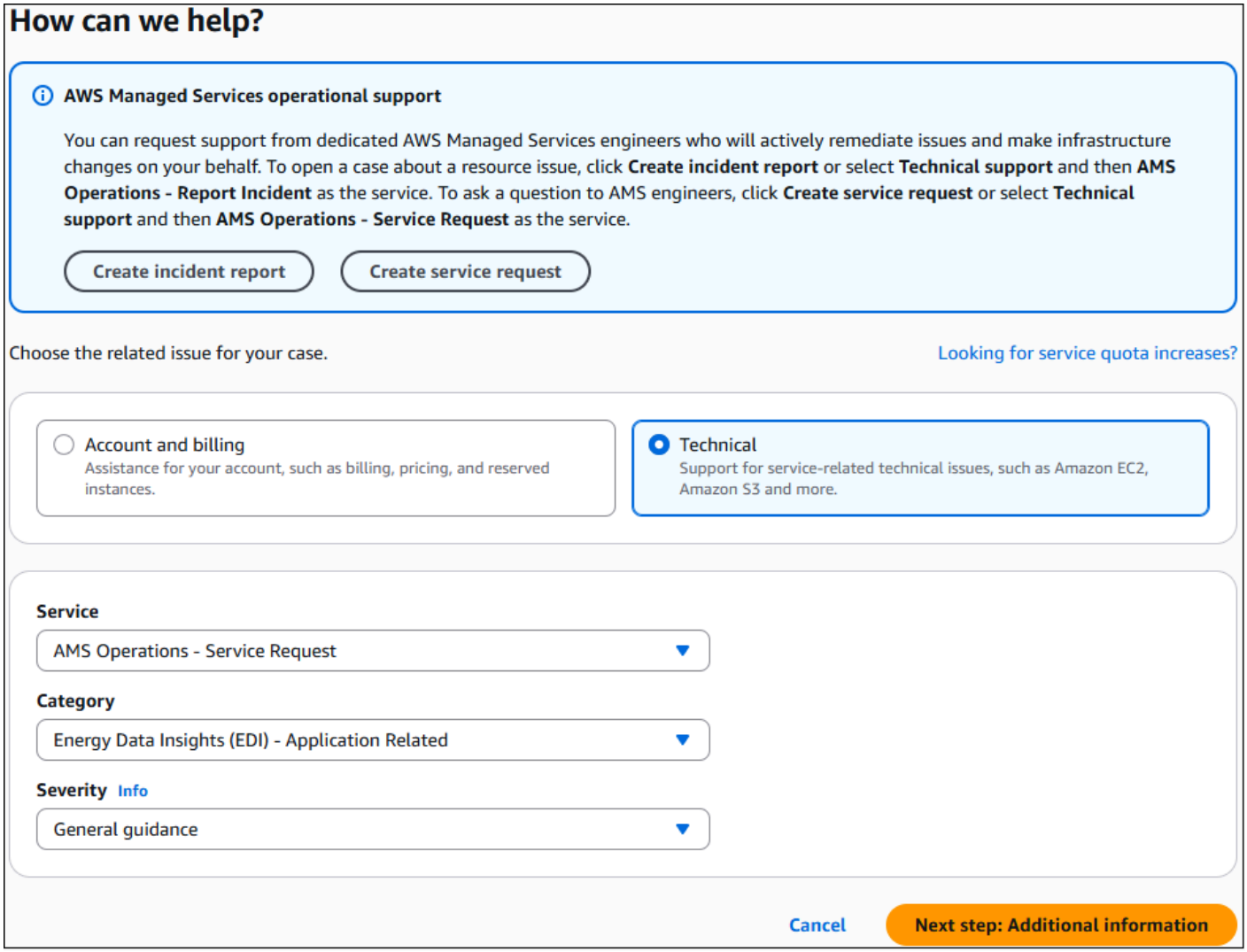
The ECO team handles service requests. The ECO team reviews your service request to make sure that it's appropriately classified as a service request or an incident. If the ECO operator reclassifies the request as an incident, the ECO incident management process begins, and you're sent a notification. The ECO operator immediately begins to resolve incidents that are within their scope. For example, if the service request is for architecture advice or other information, the operator answers your question or refers you to the appropriate resources. If the analysis of your service request identifies a bug or a feature request, then ECO sends you a notification through the service request. Because there's no estimated times for feature requests or bug fixes, the original service request is closed. Contact your E-SDM to ask follow-up questions that are related to the original service request

If the service request is out of scope for ECO operations, the operator sends the request to the appropriate AWS team or to your E-SDM. The ECO operator also sends you an email about the steps that the ECO team is taking. The service request isn't resolved until you've indicated that you're satisfied with the outcome.

