aws

User Guide

AWS B2B Data Interchange

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS B2B Data Interchange: User Guide

Copyright © 2025 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 AWS B2B Data Interchange? 1
How to get started with B2B Data Interchange 1
Accessing B2B Data Interchange 2
AWS B2B Data Interchange concepts 3
Profiles 3
Transformers 4
Trading capabilities 6
Partnerships 7
Using Transfer Family with B2B Data Interchange 8
Getting started with AWS B2B Data Interchange 10
Prerequisites for using AWS B2B Data Interchange 10
Sign up for an AWS account 10
Create a user with administrative access 11
Configure an Amazon S3 bucket 12
Amazon S3 bucket policies and permissions 13
Quick setup using the console 19
Setting up using a template 20
Transforming and generating EDI 21
Generative AI-assisted EDI mapping 21
Generative AI-assisted EDI mapping prerequisites 22
Notes about generative AI-assisted EDI mapping 22
Using generative AI-assisted EDI mapping in AWS B2B Data Interchange 23
Inbound EDI 27
Transforming inbound EDI 29
Create a profile 29
Create an inbound transformer 31
Create a trading capability for inbound EDI 33
Create a partnership for inbound EDI 35
EDI acknowledgements 37
Outbound EDI 39
Generating outbound EDI 41
Create a profile 41
Create an outbound transformer 43
Create a trading capability for outbound EDI 47

Create partnership ... 49
Delimiters for outbound EDI ... 50
Control numbers ... 51
Managing events using EventBridge ... 53
AWS B2B Data Interchange events ... 54
Sending AWS B2B Data Interchange events ... 54
Creating event patterns ... 55
Testing event patterns for AWS B2B Data Interchange events ... 56
Permissions ... 56
Additional resources ... 56
Events detail reference ... 57
Details fields for transformation events ... 57
Details fields for acknowledgement events ... 61
EventBridge Example events for B2B Data Interchange ... 64
Security ... 68
Data protection ... 68
Data encryption ... 69
No data saved ... 71
Deleting resources ... 71
Identity and access management ... 71
How AWS B2B Data Interchange works with IAM ... 71
Identity-based policy examples ... 78
Authenticating with identities ... 81
Managing access using policies ... 84
Troubleshooting ... 86
Compliance validation ... 88
Resilience ... 89
Monitoring ... 91
Monitoring with CloudWatch ... 91
EventBridge ... 94
CloudTrail logs ... 94
AWS B2B Data Interchange information in CloudTrail ... 95
Understanding AWS B2B Data Interchange log file entries ... 96
AWS CloudFormation resources ... 99
AWS B2B Data Interchange and AWS CloudFormation templates ... 99
Learn more about AWS CloudFormation ... 99

AWS PrivateLink 100
Considerations 100
Create an interface endpoint 100
Create an endpoint policy 101
Quotas 103
X12 transaction sets 104
HIPAA Transaction sets 154
Document history 157

What is AWS B2B Data Interchange?

AWS B2B Data Interchange automates the transformation and generation of Electronic Interchange Data (EDI) documents to and from JSON and XML data formats. Businesses use EDI to exchange transactional data with trading partners, such as suppliers and end customers, using common EDI standardized formats such as X12, EDIFACT, or HL7v2.

Currently, many of these businesses use EDI solutions that charge fixed licensing fees, lack operational visibility, and require tedious onboarding processes that result in transactional errors and missed SLAs. Use of these traditional EDI solutions often lead to ever-growing operational costs and damaged relationships with business partners. With B2B Data Interchange, customers can use a low-code interface to easily manage their business partner relationships and automate the transformation or generation of EDI documents at scale and with pay-as-you-go pricing.

AWS B2B Data Interchange reduces the time, complexity, and cost associated with managing and exchanging transactional data across organizational boundaries. As a result, customers can easily move data to and from their downstream business applications or data lakes and focus more on gaining insight from their data using the various analytics, artificial intelligence, and machine learning services offered by AWS.

> **Note**
>
> To estimate costs associated with using AWS B2B Data Interchange, see the pricing calculator available at AWS pricing calculator.

How to get started with B2B Data Interchange

If you are a first-time user of B2B Data Interchange, we recommend that you begin by reading Transforming and generating EDI.

For a self-paced learning experience, go through the EDI document exchange with AWS B2B Data Interchange Workshop, created by the B2B Data Interchange service team. In this workshop, you learn how to receive and transform EDI documents from your business partners using AWS B2B Data Interchange and AWS Transfer Family.

Accessing B2B Data Interchange

You can work with AWS B2B Data Interchange in any of the following ways.

AWS Management Console

The console is a web-based user interface for managing B2B Data Interchange and AWS resources. If you've signed up for an AWS account, you can access the B2B Data Interchange console by signing into the AWS Management Console and choosing B2B Data Interchange from the AWS Management Console home page.

AWS Command Line Interface

You can use the AWS command line tools to issue commands or build scripts at your system's command line to perform AWS (including B2B Data Interchange) tasks.

The AWS Command Line Interface (AWS CLI) provides commands for a broad set of AWS services. The AWS CLI is supported on Windows, macOS, and Linux. To get started, see the *AWS Command Line Interface User Guide*.

AWS SDKs

The architecture of B2B Data Interchange is designed to be programming language-neutral, using AWS supported interfaces to store and retrieve objects. You can access B2B Data Interchange and AWS programmatically by using the AWS B2B Data Interchange REST API. The REST API is an HTTP interface to B2B Data Interchange.

For information about the AWS SDKs, including how to download and install them, see Tools for AWS.

AWS B2B Data Interchange concepts

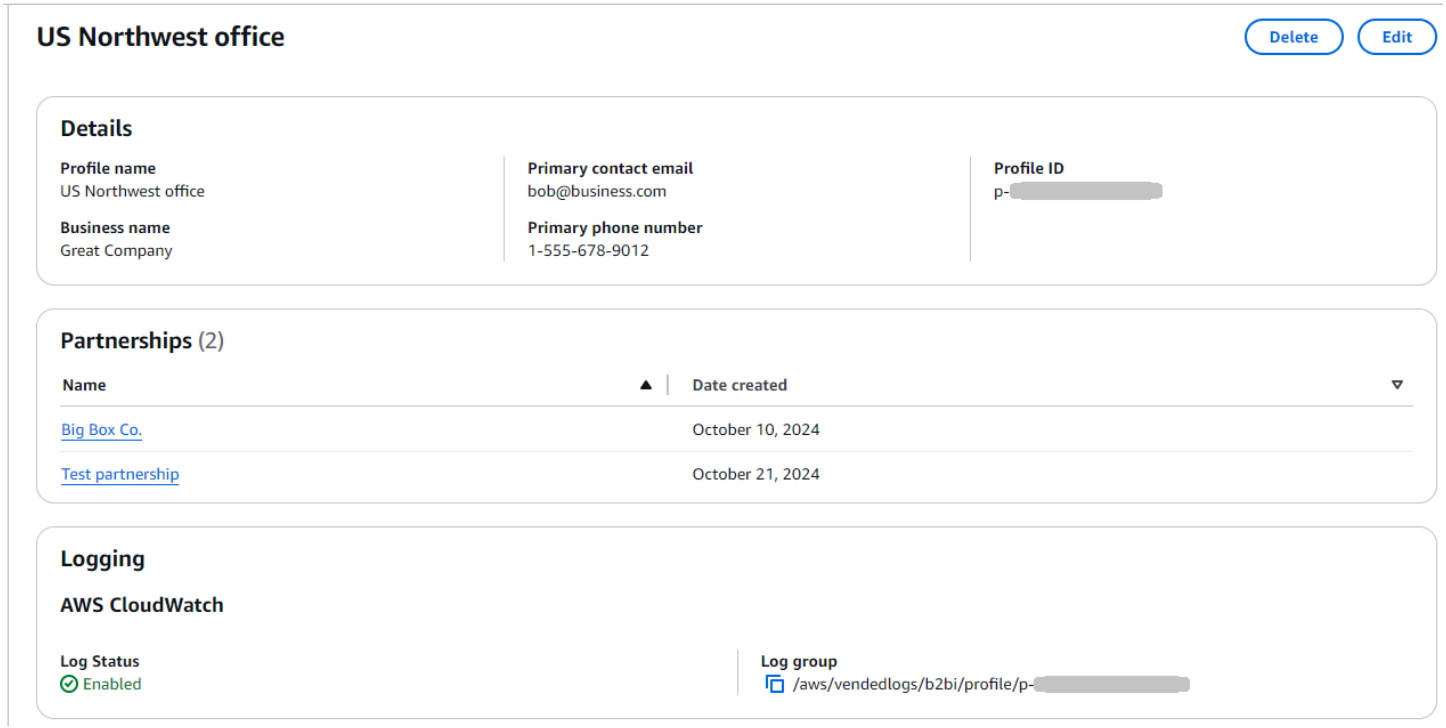
You can configure AWS B2B Data Interchange (B2B Data Interchange) to monitor specific locations in Amazon S3 to automate transformation of your X12 EDI documents to JSON/XML and to generate X12 EDI documents from JSON/XML data inputs. This topic outlines the resources needed to fully automate your EDI workflows at scale.

Topics

- Profiles
- Transformers
- Trading capabilities
- Partnerships

Profiles

A *profile* stores details and contact information about your own business. We recommend that you enable logging to monitor transformation activities and tag your profiles so that you can organize, search, and filter your profiles globally.



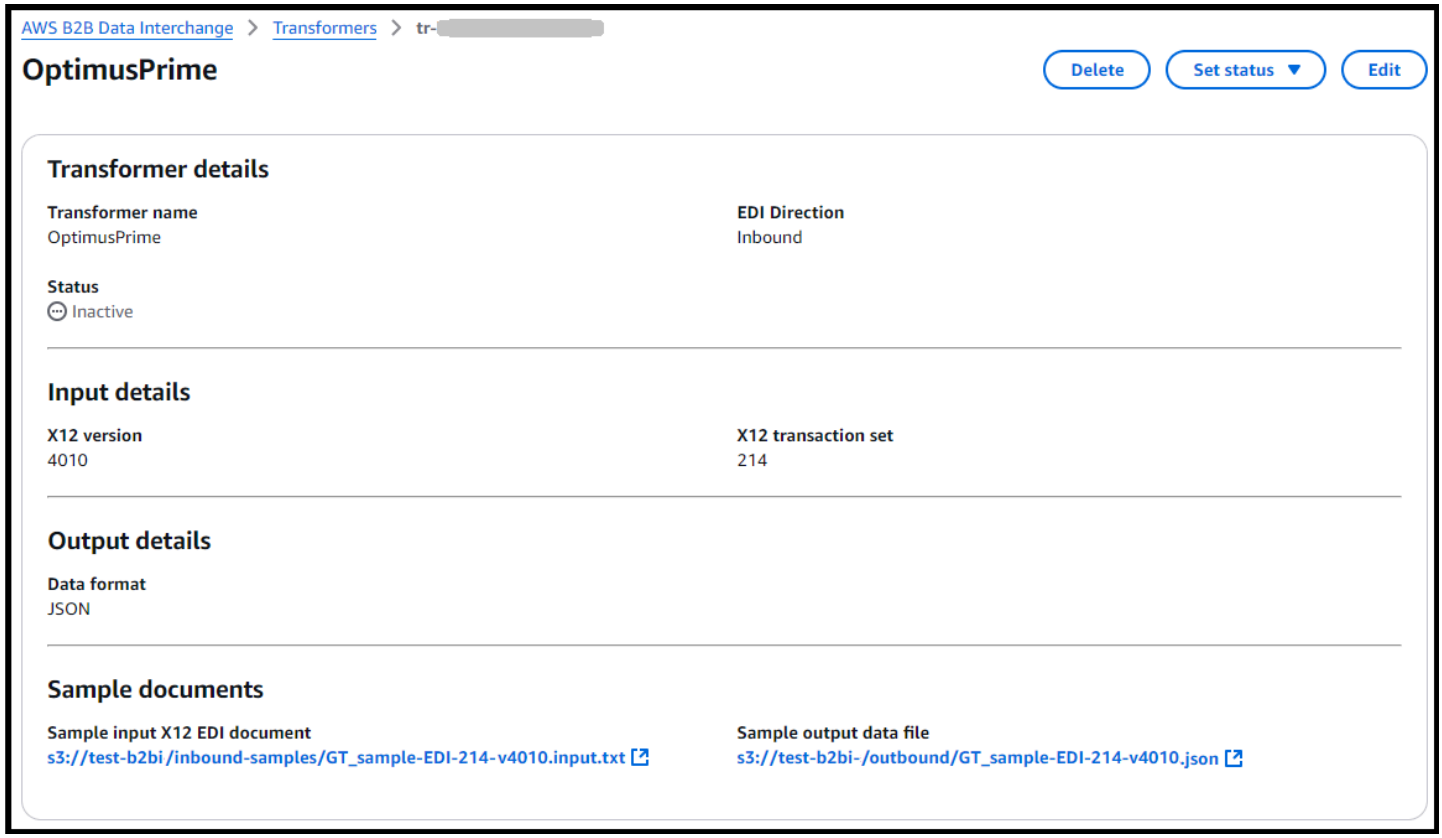
Transformers

A *transformer* allows you to provide specific instructions on how to transform or generate X12 EDI. When creating a transformer, you specify the direction of your EDI, the X12 transaction set and version, and the common data representation (either JSON or XML). We highly recommend that you provide sample input and output documents that the service uses to create a template for your transformations. Finally, if you've provided sample documents, you can use the mapping editor to customize your output to align with a specific JSON / XML schema or to align to the service-defined schema required to generate outbound EDI. The mapping editor is where you add your EDI mapping code in JSONata (for JSON) or XSLT (for XML) to customize the transformation of your data.

After you have configured your transformer resource and set it to **Active**, you can attach it to a trading capability to automate the transformation of your documents.

Note

- Transformers are created with a status of **Inactive**. To use a transformer in a trading capability, you must change its status to **Active**.
- You can only delete transformers if they are not used by any trading capability.
- JSONata and XSLT are open source query and transformation languages.


AWS B2B Data Interchange > Transformers > tr-
OptimusPrime
Delete
Set status
Edit
Transformer details
Transformer name
OptimusPrime
EDI Direction
Inbound
Status
Inactive
Input details
X12 version
4010
X12 transaction set
214
Output details
Data format
JSON
Sample documents
Sample input X12 EDI document
s3://test-b2bi/inbound-samples/GT_sample-EDI-214-v4010.input.txt
Sample output data file
s3://test-b2bi-/outbound/GT_sample-EDI-214-v4010.json

Mapping
Mapping template
Custom mapping of X12 input sample
{
"interchanges": [
{
"ISA_01_AuthorizationQualifier": "00",
"ISA_02_AuthorizationInformation": " ",
"ISA_03_SecurityQualifier": "00",
"ISA_04_SecurityInformation": " ",
"ISA_05_SenderQualifier": "02",
"ISA_06_SenderId": "CPC ",
"ISA_07_ReceiverQualifier": "ZZ",

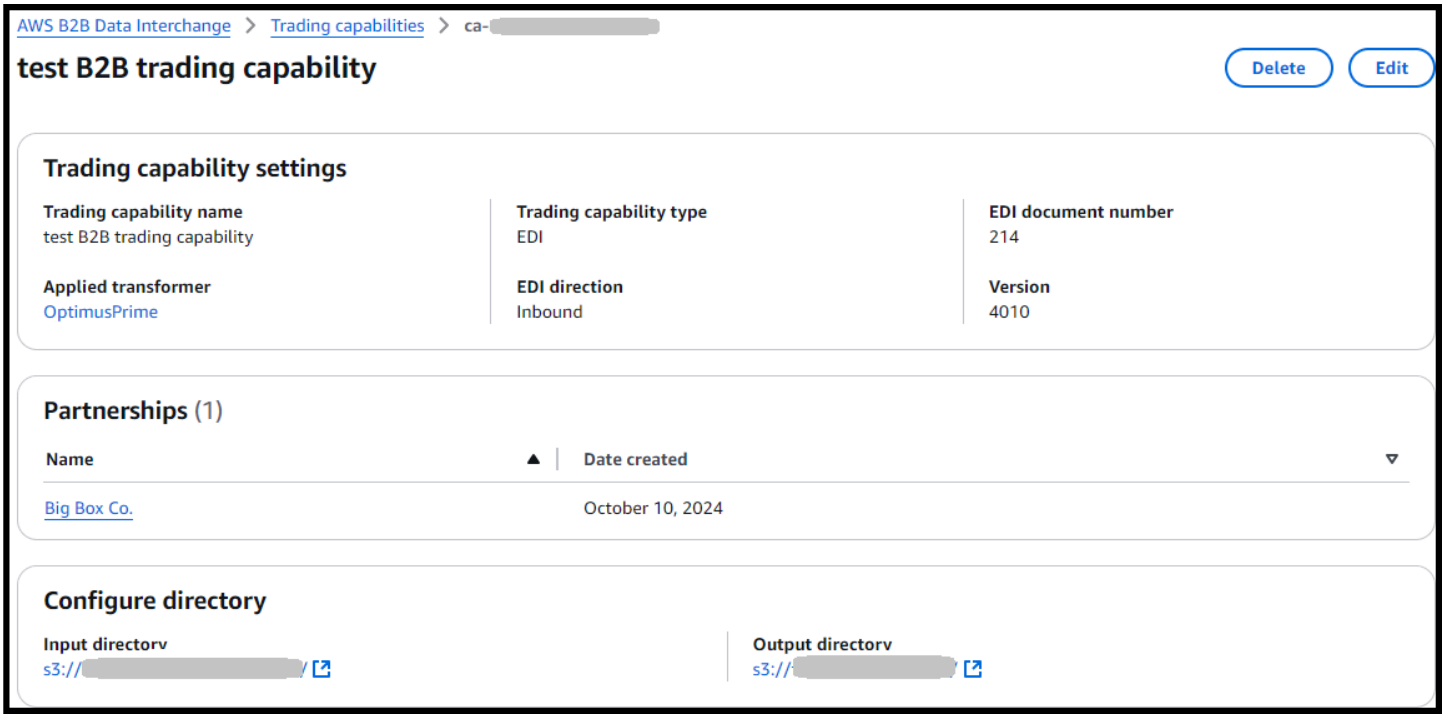
Trading capabilities

A *trading capability* contains the information required to build your event-driven EDI workflows. To create a trading capability, specify the EDI direction, add details about the EDI document number and version, choose the transformer to use to transform or generate your EDI, and specify the input and output directories used to source and store documents. Based on the EDI direction selected and the transformer attached to the trading capability, you can use the trading capability to automatically:

- Transform incoming EDI documents into JSON or XML outputs.
- Transform XML or JSON data stored in Amazon S3 into EDI documents.

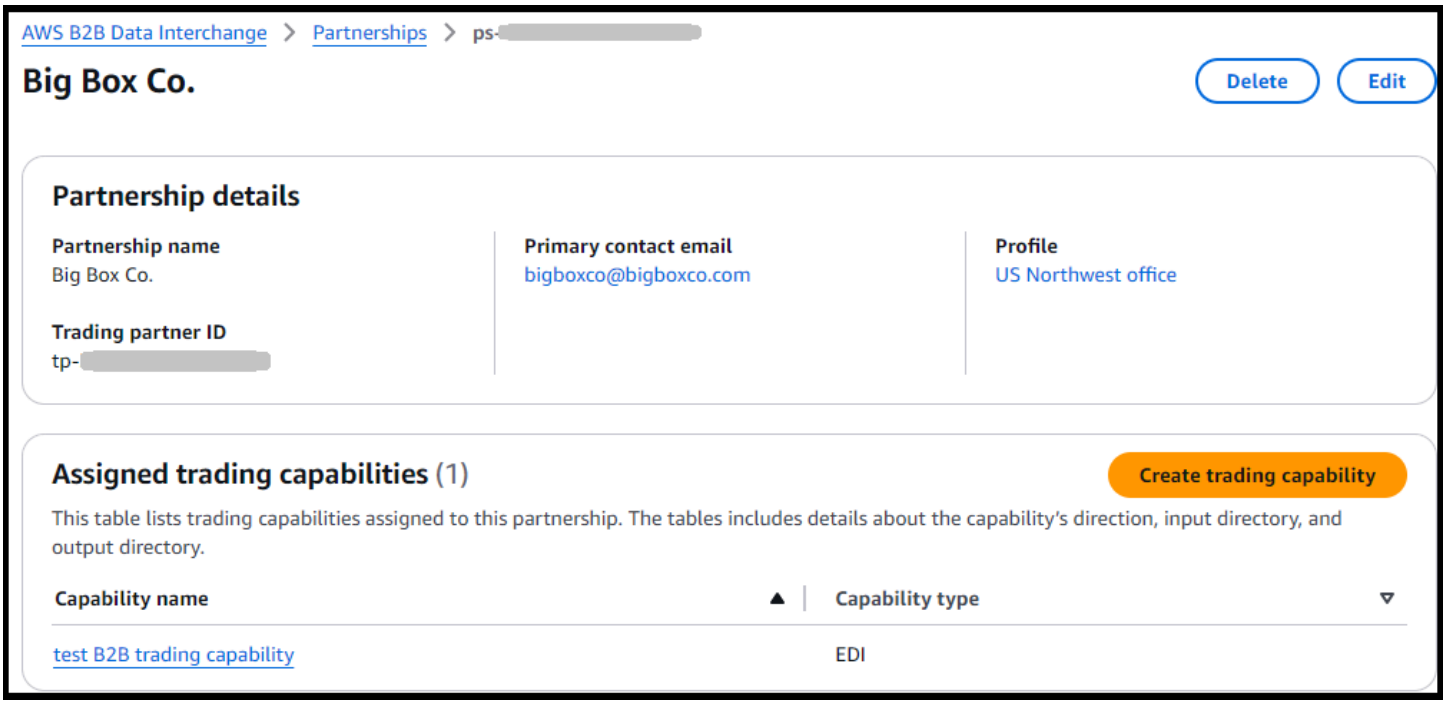
The input directory specified in your trading capability configuration is monitored using Amazon S3 events to automatically process your inbound or outbound EDI. When relevant EDI documents or JSON/XML files are uploaded to your input directory, the transformer associated with the trading capability automatically processes them.

In the case of inbound, EDI documents are automatically transformed into JSON or XML data file outputs. In the case of outbound, JSON or XML data file inputs are automatically transformed into EDI document outputs. All outputs from the transformation process are written to the output directory specified in your trading partner configuration.



Partnerships

A *partnership* represents the connection between you and your trading partner. It incorporates a profile and one or more trading capabilities. It is also where you define the interchange control header and functional group header information necessary to generate outbound EDI documents. To create a partnership, add your partner's contact information and a unique name to easily identify this partnership. You also need to select one of your business profiles and one or more trading capabilities to automatically transform inbound X12 EDI documents and to generate outbound X12 EDI documents. When you configure a partnership for generating outbound EDI documents, you must specify all the required interchange control header and functional group header values.



Using Transfer Family with B2B Data Interchange

AWS Transfer Family is a secure data transfer service that enables you to move files into and out of AWS over industry standard protocols such as SFTP, AS2, FTPS, and FTP.

You have two options to receive X12 from your trading partner using AWS Transfer Family:

- Your trading partner sends the X12 file to your Transfer Family SFTP or AS2 server.
- You retrieve X12 EDI documents from your trading partner's SFTP server using your Transfer Family SFTP connector.

In either case, inbound X12 EDI documents should be written to the dedicated partner prefix nested within the input directory of any trading capability associated with a partnership (for example, `s3://EDI-bucket/input-EDI/`*`partnership-id`*), so that B2B Data Interchange can automatically pick up the file for processing.

