

Oracle
Primavera
Unifier Adobe Sign Configuration Guide

Version 21
January 2021

Contents

Overview	5
Adobe Sign Setup	7
Configuring OAuth	11
Copyright.....	13

Overview

Note: The information provided in this document are subject to change.

The Adobe Sign admin must complete steps to assist in the initial setup and configuration of Adobe Sign as a delivery option within Unifier Stage Environment.

Specific setup instructions for the Adobe Sign integration with Unifier Stage Environment are provided in this document and are subject to change. Contact your Unifier Production Environment administrator or Technical Support with any questions about the Adobe Sign and Unifier Stage Environment integration.

Note: Documents sent to DocuSign or Adobe Sign are done over SSL (Secured Socket Layer) which is an encryption-based Internet security protocol.

Adobe Sign Setup

This section explains how to integrate Adobe Sign into the system.

Download

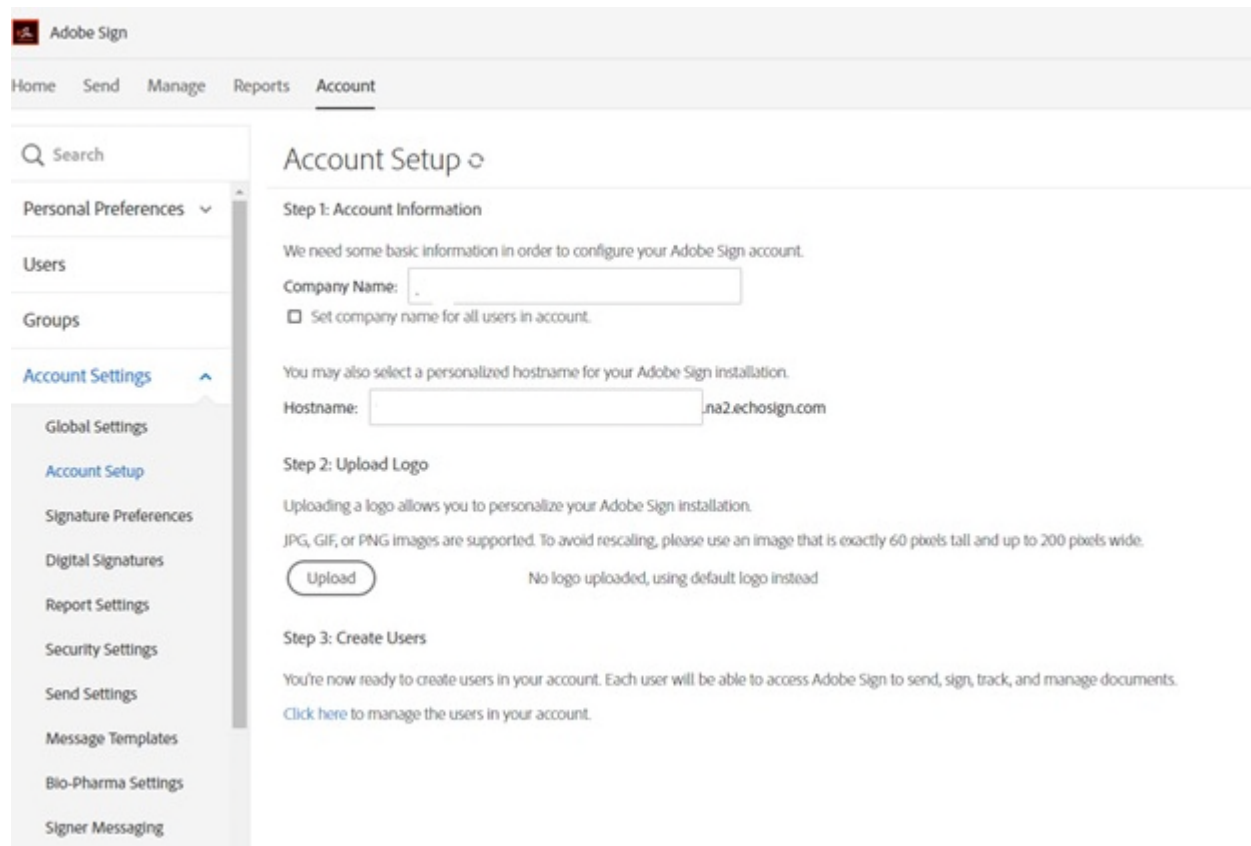
Download the Adobe Sign certificate from the echosign URL and import it to all of the Unifier nodes and restart them.

Configure

Note: You will need a developer account.

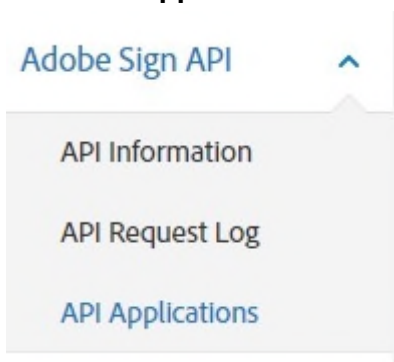
- 1) Log into **Adobe Sign**.
- 2) Click the **Account** tab.
- 3) From the left-hand navigator, click **Account Settings** to expand.
- 4) Click **Global Settings**.
- 5) Deselect the **Limited Document Visibility**, if checked.
- 6) Click the **Account Setup** tab.
- 7) Enter your company name and hostname.

Note: Ensure that you record the hostname and URL as this information must be used for Unifier.