Creating EDI service requests

To create a service request, follow these steps:

1. Sign in to the Support Center Console.
2. Choose **Create case** and then **Create service request**. The **Technical** support issue type auto-selects.



3. Choose options from the following menus:
   a. **Service** – AMS Operations – Service Request is selected by default
   b. For **Category** – select Energy Data Insights (EDI) – Application Issues
   c. **Severity** – as appropriate

   Choose **Next step: Additional information**. The **Additional information** page opens.
4. Include information about your service request and then choose **Next step: Solve now or contact us**. The **Solve now or contact us** page opens to the **Solve now** tab by default.
5. The **Solve now** tab offers AI generated suggestions for your service request. Choose **Next**, The **Contact us** tab opens.

6. On the **Contact us** tab, ensure that **English** is your preferred language because EDI supports only English for service requests. Choose a contact method:
   - **Web**, selected by default – An ECO representative emails your configured contact.
   - **Phone** – An ECO representative calls you back. Enter your AWS Region, phone number, and extension if applicable.
   - **Chat** – Chat online with an ECO representative. This option adds you to the chat queue.

   Use the **Additional contacts** option to add email addresses you want copied on your service request.
7. Choose **Submit**. A case details page opens with information on the service request and a **Correspondence** area that includes the description of the request that you created. To provide additional details or updates in status, choose **Reply**. For cases that include a lot of correspondence, choose **Load More** to view all communication.
8. After the service request has been resolved, choose **Resolve Case**. Be sure to rate the service through the 1-5 star rating to let the ECO team know how we're doing.

> **Note**
>
> If you're going to test service request functionality, we recommend that you add a no-action flag to your service request's subject, such as **AMSTestNoOpsActionRequired**. Then, you can test without starting the service request resolution process.

Monitoring and updating EDI service requests (console)

For detailed information about how to use AWS Support Center to monitor a case, incident, or service request, see Monitoring and updating an Accelerate incident in the *AMS Accelerate User Guide*.

Monitoring and updating EDI service requests (API)

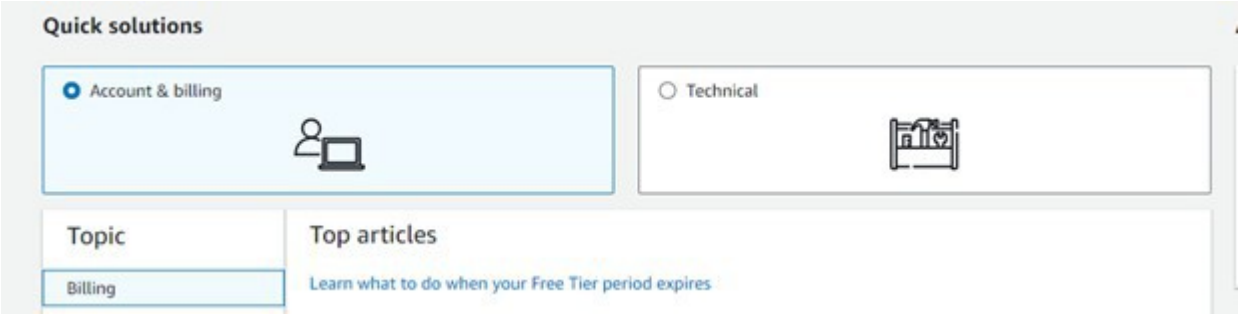
You can use the AWS Support API to create service requests and add correspondence throughout investigations of your issues and interactions with AWS Support. Similar to AWS Support, the ECO team also receives service requests programmatically created by you using the AWS Support API with the `service-ams-operations-service-request` service code.

