



Increased Security and Convenience Registration: You Have Options!

Dear client,

Now more than ever, people have concerns about fraudsters stealing their Personal Identifiable Information (PII), such as Social Security Numbers, and committing identity theft. Understandably, your employees may not want to use their PII data to register, and your company may need to adopt more secure and effective registration options. Here are the alternative options that ADP[®] has to offer, all of which you can use today:

Personal Registration Codes

With this option, each individual is assigned a unique, randomly generated, alphanumeric Personal Registration Code (PRC) with which to sign up for an account. For increased security, these codes expire after a limited period of time.

ADP distributes these codes by email to a unique work/personal email on file. You can also provide the codes to each user verbally or on paper. Depending on the services you use, the codes could also be sent automatically to your employees when they join or leave your company.

Organization Registration Codes + Associate/Employee ID

If you must use an Organizational Registration code, we recommend that you use a unique identifier known only within your company (Associate ID or Employee ID) for each individual, if you include that information in your ADP service.

ADP Federated Single Sign-On (SSO)

Today, 22 million users log on to their company network and click a link on their internal portal to access ADP services without needing an ADP-issued user ID and password. This option provides your company complete control and allows you to eliminate the employee registration process altogether.

Federated SSO is easy to set up and supports popular identity technology providers, such as Okta[®], Microsoft[®], and OneLogin[™]. Refer to the [ADP Federation Guide](#) document and contact your ADP representative to learn about the options available to you or [order it from ADP Marketplace](#).



ADP is committed to protecting your organization, your users, and your data and thanks you for your support!

Table of Contents

Registration Options for Your Organization 3

Option 1 (Most Secure): For associates (newly added to your ADP system) and terminated users (with employment status on file) 3

Option 2 (Very Secure): Unique Employee/Associate ID 3

Option 3 (Least Secure): Social Security Number (USA) 4

Safeguarding the Registration Process 6

Key Security Updates 6

Employee Registration Options 6

Personal Registration Codes (Recommended) 6

Organizational Registration Code 6

Accessing the ADP® Security Management Service 7

Viewing Your Identity Verification Options 7

Personal Registration Codes (Updated) 8

One-Time Setup to Automate the Distribution of Personal Registration Codes (New!) 8

On-Demand Distribution of Personal Registration Codes (Already Available) 8

Updating Email Address and Mobile Phone Number 9

Issuing Codes to Users 9

Issuing Code to Screen 9

Issuing Codes to Unlock Registration 10

Using the Organizational Registration Code 12

A New Type of Additional Verification 13

Registration Options for Your Organization

The information your organization has on file for your employees and the information available in your ADP services for each employee may slightly vary. To help protect your organization's information from fraud, ADP's registration process requires reliable pieces of information so we can confirm the identity of the user and allow access to the requested service.

Based on the information (Legal ID, Employee/Associate ID, unique email address, unique mobile number, personal identity information) that your organization shares with ADP, please select an option that supports your organization's registration needs.

You can use a combination of these options to address the needs of your organization.

Option 1 (Most Secure): For associates (newly added to your ADP system) and terminated users (with employment status on file)

Before using this option: Check with your ADP representative to confirm that your ADP service supports entering and maintaining employment status (hire and termination dates). Be sure to select the [one-time setup option to automate the personal registration codes](#) before you begin onboarding your users. Include unique email addresses and/or mobile phone numbers for your users.

Data Available ¹			Registration Options		
Unique emails/ mobile phones	Employee / Associate ID	Social Security numbers	Personal Registration Codes	Organizational Registration Code + Employee / Associate IDs ²	Organizational Registration Code + Social Security Numbers
✓	✓	✓	Automatically issued to email ⁴	During registration, employee can get and enter code sent to their unique emails/mobile phones on file ³	During registration, employee can get and enter code sent to their unique emails/mobile phones on file ³
✓	✓		Automatically issued to email ⁴	During registration, employee can get and enter code sent to their unique emails/mobile phones on file ³	
✓		✓	Automatically issued to email ⁴		During registration, employee can get and enter code sent to their unique emails/mobile phones on file ³

Notes:

