Evolution® HCM
by ASURE SOFTWARE

Security Guide

Advanced HR 2.0

ASURE SOFTWARE

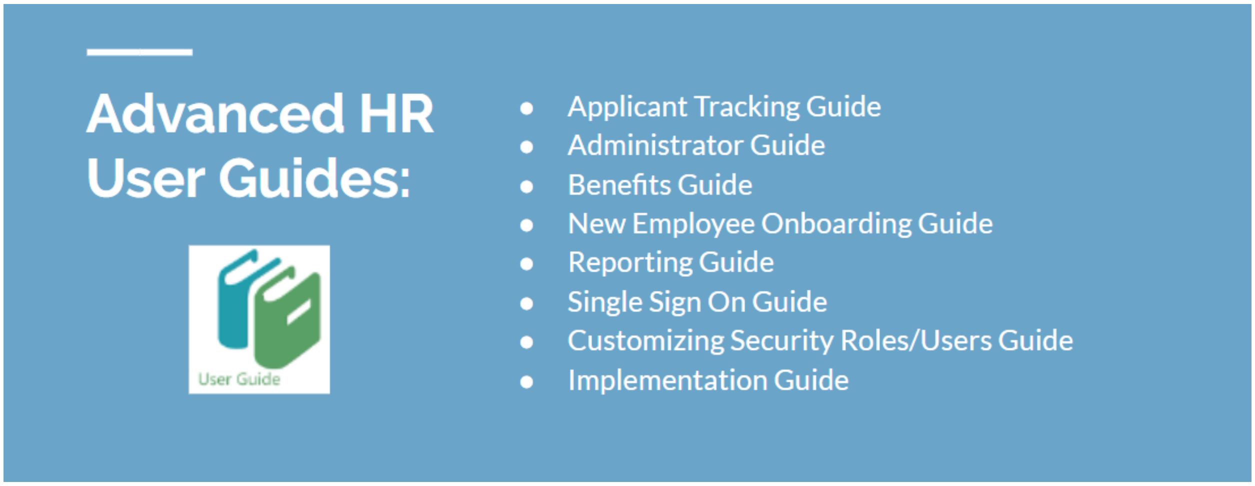
CONTENTS

Document Revision History

Doc Version	Software Version	Date	Description
1.0	2.0	9/21/2017	DRAFT in progress
1.1	2.0	9/27/2017	Two additional roles added: Base Admin Read Only and Base Applicant Tracking / Onboarding.
1.2	2.0	9/28/2017	Removed Quick Links from Base Manager role.
1.3	2.0	10/27/2017	Added security step for company onboarding for SB Admin role.
1.4	2.0	11/27/2017	Minor edits to the Resources / Permissions and other sections.
1.5	2.0	1/12/2018	Added a note about the precedence order of a customized security role.

Audience and Additional Advanced HR 2.0 Documentation

The intended audience for this guide is Service Bureau administrators and managers. It contains information about how to set up, assign, and maintain security roles in Advanced HR 2.0. The following is a list of the other Advanced HR 2.0 User Guides; all are available for download on the Evolution Resource Center:



Advanced HR User Guides:

- Applicant Tracking Guide
- Administrator Guide
- Benefits Guide
- New Employee Onboarding Guide
- Reporting Guide
- Single Sign On Guide
- Customizing Security Roles/Users Guide
- Implementation Guide

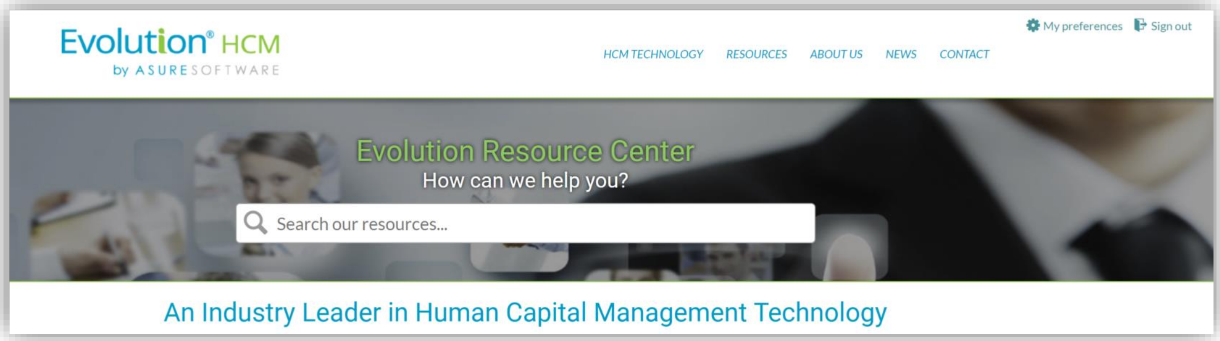
Employee end users should refer to the separate document *Getting Started: Employee End User Guide* which describes Advanced HR 2.0 from the employee user point of view.

Evolution Resource Center

You can go to the Evolution Resource Center at https://support.evolutionhcm.com to view the latest Advanced HR 2.0:

- Training Guides
- User Manuals
- Instructional Videos
- Implementation Center materials

Your comments are important to us. You can now enter your feedback directly online for any specific articles/topics in the **Evolution Resource Center**. We encourage you to tell us what you like, or what you would like changed about Evolution documentation and training materials. We are committed to continually improving our product documentation for you.


Evolution® HCM by ASURESOFTWARE
My preferences
Sign out
HCM TECHNOLOGY
RESOURCES
ABOUT US
NEWS
CONTACT
Evolution Resource Center
How can we help you?
Search our resources...
An Industry Leader in Human Capital Management Technology

Evolution Resource Center

You can also:

Email our Support Department for questions:

support@evolutionhcm.com or by calling 802-655-8347

Email our Training Department to schedule a training:

Training@evolutionhcm.com

Email our Implementations Team:

AHR_implementations@asuresoftware.com

Advanced HR 2.0 Security Guide

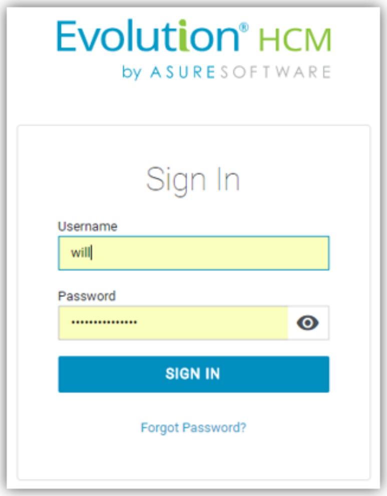
Welcome to your Advanced HR 2.0 Security Guide! This Security Guide discusses the following topics:

- A general overview of security in Advanced HR 2.0
- Assigning a security level to a user
- Cloning (copying) a security role
- Excluding a company from a user
- Associating a user to another company
- Creating an employee record filtering rule for a role

Importance: Security is an critical issue as the different security roles in Advanced HR 2.0 determine how the user interacts with the system – what they can do and see and what they cannot do. For example, an administrator requires different functionality than an end user.

Single Sign On (SSO) Feature

Note that the Single Sign On (SSO) feature will allow for users to login to a central location and access both Advanced HR 2.0 and Evolution Payroll, without the need to enter their User Credentials multiple times. When accessed, the selected product will open in a new tab in your browser. Once Single Sign On is turned on, it is on for all users in the Service Bureau. Users will login with their Evolution Username and password.



Username: will

Password: ••••••••••••••••

- Provides access to two systems.
- New login screen.
- Requires pre-work to be enabled.
- Requires the Service Bureau be using the Stowe version of Evolution Classic.
- Email addresses for users are required.

As we continue to update the Evolution product lines, Single Sign On will be rolled out for different products in the future. As with many updates to functionality, it does require some pre-work before it can be utilized. Note that Evolution Classic must be upgraded to the latest “Stowe” version.

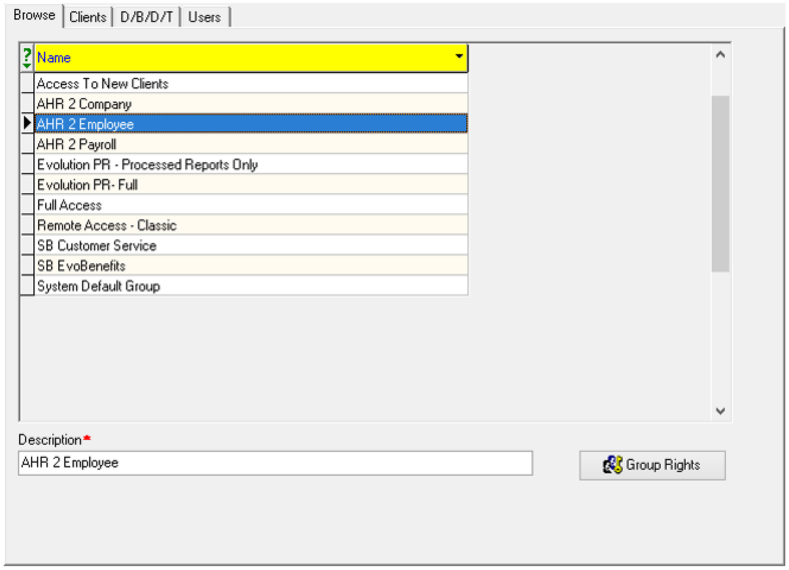
As part of the Evolution Classic preparation, three **AHR 2 Security Groups** (shown at right) must be set up. These security groups are required to ensure that the proper Payroll Rights are assigned to those users who need access to Payroll data.

You create the **AHR 2 Security Groups** in Evolution Classic by going to **Admin – Security – Groups** – the **Browse** tab. Enter the name of the security groups exactly as shown.

AHR 2 Security Templates

The AHR 2 Security templates that have been added to Evolution Classic are the following:

- AHR 2 Company
- AHR 2 Employee
- AHR 2 Payroll



Name
Access To New Clients
AHR 2 Company
AHR 2 Employee
AHR 2 Payroll
Evolution PR - Processed Reports Only
Evolution PR- Full
Full Access
Remote Access - Classic
SB Customer Service
SB EvoBenefits
System Default Group

Description*: AHR 2 Employee

User Email Addresses

Very Important:

Unique **User Email addresses** are required for all users when Single Sign On is activated. These will become the Usernames for the employees in Advanced HR 2.0. Go to **Employee – Employee - Self Serve** tab. In the **Settings** pane, enter the email address.

The employee email addresses should be entered into Evolution Classic **prior to** the Payroll Data Cutover. This can be done using EvoExchange. If the email address is not added prior to the Payroll Cutover, users will have to manually populate the email prior to enabling the Employee for Self Service.

In addition, **E/D codes** in Evolution Classic must be set to **Show in EE Portal**.

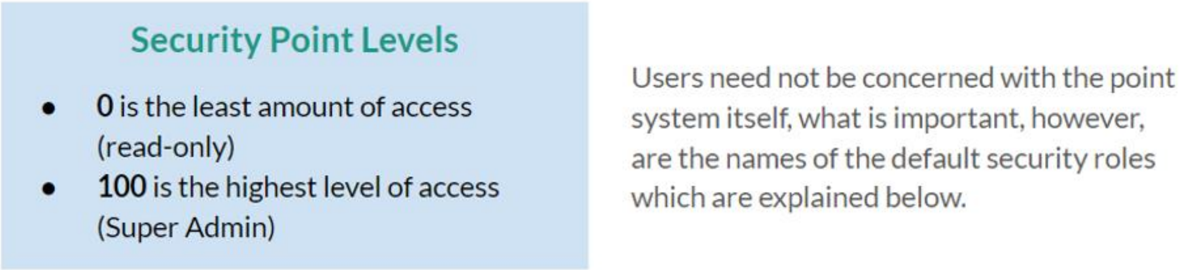
- Must be enabled on the E/Ds that will be used in Self Service.
- Go to **Company – General - E/Ds - Details** tab. In the **E/D Details** pane, click the option to **Yes**.

Note: Evolution Classic must be upgraded to the latest version, which is "Stowe." When a service bureau is ready, they should contact Support to create a non-billable case for activation.

Refer to the *AHR 2.0 Implementation Guide* (available for download on the **Evolution Resource Center**) for more information about the setup steps your Service Bureau will need to do to get ready for Advanced HR 2.0, including the steps for Single Sign On.

Security Roles Overview

Security in Advanced HR 2.0 is maintained at the Service Bureau level. The system has sophisticated security setting capabilities that allow for unique user access. Behind the scenes, the Security Level settings, known as *roles*, are based on a **0 - 100 point system** as shown below.



Security Point Levels

- 0 is the least amount of access (read-only)
- 100 is the highest level of access (Super Admin)

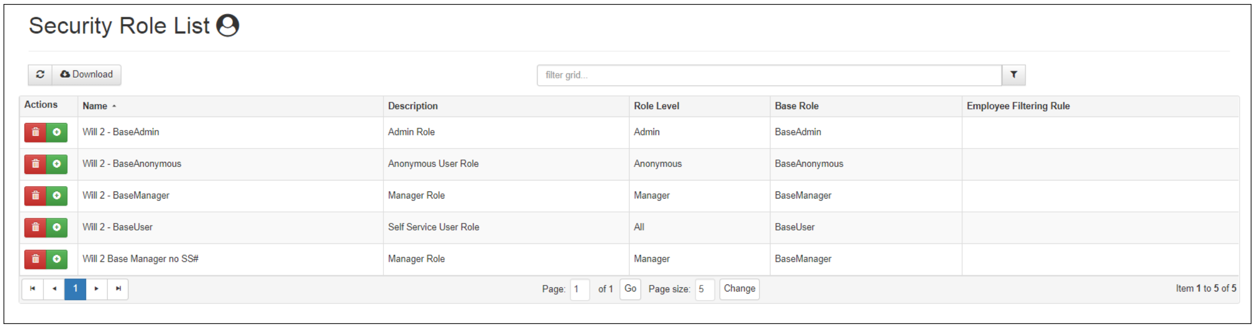
Users need not be concerned with the point system itself, what is important, however, are the names of the default security roles which are explained below.

Default Security Roles

During the initial conversion or subsequent onboarding process (the Payroll Data Cutover), each employee is set up as a user in Advanced HR 2.0 with their unique username (email) and a Security Role level for Dashboard (ESS) access.

By default, after the Payroll Cutover, a newly onboarded company in Advanced HR 2.0 is given the security roles shown in the screenshot below and listed in the following table.

Note that the final role on the following screen is a customized role not one of the default roles; more about customizing a role later in this guide.



Security Role List

Actions	Name	Description	Role Level	Base Role	Employee Filtering Rule
	Will 2 - BaseAdmin	Admin Role	Admin	BaseAdmin	
	Will 2 - BaseAnonymous	Anonymous User Role	Anonymous	BaseAnonymous	
	Will 2 - BaseManager	Manager Role	Manager	BaseManager	
	Will 2 - BaseUser	Self Service User Role	All	BaseUser	
	Will 2 Base Manager no SS#	Manager Role	Manager	BaseManager	

The following tables list these default security roles.

End User Default Security Roles

The roles listed below are for the front end user (the Service Bureau clients) to use. The user's role determines what they can or cannot do or see in the system.

Security Role Name	Notes
Base Anonymous	For Self-Service Onboarding – This role is a read-only role with no actual functionality.
Base User	Access to the **My HR** tab only. Every employee should be assigned the **Base User** role so that they can access their **My HR** tab.
Base Manager	Access to the **Manager Service** tab.
Base Admin	Access to **HR Admin** tab and **Quick Links** tab.

Service Bureau Default Security Roles

There are also other security roles intended for the Service Bureau level and not for your clients:

Security Role Name	Notes
Service Bureau (SB) Admin	Access to the **HR Admin** tab with partial Security Setting access, and the **Quick Links** tab. • Service Bureau Admins will have companies assigned to them to access. • They typically are not employees of a company.
Super Admin	Access to **HR Admin** tab with full Security Access, and the **Quick Links** tab. • This role level can see all companies that have been cutover from the service bureau's account. • Has access to all the clients that are associated with an account

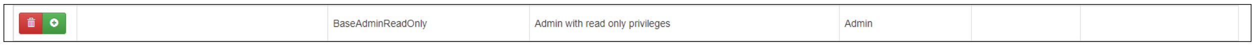
Super Admin and **SB Admin** roles have access to setting up and assigning security roles, as well as access to other high level functionality.

Important Note: Do not change/edit these Base Roles. You will instead want to clone or copy the base roles and make them specific for each company – instructions to do this are provided later in this guide.

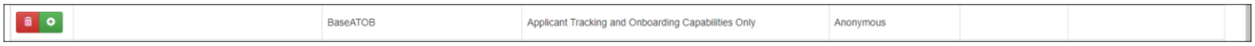
If a user is assigned multiple security roles, they would have access to the components of those roles. For example, if a user was a **Base User** and a **Base Manager**, they would have access to the **My HR** and **Manager Service** tabs (all the components of the Base Manager role).

Additional Security Roles

Security Role Name	Notes
Base Admin Read-Only	A Base Admin role with Read Only access (**BaseAdminReadOnly**). For example, to give to executives read access but not the ability to change/add records.
Base Applicant Tracking Onboarding	A Base role for use by recruiters (**BaseATOB**).



🗑 ⊕		BaseAdminReadOnly	Admin with read only privileges	Admin		

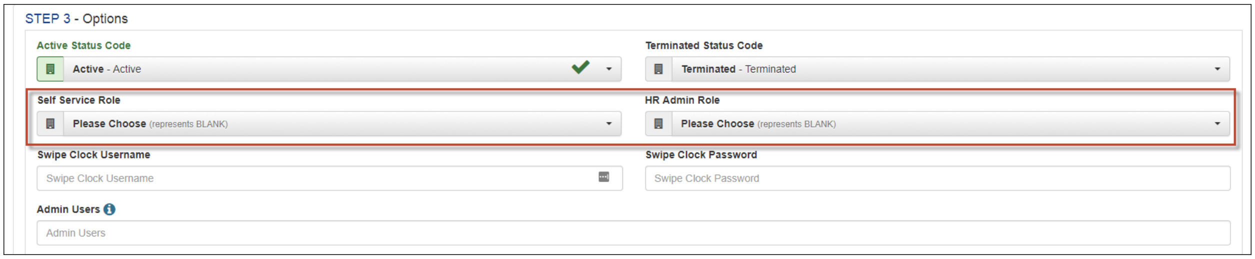


🗑 ⊕		BaseATOB	Applicant Tracking and Onboarding Capabilities Only	Anonymous		

Tip: We recommend that all users be assigned a **Base User** level role when initial onboarding occurs. This role will enable them to see their **My HR** tab. This menu tab contains employee-specific information, such as documents and contact information. It's important to note that managers and administrators will also have added security settings that are appropriate for their jobs.

Specifying Roles at Payroll Data Cutover Process

When a company is first onboarded, you optionally have the opportunity to select which base role that you want to use as a template for the **Base User (Self Service)** role, and the **Base Admin** role. The default roles that are part of the Payroll Cutover are generally meant for the end user.



STEP 3 - Options

Active Status Code: Active - Active ✓

Terminated Status Code: Terminated - Terminated

Self Service Role: Please Choose (represents BLANK)

HR Admin Role: Please Choose (represents BLANK)

Swipe Clock Username: Swipe Clock Username

Swipe Clock Password: Swipe Clock Password

Admin Users: Admin Users

The system will also create the **Anonymous** role and the **Base Manager** role at the same time (but you do not select actually these roles at the Payroll Cutover). The dropdown list of available roles includes *all roles that are not specifically assigned to a company*. This is intended to facilitate having multiple base roles for specific purposes – for example, "BaseAdmin – No Compensation" or "BaseManager – No SSN or Birthdates."

No-Company Roles

It's also important to understand, however, that users with access to multiple companies must also have *no-company roles* in order to have the menus/permissions available for them when they are NOT locked in to one of the companies to which they are linked. You can then clone the base roles which become new roles specifically for that company. Refer to Cloning a Role that is not associated with a company.

Security Role Notes

It's important to note the following additional security role related points:

- Any user *below* a Service Bureau Admin must be *associated (linked) to the company*, or companies, they can access.
- Further, in order to have any permissions, each user must be *assigned to a role*.
  - If the role is associated with a specific company, then those are the permissions the user will be entitled to when locked into that company.
  - If the role does *not* have a company specified, then they will have those permissions whether or not they locked into a company.
- Users *below* a Service Bureau Admin level can only access roles associated to the companies to which they have access, nor can they access roles that do not have companies specified – so those special "cross company" users must be set up by Service Bureau Admin level users.

During the initial conversion or subsequent onboarding process, each employee is set up as a user with their unique username (email) and a security role for that company (typically the ESS role).

Note: Roles need to be assigned to a company *before* they can be assigned to users by anyone below a Service Bureau level user (so an HR Admin can only assign roles associated with the companies to which he/she has access). Further, *no user can assign a role with a role level greater than their own role*.

A **Super Admin** or **SB Admin** should do this as part of the company onboarding process. Go to **HR Admin – Maintenance - Roles**. Using the Clone feature, you will copy a Role. Give the "cloned" Role a name that is specific to the company. For more information on how to assign roles to a company, refer to Cloning a Security Role in this document.

Let's look at the functionality of each of the default security levels as they come "out of the box."

Anonymous - Read Only Role

Note that the first default security level (**Anonymous**) is for someone who is unknown to the system – who has no security level access set. This could be an applicant who is filling out an onboarding application or someone who isn't assigned a role in general.

Users that are not logged in are anonymous users – and thus can only see the pages that do not require logging in – specifically the application and onboarding sections of Advanced HR 2.0.

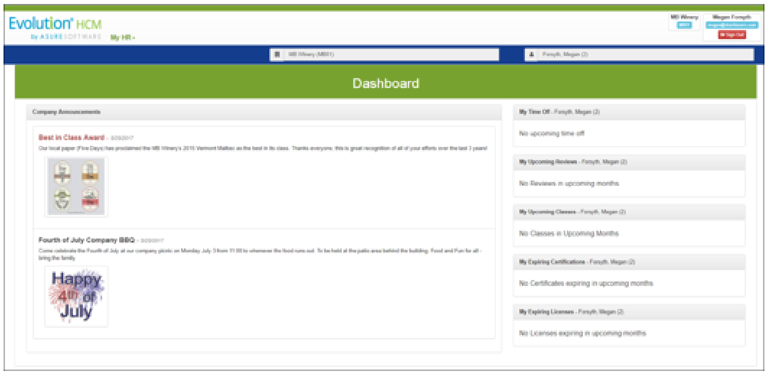
Permissions are assigned to the anonymous user role to suppress visibility or make fields required by applicants or onboarding candidates.

Base User Role

The **Base User** role is what every user should be set to. Remember that managers and administrators will also have added security settings that are appropriate for their jobs as part of their roles.

When a Base User logs in, they will be taken to the Dashboard. The Dashboard will display:

- **My HR** menu tab
- Company Announcements
- Upcoming Reviews
- Expiring Certifications and Licenses



MB Winery (MB01)

Forsyth, Megan (2)

Dashboard

Company Announcements

Best in Class Award

Our local paper (Five Days) has proclaimed the MB Winery's 2016 Vermont Malbec as the best in its class. Thanks everyone, this is great recognition of all of your efforts over the last 3 years!

Fourth of July Company BBQ

Come celebrate the Fourth of July at our company picnic on Monday, July 3 from 11:00 to whenever the food runs out. To be held at the patio area behind the building. Food and Fun for all - bring the family

My Time Off - Forsyth, Megan (2)

No upcoming time off

My Upcoming Reviews - Forsyth, Megan (2)

No Reviews in upcoming months

My Upcoming Classes - Forsyth, Megan (2)

No Classes in Upcoming Months

My Expiring Certifications - Forsyth, Megan (2)

No Certificates expiring in upcoming months

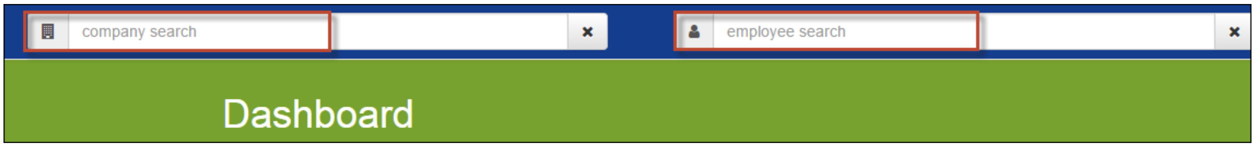
My Expiring Licenses - Forsyth, Megan (2)

No Licenses expiring in upcoming months

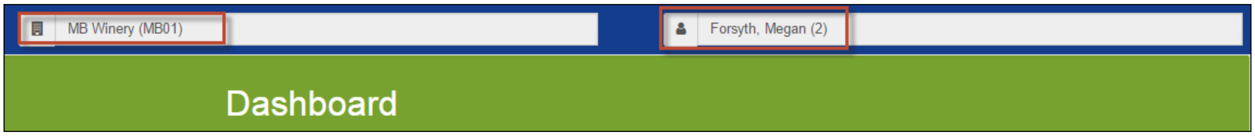
Note: For a Base User, the Dashboard will only display their own information

For an example of a Base User role, Megan Forsyth is a self service employee of the MB Winery company. She has been assigned the **Base User** security role. When a user who has been assigned a Base User role signs in to Advanced HR 2.0, they are taken to the **Dashboard**. An example is shown below. The Dashboard is really the Employee Self Serve (ESS) or the portal.

Note the **company search** and **employee search** fields just above the **Dashboard** at the top of the screen.

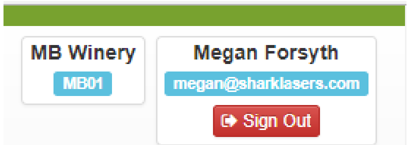


In the following example, these fields show that Megan is assigned to the MB Winery company (MB01).


MB Winery (MB01)

Forsyth, Megan (2)

Her name and the company name display at the top right of the screen, above the **Sign Out** button which is used to log out of Advanced HR 2.0.


MB Winery

MB01

Megan Forsyth

megan@sharklasers.com

Administrators can change the Dashboard settings for employees by going to **HR Admin – Company – Home Dashboard Setup**. Use the **Yes/No** toggles to select the Dashboard display settings. Set the **Review Period** settings as well. Click **Save Changes** when complete. See the *Home Dashboard Setup* section of the *Advanced HR 2.0 Administrator Guide* for more information about how to set up the Dashboard for employees.

Note: You will need to assign multiple roles to Managers and Administrators; for example, Base Admin and Base User or Base Manager and Base User. Permissions can be adjusted to allow managers or administrators to access and update their own employee records, negating the need to assign them to an ESS role. It's important to note that by default, they cannot access their own data.