For information about how to use the AWS Support API, see Managing Accelerate incidents with the support API in the *AMS Accelerate User Guide*.

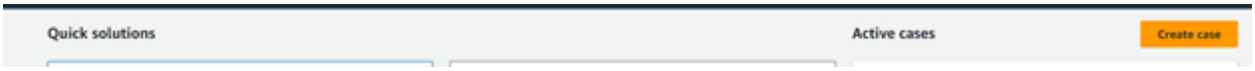
Submit EDI billing questions

To submit a billing-related question:

1. Open the Support Center Console.
2. Choose **Account & billing**.



3. Choose **Create case**.



EDI self-service reports and options

The following self-service reports are available to you:

- **Monthly billing charges report** – Details about EDI monthly billing charges.
- **Weekly incident report** –The aggregated list of incidents with its priority, severity and latest status, including:
  - Data on support cases that are categorized as incidents on the managed account
  - Incident information that's required to visualize the incident metrics for the managed account
  - Data on incident categories and the remediation status of every incident

  Both visualization and datasets are available in the Weekly incident report.

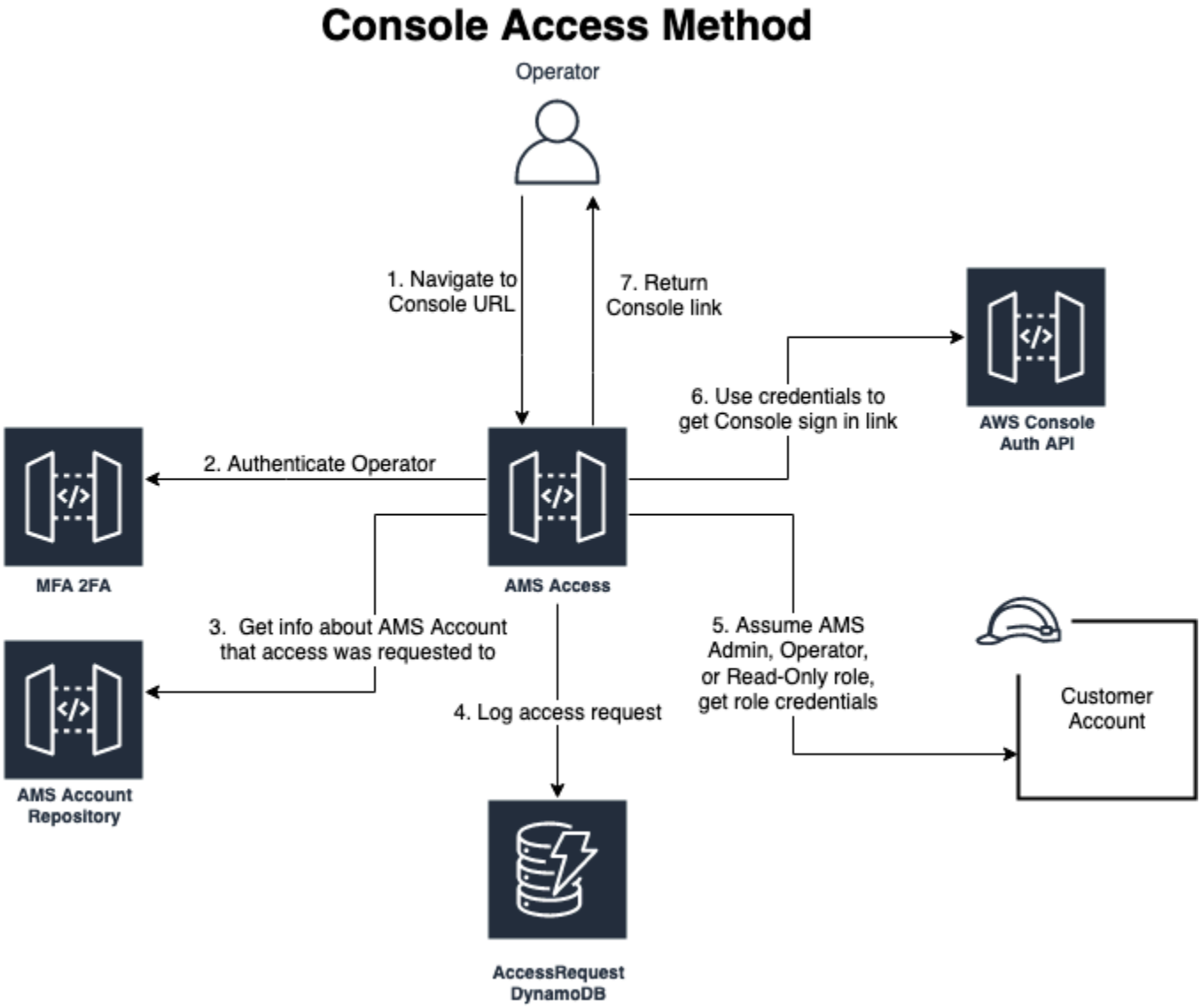
For information about how to use the AWS Support Center to submit billing questions, see Billing questions for Accelerate in the *AMS Accelerate User Guide*.