¹ All data elements must already exist in users' records at time of registration

² Requires employees to know their ID and treat it as confidential

³ During registration, employee can request a personal registration code to their unique email/mobile phone on file

⁴ Bulk option is available for sending to multiple users at one time

Option 2 (Very Secure): Unique Employee/Associate ID

Employee Registration Options

Data Available ¹			Registration Options		
Unique emails/ mobile phones	Employee / Associate ID	Social Security numbers	Personal Registration Codes	Organizational Registration Code + Employee / Associate IDs ²	Organizational Registration Code + Social Security Numbers
✓	✓	✓	Admin-issued to emails ⁴	During registration, employee can get and enter code sent to their unique emails/ mobile phones on file ³	During registration, employee can get and enter code sent to their unique emails/ mobile phones on file
✓	✓		Admin-issued to emails ⁴	During registration, employee can get and enter code sent to their unique emails/ mobile phones on file ³	
	✓	✓	Admin views code on screen and shares the code verbally or via manual email or paper-based communication	Employee/Associate ID	
	✓			Employee/Associate ID	

Notes:

¹ All data elements must already exist in users' records at time of registration

² Requires employees to know their ID and treat it as confidential

³ During registration, employee can request a personal registration code to their unique email/mobile phone on file

⁴ Bulk option is available for sending to multiple users at one time

Option 3 (Least Secure): Social Security Number (USA)

Data Available ¹				Registration Options		
Hire and term dates	Unique emails/ mobile phones	Employee / Associate ID	Social Security numbers	Personal Registration Codes	Organizational Registration Code + Employee / Associate IDs ²	Organizational Registration Code + Social Security Numbers
	✓		✓	Admin-issued to emails ⁴		During registration, employee can get and enter code sent

Employee Registration Options

						to their unique emails/ mobile phones on file
			✓	Admin views code on screen and shares the code verbally or via manual email or paper-based communication		

Important: To comply with Canadian Legal requirements, Canadian SIN or other Legal ID should not be collected, entered, or stored in this field in ADP systems.

Notes:

- ¹ All data elements must already exist in users' records at time of registration
- ² Requires employees to know their ID and treat it as confidential
- ³ During registration, employee can request a personal registration code to their unique email on file
- ⁴ Bulk option is available for sending to multiple users at one time

Disclaimer: Employee registration does not apply to admin-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.

Please refer to the [New Employee Registration quick reference card](#) for details.

If you prefer, please type:

https://support.adp.com/netsecure/pages/pub/docs/9.0/en_us/ADP_Employee_Self_Service_Registration-vrkf.pdf

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 (SecurityServicesNoReply@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> 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.

The screenshot shows the ADP Security Management Service interface. At the top, the ADP logo is on the left, and the text 'Welcome, Client Admin | CAdmin@jyotest | Security Master' is on the right. Below this is a navigation bar with 'Home', 'Myself', 'People', 'Setup', and 'Reports'. The main content area is titled 'Profile' and shows the client name 'jyotest', 'Client ID: jyotest', and 'Status: Active'. There are three tabs: 'Organizational Information', 'Settings', and 'Identity Verification Options'. The 'Identity Verification Options' tab is active. Below the tabs, there is a heading 'To verify their identity and register with our organization, employees must use:' followed by three radio button options: 'Personal Registration Code', 'Personal Registration Code or the Organizational Registration Code' (which is selected), and 'Information from their Pay/Earnings statement or W-2 and validate against an ADP service'. Below this, there is a section 'When using the Organizational Registration Code, I want all users:' with two radio button options: 'To provide the same information' and 'To choose between two combinations' (which is selected). There are three columns of verification options, each with a green checkmark: 'Associate ID' and 'Employee ID' in the first column; 'SSN/FEIN/ITIN (Full 9 digits)' and 'SSN/FEIN/ITIN (Last 4 digits)' in the second column; and 'Full Date of Birth (Month, Day, and Year)' and 'Partial Date of Birth (Month and Day)' in the third column. An 'Add Combination' button is located below these columns. Under 'Saved Combination(s):', there is one saved combination: 'Associate ID (Employee ID) + SSN/FEIN/ITIN (Full 9 digits) + Full Date of Birth (Month, Day, and Year)'. Below this, there is a section 'When using the Organizational Registration Code, additional verification may be required during registration.' with two bullet points: 'Your users with unique email address on file can be required to retrieve and enter a personal registration code.' and 'Your users who do not have a unique email address may be allowed to answer identity questions.' At the bottom, there are two checkboxes: 'Enforce email confirmation during registration for all users' and 'Allow my users to answer identity questions generated from public records'.