Similarly, you have two options to send the generated X12 to your trading partner:

- Your trading partner retrieves X12 EDI documents from your Transfer Family SFTP server.
- You send X12 EDI documents to your trading partner's server using your Transfer Family SFTP or AS2 connector.

In the case where your trading partner retrieves X12 EDI documents from your Transfer Family SFTP server, you provide your partner with authenticated access to the prefix within the output directory of the trading capability associated with the trading partnership (for example, `s3://EDI-bucket/output-EDI/`*`<capability-id>`*`/`*`<partnership-id>`*). In the case where you send X12 EDI documents to your trading partner's server with your Transfer Family SFTP or AS2 connector, you provide the absolute path of the X12 EDI document in your StartFileTransfer API operation.

You can automate the sending of X12 EDI documents to your trading partners using the B2B Data Interchange events published to Amazon EventBridge. To learn more about how to create rules for these events, see Managing AWS B2B Data Interchange events using Amazon EventBridge.

> **Note**
>
> You can use either mechanism to also send EDI acknowledgements to your trading partner. For more details, see EDI acknowledgements

For a self-paced learning experience, go through the EDI document exchange with AWS B2B Data Interchange Workshop, created by the B2B Data Interchange service team. In this workshop, you learn how to receive and transform EDI documents from your business partners using AWS B2B Data Interchange and AWS Transfer Family.

Getting started with AWS B2B Data Interchange

To use AWS B2B Data Interchange, you create profiles, transformers, capabilities, and partnerships. This topic describes how to create and configure these basic building blocks for this service. After you have met the prerequisites, follow the instructions in Transforming and generating EDI or use the Quick setup using the console

After you create the necessary resources (profile, transformer, trading capability and partnership), your trading partners can use AWS Transfer Family or any connectivity software send you X12 documents.

When the X12 documents land in the configured input folder in your Amazon S3 bucket, the documents are automatically picked up and transformed by B2B Data Interchange. Each inbound X12 EDI document transformed also generates acknowledgments (such as 999 or 997) that you can return to your partner.

Similarly, when JSON or XML files are dropped into in specified input directories in Amazon S3, B2B Data Interchange automatically transforms the files to generate X12. You can then use AWS Transfer Family servers (that use either the AS2 or SFTP protocol) to send this X12 to your trading partner.

All transformation activity and status updates, including the generation of acknowledgements, are logged to CloudWatch and emit events to Amazon EventBridge. For details, see Details fields for transformation events.

Topics

- Prerequisites for using AWS B2B Data Interchange
- Quick setup using the console
- Configure AWS B2B Data Interchange using an AWS CloudFormation template

Prerequisites for using AWS B2B Data Interchange

This topic describes how to sign up for an AWS account, create an admin user, and configure an Amazon S3 bucket to use with B2B Data Interchange.

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform tasks that require root user access.

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing **My Account**.

Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   For help signing in by using root user, see Signing in as the root user in the *AWS Sign-In User Guide*.
2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the *IAM User Guide*.

Create a user with administrative access

1. Enable IAM Identity Center.

For instructions, see Enabling AWS IAM Identity Center in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

   For a tutorial about using the IAM Identity Center directory as your identity source, see Configure user access with the default IAM Identity Center directory in the *AWS IAM Identity Center User Guide*.

Sign in as the user with administrative access

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal in the *AWS Sign-In User Guide*.

Assign access to additional users

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

   For instructions, see Create a permission set in the *AWS IAM Identity Center User Guide*.

2. Assign users to a group, and then assign single sign-on access to the group.

   For instructions, see Add groups in the *AWS IAM Identity Center User Guide*.

Configure an Amazon S3 bucket

You need to have an Amazon S3 bucket set up and ready to use. B2B Data Interchange requires buckets for storing input, output, and instruction documents. For details, see Getting started with Amazon S3.

- The Amazon S3 bucket must be in the same AWS account as the B2B Data Interchange user.
- The Amazon S3 bucket must be in the same region as the B2B Data Interchange user.

Amazon S3 bucket policies and permissions

Before you can begin transforming and generating Electronic Interchange Data (EDI) documents, you need to set up the Amazon S3 bucket policies that you need for working with B2B Data Interchange resources. This topic also provides example policies to help you get started.

Configure your Amazon S3 bucket policies

You can copy example policies as described in the preceding section. If one or both of your buckets use SSE-KMS encryption, you also need to update your AWS KMS key policy, as described in the section called “Example bucket policies”.

> **Note**
>
> For details on temporary files and directories, see Temporary files and Amazon S3 permissions.

Perform this procedure for both your input and output directories.

Configure your bucket policy

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/ and navigate to your bucket.
2. After you open the detail page for your bucket, choose the **Permissions** tab.
3. In the **Bucket policy** panel, choose **Edit**.
4. Paste in the appropriate bucket policy, depending on whether this is your input or output bucket.
5. Choose **Save** to save the policy.

Configure your Amazon S3 bucket EventBridge setting

You need to turn on Amazon EventBridge for your input and output Amazon S3 buckets.

Turn on EventBridge notifications

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/ and navigate to your bucket.

2. After you open the detail page for your bucket, choose the **Properties** tab.
3. Scroll down to the **Amazon EventBridge** panel. If notifications are off, proceed to the next step. If they are on, you can skip the remainder of this procedure.
4. To turn on EventBridge notifications, choose **Edit**.
5. Select **On**, and choose **Save changes**.

> **Note**
>
> After you enable EventBridge, it takes approximately five minutes for the changes to take effect. Wait at least 5 minutes after enabling EventBridge events before placing your files in an Amazon S3 bucket.

Temporary files and Amazon S3 permissions

For your output bucket policies, you need to have the `s3:GetObject` and `s3:DeleteObject` permissions. These permissions are required so that B2B Data Interchange read and then remove temporary files that the service uses to transform your EDI documents.

The service uses `s3:DeleteObject` to delete temporary files, which can be ten times as large as the X12 input file. If your bucket policy doesn't include `s3:DeleteObject`, the service continues to work as expected. However, B2B Data Interchange would not be able to delete these temporary files: they would then remain in Amazon S3 (and incur charges).

The service adds a new prefix to your output directory, `customerOutputDirectory/parsed`, for its use, and `customerOutputDirectory/`*`tradingPartnerId`*`/parsed` for use by Amazon S3 (if you have a partnership). These locations are used exclusively for holding temporary files. If your bucket policy includes the `s3:DeleteObject` permission, you should never see these folders. If you don't have that permission, then the temporary files continue to be written and remain in these folders.

Example bucket policies

You need to update your Amazon S3 bucket policies to include the appropriate permissions so that the B2B Data Interchange service can access your input documents and store the generated outputs.

The following are policies copied from the **Create trading capability** page. You can select **View** to view your bucket. Then, from your bucket page, choose **Permissions** > **Bucket policy** > **Edit**, and then paste this policy into the **Policy** field.

> **Note**
>
> In these examples, replace each *user input placeholder* with your own information.

Example Amazon S3 input bucket policy

Example Amazon S3 input bucket policy copied from the **Trading capabilities** page.

```
{
    "Version": "2012-10-17",
    "Id": "B2BIEdiCapabilityInputPolicy",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "b2bi.amazonaws.com"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectAttributes"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/input-folder*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                }
            }
        }
    ]
}
```

Example Amazon S3 output bucket policy

Example Amazon S3 output bucket policy copied from the **Trading capabilities** page.

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

```
    "Id": "B2BIEdiCapabilityOutputPolicy",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "b2bi.amazonaws.com"
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/output-folder/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                }
            }
        }
    ]
}
```

If you have SSE-KMS or DSSE-KMS encryption enabled on your input or output bucket, you need to update the key policy in AWS KMS. You need to add the B2B Data Interchange service principal and the appropriate permissions to the policy. To read more about data protection, see Data protection in AWS B2B Data Interchange.

Note

If you are using SSE-KMS or DSSE-KMS encryption, do not use an AWS managed key policy, as they cannot be edited.

Example Amazon S3 input AWS KMS key policy

The following example policy is for use with an encrypted input/source bucket. It includes the permission needed to decrypt an encrypted file.

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

```
    "Id": "B2BIEdiCapabilityInputKeyPolicy",
    "Statement": [
        {
            "Sid": "Allow administration of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow B2Bi access",
            "Effect": "Allow",
            "Principal": {
                "Service": "b2bi.amazonaws.com"
            },
            "Action": "kms:Decrypt",
            "Resource": "*"
        }
    ]
}
```

Example Amazon S3 output AWS KMS key policy

The following example policy is for use with an encrypted output bucket. It includes the permission needed to encrypt a file for storing into the bucket.

```
{
    "Version": "2012-10-17",
    "Id": "B2BIEdiCapabilityOutputKeyPolicy",
    "Statement": [
        {
            "Sid": "Allow administration of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow B2Bi access",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "b2bi.amazonaws.com"
            },
            "Action": "kms:GenerateDataKey",
            "Resource": "*"
        }
    ]
}
```

If you are using the same bucket for input and output, you can use either example key policy, and add in the other permission. In this case, the policy is as follows.

```
{
    "Version": "2012-10-17",
    "Id": "B2BIEdiCapabilityOutputKeyPolicy",
    "Statement": [
        {
            "Sid": "Allow administration of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow B2Bi access",
            "Effect": "Allow",
            "Principal": {
                "Service": "b2bi.amazonaws.com"
            },
            "Action": [
                 "kms:GenerateDataKey",
                 "kms:Decrypt"
             ],
            "Resource": "*"
        }
    ]
}
```

Quick setup using the console

This topic provides instructions on how to quickly setup B2B Data Interchange. From the B2B Data Interchange landing page (https://console.aws.amazon.com/b2bi/), choose the **Quick setup** option. The quick setup makes it easy for you to create the resources needed to build and run your EDI-based workflows on AWS B2B Data Interchange. Follow the steps below to connect with your trading partners and start transforming EDI data in JSON and XML to simplify your downstream integrations.

> **Note**
>
> If you don't see the landing page, select AWS B2B Data Interchange at the top of the left navigation menu.

1. The **Create profile** screen appears. Fill in your details as described in Create a profile, then select **Next**.
2. The **Create transformer** screen appears. Fill in your details as described in Create an inbound transformer or Create an outbound transformer, then select **Next**.
3. The **Create trading capability** screen appears. Fill in your details as described in Create a trading capability for inbound EDI, then select **Next**.

   > **Note**
   >
   > Make sure to choose **Copy policy**, for both your input and output directory, save the policy code, and then paste the policies into your input and output directory's bucket policy.

4. The **Create partner** screen appears. Fill in your details as described in Create a partnership for inbound EDI, then select **Next**.
5. The **Review and create** screen appears, showing all the details you've entered. You can select **Cancel**, or **Previous** if anything needs to be changed, or **Complete setup** to create your profile, transformer, trading capability and partnership.

B2B Data Interchange also provides a self-contained, AWS CloudFormation template to quickly create a B2B Data Interchange configuration. For details on how to deploy this template, see Configure AWS B2B Data Interchange using an AWS CloudFormation template.

Configure AWS B2B Data Interchange using an AWS CloudFormation template

We provide a basic stack that you can use to quickly configure all the resources you need to work with AWS B2B Data Interchange.

To configure B2B Data Interchange objects from a CloudFormation template

1. Download the template from the GitHub repository here: AWS B2B Data Interchange basic template
2. Open the AWS CloudFormation console at https://console.aws.amazon.com/cloudformation.
3. In the left navigation pane, choose **Stacks**.
4. Choose **Create stack**, and then choose **With new resources (standard)**.
5. On the **Create stack** page, do the following.
    a. In the **Prerequisite - Prepare template** section, select **Choose an existing template**.
    b. In the **Specify template** section, choose **Upload a template file**.
    c. Navigate to your saved template file, and select it.
    d. Choose **Next**.
6. On the **Specify stack details** page, name your stack, and change the names of the listed parameters as appropriate for your configuration.
7. Choose **Next**. On the **Configure stack options** page, optionally add tags and an IAM role. Then choose **Next** again.
8. On the **Review and create** page review the details for the stack that you're creating, and then choose **Submit**.

You can view the progress of your stack being creating in the AWS CloudFormation console.

Transforming and generating EDI

There are multiple ways to transform or generate X12 EDI in AWS B2B Data Interchange. This topic describes the various ways you can create and configure inbound and outbound transformations.

- *Inbound EDI*: you receive an X12 EDI document from your trading partner. AWS B2B Data Interchange converts this X12 EDI document into a JSON or XML formatted data file with a service-defined structure. You can optionally apply a mapping—written in JSONata or XSLT—to produce a custom JSON or XML formatted data file.
- *Outbound EDI*: you have a JSON or XML formatted data file containing information that you wish to incorporate into an X12 EDI document that will be sent to your trading partner. You can align your JSON or XML formatted data file to conform with the service-defined structure directly, or you can apply a mapping in JSONata or XSLT to convert your custom JSON or XML into the service-defined structure necessary to produce an outbound X12 EDI document.

As a prerequisite, you must set up bucket policies for the Amazon S3 buckets that you use with B2B Data Interchange, as described in Configure your Amazon S3 bucket policies.

Topics

- Generative AI-assisted EDI mapping
- Inbound EDI
- Outbound EDI
- Control numbers

Generative AI-assisted EDI mapping

The AWS B2B Data Interchange generative AI-assisted EDI mapping capability expedites the process of writing and testing bi-directional EDI mappings, reducing the time, effort, and costs associated with migrating your EDI workloads to AWS. This capability leverages your existing EDI documents and transactional data samples to generate mapping code using generative AI. You can then use the generated mapping code as a starting point and further customize it to produce output formats that align with downstream data integration needs.

View AWS B2B Data Interchange Generative AI-assisted EDI mapping for a brief introduction to AWS B2B Data Interchange generative AI capabilities.

Topics

- Prerequisites for using the AWS B2B Data Interchange generative AI-assisted EDI mapping capability
- Notes about generative AI-assisted EDI mapping
- Using generative AI-assisted EDI mapping in AWS B2B Data Interchange

Prerequisites for using the AWS B2B Data Interchange generative AI-assisted EDI mapping capability

Before you can use this feature, you need to enable the models in Amazon Bedrock.

> **Note**
>
> You do not incur additional AWS B2B Data Interchange charges to generate mapping code beyond the standard Amazon Bedrock Pricing.

To enable models in Amazon Bedrock

1. Sign in to the AWS Management Console and open the Amazon Bedrock console at https://console.aws.amazon.com/bedrock/.
2. From the left-hand navigation menu, choose **Model access** from the **Amazon Bedrock configurations** pane.
3. Enable all Anthropic models (AWS B2B Data Interchange currently uses Claude 3.7 Sonnet, Claude 3.5 Sonnet v1, and Claude 3 Sonnet), then choose **Next**.

   In the future, there may be newer models that we will suggest that you enable as well.
4. If prompted, you may provide your use case details for access to the Anthropic models, including your company name, URL, industry, user persona, and description of your use case.
5. Review your selected models, and if you don't need to make any changes, choose **Submit**.

Notes about generative AI-assisted EDI mapping

Note the following:

- This feature is available for both inbound and outbound EDI processing.

- To use this feature, you must upload input and output samples when you configure a transformer.
- An accuracy score is generated for each mapping, to help you determine whether additional edits are needed.
- Mapping code is generated during configuration of your transformer resource, and not a transformation runtime.
- No customer data is stored or used to train the models: each mapping generated is a one-time operation.
- Currently, the AWS B2B Data Interchange generative AI-assisted EDI mapping capability is only supported in the US East (N. Virginia) and US West (Oregon) regions.

Using generative AI-assisted EDI mapping in AWS B2B Data Interchange

The transformer configuration wizard has three steps:

1. Transformer configuration
2. Mapping configuration
3. Review and create

For details on creating bi-directional transformers, see Create an inbound transformer or Create an outbound transformer.

To use the AWS B2B Data Interchange generative AI-assisted EDI mapping capability, make sure to upload both an input and output sample in the transformer configuration step (*Step 1*) when creating or updating your transformer resource. If you've specified both an input and output sample in Step 1, you see the **Generate Mapping** option enabled during the mapping configuration step (*Step 2*).

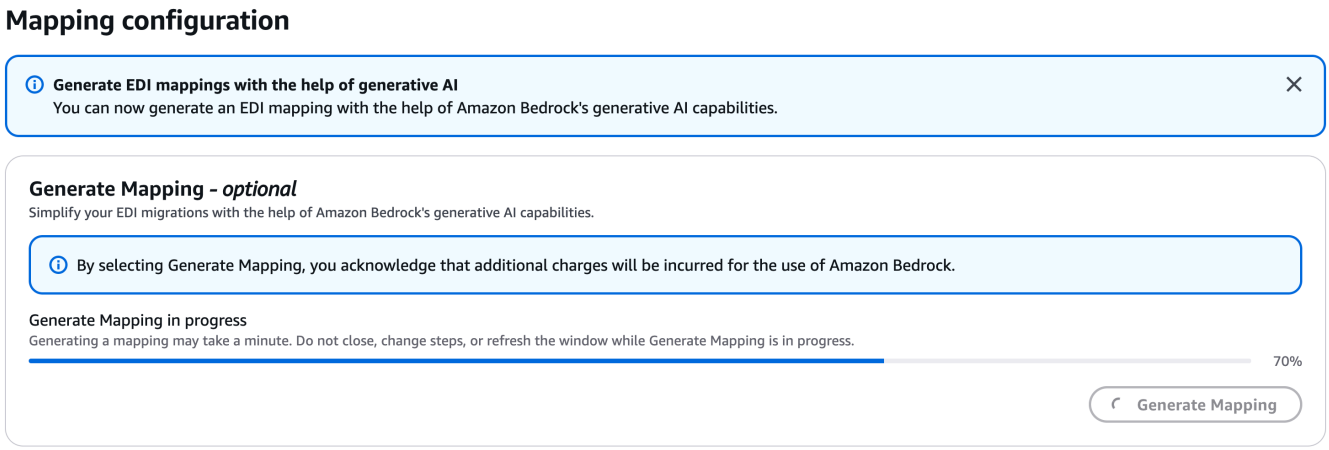
To use generative AI-assisted EDI mapping in AWS B2B Data Interchange

1. Upload your EDI document sample and JSON or XML data file sample to an Amazon S3 bucket (or buckets) with the appropriate policy and permissions. For details, see Amazon S3 bucket policies and permissions.
2. Navigate to the transformer homepage in the AWS B2B Data Interchange console. Choose **Create transformer** to create a new transformer or select an existing transformer from the list

and choose **Edit** to update the configuration. In the **Sample documents** section, specify the input and output samples that you uploaded to Amazon S3 in the previous step.

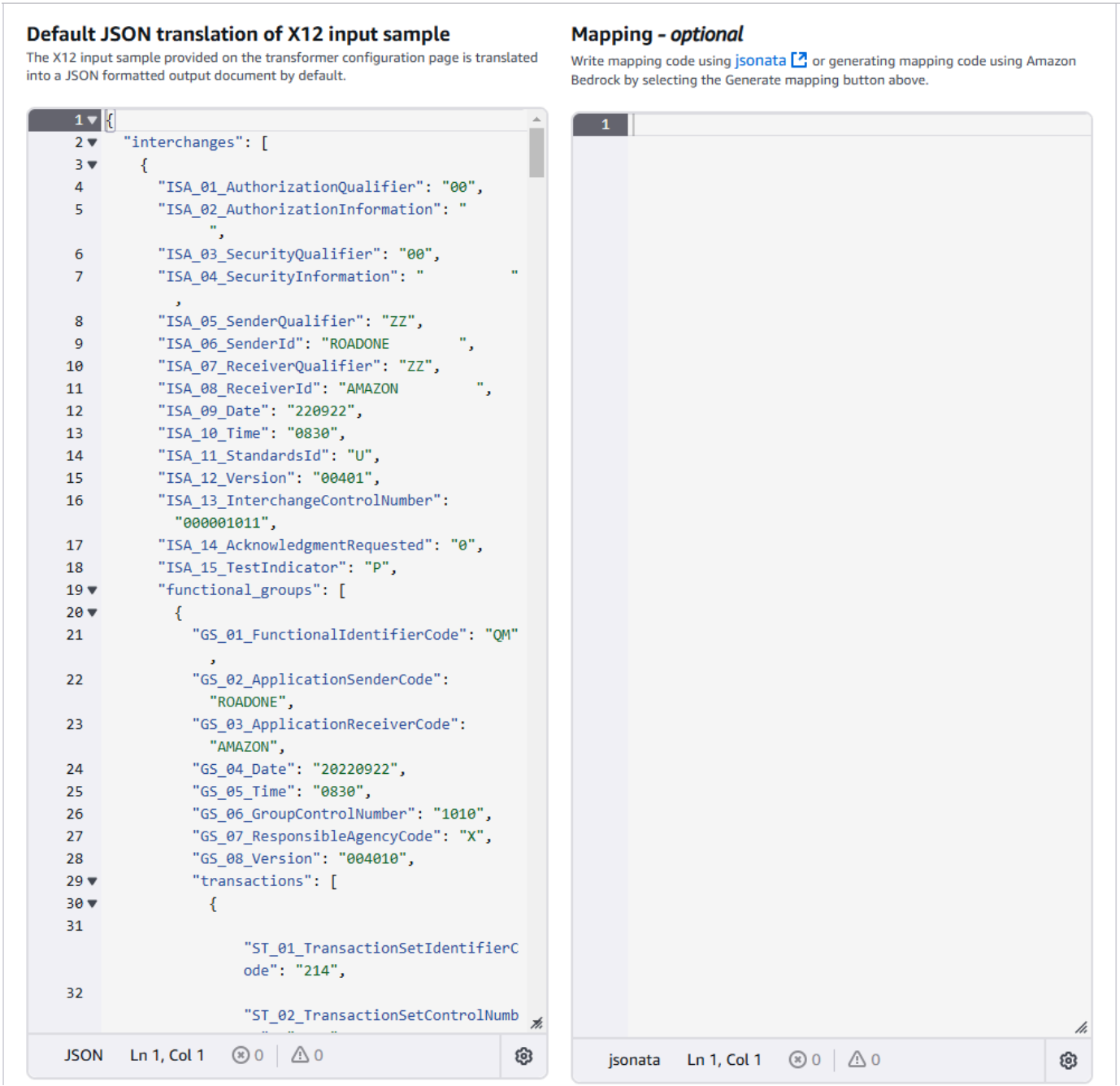
3. Select **Generate Mapping**. You can view the progress and percentage complete in the progress bar.