To learn more about visualization and dataset reporting, see Incident report (weekly) in the *AMS Accelerate User Guide*.

Access management for EDI

To protect your resources, access management allows only authorized and authenticated access.

ECO operators can access your account console and instances only in certain circumstances. The following graphic shows the authentication process that ECO operators complete before they can log into the AWS console for an EDI account.



For more information about access management, see Access management in AMS Accelerate in the *AMS Accelerate User Guide*.

EDI customer account access

Important

During the EDI account onboarding and deployment, ECO requests root user permission.

When you first create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account.

Important

We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *IAM User Guide*.

ECO uses a predefined access model to access your EDI account. For more information, see How AMS accesses your account.

For more information about ECO customer account access, see Why and when AMS accesses your account.

EDI Cloud Operations Data Portal access

At the time of onboarding, an ECO operator assumes an administrator role that allows them to access your Data Portal and fulfill initial user management requests. The ECO operator uses this role only to administer the portal, with no access to customer data.

EDI Cloud Operations customer account access reasons

In certain circumstances ECO operators can access your account console and instances to manage your resources. You can view these access events in your AWS CloudTrail logs.

EDI customer account access activity is driven by triggers in response to CloudWatch alarms and events, and incident reports or service requests that you submit. The ECO operator might perform multiple service calls and host-level activities for each access.

Access justification, the triggers, and the initiator of the trigger are listed in the following table.

Access	Initiator	Trigger
Internal problem investiga tion	ECO	Problem issue (an issue that has been identified as systemic)
Alert investigation and remediation	ECO	AWS Systems Manager operational work items (SSM OpsItems)
Incident investigation and remediation	You	Inbound support case (an incident or service request that you submit)
Inbound service request fulfillment	You	Inbound support case (an incident or service request that you submit)

For information about how to review ECO operations and automation activity in your account, see Tracking changes in your AMS Accelerate accounts, in the *AMS Accelerate User Guide*.

EDI Cloud Operations customer account access IAM roles

The ECO operators require the following roles to service your account.

> **Important**
>
> Don't modify or delete these roles.

IAM roles for AMS and ECO access to customer accounts

Role name	Description
ams-access-admin	This role has full administrative access to your account without restrictions. AMS services use this role with restrictive session policies that limit access to deploy AMS infrastructure and operate your account.
ams-access-admin-operations	This role grants AMS operators administrative permissions to operate your account. This role doesn't grant read, write, or delete permissio ns to customer content in AWS services that are commonly used as data stores, such as Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), Amazon DynamoDB, Amazon Redshift, and Amazon ElastiCache. Only qualified AMS operators who have a strong understanding of access management can assume this role. These operators serve as an escalation point for access management issues and access your accounts to troubleshoot AMS operator access issues.
ams-access-management	AMS operators manually deploy this role during onboarding. The AMS Access system requires this role to manage ams- access-roles and ams-access-managed- policies stacks.
ams-access-operations	This role has permissions to perform administr ative tasks in your accounts. This role doesn't have read, write, or delete permissio ns to customer content in AWS services that are commonly used as data stores, such as Amazon S3, Amazon RDS, Amazon DynamoDB, Amazon Redshift, and ElastiCac

