aws

User Guide

AWS B2B Data Interchange

AWS B2B Data Interchange: User Guide

Table of Contents

What is AWS B2B Data Interchange (B2Bi)?

AWS B2B Data Interchange automates the transformation of Electronic Interchange Data (EDI) documents into JSON and XML formats to simplify your downstream data integrations. Businesses use EDI documents to exchange transactional data with trading partners, such as suppliers and end customers, using standardized formats such as X12, EDIFACT, or HL7v2. Currently, AWS B2B Data Interchange only supports X12 to JSON or XML conversions.

Currently, customers use commercial solutions hosted on-premises that require manual onboarding of trading partners, resulting in larger time to onboard, a high number of transaction errors, and missed SLAs. These problems result in negative impact to their business relationships with their trading partners. With B2Bi, customers can easily onboard and manage their trading partners and automate the transformation of EDI documents into common data representations such as JSON and XML using a low-code interface. This reduces the time, complexity, and cost associated with preparing and integrating EDI data into their business applications and purpose-built data lakes. As a result, customers can now focus on using their transactional data to drive business insights using the AWS suite of analytics, artificial intelligence, and machine learning services

Topics

How to get started with B2Bi

If you are a first-time user of B2Bi, we recommend that you begin by reading Getting started with AWS B2B Data Interchange (B2Bi).

Accessing B2Bi

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 B2Bi and AWS resources. If you've signed up for an AWS account, you can access the B2Bi console by signing into the AWS Management Console and choosing B2Bi 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 B2Bi) 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 B2Bi is designed to be programming language-neutral, using AWS supported interfaces to store and retrieve objects. You can access B2Bi and AWS programmatically by using the AWS B2B Data Interchange REST API. The REST API is an HTTP interface to B2Bi.

To use the REST API, you can use any toolkit that supports HTTP. You can even use a browser to fetch objects, as long as they are anonymously readable. The REST API uses standard HTTP headers and status codes, so that standard browsers and toolkits work as expected. In some areas, we have added functionality to HTTP (for example, we added headers to support access control). In these cases, we have done our best to add the new functionality in a way that matches the style of standard HTTP usage.

AWS provides software development kits (SDKs) that consist of libraries and sample code for various programming languages and platforms (Java, Python, Ruby, .NET, iOS, Android, and so on). The AWS SDKs provide a convenient way to create programmatic access to AWS B2B Data Interchange and AWS. B2Bi is a REST service. You can send requests to B2Bi using the AWS SDK libraries, which wrap the underlying AWS B2B Data Interchange REST API and simplify your programming tasks. For example, the SDKs take care of tasks such as calculating signatures, cryptographically signing requests, managing errors, and retrying requests automatically. For information about the AWS SDKs, including how to download and install them, see Tools for AWS.

AWS B2B Data Interchange (B2Bi) concepts

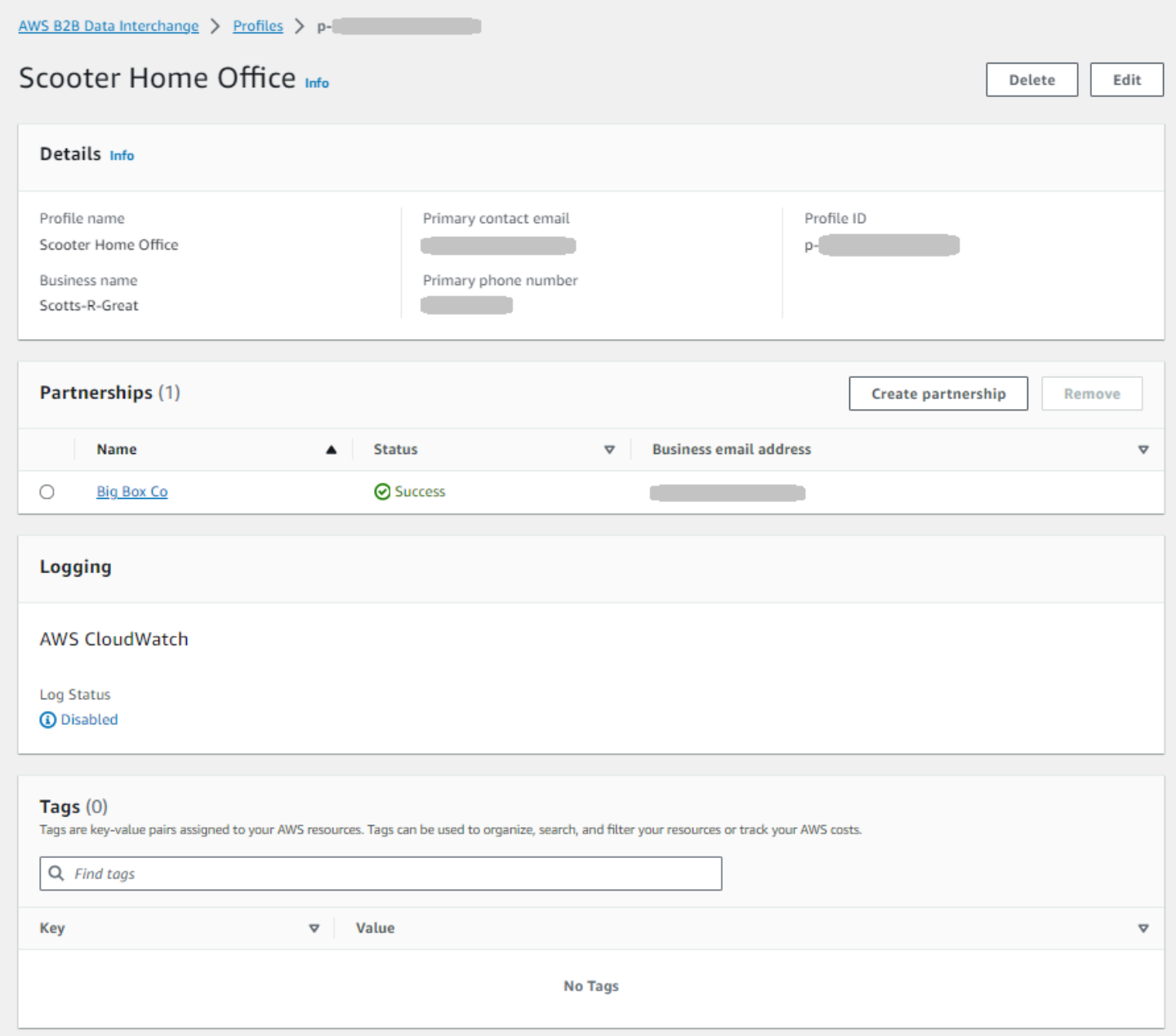
This topic outlines the features that are used in AWS B2B Data Interchange: profiles, trading capabilities, partnerships, and transformers.

Topics

Profiles

Profiles store contact information and details about your business. The information stored in your profiles is shared with your trading partners. To create a profile, add information about your company, including your business name, contact email, phone number, and a unique name to easily identify this profile. The information stored in your profiles is shared with your trading partners. You can also enable logging to monitor transformation activities or tags to organize, search, and filter your profiles.

```
// Profile
{
    profileId: "p-1234567890",
    accountId: "123456789012",
    name: "Sample Shipping Company LLC.",
    email: "customer@mailsvc.com",
    address: {...},
    websiteUrl: "www.customerpage.org",
    phone: "1234567890"
    contact: "Mary Major",
    logoRef: "https://EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com/photos/logo.jpg",
    createdAt: "2022-11-18T13:45:30",
    modifiedAt: "2022-11-18T15:45:30",
    status: "ACTIVE" // to support soft deletes
}
```