   In the **Generate Mapping - optional** pane, notice the following note: **By selecting Generate Mapping, you acknowledge that additional charges will be incurred for the use of Amazon Bedrock.**

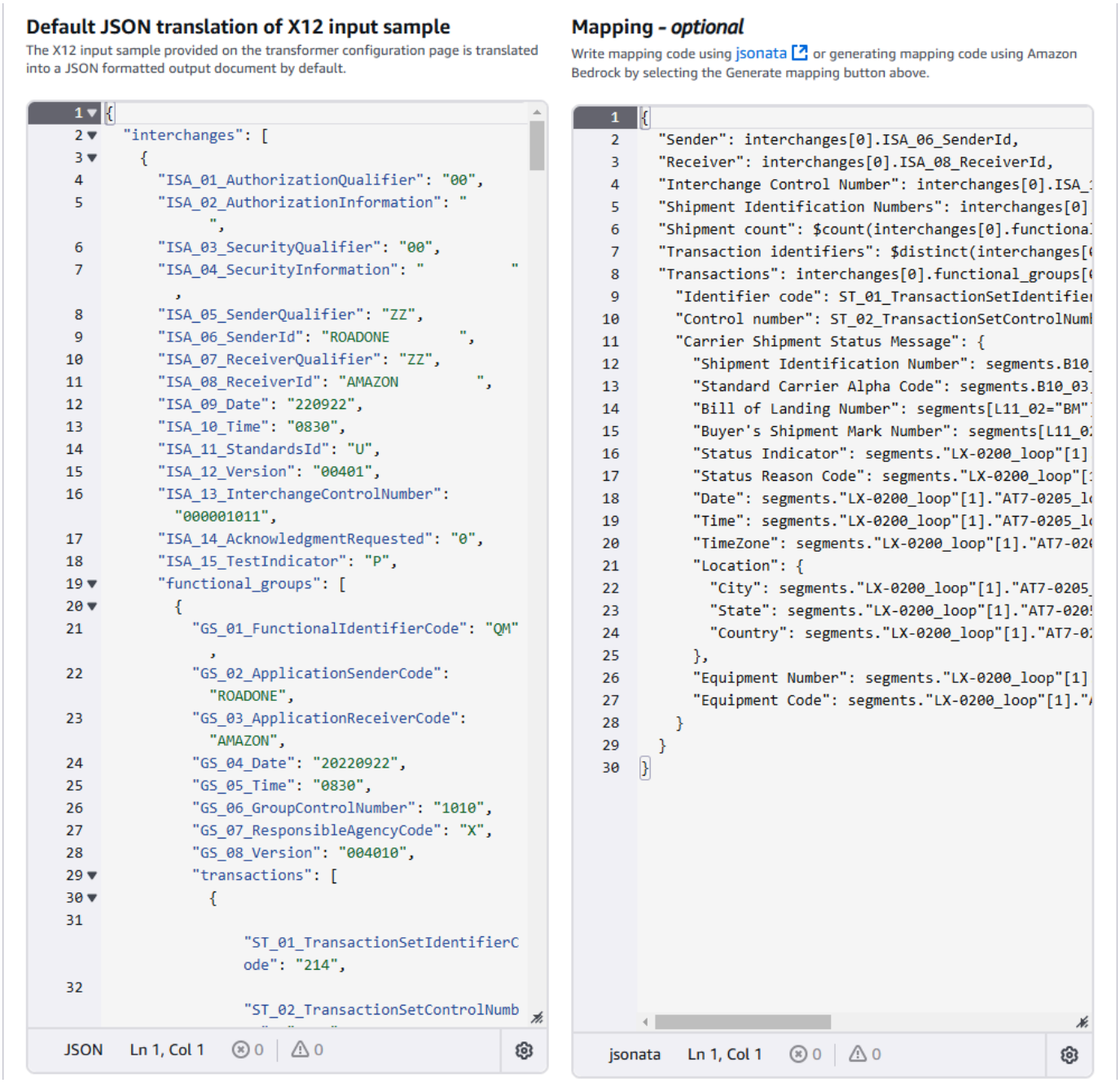


   The **Mapping editor** pane will be empty before you select **Generate Mapping** and while the mapping is being generated.

   This screen shows the **Mapping editor** panes before you select **Generate Mapping** and the Mapping pane is empty.



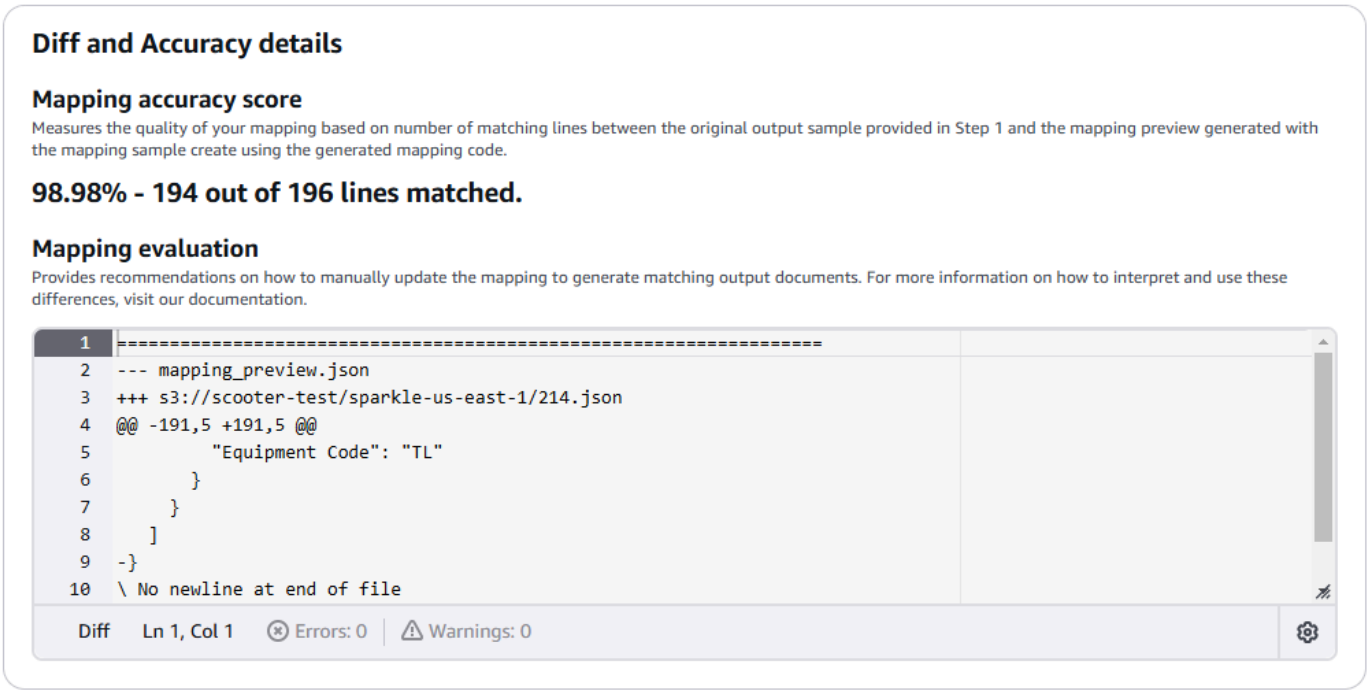
4. When the mapping completes, you see the **Generate Mapping was successful** message. You also see the **Mapping editor** has been populated with mapping code.



After the mapping has been generated, the **Diff and Accuracy details** displays the **Mapping accuracy score** and the **Mapping evaluation**. Note the following:

- The accuracy score remains active as you continue to make manual edits, and changes based on your editing.
- The score is determined by how well the provided sample output matches against the output document that is generated by the generative AI-assisted EDI mapping.

- The generated score is determined by counting the number of matching lines and divides by the total number of lines in the original output document. For example, if 19 of 20 lines match, the accuracy score is 95%.
- If you are unsatisfied with the mapping, return to Step 1 to specify alternate input and output samples. Then, return to Step 2 and select **Re-generate Mapping**. Using alternate EDI document and JSON or XML data file samples will result in new mapping code.



5. When your mapping is in a satisfactory state, select **Next** to proceed to step 3, **Review and create**.

Continue to the **Review and create** step, as described in Create an inbound transformer or Create an outbound transformer.

Inbound EDI

There are two ways that you can invoke a transformer to convert inbound X12 documents to XML or JSON format.

- **Invoking `StartTransformerJob` API**. With this approach, you create an inbound transformer that is configured to transform a specific transaction set and version into JSON or XML. You then invoke the `StartTransformerJob` action, which requires a Transformer ID, the absolute file

path in Amazon S3 for the input EDI document, and the output directory path in Amazon S3 for the transformed JSON/XML file.

Acknowledgements are stored in a generated **ACK** folder in the output directory. Subscribe to status updates using events emitted to Amazon EventBridge or invoke the `GetTransformerJob` API to poll for status updates from the invoking orchestration engine (such as AWS Step Functions).

> **Note**
>
> The **Transformer only** option only works for when you are transforming incoming X12 documents to JSON/XML, and needs to be invoked.

- **Monitoring specified locations in Amazon S3**. With this approach, you configure a transformer, trading capability, and partnership. You then drop EDI input documents into the input directory specified in the attached trading capability and B2B Data Interchange listens for Amazon S3 events to automatically transform the documents to JSON or XML files and stores the files in the specified output directory. The input and output directory used are those specified in your trading capability with your trading partner's ID added to the prefixes. As part of the partnership configuration, you specify one or more trading capabilities to use.

  For each of the trading capabilities specified in the Partnership, a trading partner ID is added as a new prefix to the input and outbound directories specified in each of the respective trading capabilities. For example, assume that you specify the following directories in your trading capability:

  - Capability input directory: `s3://EDI-bucket/input-EDI/`
  - Capability output directory: `s3://EDI-bucket/output-JSON/`

  When you associate your trading capabilities with your partnership, the service adds a prefix to both the input and output directory, changing them to the following:

  - Input directory to drop incoming X12 files becomes `s3://EDI-bucket/input-EDI/`*`<trading-partner-id>`*`/`
  - Output directory containing the transformed JSON/XML files becomes `s3://EDI-bucket/output-JSON/`*`<trading-partner-id>`*`/`
  - The acknowledgement is stored in `s3://EDI-bucket/output-JSON/`*`<trading-partner-id>`*`/ACK/`

You then drop files into the trading-partner-ID prefix in the input directory to transform EDI for that specific partner. The transformed JSON output is then written to the trading-partner-ID prefix in the output directory. Using these prefixes ensures that your EDI documents are properly transformed for each individual trading partner.

> **Note**
>
> You can associate one trading capability with multiple partnerships, and a partnership can be associated with multiple trading capabilities. Using the folder structure specified, you can use the same trading capability for multiple partners. The trading partner ID makes sure that you have clear delineation as to where the transformed EDI data for a specific partner should be stored.

Transforming inbound EDI documents

Typically, you perform the following steps to transform X12 EDI documents into JSON or XML data

1. Create a profile.
2. Create an inbound transformer.
3. Create a trading capability for inbound EDI.
4. Create a partnership for inbound EDI.
5. Test your transformation workflow. For details, see the Testing end-to-end topic from our EDI document exchange with AWS B2B Data Interchange workshop.

Create a profile

You can use *profiles* to store contact information and details about your own business and specify a unique name to easily identify this profile A profile contains the following types of information.

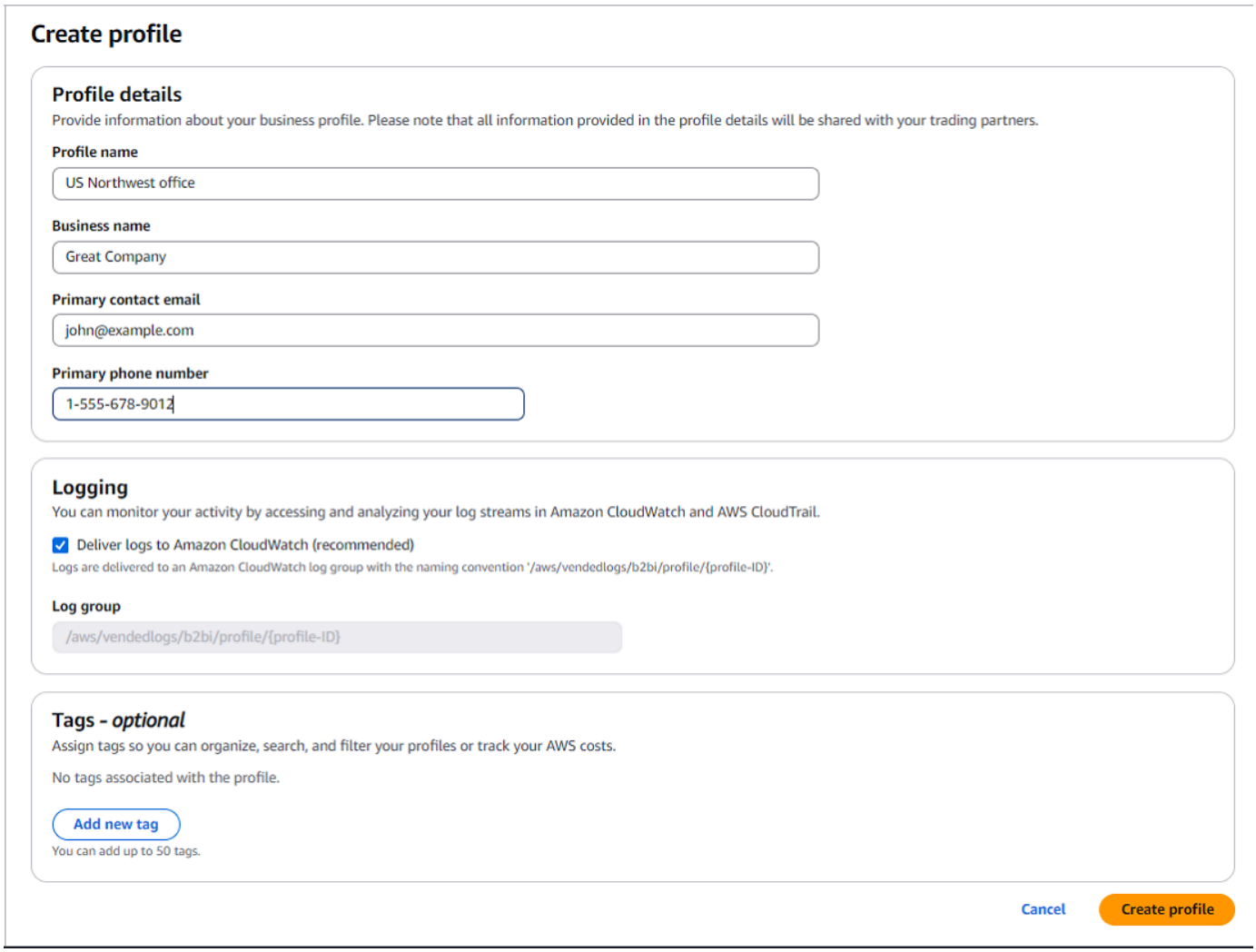
- **Profile details**: This section contains the profile name, the name of the business, a contact email address, and a phone number.

> **Note**
>
> These details are all your characteristics, not those describing your trading partner. The latter are described as part of the partnership resource.

- **Logging**: This section describes the logging configuration. You can also opt out of logging (not recommended).
- **Tagging**: Tag your profiles to easily organize, search, and filter your profiles globally.

To create a profile

1. Open the AWS B2B Data Interchange console at https://console.aws.amazon.com/b2bi/ and select **Profiles** from the navigation pane, then choose **Create profile**.
2. Enter the profile details, the name of the profile, the name of the business represented, and the contact information (email and phone number).
3. Logging is selected by default. Clear the box to turn off logging (not recommended). The log group is based on the profile ID, for example, `/aws/vendedlogs/b2bi/p-ABCDE111122223333`.
4. Optionally, add tags as needed.



Create an inbound transformer

A *transformer* describes how to process the incoming EDI documents and extract the necessary information to the output file.

> **Note**
>
> If an EDI input file contains more than one transaction, each transaction must have the same document and version, for example **`214/4010`**. If not, the transformer cannot parse the file.

To create a transformer

1. Open the AWS B2B Data Interchange console at https://console.aws.amazon.com/b2bi/ and select **Transformers** from the navigation pane, then choose **Create transformer**.
2. Select a transformer name (for example **edi-214-json**), the direction, the EDI doc number, and version. Then, provide a sample document by selecting a document from Amazon S3. The sample document can preview how your EDI documents get converted.

   a. Enter a name (no spaces).

   b. Ensure that **Inbound EDI** is selected.

   c. For **Input Details**, select an EDI document number and X12 version from the dropdown menus.

   d. For **Input Details**, select **JSON** or **XML**.

   e. Optionally, in the **Sample documents** pane, provide the bucket and prefix in Amazon S3 for the sample input and output files. This is useful for making sure the transformer functions correctly.

   f. Optionally, add tags as needed.

   g. Select **Next** to proceed to the next step in the wizard.
3. The Mapping configuration screen is displayed. If you provided a sample input document in the previous step, the default representation for your sample is displayed. You can use generative AI-assisted EDI mapping to expedite the mapping configuration. For details, see Generative AI-assisted EDI mapping.

   If you chose not to customize the output format using the **Mapping template editor**, AWS B2B Data Interchange transforms EDI document inputs using the default, service-defined format shown on the left side of your screen.

   You can also use the **Mapping template editor** to only include certain pieces of your EDI documents.

   The pieces you select are previewed in the mapping preview pane.

   The items in your mapping editor are the only items that are extracted from the input EDI document, and that are then saved to your output file, located in your Amazon S3 output location.

This example shows ref ID, shipment ID, and b of lading number, from and to city, and the shipment status code.

4. When you are happy with your mappings, choose **Next**, which takes you to the review page. Note that newly created transformers are inactive.

> **Note**
>
> A status of **Inactive** indicates that the transformer is not used in any trading capabilities: it is essentially in edit mode. When you are finished editing and updating the transformer, you change the status to **Active**. Then, you can associate the transformer with a trading capability. At this point, the transformer is essentially locked, and in production mode.

5. After your review is complete, choose **Save** to create the transformer.

Create a trading capability for inbound EDI

Trading capabilities contain the information required to build your event-driven EDI workflows. To create a trading capability, specify the EDI direction, add details about the EDI document number and version, choose the transformer to use to transform or generate your EDI, and specify the input and output directories used to source and store documents. Based on the EDI direction selected and the transformer attached to the trading capability, you can use the capability to automatically:

- Transform incoming EDI documents into JSON or XML outputs.
- Transform XML or JSON data stored in Amazon S3 into EDI documents.

To create an inbound trading capability

1. Open the AWS B2B Data Interchange console at https://console.aws.amazon.com/b2bi/ and select **Trading capabilities** from the navigation pane, then choose **Create trading capability**.
2. In the **Trading capability settings** section, enter the following information.
   - Enter a descriptive, unique name for the trading capability.
   - Select an **EDI direction**, either **Inbound** or **Outbound**.
   - Choose an **X12 version** and **X12 transaction** set from the corresponding dropdown menus.

- In the **Apply transformer** field, choose a transformer to apply to this trading capability.

3. In the **Configure directories** section, you configure both the input and output directories that are used to source and store documents.

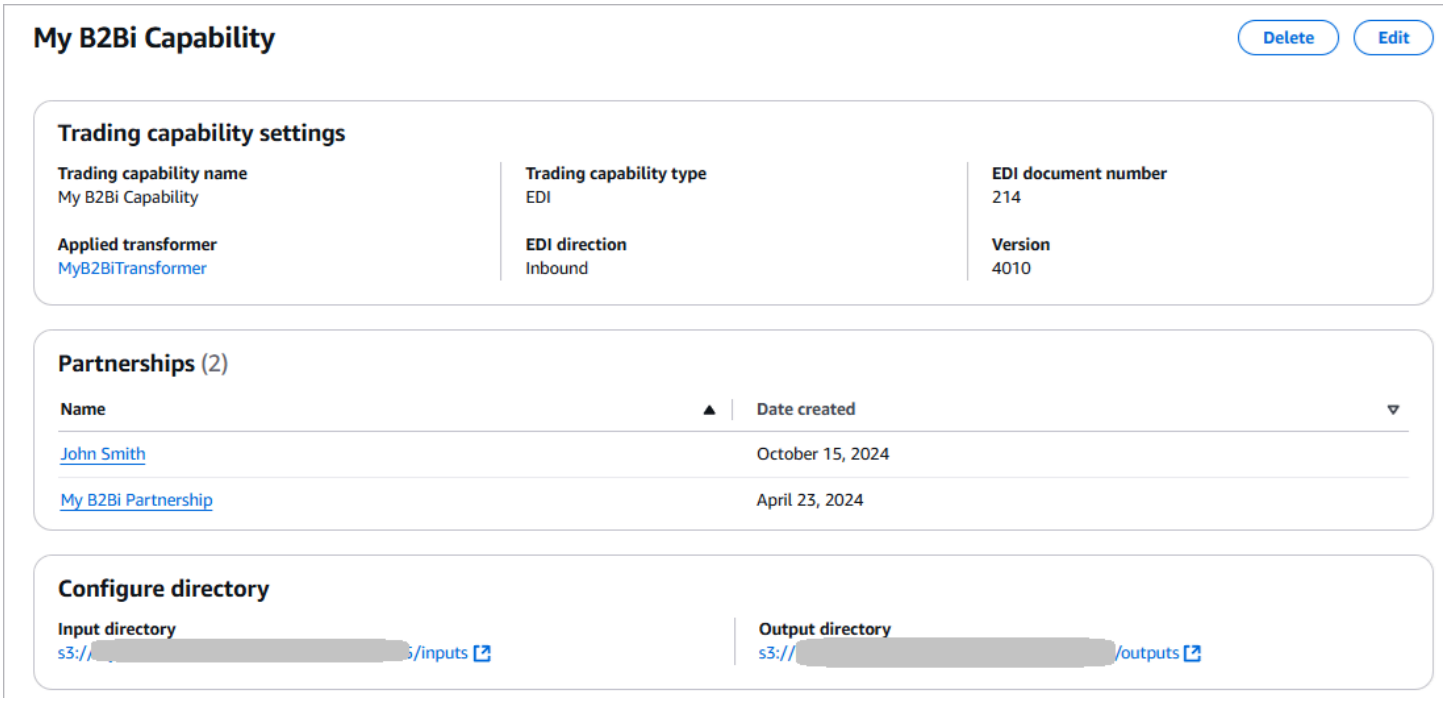
   - In the **Input directory** area, enter an Amazon S3 bucket.
   - Choose **Browse S3** to navigate to your available Amazon S3 buckets, where you can select a bucket (and optionally a prefix) to specify your input directory.

     > **Note**
     >
     > B2B Data Interchange will continuously monitor all of the prefixes of your input directory for new files. It attempts to transform every file placed into any prefix of your input directory.
     > Avoid placing files that you do not want to be transformed into your input directory or any of its prefixes.

   - Choose **Copy policy** to copy a policy that you can then paste into your input directory's bucket policy.
   - Configure your output directory in the **Output directory** area, similarly to how you configured the input directory.

     > **Note**
     >
     > B2B Data Interchange will automatically create prefixes in the specified output directory to store the transformed X12 documents.
     > Don't set your output directory as a subdirectory of your input directory: this configuration directs B2B Data Interchange to attempt processing output files as input files.

4. Optionally, add tags as needed.
5. After you have configured all of the settings, choose **Create capability**.



> **Note**
>
> - For your input and output directories, update the bucket policy (Configure your Amazon S3 bucket policies). If your input or output buckets use SSE-KMS encryption, you also need to update the policy for your AWS KMS key. For details, see the section called "Example bucket policies".
> - Enable EventBridge notifications for the Amazon S3 buckets used by the trading capability. For details, see (Configure your Amazon S3 bucket EventBridge setting).

Create a partnership for inbound EDI

A *partnership* represents the connection between you and your trading partner. It incorporates a profile and one or more trading capabilities. It is also where you define the interchange control header and functional group header information necessary to generate outbound EDI documents.

To create a partnership

1. Open the AWS B2B Data Interchange console at https://console.aws.amazon.com/b2bi/ and select **Partnerships** from the navigation pane, then choose **Create partnership**.
2. In the **Partnership details** section, provide the following information.