The screenshot shows the Adobe Sign 'Account Setup' page. The left sidebar contains a search bar and a list of navigation items: Personal Preferences, Users, Groups, Account Settings (highlighted), Global Settings, Account Setup (highlighted), Signature Preferences, Digital Signatures, Report Settings, Security Settings, Send Settings, Message Templates, Bio-Pharma Settings, and Signer Messaging. The main content area is titled 'Account Setup' and contains three steps: Step 1: Account Information, Step 2: Upload Logo, and Step 3: Create Users. Step 1 includes fields for 'Company Name' and 'Hostname' (with a dropdown showing '.na2.echosign.com'). Step 2 includes an 'Upload' button and a note about logo specifications. Step 3 includes a link to 'Click here to manage the users in your account.'

- 1) Go to the **Adobe Sign API**.
- 2) Click **API Applications**.



- 3) From the right-hand side of the window, click the plus symbol (+).

API Applications 

 Search  

[View](#) / [Edit](#) | [Deactivate](#) | [Configure OAuth for Application](#)

Oracletest2	CBjCHCAABAAAdMDh6943uXSikPsdBRUK2-6zyf02uVL	06/03/2020 04:48	ACTIVE
Oracletest1	CBjCHCAABAAAPVupMWLbaKTEb9i-rtAbikuogOBKFZ_	06/03/2020 04:48	DISABLED
oracletest	CBjCHCAABAAAggUtnAIRsaIT9p2l8xrvlenc8Bvkj	06/03/2020 04:47	DISABLED

- 4) In the Create block, enter vaules for the Name and Display Name fields.
- 5) Click to select **Partner**.
- 6) Click **Save**.

Create



Provide a name for your application to issue a set of credentials for use with Adobe Sign's API

Name:

Display Name:

Domain:

☐ CUSTOMER (This application will only have access to data within your account)

☒ PARTNER (This application will have access to any authorized Adobe Sign account)

Cancel

Save

- 7) Proceed to configure OAuth.

Configuring OAuth

In the **Configure OAuth** block, enter the Unifier redirect URL in the **Redirect URL** field box. Ensure all other fields are selected as shown in the screen capture, below:

Configure OAuth

Client ID:

Client Secret:

Note: You must keep your Client Secret confidential.

Redirect URI:

Note: The redirectUri specified in your OAuth requests must belong to this list of uris. You can mention multiple uris as comma separated list.

Enabled Scopes

You must enable the scopes that you intend to request through the OAuth protocol. Please limit the scopes that you enable to the minimum set necessary for your application, which is one of the requirements for Certification.

Please [contact support](#) if you need to change which scopes are enabled for your application. ?

Note that only Group Admins can approve OAuth requests that use the ":group" scope modifier, and only Account Admins can approve OAuth requests that use the ":account" scope modifier.

Enabled?	Scope	Modifier	Description
☒	user_read	account	View users In your account
☒	user_write	account	Create or manage users within your account
☒	user_login	account	Login on behalf of any user In your account
☒	agreement_read	account	Access documents & data on behalf of any user In your account
☒	agreement_write	account	Manage the status of documents on behalf of any user In your account
☒	agreement_send	account	Send documents on behalf of any user In your account
☐	widget_read	account	View web forms on behalf of any user In your account
☐	widget_write	account	Create, edit or publish web forms on behalf of any user In your account
☐	library_read	account	View templates and document library on behalf of any user In your account

- 1) Sign in to Unifier.
- 2) Click the **Company Workspace** tab (**Admin** mode).

11

- 3) From the left Navigator, click the company name.
- 4) From the toolbar options, click **Open** to open the **Edit Company** window.
- 5) Click the **E-signatures** tab.
- 6) From the **Default E-Signature Type** drop-down, select **Adobe Sign**.
- 7) Click to select, or check, the **Adobe Sign** block.
- 8) Enter values in the **URL**, **Client ID**, and **Client ID** fields.
- 9) Click **Generate Token**.
- 10) Enter the Adobe Sign login credentials on the pop-up window.
- 11) Click **Test Connection** and select **Active**.
- 12) Click **OK**.

The screenshot shows the 'E-Signatures' tab in a configuration window. At the top, there are tabs for 'General', 'Address', 'Security', 'Contact', and 'E-Signatures'. Below the tabs, the 'Default E-Signature Type' is set to 'AdobeSign'. There are two sections for configuring different signature types: 'DocuSign' and 'AdobeSign'. The 'DocuSign' section is currently inactive, indicated by an unchecked checkbox. The 'AdobeSign' section is active, indicated by a checked checkbox. In the 'AdobeSign' section, the 'Url' field is filled with 'https://.....na2.echosign.com', the 'Client ID' field is filled with 'CBJCHBCAABAAPnDoxO3cSG-InqujBsJA3uXx6MtX', and the 'Client Secret' field is filled with a series of asterisks. The 'Token' field is filled with '3AAABLbqZhC9UmMHjsibfXwom86kfdAY5rmfq02n3BtoRN'. The 'Status' is set to 'Active' with a selected radio button. To the right of the fields are buttons for 'Generate Token' and 'Test Connection'. At the bottom of the window are 'OK' and 'Cancel' buttons.

Default E-Signature Type: **AdobeSign**

☐ DocuSign

Url:

Account Id:

Client ID:

Client Secret:

Token:

Status: ☐ Active ☐ Inactive

☒ AdobeSign

Url:

Client ID:

Client Secret:

Token:

Status: ☒ Active ☐ Inactive

Generate Token

Test Connection

OK Cancel

Copyright

Oracle Primavera Unifier Adobe Sign Configuration Guide

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

Oracle and Java 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, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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 or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 failsafe, 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.

This software or hardware and documentation may provide access to or information on 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. 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.