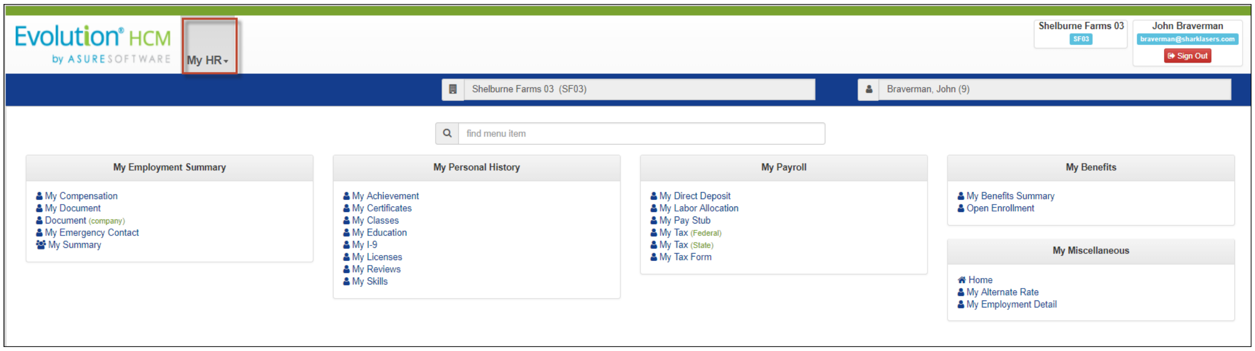
My HR for a Base User

The **My HR** menu tab is equivalent to Employee Self Service or the Employee Portal. Every employee should have this role assigned to them so that they can access their **My HR** tab.

When a Base User accesses their **My HR** menu, they can see their own information in separate tiles or panes as it pertains to:

- My Employment Summary
- My Personal History
- My Payroll (Direct Deposit and tax records)
- My Miscellaneous items (Alternate rates of pay, any applicable veterans information)

Note: It's important to note that the only way any user in Advanced HR 2.0 can have access to their **My HR** tab is if they have the **Base User** role assigned to them. This includes managers and admins – they must also have the Base User role in addition to their Manager or Admin role.



What Information Can a Base User See?

It's important to note that the *only* information that a Base User is able to see is their own. In Advanced HR 2.0, **My HR** is equivalent to the Employee Portal (also known as The Port in Version 1.0). It's also important to note that *most* of the screens in **My HR** are read only to the Base User.

The only screens that the Base User can edit are:

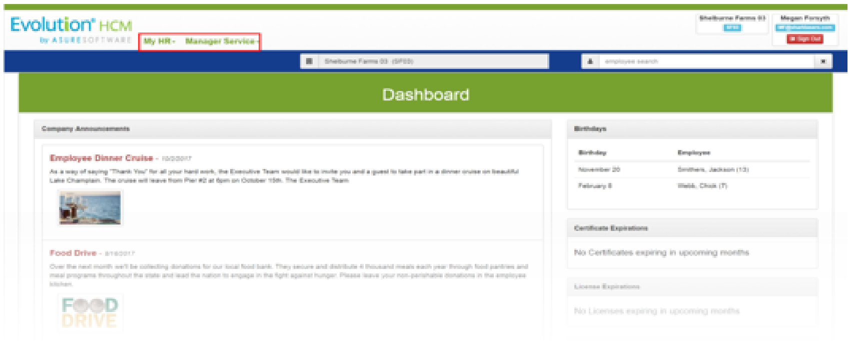
- My Employment Summary – **My Document** (adding any personal documents)
- My Employment Summary – **Emergency Contacts** (adding contacts)
- My Personal History – **My Absences** (requesting paid time off) **My I-9** (entering I-9 Form info)

Note: Permissions can be created for each role that can allow for any users in any role to update any field or record, or suppress visibility to any field or record. Refer to the *Customizing Security Roles / Users Guide*.

Base Manager Role

When a user who has been assigned a **Base Manager** signs in to Advanced HR 2.0, they will be taken to the Dashboard. There is also increased functionality available with the higher security access level of the Base Manager.

- Manager Services menu tab
- Company Announcements
- Upcoming Birthdays
- Scheduled Reviews
- Expiring Certifications and Licenses
- Time off requests
- Anniversaries



Company Announcements

Employee Dinner Cruise - 10/2/2017

As a way of saying "Thank You" for all your hard work, the Executive Team would like to invite you and a guest to take part in a dinner cruise on beautiful Lake Champlain. The cruise will leave from Pier #2 at 6pm on October 15th. The Executive Team

Food Drive - 8/16/2017

Over the next month we'll be collecting donations for our local food bank. They secure and distribute 4 thousand meals each year through food pantries and meal programs throughout the state and lead the nation to engage in the fight against hunger. Please leave your non-perishable donations in the employee kitchen.

Birthdays

Birthday	Employee
November 20	Smithers, Jackson (13)
February 8	Webb, Chick (7)

Certificate Expirations

No Certificates expiring in upcoming months

License Expirations

No Licenses expiring in upcoming months

Note: Users can have multiple Roles. In our example above, the User has a Base User Role AND a Base Manager Role.

The Dashboard for a **Base Manager** is slightly different than for a **Base User** because of the manager security role. The Dashboard for a Base Manager displays the following menu tabs at the top of the screen:

- **My HR** tab

- **Manager Services** (this tab is unique to the manager role)

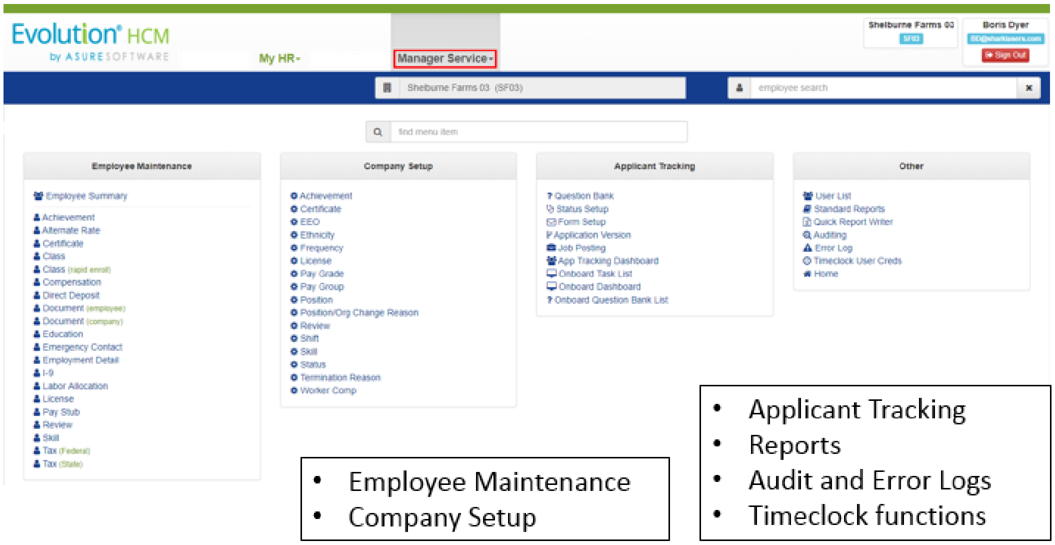
Note: Users can (and should) have multiple Roles. In our example above, the User has a Base User Role *and* a Base Manager Role (indicated by the **My HR** and **Manager Service** tabs). That is why the manager role also has the **My HR** tab. If the manager did not also have the Base User role, they would not see the **My HR** tab on their Dashboard. Permissions can be defined to allow managers to update their own records if desired.

The added menu tabs for the Base Manager also offer the following increased functionality.

Manager Service Tab for a Base Manager

A **Base Manager** can click on the **Manager Service** tab on the Dashboard, shown below, which provides more menu items to choose from than the **My HR** tab has, functionality that is important for someone at a manager level.

The **Manager Service** menu tab displays information and functionality that is important to any Manager:



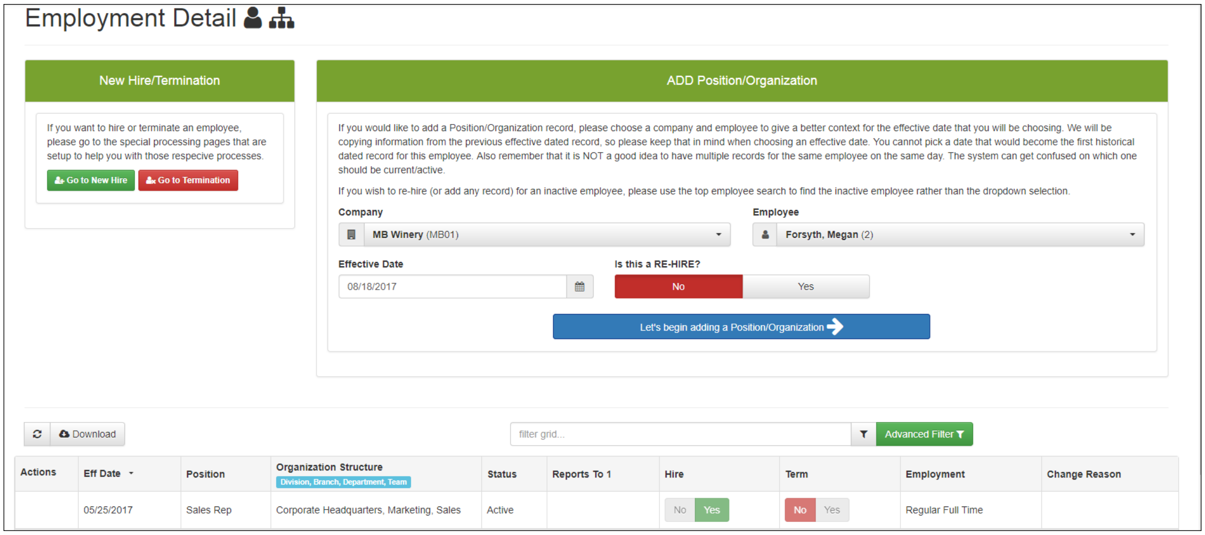
- Employee Maintenance
- Company Setup

- Applicant Tracking
- Reports
- Audit and Error Logs
- Timeclock functions

What Information can a Base Manager See?

A Base Manager has access to the information of *all* the employees that are assigned to them; that is, those employees that directly report to them (an employee can have up to three supervisors simultaneously – any of whom can access those employees via the **Manager Service** menu).

An Employee's position and organization (DBDT) assignments, status, compliance, and supervisor assignments are tracked from the **Employment Details** menu option (go to **HR Admin – Employee Maintenance – Employment Detail**). These "position and organization" records can be edited, but ideally they are intended to track the employee's history over time (tied to reporting).



Employment Detail

New Hire/Termination

If you want to hire or terminate an employee, please go to the special processing pages that are setup to help you with those respecive processes.

Go to New Hire | Go to Termination

ADD Position/Organization

If you would like to add a Position/Organization record, please choose a company and employee to give a better context for the effective date that you will be choosing. We will be copying information from the previous effective dated record, so please keep that in mind when choosing an effective date. You cannot pick a date that would become the first historical dated record for this employee. Also remember that it is NOT a good idea to have multiple records for the same employee on the same day. The system can get confused on which one should be current/active.

If you wish to re-hire (or add any record) for an inactive employee, please use the top employee search to find the inactive employee rather than the dropdown selection.

Company: MB Winery (MB01)

Employee: Forsyth, Megan (2)

Effective Date: 08/18/2017

Is this a RE-HIRE? [✓ No] Yes

Let's begin adding a Position/Organization

Download

filter grid...

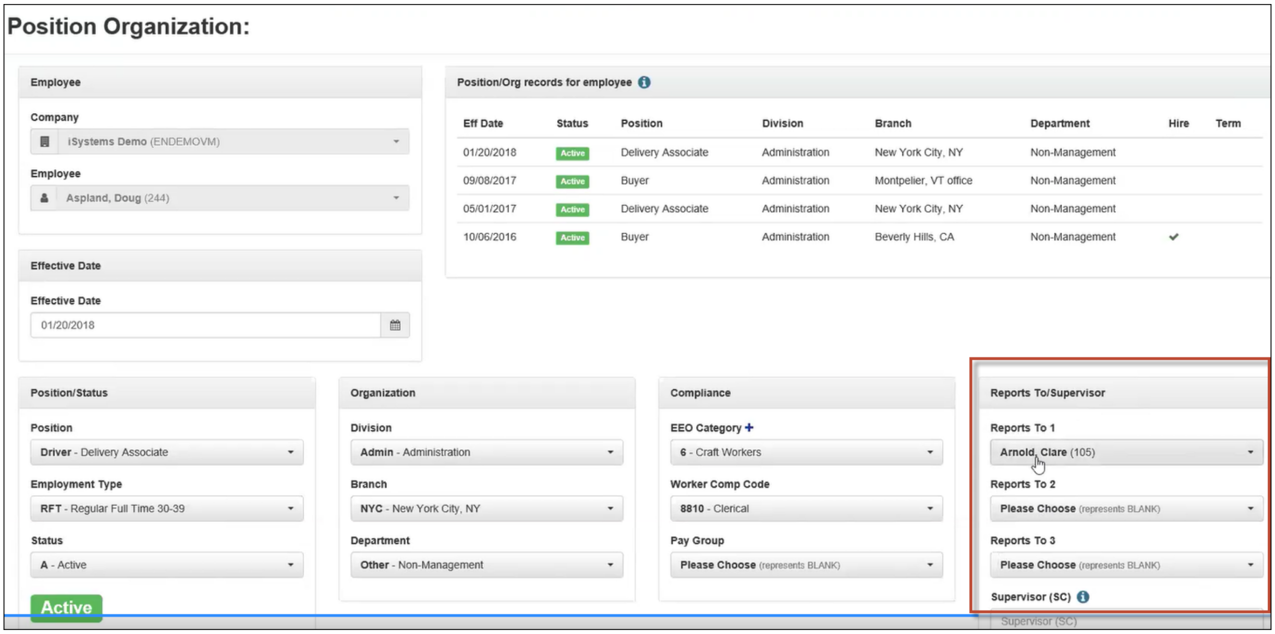
Advanced Filter

Actions	Eff Date	Position	Organization Structure Division, Branch, Department, Team	Status	Reports To 1	Hire	Term	Employment	Change Reason
	05/25/2017	Sales Rep	Corporate Headquarters, Marketing, Sales	Active		No [✓ Yes]	[✓ No] Yes	Regular Full Time	

Employment Detail screen

Select an employee and click the **Let's begin adding a Position/Organization**. **Base Managers** have the ability to edit:

- Position/Status
- Organization status
- Compliance (EEO Category, Worker Comp Code, and Pay Group)
- Reports to/Supervisor - you can assign up to three Managers (**Reports To 1, 2, 3**) and one **Supervisor**. See the following screenshot.



Position Organization:

Employee

Company: iSystems Demo (ENDEMOVM)

Employee: Aspland, Doug (244)

Position/Org records for employee

Eff Date	Status	Position	Division	Branch	Department	Hire	Term
01/20/2018	Active	Delivery Associate	Administration	New York City, NY	Non-Management		
09/08/2017	Active	Buyer	Administration	Montpelier, VT office	Non-Management		
05/01/2017	Active	Delivery Associate	Administration	New York City, NY	Non-Management		
10/06/2016	Active	Buyer	Administration	Beverly Hills, CA	Non-Management	✓	

Effective Date

Effective Date: 01/20/2018

Position/Status

Position: Driver - Delivery Associate

Employment Type: RFT - Regular Full Time 30-39

Status: A - Active

Active

Organization

Division: Admin - Administration

Branch: NYC - New York City, NY

Department: Other - Non-Management

Compliance

EEO Category: 6 - Craft Workers

Worker Comp Code: 8810 - Clerical

Pay Group: Please Choose (represents BLANK)

Reports To/Supervisor

Reports To 1: Arnold, Clare (105)

Reports To 2: Please Choose (represents BLANK)

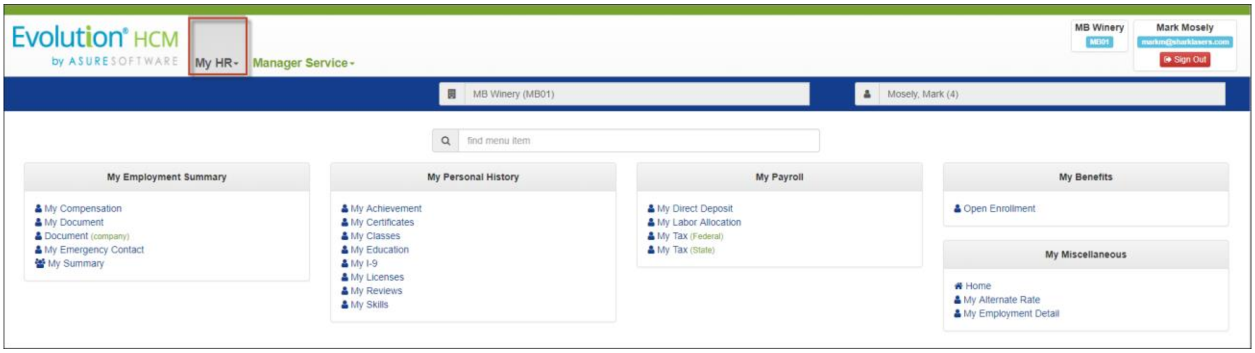
Reports To 3: Please Choose (represents BLANK)

Supervisor (SC): Supervisor (SC)

Click **Save Changes** when complete.

My HR for a Base Manager

When a **Base Manager** accesses their **My HR** menu, they can see their own information as it pertains to **Employment**, **Personal History**, **Payroll,** and **Miscellaneous** items:



MB Winery MB01

Mark Mosely markm@sharklasers.com

MB Winery (MB01)

Mosely, Mark (4)

find menu item

My Employment Summary
- My Compensation
- My Document
- Document (company)
- My Emergency Contact
- My Summary

My Personal History
- My Achievement
- My Certificates
- My Classes
- My Education
- My I-9
- My Licenses
- My Reviews
- My Skills

My Payroll
- My Direct Deposit
- My Labor Allocation
- My Tax (Federal)
- My Tax (State)

My Benefits
- Open Enrollment

My Miscellaneous
- Home
- My Alternate Rate
- My Employment Detail

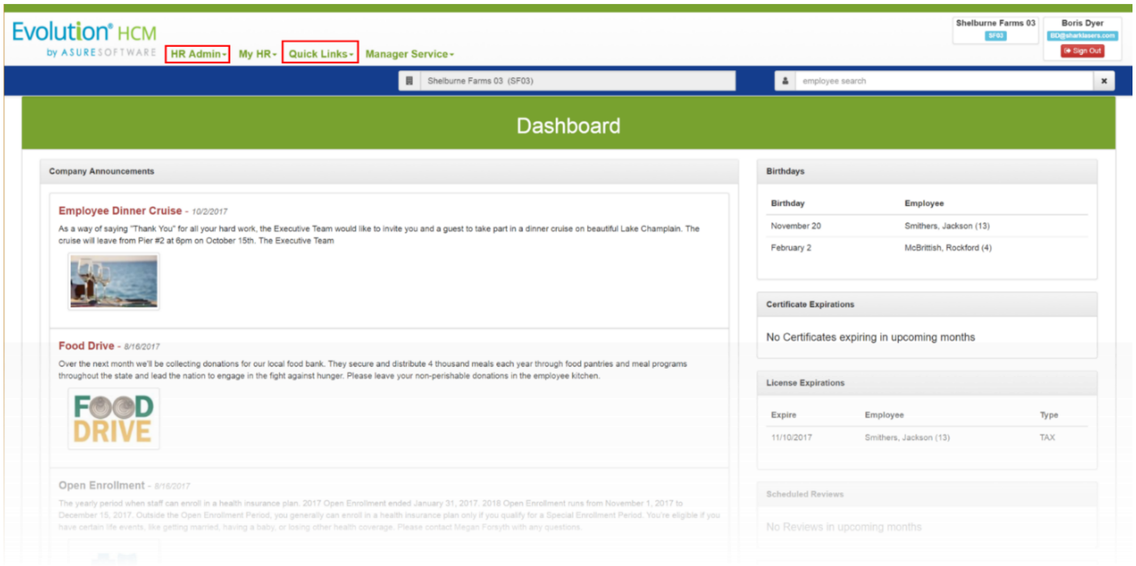
Base Manager - My HR menu

Note that the menu items on the Base Manager's **My HR** screen are the same as the **Base User** (and **Base Admin**), but what is different is the tabs at the top of each role's **My HR** screen – managers have a **Manager Service** tab and Admins have a **HR Admin** tab.

Base Admin Role

When a user who has been assigned a **Base Admin** signs in, as with any other role, they will be taken to the Dashboard. The Dashboard for a Base Admin is similar to the Base Manager but also contains additional menu items and functionality. This role is most likely the highest end user role you (the Service Bureau) will assign at the client level.

For example Boris is a **Base Admin** role user.



Company Announcements

Employee Dinner Cruise - *10/2/2017*

As a way of saying "Thank You" for all your hard work, the Executive Team would like to invite you and a guest to take part in a dinner cruise on beautiful Lake Champlain. The cruise will leave from Pier #2 at 6pm on October 15th. The Executive Team

Food Drive - *8/16/2017*

Over the next month we'll be collecting donations for our local food bank. They secure and distribute 4 thousand meals each year through food pantries and meal programs throughout the state and lead the nation to engage in the fight against hunger. Please leave your non-perishable donations in the employee kitchen.

Open Enrollment - *8/16/2017*

The yearly period when staff can enroll in a health insurance plan. 2017 Open Enrollment ended January 31, 2017. 2018 Open Enrollment runs from November 1, 2017 to December 15, 2017. Outside the Open Enrollment Period, you generally can enroll in a health insurance plan only if you qualify for a Special Enrollment Period. You're eligible if you have certain life events, like getting married, having a baby, or losing other health coverage. Please contact Megan Forsyth with any questions.

Birthdays

Birthday	Employee
November 20	Smithers, Jackson (13)
February 2	McBrittish, Rockford (4)

Certificate Expirations

No Certificates expiring in upcoming months

License Expirations

Expire	Employee	Type
11/10/2017	Smithers, Jackson (13)	TAX

Scheduled Reviews

No Reviews in upcoming months

The Dashboard for a **Base Admin** displays the following menu tabs at the top of the screen:

- **HR Admin** (this tab is unique for the Base Admin role)
- **My HR**
- **Quick Links**

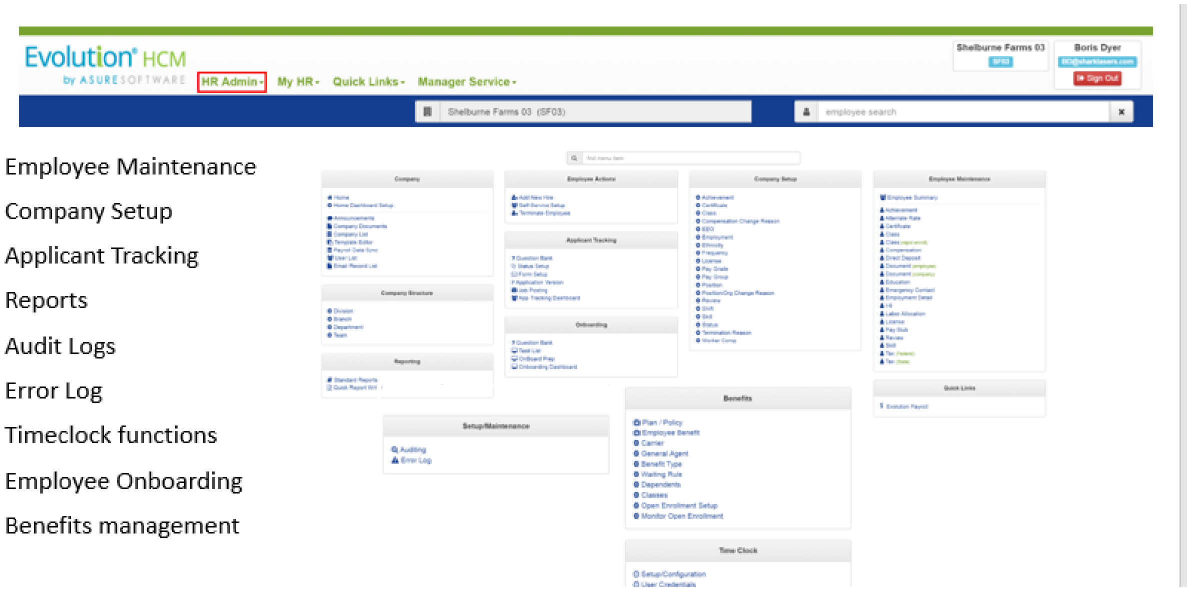
There is also increased functionality available with the higher security access level of the **Base Admin** user. In addition to the above menu tabs, the **Base Admin** will be able to see the following items on the Dashboard:

- Company announcements
- Upcoming birthdays
- Certificate and License expirations
- Scheduled reviews (managers can see these also – but only for their direct reports)
- Time off requests (their own and any that require their approval)

Note: Managers can see any report that is assigned manager level access – and they may be able to see the Quick Report Writer. Note however, that the reports are not controlled by the security engine – so if a field or page is suppressed in the application – it may still be visible in the reports if the user can access those reports.

HR Admin Tab - Base Admin

As you can see below, there is increased functionality with the higher access level of the **Base Admin** role. Most importantly, **Base Admins** have access to the **HR Admin** tab.

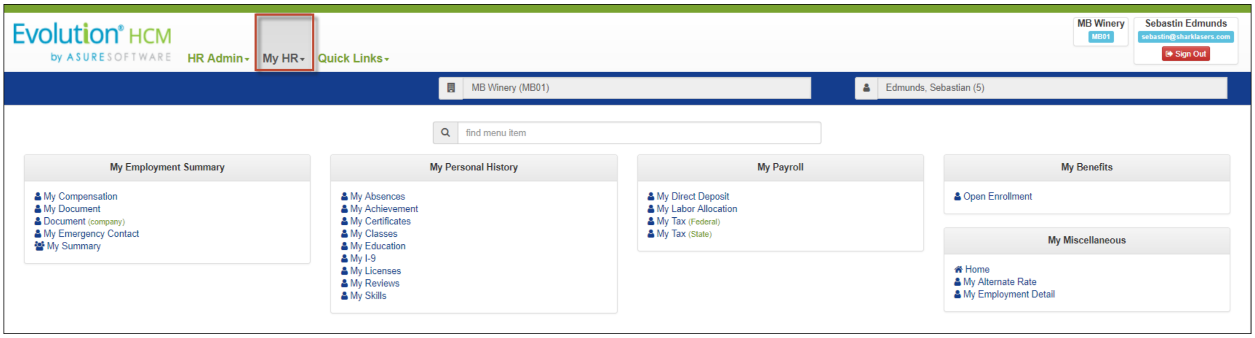


Base Admin – HR Admin tab

With access to the **HR Admin** tab, the Base Admin role has a much deeper level of potential functionality than the previously discussed roles.