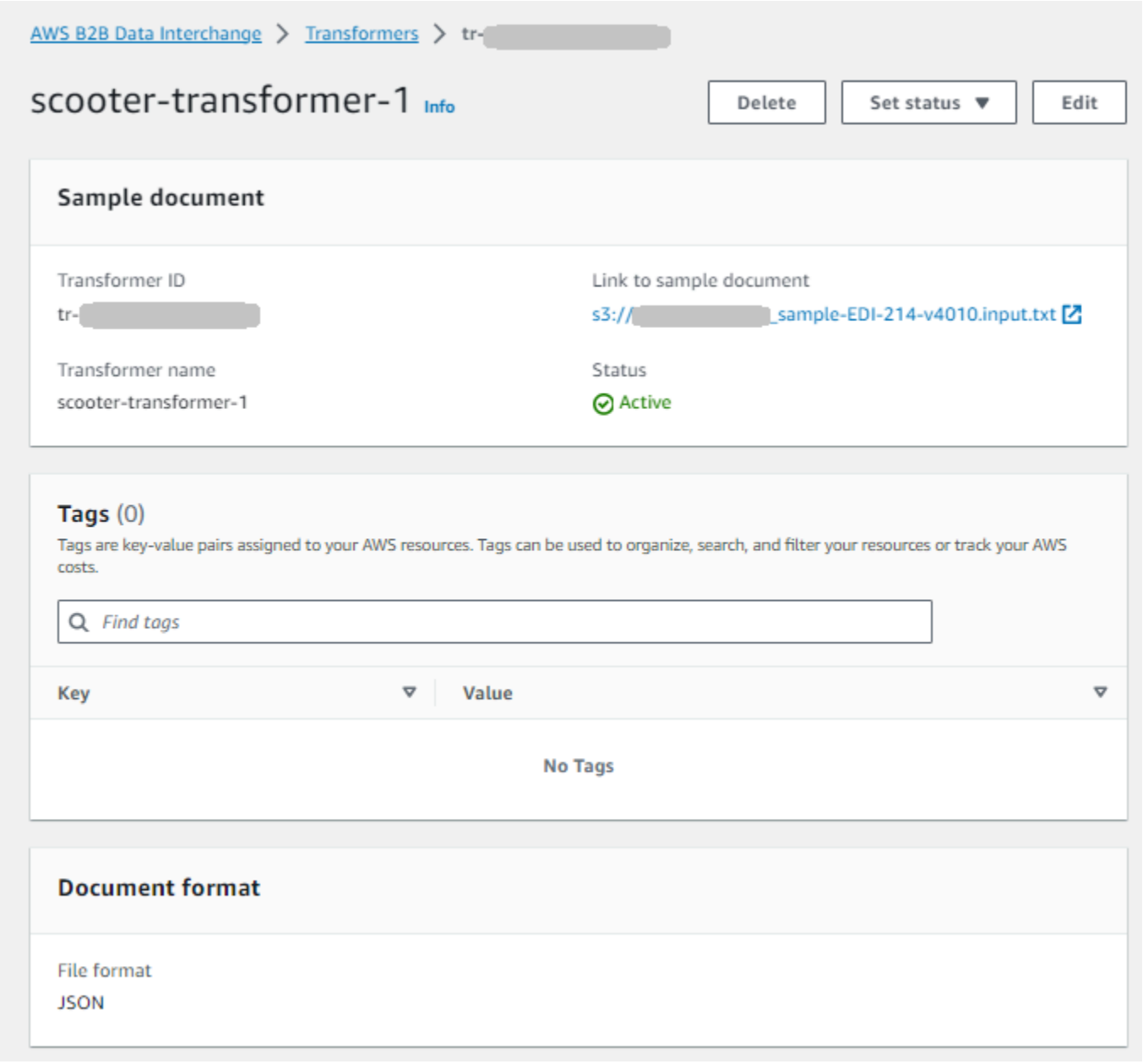


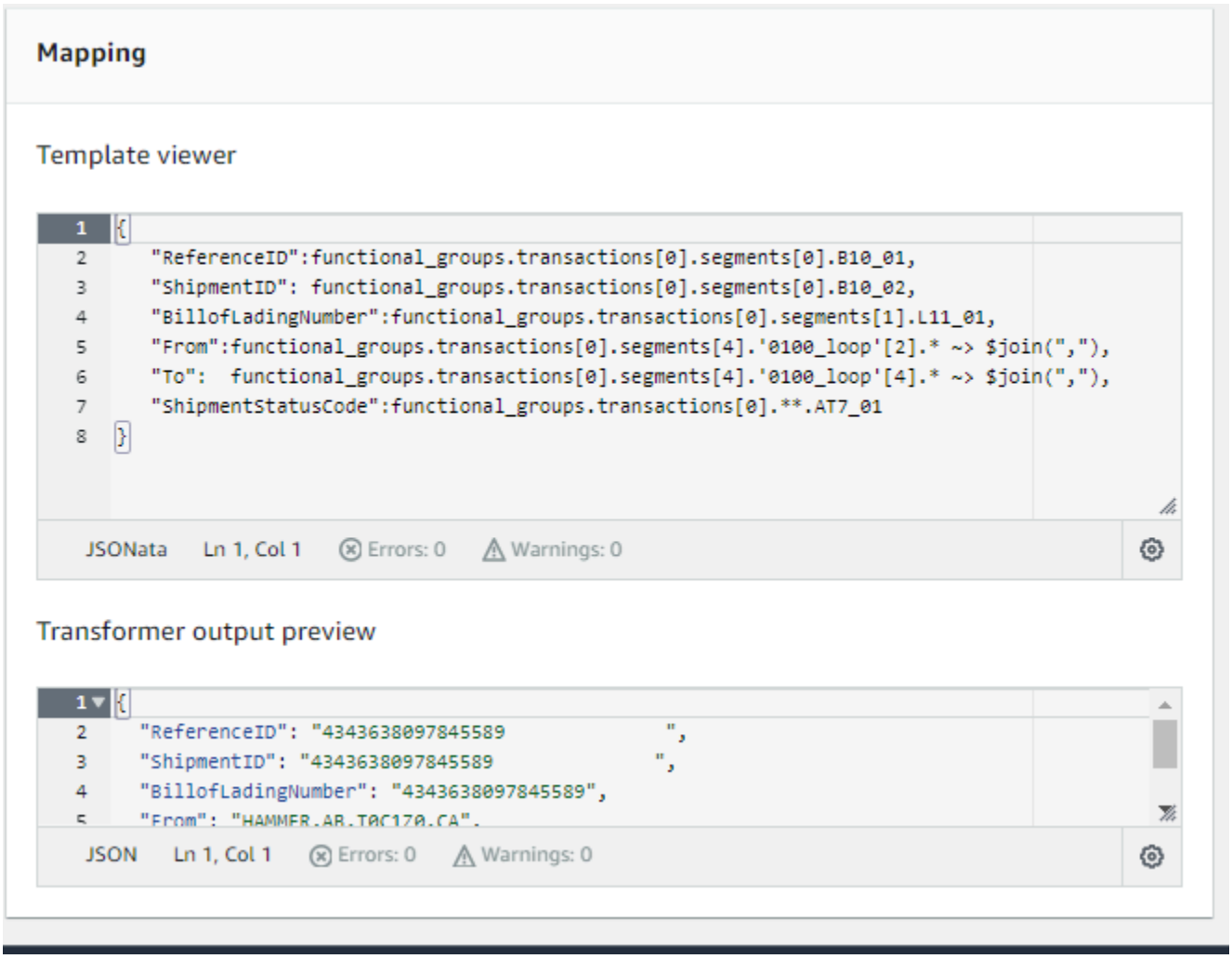
Transformers

Transformers are the heart of B2Bi. A *transformer* describes how to process the incoming EDI documents and extract the necessary information to the output file. To create a transformer, specify the incoming EDI document number and version that will be transformed. Then, reference a sample EDI document if you can provide one. The sample document is used as a template for the transformation. Finally, if you've provided a sample document, you can use the mapping editor to map the default, serviced-defined output to a custom output using JSONata for JSON or XSLT for XML.

