Partner Guide

FOR ADP AUTHORIZED USERS ONLY

ADP provides this publication “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. ADP is not responsible for any technical inaccuracies or typographical errors which may be contained in this publication. Changes are periodically made to the information herein, and such changes will be incorporated in new editions of this publication. ADP may make improvements and/or changes in the product and/or the programs described in this publication.

CONTENTS

Overview

Start the process to become an ADP® Marketplace Partner by applying for a partner account. Your application will be reviewed by ADP's Sales, Security, and Legal teams to prepare your app for the ADP Marketplace.

Applying for a Partner Account

To apply for a partner account, do the following:

1. Go to the ADP Marketplace Partner Web site.
2. Click **JOIN NOW** to access the **Signup** form.
3. On the **Register** page, enter your email address. Then, click **NEXT**.
4. On the **Partner Application** form, enter the appropriate information about yourself, your company, and your products.

If your organization has already undergone security reviews, your organization may qualify for a security review fast-track or security pre-approval. If either applies, provide the appropriate documentation when submitting your partner application, Then, do the following:

1. Review the Mutual Non-Disclosure Agreement on the Partner Application. Then, click the check box to agree.
2. Click **COMPLETE REGISTRATION**.

After you submit your partner application, you may receive a call from an ADP Business Development Representative. The representative will check your organization from a market, product, and services perspective. This call can last about 30 minutes. If there is a mutual benefit in your solution being listed on the ADP Marketplace, your ADP Business Development Representative will guide you through the process of getting through ADP's Security Review processes.

Partner Security Review

If your organization does not qualify for a security review fast-track or security pre-approval, the ADP Security team will work with you to understand your security measures and get you onboard as quick as possible. This process starts with you completing ADP's questionnaire and submitting other relevant documentation. ADP's questionnaire, built on ISO 27001, allows ADP to examine your security program. The questionnaire is available here.

The following is other documentation that will help expedite your review:

- **Policy Documentation** - For example, the following:
  - Security Policy
  - Data Retention and Destruction Policy
  - Encryption Policy
  - HR Policy
  - Computing Standard/Policy
  - Cloud Security Policy
- **Technical Documentation** - For example Data Flow Diagrams, Architectural Diagrams, and so on

Next Steps

1. Review the Security Assessment Process and reach out to the ADP team if you have questions.

2. Provide the requested documentation, such as the following:
    - Submitting the documents described in the following sections.
    - Sending in supporting documentation, and/or completing the questionnaire.
3. To discuss the requirements and explain your security program, schedule a call with the ADP Security team.
4. Receive feedback from the ADP Security team about ADP's assessment of your program. If there are any gaps, the ADP Security team will review them and work with you to develop a plan and timeline for the remedy.
5. As your partnership with ADP grows over time, the ADP Security team will continue to work with you to help you understand changes to ADP's security requirements.

Security Review Completion

ADP looks forward to partnering with you. If you need additional help with communicating your security program, you can reach the ADP Security team at GSO_Third_Party_Risk_Management@ADP.com.

ADP Partner Legal Agreement

To become an ADP Marketplace Partner, you need to review and sign a legal contract with ADP. If you intend to do the following:

- Distribute apps that access ADP data - Use Single Sign-On (SSO).
- Offer your app to be purchased on the App Store - You need to sign a Developer Participation Agreement.

ADP Partner Onboarding

If your organization has passed ADP's initial assessment and security review and signed the ADP Marketplace legal agreement, our Partner Onboarding team will work with you to create and configure your ADP Partner account. Depending on how you will be using the ADP Marketplace (referral or e-commerce), your organization may also need to be set up in billing.

Finally, the Partner Onboarding team will send you login credentials for accessing your account and publishing your apps on the ADP Marketplace.

Security Pre-Approval

In some cases, ADP will accept a prior external security review in lieu of performing ADP's own assessment.

ADP recognizes many organizations have similar, robust security programs and may have already undergone other stringent security reviews. ADP takes into consideration several external review types, and in some cases can utilize that review in lieu of performing another detailed assessment. If your organization has undergone one of the following assessments, provide the appropriatedocumentation when submitting your partner application:

- **PCI-DSS Assessment** (Find a qualified QSA here)
- **Executive Summary from a Pen Test and Vulnerability Assessment** (from a qualified external reviewer)
- **SOC2 Type II Report** (from a qualified external reviewer)
- **An Independent Third Party Audit Report** (from a qualified external reviewer for a specific regulation/requirement/law)

Security Review Fast Track

In some cases, ADP will consider a company's security programs and prior external reviews to expedite ADP's security review process.