My HR for a Base Admin

When a Base Admin accesses their **My HR** menu, they can see their own information as it pertains to **Employment**, **Personal History**, **Payroll,** and **Miscellaneous** items:



My Employment Summary
- My Compensation
- My Document
- Document (company)
- My Emergency Contact
- My Summary

My Personal History
- My Absences
- My Achievement
- My Certificates
- My Classes
- My Education
- My I-9
- My Licenses
- My Reviews
- My Skills

My Payroll
- My Direct Deposit
- My Labor Allocation
- My Tax (Federal)
- My Tax (State)

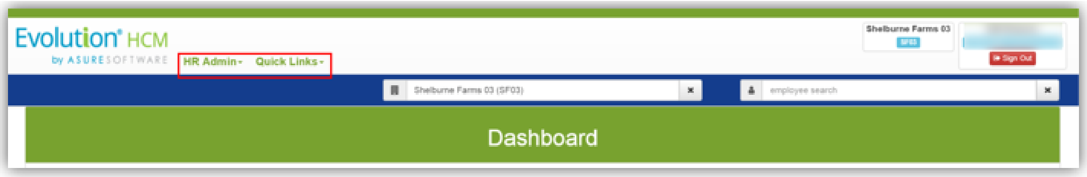
My Benefits
- Open Enrollment

My Miscellaneous
- Home
- My Alternate Rate
- My Employment Detail

Base Admin - My HR menu

Service Bureau Admin Role

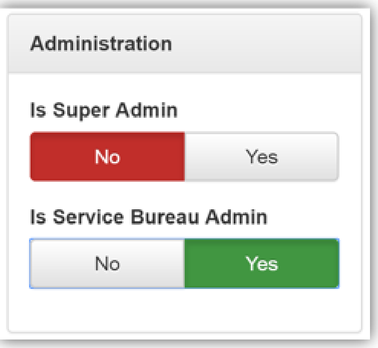
The **Service Bureau Admin** (SB Admin) is a step below the **Super Admin** level of access. The functionality for the Service Bureau Admin user level is geared more toward the administrative side. The **SB Admin** is typically not an employee of any company. Their role is typically used for your service bureau staff such as the CSR. They can be assigned companies to access however. **SB Admins** assign roles to users.



Service Bureau (SB) Admins have increased functionality. This functionality can be seen in the HR Admin and Quick Links menu tabs.

For SB Admin:

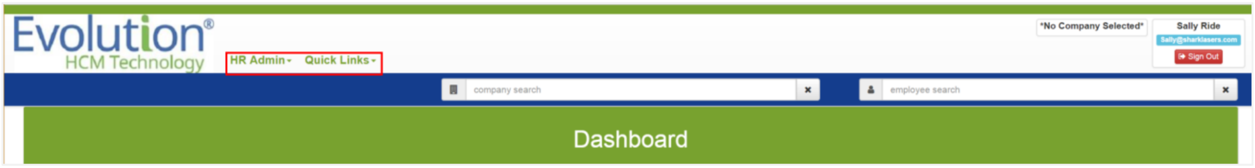
- Access to account information -
  - Ability to add companies
  - Ability to assign users to companies
  - Processing Payrolls
- SB Admins are assigned companies to access
  - They typically are not employees of a company
- Access to Security Maintenance –
  - Assign roles to users


Administration

Is Super Admin
No | Yes (No selected)

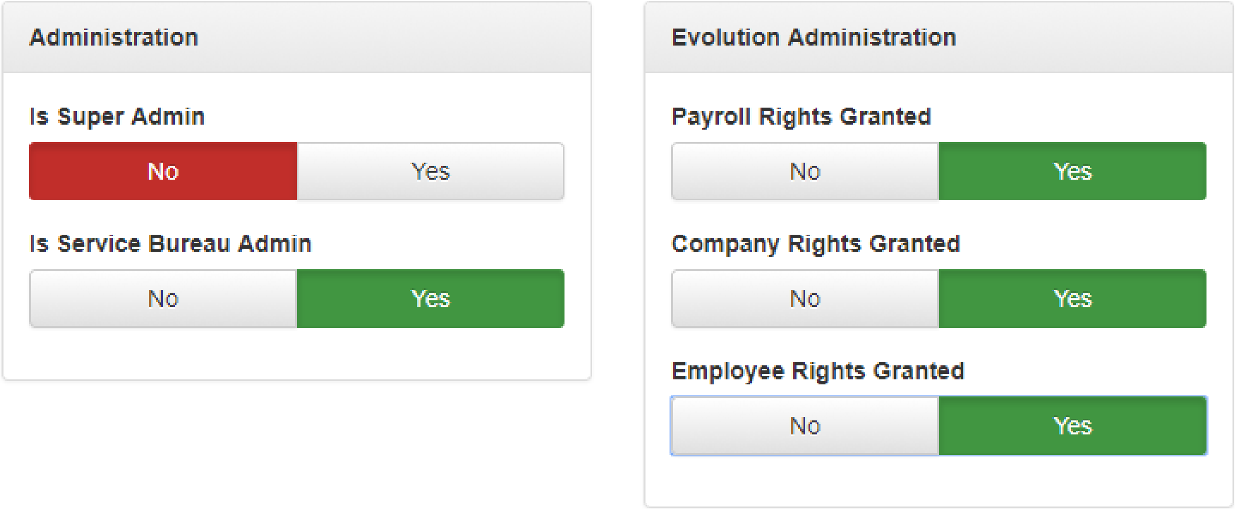
Is Service Bureau Admin
No | Yes (Yes selected)

The primary difference between a **Service Bureau Admin** and a **Super Admin** is the *Service Bureau Admin users can be excluded from accessing specific companies* – such as when they are responsible only for certain companies, or should not see specific companies (such as the Service Bureau's home company).



It is important to note that when the **SB Admin** first signs in, just like the other security levels, they are taken to a Dashboard. If you notice above, however, this Dashboard is different because it is not attached to a company – the **company search** field at the top of the screen is not locked into a company. The **SB Admins** are assigned companies to access but they typically are not employees of a company.

On the **User List** screen, you can make a user a Service Bureau Admin. Use the **Yes/No** toggles under **Administration** – **Is Service Bureau Admin**.



Administration

Is Super Admin
[✓ No] Yes

Is Service Bureau Admin
No [✓ Yes]

Evolution Administration

Payroll Rights Granted
No [✓ Yes]

Company Rights Granted
No [✓ Yes]

Employee Rights Granted
No [✓ Yes]

For Service Bureau Admins, you can assign them Evolution access in the **Evolution Administration** section as shown above. This access corresponds to the **AHR 2 Security Group** in Evolution Classic.

From the Dashboard, the two tabs that the Service Bureau Admin user has access to are the **HR Admin** and the **Quick Links** menu tabs. These tabs allow the **SB Admin** to:

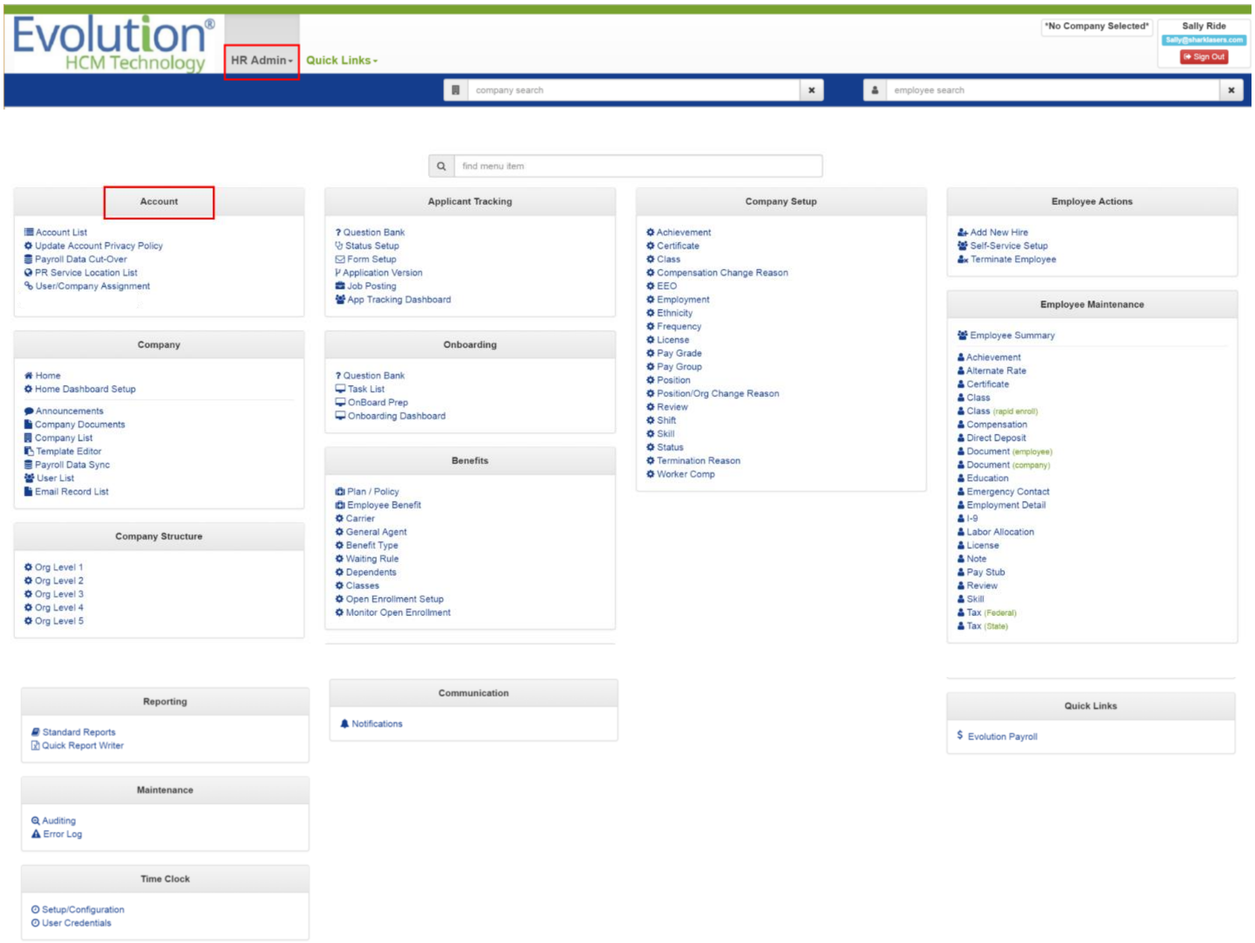
- Access Account information
  - Add companies
  - Assign users to companies
  - Process payrolls
- Company Setup
- Reporting
- Employee Setup and Maintenance

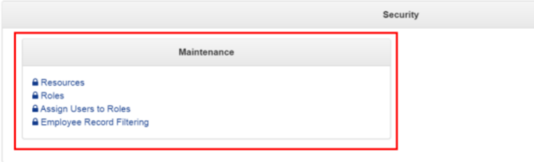
- Applicant Tracking
- Benefits
- Time Clock setup
- Security Maintenance
    - Resources
    - Assigning /Edit Roles to users
    - Assign Users to Roles
    - Create Employee Record

Note: It is important to note that as a user, you cannot do something that is higher than your security level allows. For example, if I'm a Service Bureau Admin, I can't make myself a Super Admin.

HR Admin Tab - Service Bureau Admin

The following is an example of the **HR Admin** tab for a **Service Bureau Admin** user.




Security

Maintenance

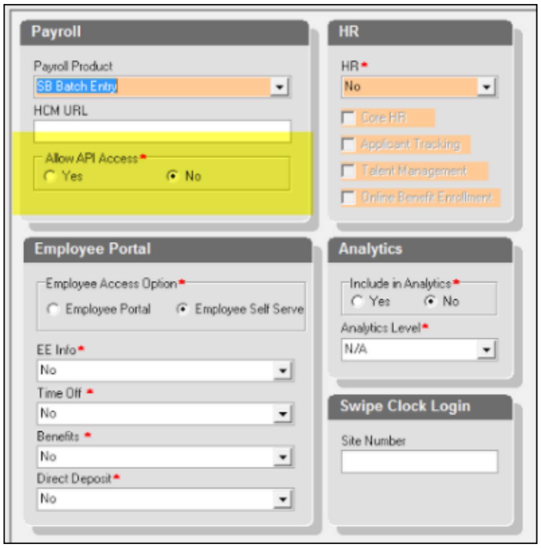
- Resources
- Roles
- Assign Users to Roles
- Employee Record Filtering

Note the **Evolution Payroll** link in the **Quick Links** menu. This is only visible because this SB Admin user has the correct security rights and **AHR 2 Security Groups** assignment in Evolution Classic.

Required Security Step for SB Admin Role for Company Onboarding

In order to make sure that SB Admins cannot onboard companies that they do not have access to in Evolution Classic, we have added a **Yes / No** field to the **Company - Payroll Products** screen called "**Allow API Access**". The primary concern here was that SB Admins could onboard the companies that they work for into the system through the Cut-Over screen in Evolution Classic. The secondary concern is that they could onboard companies that they should not have access to for whatever internal SB reason.

The **Allow API Access** field is set to **No** by default for all companies.


Payroll

Payroll Product: SB Batch Entry

HCM URL:

Allow API Access*: ○ Yes ● No

HR

HR*: No

□ Core HR

□ Applicant Tracking

□ Talent Management

□ Online Benefit Enrollment

Employee Portal

Employee Access Option*: ○ Employee Portal ● Employee Self Serve

EE Info*: No

Time Off*: No

Benefits*: No

Direct Deposit*: No

Analytics

Include in Analytics*: ○ Yes ● No

Analytics Level*: N/A

Swipe Clock Login

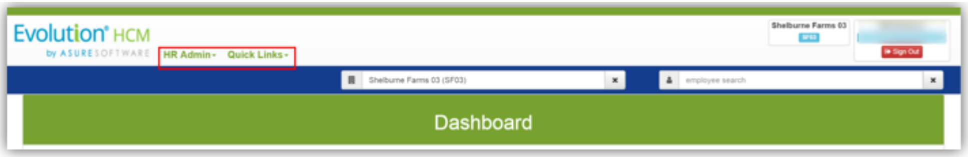
Site Number:

When the system gets a list of possible companies for payroll cutover and will read this value and if it is set to **No** *and* the user is an **SB Admin** – it will filter the company(s) out from the list. If the user is a **Super Admin** however, which in Advanced HR has access to all companies, this filter will not apply for them.

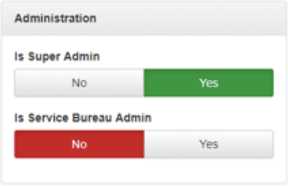
Therefore, there is an additional step before an **SB Admin** is going to onboard a company which is to go into Evolution Classic and switch the **Allow API Access** flag from **No** to **Yes**. Note that since it is placed inside the Company screen - if in Evolution Classic, the **SB Admin** has no access to this company then they will not be able to change it to **Yes**.

Super Admin Role

Super Admins are the highest level of security role. Super Admins have access to *all* of the clients associated with an account in Advanced HR 2.0. Super Admins also have the ability to Exclude companies from users. See the section in this guide Excluding a Company from a User.



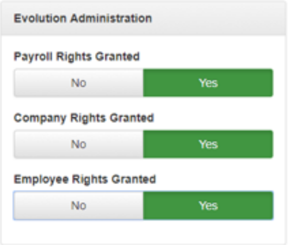
The Super Admin Role is reserved for high level Service Bureau staff. It has access to ALL the clients that are associated with an account in Advanced HR 2.0.



Administration

Is Super Admin
No [✓ Yes]

Is Service Bureau Admin
[✓ No] Yes



Evolution Administration

Payroll Rights Granted
No [✓ Yes]

Company Rights Granted
No [✓ Yes]

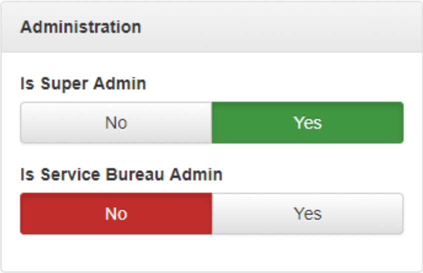
Employee Rights Granted
No [✓ Yes]

It is recommended that the **Super Admin** role be reserved only for high level service bureau staff such as Administration, Engineering, Support, or Development. Also, it's important to remember that neither SB Admins nor Super Admins should be associated to a company as an employee.

Note: It is best practice to limit the **Super Admin** security role to 2 or 3 Service Bureau staff only.

When a user who has been assigned a **Super Admin** signs in, as with any other role, they will be taken to the Dashboard.

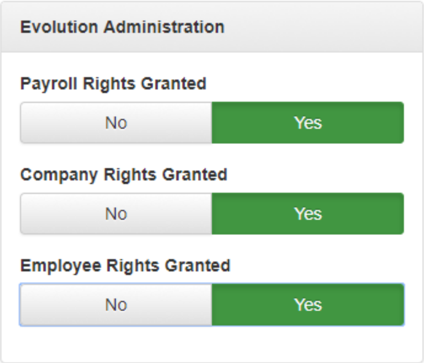
You make a user a Super Admin on the **User List** screen, in the **Administration** section, by setting the **Is Super Admin** toggle to **Yes**.



Administration

Is Super Admin
No [✓ Yes]

Is Service Bureau Admin
[✓ No] Yes



Evolution Administration

Payroll Rights Granted
No [✓ Yes]

Company Rights Granted
No [✓ Yes]

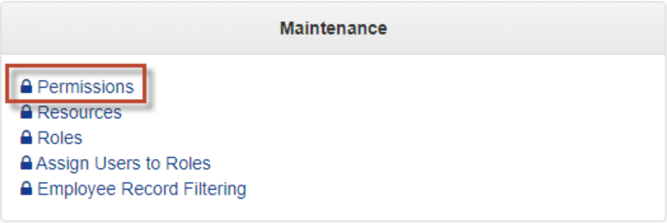
Employee Rights Granted
No [✓ Yes]

For **Super Admins**, you can assign them Evolution access in the **Evolution Administration** section of the **User List** screen as shown above. This access corresponds to the User Groups in Evolution Classic. As with SB Admins, you can assign user groups here. However, since **Super Admins** have access to all Cutover companies by default anyway, you shouldn't have to.

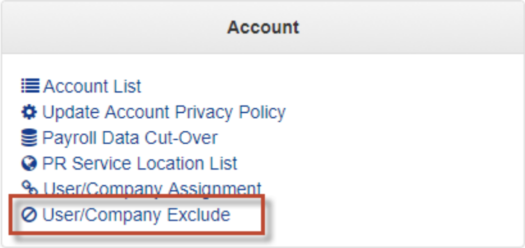
Super Admins have the ability to Exclude companies from users.

The main difference in functionality between the **SB Admin** and the **Super Admin** user role is in the **Account** and **Security** menu panes of the **HR Admin** tab.

- For **Super Admins**, on the **Security** tile, in the **Maintenance** sub-section, the **Permissions** menu item is also available.



- For **Super Admins**, on the **Account** tile, the **User/Company Exclude** menu item is also available.

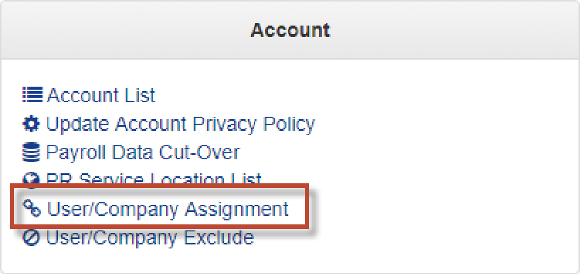


Assigning a Company to a SB Admin or a Super Admin

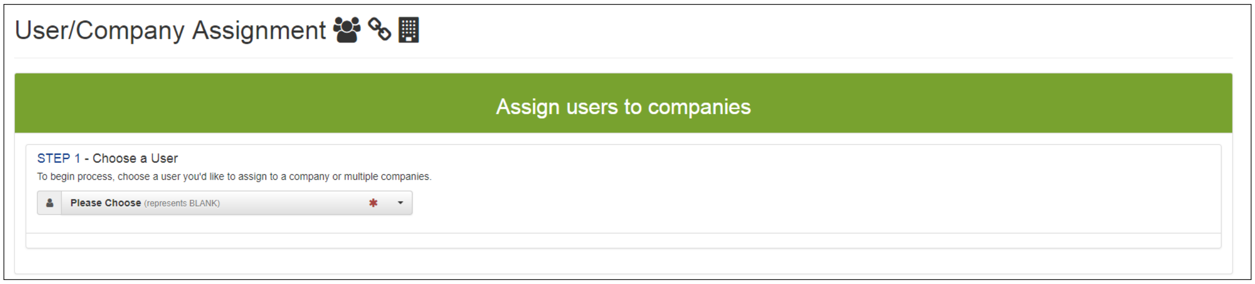
Using the Security Group functions, you can assign clients to users in Evolution Classic. You can also do it in Advanced HR 2.0.

To assign a company to a **SB Admin** or to a **Super Admin**:

1. Go to **HR Admin – Account – User/Company Assignment**.



This is where you assign a user to a company.



User/Company Assignment

Assign users to companies

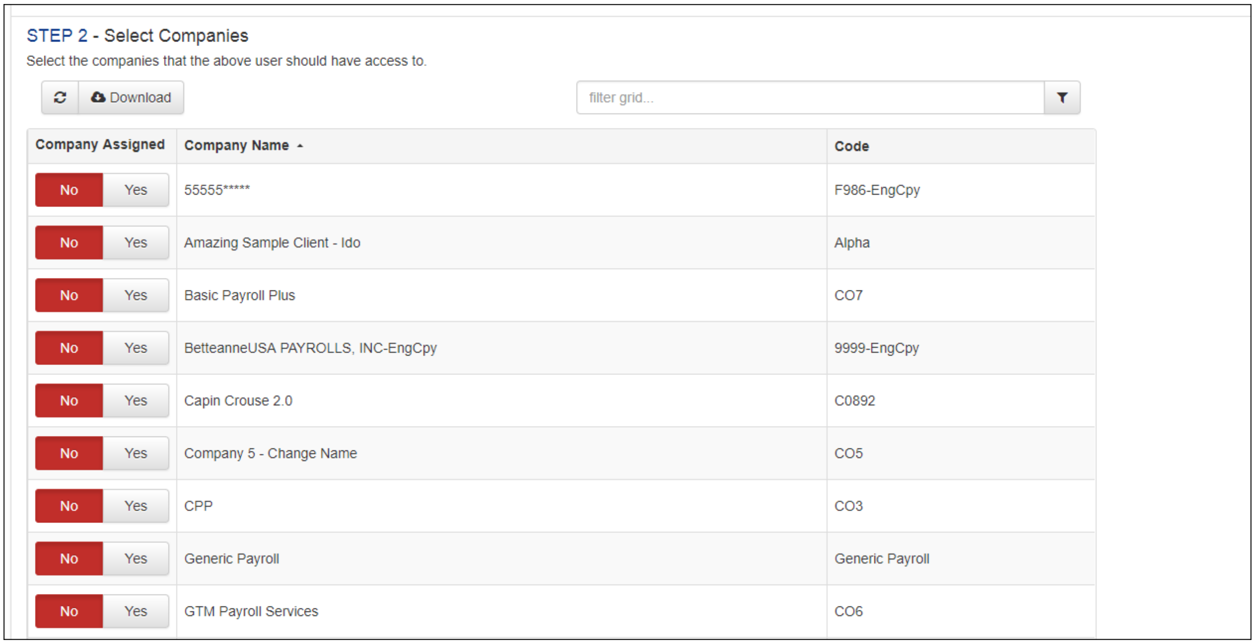
STEP 1 - Choose a User

To begin process, choose a user you'd like to assign to a company or multiple companies.

Please Choose (represents BLANK) *

2. Select the user from the dropdown. A list of all the companies that have been Cutover will display.

   Note: If you don't see the person in the dropdown this is most likely due to them not having been made a user in the system, that must be done first.
3. The system displays **Step 2 – Select Companies** - a list of all the companies from which you can designate which company or companies the user should have access to.

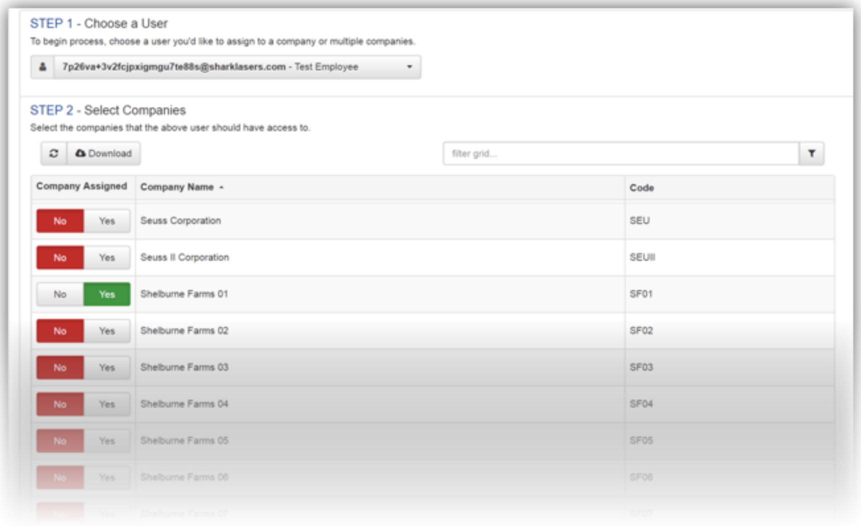


STEP 2 - Select Companies

Select the companies that the above user should have access to.

Company Assigned	Company Name	Code
No Yes	55555*****	F986-EngCpy
No Yes	Amazing Sample Client - Ido	Alpha
No Yes	Basic Payroll Plus	CO7
No Yes	BetteanneUSA PAYROLLS, INC-EngCpy	9999-EngCpy
No Yes	Capin Crouse 2.0	C0892
No Yes	Company 5 - Change Name	CO5
No Yes	CPP	CO3
No Yes	Generic Payroll	Generic Payroll
No Yes	GTM Payroll Services	CO6

4. Use the **Yes/No** toggles to turn on or off the companies that you want this user to have access to.



STEP 1 - Choose a User

To begin process, choose a user you'd like to assign to a company or multiple companies.

7p26va+3v2fcjpxigmgu7te88s@sharklasers.com - Test Employee

STEP 2 - Select Companies

Select the companies that the above user should have access to.

Company Assigned	Company Name	Code
[✓ No] Yes	Seuss Corporation	SEU
[✓ No] Yes	Seuss II Corporation	SEUII
No [✓ Yes]	Shelburne Farms 01	SF01
[✓ No] Yes	Shelburne Farms 02	SF02
[✓ No] Yes	Shelburne Farms 03	SF03
[✓ No] Yes	Shelburne Farms 04	SF04
[✓ No] Yes	Shelburne Farms 05	SF05
[✓ No] Yes	Shelburne Farms 06	SF06
[✓ No] Yes	Shelburne Farms 07	SF07

Note that for this user, they currently have access to one company (**Shelburne Farms 01**)

When this user logs in, they will only be able to log in to that company (**Shelburne Farms 01**).

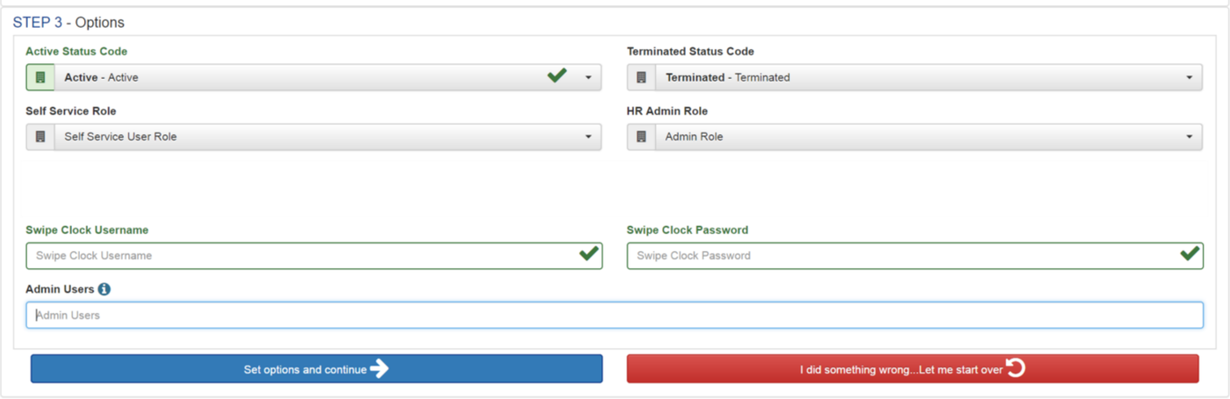
Note that you can also assign clients to users in Evolution Classic.

