# ADP Workforce Now®
# Security Guide

Version 2.0-1

# Contents

# Introduction to ADP Workforce Now

ADP Workforce Now® is a Web-based, fully integrated workforce management solution that gives your organization a single point of access to payroll, HR and benefits, and time and attendance information. This secure, easy-to-use solution gives you everything you need to maximize your workforce and communicate with your employees.

ADP Workforce Now is tailored to meet the needs of your business. Therefore, menus and menu options that you see will vary based on your role and the services your company is using.

## About This Guide

As a security master, you have the important task of assigning your employees to the appropriate security groups in ADP Workforce Now. Security groups determine what users can see and do on the site. When setting up security groups, carefully consider employees' job functions and what information employees need to access.

The *ADP Workforce Now® Security Guide* provides concepts and step-by-step instructions for planning and implementing user access security for your company. This guide contains detailed information about assigning employees to security groups, creating custom security groups, setting user permissions (access to specific features in ADP Workforce Now), and defining membership rules.

## Types of Users

ADP Workforce Now has four default types of users:

- **Employee -** views and updates personal information
- **Manager** - supervises employee tasks and manages work events
- **Practitioner** - adds and modifies content related to HR and benefits, payroll, and time and attendance data
- **Portal Administrator** - controls user privileges and the appearance of the ADP Workforce Now Web site

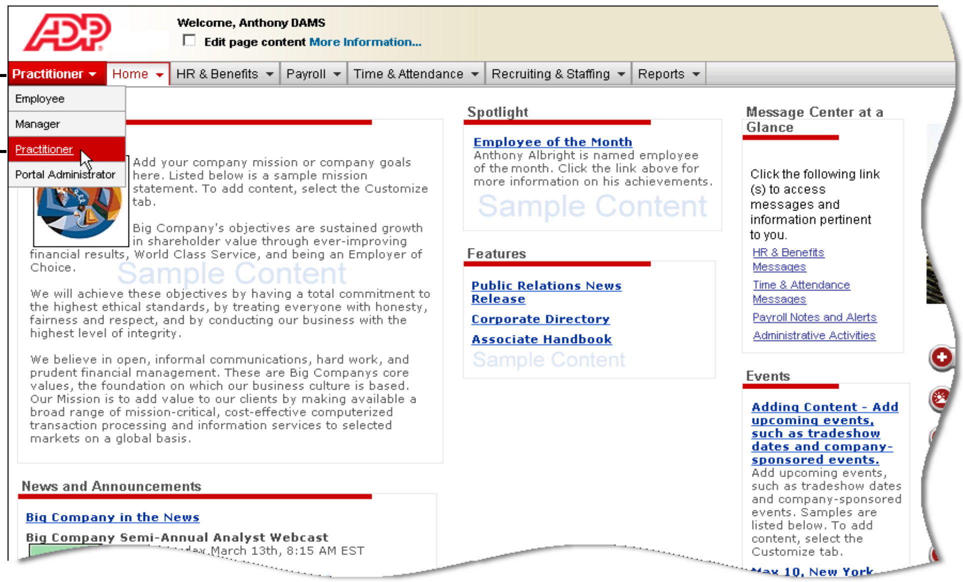
The tasks these users can perform and the pages available to them depend on the ADP modules purchased and the business decisions of the company.

# Navigating the Site

ADP Workforce Now has a customized view based on the company's setup and the role of the user (employee, manager, practitioner, or portal administrator). For example, the menus and menu items that an employee sees are different than those of the portal administrator. To perform security access tasks, make sure the role displayed in the Role Selector is Portal Administrator.

Role Selector

Menu item




# Where to Find Training and Help

You can access portal administrator training by clicking the **Support Center** link in the header at the top right of the site. Clicking this link takes you to the ADP Support Center. In the ADP Support Center, you can find additional information and guides, training materials, and other support information.

For help with a specific task, click ? **(Help)** on individual pages.

## Assistance for Other Users

ADP Workforce Now offers task assistance for employees, managers, and practitioners. Task assistance is an easy-to-use reference that contains information on job-related or personal tasks. For example, managers might use task assistance to learn how to promote an employee. Newly married employees might use task assistance to find out how to make changes to their personal information.

Users can access task assistance from the **Support** link in the header at the top right of the site. The content they see is based on their role.

## Importance of Logging Off

It is important that you log off ADP Workforce Now to ensure that no one else can access your site and view your personal information.

1. In the header at the top right of the site, click **Log Off.**
2. Click **OK** to confirm your action.
3. Close your browser window.

# Chapter 1
# Planning User Access

ADP Workforce Now® provides powerful tools for securing user access to the workforce management information at your organization. Providing thorough security around user access requires a partnership between ADP, who offers expertise in workforce management technologies and methodologies, and your staff, who understand how people need to see and use information at your company. ADP collaborates with key personnel in your organization – most notably, a trusted, high-access user called the security master – to ensure a comprehensive and successful implementation of user access security for your company.

This chapter provides concepts and instructions to support this collaborative process. Your primary task in this chapter is to work with your ADP representative to gather the information necessary so you can set up users and secure user access to ADP Workforce Now.

This chapter covers the following concepts:

- The tasks commonly performed by the security master
- The security hierarchy in ADP Workforce Now
- The forms necessary to gather information and plan user access
- The process of planning user access for your company

# What Does the Security Master Do?

The security master is responsible for:

- Setting up users with the appropriate role in the ADP security management service, the technology that authenticates users and authorizes them to log on to ADP Workforce Now
- Determining exactly how much information users should be able to see and use in ADP Workforce Now
- Working with your ADP representative to properly set up users so they have the appropriate amount of access
- Implementing user access for the ADP Workforce Now Web site
- Implementing user access for the ADP Workforce Now modules your company is using
- Maintaining user access – for example, updating access to content as the user's role changes, resetting passwords, and reissuing digital certificates
- Acting as the main point of contact for staff at your company who use ADP Workforce Now - for example, coordinating questions and inquiries from users and communicating these issues to your ADP representative

Your ADP representative will assist you with getting started with these tasks by providing support and education about how to think about and implement user access.

# The Security Master Setup Call

The Security Master Setup call occurs at the beginning of the planning process. During this virtual meeting, you (as the security master) and your ADP representative share information about the security process and begin to plan user access for ADP Workforce Now.

During this meeting:

- Your ADP representative guides you through the registration process and confirms you can log on to ADP Workforce Now.
- Your ADP representative provides you with important resources you need to complete the planning process. These resources include:
  - ADP Workforce Now Security Template
  - ADP Internet Product Security Registration form
  - *ADP Workforce Now® Security Guide* (the guide you are reading now)

  Your ADP representative shows you where to download these resources. You can also refer to "Security Master Resources" on page 3 for download instructions.
- Your ADP representative explains important concepts, such as the ADP Workforce Now security hierarchy and the process for planning user access.
- You and your ADP representative discuss how to use the ADP Internet Product Security Registration form and Security Template to gather the information needed when setting up user access security in the ADP security management service and ADP Workforce Now.

## After the Call

After this call, you will do the following:

- Review the ADP Workforce Now Security Tour, which covers the concepts discussed in the meeting. (Your ADP representative will provide details on how to access this tour.)
- Work independently to complete the ADP Internet Product Security Registration form for each user and to fill in the Security Template.

Once you have completed these tasks, you and your ADP representative will meet again to talk over questions about implementing user access and to walk through a few examples of setting up user access, based on the information you gathered on the ADP Internet Product Security Registration forms and Security Template.

**Note:** A Security Master Final Review will occur after you have set up user access for your company. This is a check back to make sure that everything has been set up correctly.

## Security Master Resources

During the Security Master Setup call, you and your ADP representative discuss a variety of information to assist you with planning user access. These resources include:

- ADP Workforce Now Security Tour
- ADP Workforce Now Security Template
- ADP Internet Product Security Registration form
- *ADP Workforce Now® Security Guide*

These resources are available on the ADP Workforce Now Web site.

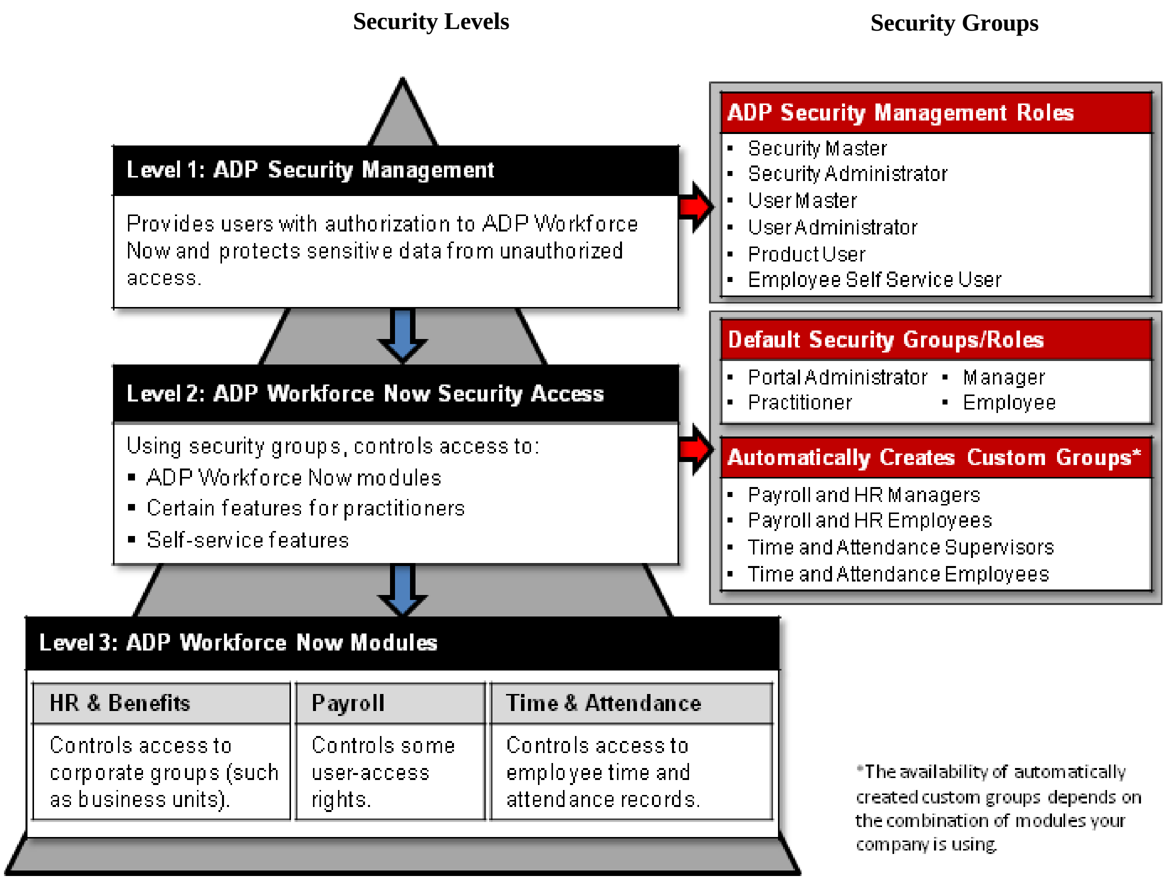
**Note:** You must complete the security management setup and ADP Workforce Now registration before you have access to the page where these resources are located. Your ADP representative will help you to successfully complete these processes. You can also refer to Chapters 2 and 3 of this guide for details.

To access the security master planning resources, follow these steps:

1. Log on to ADP Workforce Now as a portal administrator.
2. Choose **Home >Administrator Resources**.

# The ADP Workforce Now Security Hierarchy

This diagram shows the ADP technologies, process flow, and pertinent user roles required to set up secure user access to ADP Workforce Now. The security hierarchy has three levels: (1) ADP security management service implementation, (2) ADP Workforce Now Web site implementation, and (3) ADP Workforce Now module implementation.



# Levels of the Security Hierarchy

While you, as the security master, begin to work with your ADP representative to plan and implement user-access security, you are granted full access to ADP security management and ADP Workforce Now. Your ADP representative assigns these privileges to you to make sure you can access all content.

**Level 1: ADP Security Management**

***Level 1 Security Management***

During the first level of security implementation, selected users are set up through the ADP security management service, which provides authentication and authorization to ADP Internet services. During this phase,

The security master is established to oversee all additional security administrators, user masters, user administrators, and product users.

- Digital certificates are issued to all security masters, security administrators, user masters, user administrators, and product users to authenticate their identity.

The digital certificate is a "web ID card" that must be installed on the user's computer. The digital certificate provides users with broader access to ADP Workforce Now - for example, the ability to view information about employees other than themselves and to make changes to the way users can access employee records. This extra level of security is needed to ensure the integrity of ADP's services.

As the security master, you have the highest level of access of any digital certificate user and can use any aspect of ADP Workforce Now that your company is using. Other digital certificate users have more restricted rights. For example, they might be able to perform certain functions or access only certain modules of ADP Workforce Now. It is your responsibility as security master to determine exactly what these rights should be and set them up in ADP Workforce Now.

---

**Important:** You do not need to provide digital certificates to all users of ADP Workforce Now. In fact, most users – the self service users – can register with ADP Workforce Now to get a username and password without getting a digital certificate. Self service users typically can view only their own information. ADP Workforce Now managers (also self service users) can access information about the employees who report to them. However, they do not have security privileges and are not able to change the way other users access ADP Workforce Now.

---

**Level 2: ADP Workforce Now Web site**

***Level 2 ADP Workforce Now website***

After the security management setup, the security master sets up digital certificate users with ADP Workforce Now access. Your ADP representative has set up the security master with complete portal administrator privileges, so you can access all content in ADP Workforce Now. During this phase:

- You assign the digital certificate users set up in the security management service to one of the default security access groups (portal administrators and practitioners). Users can be assigned to both groups if they should have full access. These groups control which content these users can view and what tasks they can perform in ADP Workforce Now.
- Both the ADP Workforce Now Web site and the HR & Benefits module are impacted at this stage. You will make very specific decisions about the content employees can see and use in ADP Workforce Now and, if your company is using it, the HR & Benefits module.
- Portal administrators gain access to the **Security Access** menu, where they can control the content other users can see and use.

- Practitioners gain access to the modules identified in their security management product profiles.

**Level 3**
**ADP Workforce**
**Now modules**

### Level 3: ADP Workforce Now modules

The final stage of implementing security access is to set up ADP Workforce Now module access - that is, which aspects of the HR & Benefits, Payroll, and Time & Attendance modules (if your company is using them) can each employee access? You will again make very specific decisions about the content employees can see and use in each of the modules.

As you work through the planning tasks in this chapter, you will fill out a form, called the Security Template, that helps you to understand how to think about user access security at your company. Working with your ADP representative, you will implement the security plan as you work through the security levels in this guide.

# Filling in the Security Template

As your ADP representative explained during the Security Master Setup call, the purpose of the Security Template is to help you to understand:

- The types of user access you can restrict
- The methodology for securing user access in ADP Workforce Now

**Important:** You do not have to identify every access restriction on the Security Template. The purpose of filling in the template with these restrictions is to work with your ADP representative to develop a methodology that you can then implement consistently in ADP Workforce Now and the modules.

The Security Template includes columns that begin with high-level user information in left-most columns and work toward more detailed user restrictions as you progress to the right. During the discussions in the Security Master Setup call, your ADP representative might modify the columns in this form to meet your needs. However, this basic methodology - working from general to more specific - should continue to be the case.

**Tip:** The Security Template provides sample scenarios to help you understand how to plan for and assign access to the different users in your company.

# Example: A Completed Security Template

The examples in this chapter are provided in the Security Template on the **Sample Security Templates** tab. Refer to the Security Template for more information about these scenarios.

| User's Name & Job Title | ADP Security Management Role<br>Select one: | ADP Workforce Now Modules<br>Select one: | ADP Workforce Now Security Group<br>Select one: | Practitioner Permissions to Enter New Hire Information<br>Select all that apply: | Access Level<br>Select one: | Company Code, Business Unit, or Department | Benefit Restrictions | Pay Rate Restrictions | Additional Restrictions |
|---|---|---|---|---|---|---|---|---|---|
| Joan Richards, Office Manager | Security Master | All Modules | Both | ☑ Personal<br>☑ Employment<br>☑ Payroll<br>☑ Tax<br>☑ Time & Attendance<br>☐ Does Not Enter New Hires | Full | | | | |
| John Roth, Owner & President | Security Master | All Modules | Both | ☑ Personal<br>☑ Employment<br>☑ Payroll<br>☑ Tax<br>☑ Time & Attendance<br>☐ Does Not Enter New Hires | Full | | | | |
| Helen Pope, HR Generalist | Product User | All Modules | Practitioner | ☑ Personal<br>☑ Employment<br>☐ Payroll<br>☐ Tax<br>☐ Time & Attendance<br>☐ Does Not Enter New Hires | Partial | | | | Full access to HR & Benefits, read-only access to Payroll and Time & Attendance |
| George Jameson, Payroll and Time & Attendance Specialist | Product User | All Modules | Practitioner | ☐ Personal<br>☐ Employment<br>☑ Payroll<br>☑ Tax<br>☑ Time & Attendance<br>☐ Does Not Enter New Hires | Partial | | | | Full access to Payroll and Time & Attendance, read-only access to HR & Benefits |

## Column Descriptions

The following table describes the columns on the Security Template.

| Column | Description |
| --- | --- |
| User's Name & Job Title | Enter the user's name and job title.<br>**Note:** You only need to list users who require a digital certificate. |
| Security Role | Select the ADP security management role that should be assigned to the user:<br>• Security Master*<br>• Security Administrator<br>• User Master<br>• User Administrator<br>• Product User<br>*You can assign the security master role to a backup security master. This person can perform tasks during the absence of the security master. |
| ADP Workforce Now Modules | Based on the ADP Workforce Now modules your company is using, select which module(s) should be assigned to the user's security management profile:<br>• All modules<br>• Payroll<br>• HR & Benefits<br>• Time & Attendance<br>• Payroll and HR & Benefits<br>• Payroll and Time & Attendance<br>• HR & Benefits and Time & Attendance<br>These modules are assigned to the user's security management profile. |
| ADP Workforce Now Security Group | Select the default security group(s) to which the user belongs:<br>• Portal Administrator<br>• Practitioner<br>• Both<br>The Portal Administrator and Practitioner groups require digital certificates, so it is important to identify any users who belong to these groups. |
| Access Level | Select whether the user has full or partial access to ADP modules or module features (that is, entire modules or restricted access within the modules). If the user has full access, you don't need to fill out additional columns.<br>The next several columns help you to define the type of content a user with partial access can or cannot see and use. |
| Company Code, Business Unit, or Department Restrictions | Some users have access restrictions based on the organizational unit where they work – for example, a company code, business unit, or department.<br>State that the user has full access if the user does not have any access restrictions. If the user has partial restrictions, briefly state what those restrictions are. |

| | |
|---|---|
| Benefit Restrictions | Indicate whether the user can see and/or change employee benefits.<br>For example, some organizations have a benefits administrator who is responsible for overseeing benefits. In this case, the benefits administrator would be able to see and change benefits content, but other administrators, such as the payroll administrator, would not have access to this information. |
| Pay Rate Restrictions | Indicate whether the user can see and/or change pay rates.<br>Some users should not see pay rates. For example, you might set up a payroll administrator to see the hours employees work, but you don't want that person to see the rate of pay for other employees. |
| Additional Restrictions | This is a free-form column in which you can place any notes about user access that you think are important to consider. |

# Planning for Security Management Setup

Setting up users in the ADP security management service is required for any user who needs a digital certificate to log on to ADP Workforce Now, including the security master. Working with your ADP representative during this phase, you must identify each of these users and identify their level of access in the ADP security management service.

Fill in the following columns in the Security Template to identify all users who must be set up in the security management service with a digital certificate so they can then register for ADP Workforce Now:

- User's Name & Job Title
- ADP Security Management Role
- ADP Workforce Now Modules

## Security Management Roles

In addition to the security master, the ADP security management service has four security roles to which you can assign users. As a security master, you are responsible for identifying which type of access users should have and assigning them to the appropriate role during security management setup. Users in a security role (those who have a digital certificate) can manage other users in the same security role or in lower security roles.

In the **Security Role** column of the Security Template, you identify which security role the user should have.

**Important:** It is critical that you assign users to the appropriate ADP security role. Assigning a user to the wrong role can mean that person has access to sensitive information that he or she should not see. This is a significant security risk.

| Role | Description |
|---|---|
| Security Master | A security master is a highly trusted user who has complete access to all the ADP services your company uses. This user can create new security administrators, perform all the tasks of the security administrator, and maintain users in other security roles.<br>The security master should already be identified. You are only logging this role on this template in case you need to make notes concerning this person's access (in the **Additional Restrictions** column). |
| Security Administrator | A security administrator is a highly trusted user who has complete access to all the ADP services your company uses. This user can create new product users and assign the security management roles of user master, user administrator, or product user to users. He or she can create self-service users who require early access to your ADP services (if available to your company). This user can reset passwords, issue/reissue digital certificates, and issue/reissue personal identification codes (if available to your company). This user can also use security management service to manage access to ADP services for user masters, user administrators, product users, and self-service users. |
| User Master | A user master can assign the user administrator role to product users or self-service users and perform all user administrator tasks. This user can also issue/reissue personal identification codes (if available to your company), modify self-service users' information, and approve or deny self-service users registering before their information is available to ADP (if available to your company). |
| User Administrator | A user administrator can perform security tasks such as resetting passwords and reissuing digital certificates. This user can also suspend or activate self-service users. |
| Product User | A product user can access specific ADP modules. This user cannot perform administrative security tasks such as resetting passwords and reissuing digital certificates in the ADP security management service. |

## Planning the Level of Access for ADP Workforce Now

As security master, you must identify the default security groups and level of access for users who require a digital certificate.

On the Security Template, provide the following information for each user who will need to be set up in the ADP security management service:

- In the **ADP Workforce Now Security Group** column, add the core security group(s) to which the user belongs. Since only portal administrators and practitioners require digital certificates, you only need to identify users who belong to these two groups. (Refer to "Core Default Groups Requiring Digital Certificates" on page 13 for more information.)
- In the **Access Level** column, identify whether the user should have full or partial access to ADP Workforce Now.

**Important:** For all users who have full access, such as the security master, the Security Template is now complete.

## Example: Security Master Users on the Security Template

In this example, Jill Smith acts as a backup to Bob Collins, the security master.

| User's Name & Job Title | ADP Security Management Role<br>Select one: | ADP Workforce Now Modules<br>Select one: | ADP Workforce Now Security Group<br>Select one: | Practitioner Permissions to Enter New Hire Information<br>Select all that apply: | Access Level<br>Select one: | Company Code, Business Unit, or Department | Benefit Restrictions | Pay Rate Restrictions | Additional Restrictions |
|---|---|---|---|---|---|---|---|---|---|
| Bob Collins, Office Manager | Security Master | All | Both | ☑ Personal<br>☑ Employment<br>☑ Payroll<br>☑ Tax<br>☑ Time & Attendance<br>☐ Does Not Enter New Hires | Full | | | | |
| Jill Smith, Owner | Security Master | All | Both | ☑ Personal<br>☑ Employment<br>☑ Payroll<br>☑ Tax<br>☑ Time & Attendance<br>☐ Does Not Enter New Hires | Full | | | | |

## Core Default Groups Requiring Digital Certificates

You can assign users to one or more default security groups so they view the appropriate content on the ADP Workforce Now Web site. These groups also affect the kind of information users can see in the ADP Workforce Now modules.

**Note:** Chapter 3, "Setting User Access in ADP Workforce Now" on page 57, states that ADP Workforce Now actually has four (not two) core default security groups. However, only portal administrators and practitioners require digital certificates, so you only need to identify these two groups on the Security Template. Therefore, only these groups are discussed here.

| Default Security Group | How Users Are Assigned |
|---|---|
| Administrator (Portal Administrator) | Users are automatically assigned the Portal Administrator role when you set them up with the ADP Workforce Now profile in security management service.<br>The portal administrator requires a digital certificate and controls user access privileges and the appearance of the ADP Workforce Now Web site. |
| Practitioner | Users are automatically assigned the Practitioner role when you set them up with the ADP Workforce Now profile in security management service.<br>Practitioner users require digital certificates and can access the services to which they have been assigned from those being used by their company. For example, a practitioner might only be assigned to the HR & Benefits module, even though the company is using all ADP modules. |

# Planning User Access Restrictions for the ADP Workforce Now Web Site and Modules

The next planning task is to determine the restrictions on seeing and using content for each user. These restrictions affect the ADP Workforce Now Web site and HR & Benefits, Payroll, and Time & Attendance modules.

To determine what restrictions are important:

- Brainstorm with your ADP representative about the types of user information you can restrict. You might find it helpful to see a demo of the areas of ADP Workforce Now where you will set up user access. You can also review the sample scenarios provided in the Security Template.
- Meet with key staff in your company (such as the security administrators, user masters, user administrators, and product users you have identified on the Security Template) to determine what kinds of access restrictions they believe are important for the jobs they, and the people who might report to them, perform.

**Important:** You do not have to identify every restriction on the Security Template. The purpose of filling in the template with these restrictions is to work with your ADP representative to develop a methodology that you can then implement consistently in ADP Workforce Now.

For details on these steps, refer to the chapter that describes the module (Chapters 4 through 6).

## Example: Access Restrictions on the Security Template

On the Security Template, certain users are identified as having partial access. For each of these users, note these access restrictions in the last four columns on the right side of the Security Template.

| User's Name & Job Title | ADP Security Management Roles<br>Select one: | ADP Workforce Now Modules<br>Select one: | ADP Workforce Now Security Group<br>Select one: | Practitioner Permissions to Enter New Hire Information<br>Select all that apply: | Access Level<br>Select one: | Company Code, Business Unit, or Department | Benefit Restrictions | Pay Rate Restrictions | Additional Restrictions |
|---|---|---|---|---|---|---|---|---|---|
| William Jones, Payroll Specialist | Product User | Payroll | Practitioner | ☐ Personal<br>☐ Employment<br>☑ Payroll<br>☑ Tax<br>☐ Time & Attendance<br>☐ Does Not Enter New Hires | Partial | | | | No access to create manual checks |
| Karen Bailey, Time & Attendance Specialist | Product User | Time & Attendance | Practitioner | ☐ Personal<br>☐ Employment<br>☐ Payroll<br>☐ Tax<br>☑ Time & Attendance<br>☐ Does Not Enter New Hires | Partial | | | No access to pay rates | |
| Marie Johnson, HR Generalist | Product User | HR & Benefits | Practitioner | ☑ Personal<br>☑ Employment<br>☐ Payroll<br>☐ Tax<br>☐ Time & Attendance<br>☐ Does Not Enter New Hires | Partial | No access to certain corporate groups | No access to create new benefit plans | No access to executive earnings | |

# Filling in the ADP Internet Product Security Registration Form

During the Security Master Setup call, your ADP representative provided you with a user information form called the ADP Internet Product Security Registration form. Each staff member in your company who requires a digital certificate to access ADP Workforce Now must fill in this form and return it to you. This information is necessary to set up these users in the security management service.

Complete these steps:

**1** Distribute a copy of the ADP Internet Product Security Registration form to all staff members who require a digital certificate to access ADP Workforce Now (that is, all portal administrators and practitioners). Ask them to fill out the form neatly and accurately and return it to you.

**Note:** Only portal administrators and practitioners need to fill out this form, since they are the only users who require digital certificates.

**2** Gather all completed ADP Internet Product Security Registration forms from the staff members. Verify that all information has been filled out completely, including selecting the security question and answer at the bottom of the form.

**3** Inform the staff members that they should expect a confirmation e-mail from ADP. Staff members must follow the process in that e-mail to download the digital certificate. If staff members do not receive the e-mail within a reasonable amount of time, they should contact you so you can reissue the certificate or follow up with ADP.

## Chapter 2

# Setting Up Users in ADP Security Management Service

You have completed initial planning with your ADP representative and understand how you want to secure user access at your company. The process of securing user access begins with the ADP security management service, which controls user access to all ADP Internet services and ensures that unauthorized users are not able to access sensitive data. As the security master, you can use the ADP security management service to set up the security administrators, user masters, user administrators, and product users at your company who should be able to access ADP Workforce Now®.

This chapter provides details on how to do the following:

- Complete the setup process for the security master (which should already be underway)
- Set up security administrators, user masters, user administrators, and product users
- Assign users to a product profile
- Maintain user profiles, such as updating personal information, resetting passwords, and reissuing digital certificates

**Tip:** Details on all of these tasks, along with answers to frequently asked questions, are provided in ADP's security management service online help PDF.

After setting up all users in the ADP security management service, refer to Chapters 3-6 to complete user access for the ADP Workforce Now modules and features.

# Setting Up the Security Master

As the security master, you are responsible for identifying, setting up, and maintaining each user in your company who should be able to access ADP Workforce Now. Before you can set up user access for others, you must complete the ADP security management service registration process described in this chapter. Your ADP representative will guide you through the security management process.

**Note:** If you have identified a backup security master, that person should also complete this process.

## Before You Begin

Before you set up users, you must work with your ADP representative to register as a security master in the ADP security management service. During initial planning, you should have provided your ADP representative with the contact information needed to set you up as a security master. Refer to Chapter 1, “Planning User Access” on page 1, if you have not yet had this conversation.

By now, you should have received a system-generated e-mail message that contains the information you need to download your digital certificate. If you have not received this e-mail, contact your ADP representative.

## Downloading a Digital Certificate

You must download your digital certificate before you can log on to the security management service for the first time. The digital certificate identifies you as a security master for ADP Workforce Now.

**Note:** Be sure to download the digital certificate on the computer from which you plan to access the security management service and ADP Workforce Now. The digital certificate permits access only on the computer where it is installed. The certificate is valid for two years. 60 days before the expiration date, you will receive an e-mail notification with instructions for renewing the certificate.

On the computer you will use to perform administrative tasks, follow these steps:

1. Open your browser, and then open the system-generated confirmation e-mail.
2. Copy the URL from the e-mail, paste it into the browser address field, and then click **Go**.
3. On the Register for ADP Services page, copy the user ID and access code from the confirmation e-mail and paste them in the appropriate fields.

   **Important:** Make sure you don't copy extra spaces before or after the access code. If you have already registered and have an ADP services user ID and password, proceed to step 6.

4. Select the security question, and enter the answer.

**5** Create and confirm the password for your account. Passwords must conform to the following rules:

- Your password must be at least eight characters long and must contain at least one letter and one number.
- Your password is case-sensitive.
- Your password can include special characters (-! @ # $) and spaces.
- Your password cannot repeat any character more than four times. For example, AAAAAA11 is not permitted.
- You cannot reuse your last four passwords.

**Note:** For added security, your password expires every six months. Before your password is about to expire, you will be prompted to select a new password when you log in to your ADP service. Your new password is effective immediately.

**6** Click **Submit** to complete the registration process and start to download the digital certificate.

**7** The ADP Digital Certificate Download Process page will be displayed with the additional tasks that must be completed before you can download the ADP digital certificate.

**Important:** Depending on the operating system and internet browser you use, you may be required to complete additional setup tasks before you can download the ADP digital certificate. For more information, refer to "System Requirements and Setup Tasks" on page 20.

**8** Follow the instructions on the page, complete the setup tasks and click **Download Certificate** to download your digital certificate.

**9** You will receive a few security alerts. When prompted, click **Yes** to continue.

**Note:** For information to export, import, and verify the ADP digital certificate, navigate to the security management service. On the home page, select the Resources section to access the Administrator access with digital certificate Quick Reference Card.

# System Requirements and Setup Tasks

The requirements for the operating system and internet browser you use can vary based on the ADP services your company is using. Depending on the operating system and internet browser you use, you may be required to complete additional setup tasks before you can download the ADP digital certificate.

**Important:** You must complete the additional tasks displayed on the ADP Digital Certificate Download Process page before downloading the ADP digital certificate.

## Microsoft® Internet Explorer with Windows® XP

### Enable ActiveX Download

Your browser's security setting for Download Signed ActiveX Controls must be set to either Prompt or Enable.

Do the following to check this setting:

1 Select **Internet Options** from the Internet Explorer Tools menu.

2 Select the **Security** tab and click the **Trusted Sites** icon.

3 Click **Custom Level** and then verify that the Download signed ActiveX controls setting is set to either Prompt or Enable.

4 Click **OK** to close the Security Settings window.

5 Click **OK** to close the Internet Options window.

### Install ActiveX

Depending on your computer setup, you may see a warning message in the Information bar. To display the hidden contents of the page, do the following:

1 Click on the warning message in the Information bar.

2 Click **Allow Blocked Content** option.

3 In the Security Warning window, click **Yes**.

## Microsoft® Internet Explorer with Windows Vista® / Windows® 7

Complete the following steps before downloading the ADP digital certificate:

### Download the ADP Root Certificate

On the ADP Digital Certificate Download Process page, click the **Download and Install Root Certificate** link.

Do the following to complete this process:

1 In the File Download - Security Warning window, click **Save**.

2 In the Save As window, accept the default file location and file name, and then click **Save**.

3 In the Download Complete window, click **Open**.

4 In the Internet Explorer Security window, click **Allow**.

5 In the Certificate window, click **Install Certificate**.

6 On the Welcome to the Certificate Import Wizard page, click **Next**.

7 On the Certificate Store page, click **Place all certificates in the following store**, and then click **Browse**.

8 In the Select Certificate Store window, click **Trusted Root Certification Authorities**, click **OK**, click **Next**, and then click **Finish**.

9 In the Security Warning window, click **Yes**.

10 In the Certificate Import Wizard window, click **OK**.

11 Click **OK** to close the Certificate window.

### Add ADP To Trusted Sites

1 From the Internet Explorer Tools menu, select **Internet Options**.

2 In the Internet Options window, select the **Security** tab.

3 Click the **Trusted sites** icon and then click **Sites**.

4 In the **Add this website to the zone** field, type **https://*.adp.com**, then click **Add**.

5 Make sure that the **Require Server Verification For All Sites in this Zone** check box is selected, and then click **Close**.

6 Click **OK** to close the Internet Options window.

## Mozilla® Firefox and Non-Internet Explorer

The steps apply to users with Windows® XP/Windows Vista®/Windows® 7/MAC operating systems.

**Important:** The steps below may slightly vary depending on the operating system and internet browser you use.

### Download the ADP Root Certificate

On the ADP Digital Certificate Download Process page, right-click on the link to **Download and Install Root Certificate**.

**Important:** Do not close the ADP Digital Certificate Download Process page until you have downloaded your certificate.

Do the following to complete this process:

1 Right-click on the link and click **Save Link As**.

2 In the Enter Name of File to Save to window, browse to select a location to save the file.

3 In the **File Name** field, accept the default file name.

4 Select **All Files** in the Save as Type list and click **Save**.

---

**Important:** The root certificate will be saved in the specified location. If you use the Safari browser on MAC, the certificate will be saved as an A.p7s file. You must click on this file to install the certificate.

---

5 In Firefox, select **Tools>Options**.

6 Select the **Advanced>Encryption** tab and click **View Certificates**.

7 Select the **Authorities** tab and click **Import**.

8 In the Select File containing CA certificate(s) to Import window, navigate to locate the saved root certificate, save it, and then click **Open**.

9 In the Downloading Certificate window, click to select all options and click **OK**.

10 Click **OK** to close the Certificate window.

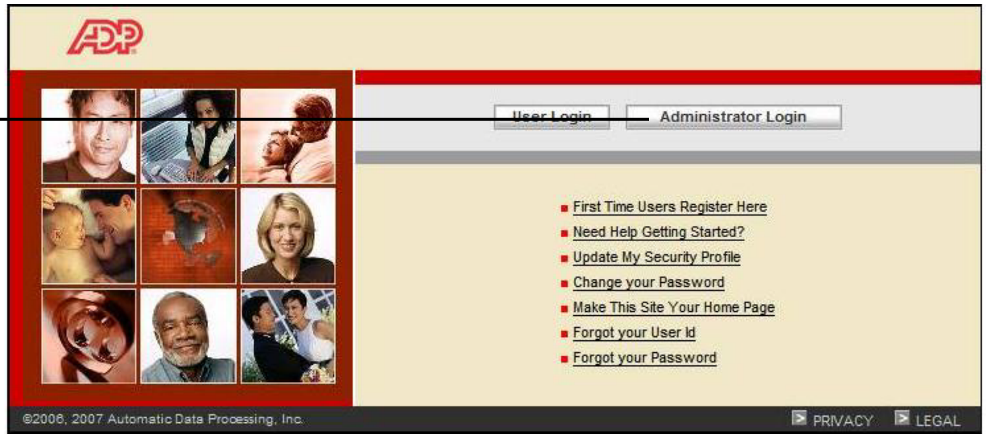
# Logging On to ADP Security Management Service

**Important:** Pop-up blockers may interfere with the display of valid pop-up windows (confirmations, forms, reports). ADP recommends that you disable pop-up blockers or set up your pop-up blocker to allow pop-ups for this site.

1 Go to: **https://portal.adp.com**

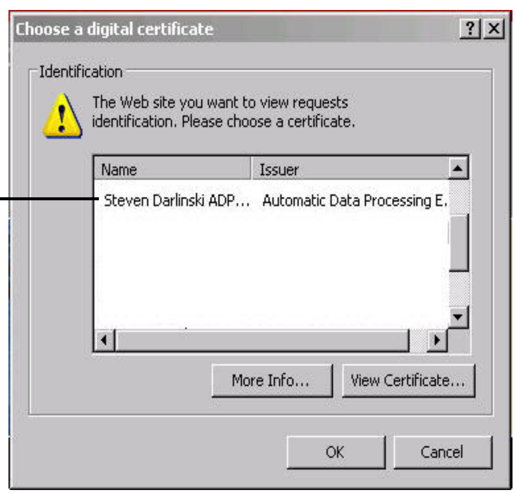
2 Click **Administrator Login**.

Digital certificate users click here to log on to ADP Workforce Now.

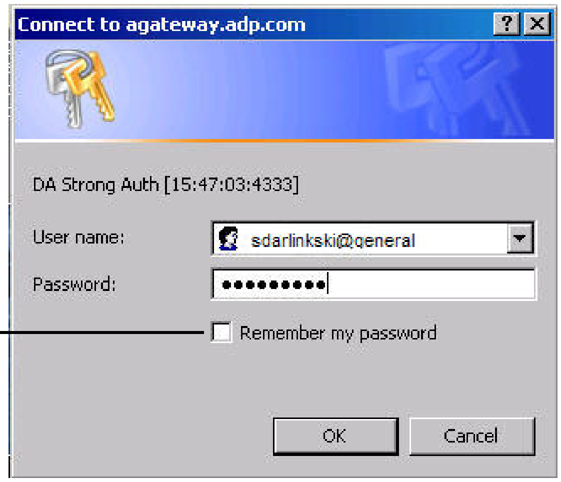



3 In the Choose a digital certificate window, select your certificate and click **OK**.

The digital certificate is labeled with your first name, last name, ADP and the expiration date of your certificate.

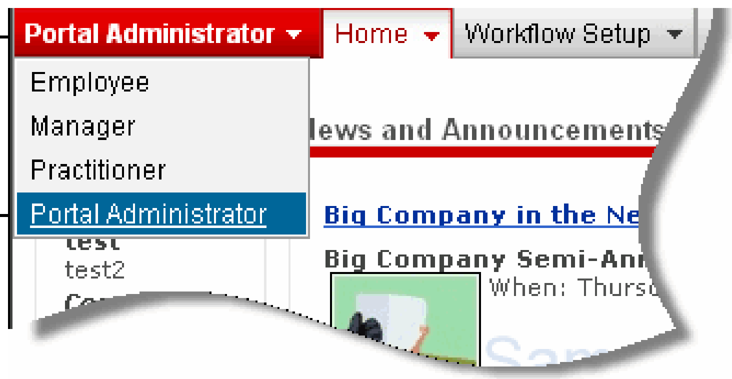


**4** In the Connect window, enter your user ID, password and click **OK**.




**Note:** This check box is disabled for added security. You cannot select this option.

**5** In ADP Workforce Now, point to the Role Selector and select **Portal Administrator**.




Role Selector

Select this role to set up user access in ADP Workforce Now.

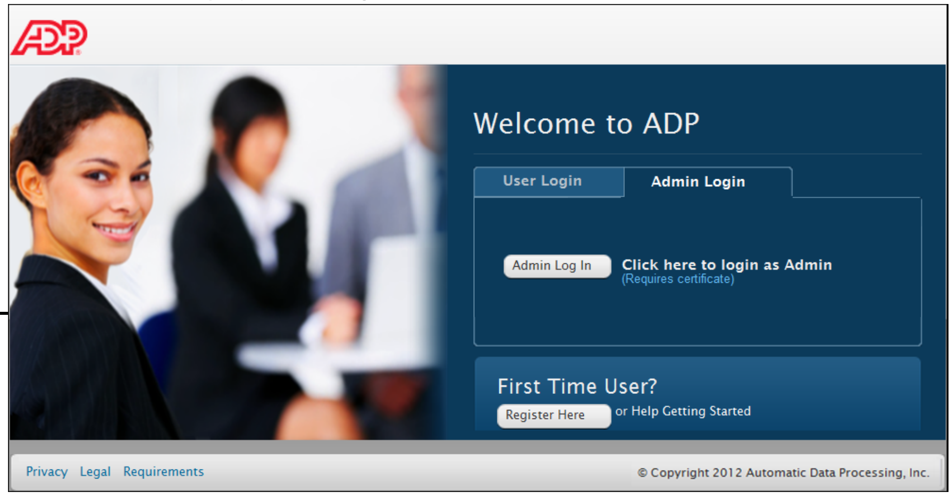
Notice that the menus change when you access the Portal Administrator role. The **Security Access** menu is now available.

**6** Select **Security Access > Security Management User Administration**.


From this menu, you can access the ADP security management service to register users.

**7** On the Welcome page, click **login**.

Select **login** to open the ADP Netsecure window.




Once you have logged on to the ADP security management service, you can set up additional users - such as security administrators and user masters (who can assist you with setting up other users) and product users (who are the daily users of the ADP Workforce Now services).