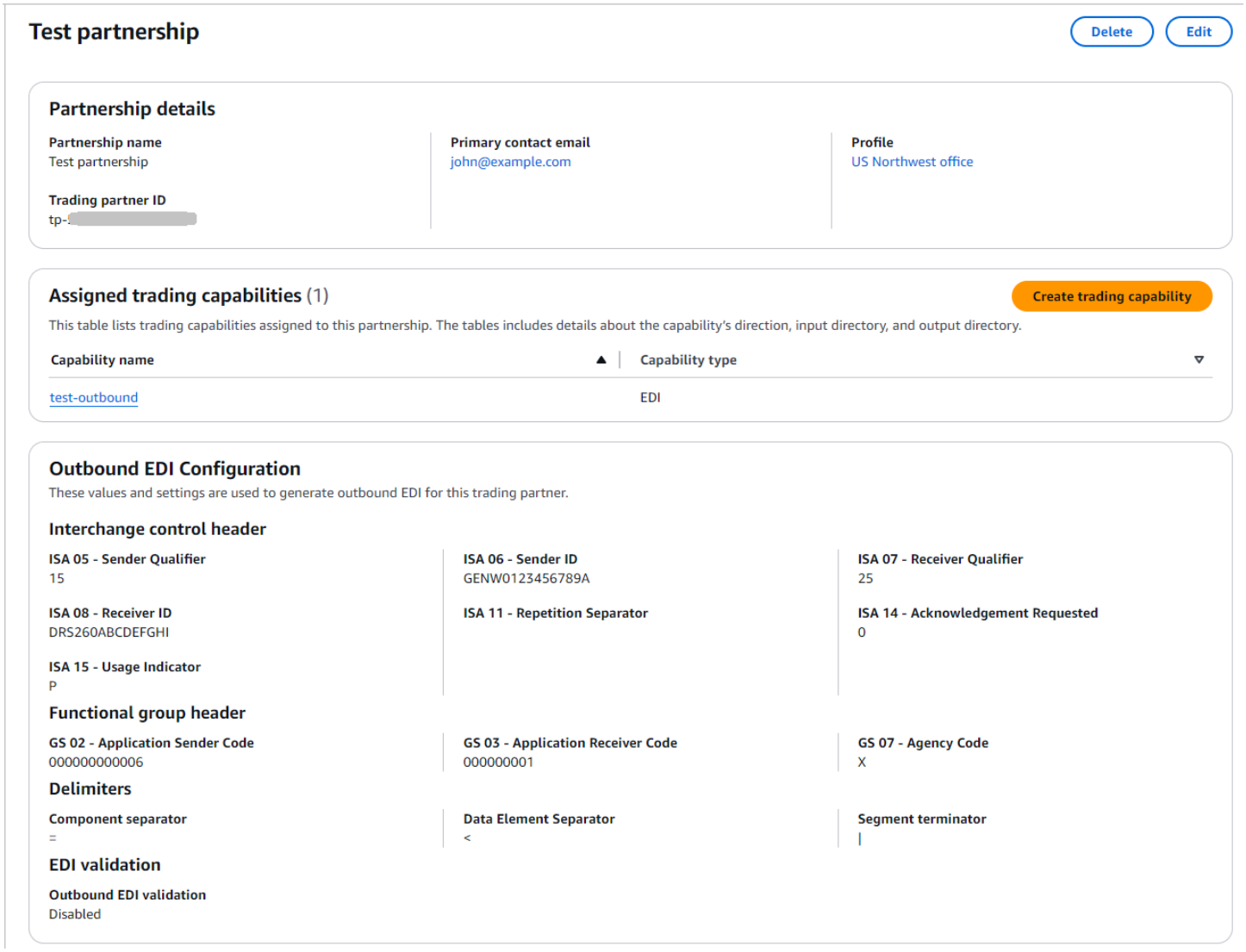
a. Enter a descriptive name for the partnership.

b. Enter an email address to associate with the partnership. Provide the trading partner's email address.

c. Choose a profile from the dropdown menu.

d. Select one or more trading capabilities from the **Trading capabilities** list.

3. Unless you intend to perform outbound EDI processing with this partner, you can skip the **Outbound EDI configuration** section.
4. Optionally, add tags as needed.
5. After you have configured all of the settings, choose **Create partnership**.



After you create a partnership, you can observe a new sub-directory, within your Amazon S3 input directory, beginning with `tp-`.

EDI acknowledgements

B2B Data Interchange automatically generates acknowledgements that you can return to your trading partner to communicate that the file was received and to report errors. The generated acknowledgement is stored in your Amazon S3 bucket alongside the transformed EDI, and an event is emitted by the B2B Data Interchange service to Amazon EventBridge.

The service generates the following types of acknowledgements:

- *TA1 interchange acknowledgements*: A TA1 is an interchange acknowledgement used to confirm the receipt of X12 EDI interchanges and to report syntactical errors. It reports the status of the processing of an interchange header and trailer by the addressed receiver or the non-delivery by a network provider. TA1 interchange acknowledgements are generated for all interchanges.
- *997 functional acknowledgements*: the 997 is a functional acknowledgement used to confirm receipt of X12 EDI transactions and to report transactional errors. A 997 acknowledgement serves as a response to an individual EDI message or group of messages. It contains information about the receipt of the upstream transaction, such as whether it has been accepted, accepted with errors or rejected. Most finance, transportation, supply chain, and communication & control transactions generate a 997 functional acknowledgement.
- *999 functional acknowledgements*: there are two types of 999 functional acknowledgement, as follows:
  - 999 functional acknowledgement for HIPAA transactions: the service generates *999 X231* acknowledgements for all X12 version 5010 HIPAA transactions.
  - 999 functional acknowledgement for non-HIPAA transactions: the service generates *999* acknowledgements for all other healthcare-related X12 transactions.

> **Note**
>
> The service generates either a 999 or 997 acknowledgement, but never both.

For details of the generated events, see Details fields for acknowledgement events.

One example use case is as follows: Retailer B responds with an EDI 997 Functional Acknowledgement, which communicates to Vendor A that their EDI 810 Invoice was received and is syntactically valid.

1. Retailer B receives X12 EDI 810 Invoice from Vendor A.
2. Retailer B responds with an EDI 997 Functional Acknowledgement, which communicates to Vendor A that their EDI 810 Invoice was received and is syntactically valid.

B2B Data Interchange creates events when generating acknowledgements (for both successful and failed scenarios). The primary value of generating these events is for returning the acknowledgement to the trading partner. You can use AWS Transfer Family (or any other data transfer service) to send these acknowledgements to your trading partner.

To learn more about using B2Bi acknowledgement events to return acknowledgements to your trading partner, see Details fields for transformation events.

Acknowledgement output paths

This section describes the output paths for acknowledgement files saved to Amazon S3.

Let's assume that a customer configures their EDI trading capability to have the following input and output directories.

- Input: s3://amzn-s3-demo-bucket/IN/
- Output: s3://amzn-s3-demo-bucket/OUT/

In this example, the absolute paths for the EDI input document and the transformed JSON or XML output are as follows:

- Inbound EDI: s3://amzn-s3-demo-bucket/IN/TP_ID/edi214xml-test83.txt
- Transformed output: s3://amzn-s3-demo-bucket/OUT/TP_ID/edi214xml-test83.txt.2023-11-21T19:26:49.774Z.xml

The path of the acknowledgement depends on whether the inbound X12 EDI document is transformed using a trading capability or transformed by directly invoking the `StartTransformerJob` API operation.

When using a trading capability, the format for the acknowledgement files is s3://amzn-s3-demo-bucket/OUT/TP_ID/ACK/*filename*.*timestamp*.997 (.TA1 for TA1 acknowledgements).

When invoking the `StartTransformerJob` API directly, acknowledgements will be written into a dedicated ACK prefix within the output location specified in the request. See the following example paths.

Acknowledgement use case example

The following are examples for the acknowledgement output filenames:

- 997 acknowledgement: `s3://amzn-s3-demo-bucket/OUT/TP_ID/ACK/edi214xml-test83.txt.2023-11-21T19:26:49.774Z.997`
- 999 X231 acknowledgement: `s3://amzn-s3-demo-bucket/OUT/TP_ID/ACK/edi835x221.xml-test83.txt.2023-11-21T19:26:49.774Z.999x231`
- TA1 acknowledgement: `s3://amzn-s3-demo-bucket/OUT/TP_ID/ACK/edi214xml-test83.txt.2023-11-21T19:26:49.774Z.TA1`

For direct transformer API calls, the format is `s3://amzn-s3-demo-bucket/OUT/ACK/`*`filename`*`.`*`timestamp`*`.997` (`.TA1` for TA1 acknowledgements).

Outbound EDI

You can use AWS B2B Data Interchange to generate X12 EDI documents for purposes of sending transactional data to your partners. AWS B2B Data Interchange also automatically generates X12 functional acknowledgements (including TA1s, 997s, and 999s) in response to inbound EDI.

For example, you may need to send an 810 Invoice after receiving an 850 Purchase Order from a manufacturing customer. Similarly, you may need to send an 835 Claim Payment after receiving an 837 Claim from a healthcare provider. Whether responding to or initiating a transaction, there are numerous scenarios where you may need to generate and send X12 EDI outbound to your trading partners. To generate outbound X12 EDI, it is common to use JSON or XML formatted data for your input. This data is typically exported from a downstream application, such as an Enterprise Resource Planning (ERP) solution or Claims Management Software (CMS) system. Now, however, you can use B2B Data Interchange to generate the X12 EDI documents.

You start with an XML or JSON formatted file as input, and use the service to generate the X12 EDI document. B2B Data Interchange then saves it to an Amazon S3 bucket that has been configured

to store your output X12 EDI documents. From Amazon S3, you can automatically send it to your trading partner using AWS Transfer Family or any other data connectivity solution.

Currently, there is one way to transform JSON- or XML-formatted data into EDI: **by dropping your JSON or XML files into Amazon S3 locations that you have specified for monitoring**. With this approach, you configure an outbound transformer that is configured to transform JSON or XML data into an X12 EDI document. You then drop JSON or XML documents into the input directory specified in the attached trading capability and B2B Data Interchange listens for Amazon S3 events to automatically transform the documents and write the generated X12 into the output directory. The input and output directory used are those specified in your trading capability with trading partner ID added to the prefixes. As part of the partnership configuration, you specify one or more trading capabilities to use.

The process is similar to the corresponding inbound process. The difference is that prefixes using the trading capability ID and trading partner ID are added to the directories that you specify in the trading capability.

For example, assume that you specify the following directories in your trading capability:

- Capability input directory: `s3://EDI-bucket/input-JSON/`
- Capability output directory: `s3://EDI-bucket/output-EDI/`

When you associate your trading capability with your partnership, the service adds prefixes to both the input and output directory, changing them to the following:

- Input directory to drop JSON or XML files becomes `s3://EDI-bucket/input-JSON/`*`<capability-id>`*`/`*`<trading-partner-id>`*
- Output directory containing the generated X12 documents becomes `s3://EDI-bucket/output-EDI/`*`<capability-id>`*`/`*`<trading-partner-id>`*

You then drop JSON or XML files into the trading-partner-ID prefix in the input directory to generate EDI. The generated EDI is then written to the trading-partner-ID prefix in the output directory.

Similar to the inbound process, this allows you to associate one trading capability with multiple partnerships, and have partnerships that are associated with multiple trading capabilities. Using the trading capability and trading partner IDs as prefixes gives you clear delineation as to where the EDI documents for a specific partner should be stored.

Generating outbound EDI documents

Typically, you perform the following steps to generate X12 EDI documents as output.

1. Create a profile
2. Create an outbound transformer
3. Write or import mapping code that the system uses to generate a valid X12 EDI document.

   You can start with an EDI document, and then run the CreateStarterMappingTemplate operation to create your mapping template.
4. Create a trading capability for outbound EDI. Make sure to select **Outbound** for the **EDI direction**.
5. Create a partnership for outbound EDI
6. Test your transformation workflow. For details, see the Testing end-to-end topic from our EDI document exchange with AWS B2B Data Interchange workshop.

   Tip: These testing instructions are written for testing inbound EDI, so you need to adapt them for testing outbound EDI.

Create a profile

You can use *profiles* to store contact information and details about your own business and specify a unique name to easily identify this profile A profile contains the following types of information.

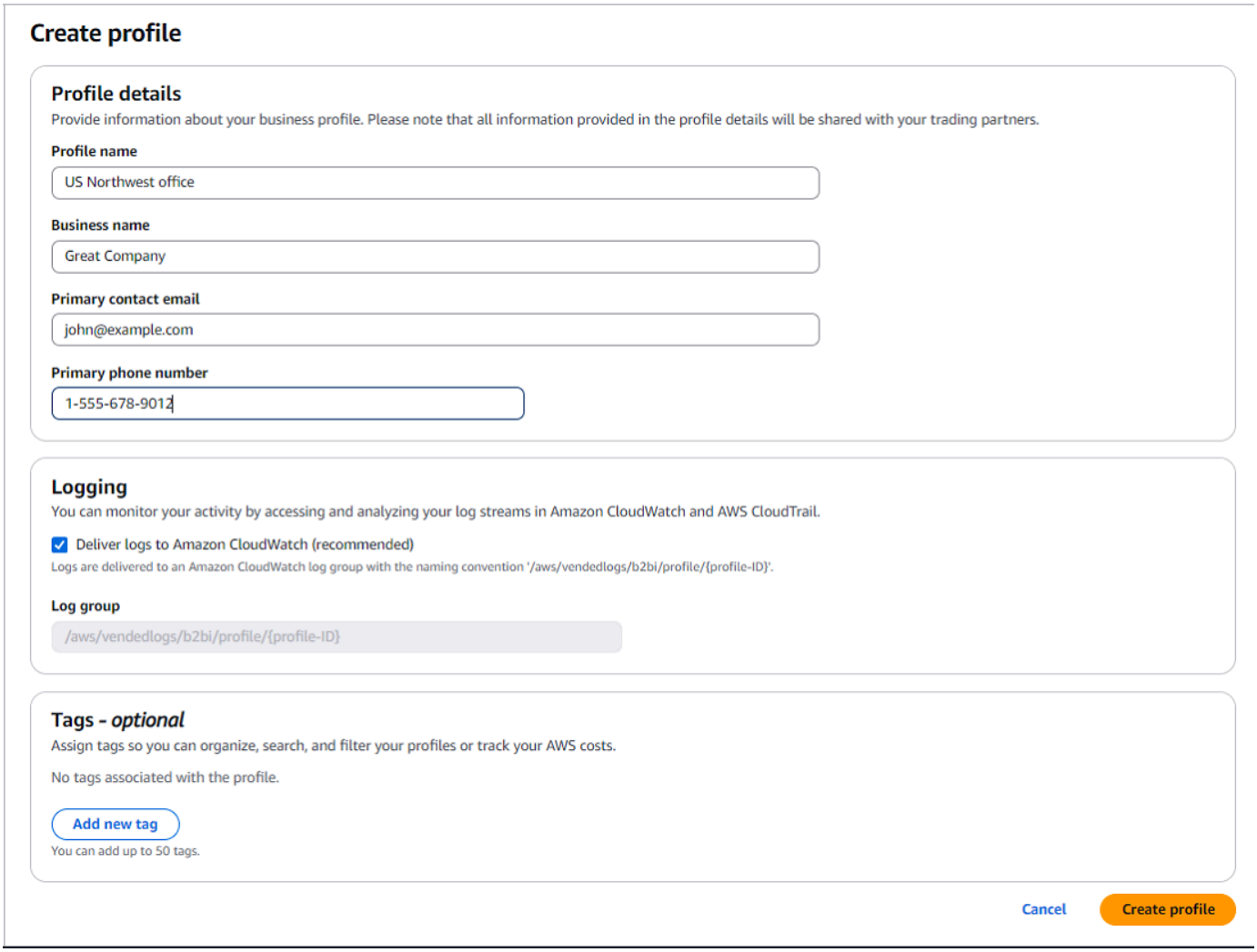
- **Profile details**: This section contains the profile name, the name of the business, a contact email address, and a phone number.

  > **Note**
  >
  > These details are all your characteristics, not those describing your trading partner. The latter are described as part of the partnership resource.

- **Logging**: This section describes the logging configuration. You can also opt out of logging (not recommended).
- **Tagging**: Tag your profiles to easily organize, search, and filter your profiles globally.

To create a profile

1. Open the AWS B2B Data Interchange console at https://console.aws.amazon.com/b2bi/ and select **Profiles** from the navigation pane, then choose **Create profile**.
2. Enter the profile details, the name of the profile, the name of the business represented, and the contact information (email and phone number).
3. Logging is selected by default. Clear the box to turn off logging (not recommended). The log group is based on the profile ID, for example, `/aws/vendedlogs/b2bi/p-ABCDE111122223333`.
4. Optionally, add tags as needed.



Create an outbound transformer

An outbound transformer takes in a sample template and produces an EDI, X12-formatted document that you can send to your trading partners.

To create an outbound transformer

1. Open the AWS B2B Data Interchange console at https://console.aws.amazon.com/b2bi/ and select **Transformers** from the navigation pane, then choose **Create transformer**.
2. On the Transformer configuration page, enter the following information.

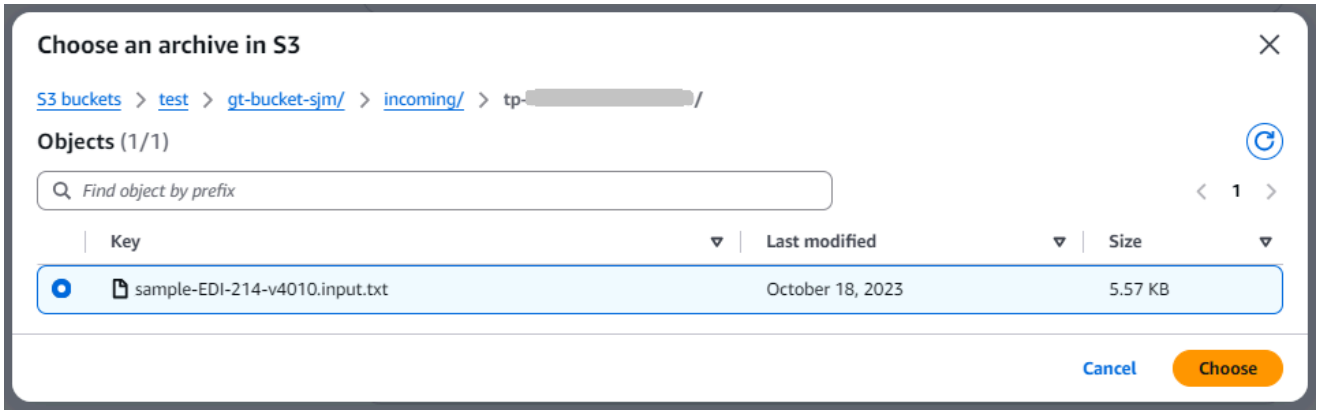
   a. Enter a name (no spaces).

   b. In **Transfer settings**, choose **Outbound EDI**, and select an EDI document number and X12 version from the dropdown menus.

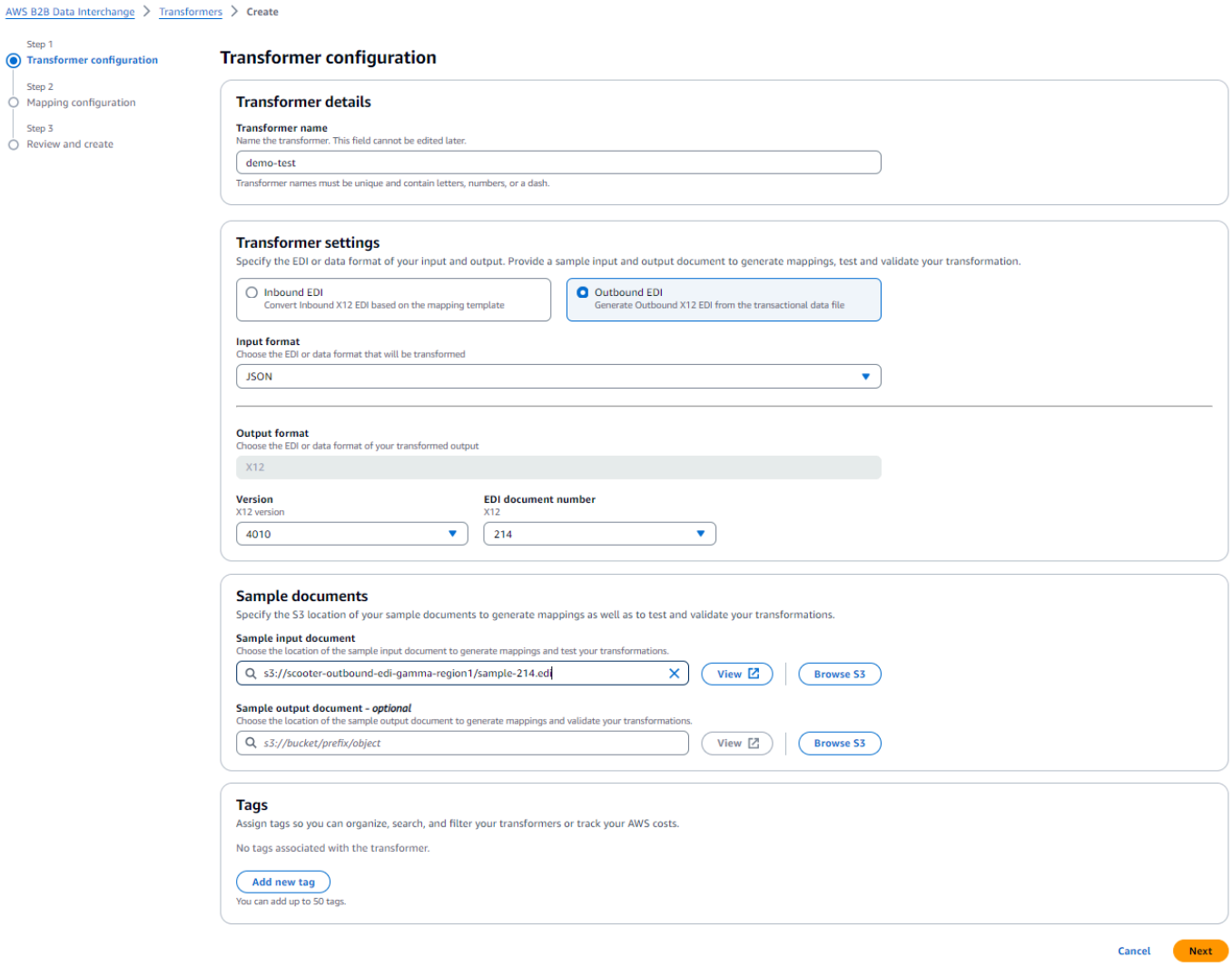
   c. For the Input format, select **JSON** or **XML**, depending upon the format for the documents to be converted by this transformer.

   d. In the **Sample documents** pane, select a sample input document, and optionally a sample output document from your available Amazon S3 buckets.

   Provide the bucket and prefix in Amazon S3 for a sample document. This is useful for making sure the transformer functions correctly.



3. Choose **Next** to proceed to the next stage of transformer creation.



4. The **Mapping configuration** screen appears, with the **Mapping editor** panel populated. You can use generative AI-assisted EDI mapping to expedite the mapping configuration. For details, see Generative AI-assisted EDI mapping.

   The items in your mapping editor are the only items that are extracted from the input EDI document, and that are then saved to your output file, located in your Amazon S3 output location.