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. In Security Management Service, 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.

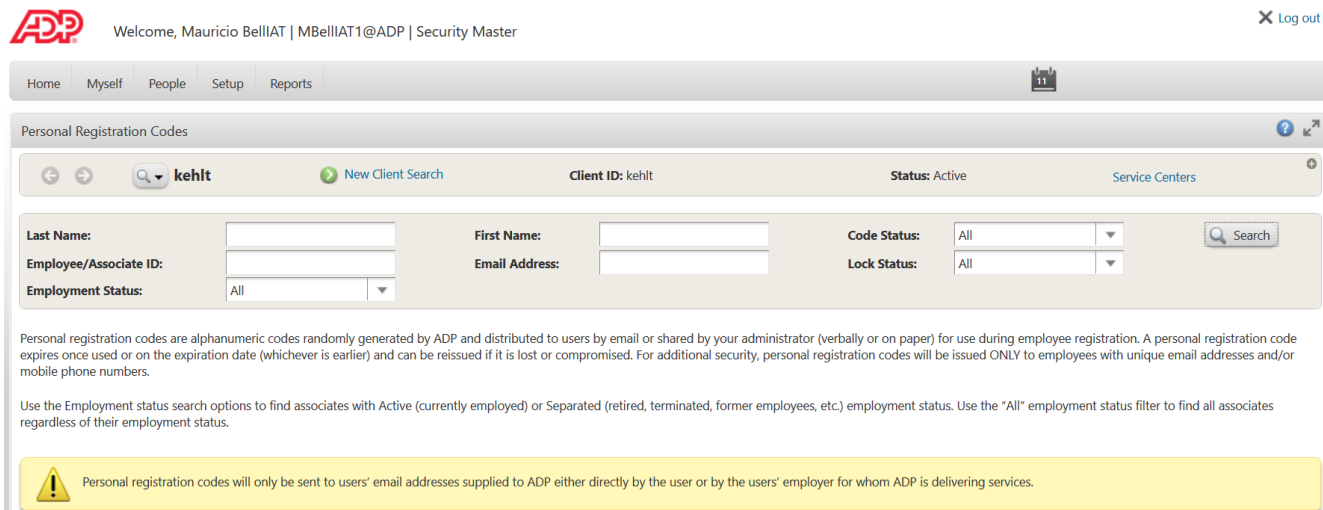
This task cannot be performed by user administrators and product users.

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

Select the Email Status	Select the Code Status	Select the Lock Status	Select the Employment Status
<ul style="list-style-type: none">• All• With Unique Email Address• With Non-Unique Email Address• Without Email Address	<ul style="list-style-type: none">• All• With Active Code• With Expired Code• None	<ul style="list-style-type: none">• All• Locked• Temporarily Locked• Unlocked	<ul style="list-style-type: none">• All• Active• Separated

Updating Email Address

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.



ADP Welcome, Mauricio Belliat | MBelliat1@ADP | Security Master X Log out

Home Myself People Setup Reports 11

Personal Registration Codes ?

kehlt New Client Search Client ID: kehlt Status: Active Service Centers

Last Name: First Name: Code Status: All

Employee/Associate ID: Email Address: Lock Status: All

Employment Status: All

Personal registration codes are alphanumeric codes randomly generated by ADP and distributed to users by email or shared by your administrator (verbally or on paper) for use during employee registration. A personal registration code expires once used or on the expiration date (whichever is earlier) and can be reissued if it is lost or compromised. For additional security, personal registration codes will be issued ONLY to employees with unique email addresses and/or mobile phone numbers.