# Setting Up Additional Users

# Setting Up Additional Users

During the planning process, each security administrator and product user filled out an ADP Internet Product Security Registration form to provide the personal information that must be entered when you set up that user. As you set up these users, you will consult these forms to enter this personal information.

**Note:** You do not need to provide digital certificates to all users of ADP Workforce Now. In fact, most users – the self service users – can register with ADP Workforce Now to get a username and password but don't require a digital certificate. self service users typically can only view their own information. ADP Workforce Now managers (also self service users) can access information about the employees who report to them. However, they do not have security privileges and are not able to change the way other users access ADP Workforce Now.

You can add new security administrators, user masters, user administrators, product users, and Self Service users (if available to your company). Your security masters and security administrators can add other users for your company. This task does not apply to user masters, user administrators, product users, and self service users.

The following table lists the user roles that are authorized to add other users:

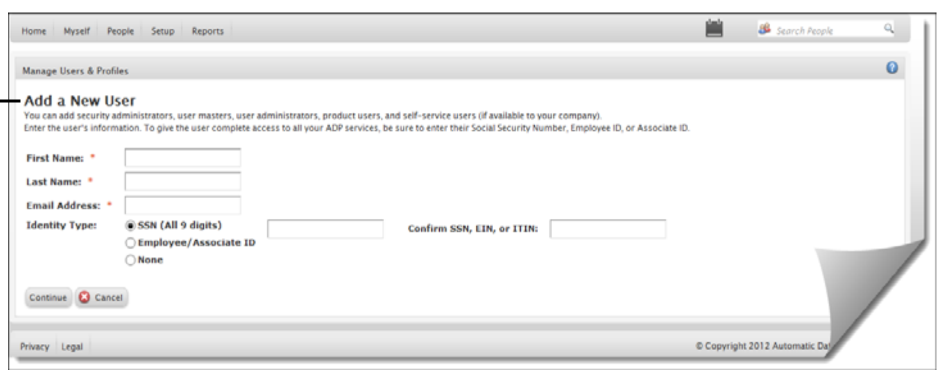
| User Role | Can Add New |
|---|---|
| Security Master | Security administrator, user master, user administrator, product user, and Self Service user (if available to your company) |
| Security Administrator | User master, user administrator, product user, and self service user (if available to your company) |
| User Master | This task does not apply |
| User Administrator | This task does not apply. |
| Product User | This task does not apply |
| Self Service User | This task does not apply. |

Go to **People > Access & Security > Manage Users & Profiles**.

**1** Click on the Add New (+) icon.

**2** Enter user information.

Add User



3 Enter personal information about the user. Make sure the e-mail address is valid and frequently checked by the user. The ADP security management service sends a system-generated confirmation e-mail to this address. This e-mail provides the user ID, access code, URL, and instructions needed to download the digital certificate, so it is important that it is sent to the correct e-mail address.

**Important:** ADP validates the information that your registering employee enters against what you, their employer, entered in the Payroll, HR, Time and Attendance, or other ADP application you use. If the information matches, the user is given access to all of your ADP services at once. If the information does not match, the user might not be able to register or may not have complete access to your ADP services.

4 Click **Continue**.

5 Select the user type.

6 Select the user role.

| Select This Option | To |
|---|---|
| User will be included in... | Add a user whose information is included in the information your company sends to ADP.<br>**Note:** If ADP cannot verify this user's identity, the user cannot download the certificate. |
| User is an independent contractor... | Add a new user not included in your ADP services. |

7 Click **Next**.

8 Assign the product profiles to allow access to ADP services, if required.

**Note:** Refer to "Assigning the ADP Workforce Now Profile to a User" on page 29 to continue.

To assign product profiles later, refer to "Assigning the ADP Workforce Now Profile to a User" on page 29

9 Click **Next**.

10 Select the security question and enter the security answer.

**Note:** This step is not required when adding an administrator having access without a digital certificate.

11 Click **Next**.

12 Review the user information.

**Note:** You can update the e-mail address, if required.

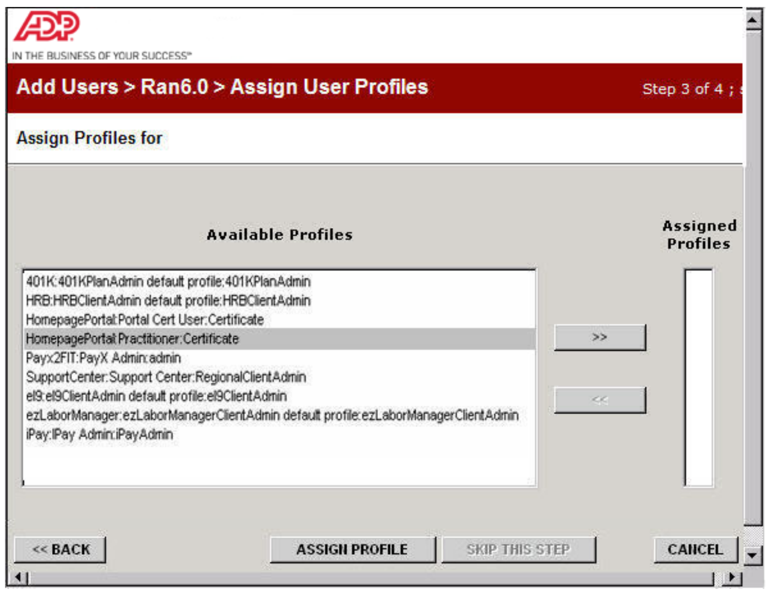
13 Click **Done**.

# Assigning the ADP Workforce Now Profile to a User

Your ADP representative has created default profiles for each ADP service your company uses. In this section, you will assign the ADP Workforce Now profile to users. All users must have this profile assigned so they can access ADP Workforce Now.

To assign the profile to a user, follow these steps:

1. On the View User Info page, click **Assign Profiles** in the left menu.
2. On the Assign User Profiles page, select **HomepagePortal** and click **>>** to move it to the Assigned Profiles list. (This profile represents ADP Workforce Now.)

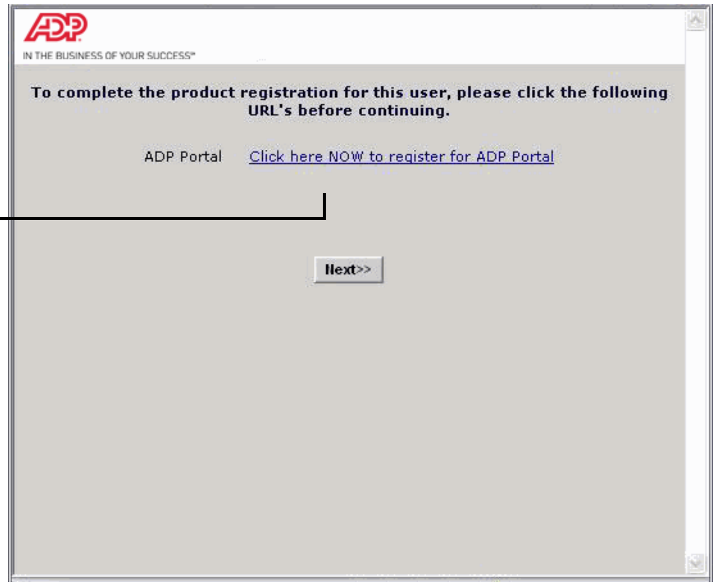



**Note:** You also might need to select additional profiles. Check with your ADP representative. If you are adding a profile to a user that is from another company but has access to your ADP services, be sure to assign a profile that is delegate enabled.

3. Click **Assign Profile**.
4. In the Assign User Profile confirmation window, click **Move to the Next Step.** Do not select **Assign Another Profile**. You must completely set up the ADP Workforce Now profile before you can assign another profile to the user.

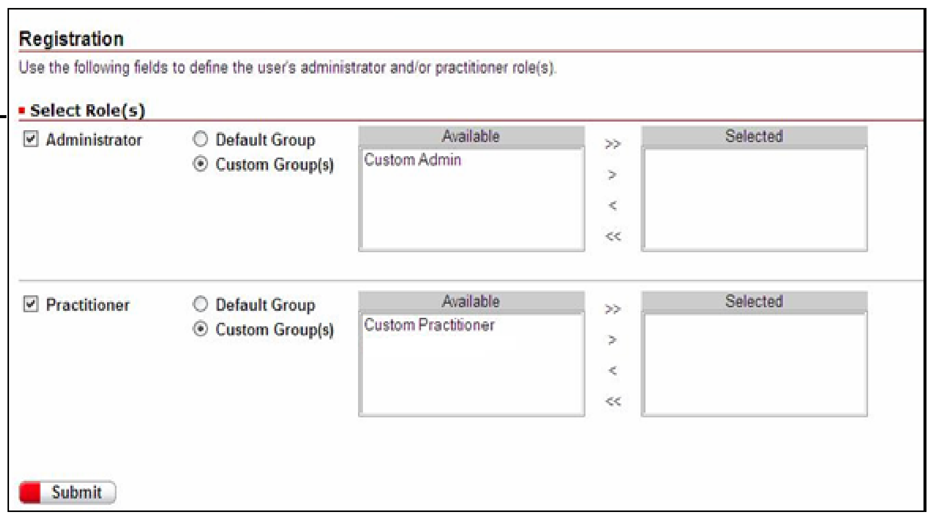
**Note:** Some ADP services require you to enter additional information. Click the URL to enter the additional information.

**5** Click the link, **Click here NOW to register for ADP Portal**.




Click this link.

**6** Select whether the user is an administrator, a practitioner, or both.




Refer to Column 4 - **ADP Workforce Now Security Role** on the Security Template to determine which role to choose.

**7** Assign the user to the appropriate security group(s). For each role you selected, choose either **Default Group** or **Custom Group(s)**. If you choose **Custom Group(s)**, move your selection(s) from the **Available** list to the **Selected** list. You cannot assign a user to both a default group and a custom group for the same role.

**Note:** If no custom security groups are available, the **Custom Group(s)** radio button is grayed out.

**8** Click **Submit**.

A system-generated e-mail will be sent to the user containing a user ID, access code, and the URL to download a digital certificate.

# Assigning the Support Center Profile to a User

The Support Center profile gives certificate users access to the Support Center Web site, where they can find additional information and training materials. This profile also gives ADP Workforce Now employees, managers, and practitioners access to ADP Workforce Now task assistance.

To assign the Support Center product profile, go to **People > Access & Security > Product Profiles**.

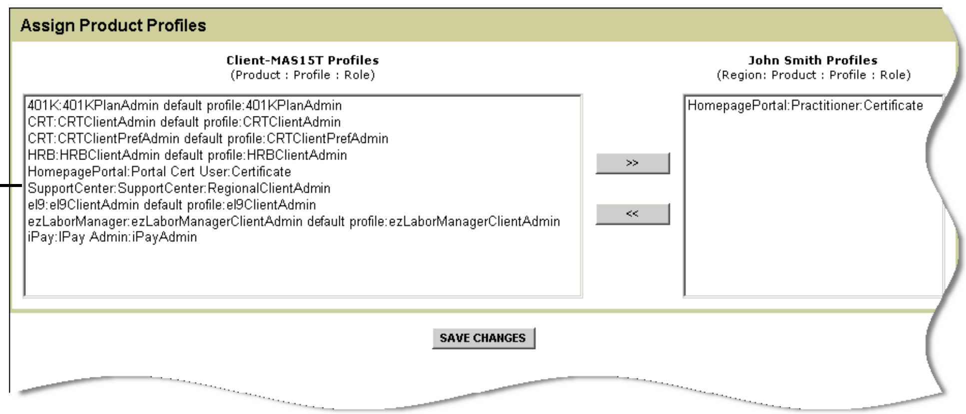
1 Select the user.

2 Click on the user's name.

3 Click to select the **Support Center** profile and move them to the Selected Product Profiles list.

4 Click **Save Changes**.

**Note**: The options available may vary based on your security role. For example, if you are the user administrator, the User Admin option will not be available to you.



# Next Steps

Your next task is to assign a product profile to the user to identify which areas of ADP Workforce Now the user can access. Your ADP representative has created a default profile for each service your company uses. The profile consists of a service, a role, and associated authorization codes (company codes). This profile allows you to control access to each of the ADP services your company is using. Refer to these chapters to assign profiles for the ADP Workforce Now modules:

| Module | Refer to This Chapter |
|---|---|
| HR & Benefits | Chapter 4, "Setting User Access for HR & Benefits" on page 97 |
| Payroll | Chapter 5, "Setting User Access for Payroll" on page 107 |
| Time & Attendance | Chapter 6, "Setting User Access for Time & Attendance" on page 123 |

**Note:** Before deciding on the product profile for the user, review the default profiles set up by your ADP representative. Each user must be assigned at least one product profile.

# Performing User Maintenance Tasks

Security masters or security administrators are responsible for supporting users by doing the following:

- Assigning a Security Role
- Adding a New User
- Finding a User
- Suspending or Activating a User
- Deleting a User
- Approving or Denying a User
- Modifying a User's Personal and Status Information
- Resetting a Password
- Assigning a Product Profile to a User

**Note:** The options available may vary based on your security role. For example, if you are the user administrator, the User Admin option will not be available to you.

**Note:** *Need Help? Refer to the Online User Assistance*
Your ADP service now offers online user assistance with the information you are looking for. You can access the task topics, additional reference information, and view the frequently asked questions.

To get started, log in to your ADP service, navigate to the page where you are looking for information, and click the Help ? icon.

## Assigning a Security Role

Security masters, security administrators, and user masters can assign user-security roles. This task does not apply to user administrators, product users, and Self Service users. Assigning an administrator role will prompt to select the e-mail address to send instructions to get started.

There are six security roles available, each with varying levels of responsibility/access. The self service user has the lowest level of responsibility (does not requires administrator access) while the security master has the highest level of responsibility.

### Security Master

A security master is a highly trusted user who has complete access to all the ADP services your company uses. Security masters requires administrator access.

User in this role can do the following:

- Create new security administrator.
- Perform all the tasks of the security administrator.
- Maintain users in other security roles.

**Note:** If your company does not have a security master and needs to establish security administrators, contact your ADP representative.

### Security Administrator

A security administrator is a highly trusted user who has complete access to all the ADP services your company uses. A security administrator requires administrator access.

User in this role can do the following:

- Create new user administrators, user masters, and product users.
- Create Self Service users who require early access to your ADP services (if available to your company based on your ADP services).
- Assign security roles of product user, user master or user administrator to users.
- Perform security tasks such as reset passwords, issue/reissue certificates.
- Issue/reissue personal identification code (if available to your company).
- Manage access to ADP services for user masters, user administrators, product users, and self service users.
- If applicable, perform applicant maintenance tasks e.g., reset passwords, suspend, activate, and/or delete applicants.

### User Master

A user master requires administrator access. User in this role can do the following:

- Assign the user administrator role and product user role.
- Perform all user administrator tasks.
- Issue/reissue personal identification code (if available to your company).
- Modify self service users' information.
- Approve or deny self service users' registering before their information is available to ADP (if available to your company).

### User Administrator

A user administrator requires administrator access. User in this role can do the following:

- Search for users and applicants (if available to your company).
- View user information.
- Perform security tasks such as reset password and issue administrator access.
- Suspend or activate self service users.
- If applicable, perform applicant maintenance tasks e.g., reset passwords, suspend, and/or activate applicants.

### Product User

A product user requires administrator access. User in this role can do the following:

- Administer ADP services e.g., payroll, human resources, or benefits.
- Access and update personal account information.
- User cannot perform security administrative functions e.g., reset passwords, issue administrator access.

### Self Service User

Certain ADP services offer employees access to their own personal information (such as pay statements or medical benefits) via self-service functionality. User in this role can do the following:

- Receive a registration code from your company.
- Use the registration code to create user ID and password to access your ADP services.
- Access and update personal account information.

**Note:** User does not need administrator access.

The following table lists the user roles that are authorized to assign other ADP security management user roles:

| User Role | Can Assign The Role Of |
|---|---|
| Security Master | Security administrator, user master, user administrator, product user, and Self Service user |
| Security Administrator | User master, user administrator, product user, and Self Service user |
| User Master | This task does not apply |
| User Administrator | This task does not apply. |
| Product User | This task does not apply |
| Self Service User | This task does not apply. |

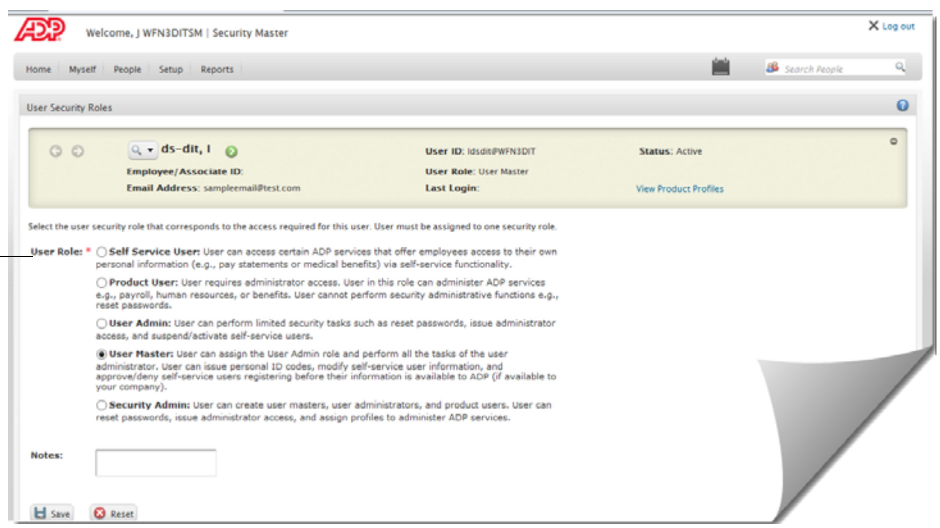
To assign the profile to a user, select **Security Access > Security Management User Administration**. Then navigate to **User Security Roles**.

1 Select the user.

2 Click to select the user role to assign to the selected user.

3 Click **Save**.

This is an example to assign the security administrator role.




4 If prompted, click **Yes** to assign product profiles.

5 To assign product profiles later, refer to "Assigning the ADP Workforce Now Profile to a User" on page 29.

6 If prompted, select the e-mail address to send an e-mail with instructions.

**Note:** You can confirm or change the user's e-mail address, if required. Depending on your user role, the ability to modify the e-mail address may vary.

**7** Click **Save**.

## Adding a New User

The following table lists the user roles that are authorized to add other users:

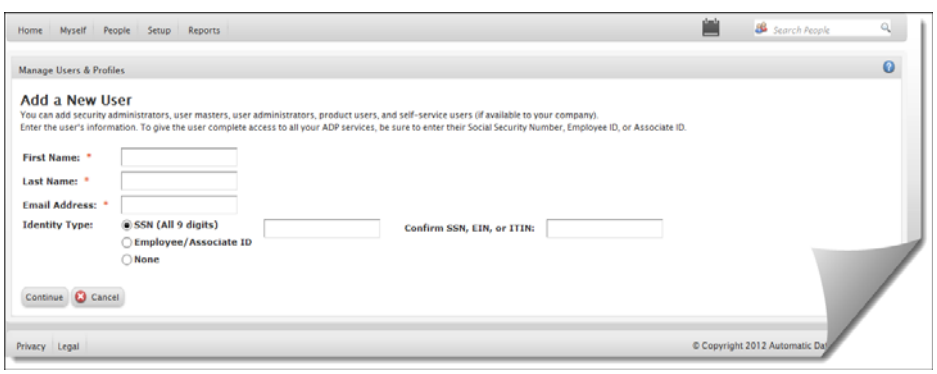
| User Role | Can Add New |
|---|---|
| Security Master | Security master, security administrator, user master, user administrator, product user, and self service user. |
| Security Administrator | Security master, security administrator, user master, user administrator, product user, and self service user. |
| User Master | Security master, security administrator, user master, user administrator, product user, and self service user. |
| User Administrator | Security master, security administrator, user master, user administrator, product user, and self service user. |
| Product User | This task does not apply |
| Self Service User | This task does not apply. |

You can add new security administrators, user masters, user administrators, product users, and self service users (if available to your company). Your security masters and security administrators can add other users for your company. This task does not apply to user masters, user administrators, product users, and self service users.

To add a new user, go to **People >Access & Security > Manage Users & Profiles.**

**1** Click on the Add New (+) icon.

**2** Enter user information.




**3** Click **Continue**.

**4** Select the user type.

**5** Select the user role.

**6** Click **Next**.

7 Assign the product profiles to allow access to ADP services, if required.

---

**Note:** To assign product profiles later, refer to **"Assigning the ADP Workforce Now Profile to a User" on page 29**.

---

8 Click **Next**.

9 Select the security question and enter the security answer.

---

**Note:** This step is not required when adding an administrator having access without a digital certificate.

---

10 Click **Next**.

11 Review the user information.

---

**Note:** You can update the e-mail address, if required.

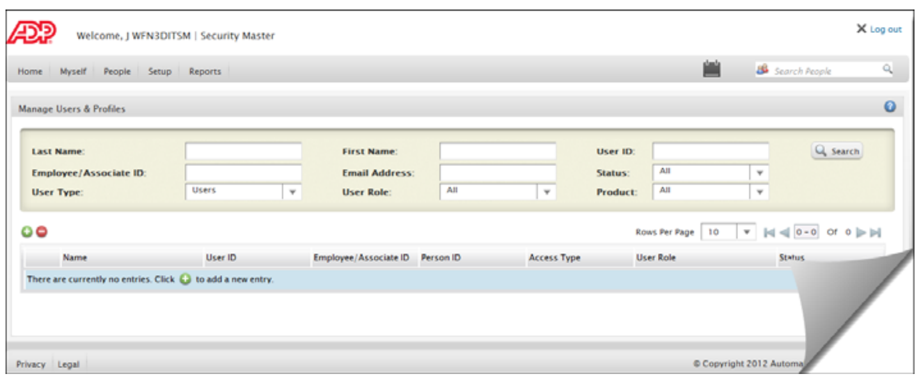
---

12 Click **Done**.

## Finding a User

Before you can change details about a user, you must locate the user in the ADP security management service. To do this, go to **People > Access & Security > Manage Users & Profiles**.

1 Click **User ID** or **User Name** and enter all or part of the user ID or user name.




## Suspending a User

The following table lists the user roles that are authorized to suspend/activate other users:

| User Role | Can Suspend |
|---|---|
| Security Master | Security master, security administrator, user master, user administrator, product user, and self service user. |
| Security Administrator | Security Administrator User master, user administrator, product user, and self service user. |

| User Role | Can Suspend |
|---|---|
| User Master | Self service user. |
| User Administrator | Self service user. |
| Product User | This task does not apply |
| Self Service User | This task does not apply. |

To suspend a user, go to **People > Access & Security > Manage Users & Profiles**.

1 Select the user.

2 Click on the user's name.

3 In the User Status field, click **Suspended**.

4 For information on the user roles you can suspend, refer to Access to Suspend/Activate Users.

5 Click **Save**.

6 Click **Yes**.

## Activating a User

When needed, you must reactivate the user to allow the user access to ADP services. When you reactivate a user, the user can log onto the security management service and/or access the products or services with his or her original user ID and password. A reactivated user does not have to repeat the registration process.

| User Role | Can Activate |
|---|---|
| Security Master | Security master, security administrator, user master, user administrator, product user, and self service user. |
| Security Administrator | Security Administrator User master, user administrator, product user, and self service user. |
| User Master | Self service user. |
| User Administrator | Self service user. |
| Product User | This task does not apply |
| Self Service User | This task does not apply. |

To activate a user, go to **People > Access & Security > Manage Users & Profiles**.

1 Select the user.

2 Click on the user's name.

3 In the User Status field, click **Active**.

4 For information on the user roles you can activate, refer to Access to Suspend/Activate Users.

5 Click **Save**.

6 Click **Yes**.

## Deleting a User

**Important:** This task cannot be undone. Once deleted, users cannot log in to access their pay statements, benefits, human resources, etc.

The following table lists the user roles that are authorized to delete other users:

| User Role | Can Delete Users |
|---|---|
| Security Master | Security master, security administrator, user master, user administrator, product user, and self service user. |
| Security Administrator | Security Administrator User master, user administrator, product user, and self service user. |
| User Master | This action does not apply. |
| User Administrator | This action does not apply. |
| Product User | This task does not apply |
| Self Service User | This task does not apply. |

To delete a user, go to **People > Access & Security > Manage Users & Profiles**.

1 Click on the user's name.

2 View the user information and click **Delete**.
For information on the user roles you can delete, refer to Access to Delete Users.

3 Click **Yes**.

**Important:** The user and user's information will be deleted permanently from your company records.

## Updating User Information

The following table lists the user roles that are authorized to update information for other users. For example, if you are a security master, you can update information for all the user roles listed. However, if you are a user administrator, you can only update information for other user administrators, product users, and self service users.

| User Role | Can Update User Information for |
|---|---|
| Security Master | Security administrator, user master, user administrator, product user, and self service user. |
| Security Administrator | User master, user administrator, product user, and self service user. |
| User Master | User administrator, product user, and self service user. |

| User Role | Can Update User Information for |
|---|---|
| User Administrator | Self service user.<br>**Note:** User administrator can only update the user status.roduct user and self service user. |
| Product User | This task does not apply. |
| Self Service User | This task does not apply. |

To update user information, go to **People > Access & Security > Manage Users & Profiles**.

**1** Select the user.

**2** Click on the user's name.

**3** Update the user information, as required.

**Note:** The information you can update may vary based on your company set up and the ADP services purchased.

**4** Click **Save**.

**Note:** If you change the e-mail address, a system-generated e-mail will be automatically sent to the previous e-mail address to notify the user of the change.

## Resetting a Password

The following table lists the user roles that are authorized to reset passwords for other users:

| User Role | Can Reset Password for |
|---|---|
| Security Master | Security administrator, user master, user administrator, product user, and self service user.<br>**Note:** Security master can update the contact e-mail address or mobile phone number to send the temporary password. |
| Security Administrator | User master, user administrator, product user, and self service user.<br>**Note:** Security administrator can update the contact e-mail address or mobile phone number to send the temporary password |
| User Master | User administrator, product user, and self service user.<br>**Note:** User master can update the contact e-mail address or mobile phone number of self service user to send the temporary password |

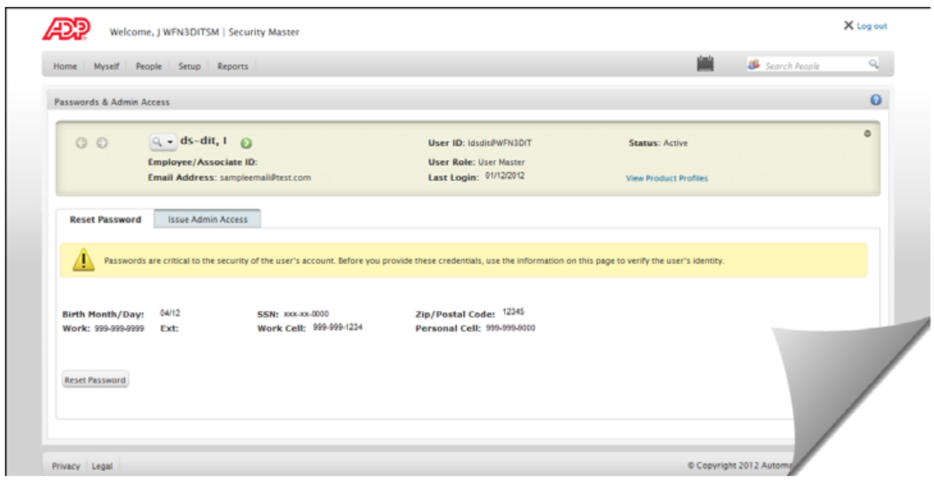
| User Role | Can Reset Password for |
|---|---|
| User Administrator | Self service user.<br>**Note:** User administrator cannot update the contact e-mail address or mobile phone number of users. |
| Product User | This task does not apply. |
| Self Service User | This task does not apply. |

To reset a user password, go to **People > Access & Security > Passwords & Admin Access**.

**1** Search for the user.

**2** Click on the user name to reset the password.

**3** Verify the identity of the user.




**4** Click **Reset Password**.

**5** Select the e-mail address or mobile phone number to send the temporary password.

**Note:** You can confirm or change the user's e-mail address or mobile phone number, if required. Depending on your user role, the ability to modify the e-mail address may vary. Refer to **Access to Reset User Password** in the online help.

**6** Click **Continue**.

**Note:** An e-mail with the temporary password will be sent to the user and a success message displays on the page.

## Issuing Admin Access

The following table lists the user roles that are authorized to issue administrator access to other users:

| User Role | Can Issue Admin Access For |
|---|---|
| Security Master | Security administrator, user master, user administrator, product user, and self service user.<br>**Note:** Security master can update the contact e-mail address to send the e-mail with instructions. |
| Security Administrator | User master, user administrator, product user, and self service user.<br>**Note:** Security administrator can update the contact e-mail address to send the e-mail with instructions |
| User Master | User administrator, product user, and self service user.<br>**Note:** User master can update the contact e-mail address for self service users |
| User Administrator | Product user and self service user.<br>**Note:** User administrator can update the contact e-mail address for self service users. |
| Product User | This task does not apply. |
| Self Service User | This task does not apply. |

To issue admin access, go to **People > Access & Security > Passwords & Admin Access**.

1 Search for the user.

2 Click on the user name.

3 Verify the identity of the user.

4 Click **Issue Admin Access**.

5 Select the e-mail address to send an e-mail with instructions.

**Note:** You can confirm or change the user's e-mail address, if required. Depending on your user role, the ability to modify the e-mail address may vary. Refer to **Access to Issue Admin Access**.

6 Click **Continue**.

**Note:** An e-mail with instructions will be sent to the user and a success message displays on the page.

## Assign / Remove Product Profiles

The following table lists the user roles that are authorized to assign/remove profile for other users:

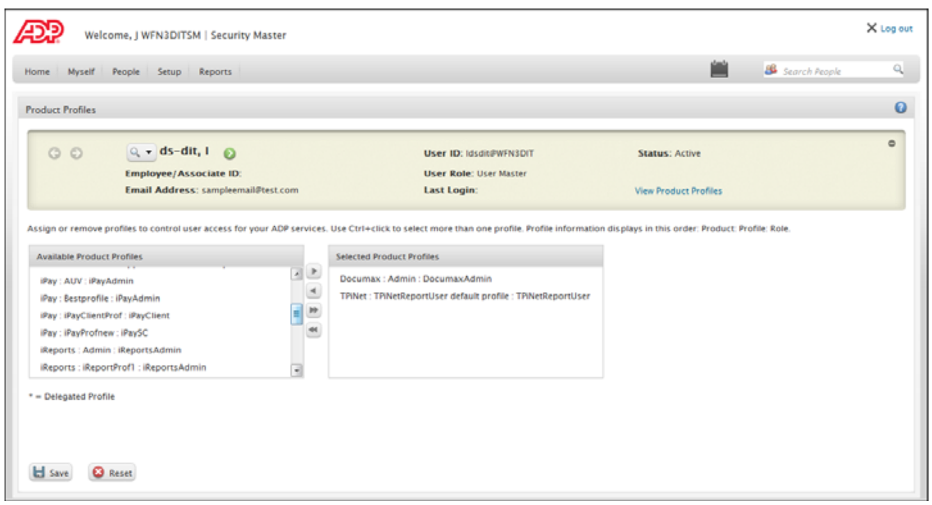
| User Role | Can Assign/Remove Profiles For |
|---|---|
| Security Master | Security administrator, user master, user administrator, product user, and self service user. |
| Security Administrator | User master, user administrator, product user, and self service user. |
| User Master | This task does not apply. |
| User Administrator | This task does not apply. |
| Product User | This task does not apply. |
| Self Service User | This task does not apply. |

To assign a product profile, go to **People > Access & Security > Product Profiles**.

1 Select the user.

2 Click on the user's name.

3 Click to select the profiles and move them to the Selected Product Profiles list.




4 Click **Save**.

# Company Maintenance Tasks

Security masters or security administrators are responsible for supporting their company through the following company maintenance tasks:

- View Your Company Information
- Update Your Company Information
- Set Up the Self Service Registration Pass code
- Manage Mobile Access for Your Users
- Manage the Use and Display of Mobile PIN
- View the Identity Verification Options
- Customize Your Support Contact Information
- Add Your Company Branding
- Creating Additional Product Profiles
- Adding a Product Profile
- Updating a Product Profile
- Deleting a Product Profile

**Note:** In addition to the information contained in this chapter, access the online help by clicking on Help on the toolbar. Online help contains comprehensive information on using the ADP security management service.

## Viewing Your Company Information

Security masters, security administrators, user masters, and user administrators can view your company information. This task does not apply to product users and self service users.

To view your company information, select **Setup > Company Information > Profile**.

1 View your company information available to ADP.

2 Click on another tab or task to navigate away from this page.

## Updating Your Company Information

Security masters, security administrators, user masters, and user administrators can update the company information settings for your company. This task does not apply to product users and self service users.

To update your company information, select **Setup > Company Information > Profile**.

1 Update the company address, web site address (URL), contact email of your administrator, and contact phone numbers.

2 Click **Save**.

3 Click **Settings** tab.

4 Update the self service registration pass code, mobile access for users, mobile PIN login, and customized support contact information.

5 Click **Save**.

# Setting Up The Self Service Registration Pass Code

Security master or security administrator must establish the self service registration pass code for your users. Your registration pass code consists of your client ID and the code you enter separated by a hyphen e.g., your client ID-your code.

**Note:** If your company uses Personal ID Codes (PICs) as the identity verification option during self service registration, users will not need the self service registration pass code.

To set up the self-service registration pass code, select **Setup > Company Information > Profile > Registration Settings**.

1. In the Self Service Registration Pass code field, enter the registration code.
2. Click **Save**.

A **letter to encourage employee registration** is available on the Home page > Resources section. Customize this letter based on the ADP services your company has purchased. Include the self service registration pass code, the URL to your ADP service web site, and provide it to your self service users (employees, consultants, or contractors). Users use this information to self register and access ADP services. Refer to **Self Service Registration process.**

# Personal Identification Code (PIC) Management

## About Personal ID Codes (PICs)

The Personal Identification Code (PIC) is an alphanumeric code that you generate in the ADP security management service for your company users. PICs are randomly generated and distributed to users by e-mail. Once issued, users enter PIC during registration to access ADP services. A PIC expires once used or within 15 days, whichever is earlier. If it has been lost or compromised, you can reissue the PIC. Click on the e-mail address field to update that information.

To take full advantage of PIC, your company should include the Social Security number (SSN) of your users in the information your company sends to ADP. If your company does not include the user’s SSN, the user will have limited access to ADP services.Contact your ADP representative for more information.

Your administrators use the PIC Management feature to do the following tasks:

- Issue Personal ID Codes (PICs)
- Issue Personal ID Codes (PICs) to All Users
- Update E-mail Addresses

**Important:** If users do not have a valid e-mail address, speak to the user and update the e-mail address of the user before you generate PIC. PIC expires within 15 days or when used for registration (whichever occurs earlier).

### Issuing Personal ID Codes (PICs)

Security masters, security administrators, and user masters can issue Personal ID Codes (PICs). This task does not apply to user administrators, product users, and Self Service users.

To issue a personal ID code, select **People > Access & Security> Personal ID Codes (PICs)**.

1 Select an item from the Users list.

2 Click **Search**.

3 View the search results.

**Note:** You can click in the e-mail address field and enter/update the e-mail address before issuing the PIC, if required.

4 Click **Other Actions.**

5 Click **Issue All PICs**.

**Note:** An e-mail with the PIC and instructions to use it during registration will be sent to all users included in your search results.

## Creating Additional Product Profiles

Your ADP representative has created default profiles for each ADP service. You can also create additional product profiles for your company. Additional product profiles do not replace the default product profiles.

## Adding a Product Profile

Security masters and security administrators can add product profiles for your company. This task is not available to user masters, user administrators, product users, and self service users.

To assign a product profile, select **Setup > Company Information > Profile**.

1 Click on the product name.

2 Click **(+)** to add a new profile.

3 Enter the profile name.

4 Select the role to be associated with the profile.

5 Select the authorization codes.

6 Click **Save**.

## Updating a Product Profile

Security masters and security administrators can update existing product profiles for your company. This task is not available to user masters, user administrators, product users, and self service users.

To update a product profile, select **Setup > Company Information > Profile**.

1. Click on the product name.
2. Click on the profile name.
3. Update the profile name and/or the authorization codes.
4. Click **Save**.

## Deleting a Product Profile

Security masters and security administrators can delete existing product profiles for your company. This task is not available to user masters, user administrators, product users, and self service users.

**Important:** Deleting a product profile removes it from all users to whom it has been assigned. This task cannot be undone.

To delete a product profile, select **Setup > Company Information > Profile**.

1. Click on the product name.
2. Click on the profile name.
3. View the profile details to verify it is the profile to be deleted.

Click **Delete**.

**Note:** You can refer to the online help for more information on the different reports.

# Reports

You can access reports from **Reports > Standard Reports > View/Run Reports**. Run reports to get information on your users and the ADP services your company has purchased. Once run, report results can be viewed or saved as a Portable Document Format (.PDF) or Comma Separated Value (.CSV) output. You can view the outputs of current and historic reports with success status.

You can run four different reports from **Reports > Standard Reports > View/Run Reports**.

| Use This Report | To |
|---|---|
| User Information | Get basic information on users such as status, user ID, security role, phone number, e-mail and business addresses. |
| Self Service User Status | Get information of self-service users who registered for specific ADP products/services. You can also get information of users who are not registered to your ADP service. This information is available only if your company sends user information to ADP. |
| Certified User Status | Get information such as security role, product profile, product role, and authorization codes as applicable. |
| Certificate Expiration | Get the expiration date and time of the digital certificates. |

## Report Tasks

You can perform any of the following tasks on your reports:

- Run a Report
- View a Report Output
- Refresh a Report Output
- Cancel a Report
- View a Report Output History
- Delete a Report
- About Reports
- Types of Reports
- Frequently Asked Questions

## Running a Report

To run a report, select **Reports > Standard Reports > Run/View Reports > Current**.

**1** Click on the name of the report you want.

**2** Enter or change the report ID as needed.

**3** Select filter options.

4 Select sorting options.

5 Select additional fields.

6 Click **Run**.

## Viewing a Report Output

You can view outputs of reports that have been executed and are in success status. To do this, select **Reports > Standard Reports > Run/View Reports > Current**.

1 Click the Action icon next to the report with success status.

2 Click on an output format.

## Refreshing a Report

You can refresh reports that have status as submitted, scheduled, or processing. To do this, select **Reports > Standard Reports > Run/View Reports > Current**.

1 Click the Action icon next to the selected report.

2 Click **Refresh**.

**Note:** The status of the selected report will be refreshed.

## Cancelling a Report

You can cancel reports that are in submitted, scheduled, or processing status. To do this, select **Reports > Standard Reports > Run/View Reports > Current**.

1 Click the Action icon next to the selected report.

2 Click **Cancel**.

## Viewing a Historic Report Output

You can view the history of a report that was run at different times. To do this, select **Reports > Standard Reports > Run/View Reports > Historic**.

1 Click the Action icon next to the report you want.

2 Click on an output format.

**Note:** The output options available vary based on the status of the report.

## Deleting a Report

You can delete current and historic reports that have status as submitted, scheduled, or processing. To do this, select **Reports > Standard Reports > Run/View Reports > Current**.

1 Click the Action icon next to the current or historic report.

2 Click **Delete**.

**3** In the Confirm Action window, click **Yes**.

**Note:** To delete one or more historic reports select the reports and click the Delete (-) icon.

# Contact Information Maintenance Tasks

You can perform any of the following contact information maintenance tasks:

- Change Your E-mail Address
- Activate Your E-mail Address
- Request a New Activation Code
- Change Your Contact Phone Number
- Activate Your Mobile Phone Number
- About Activating Your Contact Information
- About Text Messaging
- Frequently Asked Questions

## Changing Your E-mail Address

To change your e-mail address, select **Myself > Personal Information > Contact Information**.

1 In the Work and/or Personal e-mail address fields, enter a valid e-mail address.

2 Select the e-mail address that you access frequently for notification.

3 Click **Save**.

## Activating Your E-mail Address

You must activate your notification e-mail address to confirm it belongs to you and can be used when necessary. If you change the e-mail address associated with your account, you will receive a notification of change from ADP.

To activate your e-mail address, select **Myself > Personal Information > Activate Your E-mail/Mobile Phone**.

1 Select the e-mail address to send the activation code.

2 Click **Send Activation Code(s)**.

3 Enter the activation code you received from ADP.

4 Click **Submit**.

## Requesting a New Activation Code

You must activate your e-mail address and mobile phone numbers to confirm they belong to you and can be used when necessary.If you did not receive your activation code or your activation code has expired you must request a new activation code.

To request a new activation code, select **Myself > Personal Information > Activate E-mail/Mobile**.

1 Select the e-mail address and/or cell phone numbers.

2 Click **Send Activation Code.**

## Changing Your Contact Phone Numbers

To change your contact phone numbers, select **Myself > Personal Information > Contact Information**.

1 In the Phone number fields, enter your contact mobile phone numbers.

2 Select the mobile phone number you access frequently to receive text message from ADP.

3 Click **Save**.

## Activating Your Mobile Phone Number

You must activate your mobile phone numbers to confirm they belong to you and can be used when necessary. If you wish to receive forgotten credentials via your mobile phone, you must activate the mobile phone number associated with your account. If you change your mobile phone number associated with your account, you will receive a notification of change from ADP.

To activate your mobile phone number, select **Myself > Personal Information > Contact Information > Activate E-mail/Mobile**.

1 Select the mobile phone number.

2 Click **Activate E-mail/Mobile**.

3 Enter the activation code you received in a text message from ADP.

4 Click **Submit**.

## About Activating Your Contact Information

To confirm that you are the rightful owner of the contact e-mail address and mobile phone numbers associated with your account, ADP requires you to activate your contact information to receive your login information e.g., temporary password, user ID upon your request. If your contact information is not activated, the options to send your login information to your e-mail address and/or mobile phone numbers will not be available.