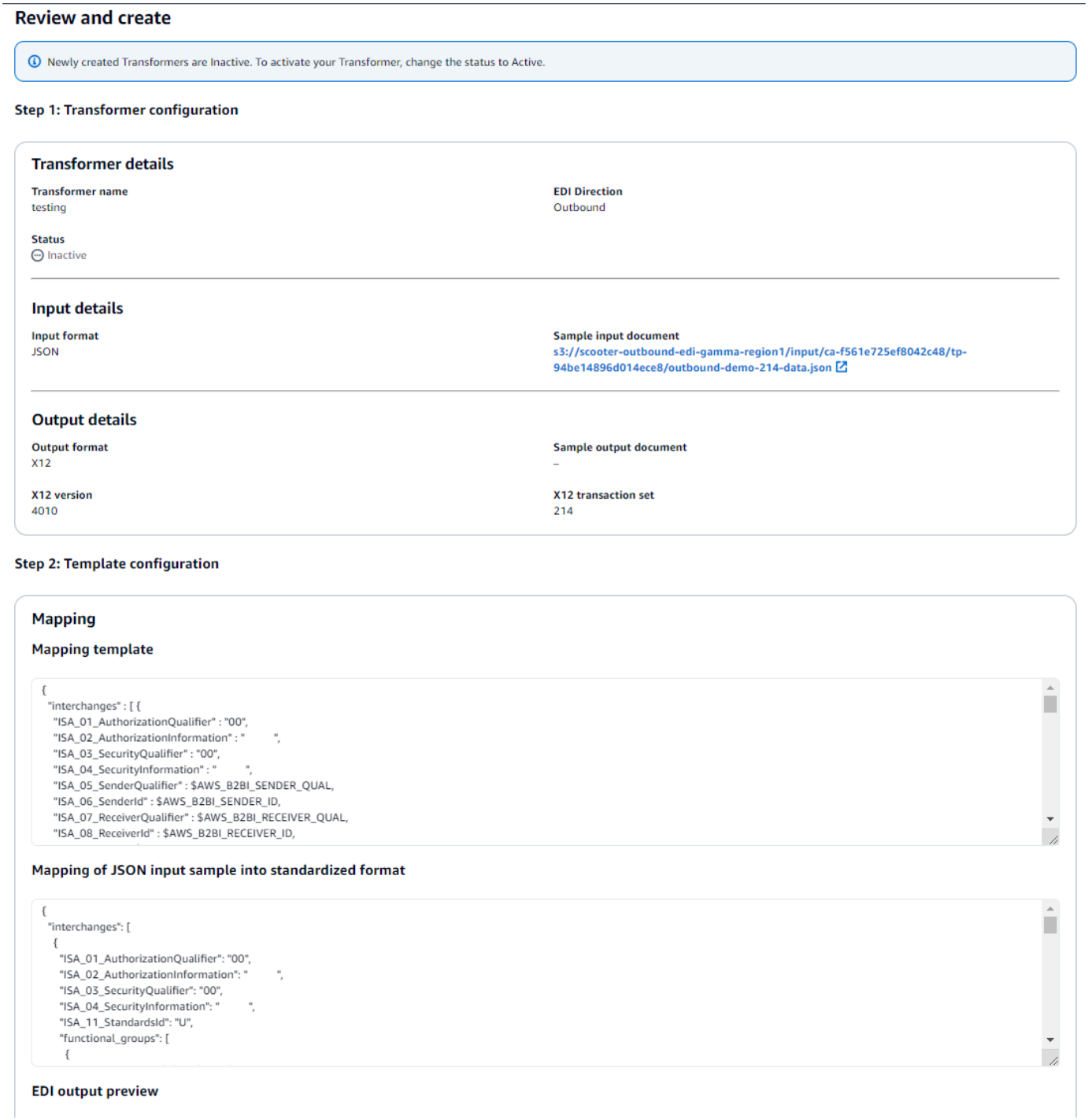
   You use the **Mapping template editor** to only include certain pieces of your EDI documents.

   If you chose not to customize the output format using the **Mapping template editor**,AWS B2B Data Interchange transforms EDI document inputs using the default, service-defined format shown on the left side of your screen.

   The pieces you select are previewed in the mapping preview pane.

5. When you are happy with your mappings, choose **Next**, which takes you to the review page. Note that newly created transformers are inactive.

> **Note**
>
> A status of **Inactive** indicates that the transformer is not used in any trading capabilities: it is essentially in edit mode. When you are finished editing and updating the transformer, you change the status to **Active**. Then, you can associate the transformer with a trading capability. At this point, the transformer is essentially locked, and in production mode.



6. After your review is complete, choose **Save** to create the transformer.

Create a trading capability for outbound EDI

Trading capabilities contain the information required to build your event-driven EDI workflows. To create a trading capability, specify the EDI direction, add details about the EDI document number and version, choose the transformer to use to transform or generate your EDI, and specify the input and output directories used to source and store documents. Based on the EDI direction selected and the transformer attached to the trading capability, you can use the capability to automatically:

- Transform incoming EDI documents into JSON or XML outputs.
- Transform XML or JSON data stored in Amazon S3 into EDI documents.

To create a trading capability

1. Open the AWS B2B Data Interchange console at https://console.aws.amazon.com/b2bi/ and select **Trading capabilities** from the navigation pane, then choose **Create trading capability**.
2. In the **Trading capability settings** section, enter the following information.
   - Enter a descriptive, unique name for the trading capability.
   - Select an **EDI direction**, either **Inbound** or **Outbound**.
   - Choose an **X12 version** and **X12 transaction** set from the corresponding dropdown menus.
   - In the **Apply transformer** field, choose a transformer to apply to this trading capability.
3. In the **Configure directories** section, you configure both the input and output directories that are used to source and store documents.
   - In the **Input directory** area, enter an Amazon S3 bucket.
   - Choose **Browse S3** to navigate to your available Amazon S3 buckets, where you can select a bucket (and optionally a prefix) to specify your input directory.

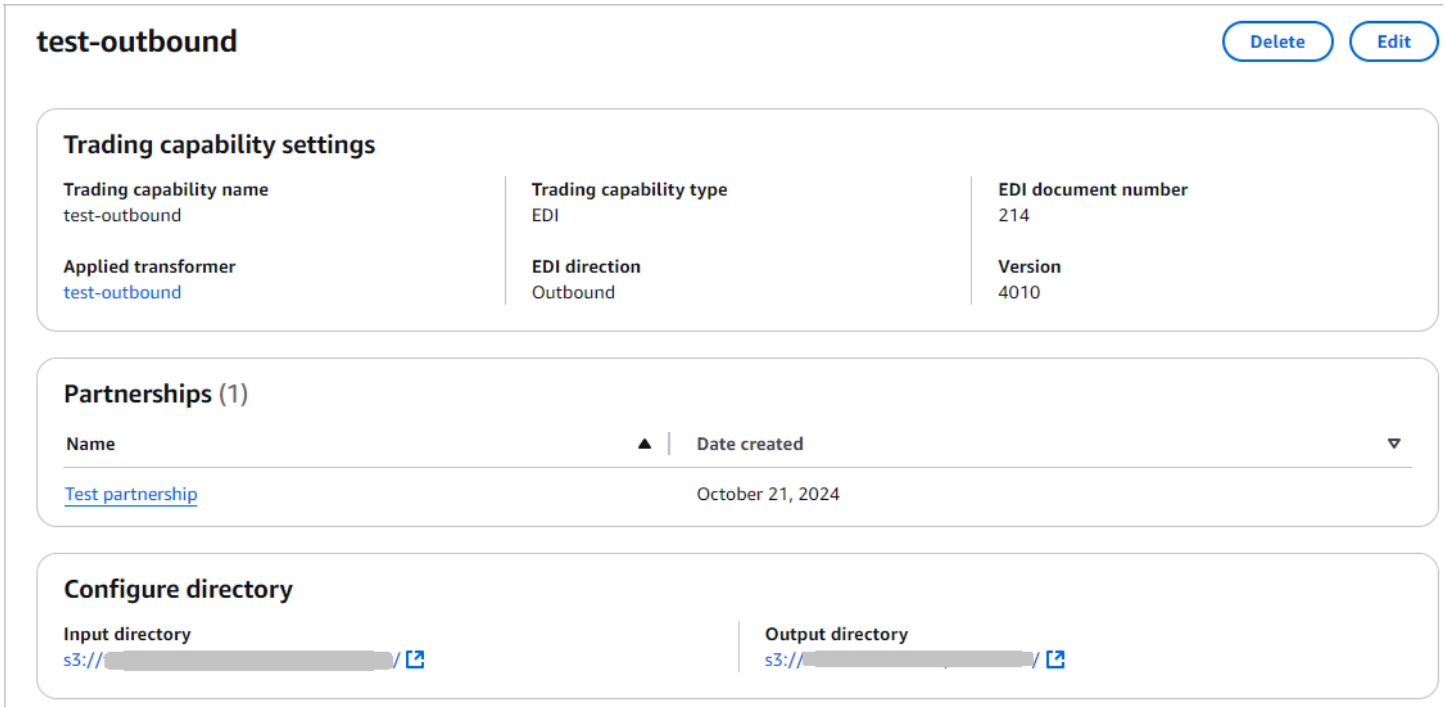
     > **Note**
     >
     > B2B Data Interchange will create and monitor prefixes in your input directory for input X12 documents (for inbound X12) or for input JSON/XML documents (for generating X12).

   - Choose **Copy policy** to copy a policy that you can then paste into your input directory's bucket policy.

- Configure your output directory in the **Output directory** area, similarly to how you configured the input directory.

> **Note**
>
> B2B Data Interchange will create prefixes in the specified output directory to store the transformed X12 documents (in the case of inbound X12) or storing the generated X12 documents (in the case of outbound X12).

4. Optionally, add tags as needed.
5. After you have configured all of the settings, choose **Create capability**.



> **Note**
>
> - For your input and output directories, update the bucket policy (Configure your Amazon S3 bucket policies). If your input or output buckets use SSE-KMS encryption, you also need to update the policy for your AWS KMS key. For details, see the section called "Example bucket policies".

- Enable EventBridge notifications for the Amazon S3 buckets used by the trading capability. For details, see (Configure your Amazon S3 bucket EventBridge setting).

Create a partnership for outbound EDI

A *partnership* represents the connection between you and your trading partner. It incorporates a profile and one or more trading capabilities. It is also where you define the interchange control header and functional group header information necessary to generate outbound EDI documents.

If you intend to perform outbound EDI transformations with this partner, fill in details in the **Outbound EDI configuration** section.

To create a partnership

1. Open the AWS B2B Data Interchange console at https://console.aws.amazon.com/b2bi/ and select **Partnerships** from the navigation pane, then choose **Create partnership**.
2. In the **Partnership details** section, provide the following information.
   a. Enter a descriptive name for the partnership.
   b. Enter an email address to associate with the partnership. Provide the trading partner's email address.
   c. Choose a profile from the dropdown menu.
   d. Select one or more trading capabilities from the **Trading capabilities** list.
3. Enter header details in the **Outbound EDI configuration**. The system uses the outbound EDI header information to format the outbound EDI document according to the needs of the partner to whom you are sending these documents.
   - Provide **Interchange control header** information: also known as the ISA segment
   - Provide **Functional group header** information: also known as the GS segment
   - Optionally, specify **Delimiters**

> **Note**
>
> When creating or updating a Partnership, you must specify all delimiters or leave them all blank. Defining certain delimiters, but not others, is not a valid configuration.

Take care when specifying delimiters: for more information, see Delimiters for outbound EDI.

- Optionally, for **EDI validation**, select **Enable outbound EDI** (selected by default)

4. Optionally, add tags as needed.
5. After you have configured all of the settings, choose **Create partnership**.

After you create a partnership, B2B Data Interchange monitors the prefixes containing the trading partner ID using Amazon S3 events.

When EDI documents are written to the partnership ID prefix, they are automatically transformed into JSON/XML files and written to the partnership ID prefix that is nested within the output directory. When JSON or XML data files are written to the partnership ID prefix they are automatically transformed into X12 EDI documents and written to the partnership ID prefix that is nested within the output directory and trading capability ID prefix.

Finally, we highly recommend that you subscribe to events emitted by B2B Data Interchange for status updates on transformation jobs. For more information, see Inbound transformations or Outbound transformations.

Delimiters for outbound EDI

If your input JSON or XML files contain any delimiters, the service replaces them with a ? (question mark) character, to ensure that all generated output files have valid EDI format.

Note the following:

- When you create your partnership and specify delimiters, make sure that none of the delimiter characters are in your input files.
- If you don't specify delimiters when you create your partnership, the system uses defaults. The default delimiters are * (asterisk), : (colon), ~ (tilde), and \n (newline).
- Make sure that your mapping template doesn't introduce any delimiter characters into the content that will be transformed to EDI.

Control numbers

This section describes how AWS B2B Data Interchange generates control numbers. A control number is an integer that is used to identify a specific interchange, functional group, or transaction within a functional group as it pertains to a specific trading partner. AWS B2B Data Interchange generates control numbers for each X12 envelope contained in a generated EDI acknowledgement or outbound EDI document. The control numbers created and maintained by B2B Data Interchange include the following:

- **Interchange Control Number**: For the ISA (interchange) envelope, B2B Data Interchange generates an interchange control number that is unique to the sender ID and receiver ID pair. For example, the first acknowledgement or outbound EDI document sent from **SEND01** to **RECV01** receives an ICN of 001. The next interchange (whether an acknowledgement or outbound EDI document) sent from **SEND01** to **REVC01** receives an ICN of 002, and so on.

  > **Note**
  >
  > Specifically, this number is unique for the I*SA05 and ISA06 (sender)* & *ISA07 and ISA08 (receiver)* combination.

- **Functional Group Control Number**: For the GS (functional group) envelope, B2B Data Interchange generates a functional group control number that is unique to the sender ID, receiver ID, and functional identifier code combination. For example, the first functional group in an interchange sent from **SEND01** to **RECV01** with a functional identifier code of FA, would be assigned a functional group control number of 001. The next functional group (whether in the same interchange or a new interchange) with the same unique combination of sender ID, receiver ID, and functional identifier code is assigned a functional group control number of 002, and so on.

  In the case where there is a functional group with the same sender ID and receiver ID, but a different functional identifier code, the functional group control number would also be 0001, as this introduces a new, unique combination of sender ID, receiver ID, and functional identifier code.

> **Note**
>
> Specifically, the functional group control number is unique for the *GS01 (functional identifier code)* & *GS02 (sender)* & *GS03 (receiver)* combination.

- **Transaction Set Control Number**: For ST (transactional level) envelope, B2B Data Interchange generates a unique transaction set control number for every transaction in a functional group. For example, if there are three transactions in a functional group, the transactions are assigned transaction set control numbers of 001, 002, and 003. In the case where there is another functional group in the same interchange with two transactions, the transactions in this functional group are assigned transaction set control numbers of 001 and 002.

The following sample EDI document shows the relationship of the three envelopes (indenting added for readability).

```
ISA*01*0000000000*01*0000000000*ZZ*ABCDEFGHIJKLMNO*ZZ*123456789012345*101127*1719*U*00400*00000
    GS*FA*999999999*4405197800*20111206*1100*1*X*004010VICS
        ST*997*0001
            AK1*PO*1421
            AK9*A*1*1*1
        SE*4*0001
    GE*1*1
IEA*1*000000001
```

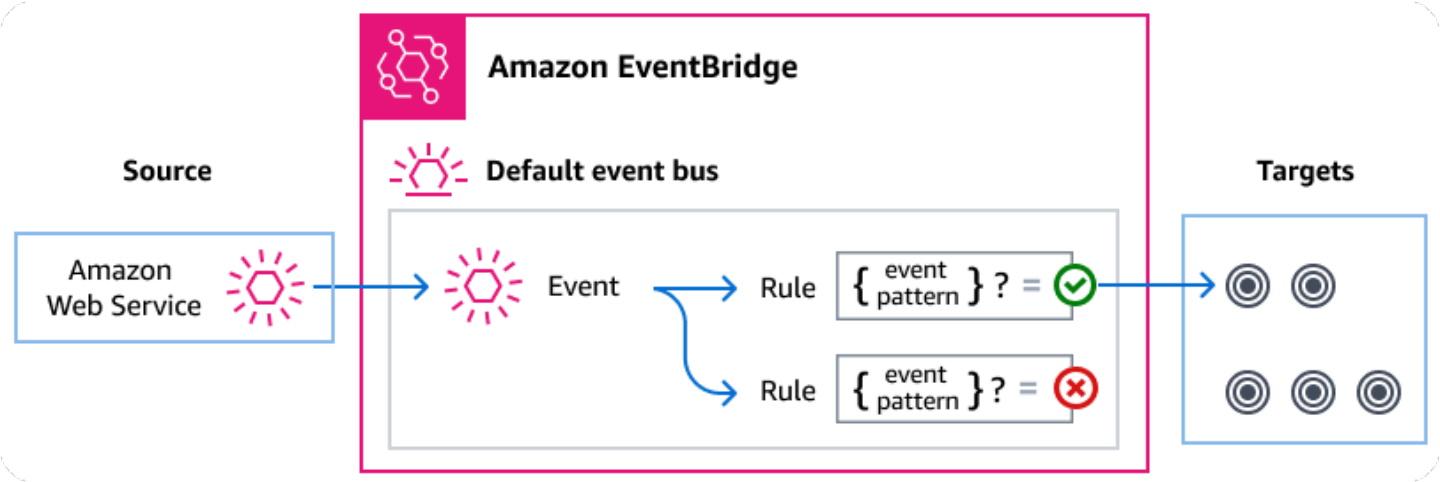
We generate control numbers for each of the X12 envelopes. All of these numbers are unique for the specific sender/receiver ID combination.

> **Note**
>
> The control numbers that we generate are also unique across AWS account and AWS Region.

Managing AWS B2B Data Interchange events using Amazon EventBridge

Amazon EventBridge is a serverless service that uses events to connect application components together, making it easier for you to build scalable event-driven applications. Event-driven architecture is a style of building loosely-coupled software systems that work together by emitting and responding to events. Events represent an operation that succeeds or fails.

As with many AWS services, AWS B2B Data Interchange generates and sends events to the EventBridge default event bus, which is automatically provisioned in every AWS account. An event bus is a router that receives events and delivers them to zero or more destinations, or *targets*. Rules you specify for the event bus evaluate events as they arrive. Each rule checks whether an event matches the rule's *event pattern*. If the event does match, the event bus sends the event to the specified target(s).



Topics

- AWS B2B Data Interchange events
- Sending AWS B2B Data Interchange events using EventBridge rules
- Amazon EventBridge permissions
- Additional EventBridge resources
- AWS B2B Data Interchange events detail reference

AWS B2B Data Interchange events

AWS B2B Data Interchange sends events to the default EventBridge event bus automatically. You can create rules on the event bus; each rule includes an event pattern and one or more targets. Events that match a rule's event pattern are delivered to the specified targets on a best effort basis. Events might be delivered out of order.

The following events are generated by AWS B2B Data Interchange. For more information, see EventBridge events in the *Amazon EventBridge User Guide*.

AWS B2B Data Interchange emits the following events to EventBridge.

Event detail type	Description
Transformation Completed	A transformation has completed successfully.
Transformation Failed	An attempted transformation has failed.
Acknowledgement Completed	An Acknowledgement was generated and written to Amazon S3.
Acknowledgement Failed	An Acknowledgement either failed to generate or failed to write to Amazon S3.

Sending AWS B2B Data Interchange events using EventBridge rules

To have the EventBridge default event bus send AWS B2B Data Interchange events to a target, you must create a rule that contains an event pattern that matches the data in the desired AWS B2B Data Interchange events.

Creating a rule consists of the following general steps:

1. Creating an event pattern for the rule that specifies:
   - AWS B2B Data Interchange is the source of events being evaluated by the rule.
   - (Optional): Any other event data to match against.

   For more information, see ???

2. (Optional): Creating an *input transformer* that customizes the data from the event before EventBridge passes the information to the target of the rule.

   For more information, see Input transformation in the *EventBridge User Guide*.

3. Specifying the target(s) to which you want EventBridge to deliver events that match the event pattern.

   Targets can be other AWS services, software-as-a-service (SaaS) applications, API destinations, or other custom endpoints. For more information, see Targets in the *EventBridge User Guide*.

For comprehensive instructions on creating event bus rules, see Creating rules that react to events in the *EventBridge User Guide*.

Creating event patterns for AWS B2B Data Interchange events

When AWS B2B Data Interchange delivers an event to the default event bus, EventBridge uses the event pattern defined for each rule to determine if the event should be delivered to the rule's target(s). An event pattern matches the data in the desired AWS B2B Data Interchange events. Each event pattern is a JSON object that contains:

- A `source` attribute that identifies the service sending the event. For AWS B2B Data Interchange events, the source is `aws.b2bi`.
- (Optional): A `detail-type` attribute that contains an array of the event types to match.
- (Optional): A `detail` attribute containing any other event data on which to match.

For example, the following event pattern matches against all events from AWS B2B Data Interchange:

```
{
  "source": ["aws.b2bi"]
}
```

The following event pattern matches all of the B2B Data Interchange events.

```
{
  "source": ["aws.b2bi"],
  "detail-type": ["Transformation Completed", "Transformation Failed"]
```

```
}
```

The following event pattern matches successful transformations for a trading partner with ID *trading-partner-id*.

```
{
  "source": ["aws.b2bi"],
  "detail-type": ["Transformation Completed"],
  "detail": {
    "trading-partner-id": [trading-partner-id]
  }
}
```

For more information on writing event patterns, see Event patterns in the *EventBridge User Guide*.

Testing event patterns for AWS B2B Data Interchange events in EventBridge

You can use the EventBridge Sandbox to quickly define and test an event pattern, without having to complete the larger process of creating or editing a rule. Using the Sandbox, you can define an event pattern and use a sample event to confirm the pattern matches the desired events. EventBridge give you the option of creating a new rule using that event pattern, directly from the sandbox.

For more information, see Testing an event pattern using the EventBridge Sandbox in the *EventBridge User Guide*.

Amazon EventBridge permissions

AWS B2B Data Interchange doesn't require any additional permissions to deliver events to Amazon EventBridge.

The targets you specify may need specific permissions or configuration. For more details on using specific services for targets, see Amazon EventBridge targets in the *Amazon EventBridge User Guide*.

Additional EventBridge resources

Refer to the following topics in the *Amazon EventBridge User Guide* for more information on how to use EventBridge to process and manage events.

- For detailed information on how event buses work, see Amazon EventBridge event bus.
- For information on event structure, see Events.
- For information on constructing event patterns for EventBridge to use when matching events against rules, see Event patterns.
- For information on creating rules to specify which events EventBridge processes, see Rules.
- For information on to specify what services or other destinations EventBridge sends matched events to, see Targets.

AWS B2B Data Interchange events detail reference

All events from AWS services have a common set of fields containing metadata about the event, such as the AWS service that is the source of the event, the time the event was generated, the account and region in which the event took place, and others. For definitions of these general fields, see Event structure reference in the *Amazon EventBridge User Guide*.

In addition, each event has a `detail` field that contains data specific to that particular event. The reference below defines the detail fields for the various AWS B2B Data Interchange events.

When using EventBridge to select and manage AWS B2B Data Interchange events, it's useful to keep the following in mind:

- The `source` field for all events from AWS B2B Data Interchange is set to `aws.b2bi`.
- The `detail-type` field specifies the event type.

  For example, `Transformation Completed`.
- The `detail` field contains the data that is specific to that particular event.

For information on constructing event patterns that enable rules to match AWS B2B Data Interchange events, see Event patterns in the *Amazon EventBridge User Guide*.

For more information on events and how EventBridge processes them, see Amazon EventBridge events in the *Amazon EventBridge User Guide*.

Details fields for transformation events

This section describes the detail fields for the following events:

- Transformation Completed
- Transformation Failed

The `source` and `detail-type` fields are included because they contain specific values for AWS B2B Data Interchange events. For definitions of the other metadata fields that are included in all events, see Event structure reference in the *Amazon EventBridge User Guide*.

```
{
  . . .,
  "detail-type": "string",
  "source": "aws.b2bi",
  . . .,
  "detail": {
    "transformer-job-id" : "string",
    "trading-partner-id" : "string",
    "start-timestamp" : "string"
    "end-timestamp" : "string",
    "x12-transaction-set" : "string",
    "x12-version" : "string",
    "input-file-s3-attributes" : {
       "bucket" : "string",
       "object-key" : "string",
       "object-size-bytes" : "number"
    },
    "output-file-s3-attributes" : {
       "bucket" : "string",
       "object-key" : "string",
       "object-size-bytes" : "number"
    },
    "failure-message" : "string",
    "failure-code" : "string",
    "ack-generation-status" : "string",
    "ack-error-code-detected" : "boolean",
    "input-format" : "string",
    "output-format" : "string",
    "validation-status" : "string"
  }
}
```

`detail-type`

Identifies the type of event.