Note

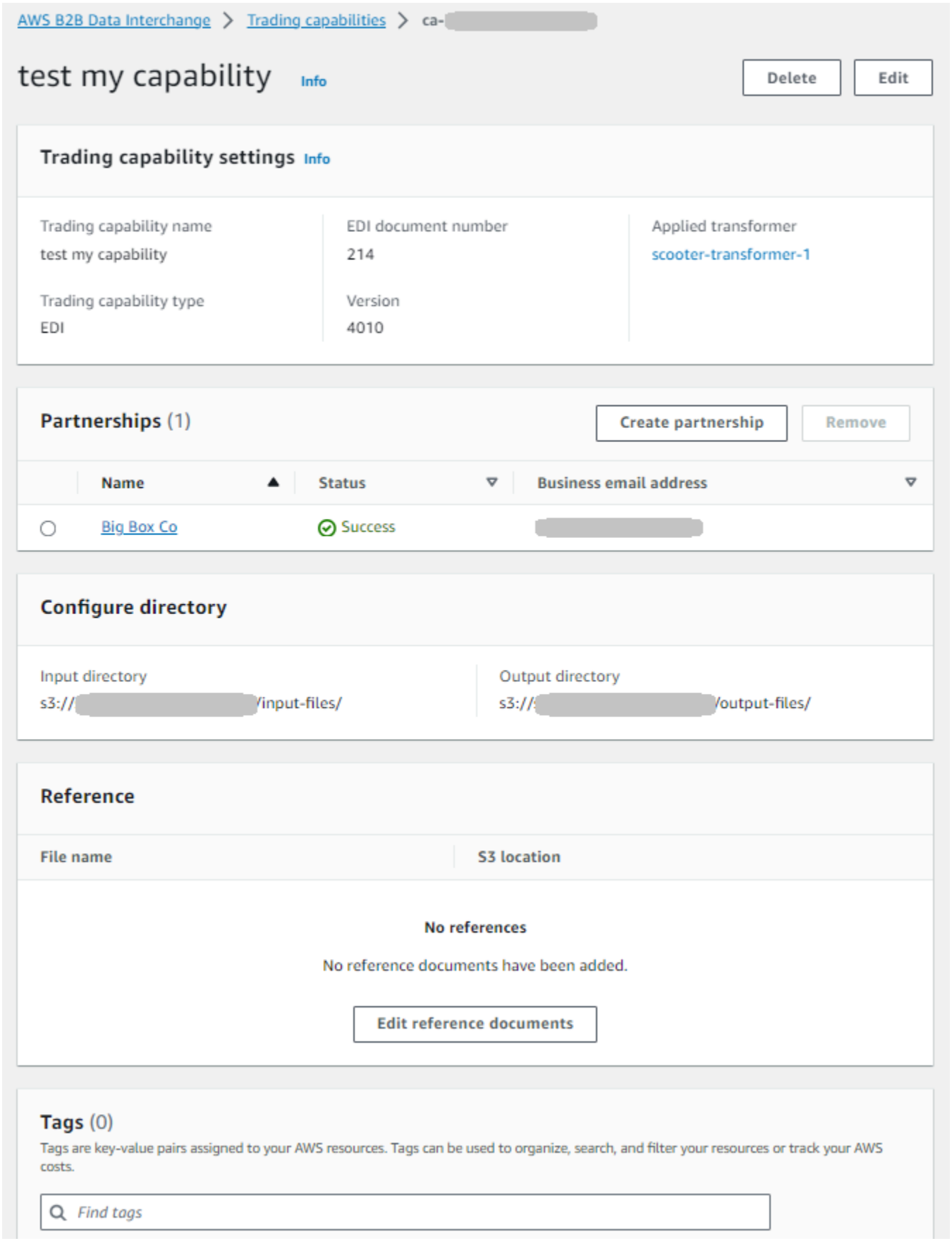
- Transformers are created with a status of **Inactive**. To use a transformer in a capability, you must change its status to **Active**.
- You can only delete transformers if they are not used in any capabilities.





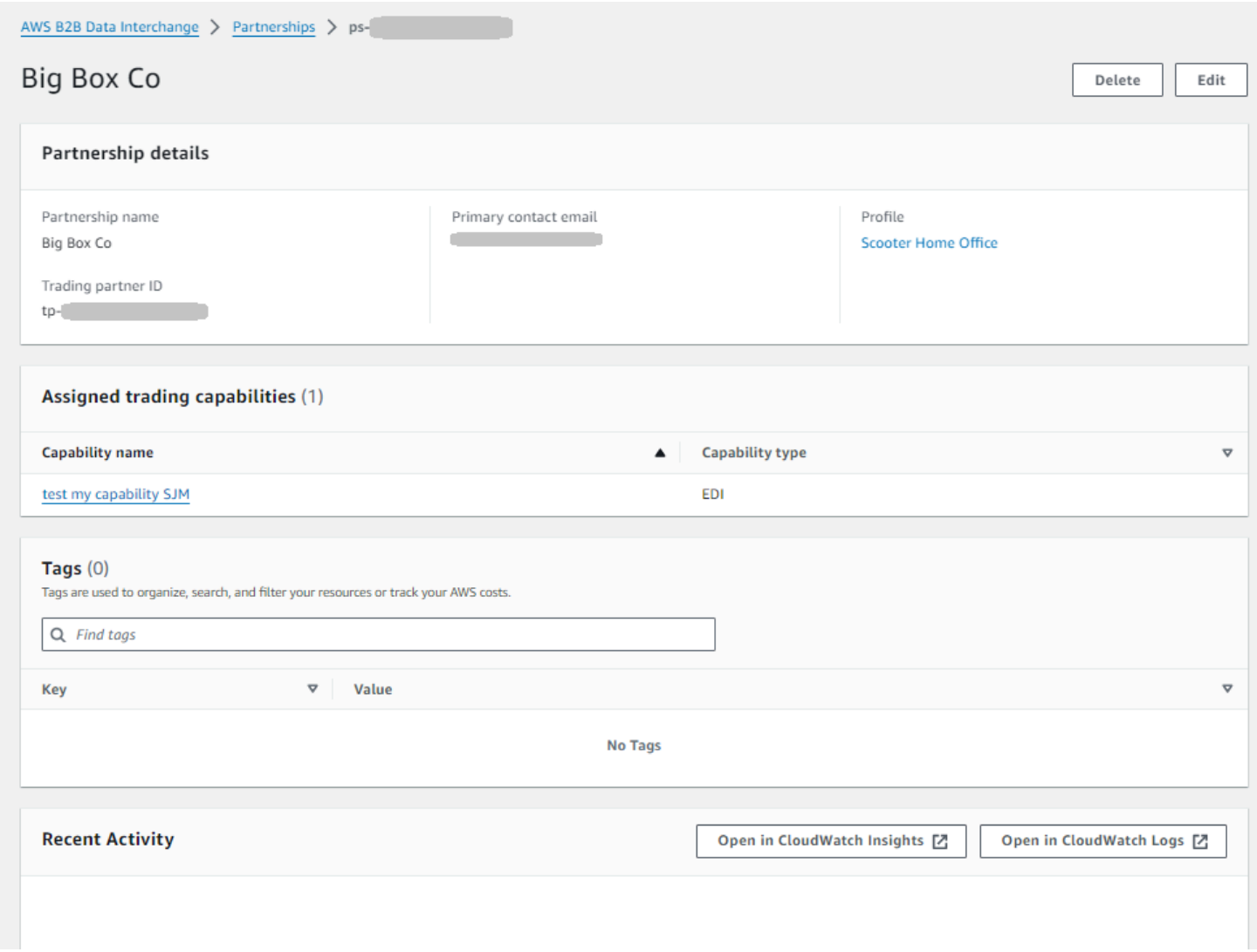
Capabilities

A *trading capability* contains the information required to transform incoming EDI documents into JSON or XML outputs. To create a trading capability, add details about the incoming EDI document number and version, choose the transformer to be used to translate the incoming documents, and specify the input and output directories used to source and store documents. You can optionally include instructions and sample documents that can be accessed by your trading partners so they can align their EDI document formats with your transformation processes.


AWS B2B Data Interchange > Trading capabilities > ca-
test my capability Info
Delete
Edit
Trading capability settings Info
Trading capability name
test my capability
Trading capability type
EDI
EDI document number
214
Version
4010
Applied transformer
scooter-transformer-1
Partnerships (1)
Create partnership
Remove
Name
Status
Business email address
Big Box Co
Success
Configure directory
Input directory
s3://
/input-files/
Output directory
s3://
/output-files/
Reference
File name
S3 location
No references
No reference documents have been added.
Edit reference documents
Tags (0)
Tags are key-value pairs assigned to your AWS resources. Tags can be used to organize, search, and filter your resources or track your AWS costs.
Find tags

Partnerships

A *partnership* represents the connection between you and your trading partner. It ties together a profile and one or more trading capabilities. 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 use for this partnership



Getting started with AWS B2B Data Interchange (B2Bi)

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.