ADP recognizes that some organizations have security programs and have other important external attestations. We will take into consideration several external review types, and utilize that review to help expedite another assessment. If your organization has undergone one of the following assessments, provide the appropriate documentation when submitting your partner application:

- **Code Review Report** (find details here)
- **ISO 27001 Certification** (find an accredited certification body here)

Beginning the Partner Security Certification Review Process

NOTE: Partner security certification is not necessary if you are only developing a Single Sign-On (SSO) integration with ADP.

To prepare your app for the ADP Marketplace, it must go through ADP's security certification review process. Our corporate security team will perform an assessment of your app to make sure it follows our strict security policies. Your app will be approved for publishing to the ADP Marketplace after it successfully passes ADP's tests for security vulnerabilities.

To begin the security certification review process, do the following:

1. An ADP representative from the Security Assessment team will contact you to setup a security consultation appointment.
2. In this meeting you will review the security assessment process and discuss expectations with a Security Assessor.
3. In this meeting, the Security Assessor will also request that you provide, with your partner application, the following independent third-party audit reports about your information security controls.
   NOTE: The following documents allow your app to be pre-approved as a referral app:
    - ISO 27001 Certificate
    - SSAE16 SOC 2 Report (includes cloud service provider and other information) or a PCI DSS Assessment.

4. If externally executed audit reports are not available, you must complete the ADP vendor questionnaire and submit the supporting documentation requested.
   NOTE: For more details about the partner review process, visit ADP's Partner Security Requirements page on the ADP Developer Community web site.

Completing App Security Certification

Your app must undergo both a Static App Security Test (SAST) and a Dynamic App Security Test (DAST) before it can be approved for publishing to the ADP Marketplace. You may choose to have ADP run the tests internally or you may select an independent third-party vendor approved by ADP to perform the tests externally.

NOTE: To understand and avoid security flaws that may impact your app, review “Top Ten Application Security Risks” on the Open Web Application Security Project (OWASP) web site.

Tests Performed by ADP

To have ADP run the tests on your app, do the following:

1. Submit and complete the ADP SAST/DAST Excel form found here before ADP begins the testing process.
2. The internal security team informs you about any prerequisites required to perform the tests. These prerequisites may include programming languages supported, pre-defined LOC count, and any special or specific checks required for the app (PCI / HIPAA, and so on).
3. The internal security team creates accounts in Checkmarx for you. Checkmarx is a product used by ADP to test your app.
4. For ADP to execute the SAST scan, you must upload the source code to the portal set up for your project.
5. For ADP to perform the DAST scan and execute a penetration test, you must provide ADP access to your environment.
6. The internal security team performs the DAST and uses Checkmarx to execute the SAST.
7. After the scanning tests have been completed, the internal security team forwards a report (in PDF format) and risk score to you.
8. You must remediate all critical and high findings in the report with explanations and justifications to remove any false positives.
9. Any vulnerabilities reported as being false positives are reviewed by ADP internally. ADP will then provide you an explanation and justification of the vulnerabilities with results.
10. After ADP reviews the scan results and your app successfully passes the tests, it is approved for integration into the ADP Marketplace.

IMPORTANT: If your app fails any tests, ADP will review the open areas with you and discuss the remediation required.

Tests Performed by an ADP-Approved Vendor

If you want an independent third-party vendor (approved by ADP) to perform the tests on your app, do the following:

1. Follow the vendor’s instructions to begin the testing process.
2. The vendor performs the tests and then submits the results to you for remediation.
3. You must remediate all critical and high findings identified by the vendor.
4. You must provide ADP a copy of the Executive Summary report from the third-party vendor. It must include proof that there are no open critical or high findings and describe a plan of action for remediation of all medium findings.
5. After ADP reviews the scan results and your app successfully passes the tests, it is approved for integration into the ADP Marketplace.

IMPORTANT: If your app fails any tests, ADP will review the open areas with you and discuss the remediation required by you and/or the vendor.