Contents

Safeguarding the Registration Process ................................................................. 2
   Key Security Updates .......................................................................................... 2
Employee Registration Options ............................................................................ 2
   Personal Registration Codes (Recommended) ....................................................... 2
   Organizational Registration Code ...................................................................... 3
   Accessing the ADP® Security Management Service .......................................... 3
Viewing Your Identity Verification Options .......................................................... 4
Personal Registration Codes (Updated) ................................................................. 6
   One-Time Setup to Automate the Distribution of Personal Registration Codes (New!) 6
   On-Demand Distribution of Personal Registration Codes (Already Available) .......... 6
Updating Email Address and Mobile Phone Number ............................................. 7
   Issuing Codes to Users ....................................................................................... 7
   Issuing Code to Screen ..................................................................................... 9
   Issuing Codes to Unlock Registration ................................................................. 9
Using the Organizational Registration Code ......................................................... 11
   The Two New Types of Additional Verification ............................................... 12
Reference Information .......................................................................................... 14

Disclaimers:

- The employee registration process does not apply to administrators and federated users.
- Previously registered users are not impacted by these security enhancements and do not need to re-register.
- The employee registration process does not apply to administrator-only services such as General Ledger Interface, ADP Reporting, and Payroll QuickView.
- The registration process outlined in this document does not apply to RUN Powered By ADP® Employee Access®.
- The registration process will vary slightly for employees registering for ADP Retirement Services on the participant website at www.mykplan.com.
Safeguarding the Registration Process

ADP is committed to protecting the privacy of your users and their personally identifiable information. To assist us in meeting that commitment, your users must register with us before using ADP services.

Key Security Updates

The employee registration process has been enhanced with additional security features to help prevent identity fraud:

- Registering users who enter an organizational registration code must complete the Google™ reCAPTCHA challenge.
- Registering users may be required to provide additional identity verification based on your organization’s verification setting.
  
  **Note:** Users can request a code to be sent to their unique mobile phone number or email address and enter it within 15 minutes to complete the verification.

- Registering users who enter incorrect identity information and repeatedly fail the registration process will be locked out and require assistance from their administrator.

Employee Registration Options

Your organization can set up the employee registration process for your unregistered users and select to use personal registration codes, which are more secure, or the organizational registration code.

Personal Registration Codes (Recommended)

Personal registration codes offer the most secure method to control access to your organization’s ADP services and several security advantages. They are:

- Randomly generated alphanumeric codes (for example, 9a7b632f)
- Uniquely associated to the individuals to whom they are issued
- Not freely available; you must issue them to your users/new hires
- Set to expire in 15 days or as soon as they are used, but can be reissued easily by an administrator
- Distributed securely in an email from ADP (SecurityServices_NoReply@adp.com) to the unique email address, or sent in a text message from ADP to the unique mobile phone number on file, or provided by your administrator in a separate communication
Organizational Registration Code

An organizational registration code consists of your client ID, a hyphen, and a code that you choose. For example, if your client ID is MyClientID and the code you choose is Alabama2235, users would enter MyClientID-Alabama2235 during registration.

For your organization’s protection, you **MUST** take the following precautions:

- Set up your organizational registration code to be meaningful and difficult to guess. For example, “MyClientID-UniqueAlphanumericCode” where the numbers and letters can represent a significant event, location, name, or some information known only within your organization.
- Treat the code as a confidential asset and do not distribute it to anyone outside of your organization.
  - Distribute the organizational registration code to your new hires in a welcome packet or custom email.
  - If necessary, display the organizational registration code on your secure intranet portal—not the public internet.
- Assign an Employee/Associate ID during the hiring process and require your users to enter the Employee/Associate ID during registration.
- Change the organizational registration code every three months.

Accessing the ADP® Security Management Service

Log on to your ADP service and use the menu option to navigate to the ADP Security Management Service. Alternately, go to [https://netsecure.adp.com](https://netsecure.adp.com) and log on as an administrator.
Viewing Your Identity Verification Options

Go to Setup > Profile > Identity Verification Options to view your organization’s identity verification options. This task does not apply to users with user master, user administrator, and product user security roles.

If changes are needed, contact your ADP representative for assistance.
On your behalf, your ADP representative selects one of the two options:

**Option 1:** Personal Registration Code or the Organizational Registration Code

ADP recommends the use of either the Associate ID or Employee ID when using the options of Social Security number and date of birth. Associate ID / Employee ID are secure pieces of personal information known to the individual, but generally unknown to other users and not advertised elsewhere within or outside of your organization.

