Becoming an ADP Marketplace Partner and understanding ADP Marketplace Security

Overview

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

Use the following procedure to apply for a partner account.

1. Go to the ADP Marketplace Partner website.
2. Click **JOIN NOW** to access the Signup form.
3. On the Register page, enter your email address, and then click **NEXT**.
4. In 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 security review fast-track or security pre-approval. If either applies, please provide the appropriate documentation when submitting your partner application.

5. Review the Mutual Non-Disclosure Agreement on the Partner Application and then click the checkbox to agree.
6. Click **COMPLETE REGISTRATION**.

After you submit your partner application, you may receive a call from an ADP Business Development Representative. The representative will evaluate your organization from a market, product, and services perspective. This call normally lasts about 30 minutes. If it is determined that there will be 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 our Security Review processes.

PARTNER SECURITY REVIEW

If your organization does not qualify for security review fast-track or security pre-approval, our security team will work with you to understand your security measures and get you onboarded quickly. This process starts with you completing our questionnaire and submitting other relevant documentation. Our questionnaire, built on ISO 27001, allows ADP to vet your security program. The questionnaire is available here.

Other documentation that will help expedite your review:

- **Policy Documentation** (ex: Security Policy, Data Retention and Destruction Policy, Encryption Policy, HR Policy, Computing Standard/Policy, Cloud Security Policy, et al)
- **Technical Documentation** (Data Flow Diagrams, Architectural Diagrams, et al)

Next Steps

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

2. Provide the requested documentation (submit the documents listed below, send in supporting documentation, and/or complete the questionnaire)
3. Schedule a call with our security team to discuss the requirements and explain your security program.
4. Receive feedback from our security team about our assessment of your program. If there are any gap areas, our team will review them with you and work with you to develop a plan and timeline for the required remediation.
5. As your partnership with ADP grows over time, our security team will continue to work with you to help you understand changes to our security requirements.

Security Review Completion

ADP looks forward to partnering with you. If you need additional help 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 will need to review and sign a legal contract with ADP.

- If you intend to distribute apps that access ADP data, use single sign-on (SSO), or can be purchased on the app store, you will need to sign a Developer Participation Agreement.

ADP PARTNER ONBOARDING

Congratulations! 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 upon how you will be using the ADP Marketplace (referral or e-commerce), your organization may also be set up in billing.

Finally, the onboarding team will send you login credentials for accessing your account and publishing your apps in the ADP Marketplace.

Security Pre-Approval

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

We recognize that many organizations have robust security programs similar to ADP and may have already undergone other stringent security reviews. We will take into consideration several external review types, and in some cases, can utilize that review in lieu of performing our own detailed assessment. If your organization has undergone one of the following assessments, please provide the appropriate documentation 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.

We recognize 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 our detailed assessment. If your organization has undergone one of the following assessments, please provide the appropriate documentation when submitting your partner application.

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

How do I begin 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 our 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 our tests for security vulnerabilities.

Use the following procedure to begin the security certification review process.

1. An ADP representative from the Security Assessment team will contact you to setup a security consultation appointment.
2. You will review in this meeting the security assessment process and discuss expectations with a Security Assessor.
3. The Security Assessor will also request in this meeting that you provide (with your partner application) the following independent third-party audit reports about your information security controls. **Note:** This information will 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 our Partner Security Requirements page on the ADP Developer Community website.

How do I complete 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) website.

Tests Performed by ADP

Follow the procedure below to have ADP run the tests on your app.

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, etc.)
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) perform the tests on your app, use the following procedure.

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

•