Activation can be done in one of the following ways:

- New employees can complete the activation of contact information during the employee self service registration process.When required, this task can also be performed from the Myself Tab.
- Existing employees must complete the activation of contact e-mail address and/or phone numbers from the Myself Tab.

**Note:** Employees and administrators/practitioners must activate their contact information after updating their account.

## About Text Messaging

ADP supports the use of text messaging to receive your login information e.g., temporary password, user ID upon your request. To get started with this process, you must select to use your mobile phone to receive text messages from ADP upon your request.

To confirm that you are the rightful owner of the contact mobile phone numbers associated with your account, ADP requires you to activate your contact information to receive your login information e.g., temporary password, user ID upon your request. Your mobile phone number must:

- Have a service from a supported mobile phone carrier.
- Be able to receive text messages.
- Not have a text message block.

**Note:** The complete Terms and Conditions associated with this feature is displayed adjacent to the mobile phone number fields on the **Myself > Contact Information** page.

## Frequently Asked Questions

**1** *How do I change my name associated with this account?*
You can contact your company administrator to update your name in your company records.

**2** *I changed my name associated with this account. How do I change my user ID?*
Your user ID was created when you first registered to access ADP services. Changing your name does not change your user ID. You can continue to use your existing user ID and password to access your ADP services. If required, your administrator can delete your user information, user ID from your company records and you can register with your updated name. However, the information previously associated with your record will not be available or associated with your new user ID. Contact your company administrator for assistance.

**3** *How often should I activate my contact e-mail address and mobile phone numbers?*
After you change your contact e-mail address and mobile phone numbers, you should activate it to confirm that is in service and available for use. If your activated mobile work phone becomes your mobile personal phone or vice versa, activation is not required.

**4** *During password change, why can I not use my previous passwords?*
To protect your account security, ADP's security policies do not allow the reuse of your last four passwords.

**5** *Are there any recommendations to increase the password strength?*
Yes. It is recommended that passwords be 12 or more characters and contain a mix of upper case and lower case letters, numbers, and special characters. For example, the mnemonic, “The first time I traveled to a foreign country I was 9 years old” can be used to create the password “tFt!t2@FC1w9y0” using the following techniques:

-Use the first letter of most words.
-Capitalize all letters in the first half of the alphabet.
-Use similar-looking substitutions i.e.,! for 1, 2 for “to”, @ for “a”, etc.

**6** *Why are previously selected security answers not displayed on the Security tab?*
ADP constantly updates its security policies and security questions that you can select from. To protect your account from unauthorized access, previously selected security answers are not displayed. When required, you can select from the current list of questions and enter answers to protect your account.

**7** *I'm not receiving an e-mail with an activation code. What can I do?*
Check your spam and junk mail folders.

**8** *I'm not receiving activation code via phone. What can I do?*
You can do one of the following:

-Make sure your carrier is supported. Refer to Terms and Conditions on the **Myself > Contact Information** page.
-Make sure your phone number doesn't have a premium message block on it.
-If it does, contact your carrier, remove it, and then follow instructions in the Terms and Conditions to turn messaging on.

# Account Security Maintenance Tasks

You can perform any of the following account security maintenance tasks:

- Change Your Password
- Change Your Security Questions and Security Answers
- About Your Security Information

## Changing Your Password

Go to **Myself > Personal Information > Security > Password**.

**1** To authorize a password change, enter your current password.

**2** Enter your new password.

**3** Re-enter your new password to confirm.

**4** Click **Save**.

## Changing Your Security Questions and Answers

Go to **Preferences > Security > Questions**.

**1** To authorize this change, enter your current password.

**2** To protect your account, select three different security questions.

**3** Enter a different security answer for each question.

**4** Click **Save**.

## About Your Security Information

To protect your ADP account, you select three different security questions and enter different security answers. For your security, the security questions and answers already associated with your account are not displayed.

If you forget your user ID, and/or password to your ADP account, you can use the Forgot Your Password and Forgot Your User ID links on your ADP service home page to retrieve your login credentials. During this process, you will be prompted to answer the security questions that you established to protect your account.

- If your entries match the information associated with your account, you identify yourself as the rightful owner of the account and can retrieve your user ID and/or reset your password.
- If your entries do not match the information associated with your account, you will not be able to retrieve your user ID and/or password. If you are unable to retrieve your account login information, be sure to avoid any typographical errors and retry your request. If the problem persists, contact your company administrator to request your user ID and/or reset your account password.

When you log in to your ADP service with your temporary password, you will be prompted to enter and confirm the new password. Use your new password to login to your account. Once you log on, be sure to update your security questions and answers to keep it current.

# Service Access Maintenance Tasks

You can perform any of the following service access maintenance tasks:

- View Your Services
- Add a Service
- Delete a Service

## Viewing Your Services

Go to **Myself > Service Access > Security > Manage Services**.

**1** View the ADP services that are available to you. Depending on your company setup, you may already have access to the ADP services available to you.

**2** Click on a different tab or option to navigate away from this page.

## Adding a Service

Go to **Myself > Service Access > Security > Manage Services**.

**1** Click **Add**, when available, to add the ADP service available to you. Depending on your company setup, you may already have access to the ADP services available to you.

**2** Follow the instructions on the page to complete adding this service.

## Deleting a Service

Go to **Myself > Service Access > Security > Manage Services**.

**1** Click **Delete**, when available, to delete the ADP service available to you. Depending on your company setup, you may not have access to delete the ADP services available to you.

**2** Follow the instructions on the page to complete this task.

# Chapter 3
# Setting User Access in ADP Workforce Now

As a security master, you were also set up as a portal administrator during the initial planning phase. Portal administrators are responsible for managing security access in ADP Workforce Now® for the modules your company is using.

After setting up users in the ADP security management service, your next task is to define which aspects of ADP Workforce Now each user should be permitted to see and use. Specifically, you will perform these tasks:

- Set up security groups to control user access in groups rather than one person at a time
- Create membership rules to further refine security group access

When you complete these tasks, you will have set up user access for this module and features:

- HR & Benefits module
- ADP Workforce Now features that affect all users, such as access to content on the company website

**Note:** You must complete the security management process, including assigning the ADP Workforce Now profile to the user, before you can complete the procedures described in this chapter.

# Logging On to the ADP Workforce Now Home Page

You must be logged on to ADP Workforce Now as a portal administrator to set up user access for ADP Workforce Now.

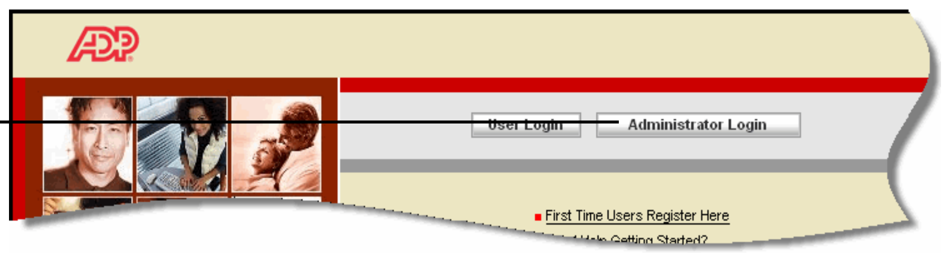
**Important:** During the planning phase, your ADP representative set up the security master and backup security master as a portal administrator. If you are an ADP security master and are unable to perform the procedures in this chapter, check with your ADP representative to make sure you have been assigned the correct security level.

To access the Portal Administrator role, follow these steps:

**Note:** Pop-up blockers may interfere with the display of valid pop-up screens (confirmations, forms, reports). ADP recommends that you disable pop-up blockers or set up your pop-up blocker to allow pop-ups for this site.

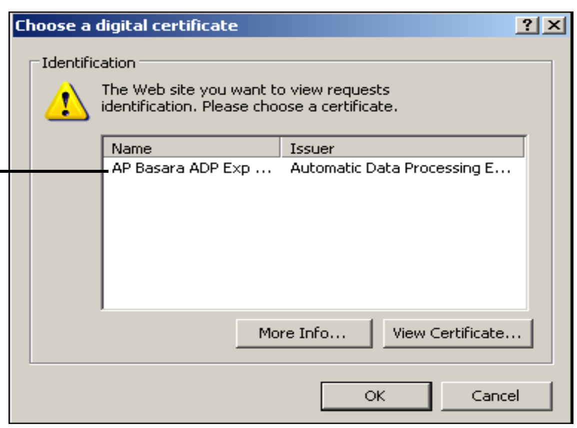
1. Go to: **https://portal.adp.com**
2. Click **Administrator Login**.

Digital certificate users click here to log on to ADP Workforce Now.



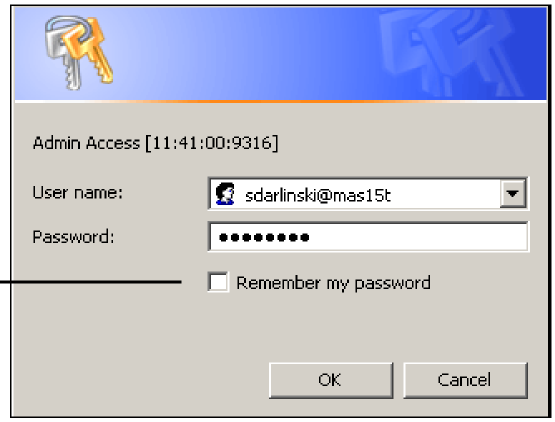

3. In the Choose a digital certificate window, select the certificate that was issued to you for your access to ADP Workforce Now, and click **OK**.

The digital certificate is labeled with your first name, last name, ADP, and the expiration date of the certificate.



**4** In the Connect window, enter your user ID and password, and then click **OK**.

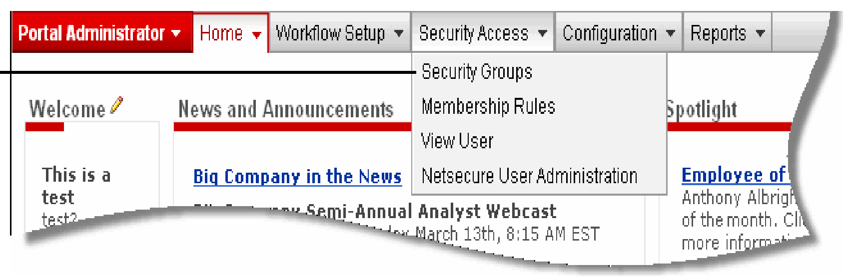
This check box is disabled for added security. You cannot select this option.




**5** In ADP Workforce Now, point to the Role Selector and select **Portal Administrator**. Notice that the menus change when you access the Portal Administrator role. The **Security Access** menu is now available.

**6** Point to the **Security Access** menu to see the available options.

From this menu, you can set up user access in ADP Workforce Now.



# Managing Security Groups

To begin assigning access to groups of users, review the security groups that are provided by ADP Workforce Now and remove permissions from the groups for features that you want to restrict from each group. These groups may include default security groups and automatically created custom security groups, depending on the modules your company is using. Removing a permission is as simple as deselecting the option describing the permission and saving the group.

If these groups don't meet your needs, you can create your own custom security groups of users and assign access at a more granular level. For example, you might want to create a security group called Non-Exempt Employees and restrict those employees from accessing specific features. New security groups can only be created after the master file has been loaded.

However, a user cannot be assigned to both a default security group and a custom security group of the same employee group type. For example, a user that is included in a custom employee security group that you create is no longer active in the default employee security group. Users can belong to more than one custom security group.

**Note:** You can view security groups that are set up for you and change certain information, such as the description, members, and permissions. You cannot delete a default security group, even if you are a security master, security administrator, or portal administrator.

## Default Security Groups

ADP Workforce Now has four default security groups. You can assign users to one or more of these groups so they view the appropriate content on the ADP Workforce Now Web site. These groups also affect the kind of information users can see in the ADP Workforce Now modules.

| Default Security Group | How Users Are Assigned |
|---|---|
| Administrator (Portal Administrator) | Users are automatically assigned the Portal Administrator role when you set them up with the ADP Workforce Now profile in ADP Netsecure.<br>The portal administrator requires a digital certificate and can control user access privileges and the appearance of the ADP Workforce Now Web site. |
| Practitioner | Users are automatically assigned the Practitioner role when you set them up with the ADP Workforce Now profile in ADP Netsecure.<br>Practitioner users require digital certificates and can access the services to which they have been assigned from those being used by their company. For example, a practitioner might only be assigned to the HR & Benefits module, even though the company is using all ADP modules. |

| Default Security Group | How Users Are Assigned |
|---|---|
| Manager | Users are automatically assigned the Manager role when you designate them as managers in one of the modules (Payroll, HR & Benefits, or Time & Attendance). This designation places the user in the Manager default security group as well.<br>Managers supervise employee tasks and oversee work events. |
| Employee | All users are automatically assigned the Employee role. You can give employees additional access by assigning them to other security groups.<br>Employees can view and update personal information. |

**Important:** Members of these default security groups can include independent contractors, consultants, and 1099 employees who used their Employer Identification number to verify their identify while registering for ADP services. These users have access to certain areas of ADP Workforce Now, depending on the product profiles that were assigned to them. For example, some employees can access ADP services to view their ADP pay statements and/or 1099s.

If needed, you can set up custom security groups for these users to further manage what the users can see on the site. For example, you may want certain users to view only the menu options they can access. For information on setting up custom security groups, refer to "Adding a Custom Security Group" on page 70.

## Automatically Created Custom Security Groups

In ADP Workforce Now, four custom security groups with associated membership rules and permissions are automatically created if your company is using one of these combinations of modules:

- Payroll and Time & Attendance
- Payroll, HR & Benefits, and Time & Attendance

These groups ensure that employees, supervisors, and managers can see and use the appropriate information.

| Automatically Created Custom Security Group | Description |
|---|---|
| Payroll and HR Employees | This group contains users who are listed as employees in the Payroll and HR & Benefits modules. |
| Payroll and HR Managers | This group contains users who are listed as managers in the Payroll and HR & Benefits modules. |
| Time and Attendance Employees | This group contains users who are listed as employees in the Time & Attendance module. |
| Time and Attendance Supervisors | This group contains users who are listed as supervisors in the Time & Attendance module. |

For example, Michael Jones is an employee whose company is using the Payroll, HR & Benefits, and Time & Attendance modules. Michael has been automatically added to the Payroll and HR Employees group. He has also been automatically added to the Time and Attendance Employees group.

When Michael points to the **Time & Attendance** menu in ADP Workforce Now, he sees all the menu options he is supposed to. He can submit a timecard, enter time off, and review his accruals.

**Important:** When users are moved into automatically created custom security groups of the same employee type as their default security group, they remain in the default group, but as inactive members, with their name and information grayed out. To make these users active in the default group, you need to remove them from the corresponding custom groups. (See "Adding or Removing Members from a Security Group" on page 79.

## Membership Rules

Each automatically created membership rule has the same name as its associated custom security group. For example, the membership rule name for the Payroll and HR Employees group is Payroll and HR Employees.

**Important:** If you set up a custom security group for terminated employees, you must add an active status to the membership rule for each automatically created custom security group of the employee type. This makes terminated employees inactive in their automatically created custom employee group(s), so the employees do not view content they should not see. For more information, refer to "Changing a Rule for an Automatically Created Custom Security Group" on page 92.

## Permissions

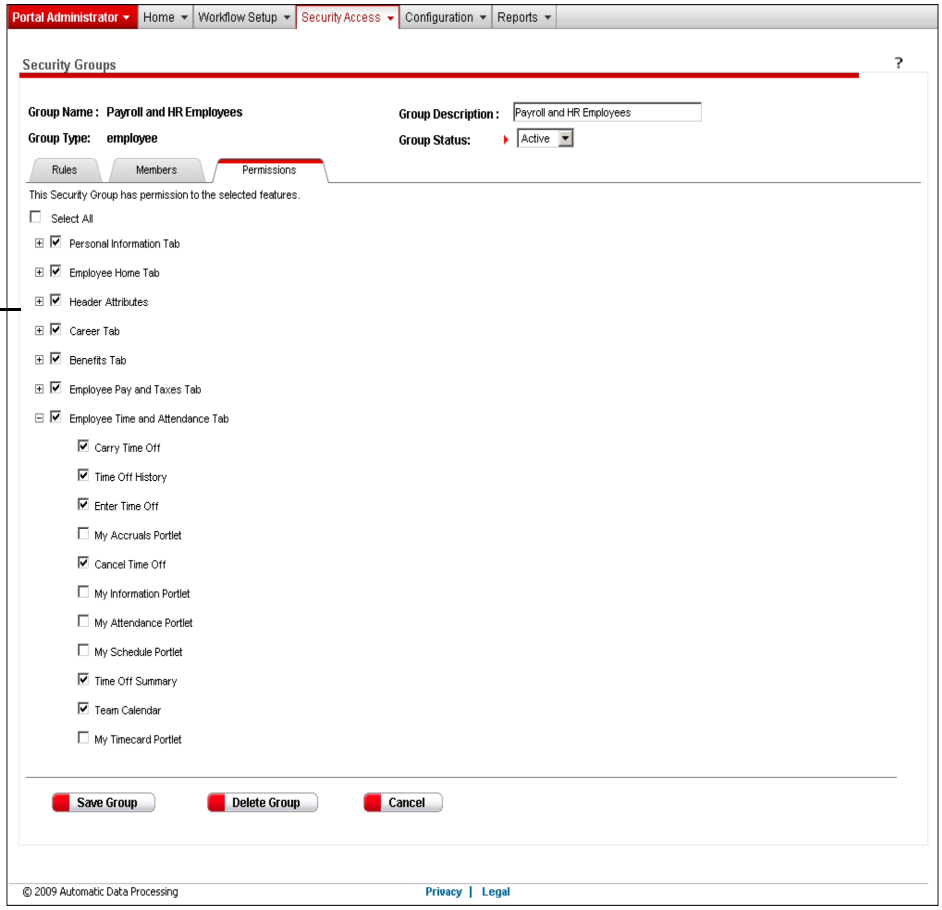
Because permissions for automatically created custom security groups are already set up, you do not need to make any manual changes to them.

The following sample screen shots show the permissions that are automatically set up for each of these groups.

**Note:** These sample screen shots show selections for users whose company is using the Payroll, HR & Benefits, and Time & Attendance modules. Your screens may look slightly different depending on your company setup.

### Payroll and HR Employees

Under **Employee Time and Attendance Tab**, all features provided by the Time & Attendance module are unchecked.



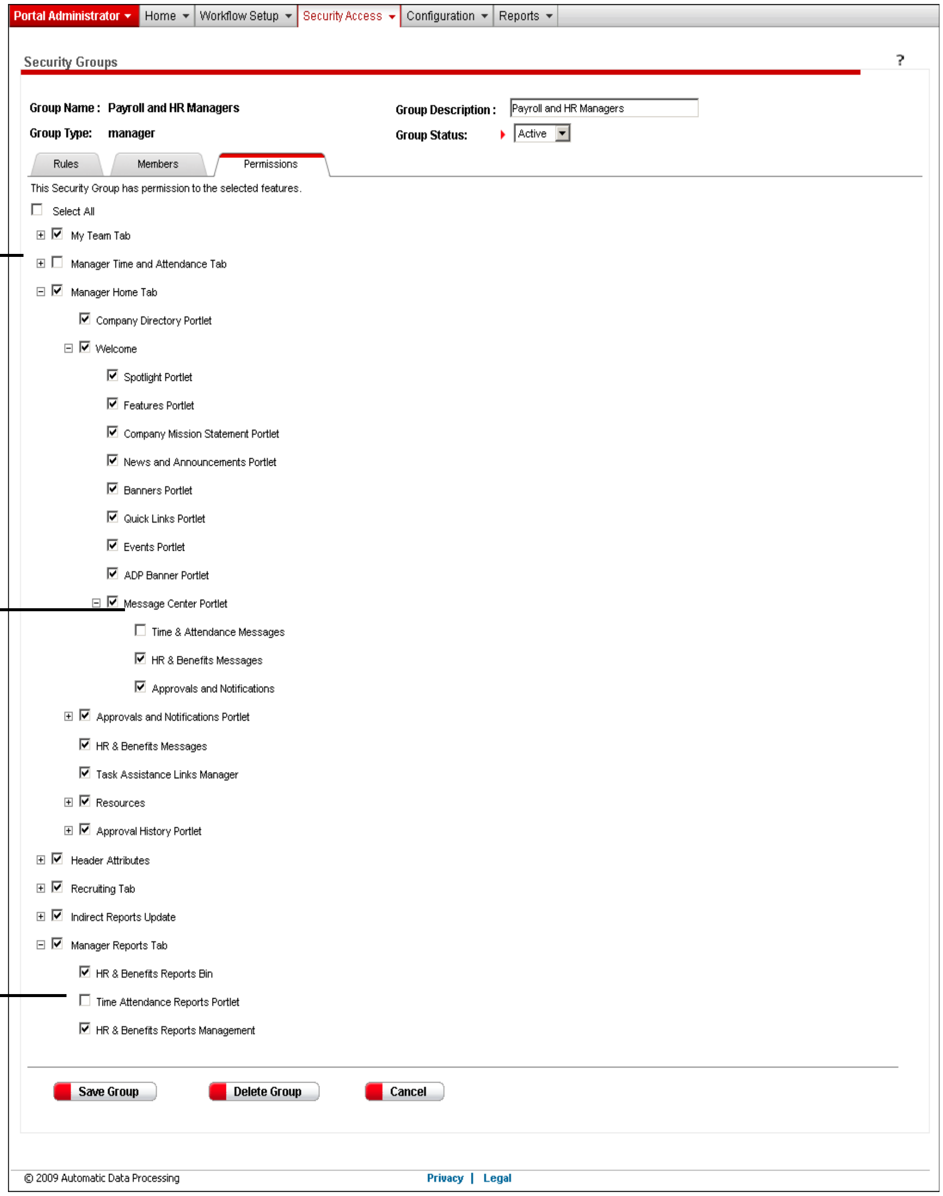

**Note:** If your company is using the HR & Benefits module, you will see permissions selected under **Employee Time and Attendance Tab** for features that are provided by the HR & Benefits module, as shown above.

### Payroll and HR Managers

**Manager Time and Attendance Tab** is unchecked.

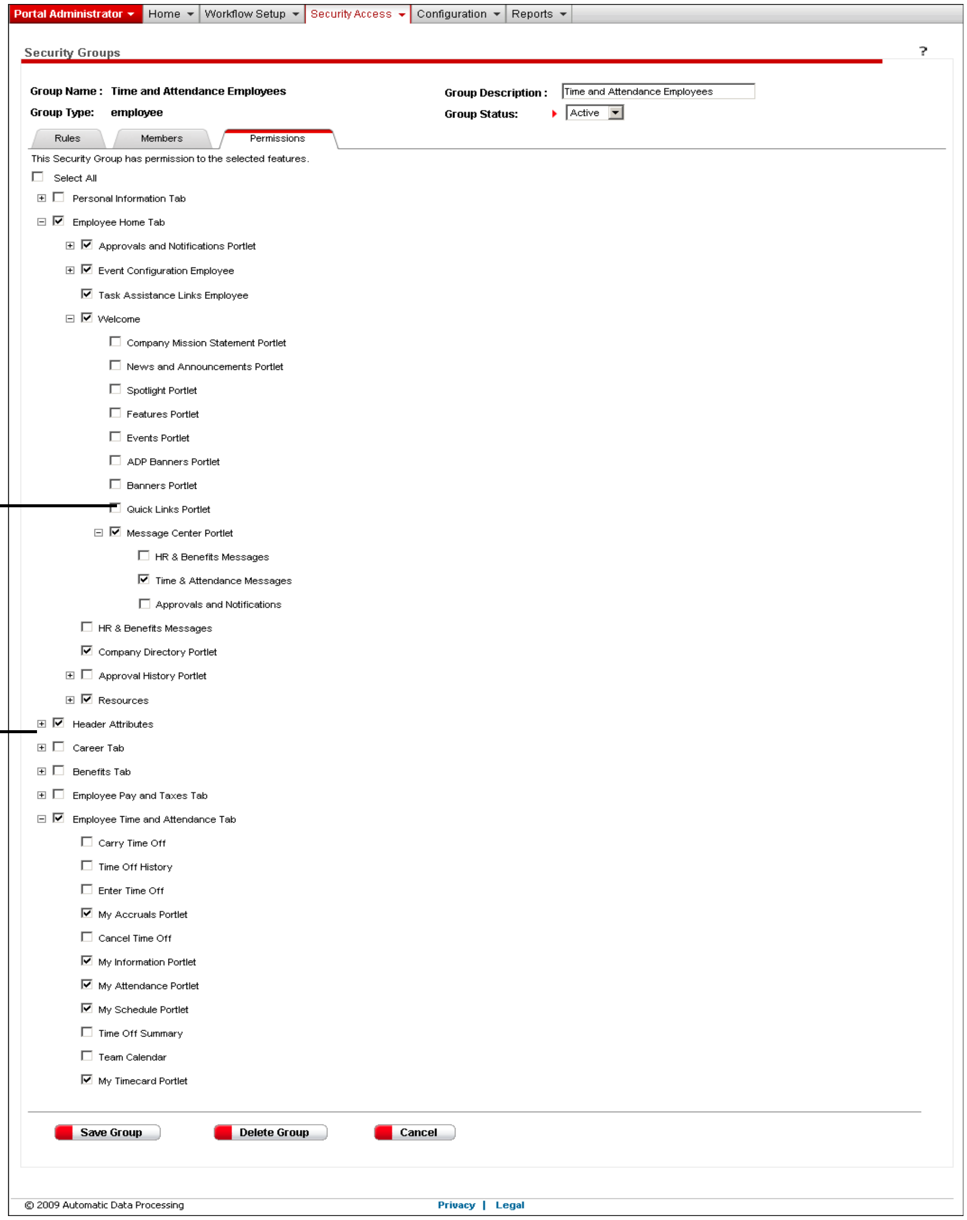
Under **Message Center at a Glance**, **Time & Attendance Messages** is unchecked.

Under **Manager Reports Tab**, **Time Attendance Reports** is unchecked.




**Note:** Other features under **Message Center at a Glance** and **Manager Reports Tab** are selected. The features you see are based on the modules your company is using.

## Time and Attendance Employees




Under **Message Center at a Glance**, **Time & Attendance Messages** is selected. **HR & Benefits Messages** is unchecked.

Under **Employee Time and Attendance Tab**, only features provided by the Time & Attendance module are selected.

---

**Note:** If your company is using the HR & Benefits module, you will see features unchecked under **Employee Time and Attendance Tab** for features that are provided by the HR & Benefits module, as shown above.

---

## Time and Attendance Supervisors

Under **Manager Time and Attendance Tab**, all features are selected.

Under **Message Center at a Glance**, **Time & Attendance Messages** is selected. **HR & Benefits Messages** is unchecked.

Under **Manager Reports Tab**, only **Time Attendance Reports** is selected.


**Note:** The features you see are based on the modules your company is using.

## User Assignments

The following table shows how Payroll, HR & Benefits, and Time & Attendance users are assigned to the automatically created custom security groups.

| User | Custom Security Group Assignment(s) |
|---|---|
| • Payroll and HR Manager | • Payroll and HR Managers<br>• Payroll and HR Employees |
| • Time and Attendance Supervisor | • Time and Attendance Supervisors<br>• Time and Attendance Employees |
| • Payroll and HR Employee | • Payroll and HR Employees |
| • Time and Attendance Employee | • Time and Attendance Employees |
| • Payroll and HR Manager<br>• Time and Attendance Supervisor | • Payroll and HR Managers<br>• Payroll and HR Employees<br>• Time and Attendance Supervisors<br>• Time and Attendance Employees |
| • Payroll and HR Manager<br>• Time and Attendance Employee | • Payroll and HR Managers<br>• Payroll and HR Employees<br>• Time and Attendance Employees |
| • Payroll and HR Employee<br>• Time and Attendance Supervisor | • Payroll and HR Employees<br>• Time and Attendance Supervisors<br>• Time and Attendance Employees |
| • Payroll and HR Employee<br>• Time and Attendance Employee | • Payroll and HR Employees<br>• Time and Attendance Employees |

# Viewing the Security Groups That Are Set Up for You

When employees register for ADP Workforce Now, they are assigned to one or more of the security groups in ADP Workforce Now. Review the permissions associated with each group so that you are aware of what users in each security group can see and do.

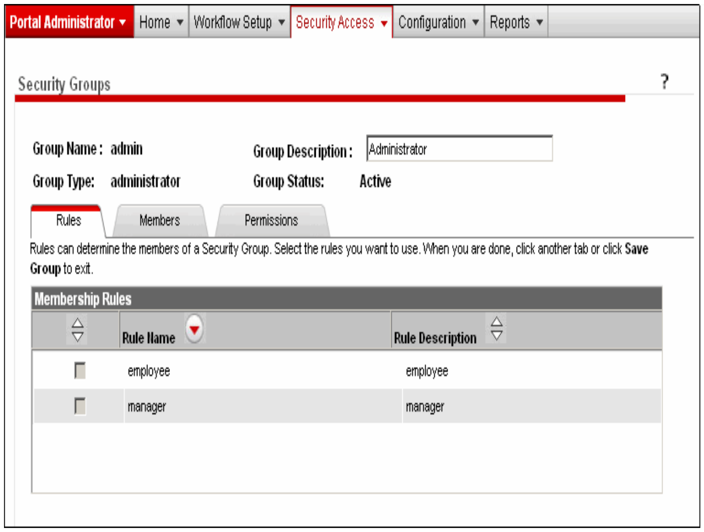
1 Point to **Security Access** and select **Security Groups**.

   The Security Group page lists all security groups that are currently defined.

2 Click the name of the security group you want to see.

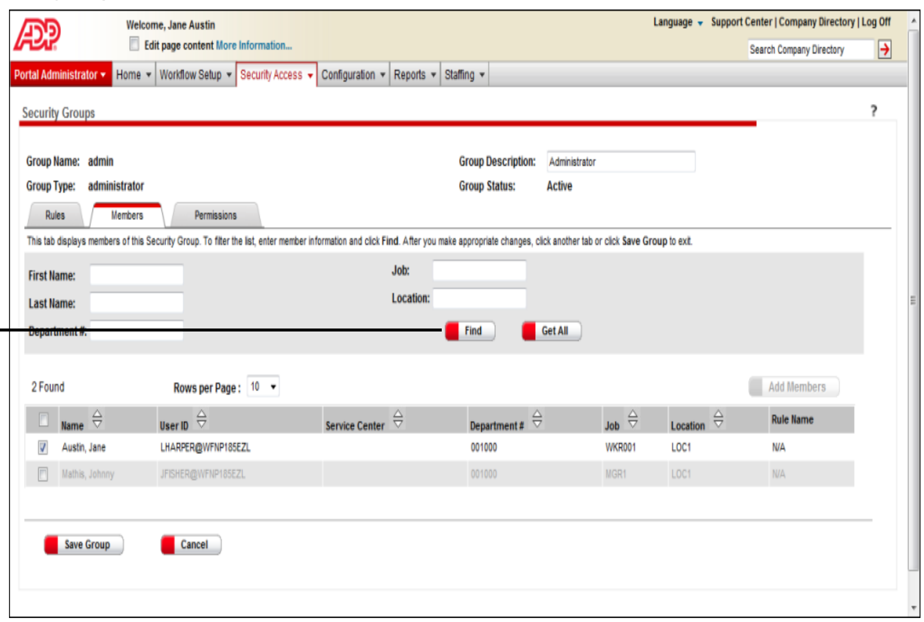
**3** On the **Rules** tab, view the membership rules for the security group.

In the following example, the **Rules** tab shows that members of the default administrator security group are also assigned to the default employee and default manager security groups.




**4** For a list of users who belong to a security group, select the **Members** tab. If the check box next to the employee's name is selected, the user is already a member of this group.

To locate a specific user, enter information in the search fields and click **Find**. **Tip**: To return the complete list, click **Get All**.

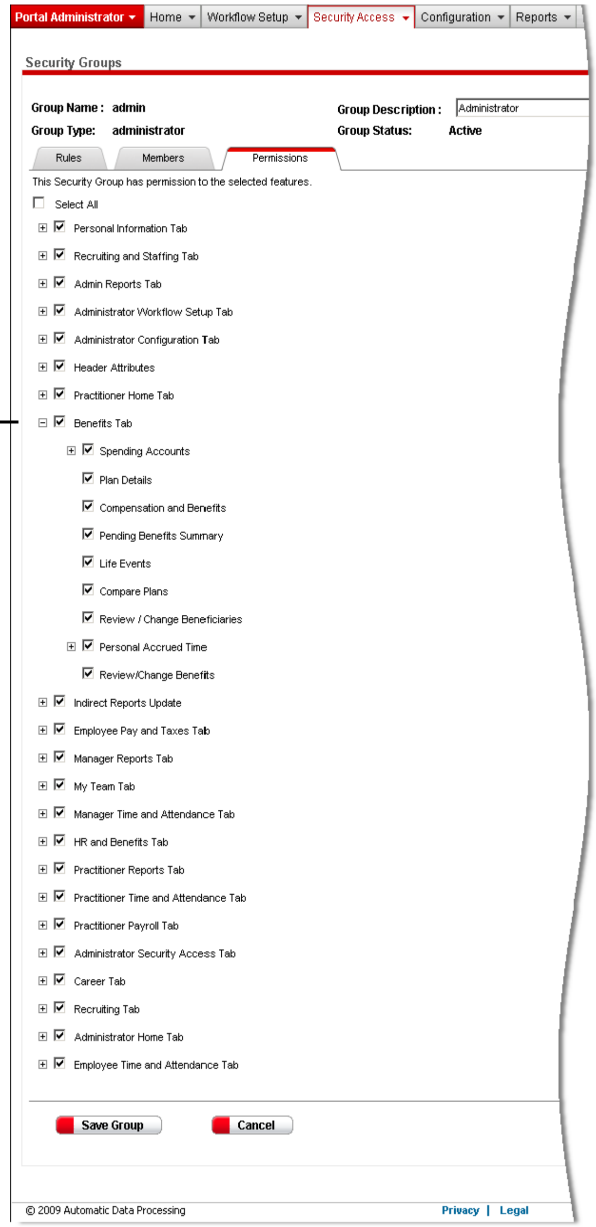



**Important:** The names and information of users in the default employee group and/or default manager group are grayed out if they are members of custom groups of the same type (employee or manager).

**5** To see the access rights that users have, select the **Permissions** tab. If the check box next to the feature is selected, the security group has permission for this feature.

**Note:** Individual users have permissions from all the groups to which they belong. To view the entire list of permissions for an individual user, see “Viewing User Permissions and Security Group Assignments” on page 83.

Click + to expand the list, or click - to collapse the list.




If needed, you can change a security group that has been set up for you, such as the corresponding description, members, and permissions. What you can change depends on whether the group is a default security group or a custom security group. For further instructions, refer to “Changing a Security Group” on page 77.

# Adding a Custom Security Group

If the security groups that are set up for you do not meet your company's needs, you can define your own groups to control user access. For example, you may need to add a custom security group for employees who have worked at the company less than 30 days. The users in this group could have a restricted view of content on the site until they have worked for 30 days or more.

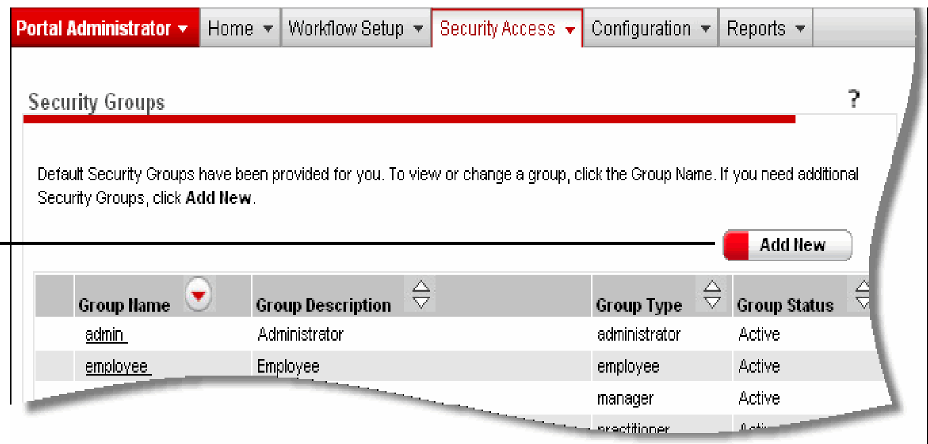
**Important:** The permissions you assign to a security group are accessible to all users in that group. As a result, it is important to make sure you (1) set up the group with the appropriate permissions and (2) add the appropriate users to the group.

To create a custom security group, follow these steps:

**1** Point to **Security Access** and select **Security Groups**.

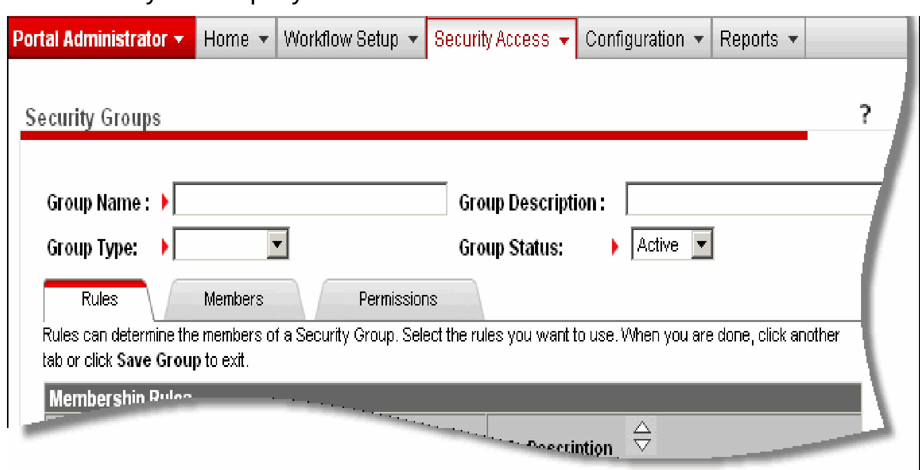
**2** Click **Add New**.

**Add New** button




**3** In the **Group Name** and **Group Description** fields, type information to help you identify members that belong to this group.

Be sure the name and description differentiate this group from other security groups. The name and description should be clearly understood by you and other administrative users in your company.



**4** Select a **Group Type**. Group type determines the members of a security group and the features and permissions that can be assigned to it. For example, if you select **employee** in the **Group Type** field, membership will be restricted to employees and permissions will be restricted to employee features.

Employees can belong to multiple group types. For example, Anthony Albright can be a member of an administrator group type and an employee group type. If the two groups have different permissions, Anthony will have access to all the features of both groups.

Employees can also belong to multiple custom groups of the same type. For example, John Smith can be a member of the New Jersey Employees group and also part of the HR Employees group. If the two groups have different permissions, John Smith will have access to all the features of both groups.

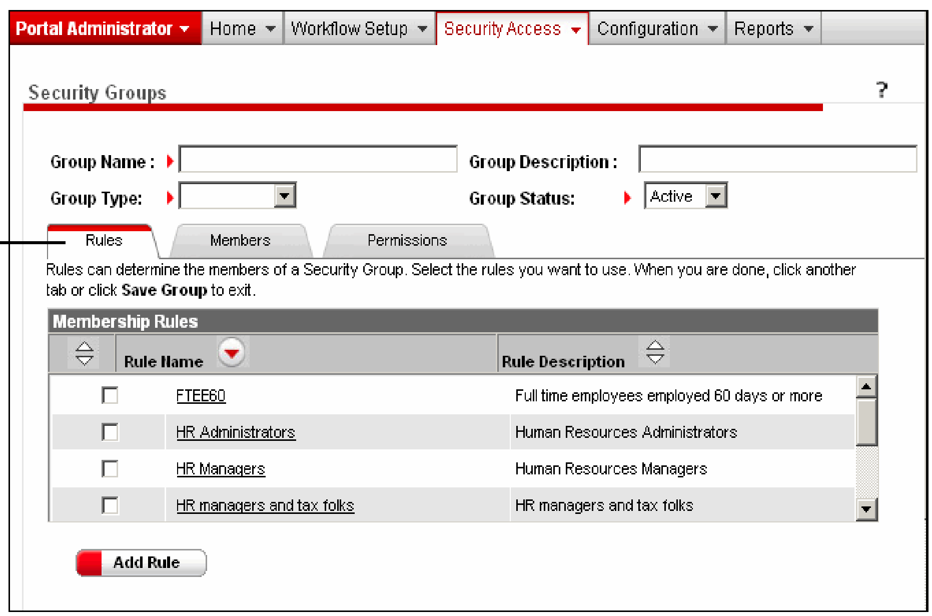
**5** Select a **Group Status**. You can deactivate a group if you want to temporarily remove it from use. Group status determines whether or not a group is currently used. For example, you may want to create a group for seasonal employees. Group status enables you to switch the group from active to inactive depending on when these seasonal employees start and stop working.

**6** Click **Save Group**. If you selected an active group status, users logging on are immediately impacted. The users already logged on are impacted at their next logon.

**7** To further define the security group, select the **Rules** tab. You can either click a check box to select an existing rule, or click **Add Rule** to create a new rule. For detailed instructions on adding a rule, refer to "Adding a Membership Rule" on page 86.