**(OR)**

**Option 2:** Personal Registration Code as the exclusive identity verification option

Your users will be prompted for one piece of personally identifiable information available in our records. Users **cannot** use the organizational registration code for registration.
Personal Registration Codes (Updated)

Personal registration codes offer the most secure method to control access to your organization’s ADP services. Your organization can use one of the two options:

One-Time Setup to Automate the Distribution of Personal Registration Codes (New!)

To support your administrators and simplify the process of issuing these codes, ADP is pleased to offer the ability to automatically issue Personal Registration Codes to your new associates and terminated users. On the Setup > Profile > Personal Registration Code page, security masters and security administrators can select this option and the time frame to issue the codes. Once set up, new associates and/or terminated users with a unique email address on file will receive an email with the personal registration code that is valid for 15 days.

- For your new associates, administrators can select to have the codes issued immediately after the new associate’s data has been entered in the ADP service or send it up to 30 days later.
- If your organization uses ADP’s services to manage the employment status of your users, administrators can select the option to issue the codes to terminated users immediately or send it up to 30 days later.

Important: To take advantage of this feature, your security master/administrator must select this option for your organization and include unique work/personal email addresses for your new associates in your ADP service.

On-Demand Distribution of Personal Registration Codes (Already Available)

Administrators with security master, security administrator, and user master security roles can view the code status and reissue codes from the People > Personal Registration Code page. In addition, administrators can support users with non-unique email addresses by issuing codes to the associate’s mobile phone number. For a user without a mobile number on file, an administrator can view and share the code with the specific user in a separate communication.

This task cannot be performed by user administrators and product users.

Use one or more search options available on the page to find the list of unregistered users.

<table>
<thead>
<tr>
<th>Select the Email Status</th>
<th>Select the Code Status</th>
<th>Select the Lock Status</th>
<th>Select the Employment Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All</td>
<td>• All</td>
<td>• All</td>
<td>• All</td>
</tr>
<tr>
<td>• With Unique Email Address</td>
<td>• With Active Code</td>
<td>• Locked</td>
<td>• Active</td>
</tr>
<tr>
<td>• With Non-Unique Email Address</td>
<td>• With Expired Code</td>
<td>• Temporarily Locked</td>
<td>• Separated</td>
</tr>
<tr>
<td>• Without Email Address</td>
<td>• None</td>
<td>• Unlocked</td>
<td></td>
</tr>
</tbody>
</table>
Updating Email Address and Mobile Phone Number

Find users without an email address or with non-unique email address and enter a unique email address for each user and click Save to update the users’ record.

If the user does not have a unique email address, update the user’s record with a unique work/personal mobile number.

Issuing Codes to Users

Personal registration codes can only be issued to users with unique work/personal email addresses or unique work/personal mobile phone numbers within your organization.

Use the search options on the page to find the users. Select to view the list or users with either the Work Email, Mobile Number or the Personal Email, Mobile Number.
Select one or more users individually to issue personal registration codes. You can also “Select all…users” to include all users in the search results.

- When viewing the Work Email, Mobile Number, select **Issue Codes > Work Email Address / Work Mobile Number** (SMS text message).
- When viewing the Personal Email, Mobile Number, select **Issue Codes > Personal Email Address, Or Personal Mobile Number** (SMS text message).

**Note:** Only users with a unique email address in your organization will receive an email from ADP ([SecurityServices_NoReply@adp.com](mailto:SecurityServices_NoReply@adp.com)). Similarly, when you issue codes to work/personal mobile number, only users with unique mobile phone numbers will receive the code in a text message from ADP.

Administrator issued personal registration codes are valid for 15 days from the date of issue.
Issuing Code to Screen

Occasionally you may encounter users without an email address/mobile phone number or users who have difficulty receiving the email/text message with the registration code due to issues with their email/cellular provider, network connection, incorrect email/mobile number on file, etc.

Use the Email Status search options on the page to find the user. Select the user and select View Codes on Screen option to display the personal registration code on the page.

![Image of ADP interface](image)

**Important:** Distribute the personal registration code (displayed on the screen) to the specific user for whom it has been issued in a separate and secure internal communication along with the registration URL. As a security measure, codes will be hidden (but remain active) when you navigate away from the page.