Role name	Description
	he. Permissions to perform AWS Identity and Access Management (IAM) write operations are also excluded from this role. AMS operators and cloud architects (CAs) can assume this role.
ams-access-read-only	This role has read-only access to your account. AMS operators and CAs can assume this role. Read permissions to customer content in AWS services that are commonly used as data stores, such as Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift, and ElastiCache, are not granted this role.
ams-access-security-analyst	This AMS security role has permissions in your AMS account to perform dedicated security alert monitoring and security incident handling. Only a few AMS Security individuals can assume this role.
ams-access-security-analyst-read-only	This AMS security role is limited to read-only permissions in your AMS account to perform dedicated security alert monitoring and security incident handling.
eks-osdu-{{$region}}-cluster-management-role	This role has permissions to perform administr ative tasks on the Amazon EKS cluster. AMS operators assume this role to access the cluster and perform any change activity.
ams_ssm_automation_role	Assumed by AWS Systems Manager to execute SSM Automation documents within your account.

Role name	Description
ams-container-connector-lambda-role-{{$region}}	AMS operators assume this role to access the cluster for any read-only operations. This role is used to access the Amazon EKS cluster through the AWSManagedServices-RunKubernetesScript document.
EDIDeploymentFulfillmentRole EDIDeploymentFulfillmentIQRole	AMS operators use this role to deploy the EDI solution and IQ ingestion on the respective accounts.
osdu-*, *edi*, *ediiq*	Don't modify or delete roles or policies starting with or having the term “osdu”, “edi”, “ediiq” in their names. EDI services use these terms to connect between the AWS resources. These terms can be case sensitive.

Security management for EDI

ECO uses AWS Managed Services (AMS) for security management. AMS uses multiple controls to protect your information assets and to help you keep your AWS infrastructure secure.

AMS maintains a library of AWS Config Rules and remediation actions so that all your accounts comply with industry standards for security and operational integrity. AWS Config Rules continuously tracks configuration changes in your recorded resources. If a change violates rule conditions, ECO reports its findings and allows you to automatically remediate violations or request remediation according to its severity. AWS Config Rules facilitate compliance with standards set by the following organizations:

- The Center for Internet Security (CIS)
- The National Institute of Standards and Technology (NIST) Cloud Security Framework (CSF)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Payment Card Industry (PCI) Data Security Standard (DSS)

AMS also uses Amazon GuardDuty to identify potentially unauthorized or malicious activity in your AWS environment. AMS monitors GuardDuty findings all day and week. AMS collaborates with you to understand the impact of the findings and identify remediation based on best practice recommendations.

AMS also uses Amazon Macie to protect your sensitive data such as personal health information (PHI), personally identifiable information (PII) and financial data.

For more information about security management for an AMS operations plan, see Security management in AMS Accelerate, in the *AMS Accelerate User guide*.

ECO security incident response

For information about security incident response, see Security incident response in AMS in the *AMS Accelerate User Guide*.

Monitoring and event management for EDI

The ECO monitors your EDI resources, including Amazon EKS resources for failures, performance degradation, and security issues.

As a managed account, ECO configures and deploys alarms for applicable EDI resources and Amazon Managed Service for Prometheus alert manager rules. ECO monitors these resources and performs incident management and remediation when needed.

ECO also relies on internal tools, such as AMS Accelerate Resource Tagger and Alarm Manager. ECO also uses native AWS services, such as AWS AppConfig, Amazon CloudWatch, Amazon EventBridge, Amazon GuardDuty, Amazon Macie, AWS Health, Amazon Managed Grafana and AWS Lambda.

Log management in EDI

ECO configures supported AWS services to collect logs. ECO uses the logs to monitor compliance and audit resources within your account.

For detailed information, see Log management in Accelerate in the *AMS Accelerate User Guide*.

Track changes in your EDI accounts

ECO provides log management and an interface that you can query through the Amazon Athena console to help you track ECO automation and changes that the ECO operations team makes.

For details on tracking changes in ECO, see Tracking changes in your AMS Accelerate accounts in the *AMS Accelerate User Guide*.

View your EDI accounts' change records

To view your EDI account change records, submit a ticket with ECO or use the Amazon Athena console.

