

Oracle® Cloud

Using the Adobe Sign Adapter with Oracle Integration Generation 2



E85523-13
December 2022

The Oracle logo, consisting of the word "ORACLE" in white, uppercase, sans-serif font, centered within a solid red square.

ORACLE®

Oracle Cloud Using the Adobe Sign Adapter with Oracle Integration Generation 2,

E85523-13

Copyright © 2019, 2022, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	iv
Documentation Accessibility	iv
Diversity and Inclusion	iv
Related Resources	v
Conventions	v

1 Understand the Adobe Sign Adapter

Adobe Sign Adapter Capabilities	1-1
What Application Version Is Supported?	1-1
About Adobe Sign Adapter Use Cases	1-1
Workflow to Create and Add an Adobe Sign Adapter Connection to an Integration	1-2

2 Create an Adobe Sign Adapter Connection

Prerequisites for Creating a Connection	2-1
Create a Connection	2-2
Configure Connection Security	2-3
Test the Connection	2-4
Upload an SSL Certificate	2-4

3 Add the Adobe Sign Adapter Connection to an Integration

Basic Information Page	3-1
Invoke Operations Page	3-2
Invoke Query Page	3-2
Summary Page	3-3

4 Troubleshoot the Adobe Sign Adapter

Specify the Port Number with the Authorized Redirect URL	4-1
--	-----

Preface

This guide describes how to configure this adapter as a connection in an integration in Oracle Integration.

**Note:**

The use of this adapter may differ depending on the features you have, or whether your instance was provisioned using Standard or Enterprise edition. These differences are noted throughout this guide.

Topics:

- [Audience](#)
- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)
- [Related Resources](#)
- [Conventions](#)

Audience

This guide is intended for developers who want to use this adapter in integrations in Oracle Integration.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our

initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

See these Oracle resources:

- Oracle Cloud
<http://cloud.oracle.com>
- *Using Integrations in Oracle Integration Generation 2*
- *Using the Oracle Mapper with Oracle Integration Generation 2*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Understand the Adobe Sign Adapter

Review the following conceptual topics to learn about the Adobe Sign Adapter and how to use it as a connection in Oracle Integration integrations. A typical workflow of adapter and integration tasks is also provided.

Topics:

- [Adobe Sign Adapter Capabilities](#)
- [What Application Version Is Supported?](#)
- [About Adobe Sign Adapter Use Cases](#)
- [Workflow to Create and Add an Adobe Sign Adapter Connection to an Integration](#)



Note:

There are overall service limits for Oracle Integration. A service limit is the quota or allowance set on a resource. See [Service Limits](#).

Adobe Sign Adapter Capabilities

The Adobe Sign Adapter enables you to prepare and send documents to Adobe Sign for review and approval.

The Adobe Sign Adapter integrates your applications with Adobe Document Cloud. You can replace your paper and ink signature processes with fully automated electronic signature workflows. Use a browser or mobile device to send, sign, track, and manage the review and signature process.

The Adobe Sign Adapter is one of many predefined adapters included with Oracle Integration. You can configure the Adobe Sign Adapter adapter as a connection in an integration in Oracle Integration.

What Application Version Is Supported?

For information about which application version is supported by this adapter, see the [Connectivity Certification Matrix](#).

See [Connectivity Certification Matrix](#).

About Adobe Sign Adapter Use Cases

The Adobe Sign Adapter can be used in scenarios such as the following.

- Select the Send Agreement for Signature operation in one integration to send an agreement for review and signing. Select and configure the REST Adapter as the trigger.

Appropriate data mapping between the REST Adapter and Adobe Sign Adapter is performed in the mapper. Invoke the integration endpoint with a REST client to send a POST request to the REST Adapter. Appropriate data mapping between the REST Adapter and Adobe Sign Adapter is performed in the mapper. The Adobe Sign Adapter sends the data as a payload while invoking the configured operation in Adobe Sign.

- Select the Get Agreement Form Data operation in the other integration to retrieve the data entered by a user when they completed the interactive agreement form fields and signed the agreement. Appropriate data mapping between the REST Adapter and Adobe Sign Adapter is performed in the mapper. The REST Adapter sends a GET request to the Adobe Sign Adapter, which returns the form data and the signed agreement.