To build and run your EDI-based workflows on AWS B2B Data Interchange, you need to create a profile, transformer, trading capability, and partnership. Follow the instructions below or use the quick setup guide to easily create each of these resources, which enable you to connect with your trading partners and start transforming EDI data into JSON and XML to simplify your downstream integrations.

Topics

Setting up

Before you can use B2Bi, you must sign up for an AWS account.

Topics

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. B2Bi requires buckets for storing input, output, and instruction documents. For details, see Getting started with Amazon S3.

- Maximum EDI (electronic data interchange) file size is 5 MB.
- The Amazon S3 bucket must be in the same AWS account as the B2Bi user.
- The Amazon S3 bucket must be in the same region as the B2Bi user.

Quick setup

This section details a quick setup. From the B2Bi landing page (https://console.aws.amazon.com/b2bi/), you can choose **Quick setup**. Additionally, we provide a self-contained, AWS CloudFormation template to quickly create a B2Bi configuration. For details, see Configure AWS B2B Data Interchange using a AWS CloudFormation template.

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 Step 1 Create a profile, then select **Next**.
2. The **Create transformer** screen appears. Fill in your details as described in Step 2 Create a transformer, then select **Next**.
3. The **Create trading capability** screen appears. Fill in your details as described in Step 3 Create a trading capability, 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 Step 4 Create a partnership, 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, capability and partnership.

Step 1 Create a profile

A *profile* is the mechanism used to create the concept of a private network. 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 characteristics for the customer, not the trading partner.

- **Logging**: This section describes the logging configuration. You can also opt out of logging (not recommended).

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.

Step 2 Create a transformer

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

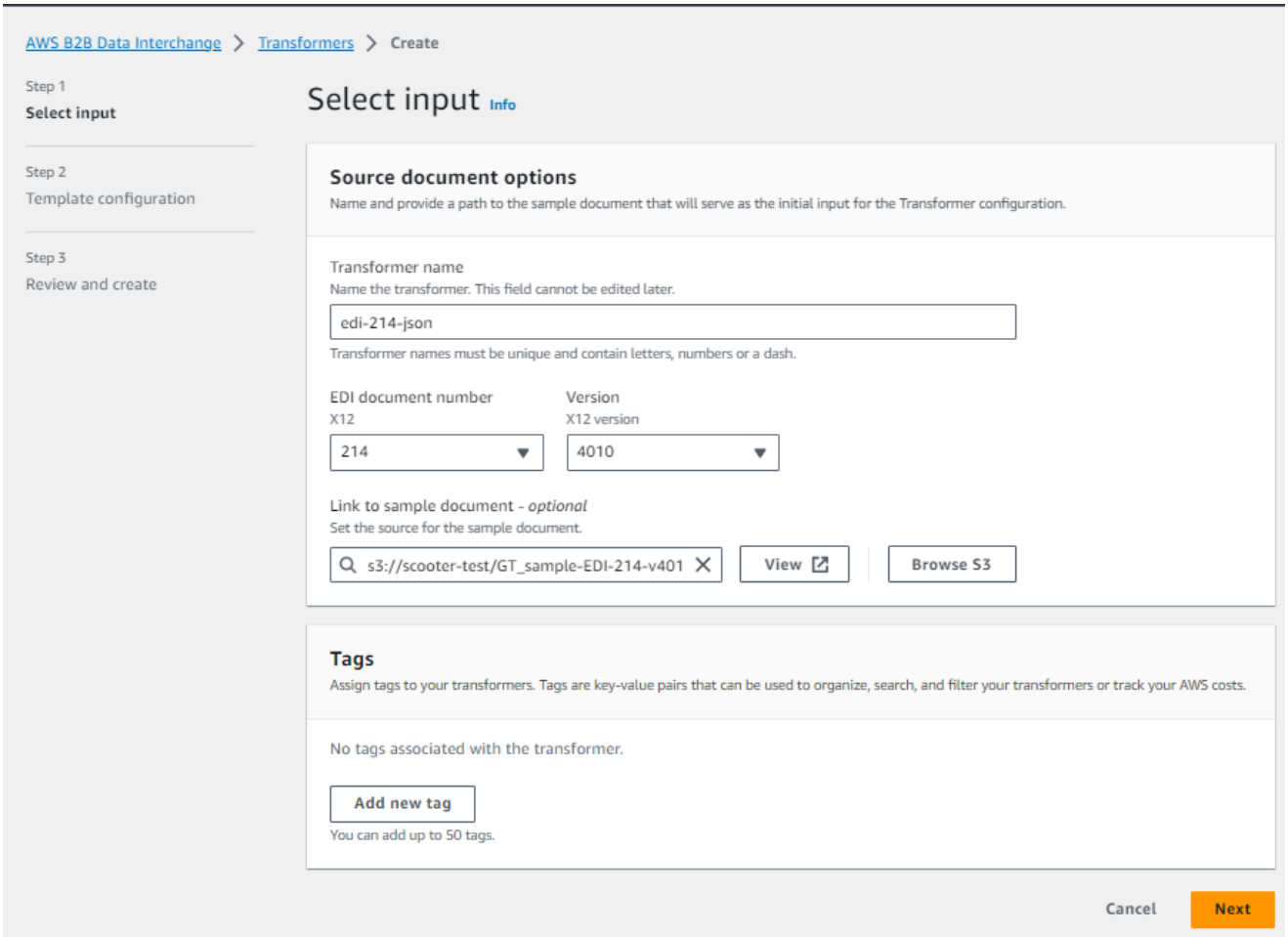
> **Note**
>
> If an EDI input file contains more than one transaction, each transaction must have the same document and version, for example **`214/4010`**. If not, the transformer cannot parse the file.

To create a transformer

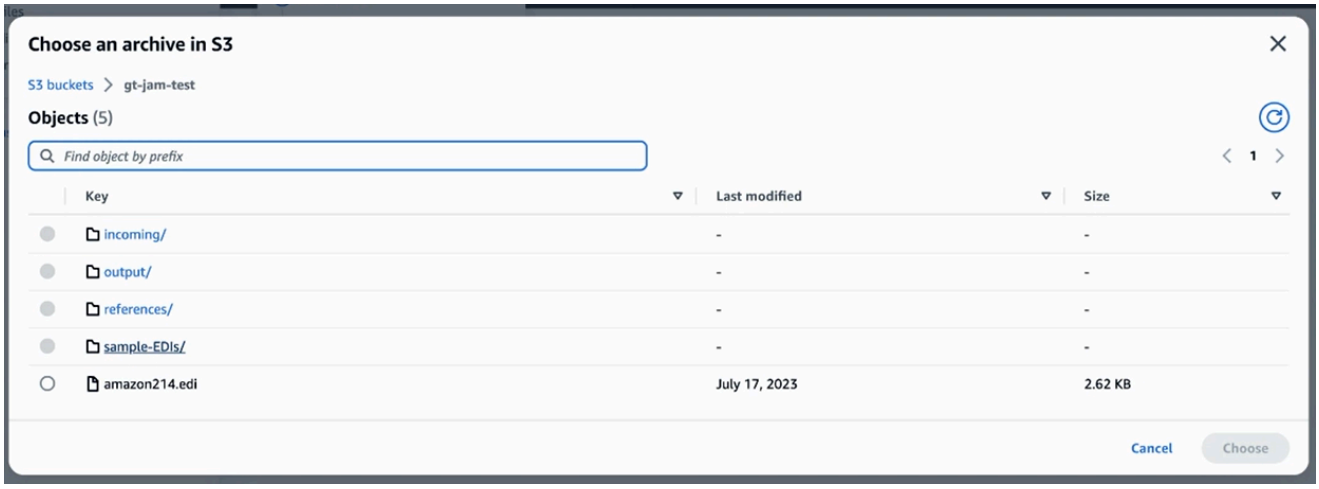
1. Open the AWS B2B Data Interchange console at https://console.aws.amazon.com/b2bi/ and select **Transformers** from the navigation pane, then choose **Create transformer**.
2. Select a transformer name (for example **edi-214-json**), the EDI doc number, and version. Then, provide a sample document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

   a. Enter a name (no spaces).