For this event, this value is either `Transformation Completed` or `Transformation Failed`.

`source`

Identifies the service that generated the event. For AWS B2B Data Interchange events, this value is `aws.b2bi`.

`detail`

A JSON object that contains information about the event. The service generating the event determines the content of this field.

For this event, this data includes:

`transformer-job-id`

The unique, system-generated identifier for a transformer run

`trading-partner-id`

The unique, system-generated identifier for a trading partner.

`start-timestamp`

The time stamp for when the transformation request begins processing.

`end-timestamp`

The time stamp for when the transformation request finishes processing.

`x12-transaction-set`

A list of supported X12 transaction sets. Transaction sets are maintained by the X12 Accredited Standards Committee.

`x12-version`

The version to use for the specified X12 transaction set.

`input-file-s3-attributes`

This parameter contains the details of the location of the AWS input storage file.

`bucket`

The container for the object in Amazon S3

`object-key`

The name assigned to the object in Amazon S3.

`object-size-bytes`

The size, in bytes, of the input file.

`output-file-s3-attributes`

This parameter contains the details of the location of the AWS output storage file.

`bucket`

The container for the object in Amazon S3

`object-key`

The name assigned to the object in Amazon S3.

`object-size-bytes`

The size, in bytes, of the output file.

`failure-message`

For failed transformations, the details for why the transform failed.

`failure-code`

For failed transformations, the reason code for why the transformations failed.

`ack-generation-status`

This field is only populated when the transformation is supposed to generate an acknowledgement. The status of acknowledgement for this transformation. Valid values are `NOT_ATTEMPTED`, `COMPLETED`, or `FAILED`.

`ack-error-code-detected`

This field is only populated for transformations that have a `COMPLETED` `ack-generation-status`. Specifies whether or not an error code was detected during the validation step of acknowledgement generation.

`input-format`

The format for the source, or input, data: either `JSON` or `XML`. Only populated for Outbound EDI transformations.

`output-format`

The format for the output file, `X12`. Only populated for Outbound EDI transformations.

`validation-status`

Only populated for Outbound EDI Transformation Completed events. Value is one of `SUCCEEDED`, `FAILED`, or `NOT_ATTEMPTED`.

Details fields for acknowledgement events

This section describes the detail fields for the following events:

- Acknowledgement Completed
- Acknowledgement Failed

The `source` and `detail-type` fields are included because they contain specific values for AWS B2B Data Interchange events. For definitions of the other metadata fields that are included in all events, see Event structure reference in the *Amazon EventBridge User Guide*.

```
{
  . . .,
  "detail-type": "string",
  "source": "aws.b2bi",
  . . .,
  "detail": {
    "transformer-job-id" : "string",
    "trading-partner-id" : "string",
    "start-timestamp" : "string"
    "end-timestamp" : "string",
    "input-x12-transaction-set" : "string",
    "input-x12-version" : "string",
    "input-file-s3-attributes" : {
       "bucket" : "string",
       "object-key" : "string",
       "object-size-bytes" : "number"
    },
    "ack-x12-type : "string",
    "ack-x12-version : "string",
    "ack-file-s3-attributes" : {
       "bucket" : "string",
```

```
        "object-key" : "string",
        "object-size-bytes" : "number"
      },
      "ack-error-code-detected : "boolean",
      "failure-message" : "string",
      "failure-code" : "string"
    }
}
```

`detail-type`

Identifies the type of event.

For this event, this value is either `Acknowledgement Completed` or `Acknowledgement Failed`.

`source`

Identifies the service that generated the event. For AWS B2B Data Interchange events, this value is `aws.b2bi`.

`detail`

A JSON object that contains information about the event. The service generating the event determines the content of this field.

For this event, this data includes:

`transformer-job-id`

The unique, system-generated identifier for a transformer run.

`trading-partner-id`

The unique, system-generated identifier for a trading partner.

`start-timestamp`

The time stamp for when the acknowledgement request begins processing.

`end-timestamp`

The time stamp for when the acknowledgement request finishes processing.

`input-x12-transaction-set`

The X12 transaction set of the input file.

`input-x12-version`

The version to use for the specified X12 transaction set.

`input-file-s3-attributes`

This parameter contains the details of the location of the AWS input storage file.

`bucket`

The container for the object in Amazon S3

`object-key`

The name assigned to the object in Amazon S3.

`object-size-bytes`

The size, in bytes, of the input file.

`ack-x12-type`

X12 type for the acknowledgement.

`ack-x12-version`

X12 version for the acknowledgement.

`ack-file-s3-attributes`

This parameter contains the details of the location of the AWS acknowledgement storage file. The acknowledgement file attributes are only included in Acknowledgement Completed events.

`bucket`

The container for the object in Amazon S3

`object-key`

The name assigned to the object in Amazon S3.

`object-size-bytes`

The size, in bytes, of the acknowledgement file.

`ack-error-code-detected`

For Acknowledgement Completed events, is either true or false, depending on whether an error code was detected.

`failure-message`

For failed acknowledgements, the details for why the event failed.

`failure-code`

For failed acknowledgements, the reason code for why the transformations failed.

EventBridge Example events for B2B Data Interchange

This section presents the details for some example events generated by B2B Data Interchange.

Example Transformation Completed event (for an event that originated from a transformer or standalone)

The following example shows an event where an inbound transformation completed successfully.

```
{
  "version": "0",
  "id": "370d77b7-cb45-60de-7fc6-cb0522a3e43d",
  "detail-type": "Transformation Completed",
  "source": "aws.b2bi",
  "account": "1234abcd5678",
  "time": "2024-03-08T19:52:48Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:b2bi:us-east-2:1234abcd5678:transformer/tr-1234567890abcdef0"
  ],
  "detail": {
    "transformer-job-id": "tj-1111aa2222bb33334444cc",
    "start-timestamp": "2024-03-08T19:52:47.418Z",
    "end-timestamp": "2024-03-08T19:52:48.089Z",
    "x12-transaction-set": "X12_214",
    "x12-version": "VERSION_4010",
    "input-file-s3-attributes": {
      "bucket": "amzn-s3-demo-bucket",
      "object-key": "edi_214_4010.txt",
      "object-size-bytes": 1034
    },
    "output-file-s3-attributes": {
      "bucket": "amzn-s3-demo-bucket1",
      "object-key": "getTransformerJobTestOutput/
edi_214_4010.txt.2024-03-12T22:57:42.182Z.json",
```

```
      "object-size-bytes": 4174
    },
    "ack-generation-status": "COMPLETED",
    "ack-error-code-detected": false
  }
}
```

Example Transformation Failed event (for an event that originated from a Capability)

The following example shows an event where a transformation failed to complete successfully.

```
{
    "version": "0",
    "id": "1ba25f10-d560-3e06-49bb-761a2de88679",
    "detail-type": "Transformation Failed",
    "source": "aws.b2bi",
    "account": "1234abcd5678",
    "time": "2024-03-09T07:29:12Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:b2bi:us-east-2:1234abcd5678:transformer/tr-1234567890abcdef0",
        "arn:aws:b2bi:us-east-2:639140540422:profile/p-11111aaaa2222bbbb3",
        "arn:aws:b2bi:us-east-2:639140540422:capability/ca-ABCDE111122223333",
        "arn:aws:b2bi:us-east-2:639140540422:partnership/ps-11112222333344445"
    ],
    "detail": {
        "trading-partner-id": "tp-aaaa11bbbb22cccc33dddd",
        "start-timestamp": "2024-03-09T07:29:12.015Z",
        "end-timestamp": "2024-03-09T07:29:12.149Z",
        "x12-transaction-set": "X12_214",
        "x12-version": "VERSION_4010",
        "failure-message": "Access denied when getting object attributes from s3://
amzn-s3-demo-bucket/myinputs/tp-aaaa11bbbb22cccc33dddd/edi_file_mar_14_2024_2.txt",
        "failure-code": "FILE_TRANSFORM_FAILED",
        "ack-generation-status": "NOT_ATTEMPTED"
    }
}
```

Example Acknowledgement Completed event

The following example shows an event where an acknowledgement completed successfully.

```
{
```

```
    "version": "0",
    "id": "1ba25f10-d560-3e06-49bb-761a2de88679",
    "detail-type": "Acknowledgement Completed",
    "source": "aws.b2bi",
    "account": "1234abcd5678",
    "time": "2024-03-09T07:29:12Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:b2bi:us-east-2:1234abcd5678:transformer/tr-1234567890abcdef0",
        "arn:aws:b2bi:us-east-2:639140540422:profile/p-11111aaaa2222bbbb3",
        "arn:aws:b2bi:us-east-2:639140540422:capability/ca-ABCDE111122223333",
        "arn:aws:b2bi:us-east-2:639140540422:partnership/ps-11112222333344445"
    ],
    "detail": {
        "trading-partner-id": "tp-aaaa11bbbb22cccc33dddd",
        "start-timestamp": "2024-03-09T07:29:12.015Z",
        "end-timestamp": "2024-03-09T07:29:12.149Z",
        "input-x12-transaction-set": "X12_214",
        "input-x12-version": "VERSION_4010",
        "input-file-s3-attributes": {
           "bucket": "amzn-s3-demo-bucket",
           "object-key": "edi_214_4010.txt",
           "object-size-bytes": 449
        },
        "ack-x12-type": "X12_997",
        "ack-x12-version": "VERSION_4010",
        "ack-file-s3-attributes": {
           "bucket": "amzn-s3-demo-bucket2",
           "object-key": "testouput/tp-1234567890abcdef0/ACK/edi_214_4010_event_1 copy
 4.txt.2024-04-23T17:00:14.007Z.json.997",
           "object-size-bytes": 379
        },
        "ack-error-code-detected": true
    }
}
```


Example Acknowledgement Failed event

The following example shows an event where an acknowledgement failed.


```
{
    "version": "0",
    "id": "1ba25f10-d560-3e06-49bb-761a2de88679",
    "detail-type": "Acknowledgement Completed",
```

```
    "source": "aws.b2bi",
    "account": "1234abcd5678",
    "time": "2024-03-09T07:29:12Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:b2bi:us-east-2:1234abcd5678:transformer/tr-1234567890abcdef0",
        "arn:aws:b2bi:us-east-2:639140540422:profile/p-11111aaaa2222bbbb3",
        "arn:aws:b2bi:us-east-2:639140540422:capability/ca-ABCDE111122223333",
        "arn:aws:b2bi:us-east-2:639140540422:partnership/ps-11112222333344445"
    ],
    "detail": {
        "trading-partner-id": "tp-aaaa11bbbb22cccc33dddd",
        "start-timestamp": "2024-03-09T07:29:12.015Z",
        "end-timestamp": "2024-03-09T07:29:12.149Z",
        "input-x12-transaction-set": "X12_214",
        "input-x12-version": "VERSION_4010",
        "input-file-s3-attributes": {
           "bucket": "amzn-s3-demo-bucket",
           "object-key": "edi_214_4010.txt",
           "object-size-bytes": 449
        },
        "ack-x12-type": "X12_997",
        "ack-x12-version": "VERSION_4010",
        "failure-message": "997 ACK generation failed. Refer to CloudWatch logs for
 full details.",
        "failure-code": "ACKNOWLEDGEMENT_FAILED"
    }
}
```

Security in AWS B2B Data Interchange

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 AWS B2B Data Interchange, 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 AWS B2B Data Interchange. The following topics show you how to configure AWS B2B Data Interchange to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your AWS B2B Data Interchange resources.

Topics

- Data protection in AWS B2B Data Interchange
- Identity and access management for AWS B2B Data Interchange
- Compliance validation for AWS B2B Data Interchange
- Resilience in AWS B2B Data Interchange

Data protection in AWS B2B Data Interchange

The AWS shared responsibility model applies to data protection in AWS B2B Data Interchange. 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 the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

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 AWS B2B Data Interchange 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.

Data encryption in Amazon S3

AWS B2B Data Interchange uses the default encryption options you set for your Amazon S3 bucket to encrypt your data. When you enable encryption on a bucket, all objects are encrypted when they are stored in the bucket. The objects are encrypted by using server-side encryption with either Amazon S3 managed keys (SSE-S3) or AWS Key Management Service (AWS KMS) managed keys

(SSE-KMS). For information about server-side encryption, see Protecting data using server-side encryption in the *Amazon Simple Storage Service User Guide*.

The following steps show you how to encrypt data in AWS B2B Data Interchange.

To allow encryption in AWS B2B Data Interchange

1. Enable default encryption for your Amazon S3 bucket. For instructions, see Amazon S3 default encryption for S3 buckets in the *Amazon Simple Storage Service User Guide*.
2. Update the AWS Identity and Access Management (IAM) role policy that is attached to the user to grant the required AWS Key Management Service (AWS KMS) permissions.
3. If you are using a session policy for the user, the session policy must grant the required AWS KMS permissions.

The following example shows an IAM policy that grants the minimum permissions required when using AWS B2B Data Interchange with an Amazon S3 bucket that is enabled for AWS KMS encryption. Include this example policy in both the user IAM role policy and session policy, if you are using one.

```
{
 "Sid": "Stmt1544140969635",
 "Action": [
  "kms:Decrypt",
  "kms:Encrypt",
  "kms:GenerateDataKey"
 ],
 "Effect": "Allow",
 "Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
}
```

Note

The KMS key ID that you specify in this policy must be the same as the one specified for the default encryption in step 1.
Root, or the IAM role that is used for the user, must be allowed in the AWS KMS key policy. For information about the AWS KMS key policy, see Using key policies in AWS KMS in the *AWS Key Management Service Developer Guide*.

No data used for service improvement

Generative AI-assisted EDI mapping uses Amazon Bedrock to assist customers with creating mapping templates. With Amazon Bedrock, your content is not used to improve the base models, and is not shared with any model providers. For more information, see https://aws.amazon.com/bedrock/faqs.

Deleting AWS B2B Data Interchange resources

You can delete the resources that you create in B2B Data Interchange. See the guidance for each resource type in following sections of the *AWS B2B Data Interchange API Reference*.

- Deleting a trading capability
- Deleting a partnership
- Deleting a profile
- Deleting a transformer

Identity and access management for AWS B2B Data Interchange

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 AWS B2B Data Interchange resources. IAM is an AWS service that you can use with no additional charge.

Topics

- How AWS B2B Data Interchange works with IAM
- Identity-based policy examples for AWS B2B Data Interchange
- Authenticating with identities
- Managing access using policies
- Troubleshooting AWS B2B Data Interchange identity and access

How AWS B2B Data Interchange works with IAM

Before you use IAM to manage access to AWS B2B Data Interchange, learn what IAM features are available to use with AWS B2B Data Interchange.

IAM features you can use with AWS B2B Data Interchange

IAM feature	B2B Data Interchange 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
Service roles	Yes
Service-linked roles	No

To get a high-level view of how B2B Data Interchange 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 B2B Data Interchange

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. You can't specify the principal in an

identity-based policy because it applies to the user or role to which it is attached. 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 B2B Data Interchange

To view examples of AWS B2B Data Interchange identity-based policies, see Identity-based policy examples for AWS B2B Data Interchange.

Resource-based policies within B2B Data Interchange

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. Adding a cross-account principal to a resource-based policy is only half of establishing the trust relationship. When the principal and the resource are in different AWS accounts, an IAM administrator in the trusted account must also grant the principal entity (user or role) permission to access the resource. They grant permission by attaching an identity-based policy to the entity. However, if a resource-based policy grants access to a principal in the same account, no additional identity-based policy is required. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Policy actions for B2B Data Interchange

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. Policy actions usually have the same name as the associated AWS API operation.

There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

To see a list of B2B Data Interchange actions, see Actions, resources, and condition keys for AWS B2B Data Interchange in the *Service Authorization Reference*.

Policy actions in B2B Data Interchange use the following prefix before the action:

```
*what is "b2bi"?
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      " *what is "b2bi"?:action1",
      " *what is "b2bi"?:action2"
         ]
```

To view examples of AWS B2B Data Interchange identity-based policies, see Identity-based policy examples for AWS B2B Data Interchange.

Policy resources for B2B Data Interchange

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. Statements must include either a `Resource` or a `NotResource` element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To see a list of B2B Data Interchange resource types and their ARNs, see GT-RESOURCES-URL in the *Service Authorization Reference*. To learn with which actions you can specify the ARN of each resource, see GT-ACTIONS-URL.

To view examples of AWS B2B Data Interchange identity-based policies, see Identity-based policy examples for AWS B2B Data Interchange.

Policy condition keys for B2B Data Interchange

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 (or `Condition` *block*) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. 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.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical `AND` operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical `OR` operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM policy elements: variables and tags in the *IAM User Guide*.

AWS supports global condition keys and service-specific condition keys. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

To see a list of B2B Data Interchange condition keys, see GT-CONDITIONS-URL in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see GT-ACTIONS-URL.

To view examples of AWS B2B Data Interchange identity-based policies, see Identity-based policy examples for AWS B2B Data Interchange.

ACLs in B2B Data Interchange

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 B2B Data Interchange

Supports ABAC (tags in policies): Partial

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. In AWS, these attributes are called *tags*. You can attach tags to IAM entities (users or roles) and to many AWS resources. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they are trying to access.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

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 B2B Data Interchange

Supports temporary credentials: Yes

Some AWS services don't work when you sign in using temporary credentials. For additional information, including which AWS services work with temporary credentials, see AWS services that work with IAM in the *IAM User Guide*.

You are using temporary credentials if you sign in to the AWS Management Console using any method except a user name and password. For example, when you access AWS using your company's single sign-on (SSO) link, that process automatically creates temporary credentials. You also automatically create temporary credentials when you sign in to the console as a user and then switch roles. For more information about switching roles, see Switch from a user to an IAM role (console) in the *IAM User Guide*.

You can manually create temporary credentials using the AWS CLI or AWS API. You can then use those temporary credentials to access AWS. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM.

Cross-service principal permissions for B2B Data Interchange

Supports forward access sessions (FAS): Yes

Service roles for B2B Data Interchange

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 B2B Data Interchange functionality. Edit service roles only when B2B Data Interchange provides guidance to do so.

Service-linked roles for B2B Data Interchange

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 AWS B2B Data Interchange

By default, users and roles don't have permission to create or modify AWS B2B Data Interchange resources. They also can't perform tasks by using the AWS Management Console, AWS Command Line Interface (AWS CLI), or AWS API. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

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 AWS B2B Data Interchange, including the format of the ARNs for each of the resource types, see Actions, Resources, and Condition Keys for AWS B2B Data Interchange in the *Service Authorization Reference*.

Topics

- Policy best practices
- Using the B2B Data Interchange console
- Allow users to view their own permissions

Policy best practices

Identity-based policies determine whether someone can create, access, or delete AWS B2B Data Interchange 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 AWS 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 B2B Data Interchange console