For more information on viewing change records using the Amazon Athena console, see Viewing your change records in the *AMS Accelerate User Guide*.

Backup and continuity management for EDI

EDI uses the default AMS backup plans with AWS Backup to centralize and automate backups of your data across AWS services. AMS backup plans provide best practices for various use cases. You can also continue to use your existing backup plans. After you onboard to an EDI backup solution, ECO provides backup reports. ECO experts continuously monitor your backup tasks so that you have a reliable backup solution.

The ECO team enables backups for Amazon RDS, DynamoDB, and Amazon EC2 instances in your account as part of the default backup plan. To learn more, see How AWS Backup works with supported AWS services, in the *AWS Backup User Guide*.

How continuity management works

AMS backup plans for EDI define how frequently AWS Backup backs up your data and the retention policy for your backups. ECO backup vaults keep your backup data organized. After you associate a compatible resource with a backup plan, AWS Backup automatically backs up the resource. The first backup is a full copy, and subsequent backups capture incremental changes.

The ECO team applies the default backup plan for your EDI environment that provides a reasonable restoration and retention period. However, there are other enhanced and data sensitive backup plans. To determine the most effective backup plan for your environment, work with your E-SDM when you're onboarding.

The following table lists the backup plan restoration and retention periods.

Default backup plan	Start time	Retention
hourly backup	N/A	N/A
daily backup	daily 4:00 UTC	7 days
weekly backup	Saturday, 2:00 UTC	4 weeks
monthly backup	First day of the month, 2:00 UTC	26 weeks
yearly backup	Jan 1, 2:00 UTC	2 years

ECO default backup plan

AWS Backup doesn't support "continuous backups" for ECO default backup plans. For information about different types of backup plans, see Continuous backups and point-in-time recovery (PITR).

Use the following tag key–value pair to identify EDI resources that you want ECO to back up.

`TAG key: ams:rt:backup-orchestrator TAG value: true`

> **Important**
>
> Backup monitoring and reporting are only available in EDI supported regions.

Resources that EDI Cloud Operations back up

The following table lists the AWS resources that ECO backs up for EDI with the default backup up plan.

AWS resource	Purpose
Data Platform	
DynamoDB	Persistent storage for OSDU management data, reference data, and metadata
Aurora PostgreSQL	Reservoir Domain Data Management Service (DDMS)
Amazon S3 (optional)	Persistent storage for all data records
Amazon EBS	Volume storage that Amazon EKS persisten t volume claims use. Applications that run in Amazon EKS, such as MongoDB to store data entitlements for authorization, and Amazon OpenSearch Service to store indexes and saved searches, require persistent storage
EDI IQ	

AWS resource	Purpose
DynamoDB	Table that contains the EDI IQ Terraform state files
RDS for MySQL	Persistent storage for EDI IQ job scans and ingestion statuses
Amazon S3 **delta_lake** folder only	The **delta_lake** folder containing the metadata of scanned data. Backed using an Amazon S3 replication rule

> **Note**
>
> By default, ECO doesn't back up the Amazon S3 data from your Data Platform account that contains OSDU data records. ECO uses the default backup plan to back up the **delta_lake** folder that contains ingestion metadata from the Amazon S3 source bucket for the EDI IQ console.

If you require changes to the default backup plan, work with your E-SDM during onboarding. Or submit a service request from your account.

ECO backup monitoring and reporting

ECO generates daily self-service reports and monthly reports on resource coverage and backup job status. Your ESDM shares the monthly reports are in Monthly Business Reviews (MBRs). To learn more about daily backup reports, see Backup report (daily) in the *AMS Accelerate User Guide*.

ECO experts monitor all your backup tasks. If a backup fails, ECO investigates the failure and informs you of the root cause and remediation options, if available.

Document history for EDI Cloud Operations Support Guide

Change	Description	Date
Updated EDI version support policy section	Updated the **EDI version support policy for Amazon EKS versions** section to reflect the latest EDI version.	September 8, 2025
Additional supported AWS Regions	The Asia Pacific (Mumbai) and Asia Pacific (Sydney) AWS Regions are now supported.	September 8, 2025
EDI Cloud Operations initial publishing.	Introducing the EDI Cloud Operations service.	July 24, 2025

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.