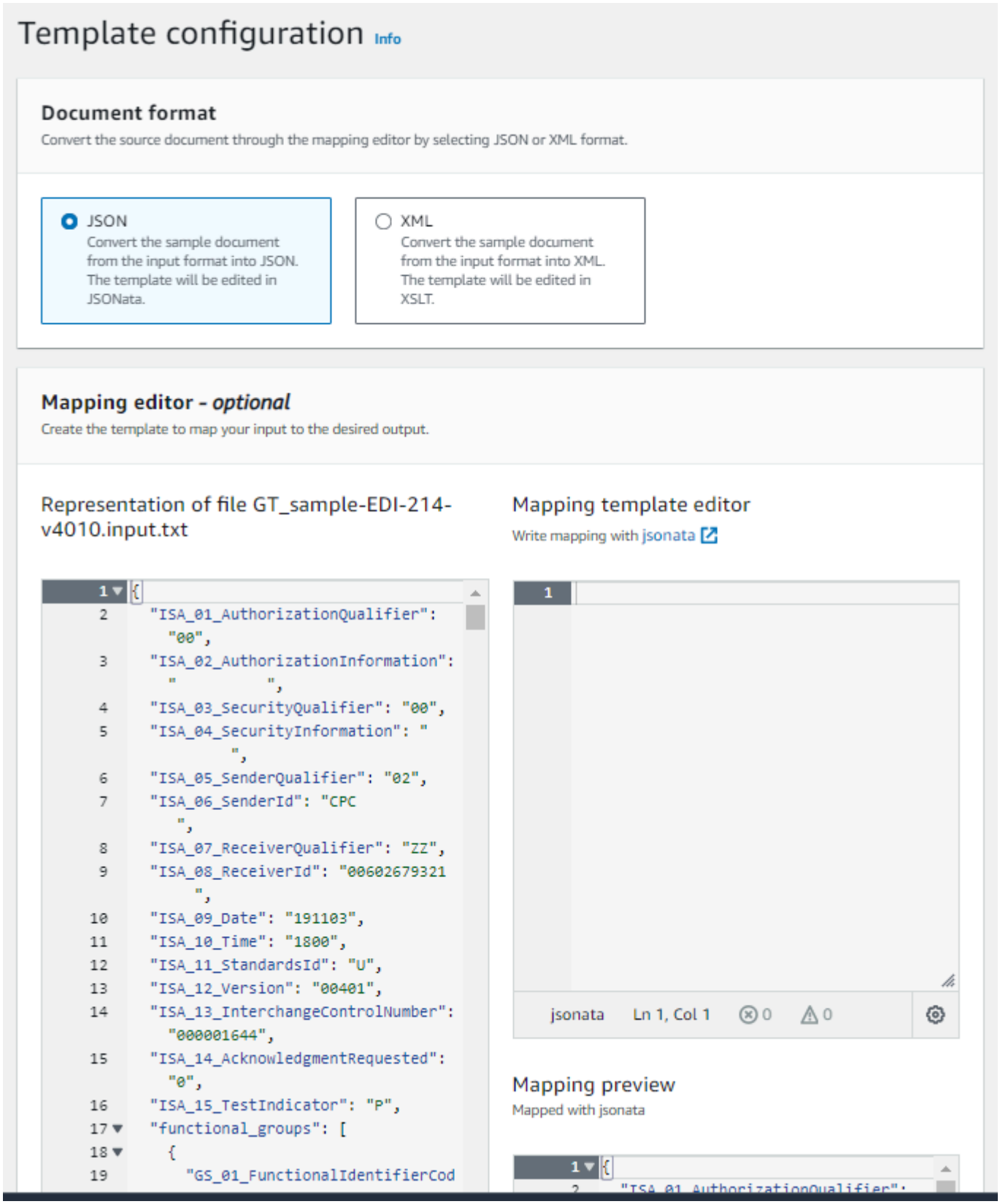
   b. Select an EDI document number and X12 version from the dropdown menus.



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

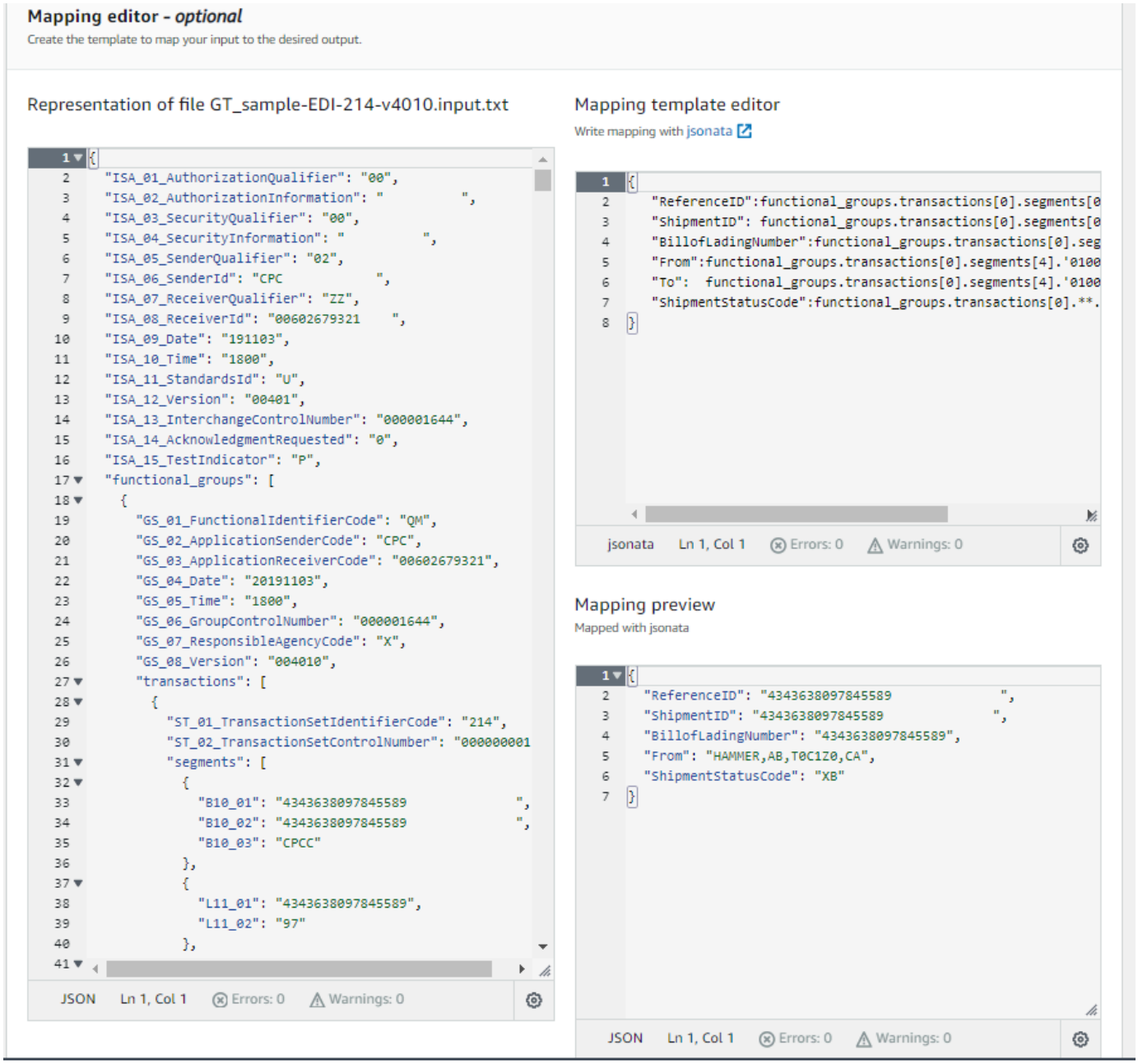


3. For the template configuration, choose the document format, JSON or XML. This populates the mapping editor, which shows the representation.


Template configuration Info
Document format
Convert the source document through the mapping editor by selecting JSON or XML format.
JSON
Convert the sample document from the input format into JSON. The template will be edited in JSONata.
XML
Convert the sample document from the input format into XML. The template will be edited in XSLT.
Mapping editor - optional
Create the template to map your input to the desired output.
Representation of file GT_sample-EDI-214-v4010.input.txt
Mapping template editor
Write mapping with jsonata
jsonata Ln 1, Col 1 0 0
Mapping preview
Mapped with jsonata

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** section.

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 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.

Step 3 Create a trading capability

A *trading capability* contains the information required to transform incoming EDI documents into JSON or XML outputs.