 **Note:**

Oracle Integration offers a number of pre-assembled solutions, known as recipes, that provide you with a head start in building your integrations. You can start with a recipe, and then customize it to fit your needs and requirements. Depending upon the solution provided, a variety of adapters are configured in the pre-assembled solutions. See the Recipes page on the Oracle Help Center.

Workflow to Create and Add an Adobe Sign Adapter Connection to an Integration

Follow a workflow to create a connection with an adapter and include the connection in an integration in Oracle Integration.

Step	Description	More Information
1	Create the adapter connections for the applications you want to integrate. The connections can be reused in multiple integrations and are typically created by the administrator.	Create an Adobe Sign Adapter Connection
2	Create the integration. When you do this, you add trigger and invoke connections to the integration.	Create Integrations and Add the Adobe Sign Adapter Connection to an Integration
3	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in <i>Using Integrations in Oracle Integration Generation 2</i>
4	(Optional) Create lookups that map the different values used by those applications to identify the same type of object (such as gender codes or country codes).	Manage Lookups in <i>Using Integrations in Oracle Integration Generation 2</i>

Step	Description	More Information
5	Activate the integration.	Manage Integrations in <i>Using Integrations in Oracle Integration Generation 2</i>
6	Monitor the integration on the dashboard.	Monitor Integrations in <i>Using Integrations in Oracle Integration Generation 2</i>
7	Track payload fields in messages during runtime.	Assign Business Identifiers for Tracking Fields in Messages and Manage Business Identifiers for Tracking Fields in Messages in <i>Using Integrations in Oracle Integration Generation 2</i>
8	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in <i>Using Integrations in Oracle Integration Generation 2</i>

2

Create an Adobe Sign Adapter Connection

A connection is based on an adapter. You define connections to the specific cloud applications that you want to integrate.

Topics:

- [Prerequisites for Creating a Connection](#)
- [Create a Connection](#)
- [Upload an SSL Certificate](#)

Prerequisites for Creating a Connection

These are the prerequisites for creating a connection with the Adobe Sign Adapter.

- [Obtain the Client ID and Client Secret](#)
- [Obtain the Subdomain](#)

Obtain the Client ID and Client Secret



Note:

To create a connection, a trusted public certificate is required. Typically, the certificate is included with Oracle Integration. If you cannot locate the public certificate, contact your administrator. If you download a public certificate, rename the file extension to `.cert`. See [Upload an SSL Certificate](#).

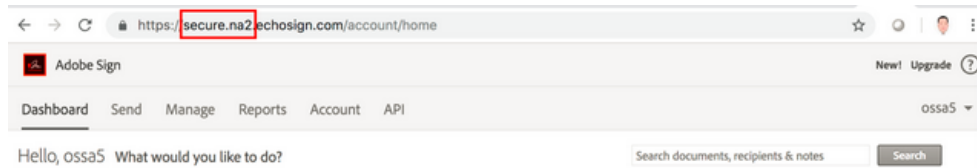
1. Create an Adobe Document Cloud Account. If you do not have an account, you can create one here: <https://acrobat.adobe.com/us/en/documents/trial-global.html>.
2. Log in to your Adobe Document Cloud Account.
3. Click your user name in the upper right corner and select **My Profile**.
4. Expand **Adobe DC Sign API** in the left pane and select **API Applications**.
5. Create a new application:
 - Click the **Create** icon in the upper right corner.
 - Enter a name and a display name for your application.
 - Select **PARTNER**.
 - Click **Save**.
6. Select the application you created in step 5.
7. Click **Configure OAuth for Application**.

8. Enter `https://{ICS_HOST}:{ICS_SSL_PORT}/icsapis/agent/oauth/callback` in the **Redirect URI** field.
9. Enable the **user_login**, **agreement_read**, **agreement_write**, **agreement_send**, and **library_read** scopes.
10. Select the **account** modifier for the **user_login**, **agreement_read**, **agreement_write**, **agreement_send**, and **library_read** scopes.
11. Copy or record the values in the **Client ID** and **Client Secret** fields. These values are required to create the connection in Oracle Integration. See [Configure Connection Security](#).
12. Click **Save**.

Obtain the Subdomain

To create a connection, you can optionally provide the subdomain.