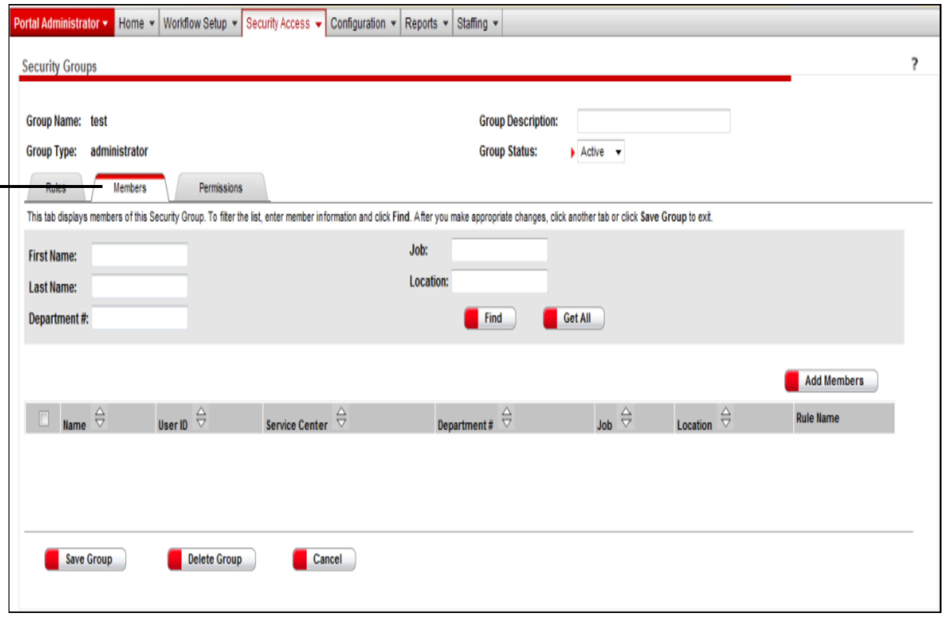
**Note:** If you don't see the **Rules** tab, speak with your ADP representative.

**Rules** tab



**8** To view members who meet the criteria for group type and members who were generated by membership rules, select the **Members** tab. To add members, click **Add Members**. To remove members, click to clear the appropriate check boxes. For detailed instructions on adding or removing members, refer to “Adding or Removing Members from a Security Group” on page 79.

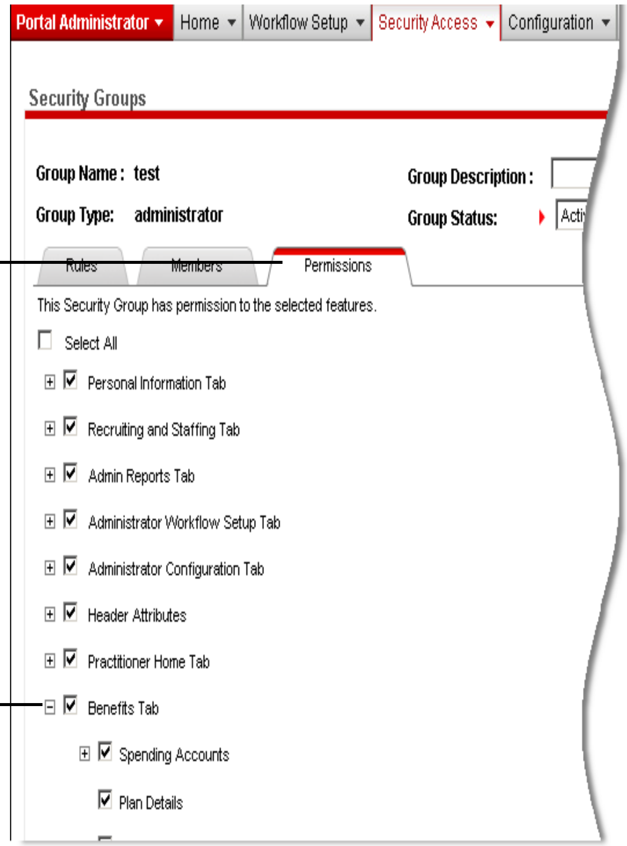
**Members** tab



9 To assign features to this security group and select whether the members can view, update, add, or delete information on the site, select the **Permissions** tab. Click to select or clear permissions. If the check box next to a feature is selected, users have permission to use this feature.

**Permissions** tab

Click + to expand the list, or click - to collapse the list.




10 When you are done with this custom security group, scroll to the bottom of the page and click **Save Group**.

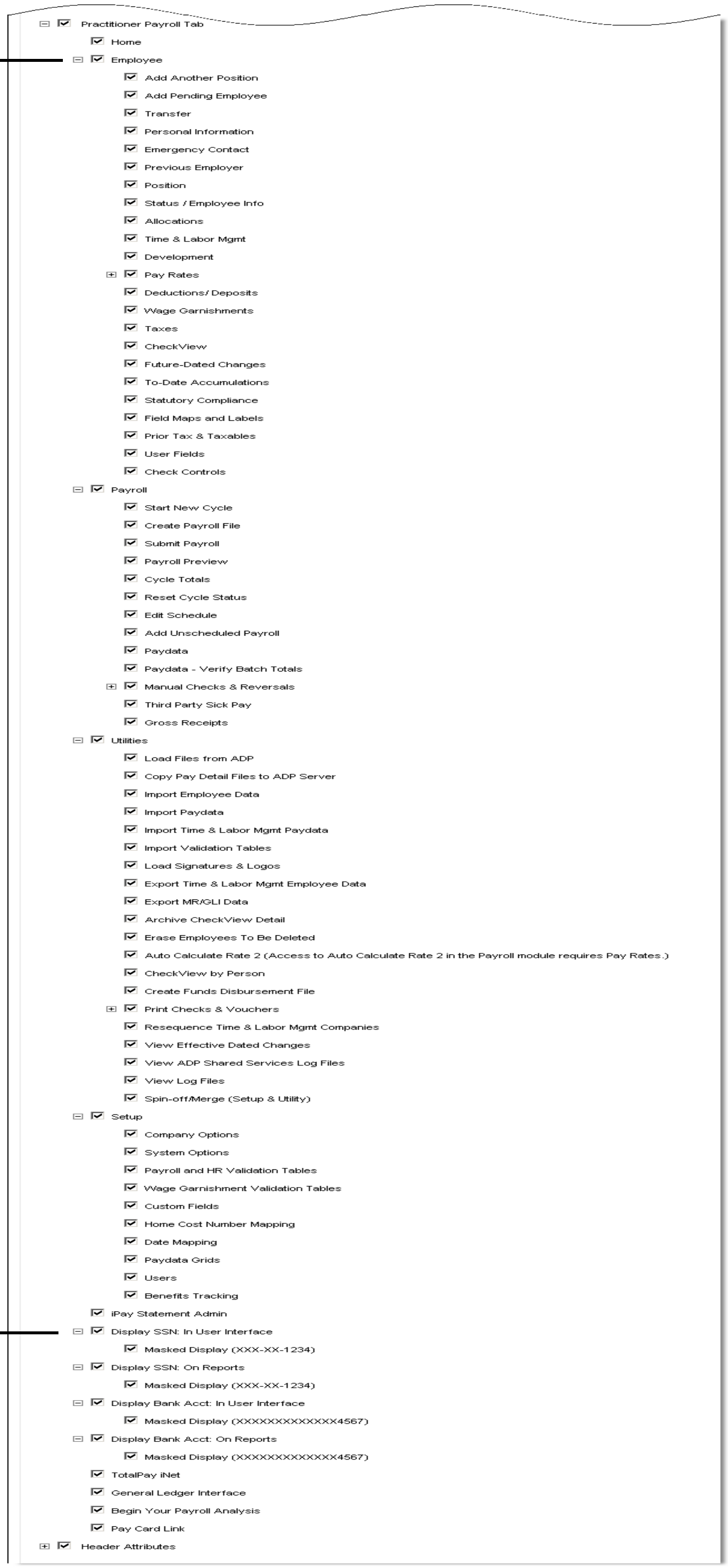
## Example: Custom Security Groups for Practitioners

You can manage access rights for different practitioners by creating custom security groups for them with the permissions you want them to have. For example, you may have payroll practitioners who only complete certain tasks in the Payroll module, or time and attendance practitioners who only set up schedules and assign them to employees. By restricting permissions, you create partial practitioner access.

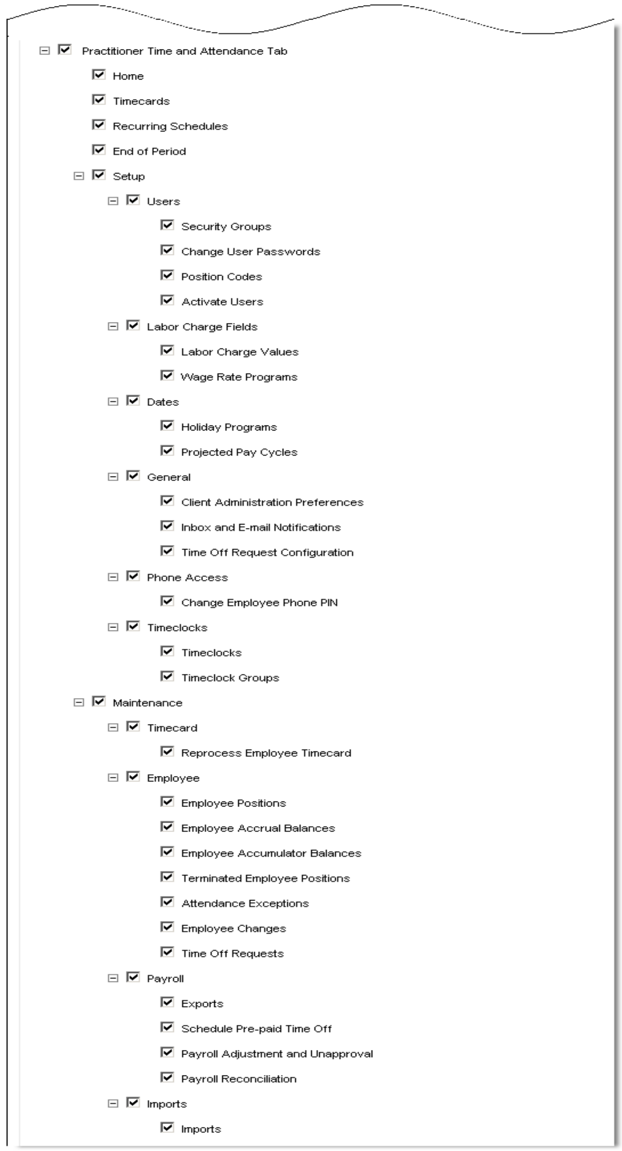
You can manage practitioner permissions for the Payroll module under **Payroll Practitioner Tab**.

Click + to expand the list, or click - to collapse the list.

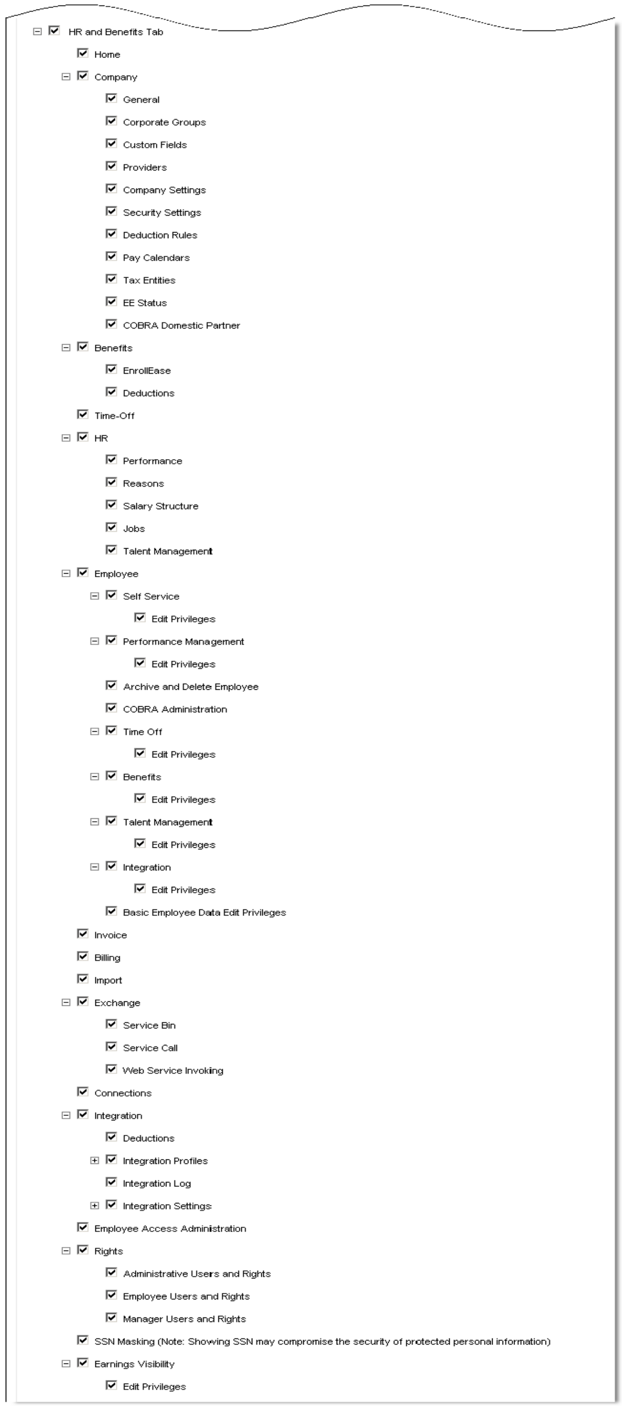
Choose to mask the display of Social Security numbers and bank deposit account numbers in this area.



You can manage practitioner permissions for the Time & Attendance module under **Practitioner Time and Attendance Tab**.



You can manage practitioner permissions for the HR & Benefits module under **HR and Benefits Tab**.



## Custom Security Groups for the New Hire Feature

If your company is using checklists for new hires that are provided by the New Hire feature, you need to set up custom security groups for the employees and managers to whom these checklists are assigned.

**Important:** You must name these custom security groups correctly and assign permissions carefully. For details, refer to Chapter 7, "Setting Up Custom Security Groups for New Hire Checklists" on page 157.

# Changing a Security Group

You can change the setup of a security group to better meet your company's needs. Changing an active security group immediately impacts all users in that group who are logging on. Users who have already logged on are affected the next time they log on.

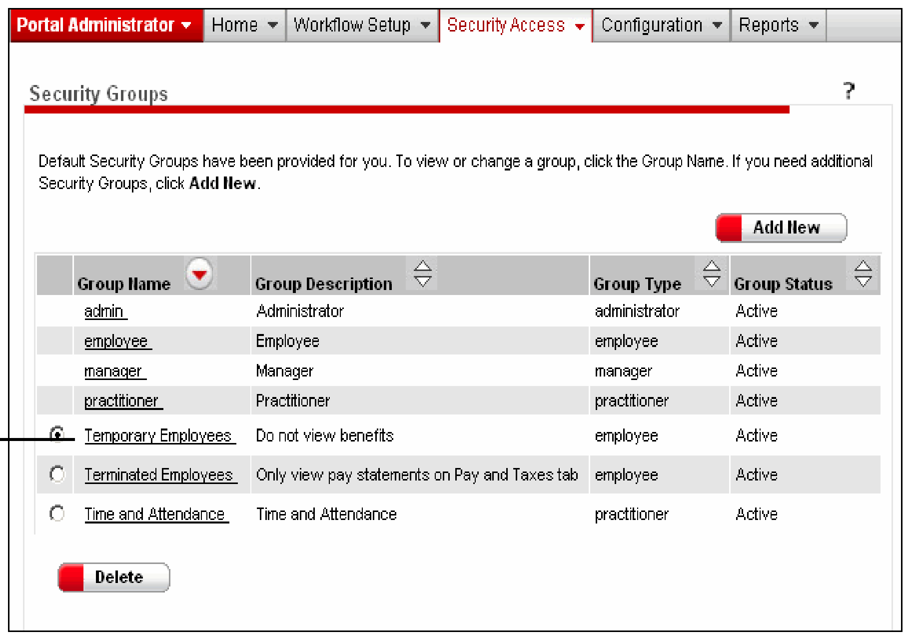
You change the description, members, and permissions for all groups. You can also change the status and membership rules for custom groups.

1 Point to **Security Access** and select **Security Groups**.

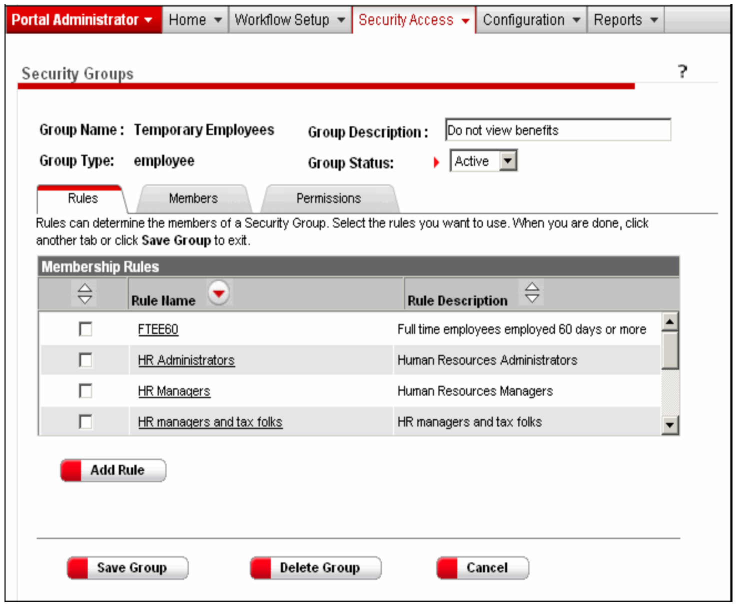
2 Click the name of the security group you want to change.

**Tip:** If your company uses membership rules, you can place your cursor over any custom security group to identify rules assigned to it.

Custom security group



**3** If needed, change information in the **Group Description** field.



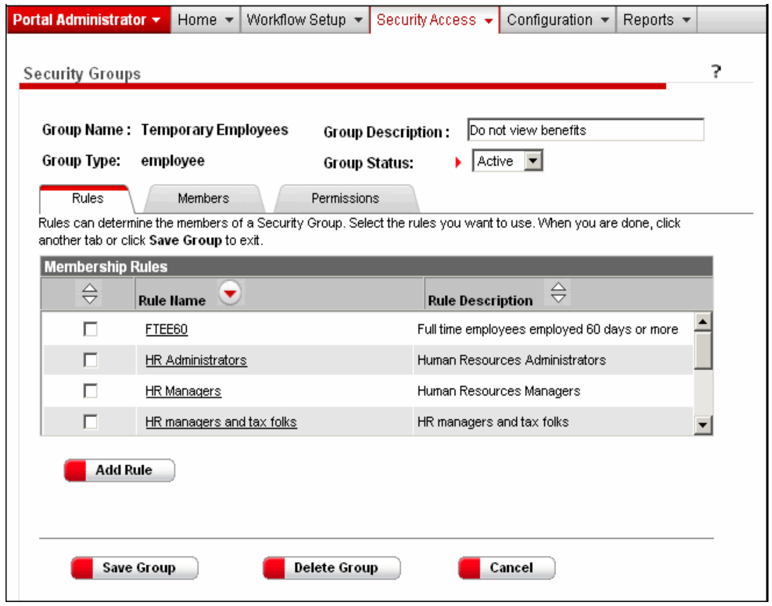

**4** If needed, change information in the **Group Status** field. This option is only available for custom groups.

**Important:** When you change a group status to active, users in that group who are logging on are immediately impacted. Users in that group who are already logged on are impacted at their next logon.

**5** If needed, add or remove membership rules. This option is only available for custom groups.

- For existing rules, either click to select or click to clear the appropriate check box.
- To add a new membership rule, click **Add Rule**.

For detailed instructions, refer to “Managing Membership Rules” on page 86.




**6** If needed, add or remove members. Instructions for this task follow in this section of the chapter.

**7** If needed, change the permissions for your group. Instructions for this task follow in this section of the chapter.

**8** When you are finished making the changes to your security group, scroll to the bottom of the page and click **Save Group**.

## Adding or Removing Members from a Security Group

**Important:** The permissions you assign to a security group are accessible to all users in that group. As a result, it is important to make sure you (1) set up the group with the appropriate permissions and (2) add the appropriate users to the group.

**1** Point to **Security Access** and select **Security Groups**.

**2** Select the group name to which you want to add or remove a member.

**3** Select the **Members** tab.

**Note:** If your company does not use the Membership Rules feature, you are automatically on the **Members** tab when you select the group name.

**4** Do one of the following:

- For an existing member, enter member information (such as last name) and click **Find**.
- For a new member, click **Add Members**. Click to select or clear the check box next to the member's name.

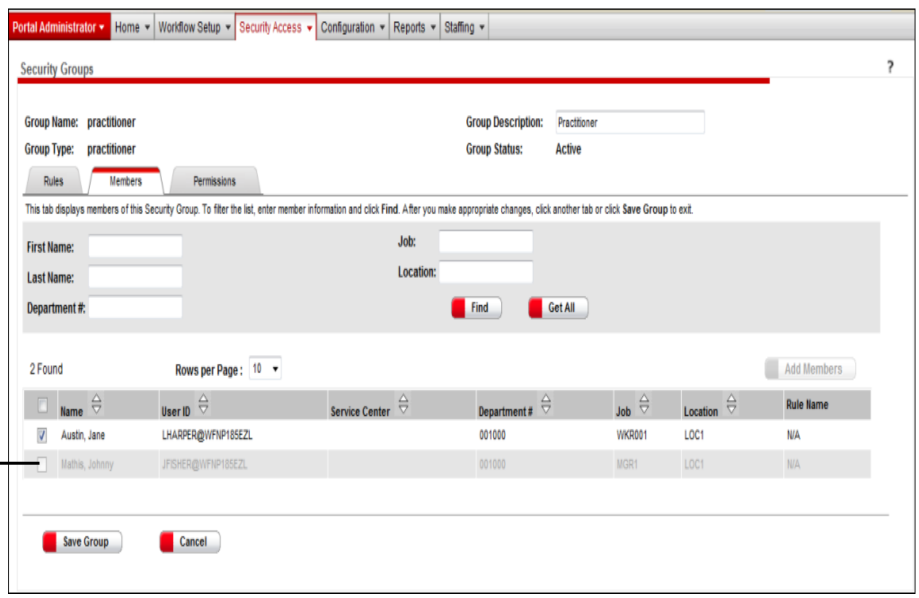
**Note:** If you removed a member who was generated by a rule, that user remains in the member's list with the name and information grayed out and the check box not selected. If you want to make the user active in the group again, click to select the check box next to the user's name.

**5** Click **Save Group**.

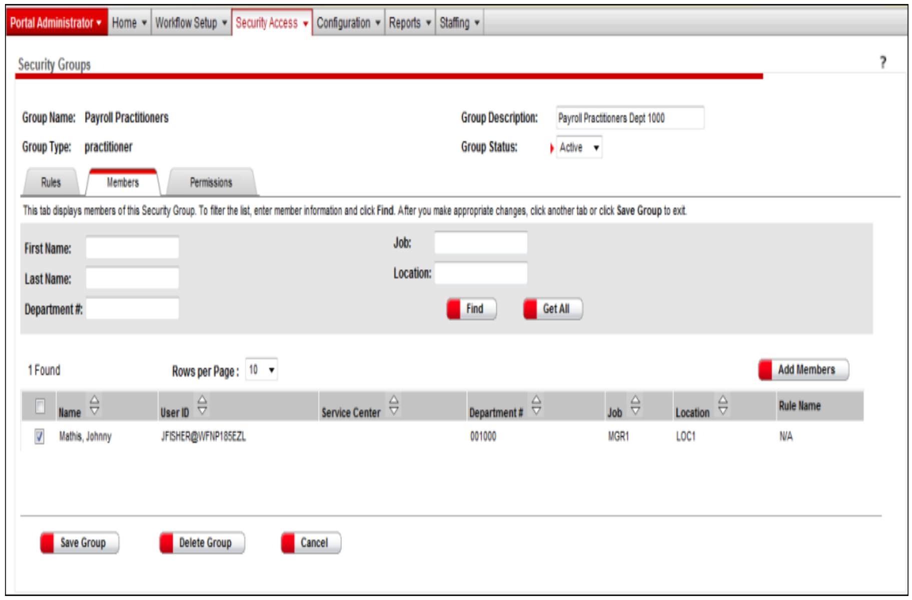
**Important:** When users are moved into custom groups of the same employee type as their default security group, they remain in the default group, but as inactive members, with their name and information grayed out. To make these users active in the default group, you need to remove them from the corresponding custom groups. After you do this, the users are automatically made active in the default group.

For example, Johnny Mathis is a member of a custom practitioner group that has partial access to payroll data. His name and information are grayed out in the default practitioner group.

Johnny Mathis is inactive in the default practitioner group.

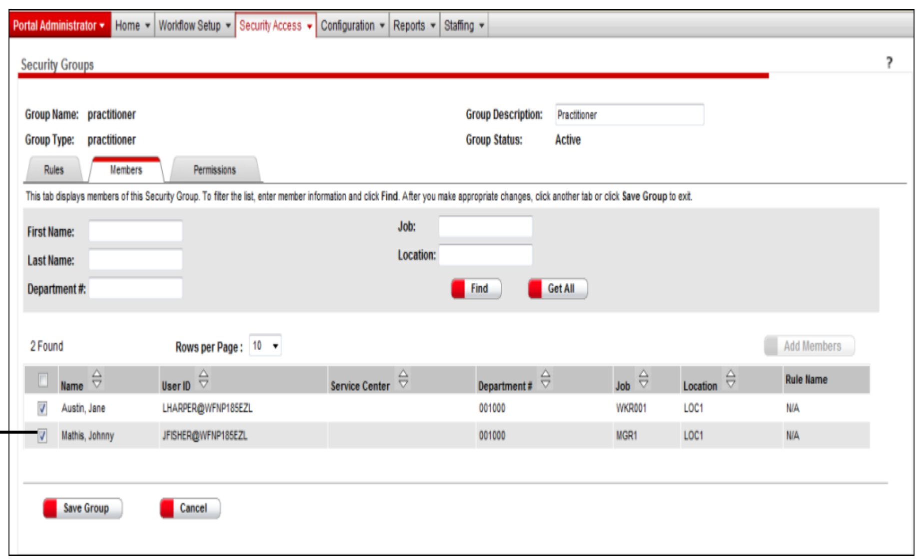


You want to give Johnny Mathis full access as a practitioner by making him active in the default practitioner group. From the custom practitioner group, click to clear the check box next to Johnny Mathis' name.




**Result:** Johnny Mathis is automatically an active member of the default practitioner group. His name and information are no longer grayed out, and the check box next to his name can now be selected.

Johnny Mathis is now active in the default practitioner group.




## Adding Permissions to a Security Group

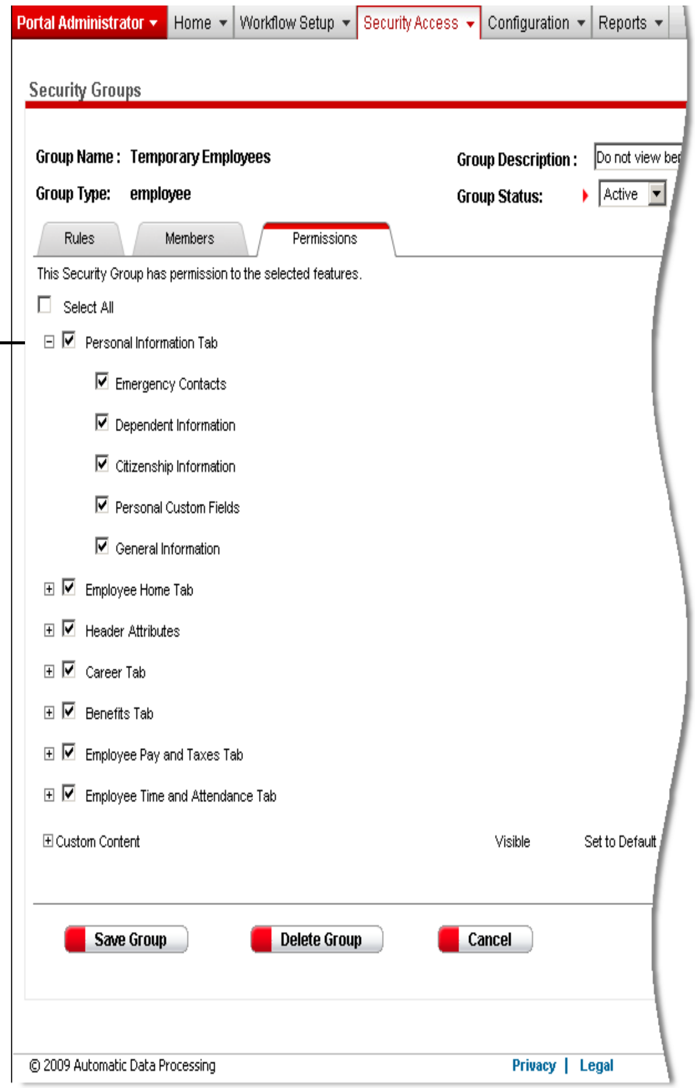
You can give members of a security group permission to access specific features.

1. Point to **Security Access** and select **Security Groups**.
2. Select the group name for which you want to add permissions.

**3** On the **Permissions** tab, select the tab name, features, and whether members can view, update, add, or delete information.

**Note:** If you have assigned custom content to a security group, it is included as a permission at the bottom of this page.

Click + to expand the list, or click - to collapse the list.




**4** Click **Save Group**.

## Changing Security Group Permissions

To change the ADP Workforce Now features to which members have access to use, select the **Permissions** tab. If the check box next to a feature is selected, users have permission to use this feature. You can change if necessary.

**1** Point to **Security Access** and select **Security Groups**.

**2** Select the group name for which you want to change permissions.

3 On the **Permissions** tab, click to select or clear the tab name, features, and whether members can view, update, add, or delete information.

**Tip:** Click the + to view all the features under each category.

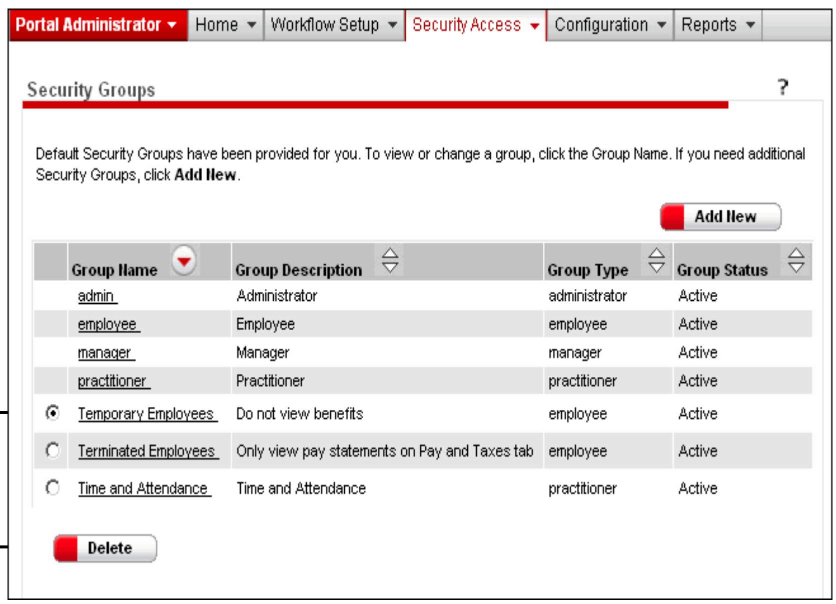
4 Click **Save Group**.

**Note:** If you want to restrict everyone's access to a specific feature, check all of the security groups that have been set up for your company and remove the permission from the groups as needed. To restrict access for one type of user, such as employees, remove the permission from the default security group and all custom security groups of the same user type.

## Deleting a Custom Security Group

Portal administrators can delete custom security groups. Default security groups cannot be deleted.

1 Point to **Security Access** and select **Security Groups**.




Custom security group

Delete option

2 Click to select the radio button next to the custom security group you want to delete.

3 Click **Delete**.

4 Click **OK** to confirm your deletion.

## Viewing User Permissions and Security Group Assignments

The View User feature allows portal administrators to see the security groups to which a user belongs as well as the comprehensive permissions for those groups.

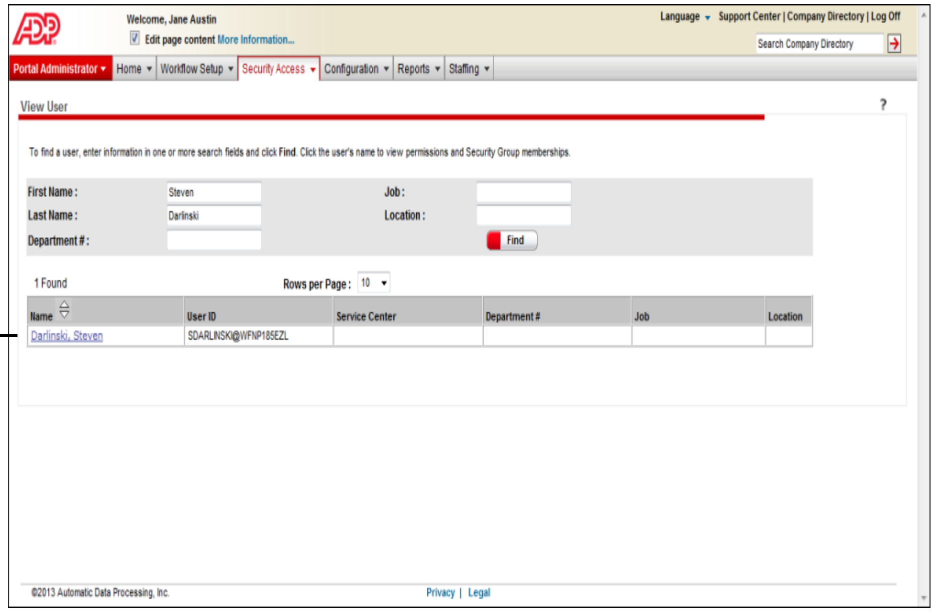
1 Point to **Security Access** and select **View User.**

2 Enter user information in one or more search fields and click **Find**.

**3** In the list of users, click the user's name.

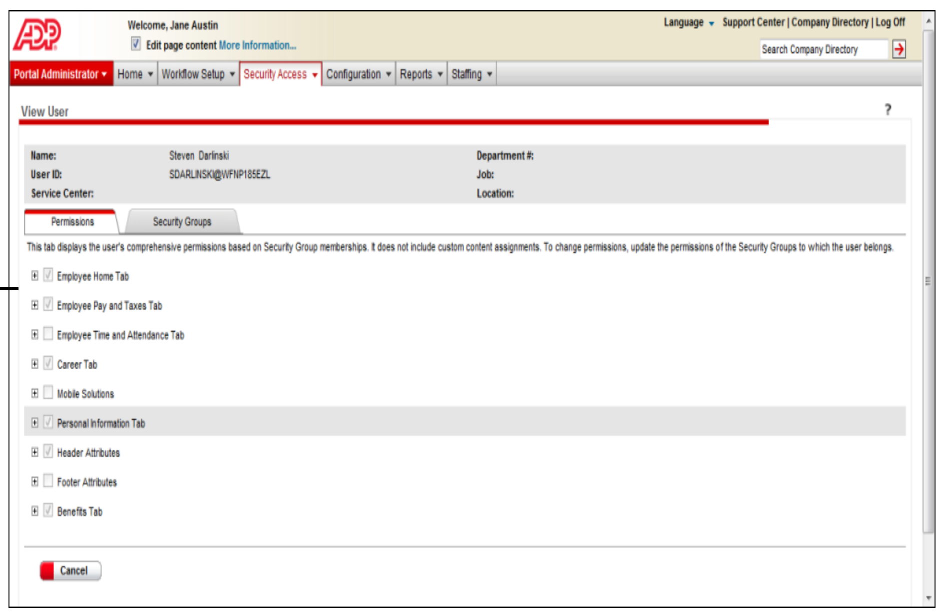
**Note:** Feature permissions are assigned to a security group and to individual employees. To change user permissions, you must change permissions for the associated security group or create a new security group for the employee.

User's name

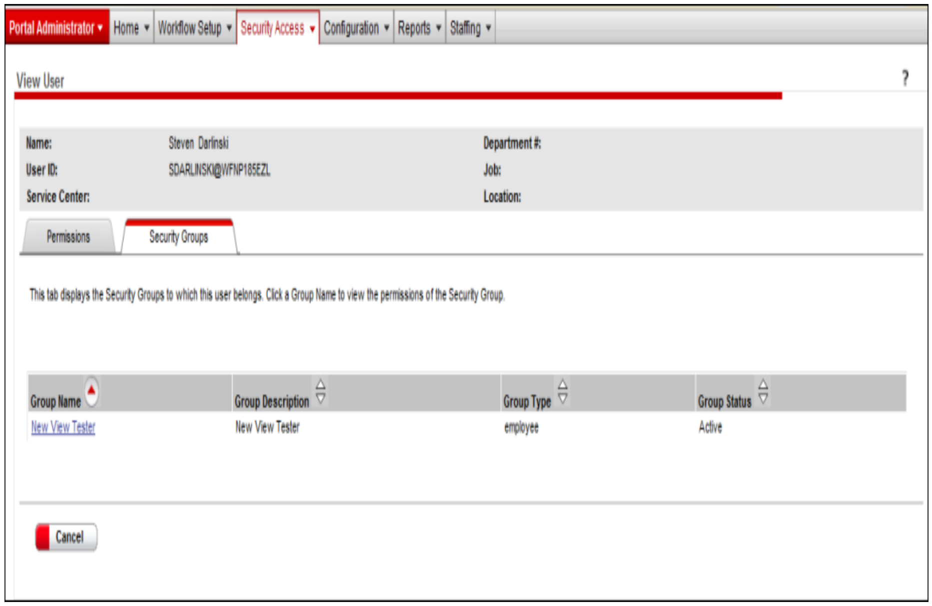



**4** To see the user's permissions, click **+** to expand the list associated with each feature.

Features to which the user has access (assigned through security groups)



**5** To see the security groups to which the user belongs, select the **Security Groups** tab.




**6** Click **Cancel** to return to the View User main page.

# Managing Membership Rules

**Important:** When adding or creating a membership rule, you must select the correct membership rule attribute and enter the correct value on the Membership Rules page. What you should select and enter depends on the combination of modules your company is using. Refer to the online Help for a list of the membership rule attributes and values. Point to **Security Access** and select **Membership Rules**, then click **?(Help)** in the top-right corner of the page. In the left-navigation column, click **See more about Membership Rule attributes and values**.

Membership rules help to define the characteristics of membership in a security group or a work group. When a membership rule is assigned to a security group, members can be granted permission to site features that are different from those of other users. When a membership rule is assigned to a work group, members can be included in the approval or notification of an event that is specific to their function.

For example, you can assign the following membership rules to a security group or a work group:

- All exempt employees
- All terminated employees
- Employees with a specific company code
- Employees that work in the HR department in San Francisco
- Employees who have been employed for 60 days or more

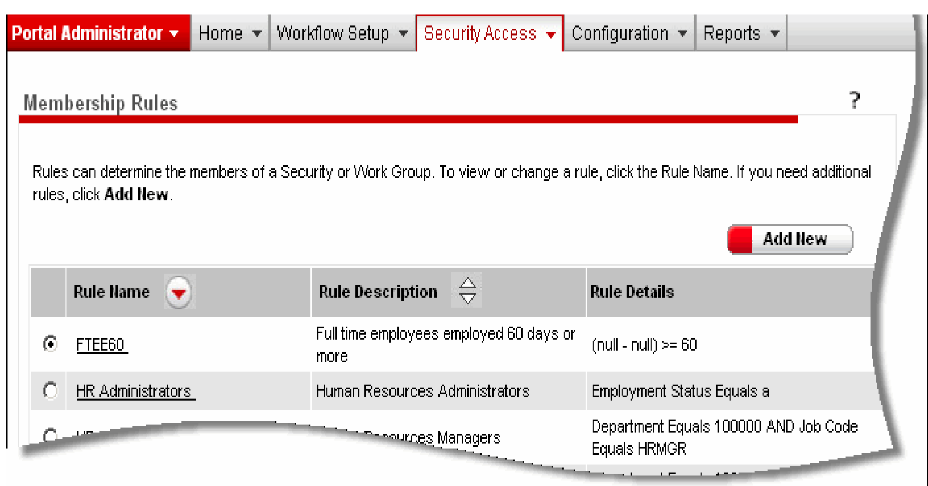
**Note:** Detailed instructions on setting up work groups are provided in the *ADP Workforce Now™ Portal Administrator Guide*.

## Adding a Membership Rule

You can add as many membership rules as needed to accurately define the security group. Be sure to use a descriptive name so it is easy to identify each rule.

1 Point to **Security Access** and select **Membership Rules**.

2 Click **Add New**.

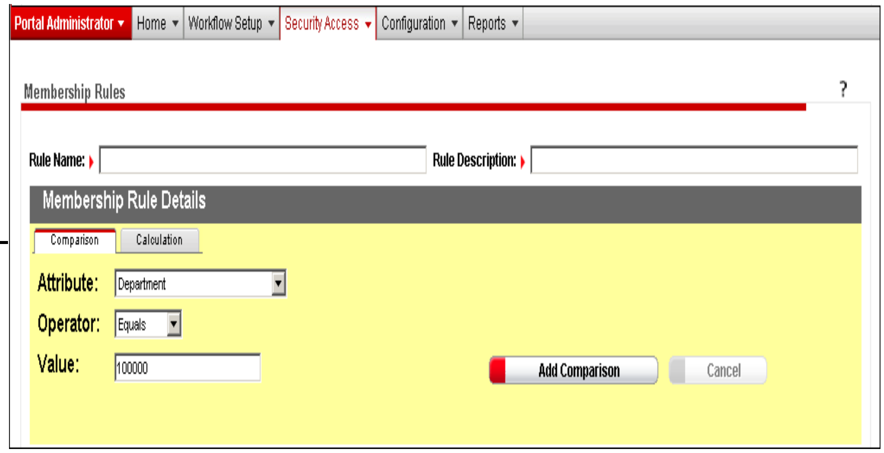


3 On the Membership Rules detail page, enter a rule name and a rule description.

**Tip:** Use language that makes the rule easy to identify when it is assigned to a security group or a work group.

4 If your rule requires a comparison statement, select an attribute and an operator, and enter a value. Then, click **Add Comparison**.