Super Admins also have the ability to Exclude a user from a company. See the section Excluding a Company from a User in this guide.

Security Roles and the Payroll Cutover

During the Payroll Cutover, in **Step 3 - Options**, you can select which roles you'd like to be part of the Cutover and associated with the client that is being onboarded. In other words, set up your default roles. Use the dropdowns for the **Self Service Role** and the **HR Admin Role**.

If you do not select a Self Service Role and an HR Admin Role in these fields in **Step 3 – Options** of the Payroll Cutover process, the new roles will not be created for the company – since there is nothing from which they can be cloned.



STEP 3 - Options

Active Status Code: Active - Active

Terminated Status Code: Terminated - Terminated

Self Service Role: Self Service User Role

HR Admin Role: Admin Role

Swipe Clock Username: Swipe Clock Username

Swipe Clock Password: Swipe Clock Password

Admin Users: Admin Users

Self Service Role

The **Self Service Role** dropdown list of available roles for ESS will only include those roles that are **Base User** (Level 10) and *are not currently assigned to a company*.

HR Admin Role

The **HR Admin Role** dropdown list of available will only include those roles that are **Base Admin** (Level 50) and *are not currently assigned to a company*.

The **Manager** and **Anonymous** roles will be created for each company on Payroll Cutover – but it is very important to note – these roles will always come from the **Base Manager** and **Anonymous** roles.

It's important to note that the roles that are part of the Payroll Cutover will be **designated** by the Client Number from Evolution Payroll. It is also very important that after Cutover, you keep these as default roles. Best practice is to "clone" security roles. Let's look at that process in more detail.

Also make note of the SwipeClock setup fields (**Swipe Clock Username** & **Swipe Clock Password**) in the above screenshot.

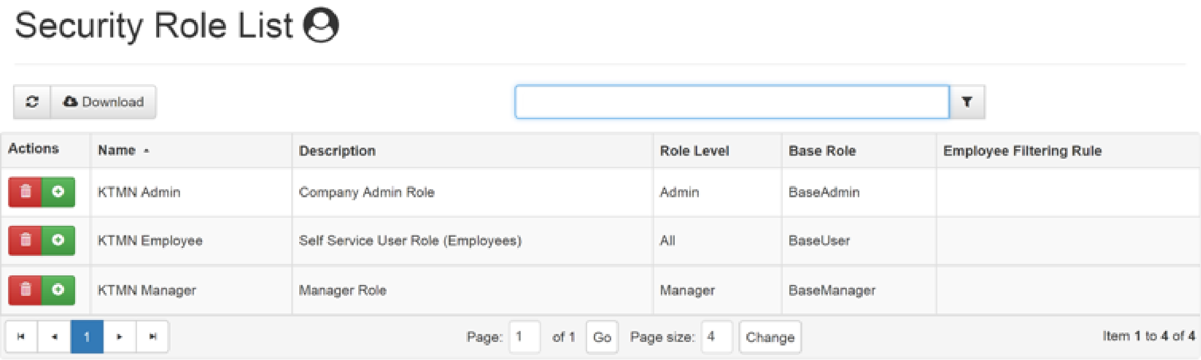
Cloning a Security Role

After a company is cutover into Advanced HR 2.0, it is given four default security roles.

Administrators have the ability to *clone* or copy a security role and associate it to a specific company; in fact, we strongly recommend this best practice. Every company should have its own security roles derived from the template base roles. Cloning allows you to copy a role multiple times, or allows you to add or take away permissions to a role. Permissions are what defines user access.

In Advanced HR 2.0 you don't "create" a Role, you **Clone** them.

Go to **HR Admin - Security – Maintenance - Roles.**



Security Role List

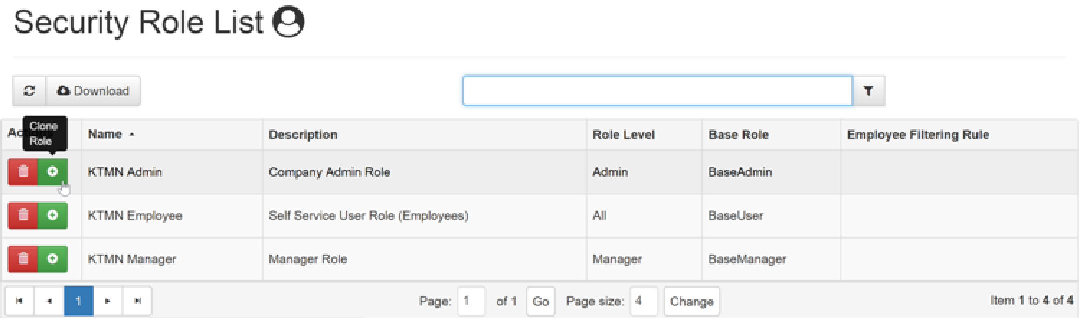
Actions	Name	Description	Role Level	Base Role	Employee Filtering Rule
🗑 ⊕	KTMN Admin	Company Admin Role	Admin	BaseAdmin	
🗑 ⊕	KTMN Employee	Self Service User Role (Employees)	All	BaseUser	
🗑 ⊕	KTMN Manager	Manager Role	Manager	BaseManager	

Page: 1 of 1 Go Page size: 4 Change Item 1 to 4 of 4

You will be taken to the **Security Role List**. The above list shows the default roles that were part of the Payroll Cutover.

Once the roles are cloned, they are then assigned to that company. A cloned role becomes *a child role* of the *parent base role*. Note that this will become important when software updates are released. A child role cloned from one of the parent base roles will, when an update occurs, have any new/changed security issues cascade down from the parent role to any child roles derived from the parent role by the cloning process. This is most likely what you want to occur. If you created a role that was not a child of one of the parent base roles, then when a software update occurs, that role will not inherit any new/changed security (Resource/Permission) issues. It is important to remember that if you alter a default role, all subsequent cloning of that role will reflect those changes.

Each default role that was part of the Payroll Cutover, should be cloned and then assigned to the company. Click on the green **Plus Sign** button in the **Action** column to begin.

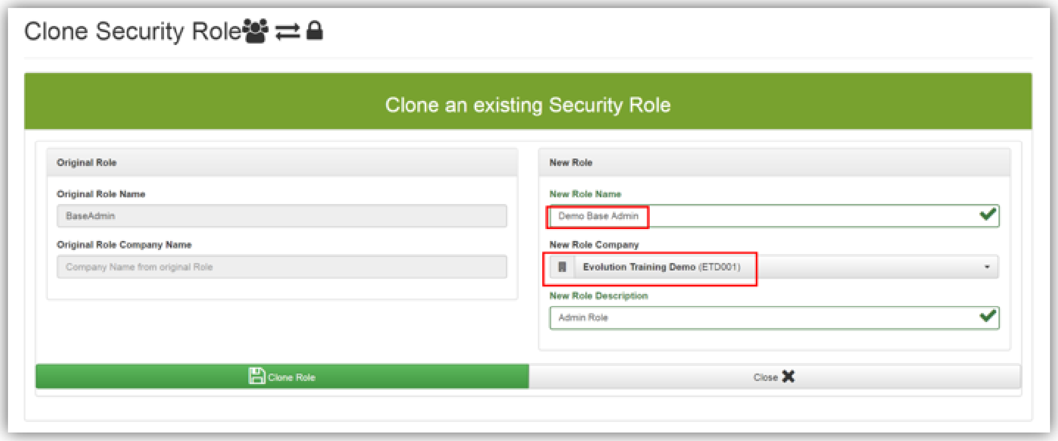


Security Role List

Ac	Name ▴	Description	Role Level	Base Role	Employee Filtering Rule
	KTMN Admin	Company Admin Role	Admin	BaseAdmin	
	KTMN Employee	Self Service User Role (Employees)	All	BaseUser	
	KTMN Manager	Manager Role	Manager	BaseManager	

Page: 1 of 1 Go Page size: 4 Change Item 1 to 4 of 4

In the example above, we are cloning the Base Admin Role.



Clone Security Role

Clone an existing Security Role

Original Role

Original Role Name: BaseAdmin

Original Role Company Name: Company Name from original Role

New Role

New Role Name: Demo Base Admin

New Role Company: Evolution Training Demo (ETD001)

New Role Description: Admin Role

It is important to remember, that when cloning a role, make the name distinct to the company that it is being attached to. Also, keep your naming consistent.

Click **Clone Role** when complete.

When a company is onboarded, you have the opportunity to select which base role that you want to use as a template; for example, for the **Base User (ESS)** role and for the **Base Admin** role. You can then clone those base roles, or any role, which become new roles specifically for that company. Any user that is below a Service Bureau Admin level must belong to a role that is associated with any company that they are accessing (see above – the no company role).

You can make a clone (copy) of the default security level roles such as **Base User**, **Base Manager**, **Base Admin**, etc., and rename the role by prefacing it with the name of the company for which it is intended. For example, for the MB Winery company, you could clone the **Base User** role and rename it to something like "**MB Winery – Base Role**." Using this method, you can make changes and add permissions to the default security roles for a specific company but still leave the original default security roles unchanged. And this method will make it clear that these roles are linked to this specific company, if you keep your naming convention consistent.

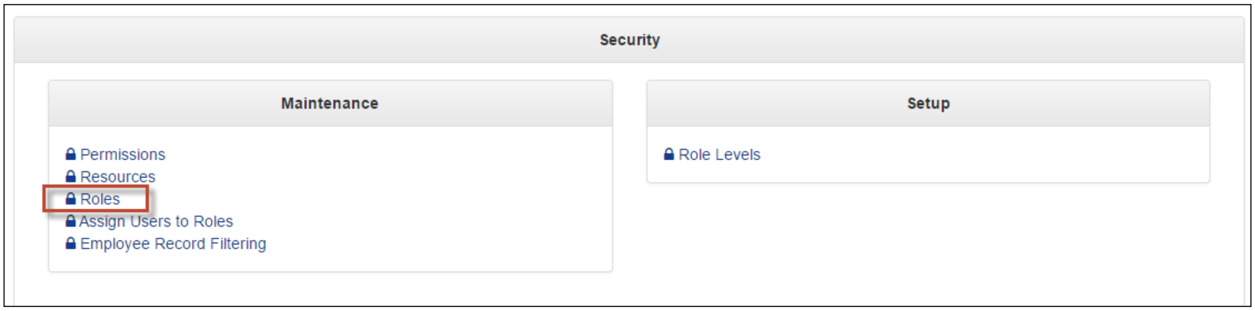
Important Note: Do not change/edit these Base Roles. You will instead want to clone or copy the base roles and make them specific for each company – instructions to do this are provided below.

The following table presents an example of cloning the three main default security roles and renaming them with company-specific names. You may also want to incorporate the Company Code into the role names.

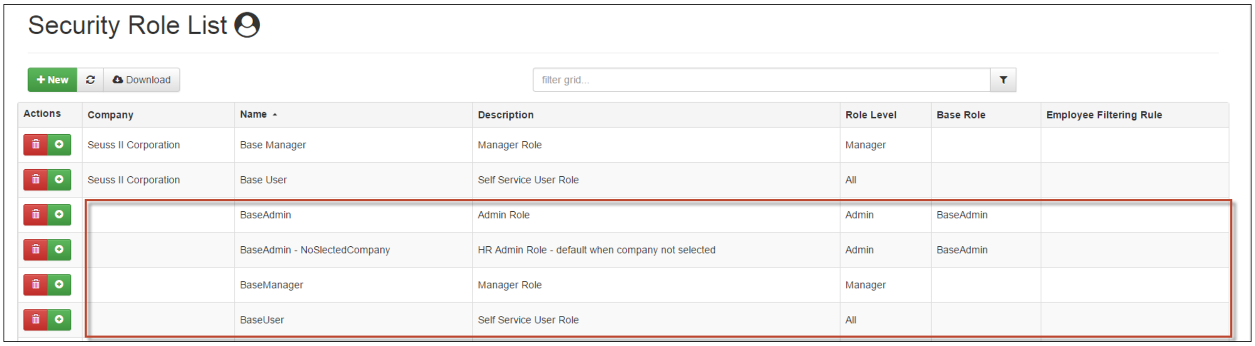
Default Security Role Name	MB Winery Company Role Names
Base User	MB Winery - Base User
Base Manager	MB Winery - Base Manager
Base Admin	MB Winery - Base Admin

To clone a default security role, follow the steps below.

1. Go to **HR Admin – Security – Maintenance – Roles**.



2. The system displays the **Security Role List** screen.

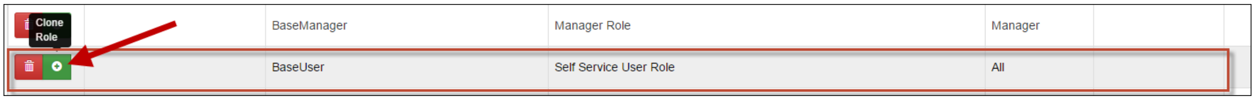


Security Role List

Actions	Company	Name	Description	Role Level	Base Role	Employee Filtering Rule
	Seuss II Corporation	Base Manager	Manager Role	Manager		
	Seuss II Corporation	Base User	Self Service User Role	All		
		BaseAdmin	Admin Role	Admin	BaseAdmin	
		BaseAdmin - NoSlectedCompany	HR Admin Role - default when company not selected	Admin	BaseAdmin	
		BaseManager	Manager Role	Manager		
		BaseUser	Self Service User Role	All		

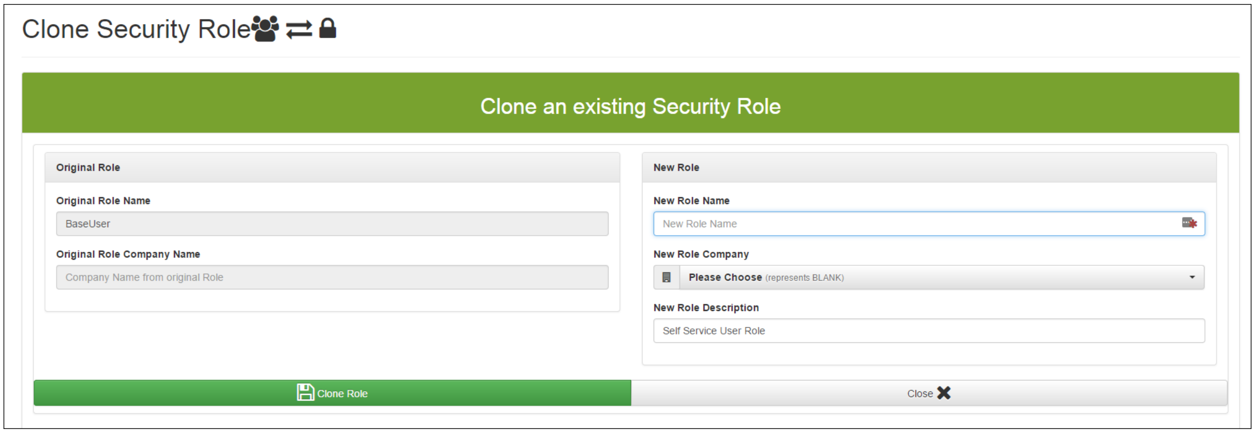
The **Security Role List** screen displays a list of the default security roles and any company-specific security roles that have been copied (cloned) from the default roles. Note that the default security roles do not display anything in the **Company** column as they are not associated with a specific company.

3. Select the default security role that you want to clone - one that is not attached to a company - for example, the **Base User** role (BaseUser - Self Service User Role) and in the **Actions** column, click on the green + plus Clone Role icon, shown at right and in the following screenshot.



	BaseManager	Manager Role	Manager
	BaseUser	Self Service User Role	All

4. The system displays the **Clone an existing Security Role** screen.



Clone Security Role

Clone an existing Security Role

Original Role

Original Role Name: BaseUser

Original Role Company Name: Company Name from original Role

New Role

New Role Name: New Role Name

New Role Company: Please Choose (represents BLANK)

New Role Description: Self Service User Role

The system displays the default security role that you are cloning in the **Original Role** section on the left side of the screen. In the **New Role** section on the right side of the screen, do the following:

5. Enter a name for the new role in the **New Role Name** field.

   Remember that best practice is to clone the role and rename it by making the role name distinct to the company it is being attached to. Also, keep the naming convention consistent for all the roles you clone for a company.

6. Select the company name from the **New Role Company** dropdown.

   The importance of this step is that when a user is then assigned this role, it will give them access to only that company.

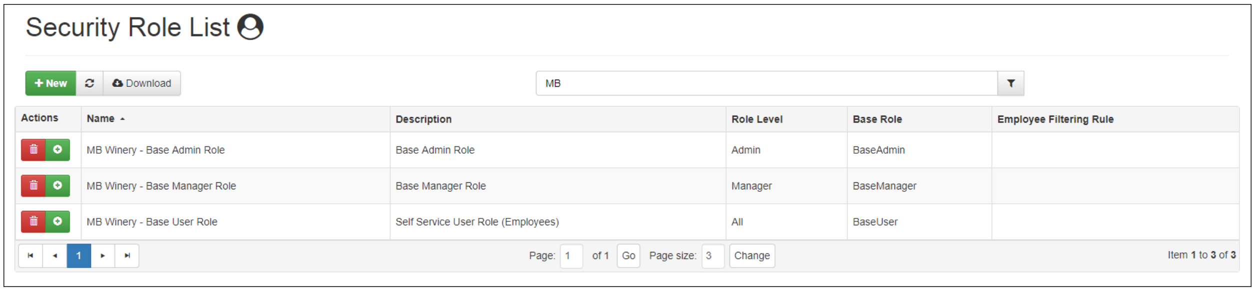
7. Enter a description for the new role in the **New Role Description** field.
8. Click on the **Clone Role** button at the bottom of the screen.

The system creates the new role for the company. The role is then ready to be assigned to a user. See the section in this guide titled Assigning a Security Role to a User.

More about Cloning Roles

Let's take an example of cloning roles. For the MB Winery, assume we cloned the Base Admin role and made it specifically for the MB Winery – we named it "**MB Winery – Base Admin Role**.

You can go to **HR Admin – Roles** screen:



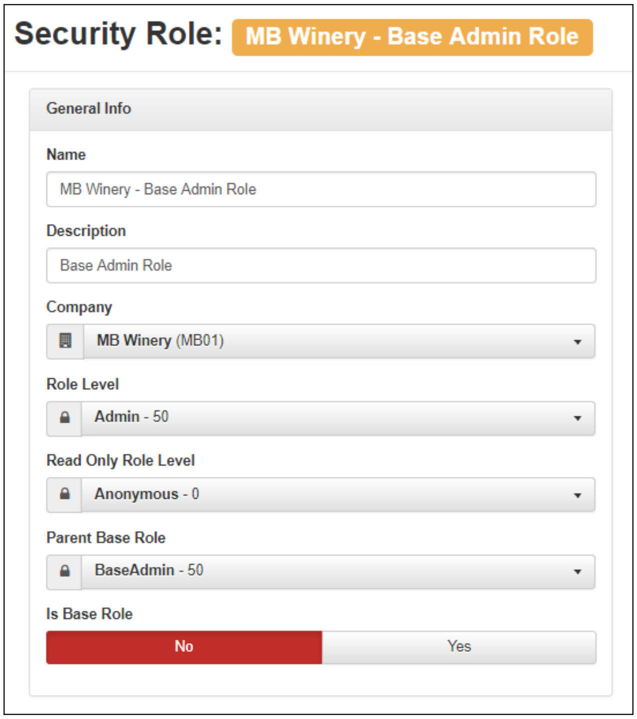
Security Role List

MB

Actions	Name	Description	Role Level	Base Role	Employee Filtering Rule
	MB Winery - Base Admin Role	Base Admin Role	Admin	BaseAdmin	
	MB Winery - Base Manager Role	Base Manager Role	Manager	BaseManager	
	MB Winery - Base User Role	Self Service User Role (Employees)	All	BaseUser	

Page: 1 of 1 Go Page size: 3 Change Item 1 to 3 of 3

Then click on a role, for example, **MB Winery – Base Admin Role**. The system displays the details about that role. The screen shows the name of the role, the description, the Company the role is for and the security role level (Admin).



Security Role: MB Winery - Base Admin Role

General Info

Name: MB Winery - Base Admin Role

Description: Base Admin Role

Company: MB Winery (MB01)

Role Level: Admin - 50

Read Only Role Level: Anonymous - 0

Parent Base Role: BaseAdmin - 50

Is Base Role: [✓ No] Yes

The **Parent Base Role** field indicates the original default role that you cloned to make this role. In our example, the **BaseAdmin** role was cloned to make the **MB Winery – Base Admin Role**. Also note, because this is a cloned role, the **Is Base Role** field indicates the role is not a Base Role.

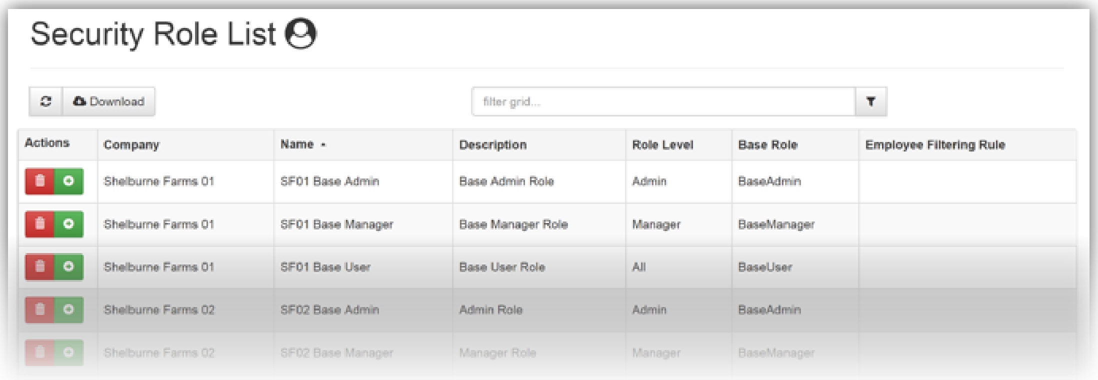
Note: It's important to know the parent base role of a role you have cloned for a company. And to remember that if, in a new release of Advanced HR 2.0, we include a new screen or a new field for an existing screen, the new screens/fields will be incorporated into the default security and assigned to the actual base roles (for example – BaseUser and BaseAdmin). In the new release of Advanced HR 2.0, the permissions for any new items will then cascade down to any roles that have been cloned from the base roles – as long as you cloned these roles originally from the parent base default roles.

Cloning a Role that is not Associated with a Company

In addition to cloning the main base roles for each company, you should also clone a role that is *not* associated with a Company which will allow you to assign a role for those users that need access to multiple clients (such as an HR Administrator for multiple franchises).

By creating a Role that is NOT associated with a Company, allows you to assign a Role for those users that need access to multiple clients (such as an HR Administrator for multiple franchises).

Go to **HR Admin-Security-Maintenance-Roles**:



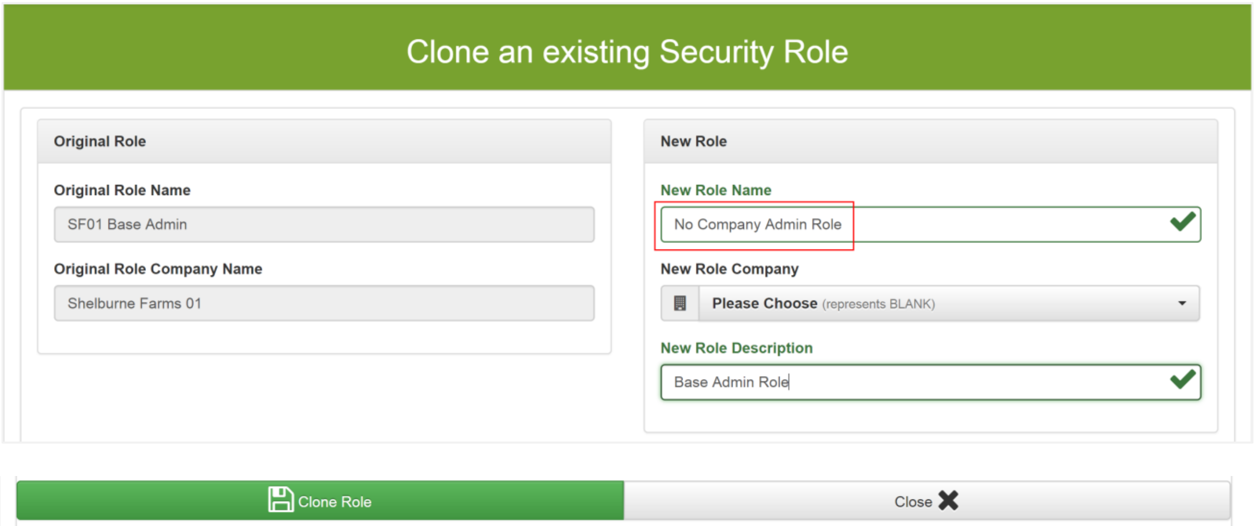
Security Role List

Actions	Company	Name	Description	Role Level	Base Role	Employee Filtering Rule
	Shelburne Farms 01	SF01 Base Admin	Base Admin Role	Admin	BaseAdmin	
	Shelburne Farms 01	SF01 Base Manager	Base Manager Role	Manager	BaseManager	
	Shelburne Farms 01	SF01 Base User	Base User Role	All	BaseUser	
	Shelburne Farms 02	SF02 Base Admin	Admin Role	Admin	BaseAdmin	
	Shelburne Farms 02	SF02 Base Manager	Manager Role	Manager	BaseManager	

Let's clone a non-associated Admin Role. Click on the green Plus Sign to clone the Base Admin Role.

To clone a role that is not associated to a company:

1. Go to **HR Admin-Security-Maintenance-Roles**:
2. Click on the green Plus Sign icon to clone the Base Admin Role.

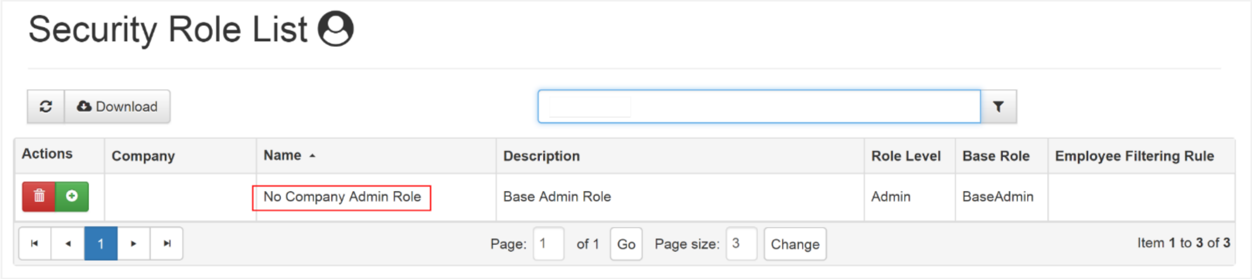


Clone an existing Security Role

Original Role	
Original Role Name	SF01 Base Admin
Original Role Company Name	Shelburne Farms 01

New Role	
New Role Name	No Company Admin Role ✓
New Role Company	Please Choose (represents BLANK)
New Role Description	Base Admin Role ✓

3. Name the Role accordingly. It will be important that you know that the Role is *not* associated with a company and that you know what level the Role is. Click **Clone Role** when complete.