To access the AWS B2B Data Interchange console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the AWS B2B Data Interchange 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 B2B Data Interchange console, also attach the B2B Data Interchange `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": "*"
        }
    ]
}
```

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see AWS Signature Version 4 for API requests in the *IAM User Guide*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Multi-factor authentication in the *AWS IAM Identity Center User Guide* and AWS Multi-factor authentication in IAM in the *IAM User Guide*.

AWS account root user

When you 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. 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*.

Federated identity

As a best practice, require human users, including users that require administrator access, to use federation with an identity provider to access AWS services by using temporary credentials.

A *federated identity* is a user from your enterprise user directory, a web identity provider, the AWS Directory Service, the Identity Center directory, or any user that accesses AWS services by using credentials provided through an identity source. When federated identities access AWS accounts, they assume roles, and the roles provide temporary credentials.

For centralized access management, we recommend that you use AWS IAM Identity Center. You can create users and groups in IAM Identity Center, or you can connect and synchronize to a set of users and groups in your own identity source for use across all your AWS accounts and applications. For information about IAM Identity Center, see What is IAM Identity Center? in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the *IAM User Guide*.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see Use cases for IAM users in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. To temporarily assume an IAM role in the AWS Management Console, you can switch from a user to an IAM role (console). You can assume a

role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Methods to assume a role in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Create a role for a third-party identity provider (federation) in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
  - **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.
  - **Service role** – 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*.

- **Service-linked role** – 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.
- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Use an IAM role to grant permissions to applications running on Amazon EC2 instances 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 is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

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**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

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*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, 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 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.

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.

Access control lists (ACLs)

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.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see Access control list (ACL) overview in the *Amazon Simple Storage Service Developer Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user

or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the *IAM User Guide*.

- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see Service control policies in the *AWS Organizations User Guide*.
- **Resource control policies (RCPs)** – RCPs are JSON policies that you can use to set the maximum available permissions for resources in your accounts without updating the IAM policies attached to each resource that you own. The RCP limits permissions for resources in member accounts and can impact the effective permissions for identities, including the AWS account root user, regardless of whether they belong to your organization. For more information about Organizations and RCPs, including a list of AWS services that support RCPs, see Resource control policies (RCPs) in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. 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*.

Troubleshooting AWS B2B Data Interchange identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with AWS B2B Data Interchange and IAM.

Topics

- I am not authorized to perform an action in B2B Data Interchange
- I am not authorized to perform iam:PassRole
- I want to allow people outside of my AWS account to access my B2B Data Interchange resources

I am not authorized to perform an action in B2B Data Interchange

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 `AWS:GetWidget` permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 AWS: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 `AWS: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 AWS B2B Data Interchange.

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 AWS B2B Data Interchange. 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 B2B Data Interchange 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 AWS B2B Data Interchange supports these features, see How AWS B2B Data Interchange 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*.

Compliance validation for AWS B2B Data Interchange

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. AWS provides the following resources to help with compliance:

- Security Compliance & Governance – These solution implementation guides discuss architectural considerations and provide steps for deploying security and compliance features.
- HIPAA Eligible Services Reference – Lists HIPAA eligible services. Not all AWS services are HIPAA eligible.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- AWS Customer Compliance Guides – Understand the shared responsibility model through the lens of compliance. The guides summarize the best practices for securing AWS services and map the guidance to security controls across multiple frameworks (including National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI), and International Organization for Standardization (ISO)).
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS. Security Hub uses security controls to evaluate your AWS resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see Security Hub controls reference.
- Amazon GuardDuty – This AWS service detects potential threats to your AWS accounts, workloads, containers, and data by monitoring your environment for suspicious and malicious activities. GuardDuty can help you address various compliance requirements, like PCI DSS, by meeting intrusion detection requirements mandated by certain compliance frameworks.
- AWS Audit Manager – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Resilience in AWS B2B Data Interchange

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.

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 Availability Zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

If you need to replicate your data or applications over greater geographic distances, use AWS Local Regions. An AWS Local Region is a single data center designed to complement an existing AWS Region. Like all AWS Regions, AWS Local Regions are completely isolated from other AWS Regions.

AWS B2B Data Interchange supports up to 3 Availability Zones and is backed by an auto scaling, redundant fleet for your connection and transfer requests.

Note the following:

- Availability Zone-level redundancy is built into the service
- There are redundant fleets for each AZ.
- This redundancy is provided automatically

For more information about AWS Regions and Availability Zones, see AWS global infrastructure.

Monitoring AWS B2B Data Interchange

Monitoring is an important part of maintaining the reliability, availability, and performance of AWS B2B Data Interchange and your other AWS solutions. AWS provides the following monitoring tools to watch AWS B2B Data Interchange, report when something is wrong, and take automatic actions when appropriate:

- *Amazon CloudWatch* monitors your AWS resources and the applications you run on AWS in real time. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify. For example, you can have CloudWatch track CPU usage or other metrics of your Amazon EC2 instances and automatically launch new instances when needed. For more information, see the Amazon CloudWatch User Guide.
- *Amazon CloudWatch Logs* enables you to monitor, store, and access your log files from Amazon EC2 instances, CloudTrail, and other sources. CloudWatch Logs can monitor information in the log files and notify you when certain thresholds are met. You can also archive your log data in highly durable storage. For more information, see the Amazon CloudWatch Logs User Guide.
- *Amazon EventBridge* can be used to automate your AWS services and respond automatically to system events, such as application availability issues or resource changes. Events from AWS services are delivered to EventBridge in near real time. You can write simple rules to indicate which events are of interest to you and which automated actions to take when an event matches a rule. For more information, see Amazon EventBridge User Guide.
- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the AWS CloudTrail User Guide.

Monitoring AWS B2B Data Interchange with Amazon CloudWatch

You can monitor AWS B2B Data Interchange using CloudWatch, which publishes logs. You can access historical information and gain a better perspective on how your web application or service is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the Amazon CloudWatch User Guide.

Logging can be enabled for each profile. When you create a profile, logging is enabled by default, unless you choose to turn off logging for the profile. When you enable logging, you see the following log groups:

- One default log group.

  This log group is named `/aws/vendedlogs/b2bi/default`.

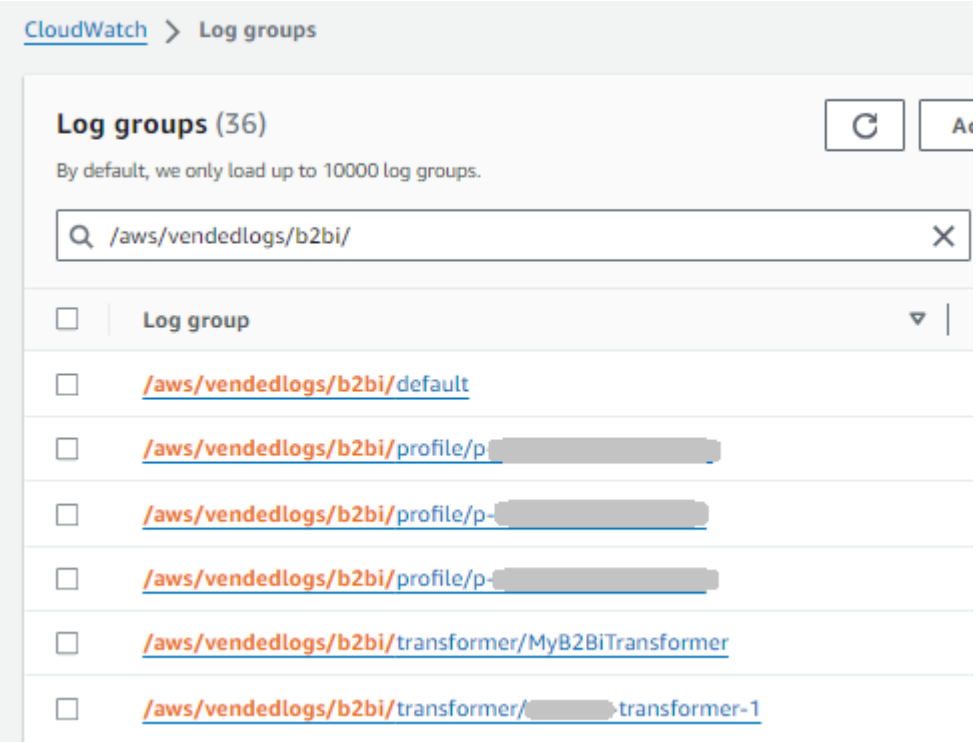
  Entries to this log group are created after a file is added to an Amazon S3 bucket, but the EDI file cannot be processed correctly.
- One log group for each profile that you create (if the profile has logging enabled).

  This log group is named `/aws/vendedlogs/b2bi/profile/`*`profile-id`*.

  Entries to this log group are created after a file is added to an Amazon S3 bucket, unless the EDI file cannot be processed correctly (logging is to the default log group in this case). The information in the EDI file is used to find a trading capability to handle the processing, and the trading capability is associated with a profile. If EDI processing fails, then there is no information available to find the trading capability and profile, and the service is unable to log to the profile log group.
- One log group for every transformer that you create (logging for transformers is always enabled).

  This log group is named `/aws/vendedlogs/b2bi/transformer/`*`transformer-name`*.

  Entries to this log group are created when a user calls the `StartTransformerJob` API. If the transformer is invoked from a trading capability, no logs are written to this group.



The following matrix describes the states and statuses that are visible in CloudWatch logs.

State/Status	Complete	Failed	In progress
Capability Match The service attempts to match the incoming file with one of the customer's existing trading capability resources	The attempt to match is successful	Attempt to match the incoming file failed	System is searching for a trading capability match
Acknowledgement The service generates acknowledgements whenever an EDI document is transformed.	An acknowledgement has been successfully completed	An acknowledgement has failed to send	System is currently attempting to send an acknowledgement

State/Status	Complete	Failed	In progress
File Transform Pertains to requests for processing transformations when initiated by calling `StartTransformerJob` .	File transformation has successfully completed	File transform has failed to complete	File transform is in progress
File Deliver The terminal state, where the system attempts to write the result of a transformation to the customer's designated output location.	File has been stored to the appropriate Amazon S3 location	File has failed to be delivered to its Amazon S3 location	Storing the file to its appropriate location is in progress

Monitoring AWS B2B Data Interchange events in Amazon EventBridge

You can monitor AWS B2B Data Interchange events in EventBridge, which delivers a stream of real-time data from your own applications, software-as-a-service (SaaS) applications, and AWS services. EventBridge routes that data to targets such as AWS Lambda and Amazon Simple Notification Service. These events are the same as those that appear in Amazon CloudWatch Events, which delivers a near real-time stream of system events that describe changes in AWS resources.

Logging AWS B2B Data Interchange API calls using AWS CloudTrail

AWS B2B Data Interchange is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS B2B Data Interchange. CloudTrail captures all API calls for AWS B2B Data Interchange as events. The calls captured include calls from the AWS

B2B Data Interchange console and code calls to the AWS B2B Data Interchange API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS B2B Data Interchange. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to AWS B2B Data Interchange, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

AWS B2B Data Interchange information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in AWS B2B Data Interchange, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing events with CloudTrail Event history.

For an ongoing record of events in your AWS account, including events for AWS B2B Data Interchange, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple regions and Receiving CloudTrail log files from multiple accounts

All AWS B2B Data Interchange actions are logged by CloudTrail and are documented in the AWS B2B Data Interchange API Reference.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.

- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element.

Understanding AWS B2B Data Interchange log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

This is an example log entry for creating a trading capability.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principal-id",
        "arn": "arn:aws:sts::account-id:assumed-role/invocation-role/role-id",
        "accountId": "account-id",
        "accessKeyId": "xxxxxxxxxxxxxxxxxxx",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "XXXXXXXXXXXXXXXXXXXX",
                "arn": "arn:aws:iam::account-id:role/invocation-role",
                "accountId": "account-id",
                "userName": "invocation-role"
            },
            "attributes": {
                "creationDate": "2023-11-24T17:24:07Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-24T17:27:05Z",
    "eventSource": "b2bi.amazonaws.com",
    "eventName": "CreateCapability",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "34.207.212.3",
```

```
    "userAgent": "example-user-agent",
    "requestParameters": {
        "name": "Integration Test EDI 214 Version 8 Update Capability",
        "type": "edi",
        "configuration": {
            "edi": {
                "type": {
                    "x12Details": {
                        "transactionSet": "HIDDEN_DUE_TO_SECURITY_REASONS",
                        "version": "HIDDEN_DUE_TO_SECURITY_REASONS"
                    }
                },
                "inputLocation": {
                    "bucketName": "HIDDEN_DUE_TO_SECURITY_REASONS",
                    "key": "HIDDEN_DUE_TO_SECURITY_REASONS"
                },
                "outputLocation": {
                    "bucketName": "HIDDEN_DUE_TO_SECURITY_REASONS",
                    "key": "HIDDEN_DUE_TO_SECURITY_REASONS"
                },
                "transformerId": "HIDDEN_DUE_TO_SECURITY_REASONS"
            }
        },
        "instructionsDocuments": [
            {
                "bucketName": "HIDDEN_DUE_TO_SECURITY_REASONS",
                "key": "HIDDEN_DUE_TO_SECURITY_REASONS"
            }
        ],
        "clientToken": "4b1da830-fb59-4d7f-afcf-0108e576d9ab"
    },
    "responseElements": {
        "capabilityId": "ca-1111aaaa2222bbbb3",
        "name": "Integration Test EDI 214 Version 8 Update Capability",
        "type": "edi",
        "configuration": {
            "edi": {
                "type": {
                    "x12Details": {
                        "transactionSet": "HIDDEN_DUE_TO_SECURITY_REASONS",
                        "version": "HIDDEN_DUE_TO_SECURITY_REASONS"
                    }
                },
                "inputLocation": {
```

```
                    "bucketName": "HIDDEN_DUE_TO_SECURITY_REASONS",
                    "key": "HIDDEN_DUE_TO_SECURITY_REASONS"
                },
                "outputLocation": {
                    "bucketName": "HIDDEN_DUE_TO_SECURITY_REASONS",
                    "key": "HIDDEN_DUE_TO_SECURITY_REASONS"
                },
                "transformerId": "HIDDEN_DUE_TO_SECURITY_REASONS"
            }
        },
        "instructionsDocuments": [
            {
                "bucketName": "HIDDEN_DUE_TO_SECURITY_REASONS",
                "key": "HIDDEN_DUE_TO_SECURITY_REASONS"
            }
        ],
        "createdAt": "2023-11-24T17:27:05.196Z"
    },
    "requestID": "abcdefgh-8765-4321-abcd-111111111111",
    "eventID": "99999999-aaaa-1111-2222-zyxwvu987654",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "recipient-account-id",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "b2bi.us-east-1.amazonaws.com"
    }
}
```

Creating AWS B2B Data Interchange resources with AWS CloudFormation

AWS B2B Data Interchange is integrated with AWS CloudFormation, a service that helps you to model and set up your AWS resources so that you can spend less time creating and managing your resources and infrastructure. You create a template that describes all the AWS resources that you want (such as profiles, partnerships, trading capabilities, and transformers), and AWS CloudFormation provisions and configures those resources for you.

When you use AWS CloudFormation, you can reuse your template to set up your AWS B2B Data Interchange resources consistently and repeatedly. Describe your resources once, and then provision the same resources over and over in multiple AWS accounts and Regions.

AWS B2B Data Interchange and AWS CloudFormation templates

To provision and configure resources for AWS B2B Data Interchange and related services, you must understand AWS CloudFormation templates. Templates are formatted text files in JSON or YAML. These templates describe the resources that you want to provision in your AWS CloudFormation stacks. If you're unfamiliar with JSON or YAML, you can use AWS CloudFormation Designer to help you get started with AWS CloudFormation templates. For more information, see What is AWS CloudFormation Designer? in the *AWS CloudFormation User Guide*.

AWS B2B Data Interchange supports creating profiles, partnerships, trading capabilities, and transformers in AWS CloudFormation. For more information, see the AWS B2B Data Interchange resource type reference in the *AWS CloudFormation User Guide*.

Learn more about AWS CloudFormation

To learn more about AWS CloudFormation, see the following resources:

- AWS CloudFormation
- AWS CloudFormation User Guide
- AWS CloudFormation API Reference
- AWS CloudFormation Command Line Interface User Guide

Access AWS B2B Data Interchange using an interface endpoint (AWS PrivateLink)

You can use AWS PrivateLink to create a private connection between your VPC and AWS B2B Data Interchange. You can access AWS B2B Data Interchange as if it were in your VPC, without the use of an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to access AWS B2B Data Interchange.

You establish this private connection by creating an *interface endpoint*, powered by AWS PrivateLink. We create an endpoint network interface in each subnet that you enable for the interface endpoint. These are requester-managed network interfaces that serve as the entry point for traffic destined for AWS B2B Data Interchange.

For more information, see Access AWS services through AWS PrivateLink in the *AWS PrivateLink Guide*.

Considerations for AWS B2B Data Interchange

Before you set up an interface endpoint for AWS B2B Data Interchange, review Considerations in the *AWS PrivateLink Guide*.

AWS B2B Data Interchange supports making calls to all of its API actions through the interface endpoint.

VPC endpoint policies are not supported for AWS B2B Data Interchange. By default, full access to AWS B2B Data Interchange is allowed through the interface endpoint. Alternatively, you can associate a security group with the endpoint network interfaces to control traffic to AWS B2B Data Interchange through the interface endpoint.

Create an interface endpoint for AWS B2B Data Interchange

You can create an interface endpoint for AWS B2B Data Interchange using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see Create an interface endpoint in the *AWS PrivateLink Guide*.

Create an interface endpoint for AWS B2B Data Interchange using the following service name:

```
com.amazonaws.region.b2bi
```

If you enable private DNS for the interface endpoint, you can make dualstack API requests to AWS B2B Data Interchange using either Regional DNS name. For example, `b2bi.us-east-1.amazonaws.com` or `b2bi.us-east-1.api.aws`.

Create an endpoint policy for your interface endpoint

An endpoint policy is an IAM resource that you can attach to an interface endpoint. The default endpoint policy allows full access to AWS B2B Data Interchange through the interface endpoint. To control the access allowed to AWS B2B Data Interchange from your VPC, attach a custom endpoint policy to the interface endpoint.

An endpoint policy specifies the following information:

- The principals that can perform actions (AWS accounts, IAM users, and IAM roles).
- The actions that can be performed.
- The resources on which the actions can be performed.

For more information, see Control access to services using endpoint policies in the *AWS PrivateLink Guide*.

Example: VPC endpoint policy for AWS B2B Data Interchange actions

The following is an example of a custom endpoint policy. When you attach this policy to your interface endpoint, it grants access to the listed AWS B2B Data Interchange actions for all principals on all resources.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "servicename:action-1",
            "servicename:action-2",
            "servicename:action-3"
         ],
         "Resource":"*"
```