1. Log in to the Dashboard.
2. Go to the **Dashboard** tab.
3. Copy the domain name. An example of the **Dashboard** tab with a domain name of `secure.na2` is shown below.



See [Configure Connection Security](#).

Create a Connection

Before you can build an integration, you have to create the connections to the applications with which you want to share data.

To create a connection in Oracle Integration:

1. In the left navigation pane, click **Home > Integrations > Connections**.
2. Click **Create**.

Note:

You can also create a connection in the integration canvas of:

- An orchestrated integration (See [Define Inbound Triggers and Outbound Invokes](#).)
- A basic routing integration (See [Add a Trigger \(Source\) Connection](#).)

3. In the **Create Connection — Select Adapter** dialog, select the adapter to use for this connection. To find the adapter, scroll through the list, or enter a partial or full name in the **Search** field and click



Search.

4. In the Create Connection dialog, enter the information that describes this connection.
 - a. Enter a meaningful name to help others find your connection when they begin to create their own integrations. The name you enter is automatically added in capital letters to the **Identifier** field. If you modify the identifier name, don't include blank spaces (for example, SALES OPPORTUNITY).
 - b. Enter optional keywords (tags). You can search on the connection keywords on the Connections page.
 - c. Select the role (direction) in which to use this connection (trigger, invoke, or both). Only the roles supported by the adapter are displayed for selection. When you select a role, only the connection properties and security policies appropriate to that role are displayed on the Connections page. If you select an adapter that supports both invoke and trigger, but select only one of those roles, you'll get an error when you try to drag the adapter into the section you didn't select. For example, let's say you configure a connection for the Oracle Service Cloud (RightNow) Adapter as only an **invoke**. Dragging the adapter to a **trigger** section in the integration produces an error.
 - d. Enter an optional description of the connection.
5. Click **Create**.

Your connection is created. You're now ready to configure the connection details, such as connection properties, security policies, connection login credentials, and (for certain connections) agent group.

Configure Connection Security

Enter connection information so your application can process requests.

1. Go to the **Connection Properties** section.

The **Security Policy** field displays **Adobe Sign OAuth Authorization Code Credentials**. This value cannot be changed. This policy supports the OAuth 2.0 framework and three-legged authentication.

2. Enter the subdomain of the authentication URL. The subdomain can be copied from the browser address after logging in to your Dashboard. For example:

- oracle.na1
- ge.na1
- google.na1
- secure.na2

A URL is automatically assembled from the subdomain you specify. For example, `https://oracle.na1.echosign.com/public/oauth`.

If you do not enter a subdomain in this field, `https://secure.echosign.com/public/oauth` is used by default.

See [Prerequisites for Creating a Connection](#).

3. Enter the client ID and client secret values you recorded when you created your Adobe Document Cloud Account application.

See [Prerequisites for Creating a Connection](#).

4. Enter the scope values in the **Scope** field.
A scope is a list of authorization permissions for the target application.
5. Click **Provide Consent**.
6. If required, enter your Adobe Document Cloud Account user name and password.
7. Click **Log In**.
8. Return to Oracle Integration to test and save the security credentials.

Test the Connection

Test your connection to ensure that it's configured successfully.

1. In the page title bar, click **Test**. What happens next depends on whether your adapter connection uses a Web Services Description Language (WSDL) file. Only some adapter connections use WSDLs.

If Your Connection...	Then...
Doesn't use a WSDL	The test starts automatically and validates the inputs you provided for the connection.
Uses a WSDL	A dialog prompts you to select the type of connection testing to perform: <ul style="list-style-type: none"> • Validate and Test: Performs a full validation of the WSDL, including processing of the imported schemas and WSDLs. Complete validation can take several minutes depending on the number of imported schemas and WSDLs. No requests are sent to the operations exposed in the WSDL. • Test: Connects to the WSDL URL and performs a syntax check on the WSDL. No requests are sent to the operations exposed in the WSDL.

2. Wait for a message about the results of the connection test.
 - If the test was successful, then the connection is configured properly.
 - If the test failed, then edit the configuration details you entered. Check for typos, verify URLs and credentials, and download the diagnostic logs for additional details. Continue to test until the connection is successful.
3. When complete, click **Save**.