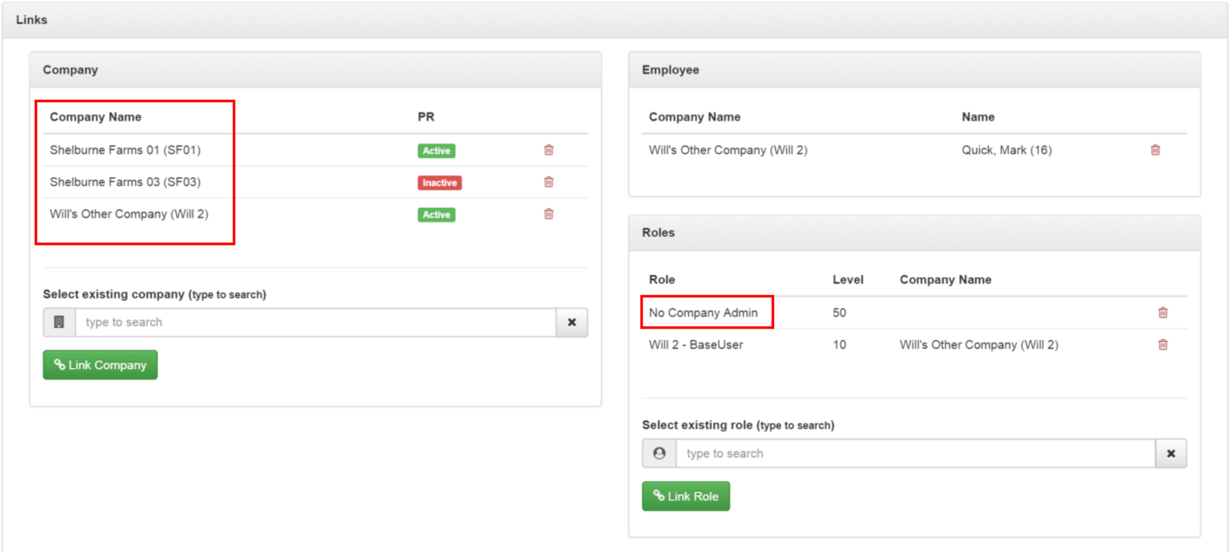
Security Role List

Actions	Company	Name	Description	Role Level	Base Role	Employee Filtering Rule
		No Company Admin Role	Base Admin Role	Admin	BaseAdmin	

Page: 1 of 1 Go Page size: 3 Change Item 1 to 3 of 3

For the end user who is assigned this role, they will be able to access multiple companies within Advanced HR 2.0. However, since this role is not associated with a company, companies need to be assigned in the **User List** screen. Go to **HR Admin - Company - User List**.

Select a user and scroll down to the **Links** section. In the **Company** section, link the Company and in the **Roles** section, link this role - **No Company Admin Role** in this example:



Links

Company

Company Name	PR	
Shelburne Farms 01 (SF01)	Active	
Shelburne Farms 03 (SF03)	Inactive	
Will's Other Company (Will 2)	Active	

Select existing company (type to search)

type to search

Employee

Company Name	Name	
Will's Other Company (Will 2)	Quick, Mark (16)	

Roles

Role	Level	Company Name	
No Company Admin	50		
Will 2 - BaseUser	10	Will's Other Company (Will 2)	

Select existing role (type to search)

type to search

Now this Role has been assigned to a user so they can have Admin Level access to multiple companies.

Assigning a Security Role to a User

The security roles you just cloned for the company are now available to assign to a user. There are different methods you can use to assign a role to a user. Typically, however, you assign a role to a user with the **User List** screen where you can also tie them to any company to which the currently logged in user can access.

User Creation is a Two-Step Process:

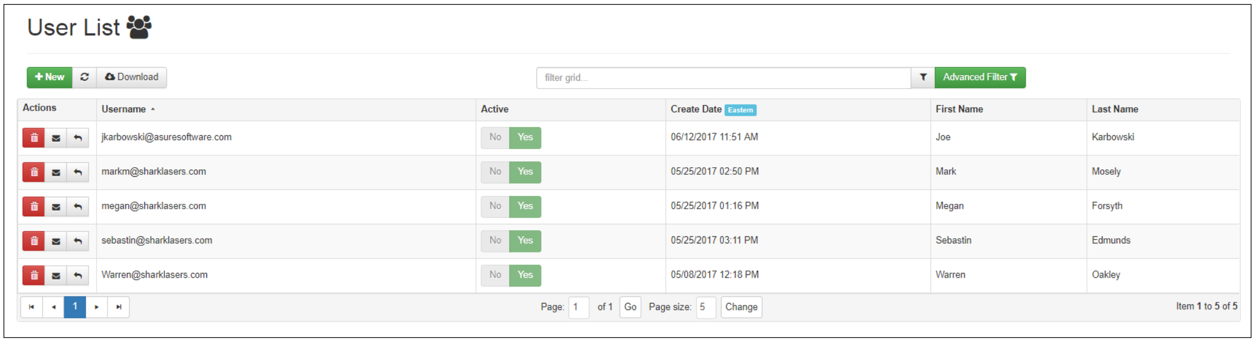
1. Create the user
2. Assign the user a role

Note: You must be an SB Admin or a Super Admin to assign a role to a user.

The person you want to assign the role for must have already been added to Advanced HR as a user in the system.

To assign a role to a (new) user:

1. Go to **HR Admin – Company – User List**. Select the company if you haven't already done so.

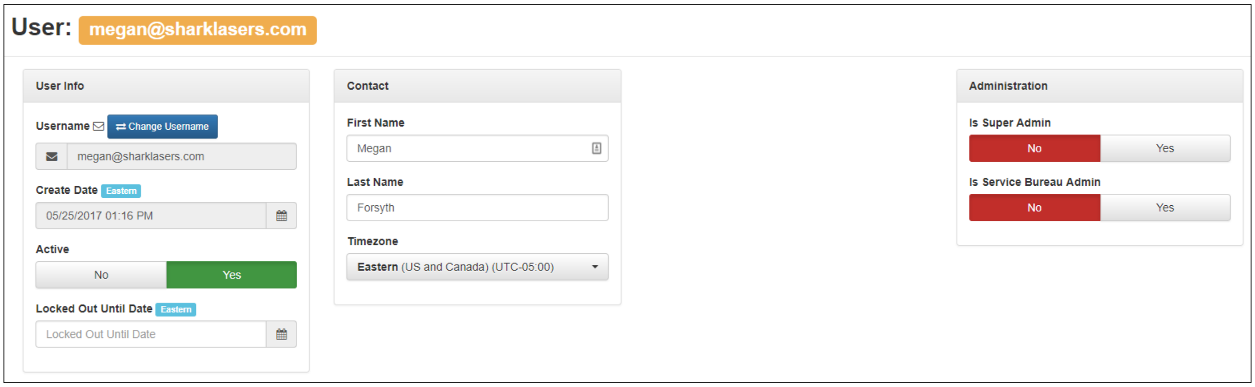


User List

Actions	Username	Active	Create Date Eastern	First Name	Last Name
	jkarbowski@asuresoftware.com	No Yes	06/12/2017 11:51 AM	Joe	Karbowski
	markm@sharklasers.com	No Yes	05/25/2017 02:50 PM	Mark	Mosely
	megan@sharklasers.com	No Yes	05/25/2017 01:16 PM	Megan	Forsyth
	sebastin@sharklasers.com	No Yes	05/25/2017 03:11 PM	Sebastin	Edmunds
	Warren@sharklasers.com	No Yes	05/08/2017 12:18 PM	Warren	Oakley

Page: 1 of 1 Go Page size: 5 Change Item 1 to 5 of 5

2. Click on the row for the user for whom you want to assign a role. For example, **Megan Forsyth**.



User: megan@sharklasers.com

User Info

Username: megan@sharklasers.com

Create Date Eastern: 05/25/2017 01:16 PM

Active: No [✓ Yes]

Locked Out Until Date Eastern: Locked Out Until Date

Contact

First Name: Megan

Last Name: Forsyth

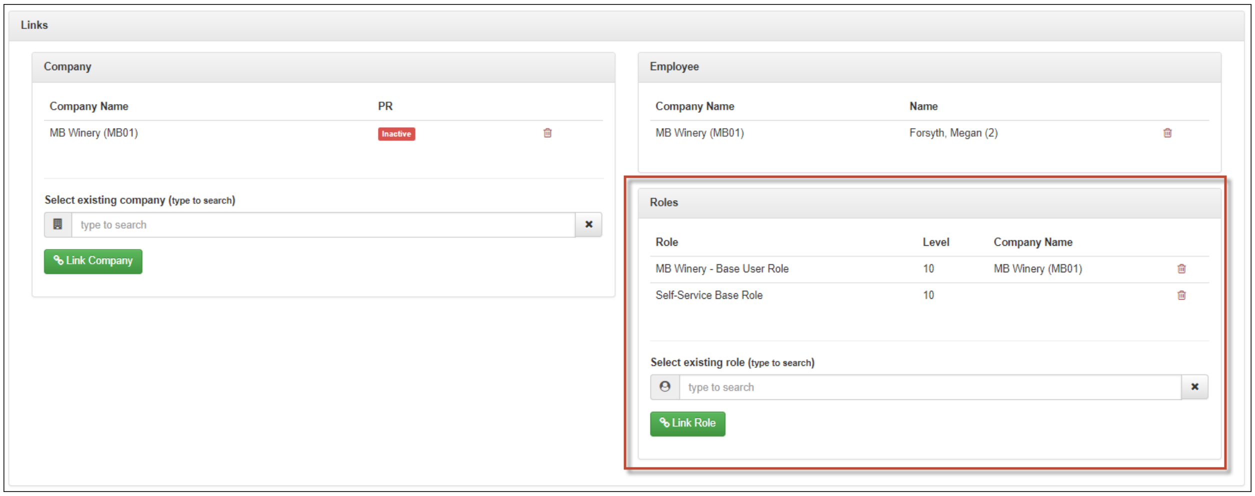
Timezone: Eastern (US and Canada) (UTC-05:00)

Administration

Is Super Admin: [✓ No] Yes

Is Service Bureau Admin: [✓ No] Yes

The system displays the Details section of the **User List** screen. Scroll down to the **Links** section of the screen, shown in the following screenshot.



Links

Company

Company Name	PR
MB Winery (MB01)	Inactive

Select existing company (type to search): type to search

Employee

Company Name	Name
MB Winery (MB01)	Forsyth, Megan (2)

Roles

Role	Level	Company Name
MB Winery - Base User Role	10	MB Winery (MB01)
Self-Service Base Role	10	

Select existing role (type to search): type to search

It is here that you can link a Role or Roles to a User. You can also link the user to a company(s) as well.

You can see in this example, in the **Company** section of the User List screen on the left side, Megan has already been linked to the company, **MB Winery**. If she had not been already assigned to the company, you could select the company from the **Select existing Company** dropdown list and click the **Link**

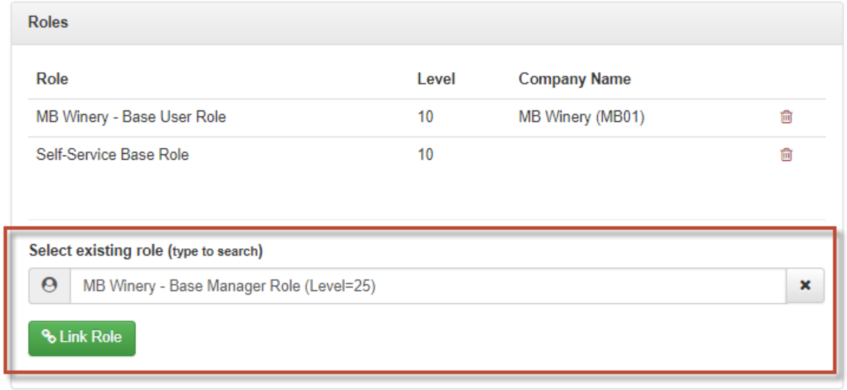
Company button

.

The right side of the User List screen, in the **Roles** section, is where you can assign a role(s) to a user. To assign a role, select an existing role (one of the roles you cloned from the default base roles) from the **Select an existing role** dropdown and then click the **Link Role** button

.

In the example above, Megan had already been assigned the Base User role. However, you could also assign her to the Base Manager role as shown in the following screenshot, by selecting the Base Manager role in the dropdown and clicking the **Link Role** button.



Roles

Role	Level	Company Name
MB Winery - Base User Role	10	MB Winery (MB01)
Self-Service Base Role	10	

Select existing role (type to search)

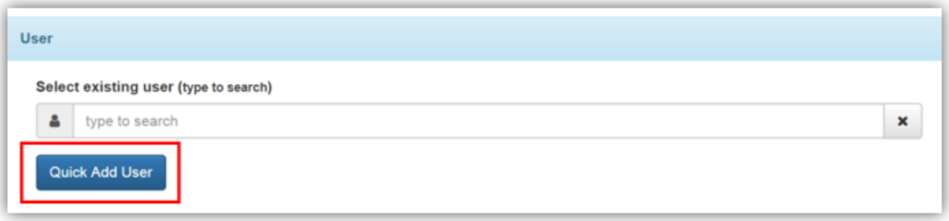
MB Winery - Base Manager Role (Level=25)

Don’t forget to click the **Save Changes** button.

The Quick Add User Feature

The Quick Add User function appears in multiple screens:

- Add New Hire
- Onboarding Prep
- Any Employee Summary screen



User

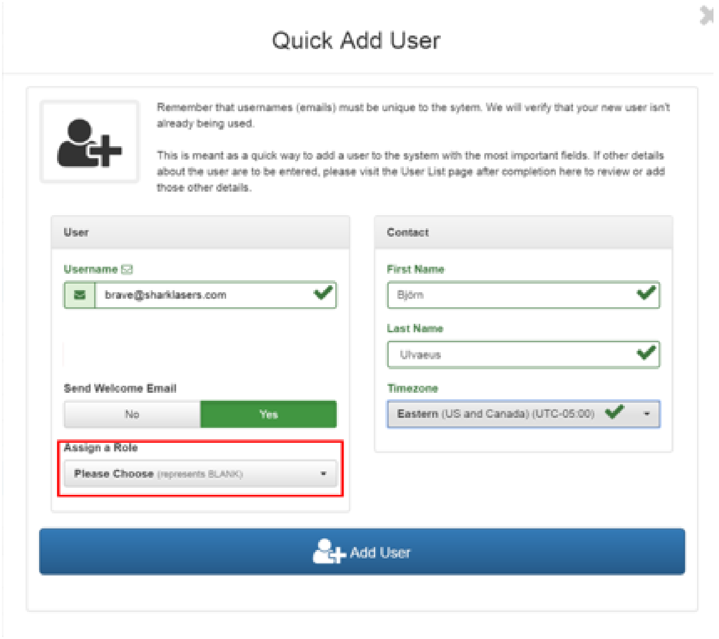
Select existing user (type to search)

type to search

It is highly recommended that you include this in your workflow. It’s purpose is to allow you to create a User, assign them to a Company, and assign a Security Role, quickly and efficiently.

The **Quick Add User** popup allows you to add a user to the system with the most important fields:

- Create Username
- Edit Contact info
- Send a Welcome Email
- Assign a Role



Quick Add User

Remember that usernames (emails) must be unique to the sytem. We will verify that your new user isn't already being used.

This is meant as a quick way to add a user to the system with the most important fields. If other details about the user are to be entered, please visit the User List page after completion here to review or add those other details.

User

Username: brave@sharklasers.com

Send Welcome Email: No [✓ Yes]

Assign a Role: Please Choose (represents BLANK)

Contact

First Name: Björn

Last Name: Ulvaeus

Timezone: Eastern (US and Canada) (UTC-05:00)

- **Assign a Role**

  In this field you can see the Roles that are associated with this company. This will allow the user a level of access to the system that is dependent on their function within the company.

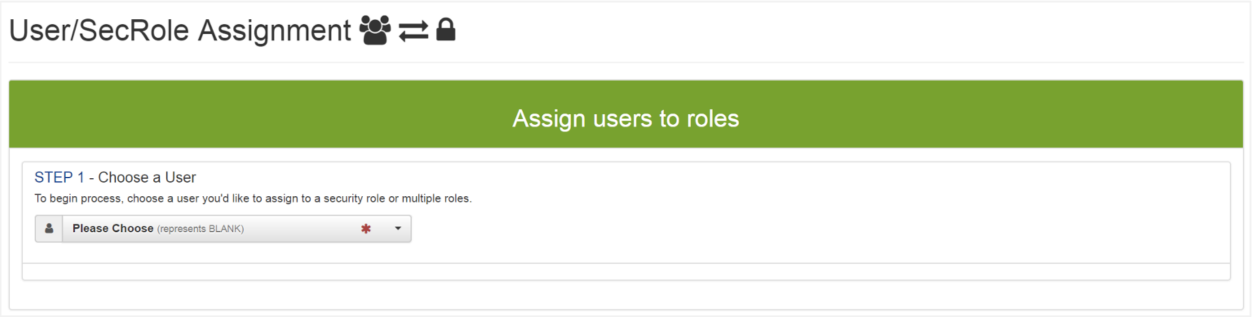
  In addition you can **Send a Welcome Email**. The Welcome Email will instruct the new hire how to access Self Serve Onboarding. Self Service Onboarding will be covered in the Applicant Tracking training guide.

Click the blue **Add User** button when complete.

Note: Remember that usernames (emails) must be unique to the system. Advanced HR 2.0 will verify that the new username is not already being used. **Quick User Add** is meant as a quick way to add a user to the system with the most important fields. If other details about the user are to be entered, go to the **Company - User List** screen after completion to review or add other details.

Another Method to Assign a User to a Role

You can also assign users to a role with the **HR Admin – Security – Maintenance – Assign Users to Roles** screen, although this method is less typically used than the one noted above (**User List** screen).



User/SecRole Assignment

Assign users to roles

STEP 1 - Choose a User

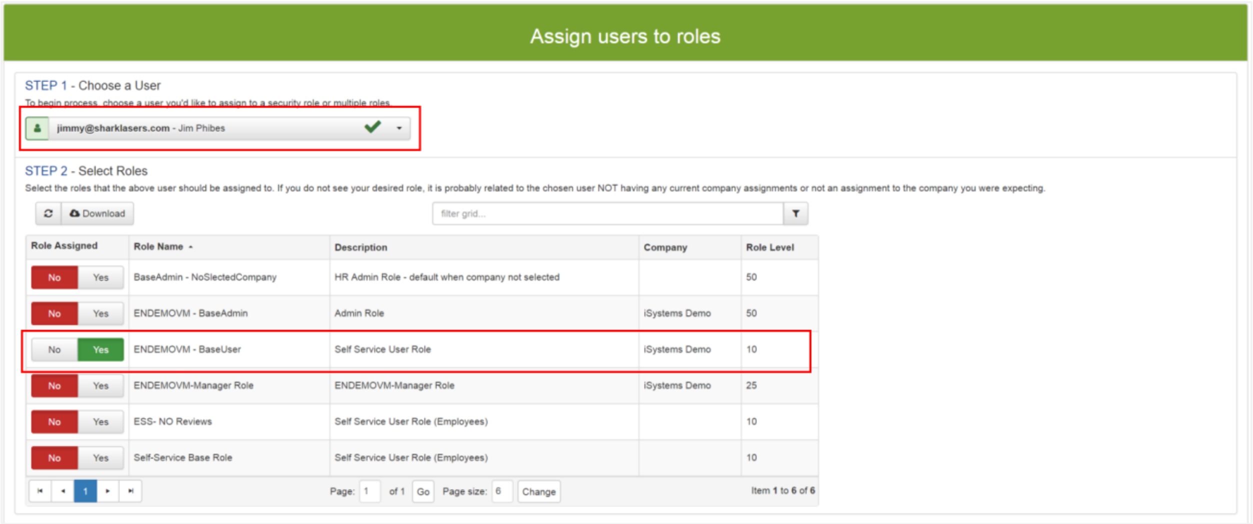
To begin process, choose a user you'd like to assign to a security role or multiple roles.

Please Choose (represents BLANK)

Select the user from the drop down list. The drop down list will display all the users in the system. Of course, it’s important to remember that unless you are signed in as a **Super Admin**, or a **SB Admin**, you won’t be able to use this feature.

When you select the user:

- You will see a list of the available **User Roles** that are currently available for the user and the company.
- Using the **Yes/No toggles**, select the desired Role(s).
- Users can have multiple Roles.



Assign users to roles

STEP 1 - Choose a User

To begin process, choose a user you'd like to assign to a security role or multiple roles.

jimmy@sharklasers.com - Jim Phibes ✓

STEP 2 - Select Roles

Select the roles that the above user should be assigned to. If you do not see your desired role, it is probably related to the chosen user NOT having any current company assignments or not an assignment to the company you were expecting.

Role Assigned	Role Name	Description	Company	Role Level
[✓ No] Yes	BaseAdmin - NoSlectedCompany	HR Admin Role - default when company not selected		50
[✓ No] Yes	ENDEMOVM - BaseAdmin	Admin Role	iSystems Demo	50
No [✓ Yes]	ENDEMOVM - BaseUser	Self Service User Role	iSystems Demo	10
[✓ No] Yes	ENDEMOVM-Manager Role	ENDEMOVM-Manager Role	iSystems Demo	25
[✓ No] Yes	ESS- NO Reviews	Self Service User Role (Employees)		10
[✓ No] Yes	Self-Service Base Role	Self Service User Role (Employees)		10

Note that in the example above, our user, Jim Phibes, is assigned a **Base User** Role. Because of this status, this user will have access to the **My HR** menu tab functionality only. In other words, when they log in, they will be able to see their own information only.

Select the **Role(s)** that the User should be assigned to. If you do not see a desired role, this could be due to the chosen user not having any current company assignments and/or not an assignment to the company you were viewing.

When Terminating an Employee

Note: After Terminating the employee, remember to adjust their **User Security Role** accordingly. Go to **HR Admin – Company – User List**. Click on the user. If, for example, they were a **Base Manager**, that level should be removed so they only have access as a **Base User**. If you choose, you can also **delete** or make them **inactive** as a user.

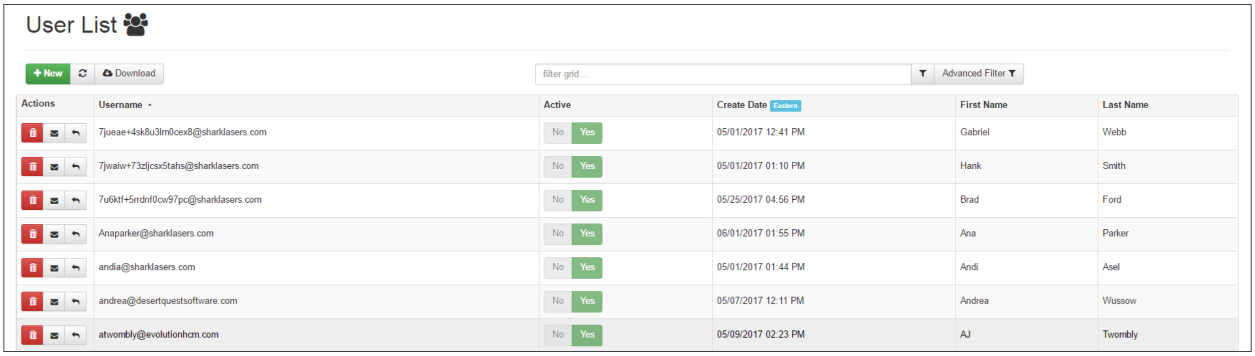
Associating a User to Another Company

Users may need to be associated to more than one company. If you need to associate a user to another company, follow these steps:

User List Screen

Each company will have a list of Users. As a **Base Admin** level or higher, you will have access to this list. First, view the company to which an existing user is currently assigned.

1. Go to **HR Admin – Company – User List**.
2. The system displays the **User List** screen. If no company has been selected, when you click on the User List, you will see a list of all Users that are in your assigned companies. If, on the other hand, you have selected a particular company, you'll see a list of Users for that company only.



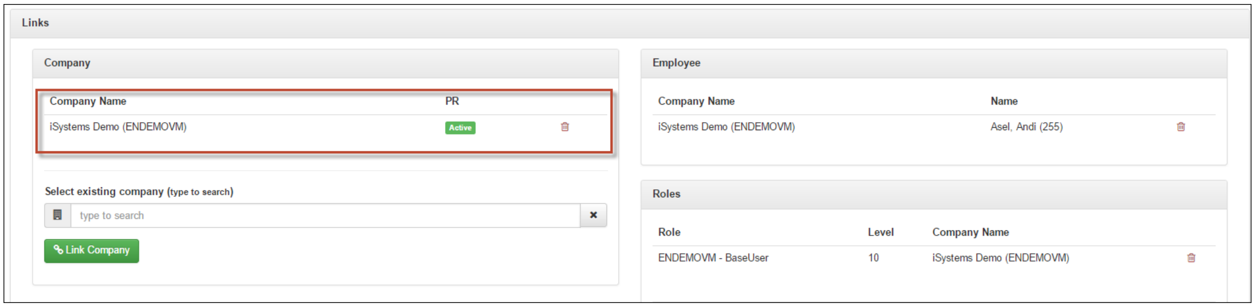
Actions	Username	Active	Create Date Eastern	First Name	Last Name
	7jueae+4sk8u3lm0cex8@sharklasers.com	No Yes	05/01/2017 12:41 PM	Gabriel	Webb
	7jwaiw+73zljcsx5tahs@sharklasers.com	No Yes	05/01/2017 01:10 PM	Hank	Smith
	7u6ktf+5rrdnf0cw97pc@sharklasers.com	No Yes	05/25/2017 04:56 PM	Brad	Ford
	Anaparker@sharklasers.com	No Yes	06/01/2017 01:55 PM	Ana	Parker
	andia@sharklasers.com	No Yes	05/01/2017 01:44 PM	Andi	Asel
	andrea@desertquestsoftware.com	No Yes	05/07/2017 12:11 PM	Andrea	Wussow
	atwombly@evolutionhcm.com	No Yes	05/09/2017 02:23 PM	AJ	Twombly

User List screen

By using the buttons in the **Actions** column, you can do the following tasks:

- Create a **New** User.
- **Delete** a User (not recommended – make them inactive instead).
- Send a **Welcome Email** to a new User with details how they can access Advanced HR 2.0.
- **Reset** a User's password.
- Access a particular User's security and access information.

3. Click on the user to which you want to associate another company with. Scroll down to the **Links** section of the **User List** screen and observe the **Company** section.