```
        }
    ]
}
```

Quotas for AWS B2B Data Interchange

Your AWS account has default quotas, formerly referred to as limits, for each AWS service. Unless otherwise noted, each quota is Region-specific. You can request increases for some quotas, and other quotas cannot be increased. To view the quotas for AWS B2B Data Interchange, open the Service Quotas console. In the navigation pane, choose **AWS services** and select **AWS B2B Data Interchange**. To request a quota increase, see Requesting a Quota Increase in the *Service Quotas User Guide*. If the quota is not yet available in Service Quotas, use the limit increase form.

AWS B2B Data Interchange is supported in the following regions: N. Virginia, Ohio, and Oregon.

Your AWS account has the following quotas related to AWS B2B Data Interchange.

Resource	Default
Maximum number of profiles per account	5
Maximum number of trading capabilities per account	100
Maximum number of transformers per account	500
Maximum number of partnerships per account	700
Maximum electronic data interchange (EDI) file size	150 MB
Maximum output JSON file size	512 MB
Maximum number of instruction/reference documents per trading capability	5
Maximum number of inbound transformation request per account	3 per second

For more information about supported AWS Regions, endpoints, and service quotas, see AWS B2B Data Interchange endpoints and quotas in the *Amazon Web Services General Reference*.

Supported X12 transaction sets

ANSI X12 defines and maintains transaction sets that establish the data content exchanged for specific business purposes. Transaction sets are identified by a numeric identifier and a name. For more details about X12 transaction sets, see X12 Transaction Sets. The following table lists the X12 transaction sets that AWS B2B Data Interchange currently supports.

> **Note**
>
> AWS B2B Data Interchange supports all transactions that are available for the 4010, 4030, 4050, 4060, and 5010 versions.

Transaction set	Description	Category	4010	4030	4050	4060	5010
100	Insurance Plan Description	Insurance	Yes	Yes	Yes	Yes	Yes
101	Name and Address Lists	Supply Chain	Yes	Yes	Yes	Yes	Yes
102	Associated Data	Communications and Controls	N/A	Yes	Yes	Yes	Yes
103	Abandoned Property Filings	Finance	N/A	Yes	Yes	Yes	Yes
104	Air Shipment	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
	Information						
105	Business Entity Filings	Finance	Yes	Yes	Yes	Yes	Yes
106	Motor Carrier Rate Proposal	Transportation	Yes	Yes	Yes	Yes	Yes
107	Request for Motor Carrier Rate Proposal	Transportation	Yes	Yes	Yes	Yes	Yes
108	Response to a Motor Carrier Rate Proposal	Transportation	Yes	Yes	Yes	Yes	Yes
109	Vessel Content Details	Transportation	Yes	Yes	Yes	Yes	Yes
110	Air Freight Details and Invoice	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
111	Individual Insurance Policy and Client Information	Insurance	N/A	Yes	Yes	Yes	Yes
112	Property Damage Report	Insurance	Yes	Yes	Yes	Yes	Yes
113	Election Campaign and Lobbyist Reporting	Finance	N/A	Yes	Yes	Yes	Yes
120	Vehicle Shipping Order	Transportation	Yes	Yes	Yes	Yes	Yes
121	Vehicle Service	Transportation	Yes	Yes	Yes	Yes	Yes
124	Vehicle Damage	Insurance	Yes	Yes	Yes	Yes	Yes
125	Multilevel Railcar Load Details	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
126	Vehicle Application Advice	Transportation	Yes	Yes	Yes	Yes	Yes
127	Vehicle Baying Order	Transportation	Yes	Yes	Yes	Yes	Yes
128	Dealer Information	Transportation	Yes	Yes	Yes	Yes	Yes
129	Vehicle Carrier Rate Update	Transportation	Yes	Yes	Yes	Yes	Yes
130	Student Educational Record (Transcript)	Finance	Yes	Yes	Yes	Yes	Yes
131	Student Educational Record (Transcript) Acknowledgment	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
132	Human Resource Information	Finance	N/A	N/A	Yes	Yes	Yes
133	Educational Institution Record	Finance	N/A	N/A	Yes	Yes	Yes
135	Student Aid Origination Record	Finance	Yes	Yes	Yes	Yes	Yes
138	Educational Testing and Prospect Request and Report	Finance	Yes	Yes	Yes	Yes	Yes
139	Student Loan Guarantee Result	Finance	Yes	Yes	Yes	Yes	Yes
140	Product Registration	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
141	Product Service Claim Response	Supply Chain	Yes	Yes	Yes	Yes	Yes
142	Product Service Claim	Supply Chain	Yes	Yes	Yes	Yes	Yes
143	Product Service Notification	Supply Chain	Yes	Yes	Yes	Yes	Yes
144	Student Loan Transfer and Status Verification	Finance	Yes	Yes	Yes	Yes	Yes
146	Request for Student Educational Record (Transcript)	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
147	Response to Request for Student Educational Record (Transcript)	Finance	Yes	Yes	Yes	Yes	Yes
148	Report of Injury, Illness or Incident	Insurance	Yes	Yes	Yes	Yes	Yes
149	Notice of Tax Adjustment or Assessment	Finance	Yes	Yes	Yes	Yes	Yes
150	Tax Rate Notification	Finance	Yes	Yes	Yes	Yes	Yes
151	Electronic Filing of Tax Return Data Acknowledgment	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
152	Statistical Government Information	Finance	Yes	Yes	Yes	Yes	Yes
153	Unemployment Insurance Tax Claim or Charge Information	Finance	Yes	Yes	Yes	Yes	Yes
154	Secured Interest Filing	Finance	Yes	Yes	Yes	Yes	Yes
155	Business Credit Report	Finance	Yes	Yes	Yes	Yes	Yes
157	Notice of Power of Attorney	Finance	Yes	Yes	Yes	Yes	Yes
158	Tax Jurisdiction Sourcing	Finance	N/A	N/A	N/A	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
159	Motion Picture Booking Confirmation	Supply Chain	Yes	Yes	Yes	Yes	Yes
160	Transportation Automatic Equipment Identification	Transportation	Yes	Yes	Yes	Yes	Yes
161	Train Sheet	Transportation	Yes	Yes	Yes	Yes	Yes
163	Transportation Appointment Schedule Information	Transportation	Yes	Yes	Yes	Yes	Yes
170	Revenue Receipts Statement	Supply Chain	Yes	Yes	Yes	Yes	Yes
175	Court and Law Enforcement Notice	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
176	Court Submission	Finance	Yes	Yes	Yes	Yes	Yes
179	Environmental Compliance Reporting	Finance	N/A	N/A	Yes	Yes	Yes
180	Return Merchandise Authorization and Notification	Supply Chain	Yes	Yes	Yes	Yes	Yes
185	Royalty Regulatory Report	Finance	Yes	Yes	Yes	Yes	Yes
186	Insurance Underwriting Requirements Reporting	Insurance	Yes	Yes	Yes	Yes	Yes
187	Premium Audit Request and Return	Insurance	N/A	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
188	Educational Course Inventory	Finance	Yes	Yes	Yes	Yes	Yes
189	Application for Admission to Educational Institutions	Finance	Yes	Yes	Yes	Yes	Yes
190	Student Enrollment Verification	Finance	Yes	Yes	Yes	Yes	Yes
191	Student Loan Pre-Claims and Claims	Finance	Yes	Yes	Yes	Yes	Yes
194	Grant or Assistance Application	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
195	Federal Communications Commission (FCC) License Application	Finance	Yes	Yes	Yes	Yes	Yes
196	Contractor Cost Data Reporting	Finance	Yes	Yes	Yes	Yes	Yes
197	Real Estate Title Evidence	Finance	Yes	Yes	Yes	Yes	Yes
198	Loan Verification Information	Finance	Yes	Yes	Yes	Yes	Yes
199	Real Estate Settlement Information	Finance	Yes	Yes	Yes	Yes	Yes
200	Mortgage Credit Report	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
201	Residential Loan Application	Finance	Yes	Yes	Yes	Yes	Yes
202	Secondary Mortgage Market Loan Delivery	Finance	Yes	Yes	Yes	Yes	Yes
203	Secondary Mortgage Market Investor Report	Finance	Yes	Yes	Yes	Yes	Yes
204	Motor Carrier Load Tender	Transportation	Yes	Yes	Yes	Yes	Yes
205	Mortgage Note	Finance	Yes	Yes	Yes	Yes	Yes
206	Real Estate Inspection	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
210	Motor Carrier Freight Details and Invoice	Transportation	Yes	Yes	Yes	Yes	Yes
211	Motor Carrier Bill of Lading	Transportation	Yes	Yes	Yes	Yes	Yes
212	Motor Carrier Delivery Trailer Manifest	Transportation	Yes	Yes	Yes	Yes	Yes
213	Motor Carrier Shipment Status Inquiry	Transportation	Yes	Yes	Yes	Yes	Yes
214	Transportation Carrier Shipment Status Message	Transportation	Yes	Yes	Yes	Yes	Yes
215	Motor Carrier Pickup Manifest	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
216	Motor Carrier Shipment Pickup Notification	Transportation	Yes	Yes	Yes	Yes	Yes
217	Motor Carrier Loading and Route Guide	Transportation	Yes	Yes	Yes	Yes	Yes
218	Motor Carrier Tariff Information	Transportation	Yes	Yes	N/A	N/A	N/A
219	Logistics Service Request	Transportation	Yes	Yes	Yes	Yes	Yes
220	Logistics Service Response	Transportation	Yes	Yes	Yes	Yes	Yes
222	Cartage Work Assignment	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
223	Consolidators Freight Bill and Invoice	Transportation	Yes	Yes	Yes	Yes	Yes
224	Motor Carrier Summary Freight Bill Manifest	Transportation	Yes	Yes	Yes	Yes	Yes
225	Response to a Cartage Work Assignment	Transportation	Yes	Yes	Yes	Yes	Yes
227	Trailer Usage Report	Transportation	N/A	Yes	Yes	Yes	Yes
228	Equipment Inspection Report	Transportation	N/A	N/A	N/A	N/A	Yes
240	Motor Carrier Package Status	Transportation	N/A	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
242	Data Status Tracking	Communications and Controls	Yes	Yes	Yes	Yes	Yes
244	Product Source Information	Supply Chain	Yes	Yes	Yes	Yes	Yes
245	Real Estate Tax Service Response	Finance	N/A	Yes	Yes	Yes	Yes
248	Account Assignment/Inquiry and Service/Status	Finance	Yes	Yes	Yes	Yes	Yes
249	Animal Toxicological Data	Supply Chain	Yes	Yes	Yes	Yes	Yes
250	Purchase Order Shipment Management Document	Transportation	Yes	Yes	Yes	Yes	Yes
251	Pricing Support	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
252	Insurance Producer Administration	Insurance	Yes	Yes	Yes	Yes	Yes
255	Underwriting Information Services	Insurance	Yes	Yes	Yes	Yes	Yes
256	Periodic Compensation	Insurance	Yes	Yes	Yes	Yes	Yes
259	Residential Mortgage Insurance Explanation of Benefits	Finance	N/A	N/A	N/A	Yes	Yes
260	Application for Mortgage Insurance Benefits	Finance	Yes	Yes	Yes	Yes	Yes
261	Real Estate Information Request	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
262	Real Estate Information Report	Finance	Yes	Yes	Yes	Yes	Yes
263	Residential Mortgage Insurance Application Response	Finance	Yes	Yes	Yes	Yes	Yes
264	Mortgage Loan Default Status	Finance	Yes	Yes	Yes	Yes	Yes
265	Real Estate Title Insurance Services Order	Finance	Yes	Yes	Yes	Yes	Yes
266	Mortgagor Property Record Change Notification	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
267	Individual Life, Annuity and Disability Application	Insurance	Yes	Yes	Yes	Yes	Yes
268	Annuity Activity	Insurance	Yes	Yes	Yes	Yes	Yes
269	Health Care Benefit Coordination Verification	Insurance	N/A	N/A	Yes	Yes	Yes
270	Eligibility, Coverage or Benefit Inquiry	Insurance	Yes	Yes	Yes	Yes	Yes
271	Eligibility, Coverage or Benefit Information	Insurance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
272	Property and Casualty Loss Notification	Insurance	Yes	Yes	Yes	Yes	Yes
273	Insurance /Annuity Application Status	Insurance	Yes	Yes	Yes	Yes	Yes
274	Healthcare Provider Information	Insurance	N/A	Yes	Yes	Yes	Yes
275	Patient Information	Insurance	Yes	Yes	Yes	Yes	Yes
276	Health Care Claim Status Request	Insurance	Yes	Yes	Yes	Yes	Yes
277	Health Care Information Status Notification	Insurance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
278	Health Care Services Review Information	Insurance	Yes	Yes	Yes	Yes	Yes
280	Voter Registration Information	Finance	Yes	Yes	Yes	Yes	Yes
283	Tax or Fee Exemption Certification	Finance	N/A	Yes	Yes	Yes	Yes
284	Commercial Vehicle Safety Reports	Transportation	N/A	Yes	Yes	Yes	Yes
285	Commercial Vehicle Safety and Credentials Information Exchange	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
286	Commercial Vehicle Credentials	Transportation	Yes	Yes	Yes	Yes	Yes
288	Wage Determination	Finance	Yes	Yes	Yes	Yes	Yes
290	Cooperative Advertising Agreements	Supply Chain	Yes	Yes	Yes	Yes	Yes
300	Reservation (Booking Request) (Ocean)	Transportation	Yes	Yes	Yes	Yes	Yes
301	Confirmation (Ocean)	Transportation	Yes	Yes	Yes	Yes	Yes
303	Booking Cancellation (Ocean)	Transportation	Yes	Yes	Yes	Yes	Yes
304	Shipping Instructions	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
309	Customs Manifest	Transportation	Yes	Yes	Yes	Yes	Yes
310	Freight Receipt and Invoice (Ocean)	Transportation	Yes	Yes	Yes	Yes	Yes
311	Canada Customs Information	Transportation	Yes	Yes	Yes	Yes	Yes
312	Arrival Notice (Ocean)	Transportation	Yes	Yes	Yes	Yes	Yes
313	Shipment Status Inquiry (Ocean)	Transportation	Yes	Yes	Yes	Yes	Yes
315	Status Details (Ocean)	Transportation	Yes	Yes	Yes	Yes	Yes
317	Delivery/ Pickup Order	Transportation	Yes	Yes	Yes	Yes	Yes
319	Terminal Information	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
322	Terminal Operations and Intermodal Ramp Activity	Transportation	Yes	Yes	Yes	Yes	Yes
323	Vessel Schedule and Itinerary (Ocean)	Transportation	Yes	Yes	Yes	Yes	Yes
324	Vessel Stow Plan (Ocean)	Transportation	Yes	Yes	Yes	Yes	Yes
325	Consolidation of Goods In Container	Transportation	Yes	Yes	Yes	Yes	Yes
326	Consignment Summary List	Transportation	Yes	Yes	Yes	Yes	Yes
350	Customs Status Information	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
352	U.S. Customs Carrier General Order Status	Transportation	Yes	Yes	Yes	Yes	Yes
353	Customs Events Advisory Details	Transportation	Yes	Yes	Yes	Yes	Yes
354	U.S. Customs Automated Manifest Archive Status	Transportation	Yes	Yes	Yes	Yes	Yes
355	U.S. Customs Acceptance/Rejection	Transportation	Yes	Yes	Yes	Yes	Yes
356	U.S. Customs Permit to Transfer Request	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
357	U.S. Customs In-Bond Information	Transportation	Yes	Yes	Yes	Yes	Yes
358	Customs Consist Information	Transportation	Yes	Yes	Yes	Yes	Yes
361	Carrier Interchange Agreement (Ocean)	Transportation	Yes	Yes	Yes	Yes	Yes
362	Cargo Insurance Advice of Shipment	Insurance	Yes	Yes	Yes	Yes	Yes
404	Rail Carrier Shipment Information	Transportation	Yes	Yes	Yes	Yes	Yes
410	Rail Carrier Freight Details and Invoice	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
412	Trailer or Container Repair Billing	Transportation	N/A	Yes	Yes	Yes	Yes
414	Rail Carhire Settlements	Transportation	Yes	Yes	Yes	Yes	Yes
417	Rail Carrier Waybill Interchange	Transportation	Yes	Yes	Yes	Yes	Yes
418	Rail Advance Interchange Consist	Transportation	Yes	Yes	Yes	Yes	Yes
419	Advance Car Disposition	Transportation	Yes	Yes	Yes	Yes	Yes
420	Car Handling Information	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
421	Estimated Time of Arrival and Car Scheduling	Transportation	Yes	Yes	Yes	Yes	Yes
422	Equipment Order	Transportation	Yes	Yes	Yes	Yes	Yes
423	Rail Industrial Switch List	Transportation	Yes	Yes	Yes	Yes	Yes
424	Rail Carrier Services Settlement	Transportation	N/A	N/A	Yes	Yes	Yes
425	Rail Waybill Request	Transportation	Yes	Yes	Yes	Yes	Yes
426	Rail Revenue Waybill	Transportation	Yes	Yes	Yes	Yes	Yes
429	Railroad Retirement Activity	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
431	Railroad Station Master File	Transportation	Yes	Yes	Yes	Yes	Yes
432	Rail Deprescription	Transportation	Yes	Yes	Yes	Yes	Yes
433	Railroad Reciprocal Switch File	Transportation	Yes	Yes	Yes	Yes	Yes
434	Railroad Mark Register Update Activity	Transportation	Yes	Yes	Yes	Yes	Yes
435	Standard Transportation Commodity Code Master	Transportation	Yes	Yes	Yes	Yes	Yes
436	Locomotive Information	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
437	Railroad Junctions and Interchanges Activity	Transportation	Yes	Yes	Yes	Yes	Yes
440	Shipment Weights	Transportation	Yes	Yes	Yes	Yes	Yes
451	Railroad Event Report	Transportation	Yes	Yes	Yes	Yes	Yes
452	Railroad Problem Log Inquiry or Advice	Transportation	Yes	Yes	Yes	Yes	Yes
453	Railroad Service Commitment Advice	Transportation	Yes	Yes	Yes	Yes	Yes
455	Railroad Parameter Trace Registration	Transportation	Yes	Yes	Yes	Yes	Yes
456	Railroad Equipment Inquiry or Advice	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
460	Railroad Price Distribution Requestor Response	Transportation	Yes	Yes	Yes	Yes	Yes
463	Rail Rate Reply	Transportation	Yes	Yes	Yes	Yes	Yes
466	Rate Request	Transportation	Yes	Yes	Yes	Yes	Yes
468	Rate Docket Journal Log	Transportation	Yes	Yes	Yes	Yes	Yes
470	Railroad Clearance	Transportation	Yes	Yes	Yes	Yes	Yes
475	Rail Route File Maintenance	Transportation	Yes	Yes	Yes	Yes	Yes
485	Ratemaking Action	Transportation	Yes	Yes	Yes	Yes	Yes
486	Rate Docket Expiration	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
490	Rate Group Definition	Transportation	Yes	Yes	Yes	Yes	Yes
492	Miscellaneous Rates	Transportation	Yes	Yes	Yes	Yes	Yes
494	Rail Scale Rates	Transportation	Yes	Yes	Yes	Yes	Yes
500	Medical Event Reporting	Insurance	Yes	Yes	Yes	Yes	Yes
501	Vendor Performance Review	Supply Chain	Yes	Yes	Yes	Yes	Yes
503	Pricing History	Supply Chain	Yes	Yes	Yes	Yes	Yes
504	Clauses and Provisions	Supply Chain	Yes	Yes	Yes	Yes	Yes
511	Requisition	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
517	Material Obligation Validation	Supply Chain	Yes	Yes	Yes	Yes	Yes
521	Income or Asset Offset	Finance	Yes	Yes	Yes	Yes	Yes
527	Material Due-In and Receipt	Finance	Yes	Yes	Yes	Yes	Yes
536	Logistics Reassignment	Supply Chain	Yes	Yes	Yes	Yes	Yes
540	Notice of Employment Status	Finance	Yes	Yes	Yes	Yes	Yes
561	Contract Abstract	Supply Chain	Yes	Yes	Yes	Yes	Yes
567	Contract Completion Status	Supply Chain	Yes	Yes	Yes	Yes	Yes
568	Contract Payment Management Report	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
601	U.S. Customs Export Shipment Information	Transportation	Yes	Yes	Yes	Yes	Yes
602	Transportation Services Tender	Transportation	Yes	Yes	Yes	Yes	Yes
620	Excavation Communication	Supply Chain	Yes	Yes	Yes	Yes	Yes
625	Well Information	Supply Chain	Yes	Yes	Yes	Yes	Yes
650	Maintenance Service Order	Supply Chain	Yes	Yes	Yes	Yes	Yes
715	Intermodal Group Loading Plan	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
753	Request for Routing Instructions	Supply Chain	N/A	Yes	Yes	Yes	Yes
754	Routing Instructions	Supply Chain	N/A	Yes	Yes	Yes	Yes
805	Contract Pricing Proposal	Supply Chain	Yes	Yes	Yes	Yes	Yes
806	Project Schedule Reporting	Supply Chain	Yes	Yes	Yes	Yes	Yes
810	Invoice	Finance	Yes	Yes	Yes	Yes	Yes
811	Consolidated Service Invoice/Statement	Finance	Yes	Yes	Yes	Yes	Yes
812	Credit/ Debit Adjustment	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
813	Electronic Filing of Tax Return Data	Finance	Yes	Yes	Yes	Yes	Yes
814	General Request, Response or Confirmation	Finance	Yes	Yes	Yes	Yes	Yes
815	Cryptographic Service Message	Communications and Controls	Yes	Yes	Yes	Yes	Yes
816	Organizational Relationships	Supply Chain	Yes	Yes	Yes	Yes	Yes
818	Commission Sales Report	Supply Chain	Yes	Yes	Yes	Yes	Yes
819	Joint Interest Billing and Operating Expense Statement	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
820	Payment Order/ Remittance Advice	Finance	Yes	Yes	Yes	Yes	Yes
821	Financial Information Reporting	Finance	Yes	Yes	Yes	Yes	Yes
822	Account Analysis	Finance	Yes	Yes	Yes	Yes	Yes
823	Lockbox	Finance	Yes	Yes	Yes	Yes	Yes
824	Application Advice	Finance	Yes	Yes	Yes	Yes	Yes
826	Tax Information Exchange	Finance	Yes	Yes	Yes	Yes	Yes
827	Financial Return Notice	Finance	Yes	Yes	Yes	Yes	Yes
828	Debit Authorization	Finance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
829	Payment Cancellation Request	Finance	Yes	Yes	Yes	Yes	Yes
830	Planning Schedule with Release Capability	Supply Chain	Yes	Yes	Yes	Yes	Yes
831	Application Control Totals	Finance	Yes	Yes	Yes	Yes	Yes
832	Price/ Sales Catalog	Supply Chain	Yes	Yes	Yes	Yes	Yes
833	Mortgage Credit Report Order	Finance	Yes	Yes	Yes	Yes	Yes
834	Benefit Enrollment and Maintenance	Insurance	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
835	Health Care Claim Payment/ Advice	Insurance	Yes	Yes	Yes	Yes	Yes
836	Procurement Notices	Supply Chain	Yes	Yes	Yes	Yes	Yes
837	Health Care Claim	Insurance	Yes	Yes	Yes	Yes	Yes
838	Trading Partner Profile	Supply Chain	Yes	Yes	Yes	Yes	Yes
839	Project Cost Reporting	Supply Chain	Yes	Yes	Yes	Yes	Yes
840	Request for Quotation	Supply Chain	Yes	Yes	Yes	Yes	Yes
841	Specifications/ Technical Information	Supply Chain	Yes	Yes	Yes	Yes	Yes
842	Nonconformance Report	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
843	Response to Request for Quotation	Supply Chain	Yes	Yes	Yes	Yes	Yes
844	Product Transfer Account Adjustment	Finance	Yes	Yes	Yes	Yes	Yes
845	Price Authorization Acknowledgment/ Status	Supply Chain	Yes	Yes	Yes	Yes	Yes
846	Inventory Inquiry/Advice	Supply Chain	Yes	Yes	Yes	Yes	Yes
847	Material Claim	Supply Chain	Yes	Yes	Yes	Yes	Yes
848	Material Safety Data Sheet	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
849	Response to Product Transfer Account Adjustment	Finance	Yes	Yes	Yes	Yes	Yes
850	Purchase Order	Supply Chain	Yes	Yes	Yes	Yes	Yes
851	Asset Schedule	Supply Chain	Yes	Yes	Yes	Yes	Yes
852	Product Activity Data	Supply Chain	Yes	Yes	Yes	Yes	Yes
853	Routing and Carrier Instruction	Supply Chain	Yes	Yes	Yes	Yes	Yes
854	Shipment Delivery Discrepancy Information	Transportation	Yes	Yes	Yes	Yes	Yes
855	Purchase Order Acknowledgment	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
856	Ship Notice/ Manifest	Supply Chain	Yes	Yes	Yes	Yes	Yes
857	Shipment and Billing Notice	Supply Chain	Yes	Yes	Yes	Yes	Yes
858	Shipment Information	Transportation	Yes	Yes	Yes	Yes	Yes
859	Freight Invoice	Transportation	Yes	Yes	Yes	Yes	Yes
860	Purchase Order Change Request - Buyer Initiated	Supply Chain	Yes	Yes	Yes	Yes	Yes
861	Receiving Advice/ Acceptance Certificate	Supply Chain	Yes	Yes	Yes	Yes	Yes
862	Shipping Schedule	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
863	Report of Test Results	Supply Chain	Yes	Yes	Yes	Yes	Yes
864	Text Message	Communications and Controls	Yes	Yes	Yes	Yes	Yes
865	Purchase Order Change Acknowledgment/ Request - Seller Initiated	Supply Chain	Yes	Yes	Yes	Yes	Yes
866	Production Sequence	Supply Chain	Yes	Yes	Yes	Yes	Yes
867	Product Transfer and Resale Report	Supply Chain	Yes	Yes	Yes	Yes	Yes
868	Electronic Form Structure	Communications and Controls	Yes	Yes	Yes	Yes	Yes
869	Order Status Inquiry	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
870	Order Status Report	Supply Chain	Yes	Yes	Yes	Yes	Yes
871	Componen Parts Content	Supply Chain	Yes	Yes	Yes	Yes	Yes
872	Residential Mortgage Insurance Application	Finance	Yes	Yes	Yes	Yes	Yes
873	Commodity Movement Services	Supply Chain	N/A	Yes	Yes	Yes	Yes
874	Commodity Movement Services Response	Supply Chain	N/A	N/A	Yes	Yes	Yes
875	Grocery Products Purchase Order	Supply Chain	Yes	Yes	Yes	Yes	Yes
876	Grocery Products Purchase Order Change	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
877	Manufacturer Coupon Family Code Structure	Supply Chain	Yes	Yes	Yes	Yes	Yes
878	Product Authorization/ De-authorization	Supply Chain	Yes	Yes	Yes	Yes	Yes
879	Price Information	Supply Chain	Yes	Yes	Yes	Yes	Yes
880	Grocery Products Invoice	Finance	Yes	Yes	Yes	Yes	Yes
881	Manufacturer Coupon Redemption Detail	Supply Chain	Yes	Yes	Yes	Yes	Yes
882	Direct Store Delivery Summary Information	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
883	Market Development Fund Allocation	Supply Chain	Yes	Yes	Yes	Yes	Yes
884	Market Development Fund Settlement	Supply Chain	Yes	Yes	Yes	Yes	Yes
885	Retail Account Characteristics	Supply Chain	Yes	Yes	Yes	Yes	Yes
886	Customer Call Reporting	Supply Chain	Yes	Yes	Yes	Yes	Yes
887	Coupon Notification	Supply Chain	Yes	Yes	Yes	Yes	Yes
888	Item Maintenance	Supply Chain	Yes	Yes	Yes	Yes	Yes
889	Promotion Announcement	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
891	Deduction Research Report	Supply Chain	Yes	Yes	Yes	Yes	Yes
893	Item Information Request	Supply Chain	Yes	Yes	Yes	Yes	Yes
894	Delivery/ Return Base Record	Supply Chain	Yes	Yes	Yes	Yes	Yes
895	Delivery/ Return Acknowledgment or Adjustment	Supply Chain	Yes	Yes	Yes	Yes	Yes
896	Product Dimension Maintenance	Supply Chain	Yes	Yes	Yes	Yes	Yes
920	Loss or Damage Claim - General Commodities	Transportation	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
924	Loss or Damage Claim - Motor Vehicle	Transportation	Yes	Yes	Yes	Yes	Yes
925	Claim Tracer	Transportation	Yes	Yes	Yes	Yes	Yes
926	Claim Status Report and Tracer Reply	Transportation	Yes	Yes	Yes	Yes	Yes
928	Automotive Inspection Detail	Transportation	Yes	Yes	Yes	Yes	Yes
940	Warehouse Shipping Order	Supply Chain	Yes	Yes	Yes	Yes	Yes
943	Warehouse Stock Transfer Shipment Advice	Supply Chain	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
944	Warehouse Stock Transfer Receipt Advice	Supply Chain	Yes	Yes	Yes	Yes	Yes
945	Warehouse Shipping Advice	Supply Chain	Yes	Yes	Yes	Yes	Yes
947	Warehouse Inventory Adjustment Advice	Supply Chain	Yes	Yes	Yes	Yes	Yes
980	Functional Group Totals	Transportation	Yes	Yes	Yes	Yes	Yes
990	Response to a Load Tender	Transportation	Yes	Yes	Yes	Yes	Yes
993	Secured Receipt or Acknowledgment	Communications and Controls	N/A	Yes	Yes	Yes	Yes
996	File Transfer	Communications and Controls	Yes	Yes	Yes	Yes	Yes

Transaction set	Description	Category	4010	4030	4050	4060	5010
997	Functional Acknowledgment	Communications and Controls	Yes	Yes	Yes	Yes	Yes
998	Set Cancellation	Transportation	Yes	Yes	Yes	Yes	Yes
999	Implementation Acknowledgment	Communications and Controls	N/A	N/A	N/A	N/A	Yes

HIPAA Transaction sets

AWS B2B Data Interchange is a Health Insurance Portability and Accountability Act of 1996 (HIPAA) eligible service and supports the following X12 version 5010 HIPAA transaction sets.

> **Note**
>
> For these transaction sets, the X12 version is `VERSION_5010_HIPAA`.

Transaction Set	Description	Supported?
270 X279	Eligibility Benefit Inquiry	Yes
271 X279	Eligibility Benefit Response	Yes
275 X210	Unsolicited Claim Attachments (from practice to payer)	*No*

Transaction Set	Description	Supported?
275 X211	Unsolicited Claim Attachments (from practice to clearinghouse to payer)	*No*
276 X212	Claim Status Request	Yes
277 X212	Claim Status Request Response	Yes
277 X214	Claim Acknowledgement	Yes
277 X364	Data Reporting Acknowledgement	*No*
278 X217	Services Review Information Review/Response	Yes
820 X218	Payroll Deducted and Other Group Premium Payment For Insurance Products Examples	Yes
820 X306	Health Insurance Exchange Related Payments	Yes
824 X186	Application Advice	*No*
834 X220	Benefit Enrollment and Maintenance	Yes
834 X307	Health Insurance Exchange: Enrollment	*No*
834 X318	Benefit Enrollment and Maintenance, Electronic Remittance Advice (ERA)	*No*

Transaction Set	Description	Supported?
835 X221	Claim Payment/Advice, Electronic Remittance Advice (ERA)	Yes
837 X222	Claim, Professional and vision claims	Yes
837 X223	Claim, Institutional claims	Yes
837 X224	Claim, Dental claims	Yes
837 X291	Professional Pre-Deter mination	*No*
837 X292	Institutional Pre-Deter mination	*No*
837 X298	Post-adjudicated Claims Data Reporting, Professional	*No*
999 X231	Implementation Acknowled gement	*No*

Document history for the AWS B2B Data Interchange User Guide

The following table describes the documentation releases for AWS B2B Data Interchange.

Change	Description	Date
Add the ability to use generative AI-assisted EDI mapping.	The AWS B2B Data Interchange generative AI-assisted EDI mapping capabilities expedite the process of writing and testing bidirectional mapping code. for details, see Generative AI-assisted EDI mapping.	November 15, 2024
Add the ability to generate X12 EDI documents	Add the ability to generate X12 EDI documents for purposes of sending transactional data to your partners. For details see Outbound EDI.	October 3, 2024
Add the ability to return acknowledgements	AWS B2B Data Interchange now automatically creates return acknowledgements for all inbound EDI files. For details, see EDI acknowledgements	April 30, 2024
Integrate with Amazon EventBridge	AWS B2B Data Interchange now automatically publishes event to Amazon EventBridge for transformation operations. For details, see Managing AWS B2B Data Interchan	March 22, 2024

Change	Description	Date
	ge events using Amazon EventBridge.	
First version of AWS B2B Data Interchange released	This initial release includes the ability to set up and exchange electronic data interchange (EDI) transactions in AWS B2B Data Interchange	November 27, 2023