Use the Employment status search options to find associates with Active (currently employed) or Separated (retired, terminated, former employees, etc.) employment status. Use the "All" employment status filter to find all associates regardless of their employment status.

! Personal registration codes will only be sent to users' email addresses supplied to ADP either directly by the user or by the users' employer for whom ADP is delivering services.

Issuing Codes to Users

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

Use the search options on the page to find the users. Select to view the list of users with either the Work Email or the Personal Email.

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, select **Issue Codes > Work Email Address**.
- When viewing the Personal Email, select **Issue Codes > Personal Email Address**.
- **Note:** Only users with a unique email address in your organization will receive an email from ADP (SecurityServicesNoReply@adp.com).

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 or users who have difficulty receiving the email with the registration code due to issues with their email/cellular provider, network connection, incorrect email 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.

The screenshot shows the ADP Security Master interface. At the top, there is a navigation bar with 'Home', 'Myself', 'People', 'Setup', and 'Reports'. A search bar is on the right. The main content area is titled 'Personal Registration Codes' and contains several search filters: Last Name, First Name, Employee/Associate ID, Email Address, Employment Status, Code Status, and Lock Status. A yellow warning banner states: 'Personal registration codes will only be sent to users' email addresses supplied to ADP by their employer for whom ADP is delivering services.' Below this, a table shows one user selected: 'Flores, Barbara' with business email 'silvia.gomes@adp.com' and personal email 'bfiores@myemail.com'. A context menu is open over the user's name, with options: 'Issue Personal Registration Codes', 'Work Email Address', 'Personal Email Address', 'View Codes on Screen', and 'Privacy Legal'. A callout box points to the 'Select all 1 users' button, and another points to the 'Issue Personal Registration Codes' menu item.

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`:



Hi John Smith,

Your company IID Zero Company is pleased to provide you an all-inclusive dashboard personalized with your information.

Signing up is easy and gives you secure and convenient means to access your information and services anytime, anywhere.

[Sign Up Now](#)

Can't click on the button above?

See your HR representative for your registration link and use code 06281zd3.

Use this code before it expires on 09/03/2020

This email is sent from an automated system, so please do not reply. 48K-C01-252HVS
ADP and the ADP logo are trademarks of ADP, Inc. ©2020 ADP, Inc.

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.

The screenshot shows the ADP Client Master interface. At the top, it says "Welcome, Client Master | CMaster@kehlt | Security Master". Below this is a navigation bar with "Home", "Myself", "People", "Setup", "Reports", and "Manage Clients". The "Profile" section shows the client name "kehlt" with a green status indicator, address "Carlos Gomes, 1235 Address23243 Old Hamburg 2, CA 12345 US", Client ID "kehlt", Contact Phone, Status "Active", and Location "ISIDDCL04".

The "Settings" tab is selected, showing "Organizational Information", "Settings", "Security Notifications", and "Identity Verification Options". Under "Organization Type", there are two columns: "Available Organization Type" (PARTNER:401K, PARTNER:TestIsabel, PARTNER:MARKETPLACE, PARTNER:TEAMPAY) and "Assigned Organization Type" (CLIENT:CLIENT, PARTNER:WFN). Below this are "Mobile Access for Users" sections for "Enabled Mobile Services" (iPay Statements QA, ADP Workforce Now, W2 Services, Retirement Services, ADP Portal) and "Disabled Mobile Services" (000AAA1, Payroll WorkCenter, MyADP, ADP freedom).

At the bottom, there are fields for "Mobile PIN Login" (Enable), "Mobile Touch ID Login" (Enable), and "Organizational Registration Code" (kehlt - alabama2235). A red callout box points to the "Organizational Registration Code" field with the text "Treat your registration code as confidential and update it regularly!".

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.

A New Type of 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.

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

Enforcing Phone or 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.

Step 2 of 3
Verify

Enter Verification Code

We sent a text with your code to ...8373.
This code is valid for 10 minutes.

Verification Code
123456

Didn't get a verification code? [Resend code](#)

Continue

During registration, a user requests a code to be sent to their unique mobile phone number on file and enters it within 15 minutes in the verification code field.

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.