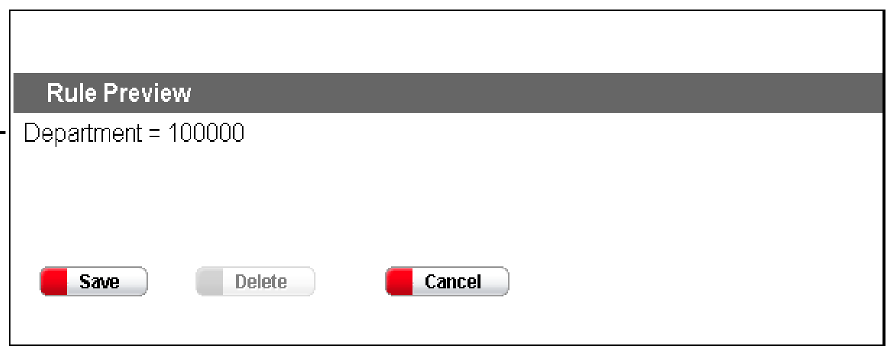
**Comparison** tab




5 Review your comparison statement in the **Rule Preview** box at the bottom of the page. If it contains red text, the comparison contains an error that you need to correct before you can continue. Hover your cursor over the red text to identify the problem. Then continue working with your comparison.

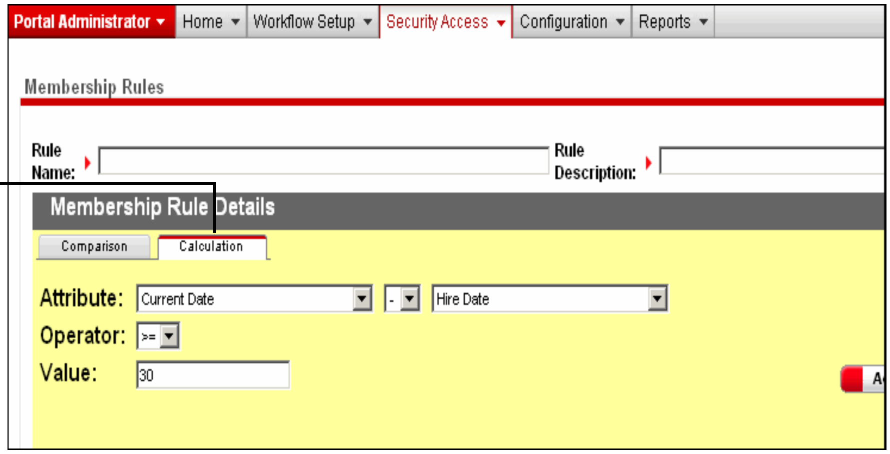
If your monitor doesn't display the entire page, scroll to the right.

Rule Preview



**6** If your membership rule requires a calculation statement, select the **Calculation** tab. In the **Attribute** field, select a variable, a mathematical symbol, and another variable. Then, select an operator and enter a value. Click **Add Calculation**.

**Calculation** tab




Use the AND and OR operators to connect multiple rule statements.

| Use | Example |
|---|---|
| **AND** if employees must meet both criteria | To create a group that includes all hourly employees whose standard hours are less than 30, click **AND** to connect the two statements:<br>(Employment Rate Type Equals Hourly) AND (Standard Hours < 30.00) |
| **OR** if they can meet one or the other criteria | To create a group that includes all hourly employees or all active employees, click **OR** to connect the two statements:<br>(Employment Rate Type Equals Hourly) OR (Employment Status Equals Active) |

Membership rules are executed in the order entered, and precedence is given to AND operators over OR operators. The following three scenarios demonstrate this execution:

1. A + B + C + D is executed (A+B) or (C+D)
2. A or B + C + D is executed A or (B+C+D)
3. A + B + C or D is executed (A+B+C) or D

Example for Scenario 3:

Membership Rule: Department Equals 100000 AND Location Equals Dallas AND Employment Rate Type Equals Salaried OR Employment Status Equals Active

Execution: (Department Equals 100000 AND Location Equals Dallas AND Employment Rate Type Equals Salaried) OR (Employment Status Equals Active)

The resulting group would consist of all salaried employees who are in Department 100000 and the Dallas location AND all active employees (independent of department, location, and employment rate type).

7 Review your calculation statement in the **Rule Preview** box at the bottom of the page. If it contains red text, the calculation contains an error. Hover your cursor over that text to identify the problem. Then continue working with your calculation.

8 When you are done, click **Save**.

## Example: Only Active Employees

1 In the **Attribute** field, select **Employment Status**.

2 In the **Operator** field, select **Starts with**.

3 In the **Value** field, type **A**.

4 Click **Add Comparison**. Your comparison statement displays in the **Rule Preview** box below.

## Example: All Exempt Employees

1 In the **Attribute** field, select **FLSA Status**.

2 In the **Operator** field, select **Equals**.

3 In the **Value** field, type **Exempt**.

4 Click **Add Comparison**. Your comparison statement displays in the **Rule Preview** box below.

## Example: Employees Who Work in the HR Department in San Francisco

1 In the **Attribute** field, select **Department**.

2 In the **Operator** field, select **Equals**.

3 In the **Value** field, type **Human Resources**.

4 Click **Add Comparison**. Your comparison statement displays in the **Rule Preview** box.

5 Click **AND** to add your second statement.

6 Click **Add a Comparison/Calculation**.

7 In the **Attribute** field, select **Location**.

8 In the **Operator** field, select **Equals**.

9 In the **Value** field, type **San Francisco**.

10 Click **Add Comparison**. Your second comparison statement displays in the **Rule Preview** box below.

## Example: Employees Who Have Been Employed for 60 Days or More

1 In the **Attribute** field, do the following:

- Select **Current Date** as the calculation variable.
- Select **-** as the mathematical symbol.
- Select **Hire Date** as the second variable.

2 In the **Operator** field, select **>=**.

3 In the **Value** field, type **60**.

4 Click **Add Calculation**. Your calculation statement displays in the **Rule Preview** box below.

## Testing a Membership Rule

Always test a membership rule after creating or changing it.

1 Point to **Security Access** and select **Security Groups**.

2 Click **Add New**.

3 Enter a group name that will help you to identify the members that belong to this group.

4 Select a group type.

5 From the **Rules** tab, select the membership rule you created.

6 Click **Members** to view the members that are generated by your membership rule. If the members are not correct, delete the security group and select **Membership Rules** to edit the membership rule.

**Important:** An important step in testing a membership rule is to check that you have used the correct attribute and value.

## Fixing a Membership Rule That Isn't Working Correctly

If the membership rule isn't working correctly, select the rule on the Membership Rules page and make sure you have:

- Selected the correct attribute. For example, you might have selected Employment Status (Active, Terminated, or Leave of Absence) when you meant to choose Employment Rate Type (Hourly or Salaried).
- Selected the correct calculation or comparison operator.
- Entered the correct value.
- Appropriately connected the rule statements with AND or OR.
- Entered the rule statements in the order they should be executed, with precedence to the AND operators over the OR operators.

## Assigning and Unassigning Membership Rules

Membership rules can be assigned to work groups or custom security groups. A change in membership rule assignments has an immediate impact on users logging on. It may change the groups to which they belong and the features to which they have access.

**Tip:** From the Security Group page, hover your cursor over a custom group name to display a brief description of membership rule assignments.

1 Point to **Security Access** and select **Security Groups**.

2 Click to select the appropriate group name.

**3** On the **Rules** tab, click to select or clear the rule you want to assign or unassign.

**4** Click **Save Group**.

## Changing a Membership Rule

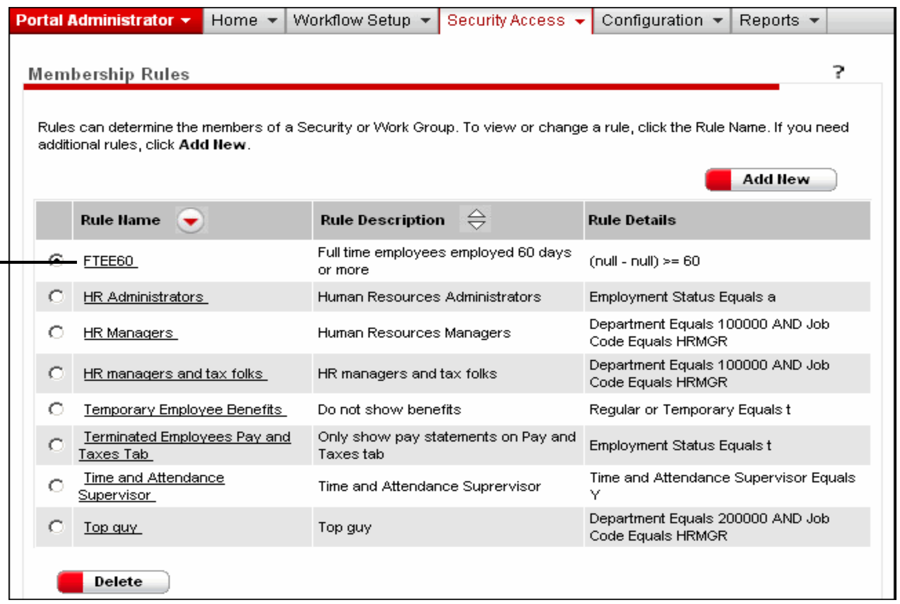
**Important:** A membership rule has an immediate impact on users who are logging on. These rules can change the groups to which the user belongs and the features they can access. If you do not want to affect users, add a new membership rule instead of changing an existing membership rule that already has users assigned.

You cannot change a membership rule that is assigned to a security group or a work group. First, you must unassign the rule from any security groups or work groups to which it is assigned. Another option is to create a new rule.

**1** Point to **Security Access** and select **Membership Rules**.

**2** Click the rule you want to change.

Rules



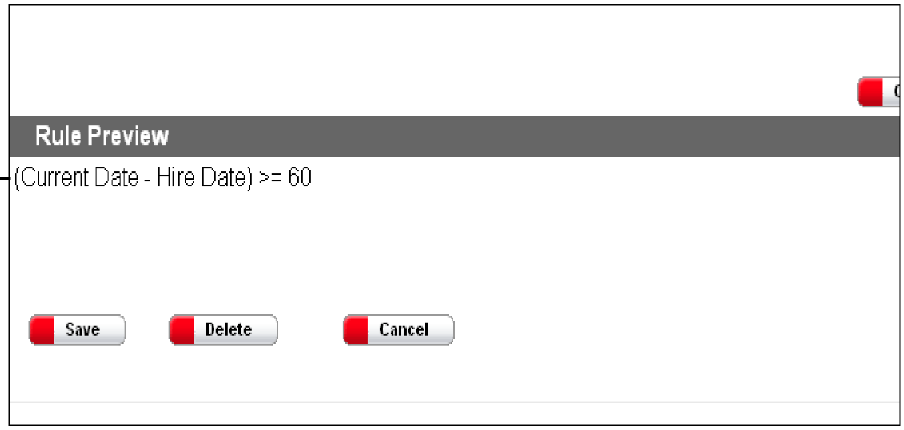

**3** If necessary, change the rule description.

**4** Change the rule.

**Tip:** Click the pencil icon to edit or the **X** to delete a rule statement. Click **Clear Rule** to delete the entire rule.

**5** Preview your revised rule statement in the **Rule Preview** box at the bottom of the page. If it contains red text, there is an error that you will need to correct before you continue. Hover your cursor over that text to identify the problem, and revise the rule to correct the problem.

Click the rule to change it.




**6** When you are done, click **Save**.

**7** Test your rule by assigning it to a security group or a work group. Then, validate the members who are generated by the rule. For more information, refer to "Adding a Membership Rule" on page 86.

## Changing a Rule for an Automatically Created Custom Security Group

If you set up a custom security group for terminated employees, you must add an active status to the membership rule for each automatically created custom security group of the employee type. This makes terminated employees inactive in their automatically created custom employee group(s), so the employees do not view content they should not see.

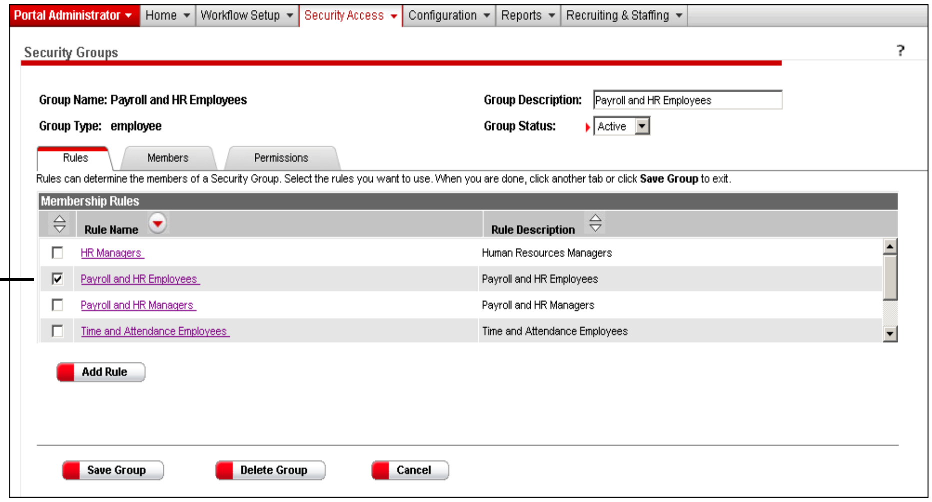
**Important:** To change a membership rule for an automatically created custom security group, first unassign the membership rule from the group. Change the rule, and then assign the new rule to the group.

**1** Point to **Security Access** and select **Security Groups**.

**2** Select the group name for which you want to unassign the current membership rule.

3 Unassign the membership rule by clicking to clear it.

Click to clear an assigned membership rule.




4 Click **Save Group**. You are returned to the updated Security Groups page.

5 Point to **Security Access** and select **Membership Rules**.

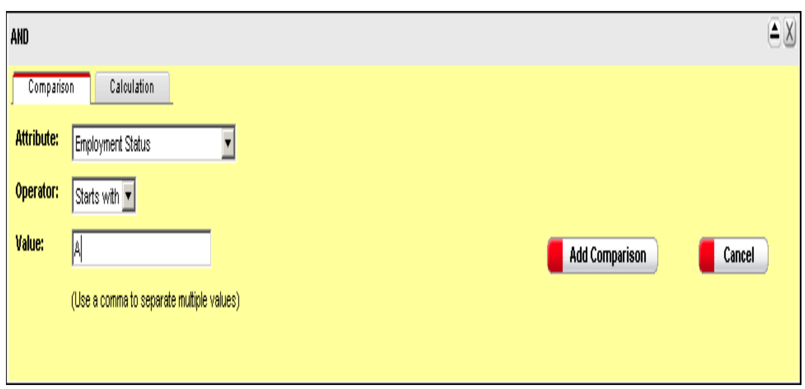
6 Click the rule you want to change.

7 Click **AND**.

8 Click **ADD a Comparison/Calculation**.

9 Add a rule statement that defines employment status as active.

- In the **Attribute** field, select **Employment Status**.
- In the **Operator** field, select **Starts with**.
- In the **Value** field, type **A**.




10 Click **Add Comparison**.

11 Preview your revised rule statement in the **Rule Preview** box at the bottom of the page, and revise the rule if necessary.

12 When you are done, click **Save**.

13 Point to **Security Access** and select **Security Groups**.

14 Select the group name for which you want to assign the revised membership rule.

15 Click to select the rule you want to assign.

**16** Click **Save Group**.

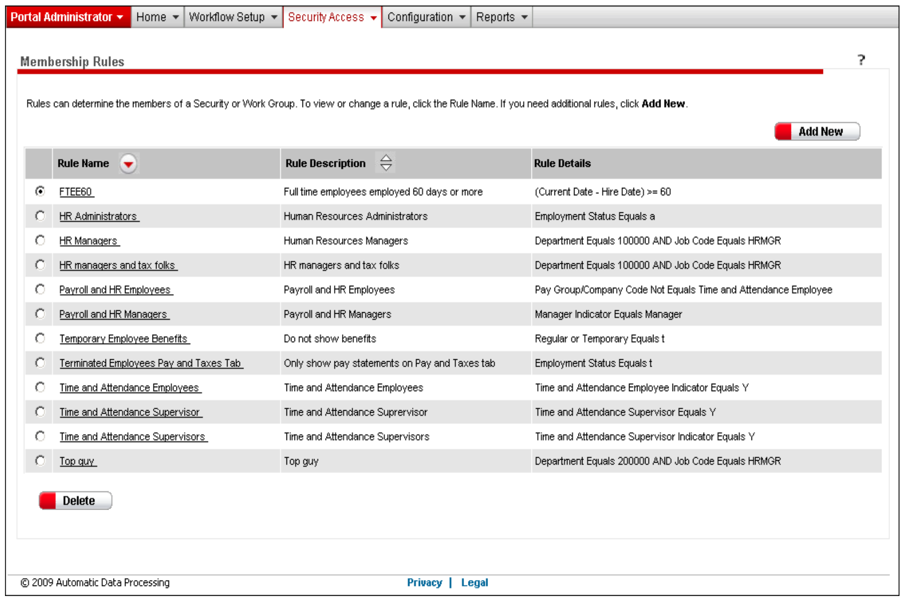
---

**Important:** If you add an employment status to one custom security group, you must add an employment status to all custom security groups of the same employee type. This ensures that members of multiple groups see only what you want them to.

---

# Deleting a Membership Rule

1. Point to **Security Access** and select **Membership Rules**.
2. Click to select the radio button next to the rule you want to delete.



3 Click **Delete**. Then click **OK** to confirm your deletion.

**Tip:** If you get a message indicating that the rule is currently assigned, you must remove it from the corresponding security group or work group before deleting it. To identify rule assignments, point to **Security Access** and select **Security Groups**. Hover your cursor over the group name.

Chapter 4

# Setting User Access for HR & Benefits

Through ADP security management service, you have set up all users who need digital certificates to access the HR & Benefits module of ADP Workforce Now®. The next stage of user security for these users is to identify which features of the HR & Benefits module they can use.

This chapter provides details on certain aspects of setting up user access in the HR & Benefits module, including:

- Assigning the HR & Benefits profile to the user
- Restricting user access by corporate groups

For additional details on restricting user access in the HR & Benefits module, refer to Chapter 3,"Setting User Access in ADP Workforce Now" on page 57.

**Important:** You must complete the  security management process, including assigning the HR & Benefits profile, for the user before you can complete the procedures described in this chapter.

# Assigning the HR & Benefits Profile to a User

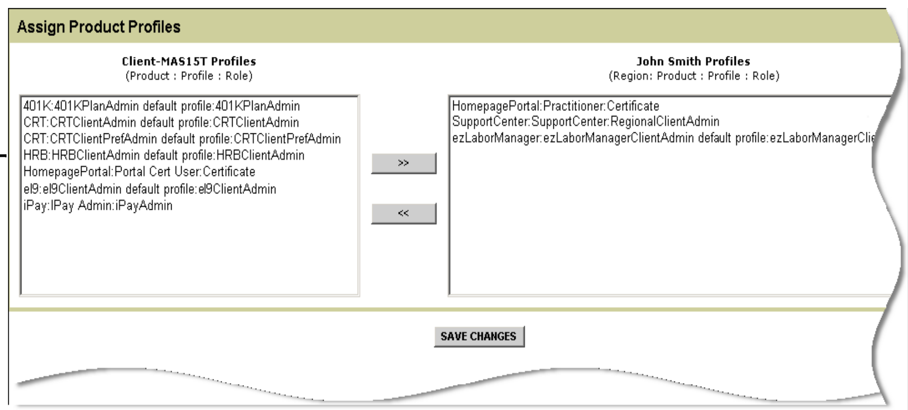
Your ADP representative has created a default profile for each module or service your company is using. This profile allows you to control access to each of these services. In this section, you will assign the HR & Benefits profile to any user you set up in ADP Netsecure who should have access to this module.

To assign the HR & Benefits profile to a user, follow these steps:

1. Access ADP Netsecure.
2. Find the user.

   For details on finding a user record in ADP Netsecure, refer to "Adding a New User" on page 36 in Chapter 2.
3. On the Find User Results page, click the user name or user ID.
4. Click **Assign Profiles**.
5. From the **Available Profiles** list, select **HRB**. (This profile represents the HR & Benefits module.)

HR & Benefits profile




**Note:** You might need to select additional profiles. Check with your ADP representative.

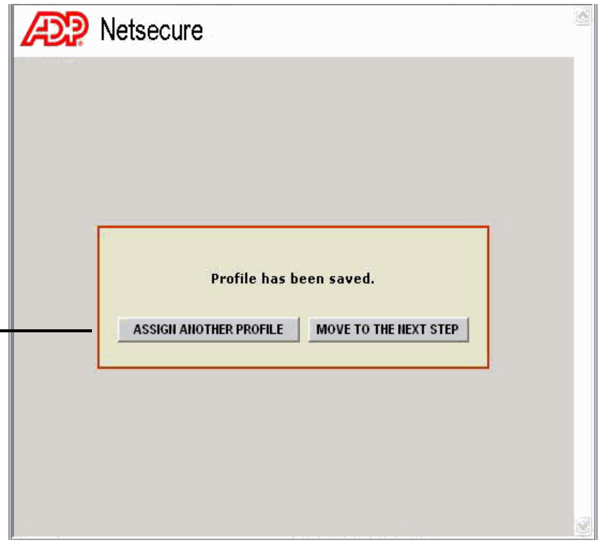
6. Click **> >** to move the profile to the **Assigned Profiles** list.

**Tip:** You might need to scroll horizontally to see the list of assigned profiles.

7. Click **Save Changes.**

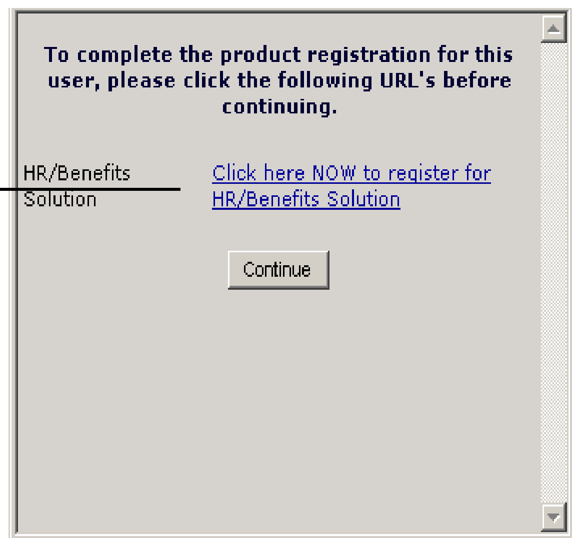
**8** A window opens with a message that tells you the profile has been saved. Click **Move to the Next Step**.

Do not select **Assign Another Profile**. You must completely set up the HR & Benefits profile before you can assign another profile to the user.




**9** Click the link, **Click here NOW to register for HR/Benefits Solution**.

Click this link.



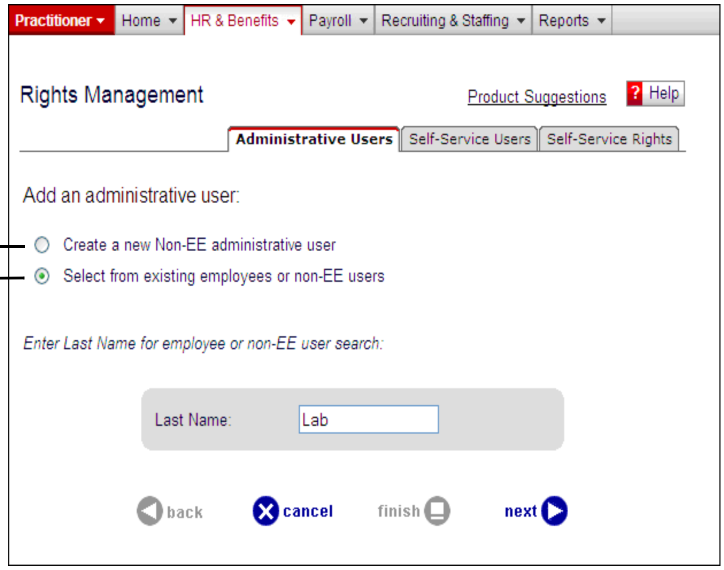

**10** Do one of the following:

- Click **Create a new Non-EE administrative user** to indicate a contract or temporary employee.
- Click **Select from existing employees or non-EE users** (for all other users).

**Important:** When selecting from existing employees or non-EE users, enter the last name exactly as it appears in the HR & Benefits module. Otherwise, you will receive an error message that the user cannot be found.

Select this option for temporary or contract users.

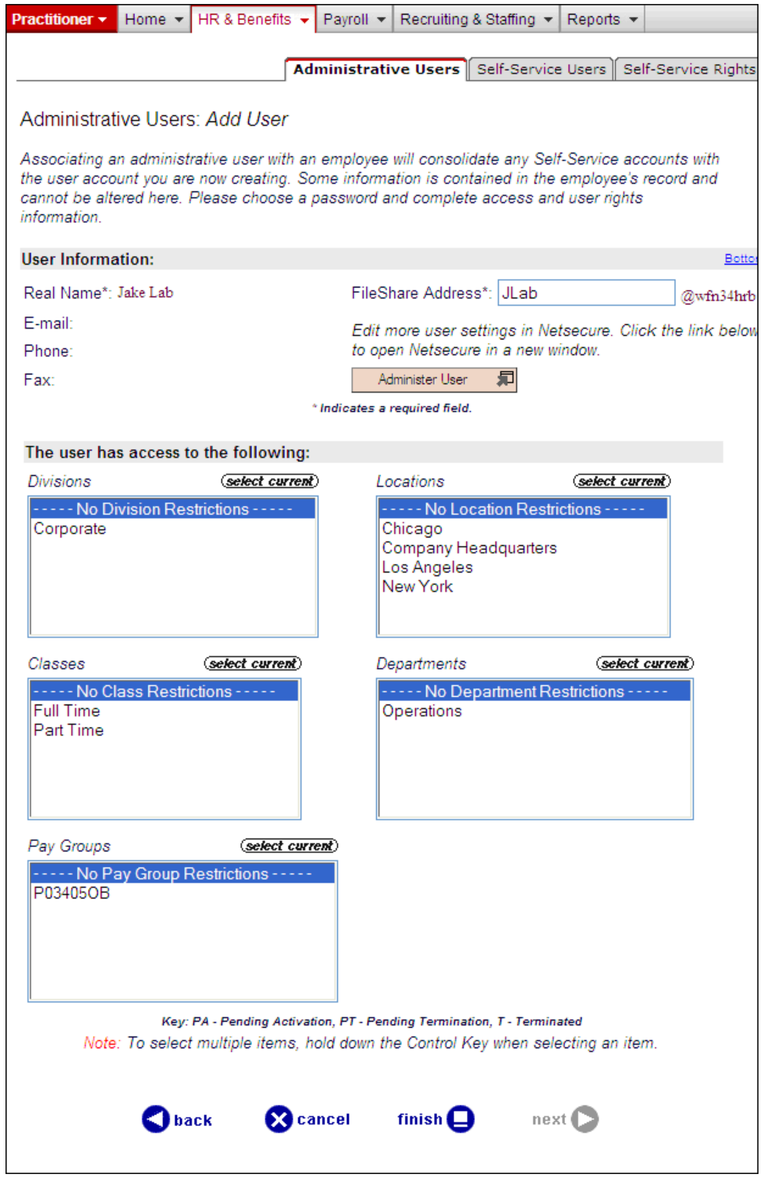
Select this option in most cases.




**11** Click **Next**.

**12** On the **Administrative Users** tab, select the business units, locations, classes, home departments, and pay groups to which the user should have access.

- If the user should have no access restrictions, click **No (Corporate Group) Restrictions** to remove all restrictions of this type.
- For users who should have access restrictions, select each setting they should be able to access. Press **Ctrl** and click to select more than one setting.




**13** Click **Finish**.

# Accessing the HR & Benefits Module

To set up user access in the HR & Benefits module:

- You must be logged on to ADP Workforce Now as a practitioner.
- You must be assigned the primary user profile in the HR & Benefits module.

**Important:** During the planning phase, your ADP representative set up the security master as the primary user. If you are an ADP Netsecure security master and are unable to perform the procedures in this chapter, check with your ADP representative to make sure you have been assigned the correct security access.

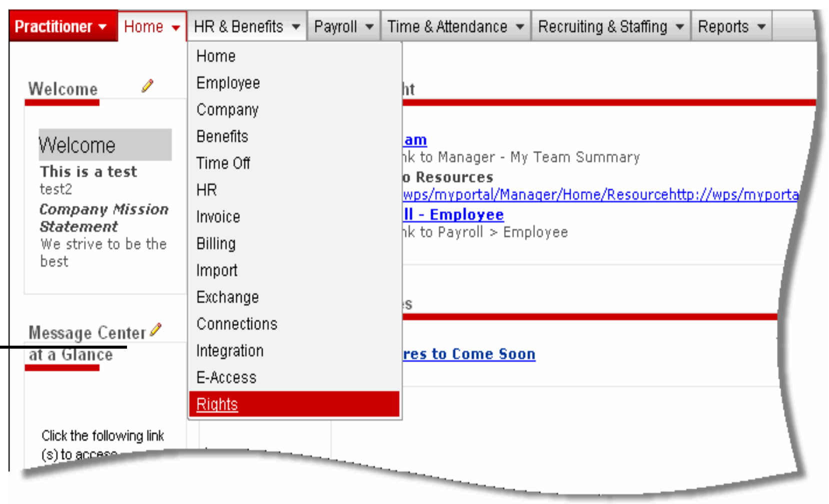
To access the practitioner role, follow these steps:

**1** Log on to ADP Workforce Now.

**2** Point to the Role Selector and select **Practitioner**. Notice that the menus change when you access the Practitioner role. The menus for all ADP Workforce Now services are available.

**3** Point to the **HR & Benefits** menu to see the available options.

From this menu, you can set up user access in the HR & Benefits module.



# Changing User Access Using Corporate Groups

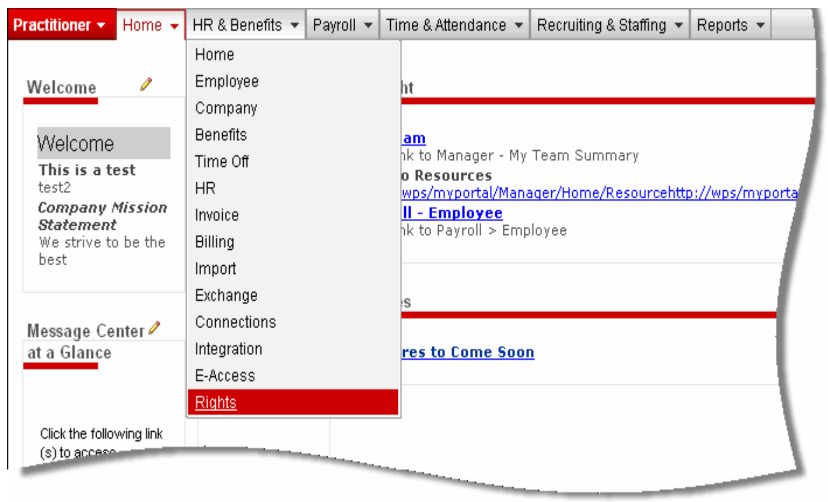
In most cases, you will restrict access to the HR & Benefits menu through the same features that control access to the ADP Workforce Now home page. These features are described in Chapter 3, "Setting User Access in ADP Workforce Now" on page 57.

The only rights you should restrict through the HR & Benefits module are for these corporate groups:

- Business units
- Locations
- Classes
- Home departments
- Pay groups

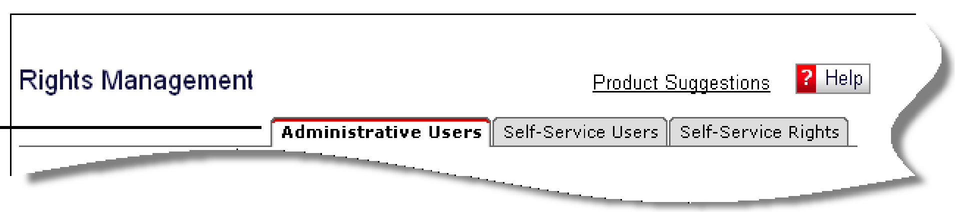
Do the following:

**1** Point to **HR & Benefits** and select **Rights**.




**2** Click the **Administrative Users** tab (if necessary).

If it is not already active, click this tab.



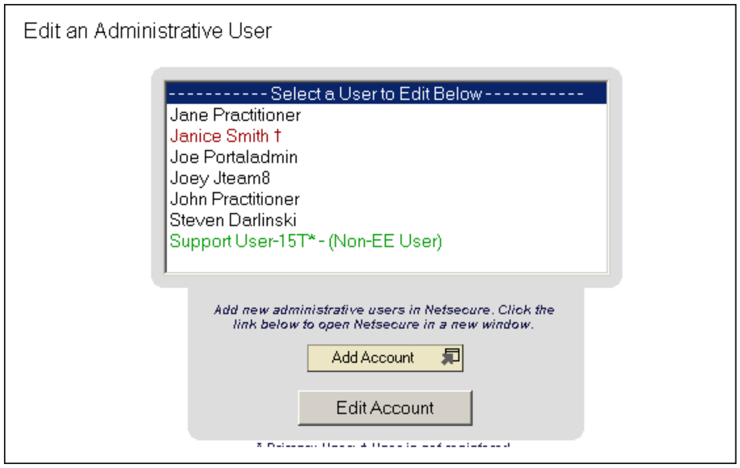
The color green identifies a primary user.

The color black identifies a non-primary user.

The color red means the digital certificate has not been loaded, or an error has occurred in the registration process for the user.

The + identifies a non-registered user.

**3** Select the user.




---

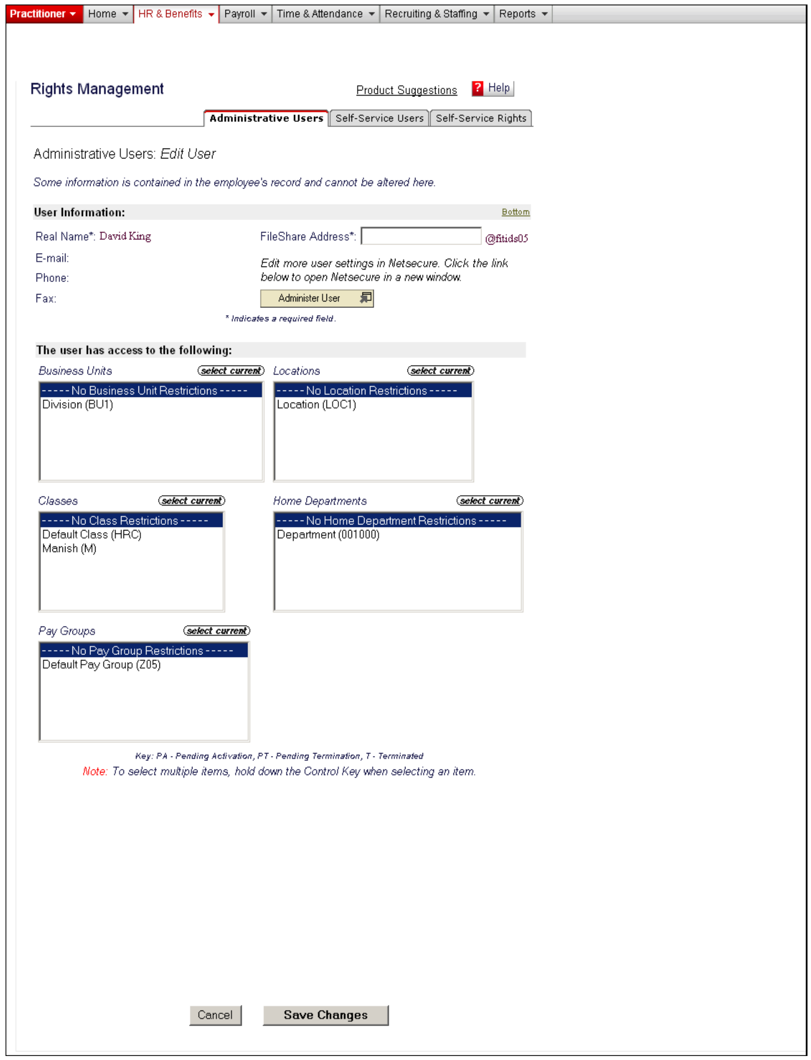
**Important:** You cannot edit the rights for the primary user. These rights are assigned to the security master. Speak with your ADP representative if you need to adjust security master rights.

---

**4** Click **Edit Account**.

**5** On the **Administrative Users** tab, select the business units, locations, classes, home departments, and pay groups to which the user should have access.

- If the user should have no access restrictions, click **No (Corporate Group) Restrictions** to remove all restrictions of this type.
- For users who should have access restrictions, select each setting they should be able to access. Press **Ctrl** and click to select more than one setting.




**6** Click **Save Changes**.

# Chapter 5
# Setting User Access for Payroll

Through the ADP security management service, you have set up all users who need digital certificates. The next stage of user security for these users is to allow them to access the Payroll module and identify which features of the Payroll module they can see and use.

This chapter provides details on these additional security features, including:

- Assigning the Payroll profile to the user
- Changing a user profile
- Deleting a user profile
- Changing a user's name, profile, or access rights
- Deleting a user

**Note:** You must complete the security management process, including assigning the Payroll profile, to the user before you can complete the procedures described in this chapter.

# Assigning the Payroll Profile to a User

Your ADP representative has created a default profile for each module/service your company is using. In this section, you will assign the Payroll profile to any user you set up in the ADP security management service who should have access to this module.

To assign the Payroll profile, go to **People > Access & Security > Product Profiles**.

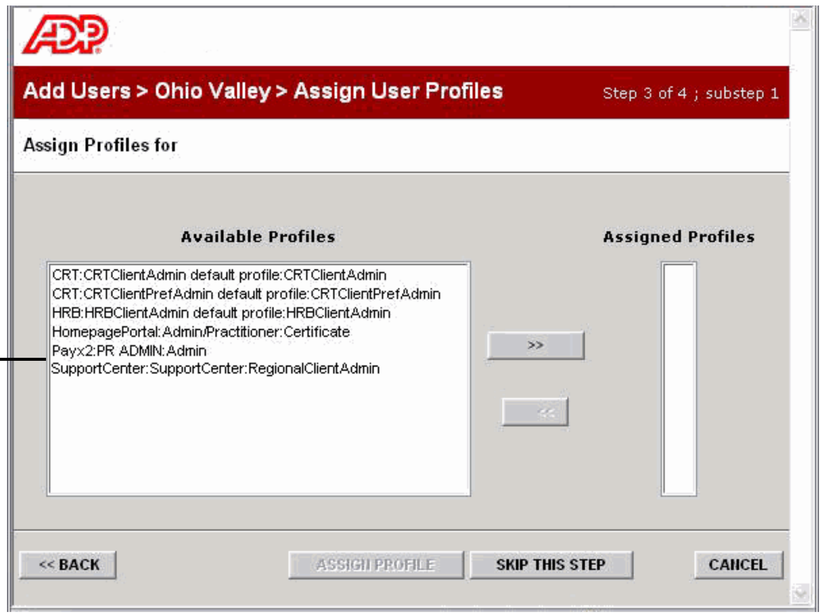
**1** Select the user.

**2** Click on the user's name.

**3** Click to select the **PayX2** profile and move it to the Selected Product Profiles list.

Payroll profile

**Note:** You might need to select additional profiles. Check with your ADP representative.



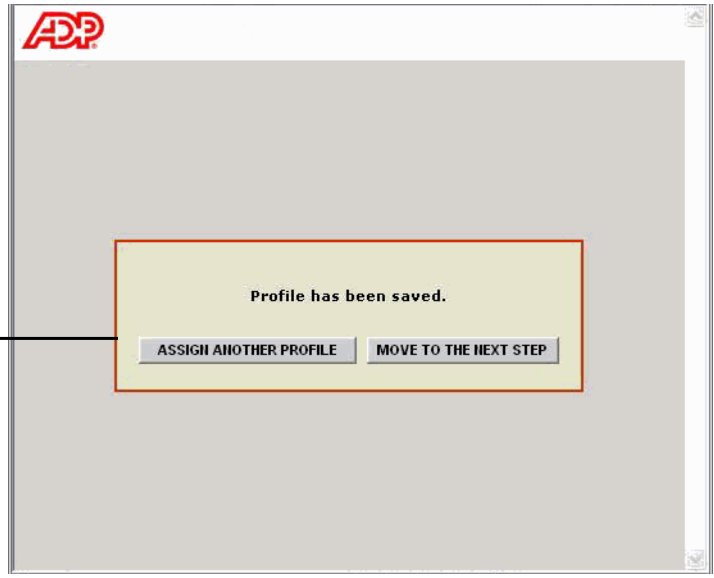

**4** Click **>>** to move the profile to the **Assigned Profiles** list.

**Tip:** You might need to scroll horizontally to see the list of assigned profiles.

**5** Click **Assign Profile**.

**6** A window opens with a message that tells you the profile has been saved. Click **Move to the Next Step.**

Do NOT select **Assign Another Profile**. You must completely set up the Payroll profile before you can assign another profile to the user.




**7** Click the link, **Click here NOW to register for Pay eXpert**.

Click this link.