Links

Company

Company Name	PR
iSystems Demo (ENDEMOVM)	Active

Select existing company (type to search)

type to search

Link Company

Employee

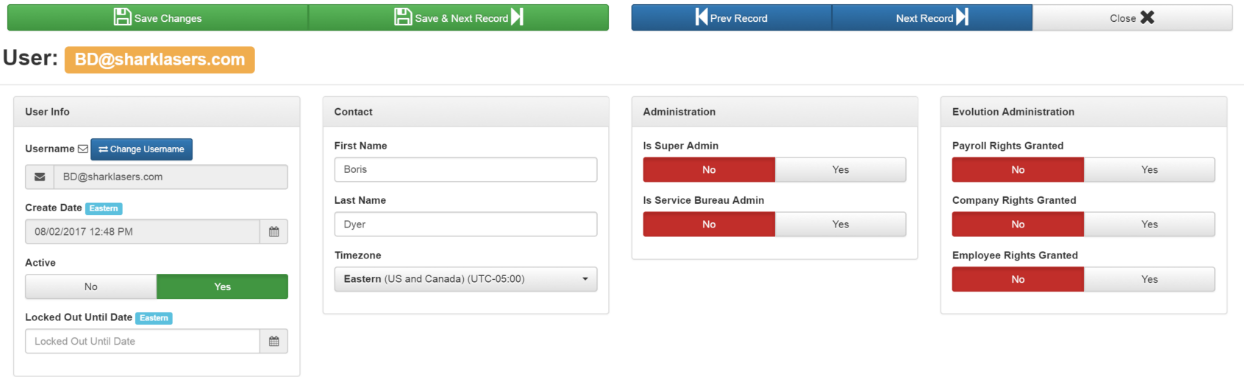
Company Name	Name
iSystems Demo (ENDEMOVM)	Asel, Andi (255)

Roles

Role	Level	Company Name
ENDEMOVM - BaseUser	10	iSystems Demo (ENDEMOVM)

When you click on the User's name you will see and be able to edit:

- **Username** and **Active/Inactive** status.
- **Contact** information.
- Assign access to **Evolution Payroll -** you can assign them Evolution access in the **Evolution Administration** section shown below. This access corresponds to the **AHR 2 Security Group** in Evolution Classic.
- Company **Links**.
- Assigned **Roles**.



User: BD@sharklasers.com

User Info

Username

BD@sharklasers.com

Create Date Eastern

08/02/2017 12:48 PM

Active: No [✓ Yes]

Locked Out Until Date Eastern

Locked Out Until Date

Contact

First Name: Boris

Last Name: Dyer

Timezone: Eastern (US and Canada) (UTC-05:00)

Administration

Is Super Admin: [✓ No] Yes

Is Service Bureau Admin: [✓ No] Yes

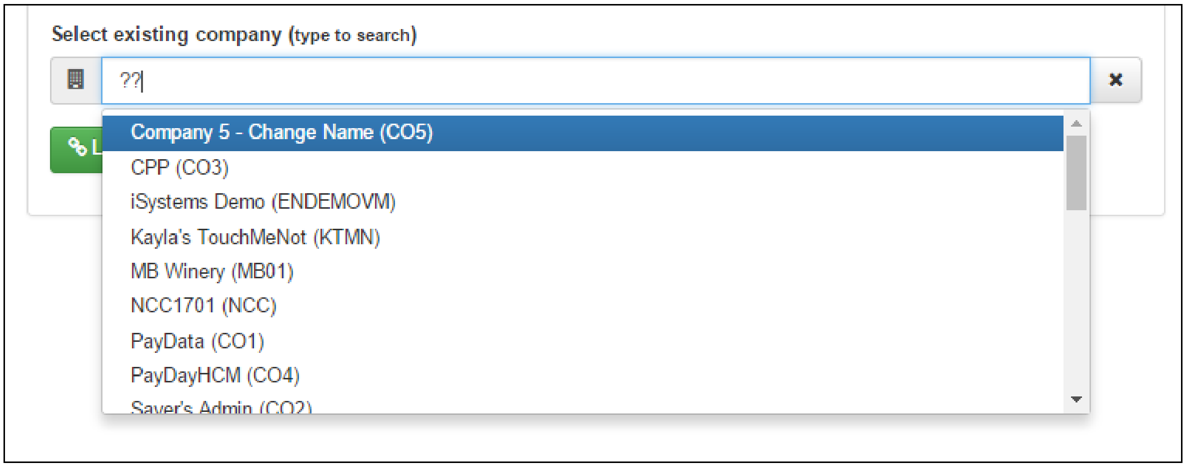
Evolution Administration

Payroll Rights Granted: [✓ No] Yes

Company Rights Granted: [✓ No] Yes

Employee Rights Granted: [✓ No] Yes

4. You can see this user is associated with the iSystems Demo company. To associate the user with another company, in the **Select existing company** field, select the different company from the dropdown list. You can type in a double question mark (**??**) which will make the company list pop up.



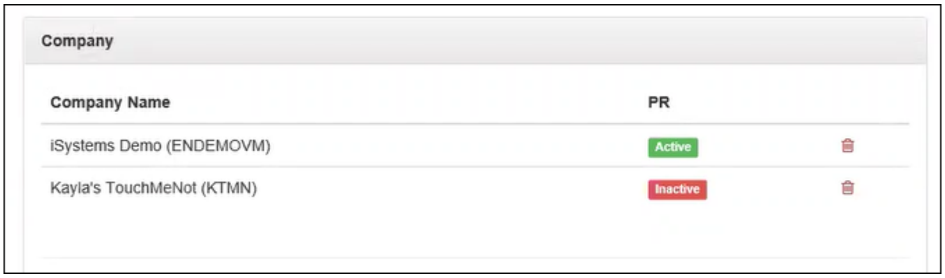
Select existing company (type to search)

??

Company 5 - Change Name (CO5)
CPP (CO3)
iSystems Demo (ENDEMOVM)
Kayla's TouchMeNot (KTMN)
MB Winery (MB01)
NCC1701 (NCC)
PayData (CO1)
PayDayHCM (CO4)
Sayer's Admin (CO2)

5. Once you select the company, click on the **Link Company** button to link the user to that (additional) company.

For example, we associated a user to two different companies. We displayed the User List screen for that user and now see the following on the **User List** screen. The user is associated with two companies: **iSystems Demo** and **Kayla's TouchMeNot.**



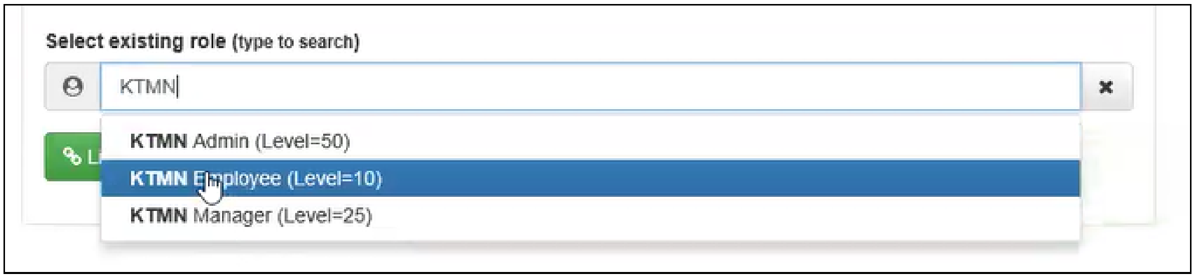
Company

Company Name	PR	
iSystems Demo (ENDEMOVM)	Active	🗑
Kayla's TouchMeNot (KTMN)	Inactive	🗑

When this user logs in, they can switch between the two companies. But remember, you also need to assign a corresponding role for the person for the new company you just assigned them to.

Assign a Corresponding Role for the User for the New Company

In the **Select existing role** field,

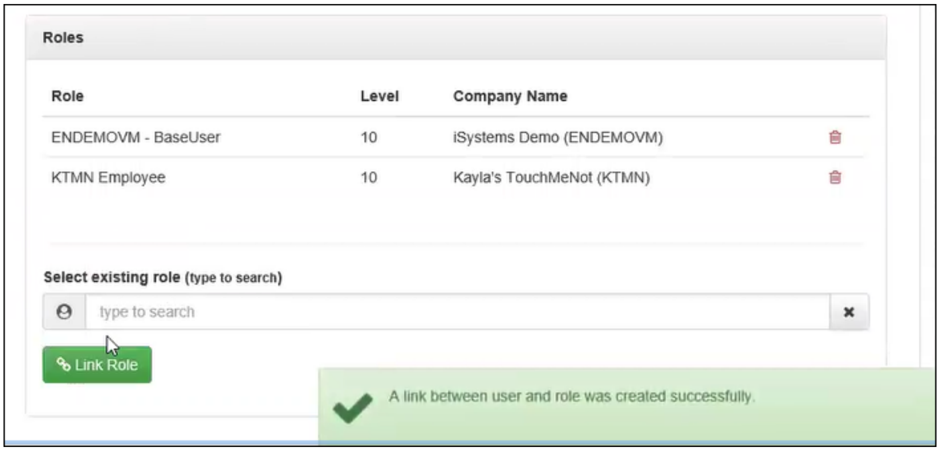


Select existing role (type to search)

KTMN

KTMN Admin (Level=50)
KTMN Employee (Level=10)
KTMN Manager (Level=25)

Select the role and then click the **Link Role** button.



Roles

Role	Level	Company Name
ENDEMOVM - BaseUser	10	iSystems Demo (ENDEMOVM)
KTMN Employee	10	Kayla's TouchMeNot (KTMN)

Select existing role (type to search)

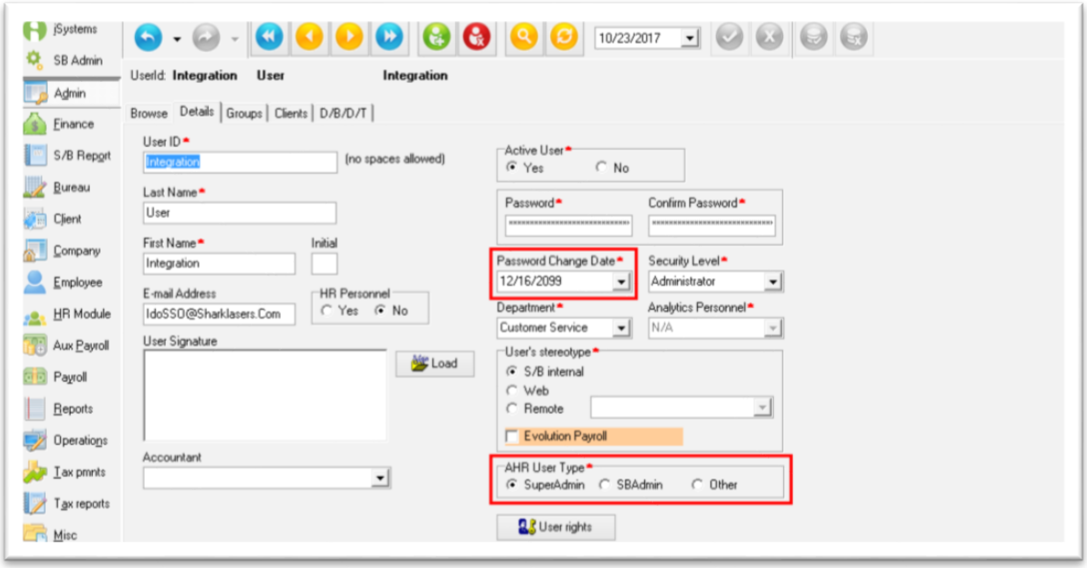
type to search

A link between user and role was created successfully.

Now, when the user switches between companies, they will have the corresponding role for each company that you set up for them.

Service Account User

The **Service Account User** is a non-user account in Evolution Classic for the purpose of enabling Evolution Single Sign On access. Service Accounts are best created by users who have full access to Evolution Classic. This account should be set to **Full Access**. Refer to the *Advanced HR 2.0 Single Sign On Guide* for information about how to create a Service Account User.



UserId: Integration User Integration

User ID*: Integration (no spaces allowed)
Last Name*: User
First Name*: Integration
Initial:
E-mail Address: IdoSSO@Sharklasers.Com
HR Personnel: ○ Yes ● No
User Signature:
Accountant:

Active User*: ● Yes ○ No
Password*: ****************************
Confirm Password*: ****************************
Password Change Date*: 12/16/2099
Security Level*: Administrator
Department*: Customer Service
Analytics Personnel*: N/A
User's stereotype*: ● S/B internal ○ Web ○ Remote
☐ Evolution Payroll
AHR User Type*: ● SuperAdmin ○ SBAdmin ○ Other

Note that if the Service Account User becomes locked at any time this will impact your ability to log in with Evolution Single Sign On.

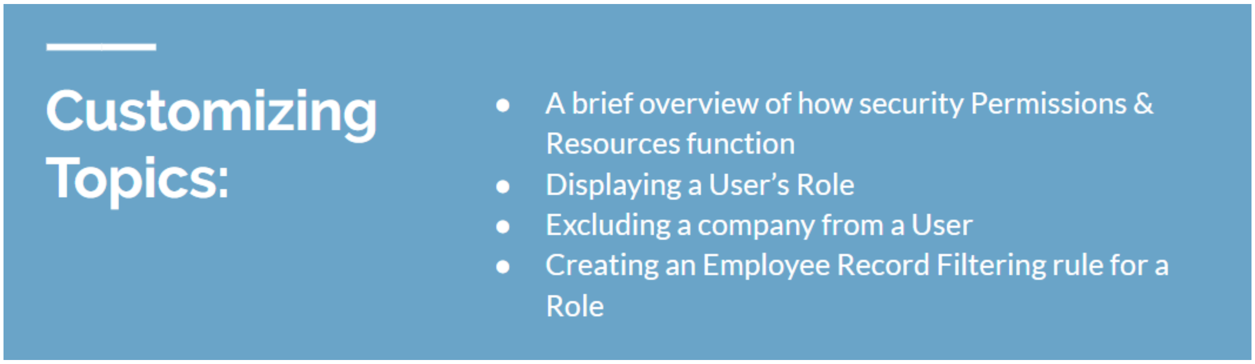
This is why the account is not a person and SHOULD NEVER BE CHANGED in any way after its been created.

Customizing Security Settings

The default security settings initially set up for a company, described in the previous section of this guide, should be sufficient for the roles a company requires. Advanced HR 2.0, however, does provide administrators with the ability to customize the security settings if you have a client with additional special or unique requirements.

Advanced HR 2.0 has 4 default Security Roles that are sufficient to cover the permissions for end users: employees, managers, and administrators. However, there are cases where a company may need to deviate from these default permissions for end users. For example, users may require less or more access to information depending on their job role within the company.

Customizing any security role is an involved process, however. This should only be done after the Service Bureau becomes familiar with Advanced HR 2.0. In addition, no customizing should take place without the Asure Software Implementation Team's input. This section of the guide describes:



Customizing Topics:

- A brief overview of how security Permissions & Resources function
- Displaying a User's Role
- Excluding a company from a User
- Creating an Employee Record Filtering rule for a Role

Note: It is highly recommended that before you begin to customize any roles or permissions, please contact our Implementation Team. For detailed information, you can also refer to the *Advanced HR 2.0 Customizing Security Roles/ Users Guide*, and the *Customizing Security Roles Training Guide* which can both be found on the **Evolution Resource Center**.

Permissions Overview

In Advanced HR 2.0, every clickable item in the system is known as a **Resource**. The default security roles allow different levels of access to these resources. To change a security role to restrict or allow access to a resource, the service bureau will need to set the **Permissions** on the resource itself.

Permissions allow the Service Bureau Admin or the Super Admin user to set security authorization for different Resource functionality. Advanced HR 2.0 comes by default with thousands of Permissions right out of the box.

It's important to be aware that Permissions functionality to resources can be:

- Role based and/or
- User based

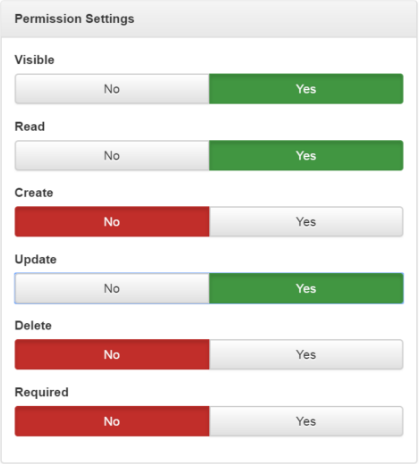
Note: Permissions will always override **Resources**. The system looks to the Permissions first before considering the user’s role and resources.

It’s important to note that if the permission to a **Form** type resource is disabled for a role/user, but the corresponding **Menu Item** permission is not, the role/user will be able to see the Menu Item. However, they will not be able to access it. Hence, the fields and buttons within the form are disabled too since the role/user is unable to get into the form. This means that the Form type permission takes precedence over Menu Item, Database, and the Control types.

When the Form type resource is disabled, then the role/user will not have access to the screen. Similarly, if a Form type is enabled for a role/user, but its corresponding Menu Item type is disabled, the role/user can still get to the form by directly entering the URL to the form (if the URL is known to the user). Therefore, it is best practice to ensure that when customizing roles, you disable/enable both the Form and the Menu Item.

Example

Let’s consider an example. Assume that there are system values that define Absence Types (this is not an actual screen, just used as an example). Perhaps you would like your Base Admin role (Base Admin) to have access to Absence Types. However, you only want them to be able to update, and not have the ability create or delete Absence Types. The following screenshot is an example of how you would use permissions to control access to the Absence Types by setting the **Yes/No** toggles.



Permission Settings

Visible
No [✓ Yes]

Read
No [✓ Yes]

Create
[✓ No] Yes

Update
No [✓ Yes]

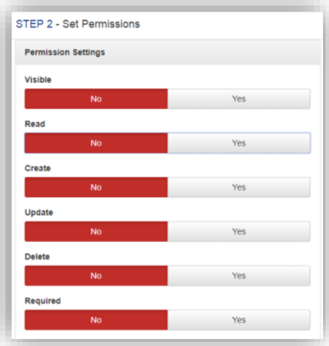
Delete
[✓ No] Yes

Required
[✓ No] Yes

You can see in this example that any user who is assigned this role can view and update the Absence Types for employees, but will not be able to create or delete an absence type or make it a required field.

Note: What is the difference between **Visible** and **Read**? **Visible** will allow the user to actually see the menu item. **Read** will allow the user to click on it and open it. Of course, combining this with **Update** will allow for editing.

If the goal is to disable a role from seeing the Form Type completely, you would set all the **Permission Settings** to **No** and then **Save**. That Form would then be disabled for that role.



STEP 2 - Set Permissions

Permission Settings

Visible
No | Yes

Read
No | Yes

Create
No | Yes

Update
No | Yes

Delete
No | Yes

Required
No | Yes

Note that Permissions set in Advanced HR 2.0 do not impact the user's experience in Evolution Payroll.

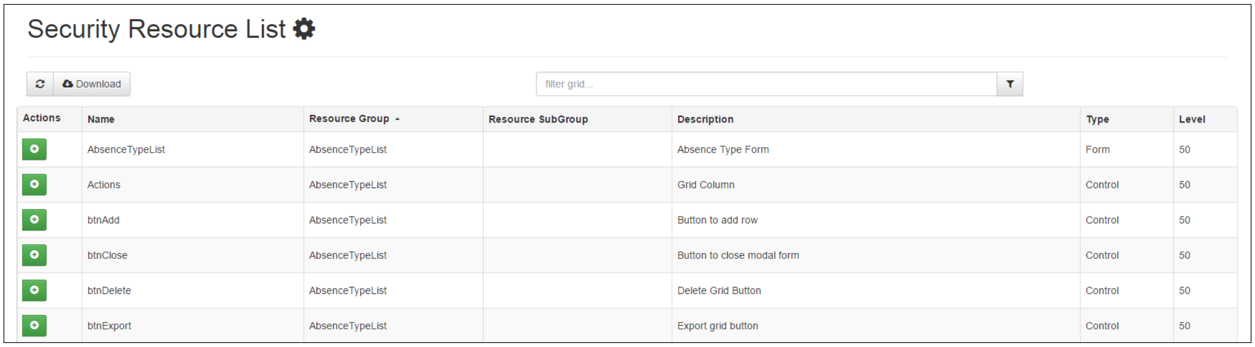
Resources Overview

In Advanced HR 2.0, every clickable item in the system is known as a **Resource**. The default security roles allow different levels of access to these resources. To change a security role to restrict or to allow access to a Resource, the service bureau will need to set the Permission on the Resource itself.

Resources are what the user is giving Permissions to.

Note: It is possible for a Super Admin or a Service Bureau Admin to change the security level of a Resource. However, this is NOT recommended. As stated previously, there are over 4,900 Resources in the system. These Resources touch everything from a Refresh button on an Absentee List to the ability to perform a Payroll Data Cutover. It is very important to use the Resources defaults, adding or limiting the Permissions as needed.

For example, while logged in as a Super Admin, go to **HR Admin – Security – Maintenance - Resources**. You will be taken to the **Security Resource List** screen.



Security Resource List

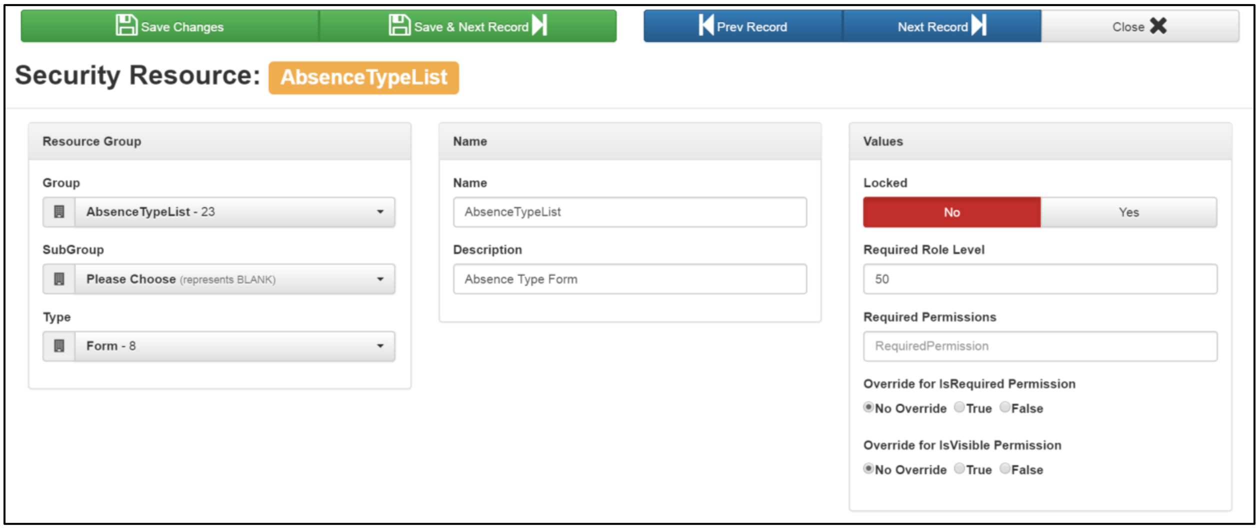
Actions	Name	Resource Group	Resource SubGroup	Description	Type	Level
●	AbsenceTypeList	AbsenceTypeList		Absence Type Form	Form	50
●	Actions	AbsenceTypeList		Grid Column	Control	50
●	btnAdd	AbsenceTypeList		Button to add row	Control	50
●	btnClose	AbsenceTypeList		Button to close modal form	Control	50
●	btnDelete	AbsenceTypeList		Delete Grid Button	Control	50
●	btnExport	AbsenceTypeList		Export grid button	Control	50

Security Resource List screen

The **Security Resource List** screen has the following column fields:

Column	Description
Actions ⊕	Allows the user to create (Add) Permissions based on a Resource and/or assign it to a Role or to a User.
Name	The name of the resource. Click on the Name to view the details of the Resource. With the detail open, the user can edit and save changes to the Resource.
Resource Group	A grouping of related Resources. For example, in the previous screen shot, Absence Type has different components that can all be edited. The resource group is typically the name of the page on which the resource appears. For example – all of the fields and controls relating to absence types are in the group "AbsenceTypeList" – which is the name of the page from the URL when accessing that page.
Resource Subgroup	Generally, this is not applicable. Sub-groups are not typically used, but are occasionally when developers find it necessary to identify different sections on the same web page, or form.
Description	The description of the resource.
Type	The type of resource it is. (**Form**, **Control**, **Database**).
Level	Which Security Role can access the Resource. For example, if the level is 25, this refers to a Base Manager. Any user with at least a Base Manager Role will be able to see/interact with this Resource.

Here is an example of opening the detail for a Resource – in this case for the Absence Type.



Security Resource: AbsenceTypeList

Resource Group

Group: AbsenceTypeList - 23

SubGroup: Please Choose (represents BLANK)

Type: Form - 8

Name

Name: AbsenceTypeList

Description: Absence Type Form

Values

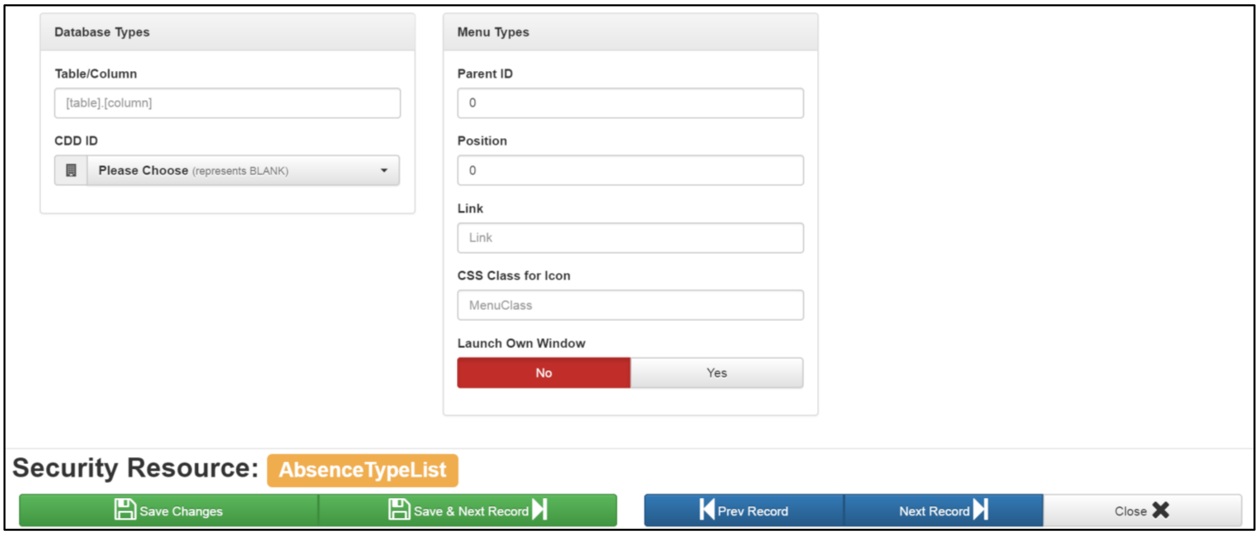
Locked: No | Yes

Required Role Level: 50

Required Permissions: RequiredPermission

Override for IsRequired Permission: ● No Override ○ True ○ False

Override for IsVisible Permission: ● No Override ○ True ○ False



Database Types

Table/Column: [table].[column]

CDD ID: Please Choose (represents BLANK)

Menu Types

Parent ID: 0

Position: 0

Link: Link

CSS Class for Icon: MenuClass

Launch Own Window: [✓ No] Yes

Security Resource: AbsenceTypeList

For more information about Permissions and Resources, see the *Security Resources* section of this guide.