To create a 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 capability.
   - Choose an EDI document number and version from the corresponding dropdown menus.
   - Choose a transformer to determine how the incoming EDI documents should be transformed.
3. In the **Configure directory** section, you configure both the input and output directories that are used to source and store documents. The input directory is the location form where we

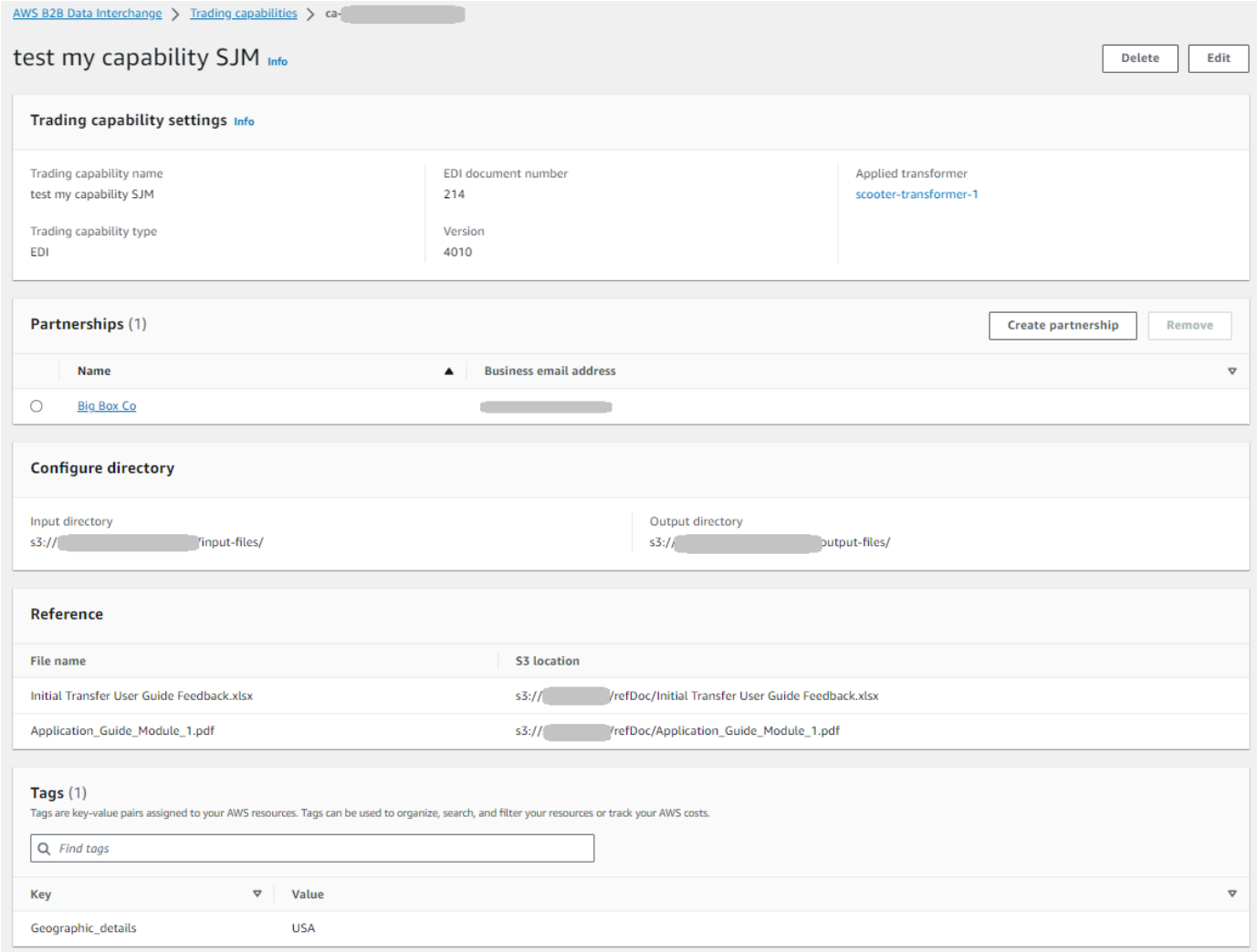
source EDI document input, and the output directory is where we store the translated JSON or XML output files.

- In the **Input directory** area, enter an Amazon S3 bucket.

  > **Note**
  >
  > 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.

- For **Add permissions**, 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.
- For your input and output directories, update the bucket policy (Configure your Amazon S3 bucket policies) and turn on EventBridge notifications (Configure your Amazon S3 bucket EventBridge setting).
- 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”.

4. In the **Reference - *optional*** panel, choose one or more files to share with your trading partner. Provide instructions and sample documents that can be accessed by your trading partners, so that they can align their EDI document formats with your transformation processes. You can directly enter the Amazon S3 path to a file, or choose **Browse S3** to navigate to one or more files.
5. Optionally, add tags as needed.
6. After you have configured all of the settings, choose **Create capability**.



Example bucket policies

You need to update your Amazon S3 bucket policies to include the appropriate permissions so that the B2Bi service can access EDI documents and store transformed JSON / XML outputs. When you create a capability, you have the option to copy a bucket policy that contains the correct permissions to work with your input and output Amazon S3 buckets.

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:::DOC-EXAMPLE-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:::DOC-EXAMPLE-BUCKET/output-folder/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                }
            }
        }
    ]
}
```

If you have SSE-KMS encryption enabled on your input or output bucket, you need to update the key policy in AWS KMS. You need to add the B2Bi service principal and the appropriate permissions to the policy.

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": "*"
        }
    ]
}
```

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**.

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 B2Bi 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, B2Bi 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.

Step 4 Create a partnership

A *partnership* represents the connection between you and your trading partner. It ties together a profile and one or more trading capabilities.

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. Enter a descriptive name for the partnership.
3. Enter an email address to associate with the partnership. Provide the trading partner's email address.
4. Choose a profile from the dropdown menu.
5. Select one or more trading capabilities from the **Trading capabilities** list.
6. Optionally, add tags as needed.
7. 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-`.

Next steps

Your trading partners can use AWS Transfer Family or any connectivity option to route incoming EDI documents to the configured input folder, where they will be picked up and transformed by B2Bi. You and your partners can see recent activity in CloudWatch Logs. Additionally, inbound EDI files automatically create a return acknowledgement to the trading partner, in the form of an Amazon EventBridge event. For details, see AWS B2B Data Interchange acknowledgements.

Configure AWS B2B Data Interchange using a 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 B2Bi 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.

AWS B2B Data Interchange acknowledgements

Customers often have a need to return acknowledgements whenever they receive inbound EDI files. The purpose of an acknowledgement is to tell their trading partner that they have received the file and to report errors.

B2Bi automatically generates X12 EDI acknowledgements whenever an EDI document is transformed by the service. The service creates an acknowledgement, which is stored in Amazon S3 alongside the transformed EDI, and then publishes an event to Amazon EventBridge. We generate two types of acknowledgements:

- *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.
- *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.

All inbound X12 transactions receive a TA1, while only certain transactions receive a 997. Finance, transportation, supply chain, and communication & control transactions typically receive a 997. These acknowledgements are created by default, and are not configurable.

> **Note**
>
> We don't currently support the 999 acknowledgement for healthcare-specific transactions or 999x231a acknowledgement for HIPAA-compliant X12 transactions.

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. Vendor A sends Retailer B an EDI 810 Invoice.
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.

B2Bi 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.

File output paths

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

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

- Input: s3://*DOC-EXAMPLE-BUCKET*/IN/
- Output: s3://*DOC-EXAMPLE-BUCKET*/OUT/

For this configuration, the following are the paths for the input and corresponding transformed output directories:

- Inbound EDI: s3://*DOC-EXAMPLE-BUCKET*/IN/TP_ID/edi214xml-test83.txt
- Transformed output: s3://*DOC-EXAMPLE-BUCKET*/OUT/TP_ID/edi214xml-test83.txt.2023-11-21T19:26:49.774Z.xml

The format for the acknowledgement filename depends on whether the incoming EDI document uses a capability or is called by the `StartTransformerJob` API.

When using a capability, the format for the acknowledgement files is s3://*DOC-EXAMPLE-BUCKET*/OUT/TP_ID/ACK/*filename*.*timestamp*.997 (.TA1 for TA1 acknowledgements).