Upload an SSL Certificate

Certificates are used to validate outbound SSL connections. If you make an SSL connection in which the root certificate does not exist in Oracle Integration, an exception is thrown. In that case, you must upload the appropriate certificate. A certificate enables Oracle Integration to connect with external services. If the external endpoint requires a specific certificate, request the certificate and then upload it into Oracle Integration.

To upload an SSL certificate:

1. In the left navigation pane, click **Home > Settings > Certificates**.

All certificates currently uploaded to the trust store are displayed in the Certificates dialog. The



link enables you to filter by name, certificate expiration date, status, type, category, and installation method (user-installed or system-installed). Certificates installed by the system cannot be deleted.

Certificates Upload			
6 Certificates			
Installed By: User X			
Name	Type	Category	Status
mykey3 EXPIRES IN 1 MONTHS	X.509	Identity	Configured
mykey2 EXPIRED	X.509	Identity	Configured
recert1586867745048 EXPIRES IN 4 YEARS	X.509	Trust	Configured
recert1586863610817 EXPIRES IN 4 YEARS	X.509	Trust	Configured
recert1586857607511 EXPIRES IN 4 YEARS	X.509	Trust	Configured
recert1586857416600 EXPIRES IN 4 YEARS	X.509	Trust	Configured

2. Click **Upload** at the top of the page. The Upload Certificate dialog box is displayed.
3. Enter an alias name and optional description.
4. In the **Type** field, select the certificate type. Each certificate type enables Oracle Integration to connect with external services.
 - **X.509 (SSL transport)**
 - **SAML (Authentication & Authorization)**
 - **PGP (Encryption & Decryption)**

X.509 (SSL transport)

1. Select a certificate category.
 - a. **Trust:** Use this option to upload a trust certificate.
 - i. Click **Browse**, then select the trust file (for example, .cer or .crt) to upload.
 - b. **Identity:** Use this option to upload a certificate for two-way SSL communication.
 - i. Click **Browse**, then select the keystore file (.jks) to upload.
 - ii. Enter the comma-separated list of passwords corresponding to key aliases.

Note:

When an identity certificate file (JKS) contains more than one private key, all the private keys must have the same password. If the private keys are protected with different passwords, the private keys cannot be extracted from the keystore.

- iii. Enter the password of the keystore being imported.

- c. Click **Upload**.

SAML (Authentication & Authorization)

1. Note that **Message Protection** is automatically selected as the only available certificate category and cannot be deselected. Use this option to upload a keystore certificate with SAML token support. Create, read, update, and delete (CRUD) operations are supported with this type of certificate.
2. Click **Browse**, then select the certificate file (.cer or .crt) to upload.
3. Click **Upload**.

PGP (Encryption & Decryption)

1. Select a certificate category. Pretty Good Privacy (PGP) provides cryptographic privacy and authentication for communication. PGP is used for signing, encrypting, and decrypting files. You can select the private key to use for encryption or decryption when configuring the stage file action.
 - a. **Private:** Uses a private key of the target location to decrypt the file.
 - i. Click **Browse**, then select the PGP file to upload.
 - ii. Enter the PGP private key password.
 - b. **Public:** Uses a public key of the target location to encrypt the file.
 - i. Click **Browse**, then select the PGP file to upload.
 - ii. In the **ASCII-Armor Encryption Format** field, select **Yes** or **No**. **Yes** shows the format of the encrypted message in ASCII armor. ASCII armor is a binary-to-textual encoding converter. ASCII armor formats encrypted messaging in ASCII. This enables messages to be sent in a standard messaging format. This selection impacts the visibility of message content. **No** causes the message to be sent in binary format.
 - iii. From the **Cipher Algorithm** list, select the algorithm to use. Symmetric-key algorithms for cryptography use the same cryptographic keys for both encryption of plain text and decryption of cipher text.
- c. Click **Upload**.

3

Add the Adobe Sign Adapter Connection to an Integration

When you drag the Adobe Sign Adapter into the invoke area of an integration, the Adapter Endpoint Configuration Wizard appears. This wizard guides you through configuration of the Adobe Sign Adapter endpoint properties.