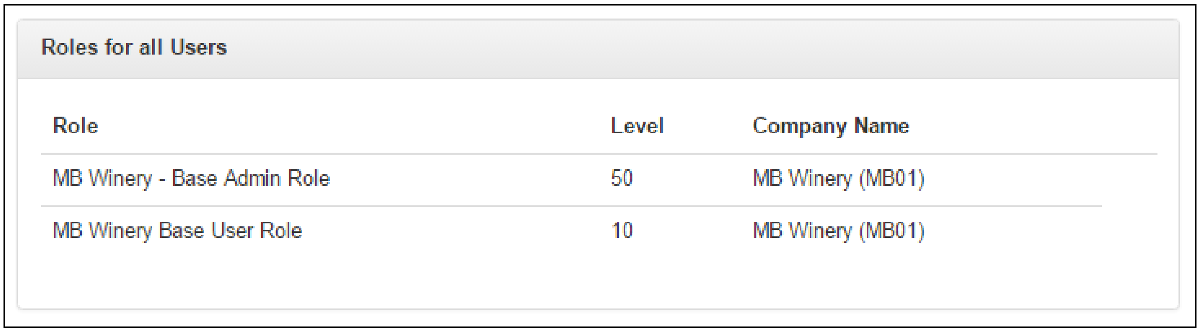
Displaying a User’s Role

You can see the role(s) that have been assigned to a user in:

- The **Employee Summary** screen
- The **User List** screen
- **Assign Users to Roles** screen (See *Appendix A* in this guide).

A User with Multiple Roles

Note that users can and should be assigned multiple roles, in the following sample **Employee Summary** screen, you can see that Sebastian Edmunds has been assigned to two roles for the MB Winery company: **Base Admin Role** and the **Base User Role**.



Roles for all Users

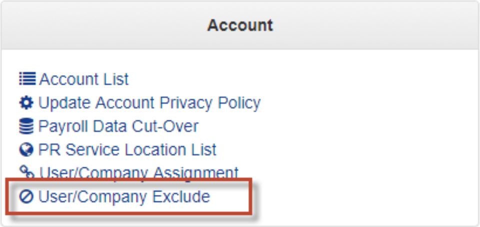
Role	Level	Company Name
MB Winery - Base Admin Role	50	MB Winery (MB01)
MB Winery Base User Role	10	MB Winery (MB01)

Excluding a Company from a User

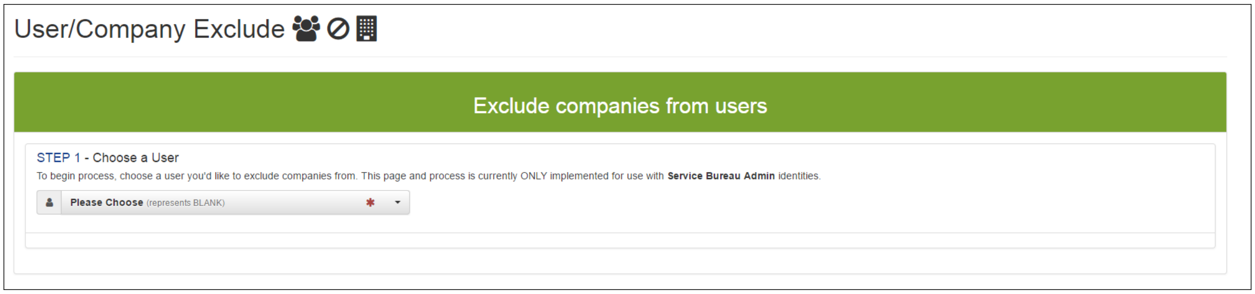
A user with the **Super Admin** role can block or exclude a user from accessing a company (or multiple companies), perhaps from a **Service Bureau Administrator**. This also might be useful to exclude a user from your internal Service Bureau company.

To exclude a company from a user:

1. Go to **HR Admin** – **Account** – **User/Company Exclude**.



2. The system displays the **Exclude Companies from Users** screen.



User/Company Exclude

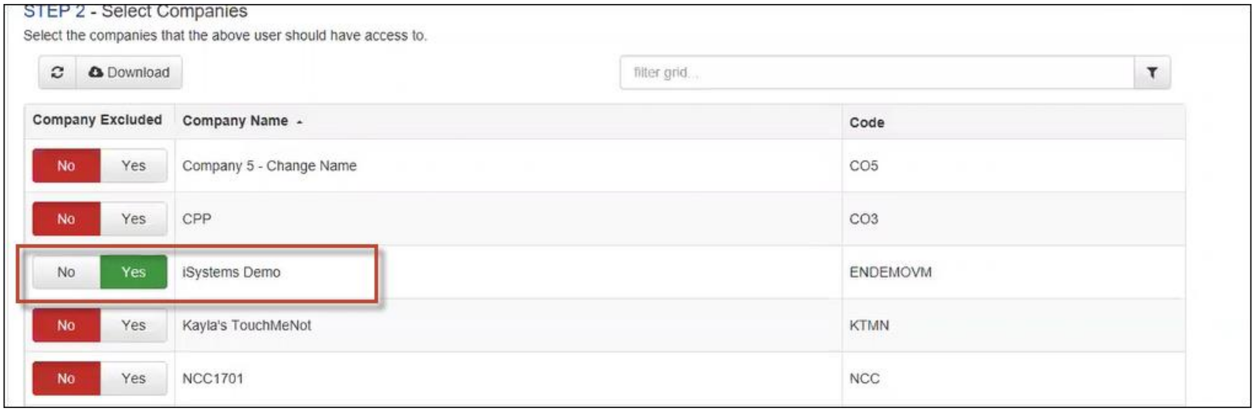
Exclude companies from users

STEP 1 - Choose a User

To begin process, choose a user you'd like to exclude companies from. This page and process is currently ONLY implemented for use with **Service Bureau Admin** identities.

Please Choose (represents BLANK) *

3. In the **Step 1 – Choose a User** section, select the user from which you want to block access to. The dropdown will list all the users, Service Bureau Administrator users in this example.
4. In the **Step 2** – **Select Companies** section, the system lists all the companies which have been onboarded and displays whether the user has access to them (the **Yes/No** toggles). For example, this user has access to the iSystems Demo company.



STEP 2 - Select Companies

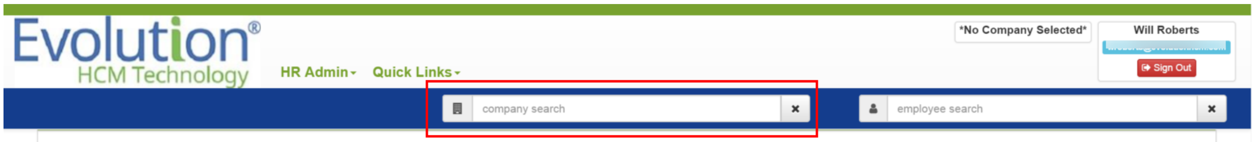
Select the companies that the above user should have access to.

Company Excluded	Company Name	Code
No Yes	Company 5 - Change Name	CO5
No Yes	CPP	CO3
No Yes	iSystems Demo	ENDEMOVM
No Yes	Kayla's TouchMeNot	KTMN
No Yes	NCC1701	NCC

5. To exclude a user from access to a company, under the **Company Excluded** column, for that company row, change the toggle switch from **Yes** to **No**.

The user will then no longer be able to log into the iSystems Demo company and also cannot view any reporting data from the company.

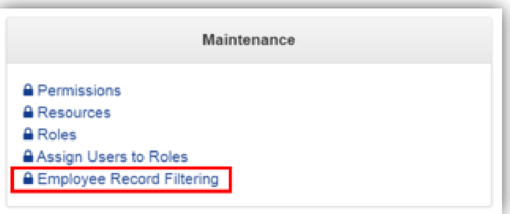
Note: If a user has access to multiple companies, they will be able to use the Company Search bar, located at the top of every screen.



Simply start typing the company name in the company search box and Advanced HR 2.0 will autocomplete the name, as long as you have access to it.

Creating an Employee Record Filtering Rule for a Role

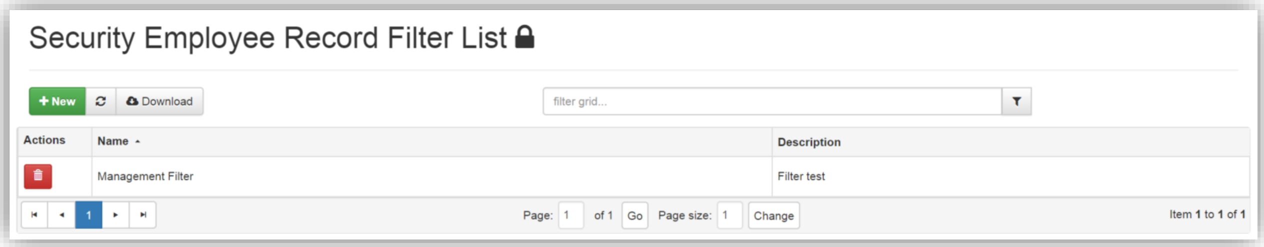
Administrators can add an Employee Record filter rule to apply for a particular role or group. For example, you may want to exclude a role's access to a specific organization (DBDT) structure, or to a specific position.



The **Employee Record Filtering** feature allows the user to add rules that can be applied to specific groups or roles.

Go to **HR Admin – Security – Maintenance - Employee Record Filtering**

The **Security Employee Record Filter List** screen displays any filters for all the companies that are attached to the Service Bureau.



Security Employee Record Filter List

+ New | Download | filter grid...

Actions	Name	Description
🗑	Management Filter	Filter test

Page: 1 of 1 Go Page size: 1 Change Item 1 to 1 of 1

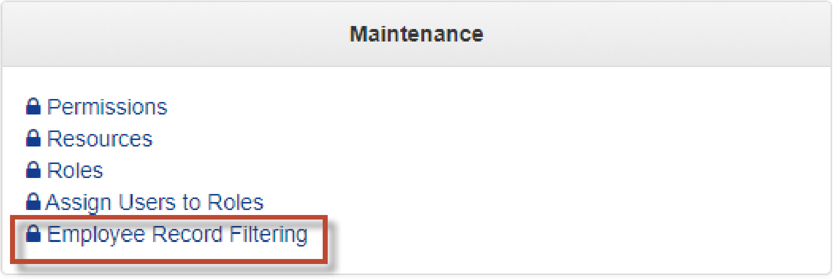
You can add a filtering rule that precludes access to specific DBDT records, and/or specific positions, and then assign that to a security role(s). So, if you don't want anyone in the ABC company in a certain Admin role to see anyone in the "Executives" team – you could create an employee filtering rule as indicated and assign it to the "ABC-HRAdmin-NoExecs" role which would be a clone of the default "ABC – Admin" role.

To do this you first create an employee record filter rule and then you apply the filter to a role. Both steps are described below.

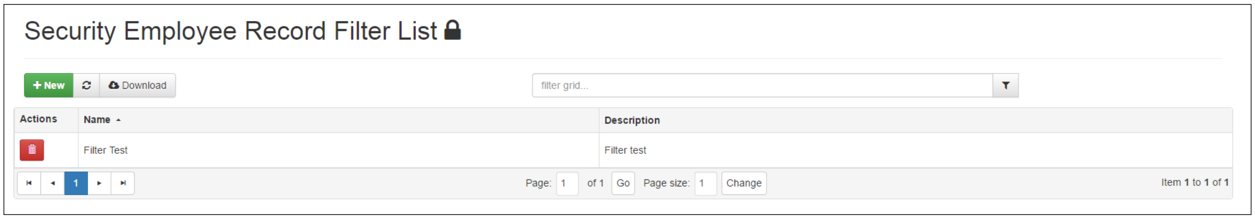
Step 1: Creating an Employee Record Filter Rule

To create a new employee record filter:

1. Go to **HR Admin – Maintenance – Employee Record Filtering**.



2. The system displays the **Security Employee Record Filter List** screen.

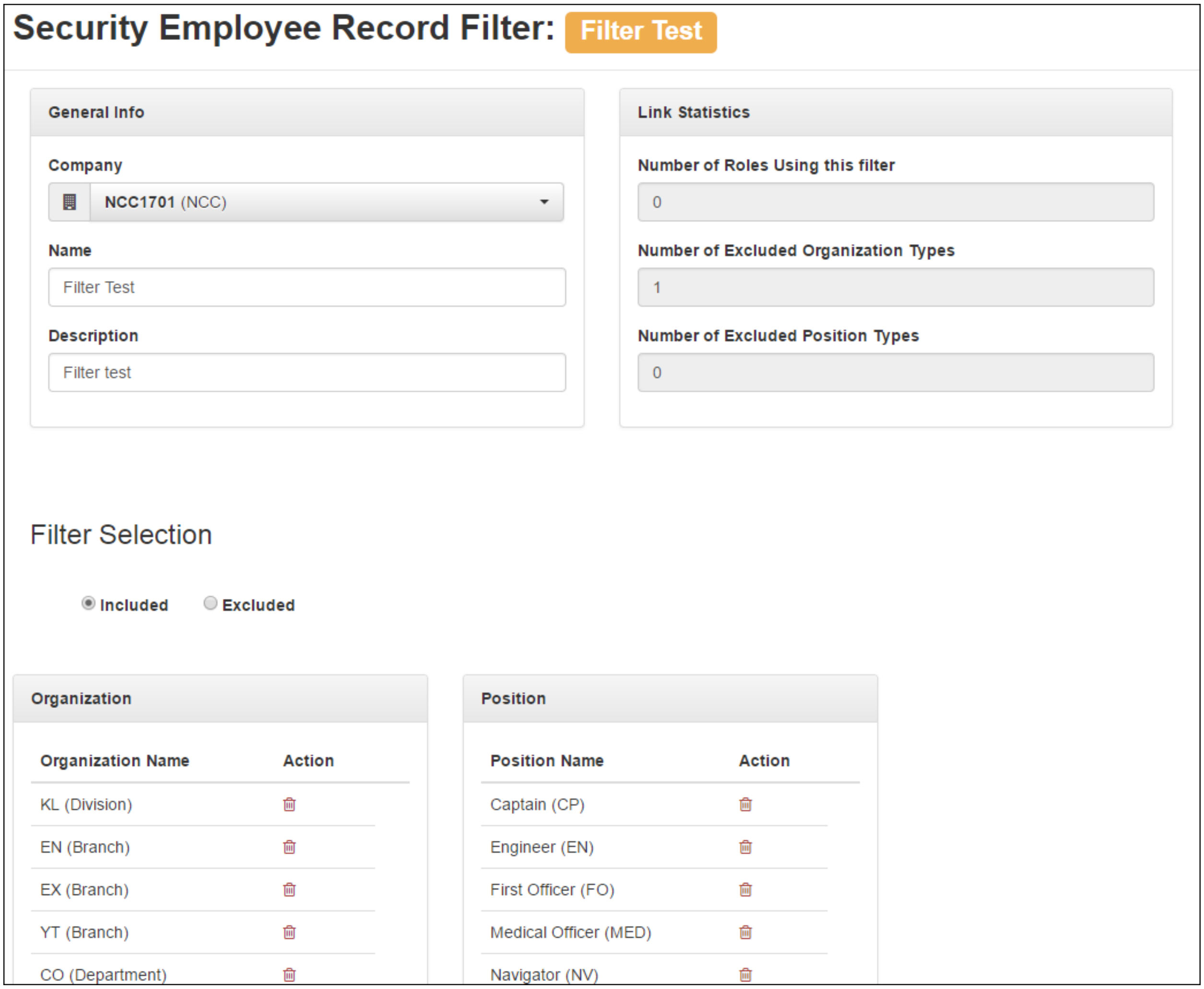


Actions	Name	Description
🗑	Filter Test	Filter test

Page: 1 of 1 Go Page size: 1 Change Item 1 to 1 of 1

3. The summary screen lists any existing employee record filters for all the companies that are attached to the Service Bureau.

4. To create a new employee record filter, click the **+ New** button.



Security Employee Record Filter: Filter Test

General Info

Company: NCC1701 (NCC)

Name: Filter Test

Description: Filter test

Link Statistics

Number of Roles Using this filter: 0

Number of Excluded Organization Types: 1

Number of Excluded Position Types: 0

Filter Selection

● Included ○ Excluded

Organization

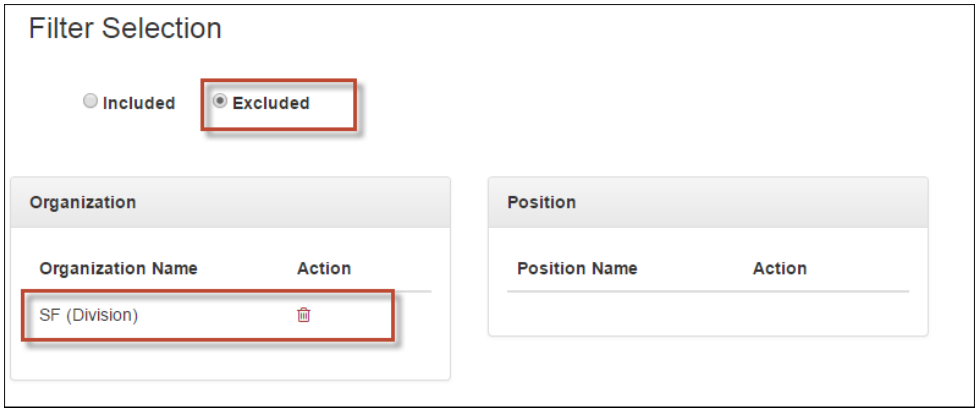
Organization Name	Action
KL (Division)	🗑
EN (Branch)	🗑
EX (Branch)	🗑
YT (Branch)	🗑
CO (Department)	🗑

Position

Position Name	Action
Captain (CP)	🗑
Engineer (EN)	🗑
First Officer (FO)	🗑
Medical Officer (MED)	🗑
Navigator (NV)	🗑

5. Select the **Company** if it is not already selected. Enter a **Name** for the filter.
6. Click the appropriate **Filter Selection** option: **Included** or **Excluded** to either include or exclude Organizations and/or Positions from a role.

You can see every **Organization** structure on the left side of the screen that is included and every **Position** that is included. If you want to exclude any of these Organizations or Positions, in the **Action** column, click on the Trash can icon to not include them. They will now be removed from the **Included** list. If you change the **Filter Selection** to **Excluded**, you will see those items that you just excluded are now displaying on the **Excluded** list. For example, if you excluded the SF (Division) off of the **Included** list, then when you display the **Excluded** list will look like the following screenshot.



Filter Selection

○ Included ● Excluded

Organization

Organization Name	Action
SF (Division)	🗑

Position

Position Name	Action

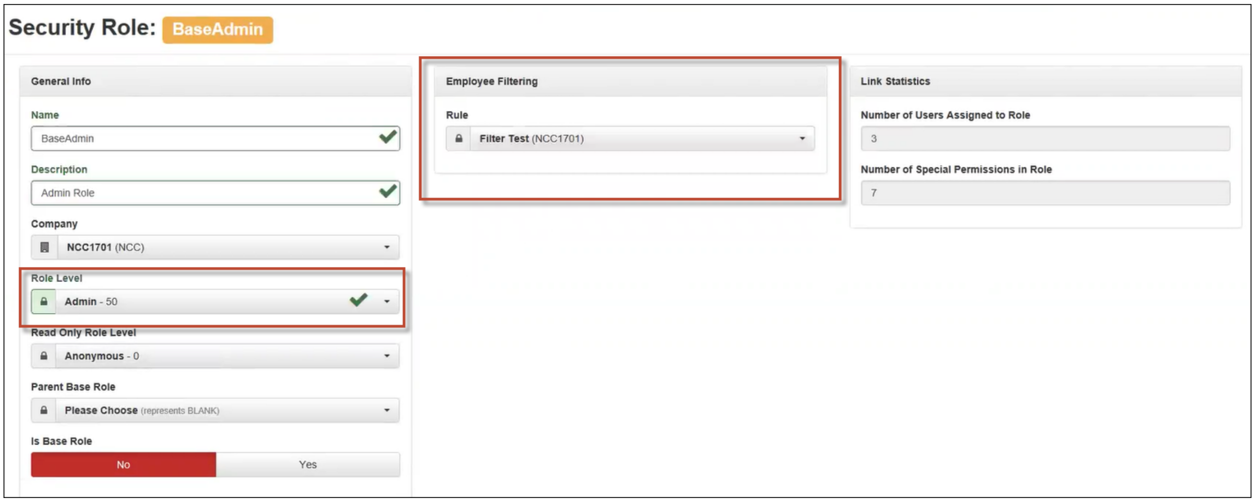
The result is that any employee that is associated with a role which is associated with this Employee Filter rule list, will not be able to see any SF Division employee records. An example might be if you want a role not to be able to view an Executive group's records.

Step 2: Applying an Employee Filter Rule to an Employee Role

To apply an employee filter list rule to a role:

Go to the **Security Role** screen (**HR Admin – Maintenance – Roles**). Select the Role with which you want to associate this filter.

In the **Employee Filtering** section, select the Filter rule you want to associate from the **Rule** dropdown list. Click the **Save Changes** button when complete.



Security Role: BaseAdmin

General Info

Name: BaseAdmin

Description: Admin Role

Company: NCC1701 (NCC)

Role Level: Admin - 50

Read Only Role Level: Anonymous - 0

Parent Base Role: Please Choose (represents BLANK)

Is Base Role: No / Yes

Employee Filtering

Rule: Filter Test (NCC1701)

Link Statistics

Number of Users Assigned to Role: 3

Number of Special Permissions in Role: 7

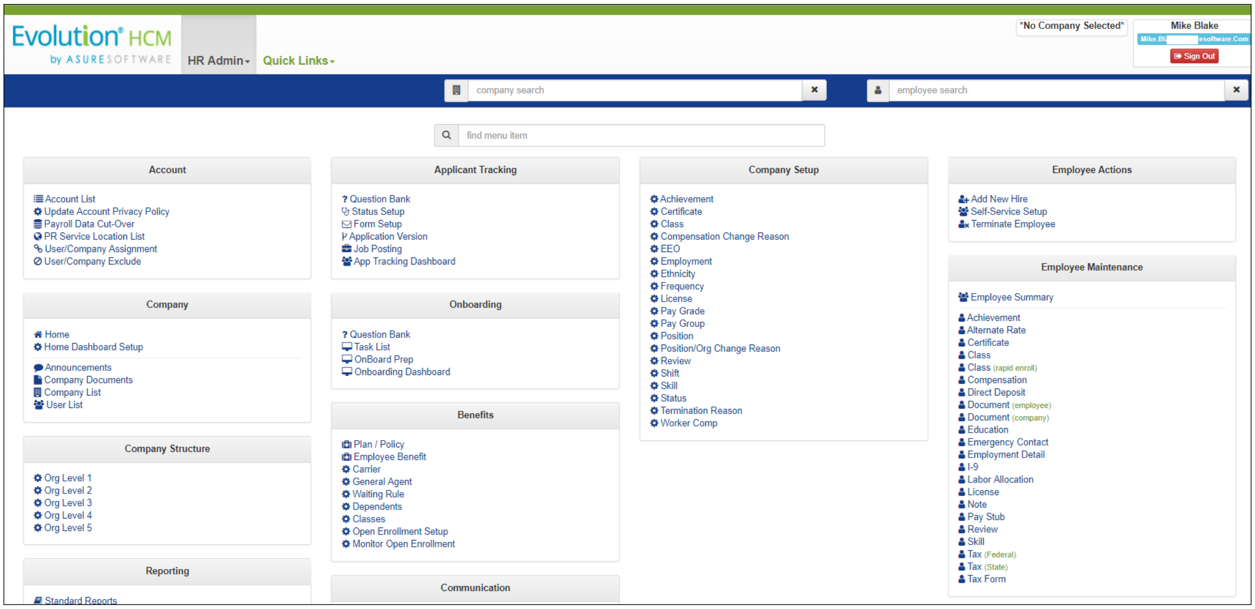
In the example above, you can see that the **Admin** role has an Employee Filter List rule associated with it (**Filter Test**). The result is, for anyone who logs in with this role, they will not be able to access the SF Division employee records.

Note: You can define one employee filter rule per security role. You can only apply one filter role to each user.

A Best Practice to follow is if you have created a role that has an Employee Filter list rule associated with it, that you include in the Role **Description** field, some text that makes it obvious what the filter does.

Security Resources - A Deeper Dive

Let’s take a more in depth look at the security resources in Advanced HR 2.0. In terms of security, every clickable item in the system is known as a **Resource**. For example, on the **HR Admin** menu shown below, every menu item is one kind of resource.



Account
- Account List
- Update Account Privacy Policy
- Payroll Data Cut-Over
- PR Service Location List
- User/Company Assignment
- User/Company Exclude

Company
- Home
- Home Dashboard Setup
- Announcements
- Company Documents
- Company List
- User List

Company Structure
- Org Level 1
- Org Level 2
- Org Level 3
- Org Level 4
- Org Level 5

Reporting
- Standard Reports

Applicant Tracking
- ? Question Bank
- Status Setup
- Form Setup
- Application Version
- Job Posting
- App Tracking Dashboard

Onboarding
- ? Question Bank
- Task List
- OnBoard Prep
- Onboarding Dashboard

Benefits
- Plan / Policy
- Employee Benefit
- Carrier
- General Agent
- Waiting Rule
- Dependents
- Classes
- Open Enrollment Setup
- Monitor Open Enrollment

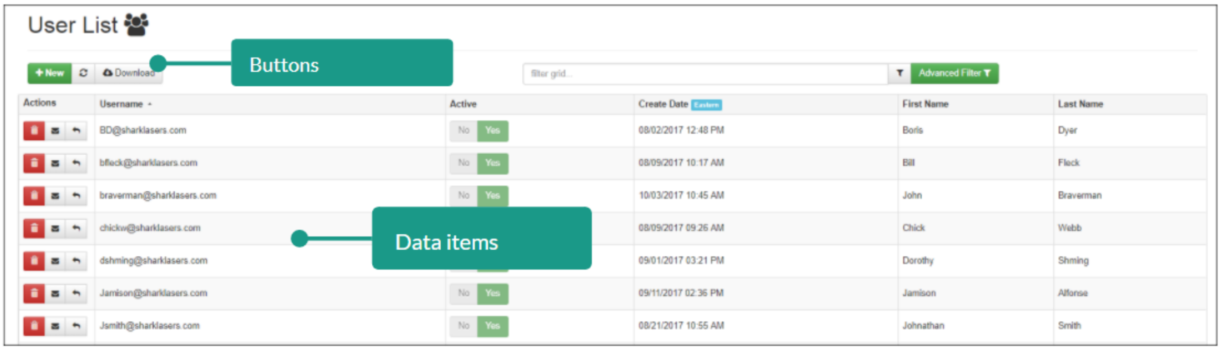
Communication

Company Setup
- Achievement
- Certificate
- Class
- Compensation Change Reason
- EEO
- Employment
- Ethnicity
- Frequency
- License
- Pay Grade
- Pay Group
- Position
- Position/Org Change Reason
- Review
- Shift
- Skill
- Status
- Termination Reason
- Worker Comp

Employee Actions
- Add New Hire
- Self-Service Setup
- Terminate Employee

Employee Maintenance
- Employee Summary
- Achievement
- Alternate Rate
- Certificate
- Class
- Class (rapid enroll)
- Compensation
- Direct Deposit
- Document (employee)
- Document (company)
- Education
- Emergency Contact
- Employment Detail
- I-9
- Labor Allocation
- License
- Note
- Pay Stub
- Review
- Skill
- Tax (Federal)
- Tax (State)
- Tax Form

On a screen such as the **User List** screen shown below, every data item displaying in the grid is another kind of resource. Every button on the screen is also a type of resource.