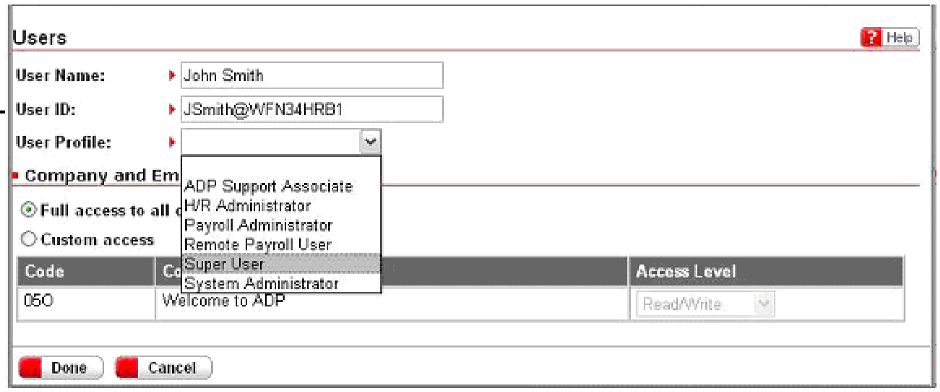

**8** On the Users page, select **Payroll Administrator** in the **User Profile** field.

**Note:** During the planning phase of setting up user access, you noted access restrictions that might affect whether you should use the default user profiles for the Payroll module or create new ones. If a default profile does not meet your needs, you can modify it or create your own user profiles. Speak with your ADP representative to determine whether to use the default profiles or create new ones.

**Important:** The super user profile can only be assigned to one user in the Payroll module and your ADP representative has already assigned this profile to the security master.

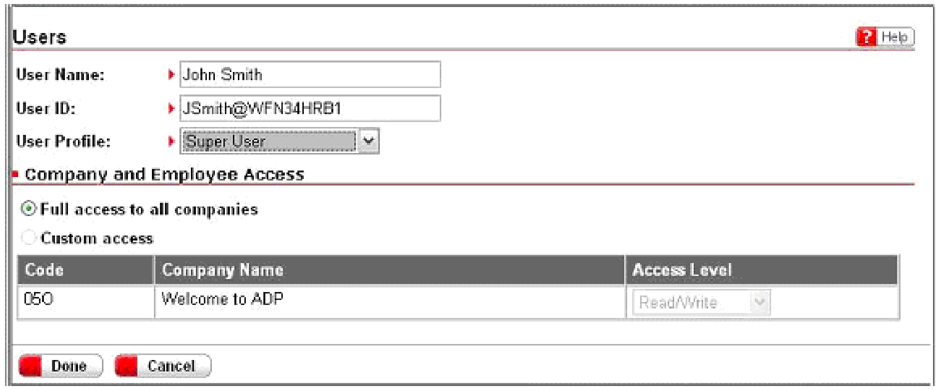
Do not assign the ADP support associate user profile to a user unless requested to do so by your ADP representative.

Be sure to select the correct user profile for this user. **Remember:** All access rights in the Payroll module are controlled through this profile.



**9** Select whether the user has full access to all companies or custom access.

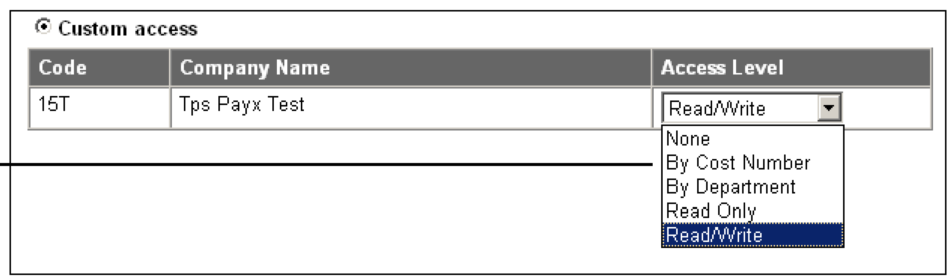
In this area, set up the level of access the user should have.




| To | Select This Option |
|---|---|
| Allow the user full access to all types of data for the company | **Full access to all companies** and go to Step 14. |
| Allow the user to access the company, but restrict access to specific types | **Custom access** and go to Step 12. |

**10** Select the appropriate access level for this user.

Select the access level from this list.



**11** If you selected custom access, select the access level the user will have to information (such as pay rates and salary history) in the Payroll module.

| To | Select This Option from the Access Level List |
|---|---|
| Allow no access | **None**<br>**Note:** If you change the access level of the user's default current company to none, the default will reset to the parent code. If the user does not have access to the parent code, then the default is set to the company with the highest alphabetical order. |
| Allow read-only access | **Read Only** |
| Allow read/write access | **Read/Write** |
| Allow access to selected departments within a company | By **Department**, then select the companies that apply. For employees within these departments, the user will have full read/write access to the functions and pages permitted by the user profile.<br>You can set up a maximum of 570 departments. However, ADP recommends a maximum of 200 departments. Hold down the **Control** key or the **Shift** key and select multiple departments.<br>**Note:** If you do not select at least one department for a company, you will not be able to view any employees for the associated company. |
| Allow access to selected cost numbers within a company | By **Cost Number**, and then select the cost numbers that apply.<br>**Note:** If you do not select at least one cost number for a company, you will not be able to view any employees for the associated company. |

**12** Click **Done**.

**13** A window confirms you have successfully set up the user in the Payroll module. Click **Close**.

# Accessing the Payroll Module

To set up user access in the Payroll module:

- You must be logged on to ADP Workforce Now as a practitioner.
- You must also be assigned the super user profile in the Payroll module.

**Important:** During the planning phase, your ADP representative set up the security master as the Payroll super user. If you are an ADP security master and are unable to perform the procedures in this chapter, check with your ADP representative to make sure you have been assigned the correct security level.

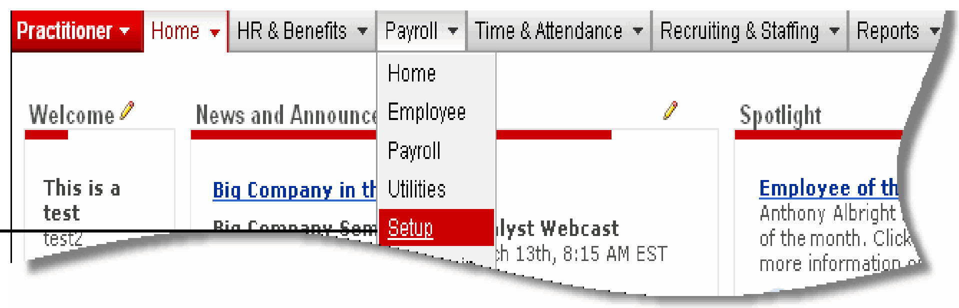
To access the Practitioner role, follow these steps:

**1** Log on to ADP Workforce Now.

**2** Point to the Role Selector and select **Practitioner**. Notice that the menus change when you access the Practitioner portal role. The menus for all Workforce Now services are available.

**3** Highlight the **Payroll** menu to see the available options. From this menu, you can set up all aspects of user access in ADP Workforce Now for the Payroll module.

From this menu, you can set up user access in the Payroll module.



# Setting Up User Profiles

During the planning phase, your ADP representative discussed how the access restrictions you identified relate to the Payroll default user profiles. You might have decided to adjust the default profiles to better suit the needs of your organization.

The Payroll user profiles control the type of information that users can view and the functions they can perform in the Payroll module. You selected a user profile when you assigned the Payroll profile to the user.

The Payroll module provides the following default profiles:

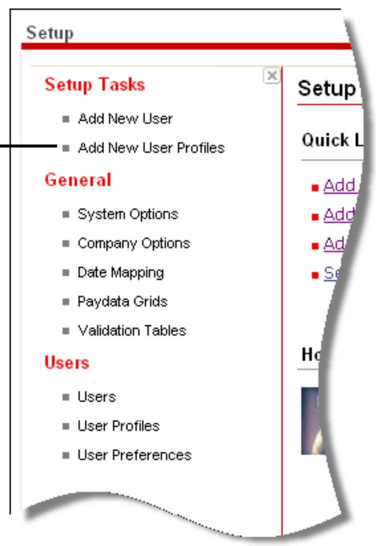
- Super user (assigned by your ADP representative to you, as security master)
- Payroll administrator
- H/R administrator
- System administrator
- Remote Payroll user

## Adding a New User Profile

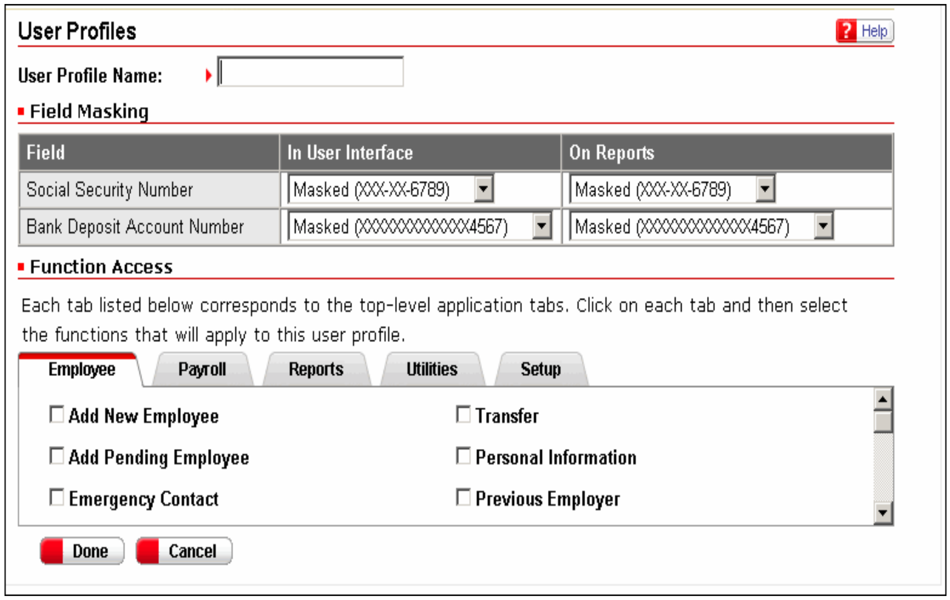
1 Select **Payroll** > **Setup**.

2 From the **Setup Tasks** menu, select **Add New User Profiles**.

Add New User Profile



**3** On the User Profiles page, enter a unique user profile name. Choose a name that is descriptive, easy to understand, and differentiates the user from other users.




**4** Select an option to control Social Security number display in the user interface.

**Note:** It is recommended that you keep the default value of **Masked Display (XXX-XX-6789)** or select **No Display** (blank) for user profiles other than Super User. Display of entire employee Social Security numbers is not recommended. The option you select also controls the display of dependent Social Security numbers, Federal IDs, and beneficiary Social Security numbers in the user interface.

**5** Select an option to control Social Security number display on reports.

**Note:** It is recommended that you keep the default value of **Masked Display (XXX-XX-6789)** or select **No Display** (blank) for user profiles other than Super User. Display of entire employee Social Security numbers is not recommended. The option you select also controls the display of dependent Social Security numbers, Federal IDs, and beneficiary Social Security numbers on reports.

**6** Select an option to control bank deposit account number display in the user interface.

**Note:** It is recommended that you keep the default value of **Masked Display (XXXXXXXXXXXXX4567)** or select **No Display** (blank) for user profiles other than Super User. Display of entire employee bank deposit account numbers is not recommended. The option you select also controls the display of the transit/ABA number on reports.

**7** Select an option to control bank deposit account number display on reports.

**Note:** It is recommended that you keep the default value of **Masked Display (XXXXXXXXXXXX4567)** or select **No Display** (blank) for user profiles other than Super User. Display of entire employee bank deposit account numbers is not recommended. The option you select also controls the display of the transit/ABA number on reports.

8 On each tab, select the functions that a user with this profile will be able to perform.

**Tip:** Functions are grouped according to the tasks a user can perform on each page in the Payroll module.

9 Click **Done**.

## Changing a User Profile

Use the User Profiles page to change the access assigned to a user profile. Changes to a user profile take effect the next time users with this profile log on.

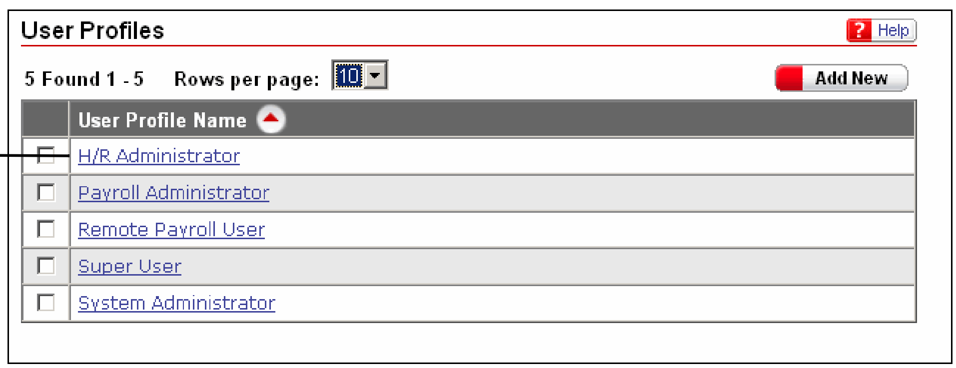
**Note:** You cannot modify the Super User profile.

1 Select **Payroll** > **Setup**.

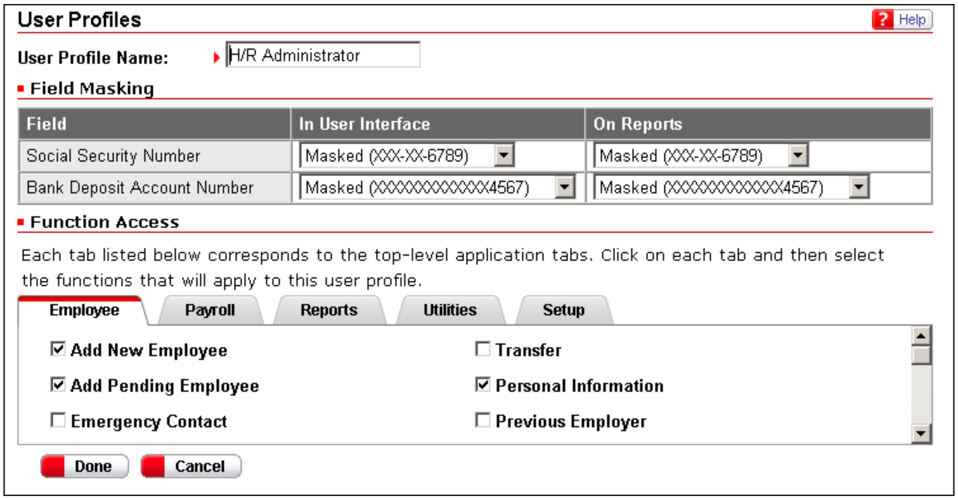
2 From the **Users** category, select **User Profiles.**

3 Click the user profile you want to change.

The profile names are links that when clicked display the details of the profile.



4 Select options to control Social Security number and bank deposit account number display in the user interface and on reports.




**Note:** If you are changing options for Social Security number display and bank deposit account number display in the user interface and on reports, it is recommended that you keep the default value of **Masked Display** or select **No Display** for user profiles other than Super User. Display of entire employee Social Security numbers and bank deposit account numbers is not recommended. The option you select for Social Security number also controls the display of dependent Social Security numbers, Federal IDs, and beneficiary Social Security numbers. The option you select for bank deposit account number also controls the display of the transit/ABA number.

5 On each tab, make the appropriate changes and then click **Done**.

## Deleting a User Profile

You cannot delete a user profile that has users assigned to it. You must first assign the users to another profile and then delete the original profile. Use the Users page to assign users to another profile. Then use the User Profiles page to delete the profile.

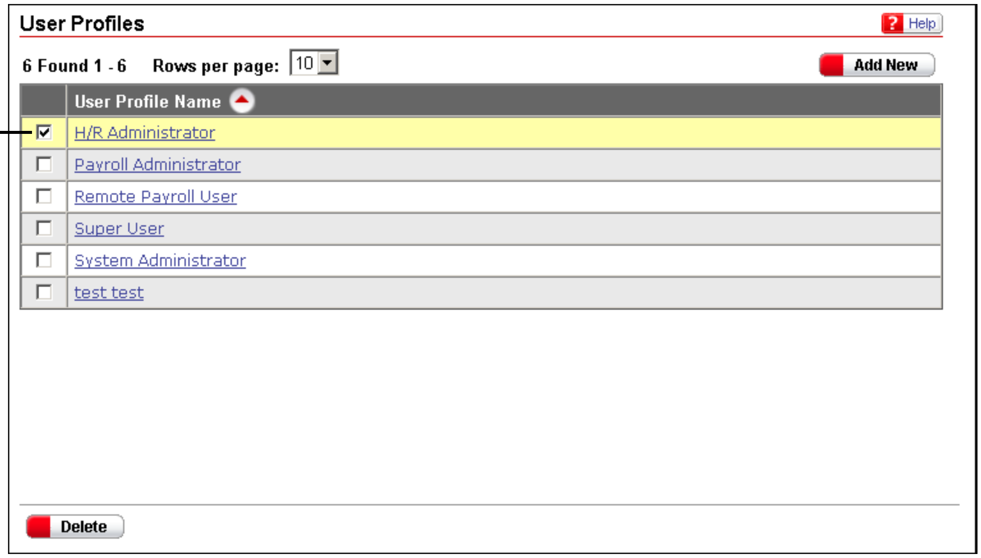
**Note:** You cannot delete the super user profile.

1 Select **Payroll** > **Setup**.

2 From the **Users** category, select **User Profiles.**

**3** Click to select the check box next to the user profile you want to delete.

A selected check box tags the user profile for deletion.




**4** Click **Delete**.

**5** Click **OK** at the deletion confirmation message.

# Changing User Information

Use the Users page to change details about the user, such as name, user profile, or access rights. These changes take effect the next time the user logs on. You cannot change a user's ID. You must delete the user ID you want to change and then create a new one.

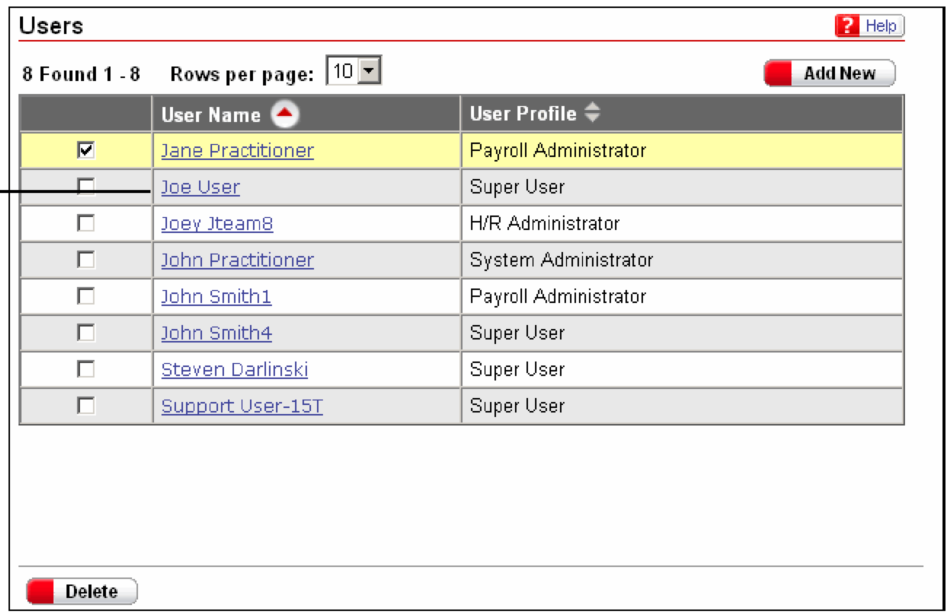
**Note:** Do not enter a password unless directed to do so by your ADP support representative.

1 Select **Payroll** > **Setup Tasks**.

2 From the **Users** category, select **Users.**

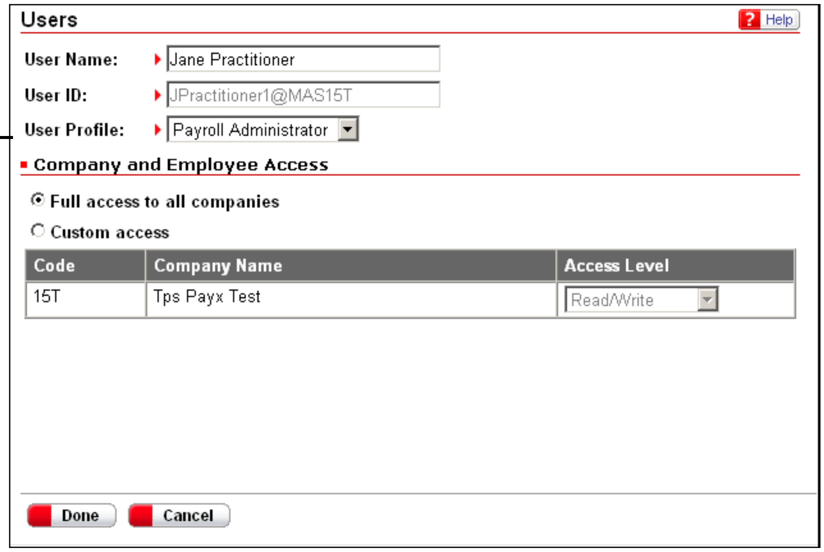
3 Click the name of the user whose details you want to change.

Click the link to open the details for a user.



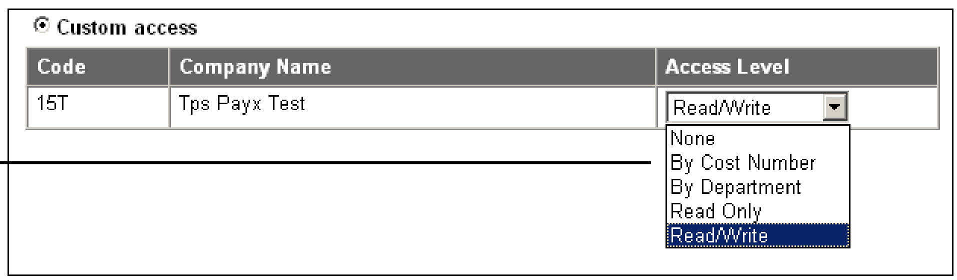
**4** On the detail page for that user, make appropriate changes.

**Remember:** You cannot assign the super user profile. This profile has already been assigned to the security master.




**5** If you selected custom access, then select the access level the user will have to information (such as pay rates and salary history) in the Payroll module.

Select the access level from this list.




| To | Select This Option from the Access Level List |
|---|---|
| Allow no access | None<br><br>**Note:** If you change the access level of the user's default current company to None, the default will reset to the parent code. If the user does not have access to the parent code, then the default is set to the company with the highest alphabetical order. |
| Allow read-only access | **Read Only** |
| Allow read/write access | **Read/Write** |

| To | Select This Option from the Access Level List |
| --- | --- |
| Allow access to selected departments within a company | By Department, then select the companies that apply. For employees within these departments, the user will have full Read/Write access to the functions and pages permitted by the user profile.<br><br>You can set up a maximum of 570 departments. However, ADP recommends a maximum of 200 departments. Hold down the Control key or the Shift key and select multiple departments.<br><br>**Note:** If you do not select at least one department for a company, you will not be able to view any employees for the associated company. |
| Allow access to selected cost numbers within a company | By Cost Number, and then select the cost numbers that apply.<br><br>**Note:** If you do not select at least one cost number for a company, you will not be able to view any employees for the associated company. |

6 Click **Done**.

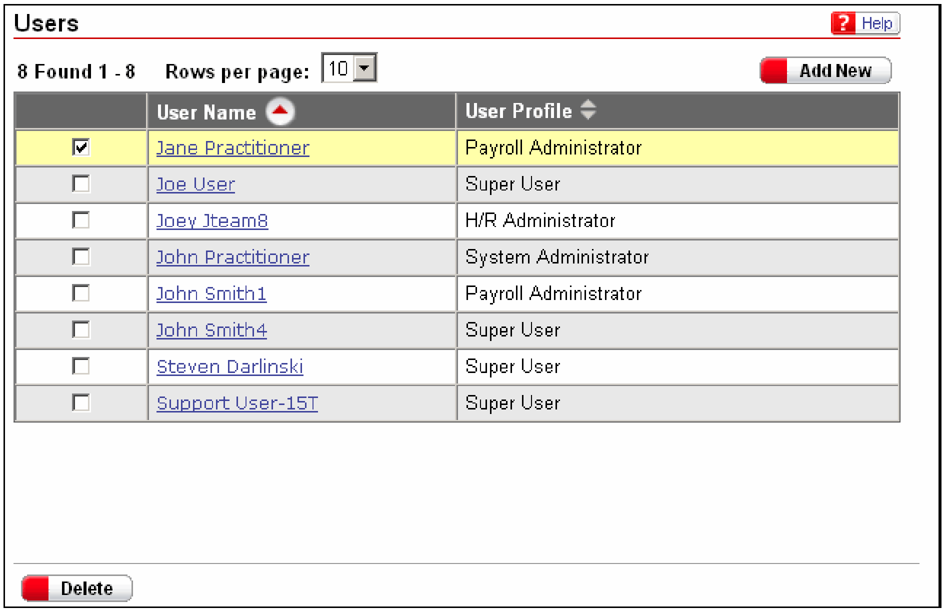
## Deleting a User

From the Users page, you can delete a user from the Payroll module.

1 Select **Payroll** > **Setup**.

2 From the **Users** category, select **Users**.

**3** Click to select the check box next to the user profile you want to delete.




**4** Click **Delete**.

**5** Click **OK** to confirm the deletion.

# Chapter 6
# Setting User Access for Time & Attendance

Through the ADP security management service, you have set up all users who need digital certificates to access the Time & Attendance module of ADP Workforce Now®. The next stage of user security for these users is to allow them to access the Time & Attendance module and identify which features of the Time & Attendance module they can use.

This chapter provides details on these additional security features, including:

- Assigning the Time & Attendance profile to the user
- Managing Time & Attendance security groups
- Managing user access in the Time & Attendance module

**Note:** You must complete the security management process, including assigning the Time & Attendance profile, to the user before you can complete the procedures described in this chapter.

# Assigning the Time & Attendance Profile to a User

Your ADP representative has created a default profile for each service your company is using. This profile allows you to control access to each of these services. In this section, you will assign the Time & Attendance profile to any user you set up in the ADP security management service who should have access to this module.

To assign Time & Attendance profile, go to **People > Access & Security > Product Profiles**.

**1** Select the user.

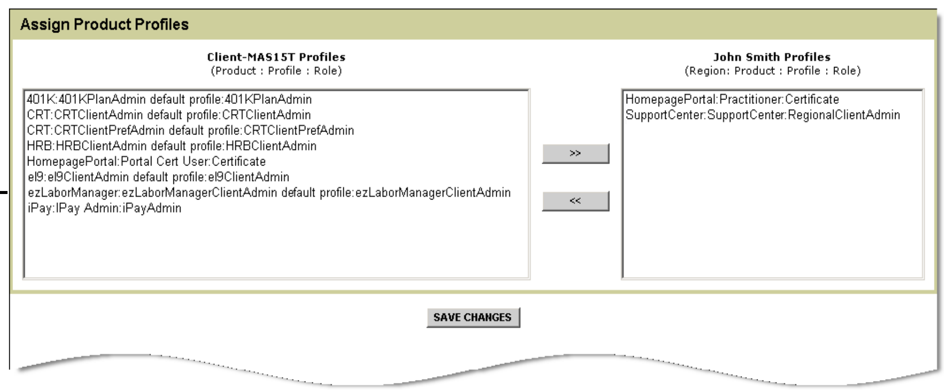
**2** Click on the user's name.

**3** Click to select the **Time & Attendance** profile and move it to the Selected Product Profiles list.

**4** Click **Assign Profiles**.

**5** From the **Available Profiles** list, select the profile for the Time & Attendance module.

Time & Attendance profile




**Note:** You also might need to select additional profiles. Check with your ADP representative.

**6** Click **> >** to move the profile to the **Assigned Profiles** list.

**Tip:** You might need to scroll horizontally to see the list of assign profiles.

**7** Click **Save Changes.**

8 A window opens with a message that tells you the profile has been saved. Click **Move to the Next Step.**

Do not select **Assign Another Profile**. You must completely set up the Time & Attendance profile before you can assign another profile to the user.


9 Click the link, **Click here NOW to register for ezLaborManager**.

Click this link.


10 The next window confirms that you have successfully set up the user in the Time & Attendance module. Click **Close**.

Continue to "Managing Time & Attendance Security Groups" on page 128 to restrict user access in the Time & Attendance module.

# Accessing the Time & Attendance Module

To set up user access in the Time & Attendance module:

- You must be logged on to ADP Workforce Now as a practitioner.
- You must be assigned the EL_ALL user profile in the Time & Attendance module.

**Important:** During the planning phase, your ADP representative set up the security master and backup security master with EL_ALL access in Time & Attendance. If you are an ADP security master and are unable to perform the procedures in this chapter, check with your ADP representative to make sure you have been assigned the correct security access.

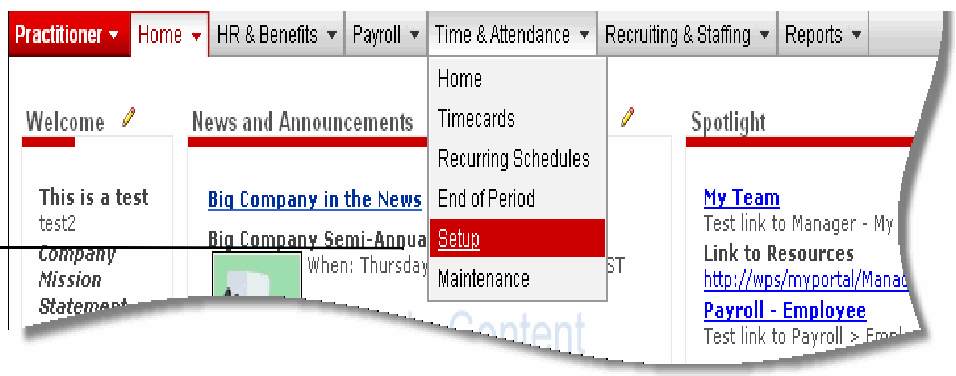
To access the Practitioner role, follow these steps:

**1** Log on to ADP Workforce Now.

**2** Point to the Role Selector and select **Practitioner**. Notice that the menus change when you access the Practitioner role. The menus for all Workforce Now services are now available.

**3** Point to the **Time & Attendance** menu to see the available options. From this menu, you can set up all aspects of user access in ADP Workforce Now.

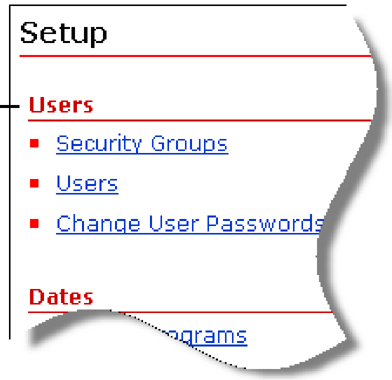
From this menu, you can set up user access in the Time & Attendance module.



# The Time & Attendance Setup Page

The links on the Setup page are grouped into four sections: **Users**, **Labor Charge Fields**, **Dates**, and **General**. To manage security, you are most concerned with the **Users** section.

In the **Users** section, you can set up user access for the Time & Attendance module.




The **Users** section contains these options:

- **Security Groups:** Allows you to assign employees to Time & Attendance security groups. Security group assignments control which supervisors and administrators can access employee records.
- **Users:** Allows you to assign Time & Attendance access rights to employees.
- **Change User Passwords:** All passwords are set up through the ADP security management service. This option redirects you to security management to reset user passwords.

## Employees vs. Users

In Time & Attendance, security groups control who can view and edit employee records. Employees and users have a different relationship to security groups. The following explains the difference:

- An employee is a person whose Time & Attendance information is recorded in the Time & Attendance module. An employee cannot access the Time & Attendance module unless he/she is also a user.
  Employees are assigned *to* a security group. This means they are members of the security group, but they cannot view the records of other employees.
- A user is an employee who has been given access by an administrator to the Time & Attendance module. A user can access the module to clock in and out, view benefits information, and perform other tasks.
  Users are assigned *access* to a security group. This means they can view the employees who are members of security groups to which they have been given access. However, giving a user access does not make the user a member of the security group.

# Managing Time & Attendance Security Groups

The Time & Attendance module has its own security groups feature. You must set up security groups in the Time & Attendance module to manage security groups in this module.

As the security master, you can perform tasks related to Time & Attendance security groups, such as:

- Create security groups
- Assign employees to security groups
- Assign user access to security groups
- Edit security group descriptions
- Remove employees from security groups
- Remove user access to security groups
- Delete security groups

**Important:** In Chapter 3, "Setting User Access in ADP Workforce Now" on page 57, you set up security groups to manage access to ADP Workforce Now. These groups do not control access to content in the Time & Attendance module. You must set up separate security groups within the Time & Attendance module to manage access to content in this module.

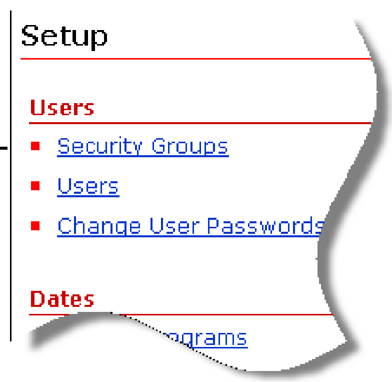
In ADP Workforce Now, four custom security groups with associated membership rules and permissions are automatically created if your company is using one of these combinations of modules: (1) Payroll and Time & Attendance or (2) Payroll, HR & Benefits, and Time & Attendance. These groups are managed through the **Security Groups** menu option on the **Security Access** menu. Refer to Chapter 3, "Setting User Access in ADP Workforce Now" on page 57, for details on these groups.

## Creating a Security Group

To create a security group, follow these steps:

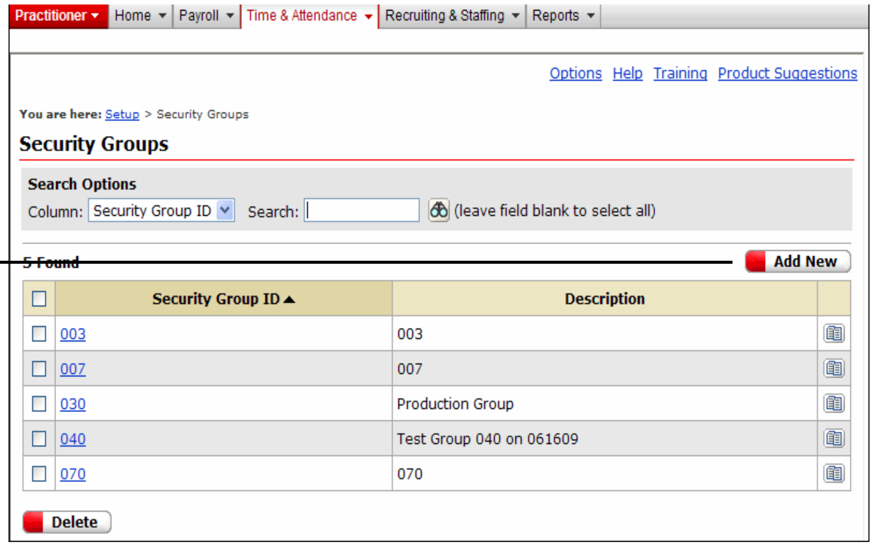
1. Select **Time & Attendance > Setup**.
2. From the **Users** section, select **Security Groups**.

Select this option to create a new security group.



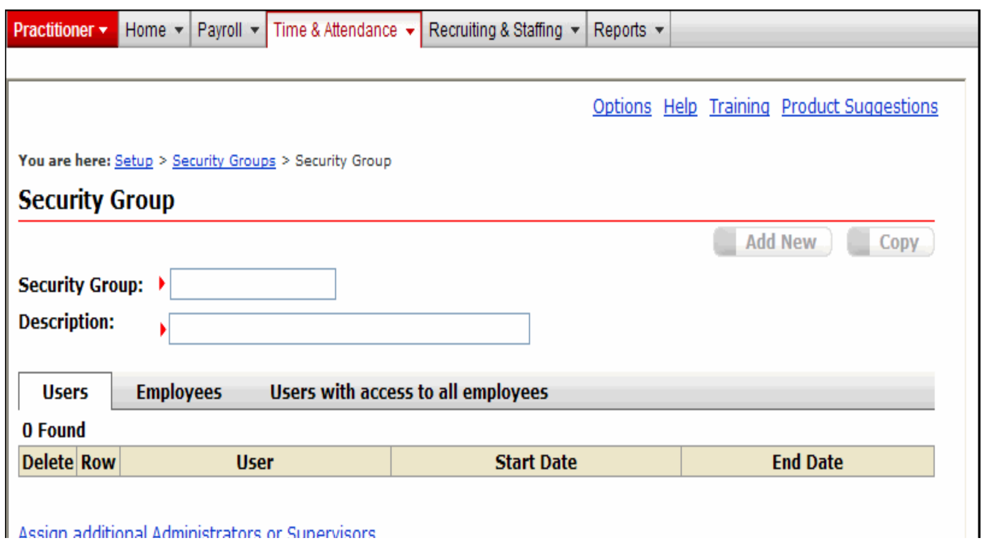
**3** On the **Security Groups** page, click **Add New**.

Add New




**4** In the **Security Group** field, type a unique ID for the new security group.

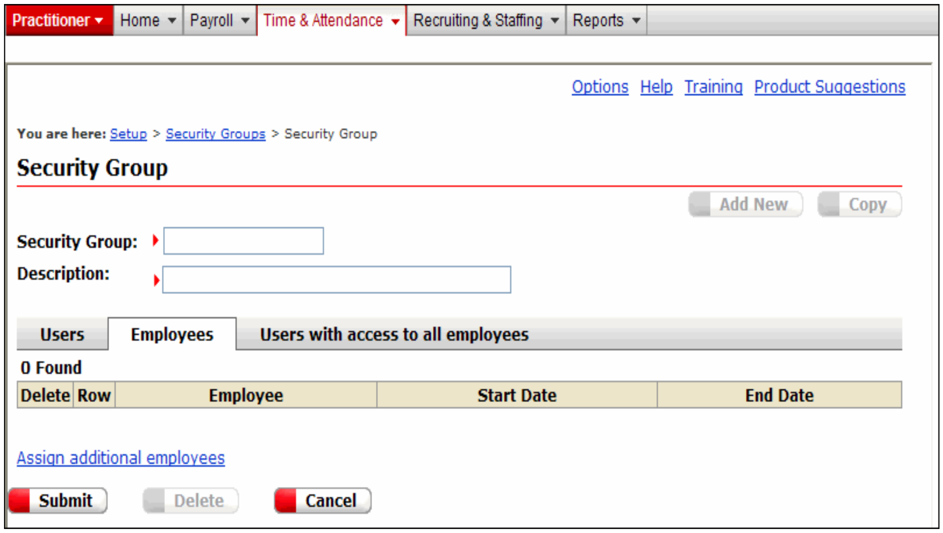
**5** In the **Description** field, type a short description of the security group.




**Note:** Be sure to choose a descriptive name for the group. If you need to change the name of an existing security group, you must remove all employees from the group, create a new security group with the desired name, and then reassign the employees to the new group.

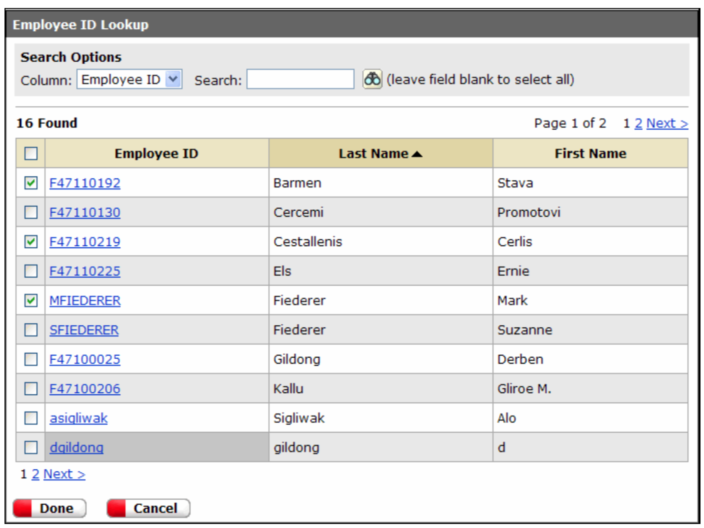
**6** Select the **Employees** tab. The Employees tab displays all employees who are currently members of the security group.

Since you are creating a new group, no employees are listed yet.

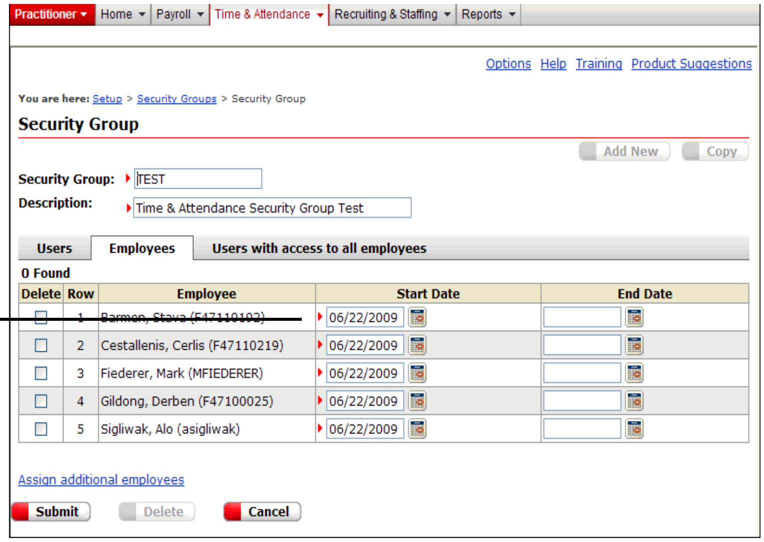



**7** Click the **Assign Additional Employees** link.

**8** Click to select the check box for each employee that you want to add to the security group.



**9** Click **Done**.




The **Start Date** field is automatically filled in with the current date.