Issuing Codes to Unlock Registration

Users who enter incorrect identity information during registration will fail the registration process. If your users repeatedly attempt to register with incorrect identification, they will be locked out of the registration and require assistance from their administrator.

Once locked, users must be issued a personal registration code by an administrator to complete the registration. Use the Locked Status search option to find users with locked status and issue a personal registration code to unlock the registration process.

**Security Tip:** Be sure to verify the identity of the user requesting assistance before you issue a personal registration code. On the People > Personal Registration Codes page, find the user and hover-over the user’s name to view some identity information that you can use for verification.
Next Step

Your users receive an email with the personal registration code from sender SecurityServices_NoReply@adp.com:

Welcome, SALLY BRUDER

Register today to get access to ADP services. Use the following personal registration code when you register.

Note: This personal registration code is valid for 15 days from the date of issue.

Your Personal Registration Code: bcgy0sba

Before you begin the registration process, make sure that you have the internet address (URL) of ADP's Internet service(s). If you do not have this information, Contact your organization's administrator for assistance.

Instructions:

1. Open your Internet browser.
2. Use the URL provided by your organization's administrator to access your ADP service web site.
3. Enter your personal registration code and follow the instructions on the site.
   Note: Do not use previously issued personal registration codes, as they are expired and are not valid.

Have questions or need assistance? Contact your organization's administrator for assistance.

This email has been sent from an automated system. DO NOT REPLY.
Message ID: D1-08C-A06-18CR98

Important: You must provide the URL of your ADP service to your users in a separate and secure internal communication.
Using the Organizational Registration Code

Your security master, security administrator, or your ADP representative can establish the organizational registration code for your organization.

Go to Setup > Profile > Settings and set up the organizational registration code. The new code becomes effective immediately and must be updated regularly to prevent misuse.

Additional Verification with Organizational Registration Code

As part of ADP’s commitment to help safeguard your users from fraud due to identity theft, identity verification options based solely on the Social Security number, without an Employee ID or Associate ID, will now require additional verification.

Treat your registration code as confidential and update it regularly!
The Two New Types of Additional Verification

Depending on your organization's verification setting, for additional verification, users may be required to enter a code sent to their unique email or mobile phone number on file or answer up to 4 identity questions generated from public records and other commercially available data sources.

Important: If your organization requires users to provide either an Associate ID or Employee ID during registration, additional verification is optional.

Type 1: Enforcing Email Confirmation

This form of verification requires a registering user to enter a code sent to their email or mobile phone number on file to confirm their access to the email/phone and prove their identity. For a user to use this form of verification, their email or mobile phone number must be unique within your organization.

To determine which users share email addresses, run the Associate Information Report with the additional fields of work email and personal email selected. For your unregistered users, unique email addresses and mobile phone numbers must be included in the user information shared with ADP or can be updated on the Personal Registration Code page.

Note: If your identity verification option includes either an Employee ID or Associate ID, you can also take advantage of this additional verification. Contact your ADP representative for
assistance. Users whose emails or mobile phone number are shared within your organization must contact their administrator to request a personal registration code and enter the administrator-issued code. In addition, email uniqueness will be enforced when you manage your users and when your users update their contact information.

**Type 2: Requiring Users to Answer Identity Questions**

This form of verification requires your users to answer up to 4 identity questions generated from public records and other commercially available data sources.

Users must respond within 30 seconds to each question to prove their identity.

**Note:** If you prefer not to offer this option for your users, you can contact your ADP representative to turn it off. If your organization relies on the use of Social Security number for identity verification and you request this option to be turned off, your users will be required to enter a code sent to their unique email on file or contact an administrator to request a personal registration code.

These identity questions and their answer choices are generated from public records and other commercially available data sources.

They are not used for any purpose other than to verify the identity of your registering user and are not shared with your organization.
Reference Information

On the **Security Management Service > Home Page > Resources** section, access the registration quick reference cards and customize them for your organization, if needed.

For your quick reference, current version and recently enhanced registration process documents are available on the Resources section. Your registration experience may vary based on the ADP services purchased; however, the overall process remains unchanged. In addition, you can customize the letter to encourage registration by including the URL of your ADP service, registration information, and provide it to your unregistered users.

**ADP appreciates your support and cooperation to protect your organization, your users, and your data.**