These topics describe the wizard pages that guide you through configuration of the Adobe Sign Adapter as an invoke in an integration. The Adobe Sign Adapter cannot be used as a trigger in an integration.

Topics:

- [Basic Information Page](#)
- [Invoke Operations Page](#)
- [Invoke Query Page](#)
- [Summary Page](#)

Basic Information Page

You can enter a name and description on the Basic Info page of each trigger and invoke adapter in your integration.

Element	Description
What do you want to call your endpoint?	Provide a meaningful name so that others can understand the responsibilities of this connection. You can include English alphabetic characters, numbers, underscores, and dashes in the name. You cannot include the following: <ul style="list-style-type: none">• Blank spaces (for example, My Inbound Connection)• Special characters (for example, #;83& or righ(t)now4)• Multibyte characters
What does this endpoint do?	Enter an optional description of the connection's responsibilities. For example: This connection receives an inbound request to synchronize account information with the cloud application.

Invoke Operations Page

Enter the Adobe Sign Adapter invoke operation values for your integration.

The table provides definitions for the Adobe Sign API operations that can be performed on the invoke connection. These operations are listed on the Adobe Sign Adapter Operations page.

Operation	Description
Send Agreement for Signature	Creates an agreement and then sends it for a signature.
Get Agreement List for User	Returns a list of agreements for a specific user.
Get Agreement Status	Returns the latest status of a specific agreement.
Get Document Ids of Agreement	Returns the IDs of the primary and supporting documents for a specific agreement.
Get Document URL	Returns the URL of a specific document.
Cancel an Agreement	Cancels an agreement and changes its status to cancel.
Delete an Agreement	Deletes all documents associated with an agreement.
Get document of an agreement	Returns the file stream of a document of an agreement.
Get information of the documents associated with an agreement	Returns a single, combined PDF document for the documents associated with an agreement.
Get agreement form data	Returns the data entered by the user into interactive form fields when they signed the agreement.
Get the audit trail of an agreement	Returns the audit trail of an agreement identified by the agreement ID.
Upload a document	Uploads a document and obtains returns the ID of the document.
Get User Workflows	Returns workflows for a user.
Get details of a Workflow	Returns the details of a workflow.
Create and Send an agreement out for signature	Creates an agreement, sends it for signatures, and returns the agreement ID in the response to the client.
Send Agreement for signature to multiple recipients	Sends an agreement to multiple recipients for their signature. Each recipient is sent a copy of the agreement for review and authorization.
Element	Description
Select Operation	Select the API operation to perform.

Invoke Query Page

Enter the Adobe Sign Adapter query parameters.

You can configure the request query parameters on the Adobe Sign Adapter Request Parameters page. This page is displayed when you select an operation that includes request parameters. The parameters that are displayed are dependent on the operation selected. For example, the parameters in the table are available for the operation `Get agreement list of the user`.

Parameter	Description
query	Identifies the search query string.
externalNamespace	Identifies the external namespace for which information should be returned.
externalID	Identifies the external ID for which information should be returned.
externalGroup	Identifies the external group for which information should be returned.

Summary Page

You can review the specified adapter configuration values on the Summary page.

Element	Description
Summary	<p>Displays a summary of the configuration values you defined on previous pages of the wizard.</p> <p>The information that is displayed can vary by adapter. For some adapters, the selected business objects and operation name are displayed. For adapters for which a generated XSD file is provided, click the XSD link to view a read-only version of the file.</p> <p>To return to a previous page to update any values, click the appropriate tab in the left panel or click Back.</p> <p>To cancel your configuration details, click Cancel.</p>

4

Troubleshoot the Adobe Sign Adapter

Review the following topics to learn about troubleshooting issues with the Adobe Sign Adapter.

Topics:

- [Specify the Port Number with the Authorized Redirect URL](#)

Additional integration troubleshooting information is provided. See Troubleshoot Oracle Integration in *Using Integrations in Oracle Integration Generation 2* and the [Oracle Integration Troubleshooting page](#) in the Oracle Help Center.

Specify the Port Number with the Authorized Redirect URL

When configuring the authorized redirect URL, ensure that you specify the port number. For example:

```
https://host:443/icsapis/agent/oauth/callback
```

Not specifying the port number in the URL results in an error saying the application wasn't authorized for the redirect URL.