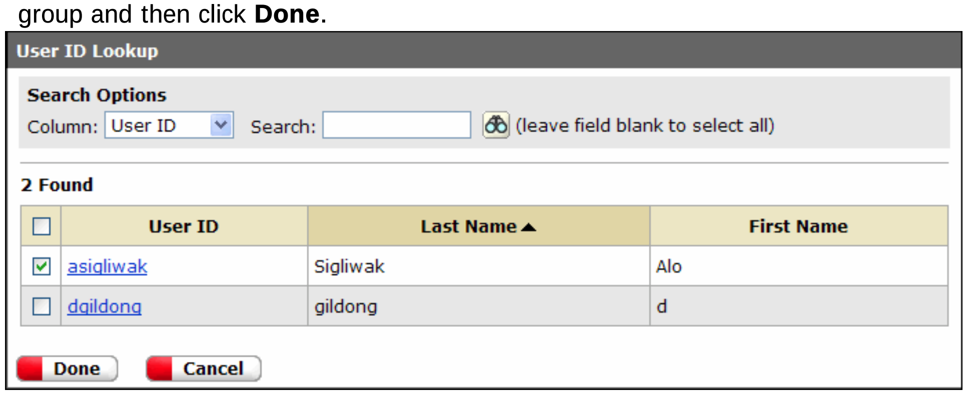
**10** On the **Security Group** page, the **Start Date** field is automatically filled in with the current date. The date in this field indicates when an employee begins being a member of the security group. To change the start date click the button and then selecting a different date

**11** To enter an end date on which the employee will stop being a member of the security group, click the button next to the **End Date** field and then select a date. If you want the employee to be a member of the security group indefinitely, do not enter a date in the **End Date** field.

**12** Select the **Users** tab. The **Users** tab displays all users who currently have access to the security group. Users listed on this tab can view and edit the employees who are listed on the **Employees** tab. (Because you are creating a new security group, no users should be listed on this tab yet.)

**13** Click the **Assign additional administrator or supervisors** link.

**14** Click to select the check box for each user who should have access to the security group and then click **Done**.

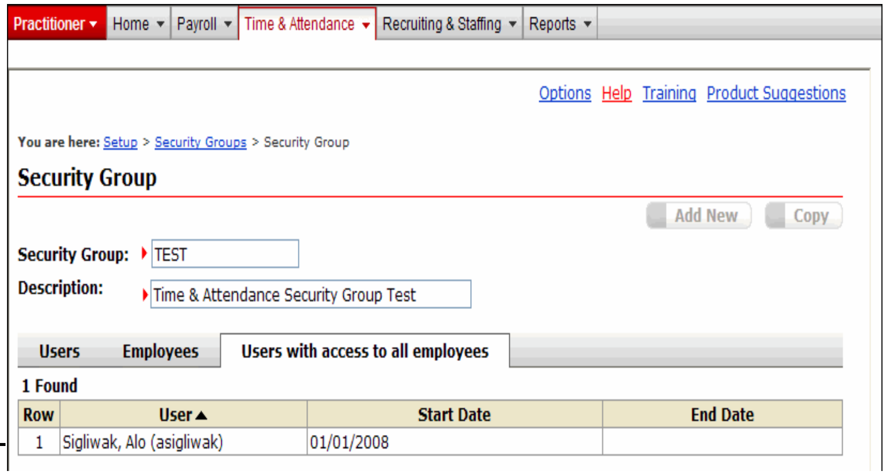



**15** On the **Security Group** page, the **Start Date** field is automatically filled in with the current date. The date in this field indicates when a user can begin accessing the employees in the security group. To change the start date click the button and select a different date.

**16** To enter an end date on which the user will no longer have access to the security group, click the button next to the **End Date** field and then select an end date. If you want the user to have access to the security group indefinitely, do not enter a date in the **End Date** field.

**17** Click the **Users with access to all employees** tab to see which users have full access to employee records.

This user has full access to all employees.




**18** Click **Submit**.

## Creating Security Groups by Copying Existing Security Groups

Copying a security group is a quick way to create a new security group based on an existing security group ID, description, employee assignments, and user assignments. The security group from which the copy is created remains unchanged in the list of groups.

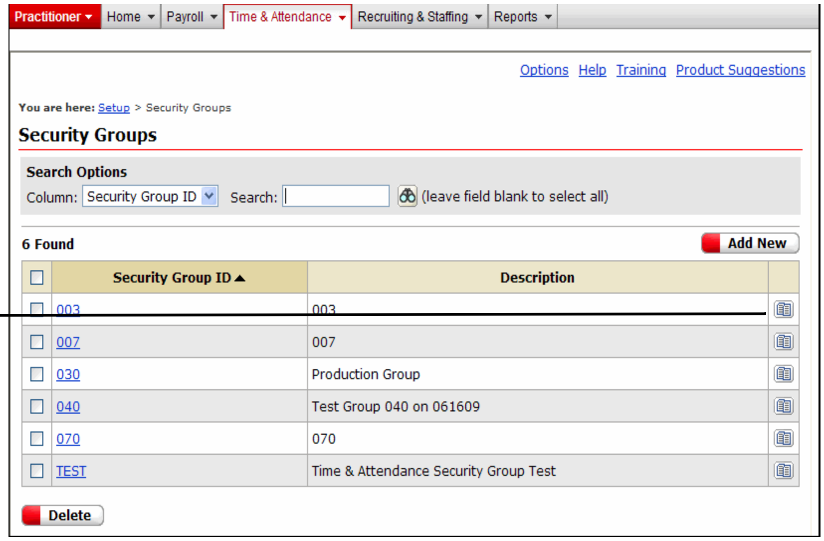
To create a new security group by copying an existing group, follow these steps:

**1** Select **Time & Attendance > Setup**.

**2** From the **Users** section, select **Security Groups**.

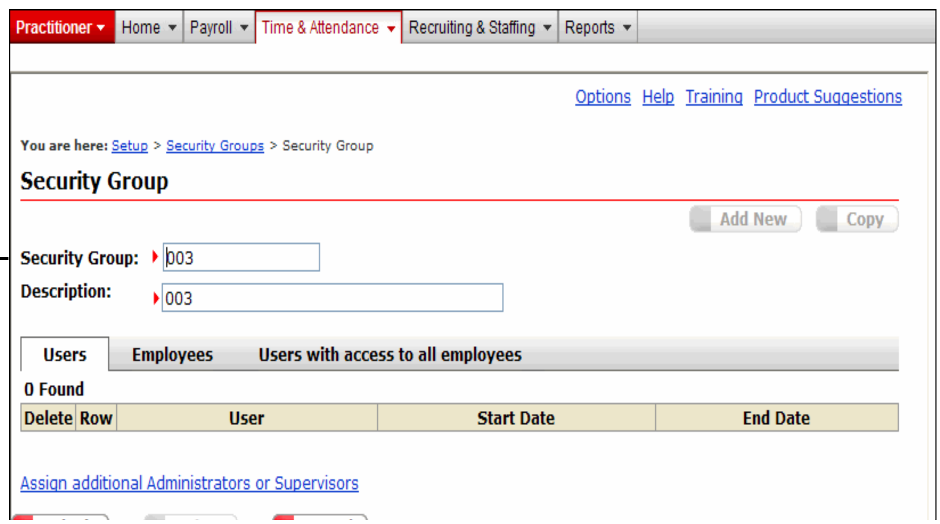
**3** On the **Security Groups** page, click the button to the right side of the security group that you want to copy.

Copy button




**4** On the Security Group page, the details of the security group is displayed. Enter a new security group ID in the **Security Group** field.

Edit the fields for the copied employee record to make it unique.




**5** In the **Description** field, create a unique description for the new security group.

**6** On the **Users** tab, make any necessary edits to the list of users who have access to the security group.

**7** On the **Employees** tab, make any necessary edits to the list of employees who are members of the security group.

**8** Click **Submit**. The new security group displays in the list of existing security groups.

# Assigning Employees to Security Groups

As a security master, you can assign an employee to a security group. Employees are grouped into security groups to control who can access their information in the Time & Attendance module.

**Note:** EL_ALL is a special security group that allows certain administrators to view all employees, regardless of the employees' security group settings. If you are setting up a payroll administrator or other administrator who needs access to all employees, add the administrator to the EL_ALL security group.

1 Select **Time & Attendance > Setup**.

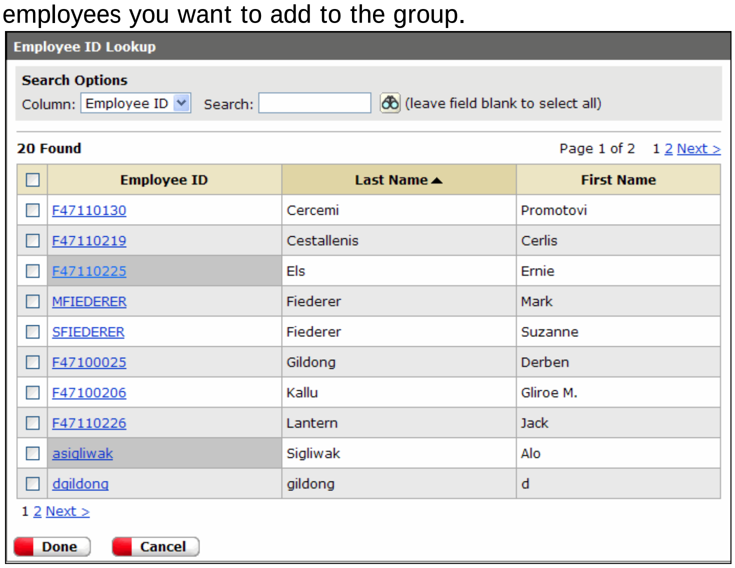
2 From the **Users** section, select **Security Groups**.

3 On **Security Groups** page, click to select the check box next to the security group for which you want to add employees.

4 Click the **Employees** tab to see all employees who are currently members of the security group.

5 Click the **Assign additional employees** link.

6 In **Employee ID Lookup** window, click to select the check box for all those employees you want to add to the group.




**Note:** The Employee ID Lookup window lists only the employees you are allowed to view. Employees are sorted alphabetically by last name. You can quickly change the sort order by clicking the **Employee ID** or **First Name** column headings.

To search for a specific name in the list, select **Last Name** from the **Column** drop-down menu, enter a last name in the **Search** field, and then click the button. Doing this saves the search option (**Last Name** in this example) as your default setting for the **Column** menu in all Employee ID Lookup windows. You can also select **First Name** or **Employee ID** from the **Column** menu, enter a first name or employee ID, and click the button. The **First Name** or **Employee ID** option is then saved as the default setting.

7 Click **Done**.

8 On the **Security Group** page, the **Start Date** field is automatically filled in with the current date. The date in this field indicates when a user can begin accessing the employees in the security group. To change the start date click the button and select a different date.

9 To enter an end date on which the user will no longer have access to the security group, click the button next to the **End Date** field and then select an end date. If you want the user to have access to the security group indefinitely, do not enter a date in the **End Date** field.

10 When you have selected all employees you want as members of the security group, click **Submit**.

## Assigning User Access to Security Groups

As a security master, you can assign security group access to users. When you assign access to a user, the user can view and edit the records of all employees who belong to the security group. Note that assigning a user access to a security group does not make the user a member of the group. It only allows the user access to the records of the employees who are members of the group.

**Example**

You supervise the Sales group, and all of your employees are assigned to the Sales security group. You are also a member of the Sales security group, but you cannot see your employees' records. Why not?

To view an employee's record, you must be assigned access to that employee's security group. Access to employee records is controlled by the security group settings associated with your Time & Attendance user ID, rather than the security groups you and your employee are members of. You are probably set up as a member of the Sales group, but you have not been configured to give you access to employees in the Sales group. Contact your payroll or system administrator to have your user settings changed.

To assign security group access to users, follow these steps:

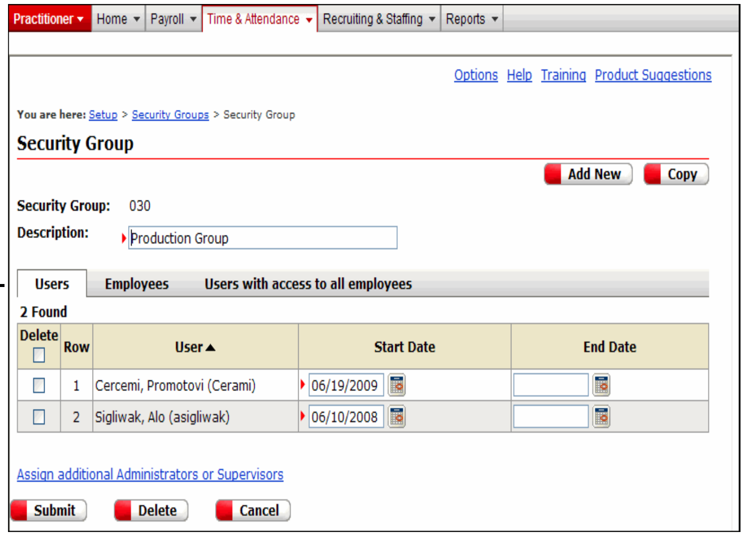
1 Select **Time & Attendance > Setup**.

2 From the **Users** section, select **Security Groups**.

3 In the **Security Group ID** column, click the security group for which you want to assign access to users.

**4** On the Security Group page, all users who currently have access to the security group are listed. Click the **Assign additional users or supervisors** link.

The **Users** tab lists all users who have access to this security group.



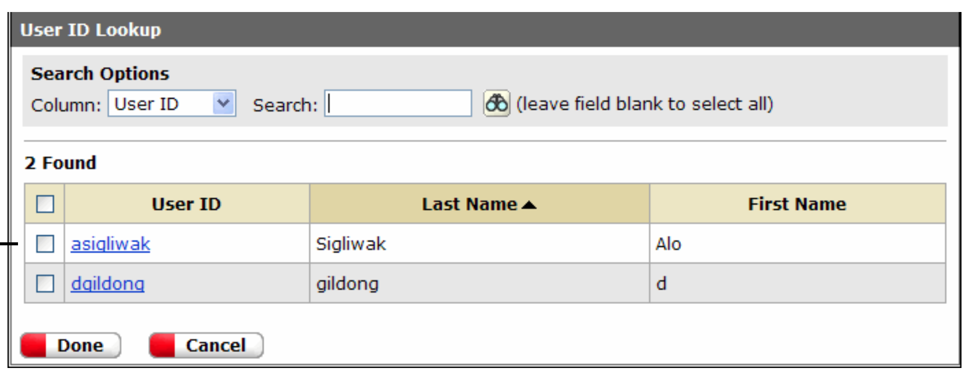

**5** In the **User ID Lookup** window, click to select the check box next to the users you want to add to the security group and then click **Done**.

---

**Note:** The User ID Lookup window lists only the employees you are allowed to view. Employees are sorted alphabetically by last name. You can quickly change the sort order by clicking the **Employee ID** or **First Name** column headings. To search for a specific name in the list, select **Last Name** from the **Column** drop-down menu, enter a last name in the **Search** field, and then click the button. Doing this saves the search option (**Last Name** in this example) as your default setting for the **Column** menu in all Employee ID Lookup windows. You can also select **First Name** or **Employee ID** from the **Column** menu, enter a first name or employee ID, and click the button. The **First Name** or **Employee ID** option is then saved as the default setting.

---

Click to select the check box for the users you want to assign to the group.




**6** On the **Security Group** page, the **Start Date** field is automatically filled in with the current date. The date in this field indicates when a user can begin accessing the employees in the security group. To change the start date by click the button and select a different date.

7 To enter an end date on which the user will no longer have access to the security group, click the button next to the **End Date** field and then select an end date. If you want the user to have access to the security group indefinitely, do not enter a date in the **End Date** field.

8 When you have selected all users you want to have access to the security group, click **Submit**.

# Editing a Security Group's Configuration

As a security master, you can perform a variety of maintenance tasks to keep security groups up to date.

## Editing a Security Group's Description

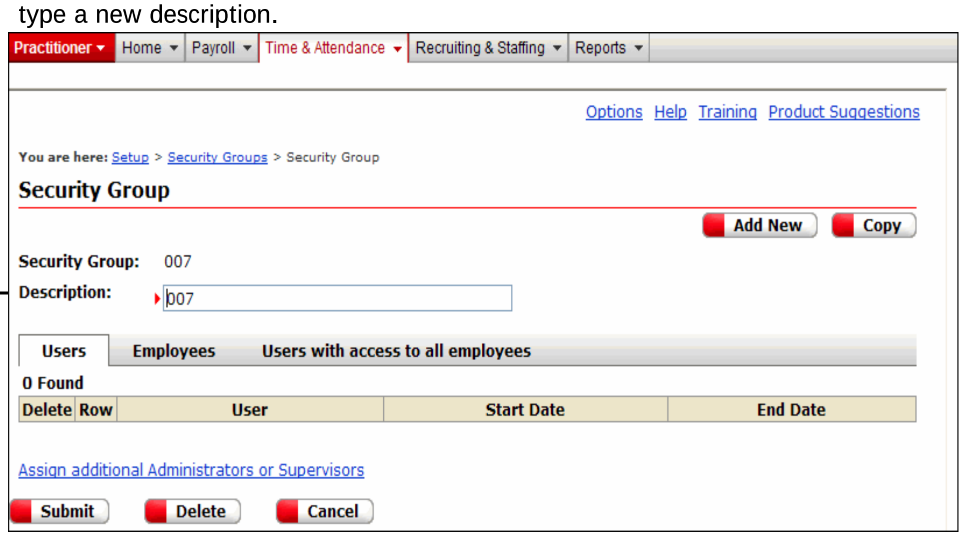
1 Select **Time & Attendance > Setup**.

2 From the **Users** section, select **Security Groups**.

3 Select the ID for the security group with the description that you want to edit.

4 On the **Security Group** page, delete the current entry in the **Description** field and type a new description.

Change this field to update the description.




5 Click **Submit**.

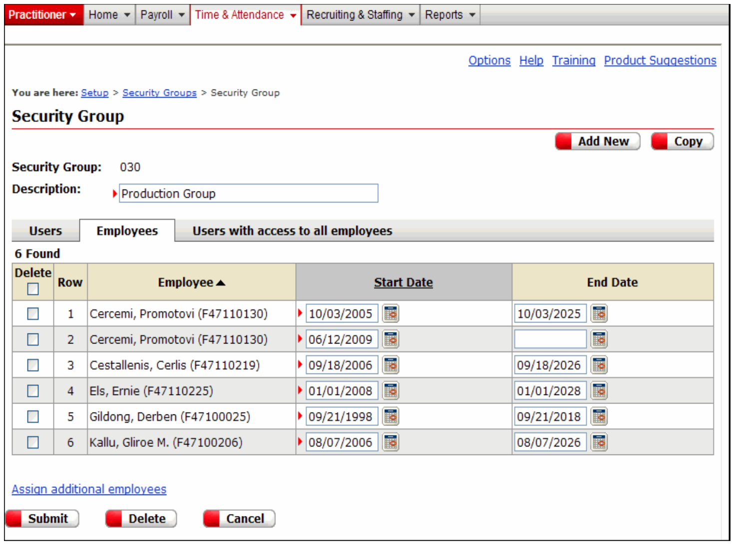
## Adding Employees to a Security Group

1 Select **Time & Attendance > Setup**.

2 From the **Users** section, select **Security Groups**.

3 Click the **Security Group ID** for the security group that you want to edit.

**4** On the **Security Group** page, click the **Employees** tab.




**5** Click the **Assign additional employees** link.

**6** In the **Employee ID Lookup** window, click to select the check box for each employee you want to add as a member of the security group, and then click **Done**.

**7** On the **Security Group** page, the **Start Date** field is automatically filled in with the current date. The date in this field indicates when a user can begin accessing the employees in the security group. To change the start date by click the button and select a different date.

**8** To enter an end date on which the user will no longer have access to the security group, click the button next to the **End Date** field and then select an end date. If you want the user to have access to the security group indefinitely, do not enter a date in the **End Date** field.

**9** To delete employees from the security group, click to select the check box in the **Delete** column on the Security Group page for each employee that you want to delete.

**10** Click **Submit**.

## Changing the Users Who Can Access a Security Group

**1** Select **Time & Attendance > Setup**.

**2** From the **Users** section, select **Security Groups**.

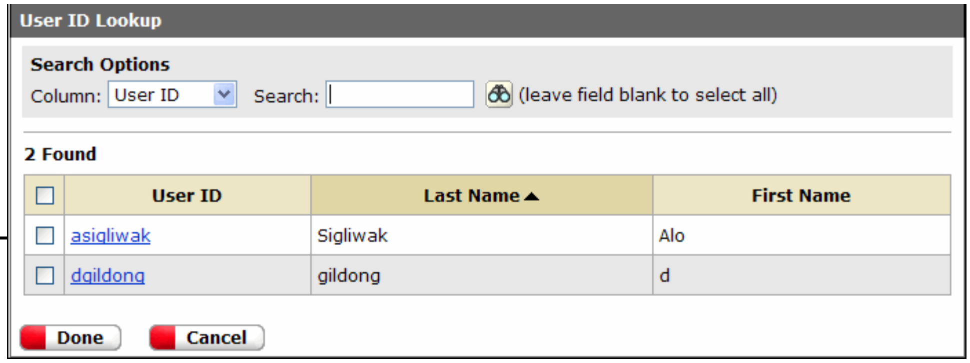
**3** Click the **Security Group ID** for the security group that you want to edit.

**4** On the **Security Group** page, click the **Users** tab.

**5** Click the **Assign additional users** link.

6 In the **User ID Lookup** window, click to select the check box for each user whom you want to have access to the security group and then click **Done**.

Click to select the check box for the user who should be able to access this group.




7 On the **Security Group** page, the **Start Date** field is automatically filled in with the current date. The date in this field indicates when a user can begin accessing the employees in the security group. To change the start date by click the button and select a different date.

8 To enter an end date on which the user will no longer have access to the security group, click the button next to the **End Date** field and then select an end date. If you want the user to have access to the security group indefinitely, do not enter a date in the **End Date** field.

9 To remove a user's access to the security group, click to select the check box in the **Delete** column on the Security Group page for each user that you want to remove access from.

10 Click **Submit**.

## Viewing a List of Users Who Have Access to All Employees

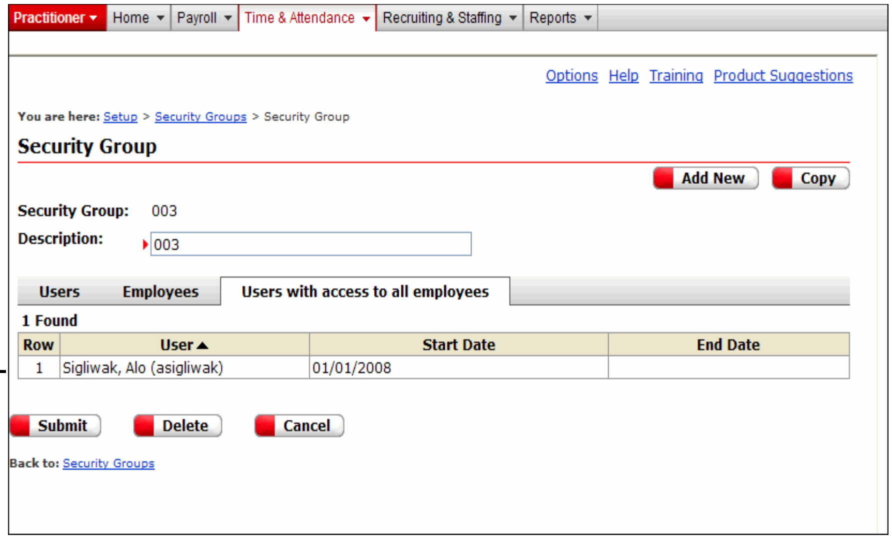
1 Select **Time & Attendance > Setup**.

2 From the **Users** section, select **Security Groups**.

3 On the **Security Groups** page, click the ID for any security group in the list.

**4** Click the **Users with access to all employees** tab. Users with access to all security groups are listed.

This group can access all security groups.




**Note:** You cannot edit any of the assignments on this tab. The information is read-only.

## Removing Employees from Security Groups

To remove employees from a security group, follow these steps:

**1** Select **Time & Attendance > Setup**.

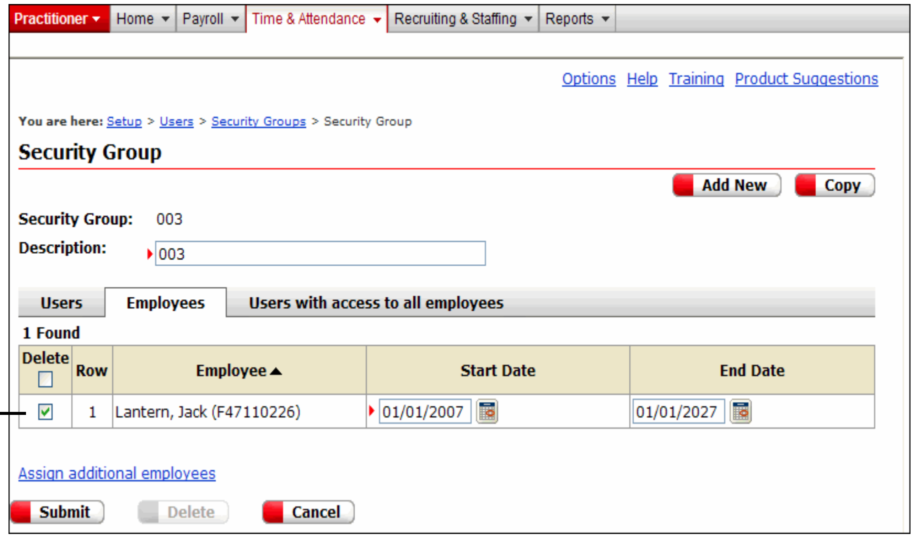
**2** From the **Users** section, select **Security Groups**.

**3** In the **Security Group ID** column, click the security group containing the employee whom you want to remove.

**4** Select the **Employees** tab. The Employees tab lists all employees who are currently members of the security group

5 In the **Delete** column, click to select the check box for each employee whom you want to remove from the security group.

Click to select the check box for the employee you are removing from this group.




6 Click **Submit**.

## Removing User Access to Security Groups

If you have the necessary authorization, you can remove a user's access to a security group. When you remove a user's access, he/she can no longer view the records of the employees who belong to the security group.

To remove a user's access to a security group:

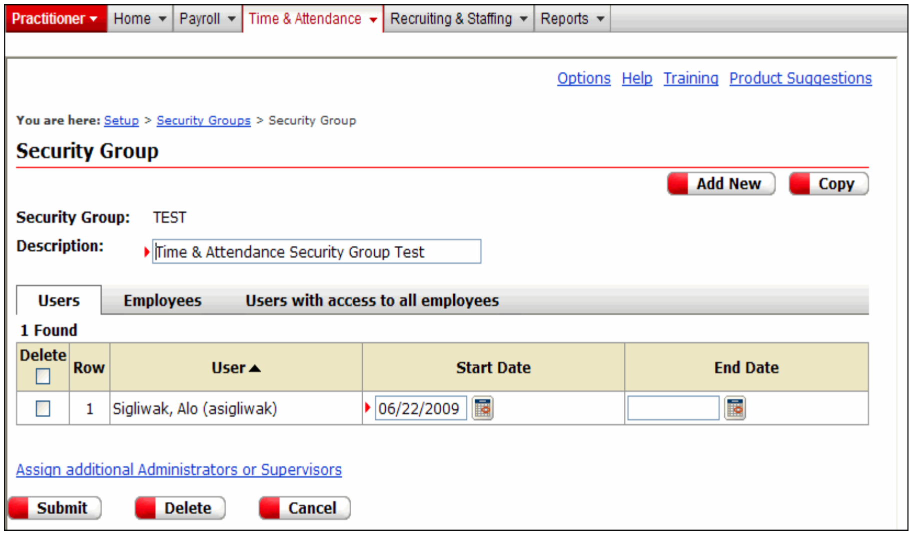
1 Select **Time & Attendance > Setup**.

2 From the **Users** section, select **Security Groups**.

3 In the **Security Group ID** column, click the security group containing the user whose access you want to remove.

4 Select the **Users** tab. The Users tab lists all users who can currently access the security group.

5 In the **Delete** column, click to select the check box for each user whose access you want to remove from the security group.




6 Click **Submit**.

## Deleting Security Groups

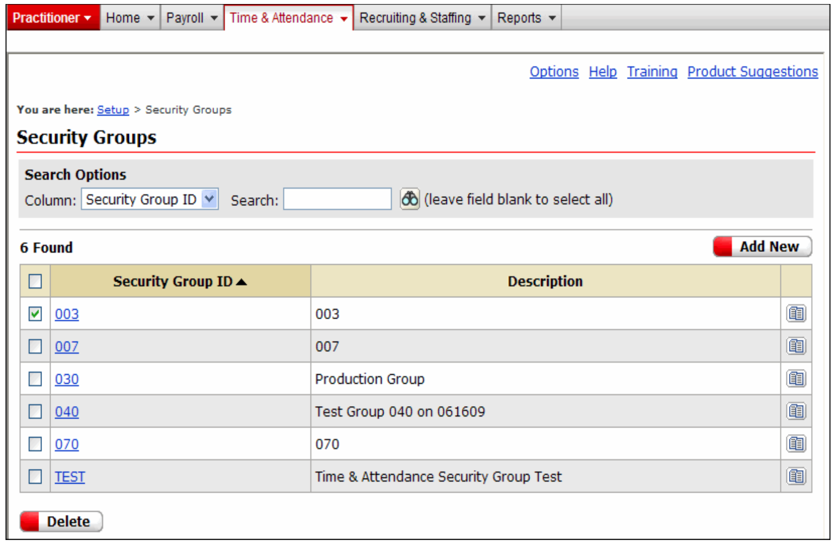
As a security master, you can delete security groups that are not currently being used.

**Important:** You cannot delete a security group if one or more employees are assigned to it. To delete a security group, you must first remove all employees from that security group.

1 Select **Time & Attendance > Setup**.

2 From the **Users** section, click to select **Security Groups**.

**3** On the **Security Groups** page, click to select the check box next to each security group you want to delete.




**4** Click **Delete**.

**5** In the confirmation dialog box, click **OK**.

# Managing User Access

As a security master, you can perform user-management tasks such as these:

- Assign Time & Attendance access to employees
- Assign user access to security groups
- Change an active user's status to inactive
- Reactivate inactive users
- Configure supervisor users to emulate other supervisors
- Allow a user to access locked pay cycles
- Delete a user's access from Time & Attendance

**Important:** If you are using the ADP payroll module that has an Integrated Employee Editor (a version of the Time & Attendance Employees and User pages that exists inside the payroll module), you should add users and make changes to user records in that ADP payroll module. Do not make user changes in Time & Attendance. If you are **not** using an integrated ADP payroll module, you can use the following instructions to add and change user records.

## Assigning Time & Attendance Access to Employees

Some employees are automatically assigned user access to Time & Attendance as part of an import. Use the instructions below to manually assign user access to employees.

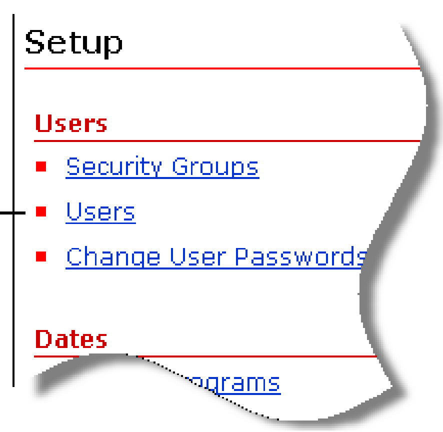
**Note:** An employee must already exist in the Time & Attendance database before you can assign user access to the employee.

Some employees are automatically assigned user access to Time & Attendance as part of an import. Use the instructions below to manually assign user access to employees.

**1** Select **Time & Attendance > Setup**.

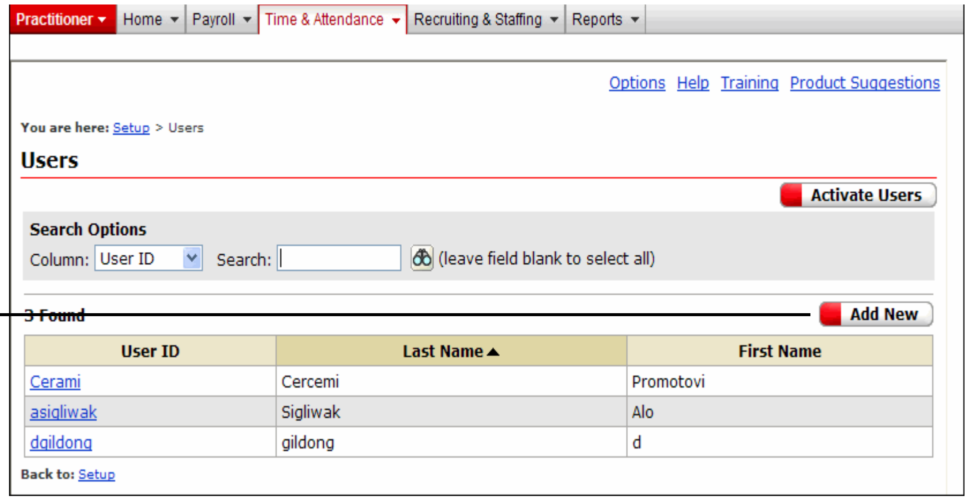
**2** In the **Users** section, click **Users**.

Select this option to assign user access.



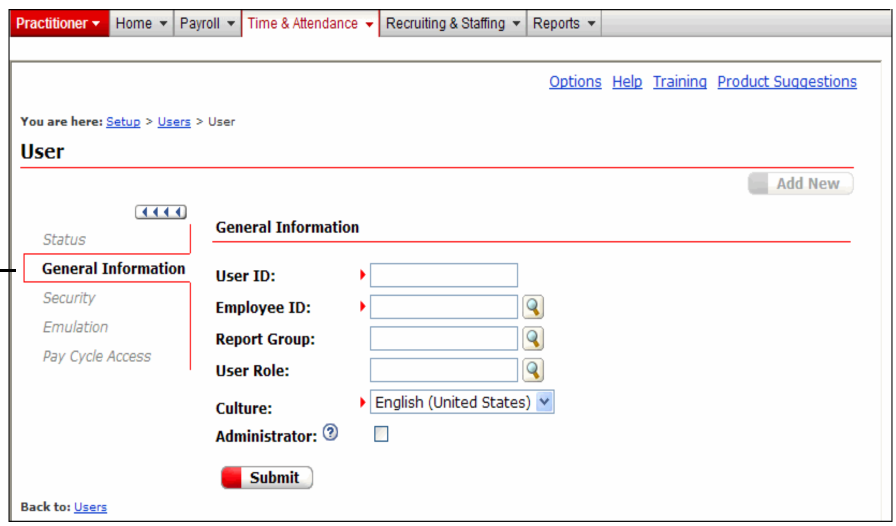
**3** On the Users page, click **Add New**.

**Add New** button




**4** On the User detail page, select the **General Information** option.

**General Information** option




**5** In the **User ID** field, enter the user's ID.

**6** Click the button next to the **Employee ID** field, and then select the employee to whom you want to assign access to Time & Attendance. All users to whom you have access are listed.

**Tip:** To sort the list by user ID, last name, or first name, click the **User ID**, **Last Name**, or **First Name** column heading. To search for a specific name, select **Last Name** from the **Column** drop-down menu, enter a last name in the **Search** field, and then click the button. (You can also search by a user ID or first name.)

**7** Click the button next to the **Report Group** field, and then select the user's report group.

8 If the user should have administrator rights, click the button next to the **User Role** field, and then select the appropriate user role.

**Note:** A user role only needs to be defined for administrator users. For supervisors, access to supervisor services and supervisory functions is enabled when you click the **Is Supervisor** box in the employee record. Do not assign a user role to users who should not have access to administrator services.

9 In the **Culture** field, select the language in which the Time & Attendance module should be displayed to the user.

10 If you have assigned the user an administrator role and you also want the user have additional capabilities, click to select the **Administrator** check box. For a list of the additional capabilities, click the icon next to the **Administrator** check box.

**Note:** If you select the **Administrator** check box, you must also select a user role in the **User Role** field.

11 Click **Submit**. (After you click **Submit**, you can enter additional information in the user's profile.)

## Assigning User Access to Security Groups

When you assign access to a security group, you are only giving the user access to those groups for supervisory or administrative purposes. You are not making the user a member of the group. Supervisors should be assigned access to all security groups for the employees they manage. Administrators who perform end-of-period operations should be assigned access to a special company-wide security group.

To assign access to a security group, follow these steps:

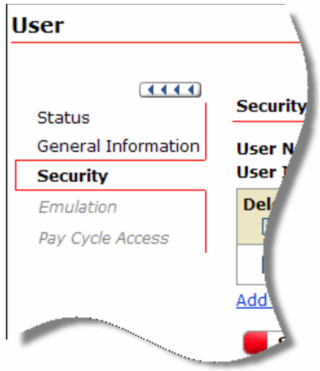
**Note:** If the user you created is a supervisor or an administrator, you must assign the user access to the security groups that contain the employees whose records you want him or her to have access to. If the user needs to have access to all employees in the company (to perform end-of-period operations, for example), select the EL_ALL security group.

1 Select **Time & Attendance > Setup**.

2 In the **Users** section, click **Users**.

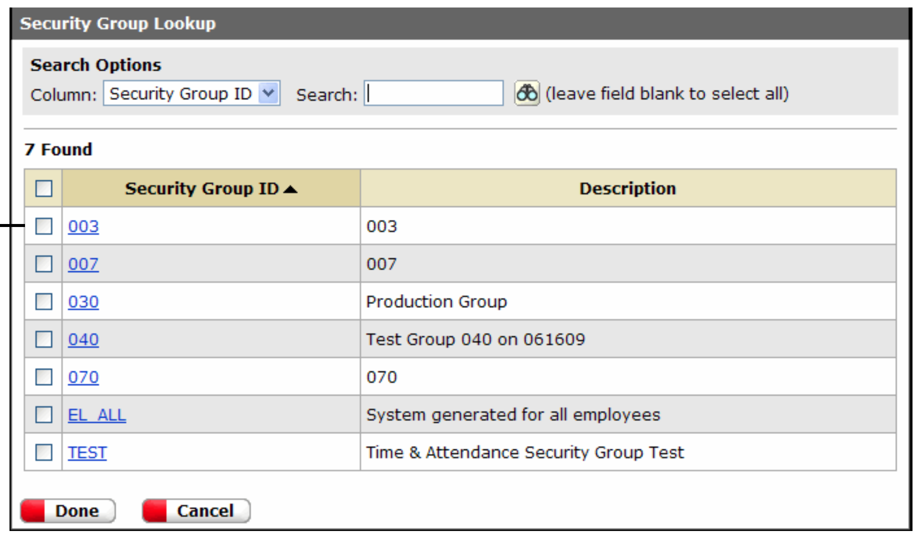
**3** On the User detail page, select the **Security** option and then click **Add additional Security Groups**.

Security option




**4** In the **Security Group Lookup** window, click to select the check box for each security group to which you want to assign the user access and click **Done**.

Click to select the check box for the security group to which you want to assign user access.




**5** On the **Users** page, select the user whose access to security groups you want to configure. All users to whom you have access are listed alphabetically by last name.

**Tip:** To sort the list by user ID, last name, or first name, click the **User ID**, **Last Name**, or **First Name** column heading. To search for a specific name, select **Last Name** from the **Column** drop-down menu, enter a last name in the **Search** field, and then click the button. (You can also search by a user ID or first name.)

**6** To assign the user access to other security groups, click the **Add additional Security Groups** link.

**7** In the **Security Group Lookup** window, click to select the check box next to each security group to which you want the user to have access, and then click **Done**.

8 In the **Start Date** column, the current date is automatically entered in the **Start Date** field. This date indicates when the user will begin having access to the employees in the security groups. To change this date, click the button to the **Start Date** field for each security group and then select a different date.

9 To enter a date on which you want the user to stop having access to a security group, click the button next to the **End Date** field and then select a date. If you want the user to have access to a security group indefinitely, do not enter a date in the **End Date** field.

10 Click **Submit**.

**Note:** To view a complete list of security groups to which the user can access in Time & Attendance, click the **View Employee - User Security Group Assignments** link on the right side of the page.

## Viewing Security Group Assignments

As an administrator you can quickly view the current security group assignments for employees and users that you have access to.

1 Select **Time & Attendance > Setup**.

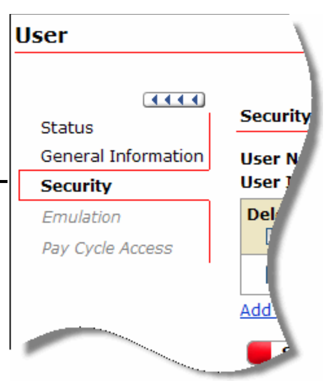
2 In the **Users** section, click **Users**.

3 Select the **User ID** for the user whose security group assignment you want to check. All users to whom you have access are listed alphabetically by last name.

**Tip:** To sort the list by user ID or first name, click the **User ID** or **First Name** column heading. To search for a specific name, select **Last Name** from the **Column** drop-down menu, enter a last name in the **Search** field, and then click the button. (You can also search by a user ID or first name.)

4 On the **User** page, click the **Security** option.

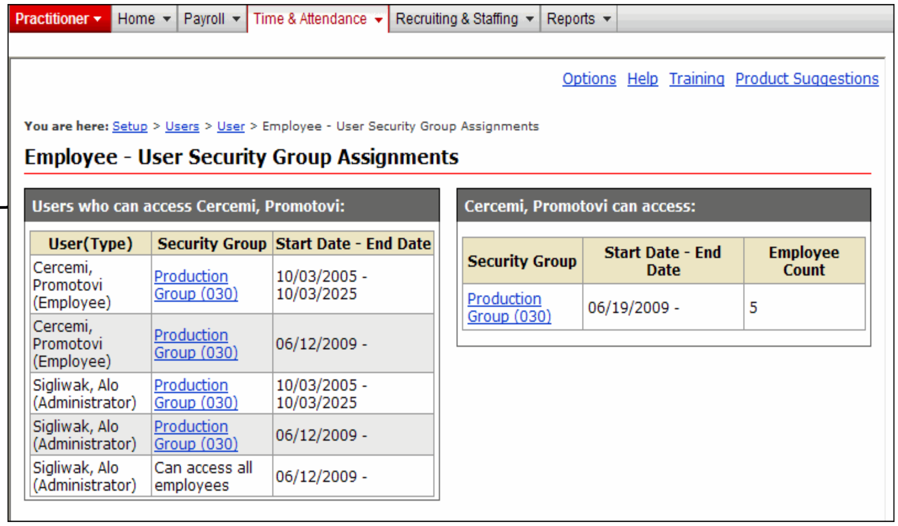
Security option




All security groups to which the user currently has access are listed. If no security groups have been assigned yet, the list is blank.