The following are examples for the acknowledgement output filenames:

- 997 acknowledgement: s3://*DOC-EXAMPLE-BUCKET*/OUT/TP_ID/ACK/edi214xml-test83.txt.2023-11-21T19:26:49.774Z.997

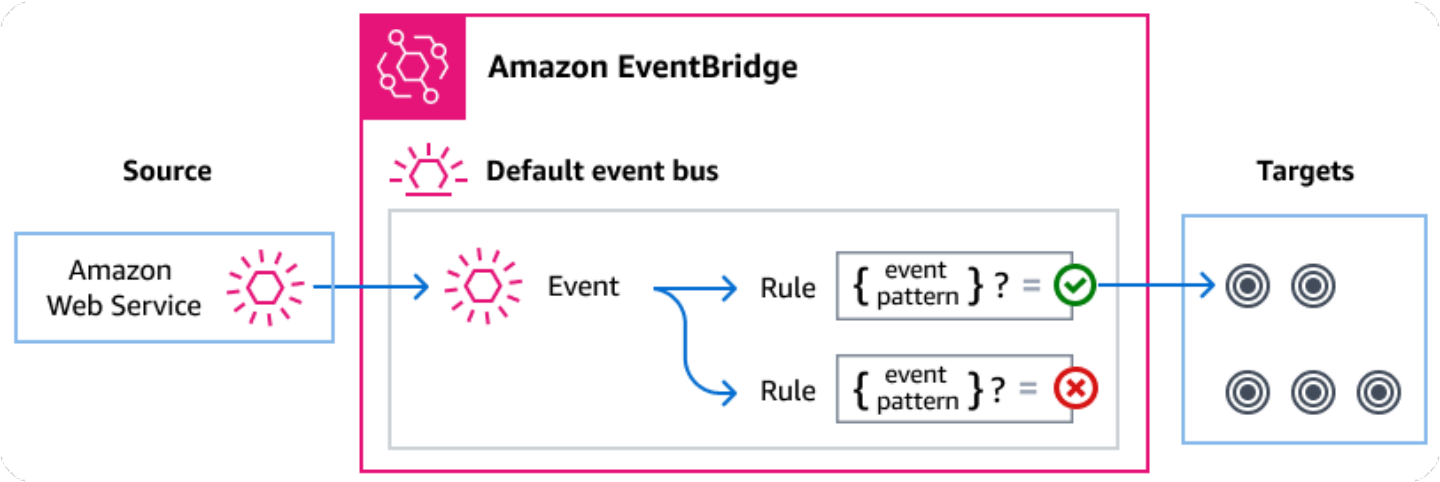
- TA1 acknowledgement: s3://*DOC-EXAMPLE-BUCKET*/OUT/TP_ID/ACK/edi214xml-test83.txt.2023-11-21T19:26:49.774Z.TA1

For direct transformer API calls, the format is s3://*DOC-EXAMPLE-BUCKET*/OUT/ACK/*filename*.*timestamp*.997 (.TA1 for TA1 acknowledgements).

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 B2Bi 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"
  }
}
```

`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.

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 B2Bi

This section presents the details for some example events generated by B2Bi.

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

The following example shows an event where a 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": "DOC-EXAMPLE-BUCKET",
      "object-key": "edi_214_4010.txt",
      "object-size-bytes": 1034
    },
    "output-file-s3-attributes": {
      "bucket": "DOC-EXAMPLE-BUCKET1",
      "object-key": "getTransformerJobTestOutput/
edi_214_4010.txt.2024-03-12T22:57:42.182Z.json",
      "object-size-bytes": 4174
    }
  }
}
```

Example Transformation Failed example 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://DOC-
EXAMPLE-BUCKET/myinputs/tp-aaaa11bbbb22cccc33dddd/edi_file_mar_14_2024_2.txt",
        "failure-code": "FILE_TRANSFORM_FAILED"
```

```
    }
}
```

Example Acknowledgement Completed example 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": "DOC-EXAMPLE-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": "DOC-EXAMPLE-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 example 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": "DOC-EXAMPLE-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 (B2Bi)

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 (B2Bi)

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.
- 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 140-2 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) 140-2.

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*.

Deleting AWS B2B Data Interchange resources

You can delete the resources that you create in B2Bi. See the guidance for each resource type in following sections of the *AWS B2B Data Interchange API Reference*.

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

Identity and access management for AWS B2B Data Interchange (B2Bi)

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 (B2Bi)
- Troubleshooting AWS B2B Data Interchange (B2Bi) 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	B2Bi support
Identity-based policies	Yes
Resource-based policies	No

IAM feature	B2Bi support
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 B2Bi 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 B2Bi

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 Creating IAM 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 B2Bi

To view examples of AWS B2B Data Interchange identity-based policies, see Identity-based policy examples for AWS B2B Data Interchange (B2Bi).

Resource-based policies within B2Bi

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 How IAM roles differ from resource-based policies in the *IAM User Guide*.

Policy actions for B2Bi

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 B2Bi actions, see Actions, resources, and condition keys for AWS B2B Data Interchange in the *Service Authorization Reference*.

Policy actions in B2Bi 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 (B2Bi).

Policy resources for B2Bi

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 B2Bi 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 (B2Bi).

Policy condition keys for B2Bi

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 B2Bi 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 (B2Bi).

ACLs in B2Bi

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 B2Bi

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 What is ABAC? 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 B2Bi

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 Switching to a 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 B2Bi

Supports forward access sessions (FAS)	Yes

Service roles for B2Bi

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 Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.

> **Warning**
>
> Changing the permissions for a service role might break B2Bi functionality. Edit service roles only when B2Bi provides guidance to do so.

Service-linked roles for B2Bi

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 (B2Bi)

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 Creating IAM policies 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 B2Bi 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 IAM Access Analyzer policy validation 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 Configuring MFA-protected API access 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 B2Bi 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 B2Bi console, also attach the B2Bi *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": "*"
        }
    ]
}
```

Troubleshooting AWS B2B Data Interchange (B2Bi) 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 B2Bi

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 B2Bi 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 How IAM roles differ from resource-based policies in the *IAM User Guide*.

Compliance validation for AWS B2B Data Interchange (B2Bi)

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 and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.
- Architecting for HIPAA Security and Compliance on Amazon Web Services – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

  > **Note**
  >
  > Not all AWS services are HIPAA eligible. For more information, see the HIPAA Eligible Services Reference.

- 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.
- 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 (B2Bi)

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 (B2Bi)

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 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 collects raw data and processes it into readable, near real-time metrics. These statistics are kept for 15 months, so that 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`.

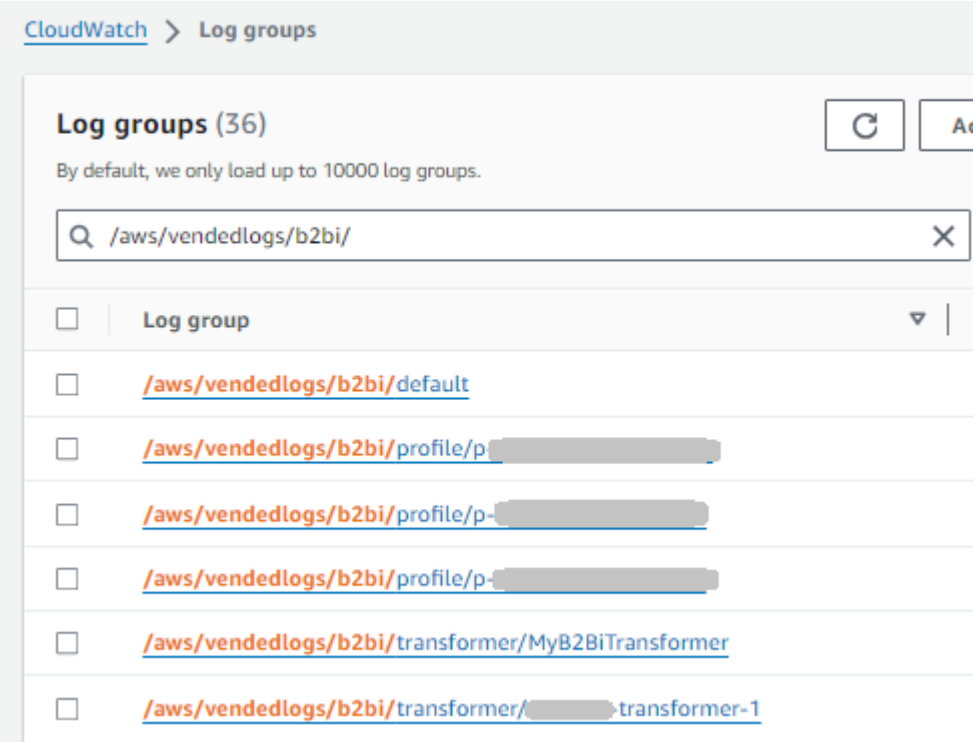
  Entries to this log group are created after a file is added to an Amazon S3 bucket, but the EDI file cannot be processed correctly.
- One log group for each profile that you create (if the profile has logging enabled).