5 Click **Employee - User Security Group Assignments**.

Details of the assignment




Users who can access Cercemi, Promotovi:

| User(Type) | Security Group | Start Date - End Date |
|---|---|---|
| Cercemi, Promotovi (Employee) | Production Group (030) | 10/03/2005 - 10/03/2025 |
| Cercemi, Promotovi (Employee) | Production Group (030) | 06/12/2009 - |
| Sigliwak, Alo (Administrator) | Production Group (030) | 10/03/2005 - 10/03/2025 |
| Sigliwak, Alo (Administrator) | Production Group (030) | 06/12/2009 - |
| Sigliwak, Alo (Administrator) | Can access all employees | 06/12/2009 - |

Cercemi, Promotovi can access:

| Security Group | Start Date - End Date | Employee Count |
|---|---|---|
| Production Group (030) | 06/19/2009 - | 5 |

Under the **Users who can access [NAME OF EMPLOYEE]** section, the following information is displayed in each column:

- **User (Type)**: Lists all Time & Attendance users who can view the records of the employee you selected in step 3.
- **Security Group**: Lists the security groups to which the selected employee belongs. You can click the security group name to view details about the security group's configuration. (If a user has access to all employees in the company, the Can access all employees message is displayed, which cannot be clicked.)
- **Start Date - End Date**: Lists the date the employee became a member of the security group and the date (if any) the employee will stop being a member of the security group.

Under the **[NAME OF EMPLOYEE] can access** section, the following information is displayed in each column:

- **Security Group**: Lists all security groups to which the employee you selected in step 3 has access to. You can click the security group name to view details about the security group's configuration. If the employee does not have access to any security groups, this section is blank.
- **Start Date - End Date**: Lists the date the employee began having access to the security group and the date (if any) the employee will stop having access to the security group.
- **Employee Count:** The number of employees who are members of the security group.

# Configuring Which Users Are Allowed to Emulate a Selected User

1 Select **Time & Attendance > Setup**.

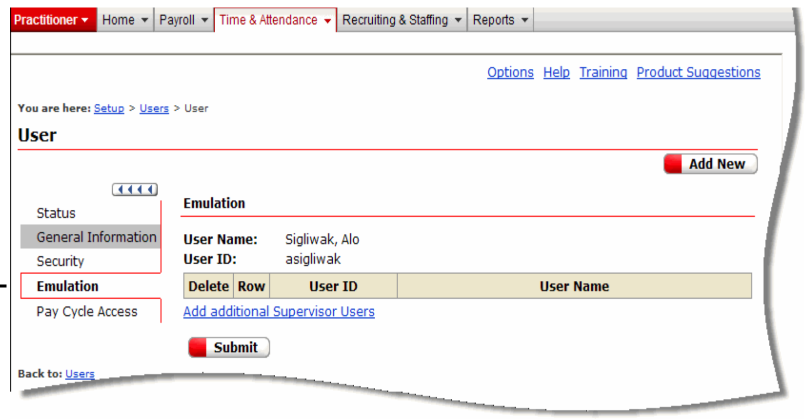
2 In the **Users** section, click **Users**.

3 On the **Users** page, select a user.

4 Select the **Emulation** option. All users who already have permission to emulate the selected user are listed. If no users have been given permission, the list is blank.

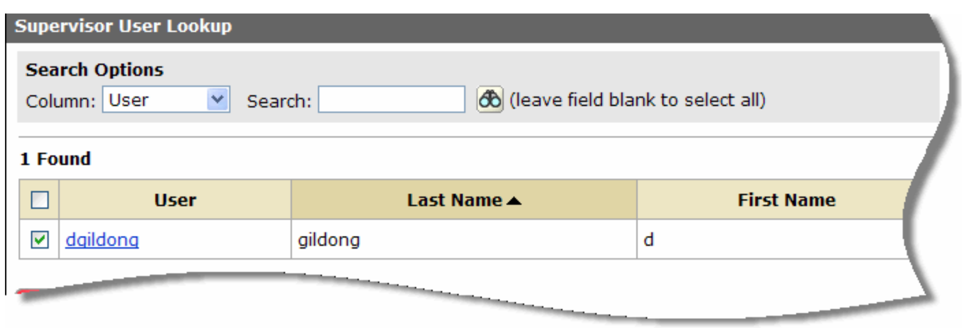
**Note:** Only supervisors and administrators can be emulated. If you selected a user in Step 3 who is not a supervisor or administrator, the **Emulation** option is not available on the User page.

Emulation option




5 Click **Add Additional Supervisor Users**.

6 In the **Supervisor User Lookup** window, click to select the check box for each supervisor or administrator you want to give permission to emulate the user and click **Done**.




7 Click **Done**.

8 Click **Submit**.

## Changing an Active User's Status to Inactive

You can change an active user's status to inactive when the user is temporarily not working. You might need to do this if a user takes maternity leave, for example.

When a user's status is inactive, the user cannot access the Time & Attendance application. However, the user's profile is not deleted from Time & Attendance. The status can be changed back to active at any time. The user’s settings continue to be stored in the Time & Attendance database so that you do not have to re-enter them if you reactivate the user later.

If a user will never again need access to Time & Attendance, you can permanently delete a user's access. Deleting a user permanently removes the individual's access from Time & Attendance, but does not affect the person’s employee data.

**Note:** Some employees are automatically assigned user access to Time & Attendance as part of an import. Use the following information when you need to manually change user access for employees.

To change an active user's status to inactive:

1 Select **Time & Attendance > Setup**.

2 In the **Users** section, click **Users**.

3 On the **Users** page, select the user whose status you want to change. All users to whom you have access are listed.

> **Tip:** To sort the list by user ID, last name, or first name, click the **User ID**, **Last Name**, or **First Name** column heading. To search for a specific name, select **Last Name** from the **Column** drop-down menu, enter a last name in the **Search** field, and then click the button. (You can also search by a user ID or first name.)

4 Select **Status** from the menu on the left.

5 On the **User** page, click **Inactivate User**.

6 In the confirmation dialog box, click **OK**.

> **Note:** A user's current status displays to the right of the user's name on the User page. When a user's status is inactive, the user still appears in the list of users on the main Users page. To see a list of inactive users, click **Activate Users** on the Users page.

## Reactivating an Inactive User

You may be asked to reactivate a user who is returning to your company from a leave of absence, such as maternity leave. Your company may also be configured so that if a user enters incorrect login information more than a predetermined number of times, that user's account will be inactivated. The user will then have to contact you to reactivate his/her account. This is done as a security precaution.

To reactivate inactive users:

1 Select **Time & Attendance > Setup**.

2 In the **Users** section, click **Users**.

3 On the top right side of the Users page, click **Activate Users**. The Activate Users page opens, which lists all inactive users to whom you have access.

4 In the **Activate** column, click to select the check box for each user you want to activate.

**Tip:** To select all users in the list, click the check box in the header row of the Activate column.

5 Click **Activate Selected Users**.

6 Click **OK**.

**Note:** When you click **OK**, the page is refreshed with the users you selected removed from the list. After the page refreshes, you can activate additional users, or return to the main Users page by clicking the **Users** link in the **You are here** path at the top of the page.

## Deleting a User's Access to Time & Attendance

When you delete a user, only the user's access to Time & Attendance is removed. The user's employee record is not changed or deleted.

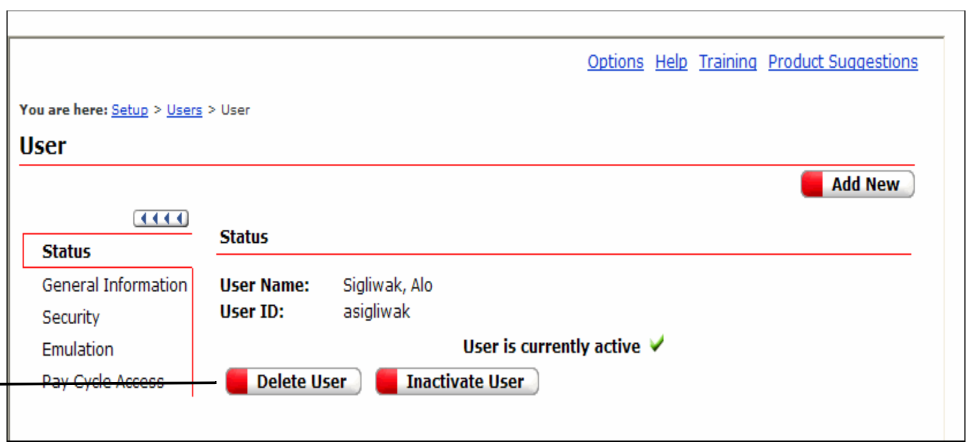
1 Select **Time & Attendance > Setup**.

2 In the **Users** section, click **Users**.

3 On the **Users** page, select a user.

4 Click **Delete User**.

Delete User button




5 Click **OK**.

## Configuring Supervisor Users to Emulate Other Supervisors

User emulation allows a supervisor or administrator to log on to Time & Attendance as another user to resolve timecard exceptions, run end-of-period operations, and perform other basic supervisor tasks for the other user's employees. This may be required if a supervisor is out sick or on vacation.

---

**Tip:** If you have permission to emulate another user, log on to Time & Attendance normally, and then click the **Options** button in the upper-right corner of any main page. In the Options window, click to select the **Emulation** check box, choose the user you want to emulate from the drop-down menu, and then click **Submit**. (For more detailed instructions, see "Configuring Which Users Are Allowed to Emulate a Selected User" on page 150.

---

1. To Select **Time & Attendance > Setup**.
2. In the **Users** section, click **Users**.
3. On the **Users** page, select the user for whom you want to configure user emulation. All users to whom you have access are listed.

   **Tip:** To sort the list by user ID, last name, or first name, click the **User ID**, **Last Name**, or **First Name** column heading. To search for a specific name, select **Last Name** from the **Column** drop-down menu, enter a last name in the **Search** field, and then click the button. (You can also search by a user ID or first name.)

4. Select the **Emulation** option.

   **Note:** All users who already have permission to emulate the selected user are listed. If no users have been given permission, the list is blank.

5. To remove a user's permission, click to select the check box in the **Delete** column for each supervisor whose emulating permission you want to remove, and then click **Submit**.
6. To assign other users permission to emulate the selected user, click the **Add additional Supervisor Users** link.
7. On the **Supervisor User Lookup** page, click to select the check box next to each supervisor or administrator you want to give permission to emulate the user. Note that a user must have supervisor rights to emulate other supervisors.

   **Tip:** To select all supervisors in the list, click the check box to the left of the **User** heading.

8. Click **Done**.
9. On the User page, click **Submit**.

## Allowing a User to Access Locked Pay Cycles

When your payroll administrator begins processing payroll for a pay cycle, he or she will lock the pay cycle so that no further changes can be made to employee timecard data for that pay cycle. In some special circumstances, however, an administrator user may need to be able to modify this data after the pay cycle has been locked. For example, an administrator may need to edit a time pair that is causing an exception that is holding up payroll processing. As an administrator, you can assign other administrators permission to access locked pay cycles.

**Note:** If a user has access to a locked pay cycle, he/she can make changes until the pay cycle is rolled. After payroll has been processed and the cycle has been rolled, any changes to the closed pay period must be made with a payroll adjustment.

Administrators who do not have access to locked pay cycles can still view data for locked pay cycles, but they will receive an error message if they attempt to edit data for that cycle.

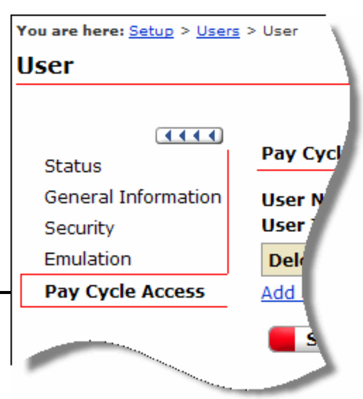
To configure access to locked pay cycles, follow these steps:

1. Select **Time & Attendance > Setup**.
2. In the **Users** section, click **Users**.
3. On the **Users** page, select the user whose access to locked pay cycles you want to configure. All users to whom you have access are listed.

   **Tip:** To sort the list by user ID, last name, or first name, click the **User ID**, **Last Name**, or **First Name** column heading. To search for a specific name, select **Last Name** from the **Column** drop-down menu, enter a last name in the **Search** field, and then click the button. (You can also search by a user ID or first name.)

4. Select the **Pay Cycle Access** option.

**Pay Cycle Access** option

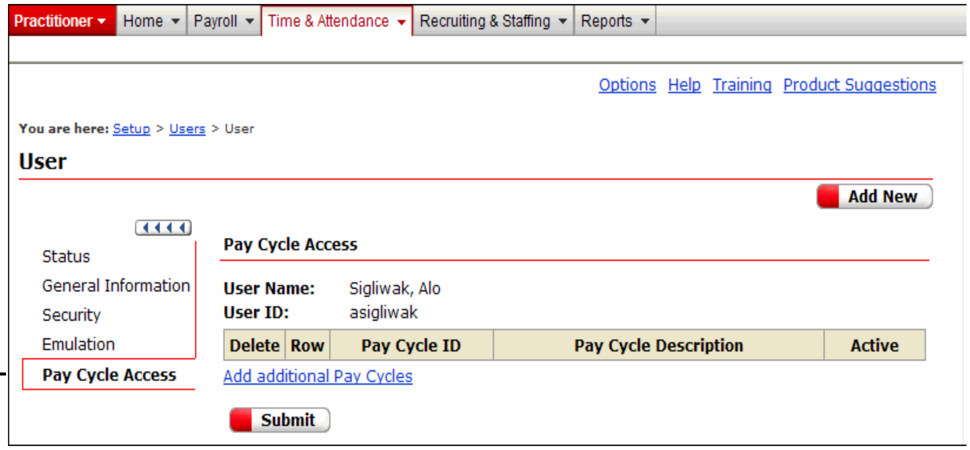



   **Note:** All pay cycles to which the user already has access are listed. If no pay cycles have been assigned yet, the list is blank.

5. If you want to delete a user's access to a locked pay cycle, click to select the check box in the **Delete** column next to the pay cycle you want to delete, and then click **Submit**.

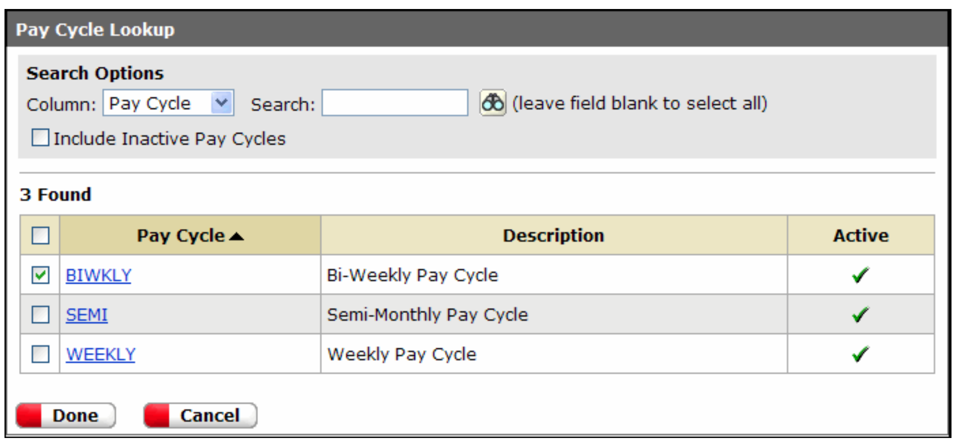
**6** To assign the user access to other locked pay cycles, click the **Add additional Pay Cycles** link.

**Pay Cycle Access** option




**7** On the **Pay Cycle Lookup** page, click to select the check box next to each pay cycle to which you want to give the user access, and then click the **Done** button.

**Tip:** To select all pay cycles in the list, click the check box to the left of the Pay Cycle heading, and then click **Done**.




**8** On the User page, click **Submit**.

# Deleting User Access from Time & Attendance

Deleting a user's access removes that user's ability to access the Time & Attendance module. The user's employee record is not changed or deleted.

**Tip:** If you only want to remove access to Time & Attendance temporarily, you can set a user's status to inactive. You can then reactivate the user at any time without having to re-enter the user's data.

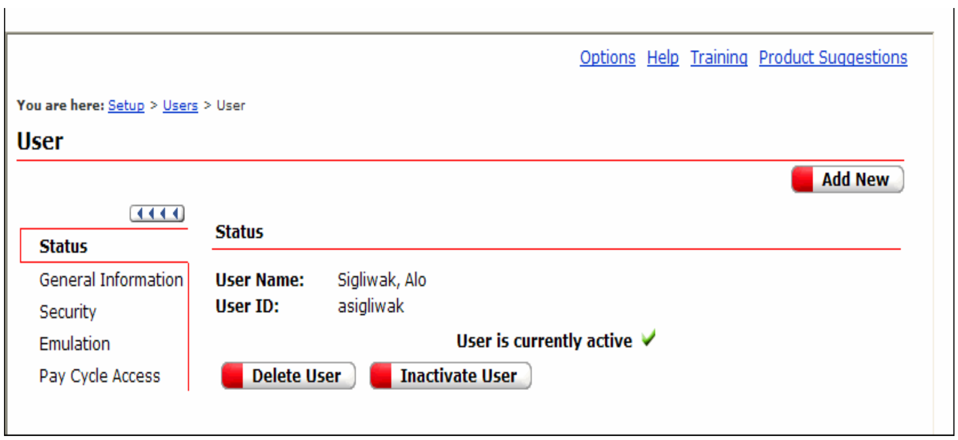
To permanently delete a user's access to Time & Attendance, follow these steps:

1 Select **Time & Attendance > Setup**.

2 In the **Users** section, click **Users**. All users to whom you have access are listed.

> **Tip:** To sort the list by user ID, last name, or first name, click the **User ID**, **Last Name**, or **First Name** column heading. To search for a specific name, select **Last Name** from the **Column** drop-down menu, enter a last name in the **Search** field, and then click the button. (You can also search by a user ID or first name.)

3 Click the user ID of the user you want to delete. The User's information is displayed.




4 Click **Delete User**.

5 In the confirmation dialog box, click **OK**.

# Chapter 7
# Setting Up Custom Security Groups for New Hire Checklists

The ADP Workforce Now™ New Hire feature allows portal administrators to create custom checklists to track new hire tasks, such as ordering a computer. Checklists are organized by the employees who will complete the tasks. For example, a checklist can be sent to a technical support employee who sets up phone service and an Internet connection. A checklist can also be sent to a manager who provides training manuals to a new hire and reviews corporate policy guidelines with this person.

In order to access checklists and complete assigned tasks, employees must be assigned to the Employee Checklists custom security group. Managers must be assigned to the Manager Checklists custom security group. These groups need to be set up.

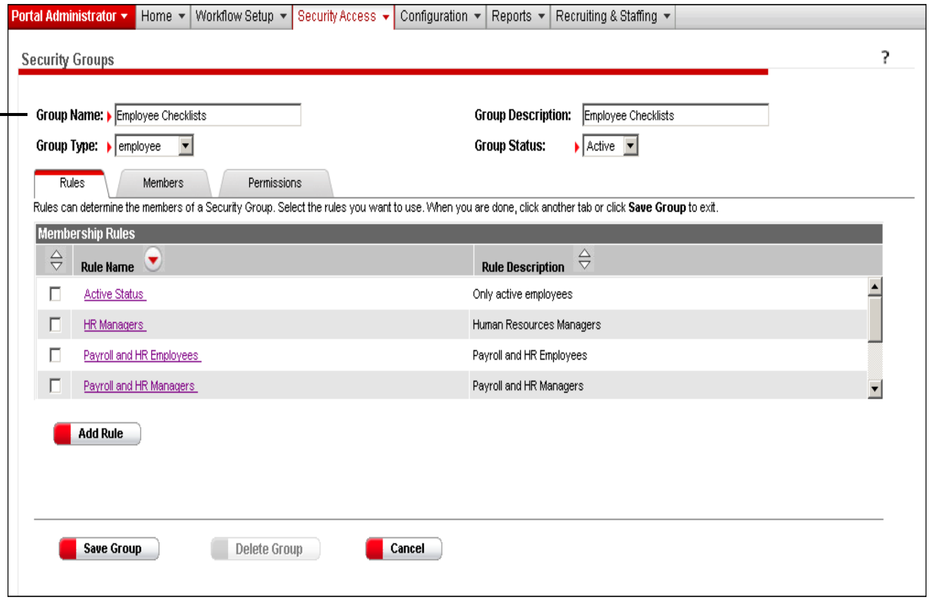
As a security master, you were also set up as a portal administrator during the initial planning phase. Portal administrators are responsible for setting up security groups to control user access to features in ADP Workforce Now.

**Important:** The Employee Checklists and Manager Checklists custom security groups must be created using these exact names. Permissions for each group must be assigned carefully to ensure that members of these groups see only what they are supposed to.

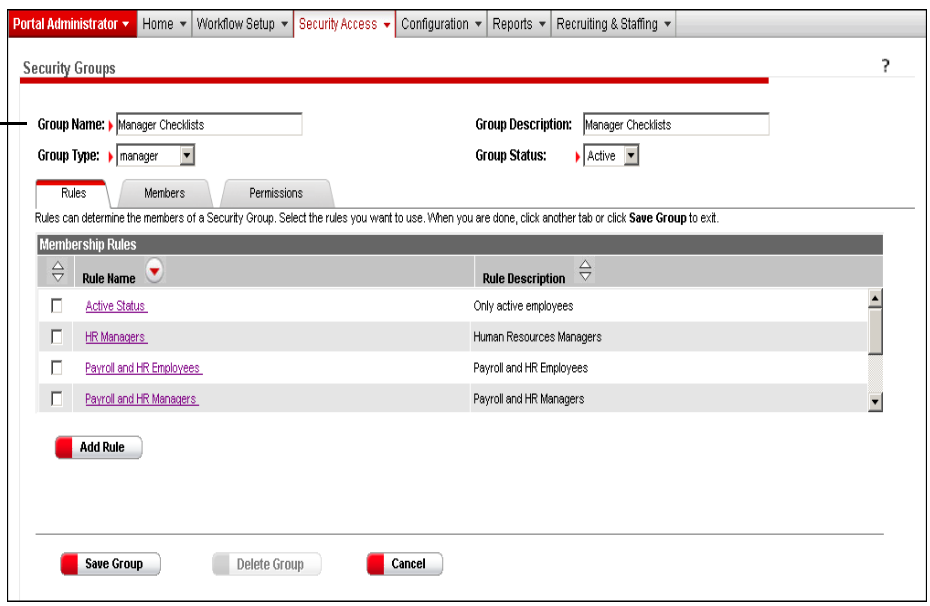
## Naming the Employee and Manager Groups

When setting up the Employee Checklists and Manager Checklists custom security groups, name the groups exactly as shown in the screen shots that follow. You must capitalize the first letter of both words and include one space between Employee/Manager and Checklists.

Employee Checklists group




Manager Checklists group




**Note:** Detailed instructions on setting up custom security groups are provided in Chapter 3: "Setting User Access in ADP Workforce Now" on page 57.

# Assigning Permissions to the Employee and Manager Groups

When setting up the Employee Checklists and Manager Checklists custom security groups, you need to assign permissions carefully.

**Important:** Make sure that members whom you add to the Employee Checklists and Manager Checklists custom security groups keep the same permissions that were assigned to them in other security groups to which they belong. You do not want to expose the users to content they should not see. You do not want to remove existing permissions, either.

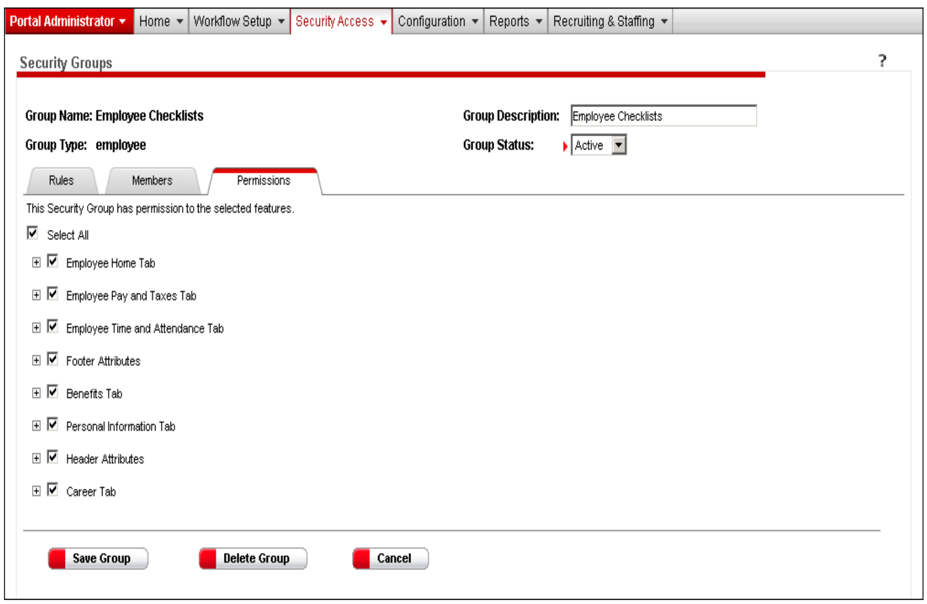
## Example 1: When to Maintain Default Security Group Permissions

If all members of the Employee Checklists or Manager Checklists custom security group that you are setting up are being pulled from a default security group of the same employee type, assign the same permissions as this default group.

For example, all the members that you assign to the Employee Checklists group are now inactive in the default employee security group. These members will not be able to view the options selected for the default group unless you select the same options for the Employee Checklists group.

On the **Permissions** tab, assign the same permissions as the default security group.

In this example, the permissions that are selected for the Employee Checklists custom security group are the same ones selected for the default employee security group.



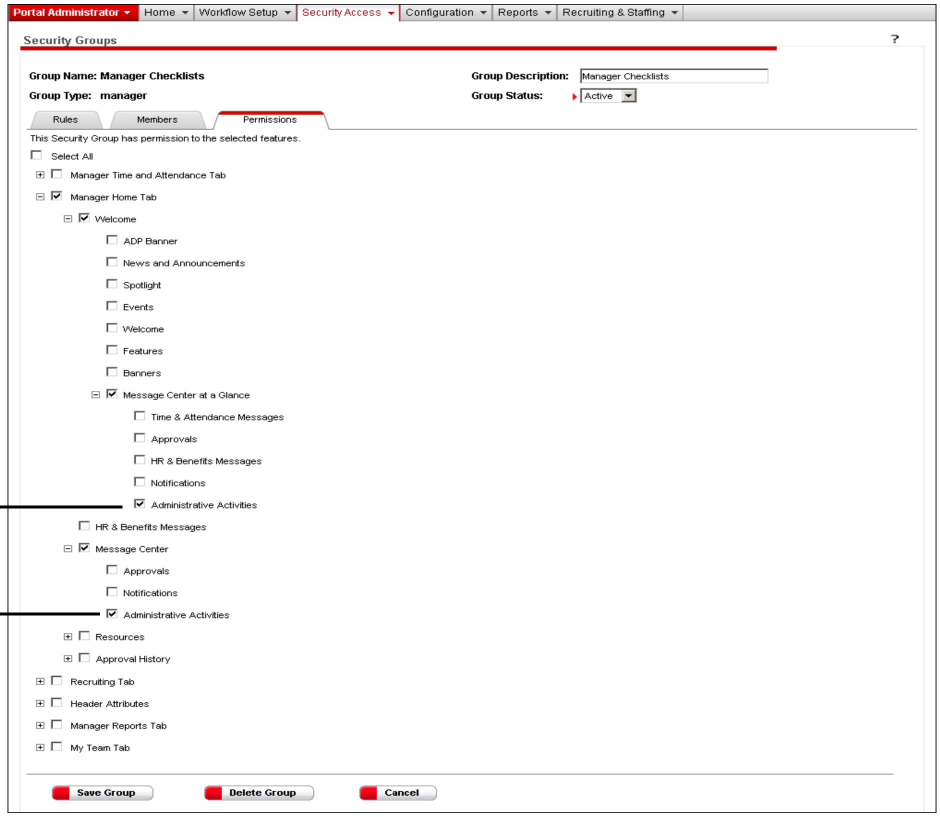

**Important:** The permissions selected should include the Administrative Activities options that allow users to receive new hire checklists. The screen shot in Example 2 shows where these options are selected.

## Example 2: When to Assign Only the Administrative Activities Options

If members of the Employee Checklists or Manager Checklists custom security group that you are setting up belong to different security groups of the same employee type, only select the Administrative Activities options. These options allow the members to receive new hire checklists that are assigned to them, but they do not change what the individual members currently see and do on the site.

For example, some members that you assign to the Manager Checklists custom security group were active users in the default manager security group. Other members belong to more than one custom manager security group. Because these members belong to different security groups, they have access to different areas in ADP Workforce Now. You do not want to change these individual rights.

On the **Permissions** tab, only select the two Administrative Activities options.




Click to select **Administrative Activities** under **Message Center at a Glance**.

Click to select **Administrative Activities** under **Message Center**.

Click to clear all other permissions.

**Note:** Detailed instructions on setting up custom security groups are provided in Chapter 3: “Setting User Access in ADP Workforce Now” on page 57.

# Appendix A: Selecting Membership Rule Attributes and Values

When adding or changing a membership rule, you will need to select the correct membership rule attributes and enter the correct values on the Membership Rules page. The following tables provide information for selecting membership rule attributes and values based on fields and values in your ADP Workforce Now® modules.

The attributes and values you select when adding or changing membership rules depend on the combination of modules your company is using. Tables 1, 2, and 3 provide membership rule attributes and values, and the corresponding system of record fields and values, for each module.

To find attributes and values, locate the combination of modules your company is using below. Reference the tables listed for your module combination to determine the membership rule attributes and values you should use.

| If you have… | Use… |
|---|---|
| Payroll module, HR & Benefits module, and Time & Attendance module | Table 2, HR & Benefits Module and<br>Table 3, Time & Attendance Module |
| Payroll module and HR & Benefits module | Table 2, HR & Benefits Module |
| Payroll module and Time & Attendance module | Table 1, Payroll Module and<br>Table 3, Time & Attendance Module |
| Payroll module | Table 1, Payroll Module |

## Table 1. Payroll Module

| Membership Rule Attribute | Payroll Module Field | Payroll Module Value(s) | Membership Rule Value(s) | Notes |
|---|---|---|---|---|
| EEOC Job Classification Code | Statutory Compliance ▸ VETS / EEO | • Executive/Senior Level Officials and Managers<br>• First/Mid-Level Officials and Managers<br>• Professionals<br>• Technicians<br>• Sales Workers<br>• Administrative Support Workers<br>• Craft Workers<br>• Operatives<br>• Laborers and Helpers<br>• Service Workers | • 1.1<br>• 1.2<br>• 2<br>• 3<br>• 4<br>• 5<br>• 6<br>• 7<br>• 8<br>• 9 | Attribute is valid only if HR functionality is turned on in the Payroll module. |
| Compensation Manager | — | — | — | Attribute not used. |
| Location | Employee ▸ Position ▸ Position ▸ Location | Client-defined | Client-defined | Membership rule values should match the client-defined values in the module. |
| Time and Attendance Supervisor | — | — | — | Attribute not used. |
| Payroll Standard Hours | Employee ▸ Pay Rates ▸ Current Rates ▸ Standard Hours | Client-defined | Client-defined | Membership rule values should match the client-defined values in the module. |

| | | | | |
|---|---|---|---|---|
| Pay Group/ Company Code | None | Assigned by ADP, Inc. | Company code assigned by ADP, Inc. | Company Code is created and assigned when your company is set up. |
| Department | Employee ▸ Position ▸ Position ▸ Home Department ▸ Code | Client-defined | Client-defined | In the Payroll module, click the plus sign (+) on the **Home Department** field to display the **Code** field. |
| Employment Rate Type | Employee ▸ Pay Rates ▸ Current Rates ▸ Rate | • Hourly<br>• Salary<br>• Daily | • Hourly<br>• Salaried<br>• Daily | |
| Employment Status | Employee ▸ Position ▸ Status ▸ Current Status | • Active<br>• Terminated<br>• Leave<br>• Deceased | • Active<br>• Terminated<br>• Leave of Absence<br>• Deceased | |
| FLSA Status | Employee ▸ Position ▸ Position ▸ FLSA | Client-defined | Client-defined | Membership rule values should match the client-defined values in the module. |
| Shift | Employee ▸ Position ▸ Position ▸ Assigned Shift | Client-defined | Client-defined | Membership rule values should match the client-defined values in the module. |
| Performance Manager | — | — | — | Attribute not used. |
| Regular or Temporary | Employee ▸ Position ▸ Position ▸ Employee Type | CONS<br>CONT<br>COOP<br>TEMP<br>Client-defined | TEMP<br>TEMP<br>TEMP<br>TEMP<br>Client-defined | If client-defined values are used, the membership rule value should match the client-defined value. |
| Standard Hours | — | — | — | Attribute not used. |

| | | | | |
|---|---|---|---|---|
| Bargaining Unit | Employee ▸ Position ▸ Position ▸ Union Code | Client-defined | Client-defined | Membership rule values should match the client-defined values in the module. |
| Full or Part Time | Employee ▸ Position ▸ Position ▸ Employee Type | • FTR<br>• PTR<br>• Client-defined | • FTR<br>• PTR<br>• Client-defined | The **Full or Part Time** attribute and values are applicable only if **FTR** or **PTR** is selected in the **Employee Type** field in the Payroll module.<br>If client-defined values are used, the membership rule value should match the client-defined value. |
| Job Code | Employee ▸ Position ▸ Position ▸ Job Title ▸ Code | Client-defined | Client-defined | In the Payroll module, click the plus sign (+) on the **Job Title** field to display the **Code** field.<br>Membership rule values should match the client-defined values in the module. |
| Manager | Employee ▸ Position ▸ Position ▸ **This is a supervisor position** check box | Check box is selected | Manager | |

| | | | | |
|---|---|---|---|---|
| Time and Attendance Employee | — | — | — | Attribute not used. |
| Hire Date | Employee ▸ Position ▸ Status ▸ Hire Date | Client-defined | Client-defined | Membership rule values should match the client-defined values in the module. |

## Table 2. HR & Benefits Module

| Membership Rule Attribute | HR & Benefits Module Field | HR & Benefits Module Value(s) | Membership Rule Value(s) | Notes |
|---|---|---|---|---|
| EEOC Job Classification Code | — | — | — | Attribute not used. |
| Compensation Manager | — | — | — | Attribute not used. |
| Location | Company ▸ Corporate Groups ▸ **Structure** drop-down list ▸ Location ▸ Add/Edit ▸ Location Name<br><br>Company ▸ Corporate Groups ▸ **Structure** drop-down list ▸ Location ▸ Add/Edit ▸ Auxiliary 1<br>Auxiliary 2<br>Auxiliary 3<br>Auxiliary 4<br>Auxiliary 5 | Client-defined | Client-defined | Depending on how your company is set up, you can establish rules based on the **Location Name** field or the **Auxiliary** field, but not both. See the **Location Code** field in the Integration Profile (Integration ▸ Integration Profile).<br>Membership rule values should match the client-defined values in the module. |
| Time and Attendance Supervisor | — | — | — | Attribute not used. |
| Payroll Standard Hours | Employee ▸ Earnings ▸ edit/ view ▸ Hours per Week | Client-defined | Client-defined | Membership rule values should match the client-defined values in the module. |

| | | | | |
|---|---|---|---|---|
| Pay Group / Company Code | Company ▸ Corporate Groups ▸ **Structure** drop-down list ▸ Pay Group | Assigned by ADP, Inc. | Company code assigned by ADP, Inc. | The Company code is created and assigned when your company pay groups are set up.<br>The Company code is the second, third, and fourth characters in the Pay Group Name. |
| Department | Company ▸ Corporate Groups ▸ **Structure** drop-down list ▸ Department ▸ Add/Edit ▸ Department Name<br><br>Company ▸ Corporate Groups ▸ **Structure** drop-down list ▸ Department ▸ Add/Edit ▸ Auxiliary 1<br>Auxiliary 2<br>Auxiliary 3<br>Auxiliary 4<br>Auxiliary 5 | Client-defined | Client-defined | Depending on how your company is set up, you can establish rules based on the **Department Name** field or the **Auxiliary** field, but not both. See the **Home Department** field in the Integration Profile (Integration ▸ Integration Profile).<br>Membership rule values should match the client-defined values in the module. |
| Employment Rate Type | Employee ▸ Earnings ▸ edit/view ▸ per | • Hour<br>• Week<br>• Two Weeks<br>• Half Month<br>• Month<br>• Quarter<br>• Year | • Hourly<br>• Salaried<br>• Salaried<br>• Salaried<br>• Salaried<br>• Salaried<br>• Salaried | |

| | | | | |
|---|---|---|---|---|
| Employment Status | Employee ▸ Status ▸ Status Today | • Active<br>• Terminate<br>• Retire<br>• Place on Leave<br>• Deceased (Client-defined) | • Active<br>• Terminated<br>• Retired<br>• Leave of Absence<br>• Deceased (Client-defined) | Search for an employee in the Employee Management Center, and then select **Status**. Click **edit** to display **Status Today**.<br>Employee Status is Active by default when employees are added in the HR & Benefits module.<br>Define the Deceased value in Company ▸ EE Status. Select **Terminated** in the **Type** field and add the value. The value must be Deceased for a membership rule to work.<br>If managers are on leave, terminated, retired, or deceased, they are removed from the manager role, so rules based on these values will not apply. |
| FLSA Status | HR ▸ Jobs ▸ FLSA Code | • Exempt<br>• Non-exempt | • Exempt<br>• Non-exempt | Select a job from the Job Table and click edit or view to display the **FLSA Code** field. |

| | | | | |
|---|---|---|---|---|
| Shift | Company ▸ Custom Fields | Client-defined | Client-defined | A custom field can be defined in the Company ▸ Custom Fields tab.<br>Depending on how your company is set up, you can establish rules based on the **Assigned Shift** field. See the **Assigned Shift** field in the Integration Profile (Integration ▸ Integration Profile).<br>Membership rule values should match the client-defined values in the module. |
| Performance Manager | — | — | — | Attribute not used. |
| Regular or Temporary | — | — | — | Attribute not used. |
| Standard Hours | — | — | — | Attribute not used. |
| Bargaining Unit | — | — | — | Attribute not used. |
| Full or Part Time | — | — | — | Attribute not used. |

| | | | | |
|---|---|---|---|---|
| Job Code | HR ▸ Jobs ▸ Job Code<br><br>HR ▸ Job Title ▸ Name | Client-defined | Client-defined | Depending on how your company is set up, you can establish rules based on job codes or job names, but not both. See the **Job Code** field in the Integration Profile (Integration ▸ Integration Profile).<br><br>Job codes and job names are assigned by the client when adding jobs on the Add Job Title page.<br><br>Membership rule values should match the client-defined values in the module. |
| Manager | HR ▸ Jobs ▸ Management Position? | **Yes** radio button is selected | Manager | The **Management Position?** field displays on the Add Job Title page or Edit Job Title page after selecting a management position from the Job Table and clicking **Add** or **Edit**. |
| Time and Attendance Employee | — | — | — | Attribute not used. |
| Hire Date | Employee ▸ Work ▸ edit/view ▸ Date of Hire/Rehire | Client-defined | Client-defined | Membership rule values should match the client-defined values in the module. |

## Table 3. Time & Attendance Module

| Membership Rule Attribute | Time & Attendance Module Field | Time & Attendance Module Value(s) | Membership Rule Value(s) | Notes |
|---|---|---|---|---|
| EEOC Job Classification Code | — | — | — | Attribute not used. |
| Compensation Manager | — | — | — | |
| Location | — | — | — | Attribute not used. |
| Time and Attendance Supervisor | Employee ▸ Supervisor Flag ▸ **Is Supervisor** check box | Check box is selected | Y for employees who are managers or supervisors<br>N for employees who are not managers or supervisors | |
| Payroll Standard Hours | — | — | — | Attribute not used. |
| Pay Group / Company Code | — | — | — | Attribute not used. |
| Department | Maintenance ▸ Employees ▸ Main ▸ Department | Client-defined | Client-defined | Membership rule values should match the client-defined values in the module. |
| Employment Rate Type | — | — | — | Attribute not used. |
| Employment Status | Maintenance ▸ Employees ▸ Status<br>Terminated Employees ▸ Status | **Employee is Active** is selected<br>**Employee is Inactive** is selected<br>**Employee Scheduled for Termination** is selected | Active<br>Leave of Absence<br>Terminated | |
| FLSA Status | — | — | — | Attribute not used. |

| | | | | |
|---|---|---|---|---|
| Shift | — | — | — | Attribute not used. |
| Performance Manager | — | — | — | |
| Regular or Temporary | — | — | — | Attribute not used. |
| Standard Hours | — | — | — | |
| Bargaining Unit | — | — | — | |
| Full or Part Time | — | — | — | Attribute not used. |
| Job Code | Maintenance ▸ Employees ▸ Main ▸ Job | Client-defined | Client-defined | The **Job** field in the Time and Attendance module may or may not display depending on how your company was set up.<br>Membership rule values should match the client-defined values in the module. |
| Manager | — | — | — | Attribute not used. |
| Time and Attendance Employee | None. | None. | Y for active employees<br>N for terminated employees | |
| Hire Date | — | — | — | Attribute not used. |