  This log group is named `/aws/vendedlogs/b2bi/profile/p-`*`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 capability to handle the processing, and the capability is associated with a profile. If EDI processing fails, then there is no information available to find the 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 capability, no logs are written to this group.



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 (B2Bi) 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 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": "XXXXXXXXXXXXXXXXXXXXX",
                "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 (B2Bi) 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, 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, 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 (B2Bi) 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 API requests to AWS B2B Data Interchange using its default Regional DNS name. For example, `b2bi.us-east-1.amazonaws.com`.

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 (B2Bi)

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 capabilities per account	100
Maximum number of transformers per account	500
Maximum number of partnerships per account	700
Maximum EDI (electronic data interchange) file size	5 MB
Maximum number of instruction/reference documents per capability	5
Maximum number of inbound transformation request per account	3 per second

Supported X12 transaction sets

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.

			Version supported for Transaction set		
Transaction set	**Description**	**Category**	**4010**	**4030**	**5010**
110	Air Freight Details and Invoice	Transportation	Yes	Yes	Yes
180	Return Merchandise Authorization and Notification	Supply Chain	Yes	Yes	Yes
204	Motor Carrier Load Tender	Transportation	Yes	Yes	Yes
210	Motor Carrier Freight Details and Invoice	Transportation	Yes	Yes	Yes
211	Motor Carrier Bill of Lading	Transportation	Yes	Yes	Yes
214	Transportation Carrier Shipment	Transportation	Yes	Yes	Yes

			Version supported for Transaction set		
Transaction set	**Description**	**Category**	**4010**	**4030**	**5010**
	Status Message				
215	Motor Carrier Pickup Manifest	Transportation	Yes	Yes	Yes
259	Residential Mortgage Insurance Explanation of Benefits	Finance	*No*	*No*	Yes
260	Application for Mortgage Insurance Benefits	Finance	Yes	Yes	Yes
266	Mortgage or Property Record Change Notification	Finance	Yes	Yes	Yes
269	Health Care Benefit Coordination Verification	Insurance	*No*	*No*	Yes
270	Eligibility, Coverage or Benefit Inquiry	Insurance	Yes	Yes	Yes

			Version supported for Transaction set		
Transaction set	**Description**	**Category**	**4010**	**4030**	**5010**
271	Eligibility, Coverage or Benefit Information	Insurance	Yes	Yes	Yes
274	Healthcare Provider Information	Insurance	*No*	Yes	Yes
275	Patient Information	Insurance	Yes	Yes	Yes
276	Health Care Claim Status Request	Insurance	Yes	Yes	Yes
277	Health Care Information Status Notification	Insurance	Yes	Yes	Yes
278	Health Care Services Review Information	Insurance	Yes	Yes	Yes
310	Freight Receipt and Invoice (Ocean)	Transportation	Yes	Yes	Yes
315	Status Details (Ocean)	Transportation	Yes	Yes	Yes

			Version supported for Transaction set		
Transaction set	**Description**	**Category**	**4010**	**4030**	**5010**
322	Terminal Operations and Intermodal Ramp Activity	Transportation	Yes	Yes	Yes
404	Rail Carrier Shipment Information	Transportation	Yes	Yes	Yes
410	Rail Carrier Freight Details and Invoice	Transportation	Yes	Yes	Yes
417	Rail Carrier Waybill Interchange	Transportation	Yes	Yes	Yes
421	Estimated Time of Arrival and Car Scheduling	Transportation	Yes	Yes	Yes
426	Rail Revenue Waybill	Transportation	Yes	Yes	Yes
810	Invoice	Finance	Yes	Yes	Yes

			Version supported for Transaction set		
Transaction set	**Description**	**Category**	**4010**	**4030**	**5010**
820	Payment Order/Remittance Advice	Finance	Yes	Yes	Yes
824	Application Advice	Finance	Yes	Yes	Yes
830	Planning Schedule with Release Capability	Supply Chain	Yes	Yes	Yes
832	Price/Sales Catalog	Supply Chain	Yes	Yes	Yes
834	Benefit Enrollment and Maintenance	Insurance	Yes	Yes	Yes
835	Health Care Claim Payment/Advice	Insurance	Yes	Yes	Yes
837	Health Care Claim	Insurance	Yes	Yes	Yes
844	Product Transfer Account Adjustment	Finance	Yes	Yes	Yes

			Version supported for Transaction set		
Transaction set	**Description**	**Category**	**4010**	**4030**	**5010**
846	Inventory Inquiry/Advice	Supply Chain	Yes	Yes	Yes
849	Response to Product Transfer Account Adjustment	Finance	Yes	Yes	Yes
850	Purchase Order	Supply Chain	Yes	Yes	Yes
852	Product Activity Data	Supply Chain	Yes	Yes	Yes
855	Purchase Order Acknowledgement	Supply Chain	Yes	Yes	Yes
856	Ship Notice/Manifest	Supply Chain	Yes	Yes	Yes
860	Purchase Order Change Request - Buyer Initiated	Supply Chain	Yes	Yes	Yes

			Version supported for Transaction set		
Transaction set	**Description**	**Category**	**4010**	**4030**	**5010**
861	Receiving Advice/Acceptance Certificate	Supply Chain	Yes	Yes	Yes
864	Text Message	Communications & Controls	Yes	Yes	Yes
865	Purchase Order Change Acknowledgement/Request - Seller Initiated	Supply Chain	Yes	Yes	Yes
869	Order Status Inquiry	Supply Chain	Yes	Yes	Yes
870	Order Status Report	Supply Chain	Yes	Yes	Yes
940	Warehouse Shipping Order	Supply Chain	Yes	Yes	Yes
945	Warehouse Shipping Advice	Supply Chain	Yes	Yes	Yes
990	Response to a Load Tender	Transportation	Yes	Yes	Yes

			Version supported for Transaction set		
Transaction set	**Description**	**Category**	**4010**	**4030**	**5010**
997	Functional Acknowledgement	Communications & Controls	Yes	Yes	Yes
999	Implementation Acknowledgement	Communications & Controls	*No*	*No*	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
270 X279	Eligibility Benefit Inquiry
271 X279	Eligibility Benefit Response
275 X210	Unsolicited Claim Attachments (from practice to payer)
275 X211	Unsolicited Claim Attachments (from practice to clearinghouse to payer)
276 X212	Claim Status Request

Transaction Set	Description
277 X212	Claim Status Request Response
277 X214	Claim Acknowledgement
277 X364	Data Reporting Acknowledgement
278 X217	Services Review Information Review/Response
820 X218	Payroll Deducted and Other Group Premium Payment For Insurance Products Examples
820 X306	Health Insurance Exchange Related Payments
824 X186	Application Advice
834 X220	Benefit Enrollment and Maintenance
834 X307	Health Insurance Exchange: Enrollment
834 X318	Benefit Enrollment and Maintenance, Electroni c Remittance Advice (ERA)
835 X221	Claim Payment/Advice, Electronic Remittance Advice (ERA)
837 X222	Claim, Professional and vision claims
837 X223	Claim, Institutional claims
837 X224	Claim, Dental claims
837 X291	Professional Pre-Determination
837 X292	Institutional Pre-Determination
837 X298	Post-adjudicated Claims Data Reporting, Professional
999 X231	Implementation Acknowledgement

Document history for the AWS B2B Data Interchange (B2Bi) User Guide

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

Change	Description	Date
Add the ability to return acknowledgements	AWS B2B Data Interchange now automatically creates return acknowledgements for all inbound EDI files. For details, see AWS B2B Data Interchange 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 Interchange events using Amazon EventBridge.	March 22, 2024
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