Actions	Username	Active	Create Date Eastern	First Name	Last Name
	BD@sharklasers.com	No Yes	08/02/2017 12:48 PM	Boris	Dyer
	bfleck@sharklasers.com	No Yes	08/09/2017 10:17 AM	Bill	Fleck
	braverman@sharklasers.com	No Yes	10/03/2017 10:45 AM	John	Braverman
	chickw@sharklasers.com		08/09/2017 09:26 AM	Chick	Webb
	dshming@sharklasers.com		09/01/2017 03:21 PM	Dorothy	Shming
	Jamison@sharklasers.com	No Yes	09/11/2017 02:36 PM	Jamison	Alfonse
	Jsmith@sharklasers.com	No Yes	08/21/2017 10:55 AM	Johnathan	Smith

Resource Control Types

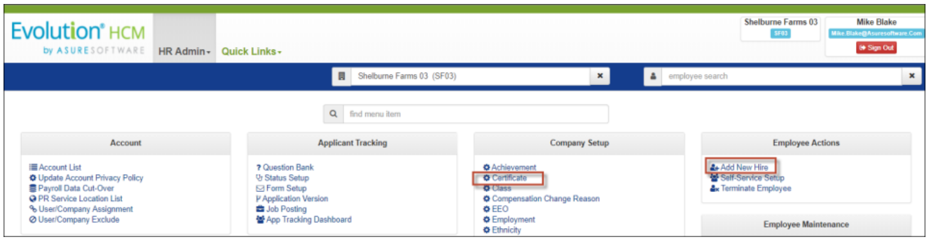
Security Resource Types in Advanced HR 2.0 consist of the following four general categories:

Resource Control Types:

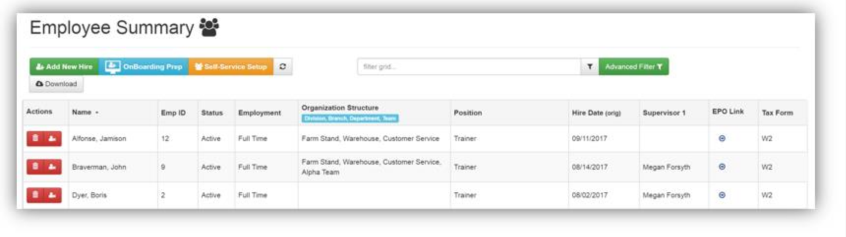
- Form
- Control
- MenuItem
- Database

Each item is described in the following table.

<table>
<tr><th>Resource Type</th><th>Description</th></tr>
<tr><td><b>Menu Item</b></td><td>The Menu Item resource type are items that display in the system as menu choice links. For example, HR Admin – Employee Actions – <b>Add New Hire</b>, or HR Admin – Company Setup - <b>Certificate</b>. When a menu item link is clicked, the user will then be brought to the <b>Form</b> resource type level.

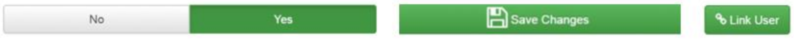

</td></tr>
<tr><td><b>Form</b></td><td>This involves permissions to a specific screen.

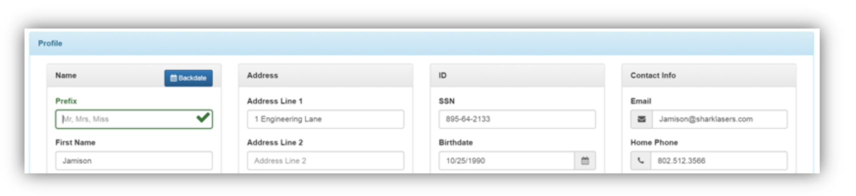
For example, when a user clicks a link on a menu, they will be brought to a Summary screen. This is the Form level resource.


Employee Summary

<table>
<tr><th>Actions</th><th>Name</th><th>Emp ID</th><th>Status</th><th>Employment</th><th>Organization Structure
Division, Branch, Department, Team</th><th>Position</th><th>Hire Date (orig)</th><th>Supervisor 1</th><th>EPO Link</th><th>Tax Form</th></tr>
<tr><td></td><td>Alfonse, Jamison</td><td>12</td><td>Active</td><td>Full Time</td><td>Farm Stand, Warehouse, Customer Service</td><td>Trainer</td><td>09/11/2017</td><td></td><td>⊜</td><td>W2</td></tr>
<tr><td></td><td>Braverman, John</td><td>9</td><td>Active</td><td>Full Time</td><td>Farm Stand, Warehouse, Customer Service, Alpha Team</td><td>Trainer</td><td>08/14/2017</td><td>Megan Forsyth</td><td>⊜</td><td>W2</td></tr>
<tr><td></td><td>Dyer, Boris</td><td>2</td><td>Active</td><td>Full Time</td><td></td><td>Trainer</td><td>08/02/2017</td><td>Megan Forsyth</td><td>⊜</td><td>W2</td></tr>
</table>

Form Types have the word “<b>List</b>” appended to the <b>Name</b>. For example, “EmployeeCompensationList.”</td></tr>
<tr><td><b>Control</b></td><td>The Control resources are the buttons on the various screens. For example, <b>Save Changes</b>, <b>Link User</b>, and <b>No/Yes</b> are all buttons meaning they are Control resources.


</td></tr>
</table>

Resource Type	Description
Database	The Database resource refers to fields within the Form type resource, such as **First Name**, **City**, **Birthdate**, etc. This involves permissions to the information on a specific screen; it may also contain links.  Profile Name Backdate Prefix: Mr, Mrs, Miss First Name: Jamison Address Address Line 1: 1 Engineering Lane Address Line 2: Address Line 2 ID SSN: 895-64-2133 Birthdate: 10/25/1990 Contact Info Email: Jamison@sharklasers.com Home Phone: 802.512.3566

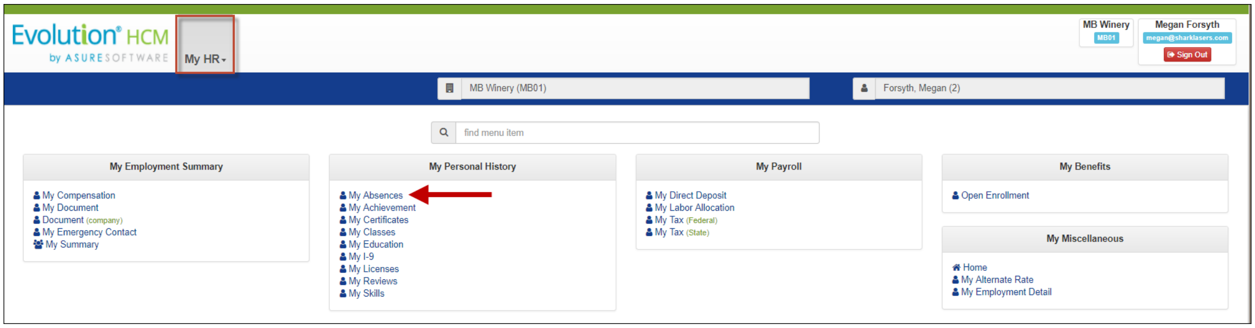
Note that there is one set of resources per Service Bureau.

Making Changes to Resources

Generally, the default resources for the different security user level roles described earlier in this guide (set up during your implementation) will be sufficient for your Service Bureau / Company. However, Super Admin users with the proper security access and the necessary experience, can make modifications to some of the system security resources.

Important Note: However, we strongly recommend that you do *not* try to customize security resources and permissions. Instead, check with the Evolution Implementation team to determine if changes are required and if so, to have them assist you in this effort.

For example, let's take a hypotheical **My Absences** screen, shown below, on the **My HR** menu. Usually, **Base User** employees will have access to the **My Absences** screen (**My HR – My Personal History – My Absences**).



MB Winery (MB01)

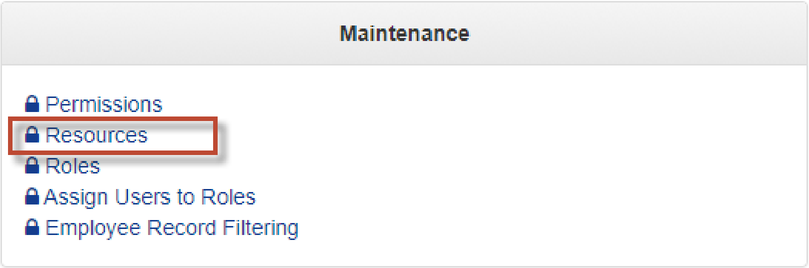
Forsyth, Megan (2)

My Absences menu item on a Base User's My HR screen

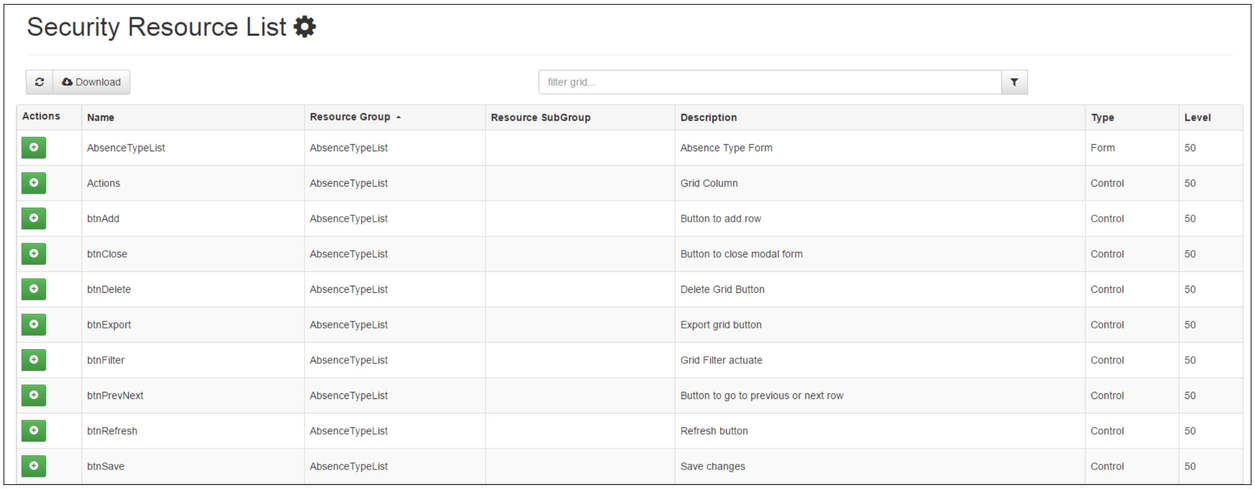
Let's assume that you want to remove the access to the **My Absences** screen for employees on the **My HR** menu. Perhaps the employees are using SwipeClock and you do not want them to have the ability to make a Time Off Request on the **My Absences** screen from the **My HR** menu.

To make changes to a Security Resource, the first thing to do is to display the **Security Resource List**:

1. Go to **HR Admin – Security – Maintenance – Resources**.



2. The system displays the **Security Resource List** screen.



Actions	Name	Resource Group	Resource SubGroup	Description	Type	Level
⊕	AbsenceTypeList	AbsenceTypeList		Absence Type Form	Form	50
⊕	Actions	AbsenceTypeList		Grid Column	Control	50
⊕	btnAdd	AbsenceTypeList		Button to add row	Control	50
⊕	btnClose	AbsenceTypeList		Button to close modal form	Control	50
⊕	btnDelete	AbsenceTypeList		Delete Grid Button	Control	50
⊕	btnExport	AbsenceTypeList		Export grid button	Control	50
⊕	btnFilter	AbsenceTypeList		Grid Filter actuate	Control	50
⊕	btnPrevNext	AbsenceTypeList		Button to go to previous or next row	Control	50
⊕	btnRefresh	AbsenceTypeList		Refresh button	Control	50
⊕	btnSave	AbsenceTypeList		Save changes	Control	50

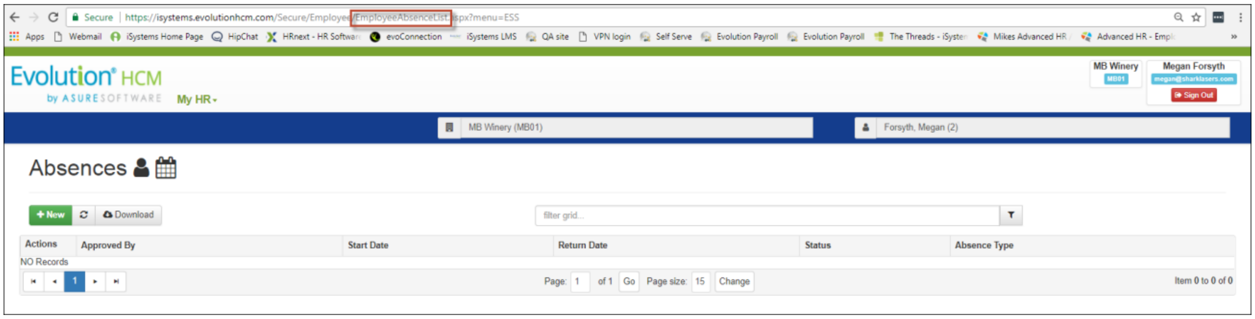
Security Resource List screen

Only a small portion of the **Security Resource List** screen is shown in the screenshot above. If you scroll down to the bottom of the page, you would see that there are more than 4700 resources in the list!

Item **1** to **15** of **4759**

The challenge for the Super Admin user with making changes to the Security Resource List is knowing which resources pertain to the item you want to make changes to. In our example, let's assume that we want to make a change to the **My Absences** screen. We need to know how to narrow the **Security Resource List** screen to display just the resources for the item we want to change.

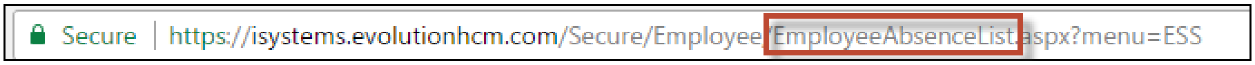
A good practice if you want to make resource changes to a screen, is that you should first display that screen and obtain some information from it. In our example it is the **My Absences** screen, shown below.



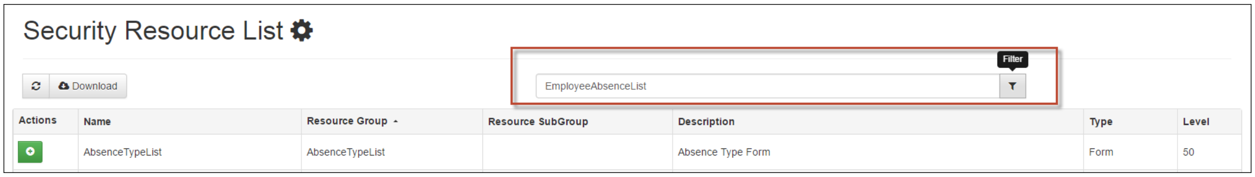
Absences

Actions	Approved By	Start Date	Return Date	Status	Absence Type
NO Records					

When you have the screen displayed, look in the browser's URL line above the screen – a closeup view is shown below.


Secure | https://isystems.evolutionhcm.com/Secure/Employee/EmployeeAbsenceList.aspx?menu=ESS

Notice the text after the "Employee/": **EmployeeAbsenceList**. This is the key information you need to know in order to display the corresponding resources in the **Security Resource List** screen. You can copy this text from the browser URL line, then return to the **Security Resource List** screen, and paste the text into the **filter grid** search box at the top of the **Security Resource List** screen, as shown in the following screenshot.

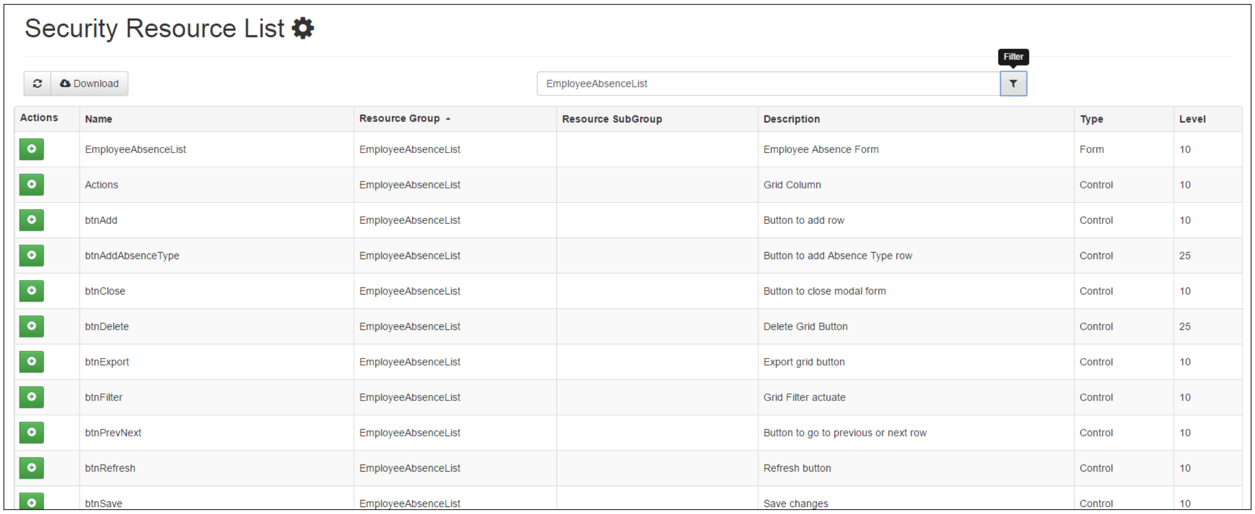

Security Resource List

EmployeeAbsenceList

Actions	Name	Resource Group ▲	Resource SubGroup	Description	Type	Level
⊕	AbsenceTypeList	AbsenceTypeList		Absence Type Form	Form	50

Using the Filter Grid to Find Resources

Click on the filter icon at the right of the filter grid search box. The system then redisplays, and will now show a list of all the security resources related to the **My Absences** screen only (EmployeeAbsenceList). They are grouped by the **Resource Group** column. All of the security resources of the **My Absences** screen are displayed on the list (45 different resource items in this example). That's a lot better than scrolling through all 4700+ resources!



Security Resource List

EmployeeAbsenceList

Actions	Name	Resource Group ▲	Resource SubGroup	Description	Type	Level
⊕	EmployeeAbsenceList	EmployeeAbsenceList		Employee Absence Form	Form	10
⊕	Actions	EmployeeAbsenceList		Grid Column	Control	10
⊕	btnAdd	EmployeeAbsenceList		Button to add row	Control	10
⊕	btnAddAbsenceType	EmployeeAbsenceList		Button to add Absence Type row	Control	25
⊕	btnClose	EmployeeAbsenceList		Button to close modal form	Control	10
⊕	btnDelete	EmployeeAbsenceList		Delete Grid Button	Control	25
⊕	btnExport	EmployeeAbsenceList		Export grid button	Control	10
⊕	btnFilter	EmployeeAbsenceList		Grid Filter actuate	Control	10
⊕	btnPrevNext	EmployeeAbsenceList		Button to go to previous or next row	Control	10
⊕	btnRefresh	EmployeeAbsenceList		Refresh button	Control	10
⊕	btnSave	EmployeeAbsenceList		Save changes	Control	10

Displaying a list of the security resources for the My Absences screen (EmployeeAbsenceList)

We need to do two things to make the intended changes to the **My Absences** screen:

- Make a change to the **Form** resource for the My Absences screen
- Make a change to the **Menu Item** resource for the My Absences screen

When Customizing Roles - Disable both the Form and the MenuItem

It's important to note that if the permission to a **Form type** resource is disabled for a role/user, but the corresponding **Menu Item permission** is not, the role/user will be able to see the Menu Item. However, they will not be able to access it. Hence, the fields and buttons within the form are disabled too, since the role/user is unable to get into the form. This means that the Form type permission takes precedence over Menu Item, Database, and the Control types.

When the **Form type resource** is disabled, then the role/user will not have access to the screen. Similarly, if a Form type is enabled for a role/user, but its corresponding Menu Item type is disabled, the role/user can still get to the form by directly entering the URL to the form (if the URL is known to the user).

It is best practice to ensure that when customizing roles, you disable/enable both the Form and the Menu Item.

Precedence Order of a Customized Security Role

Note: When you make any customizations to a security role and assign it to a user, it's important to be aware of the following point. If the user has any other default security role(s) that set the opposite functionality, then the customized role will not take precedence over the user's other default security role.

For example, if a user is already a default Base Admin, and you assign them a customized Base Admin role, the user will have the functionality of the default Base Admin role, and not the customized role.

Document any Security Changes you Make

If you do make customized changes to security roles, resources, and/or permissions, it is very important that you **document the security roles changes you make**, both for the benefit of your Service Bureau/Client and in order for the Asure Implementation team to be able to assist you if you encounter issues. If you do not document any customized security changes you have made over time, we will be unable to properly assist you.

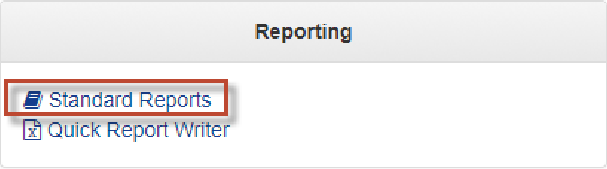
Note: For those few Administrators who may require a more detailed explanation of customizing security roles, permissions and users, refer to the separate document *Customizing Security Roles and Users Guide* posted on the Advanced HR 2.0 - **Implementations Center** section of the **Evolution Resource Center**.

Generating a Report of All User and Role Records

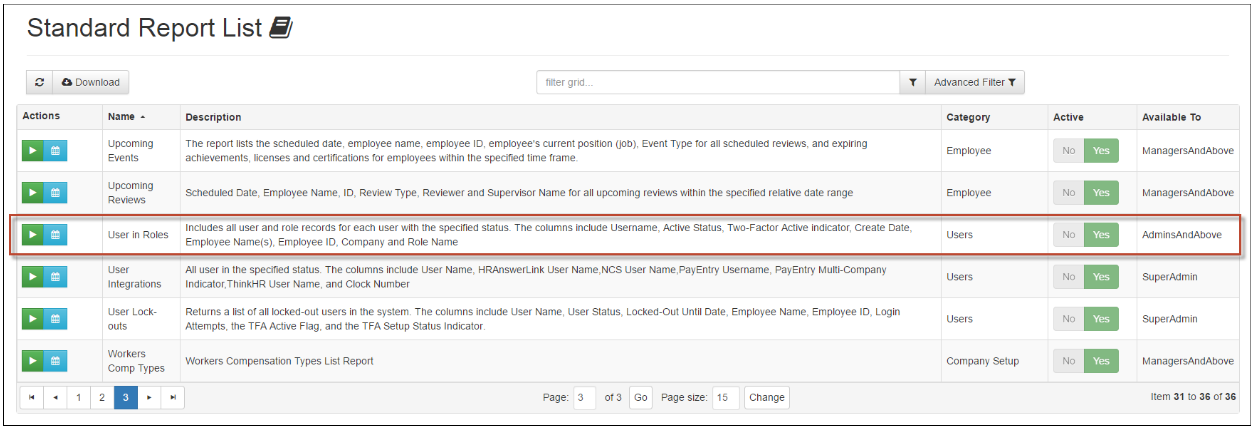
Advanced HR 2.0 comes with many Standard Reports by default. Any user with a **Base Manager** Role or higher, can run a standard report. One of the standard reports is specifically designed to run reports on which users have what roles.

To do this:

1. Go to **HR-Admin – Reporting – Standard Reports**.



2. The system displays the menu of **Standard Reports** screens.



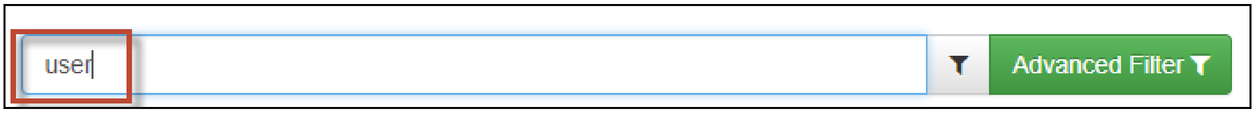
Standard Report List

Actions	Name	Description	Category	Active	Available To
▶	Upcoming Events	The report lists the scheduled date, employee name, employee ID, employee's current position (job), Event Type for all scheduled reviews, and expiring achievements, licenses and certifications for employees within the specified time frame.	Employee	No [✓ Yes]	ManagersAndAbove
▶	Upcoming Reviews	Scheduled Date, Employee Name, ID, Review Type, Reviewer and Supervisor Name for all upcoming reviews within the specified relative date range	Employee	No [✓ Yes]	ManagersAndAbove
▶	User in Roles	Includes all user and role records for each user with the specified status. The columns include Username, Active Status, Two-Factor Active indicator, Create Date, Employee Name(s), Employee ID, Company and Role Name	Users	No [✓ Yes]	AdminsAndAbove
▶	User Integrations	All user in the specified status. The columns include User Name, HRAnswerLink User Name,NCS User Name,PayEntry Username, PayEntry Multi-Company Indicator,ThinkHR User Name, and Clock Number	Users	No [✓ Yes]	SuperAdmin
▶	User Lock-outs	Returns a list of all locked-out users in the system. The columns include User Name, User Status, Locked-Out Until Date, Employee Name, Employee ID, Login Attempts, the TFA Active Flag, and the TFA Setup Status Indicator.	Users	No [✓ Yes]	SuperAdmin
▶	Workers Comp Types	Workers Compensation Types List Report	Company Setup	No [✓ Yes]	ManagersAndAbove

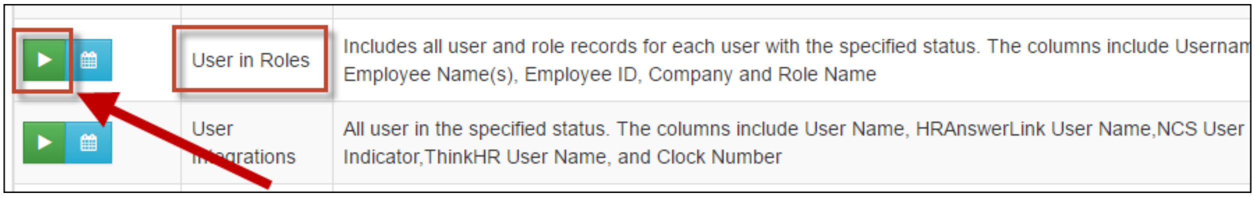
1 2 3 Page: 3 of 3 Go Page size: 15 Change Item **31** to **36** of **36**

3. Scroll to the **User in Roles** report.

   Note: You can quickly find the Users in Roles report by searching for the term “**user**” in the filter grid field at the top of the Standard Report List screen.

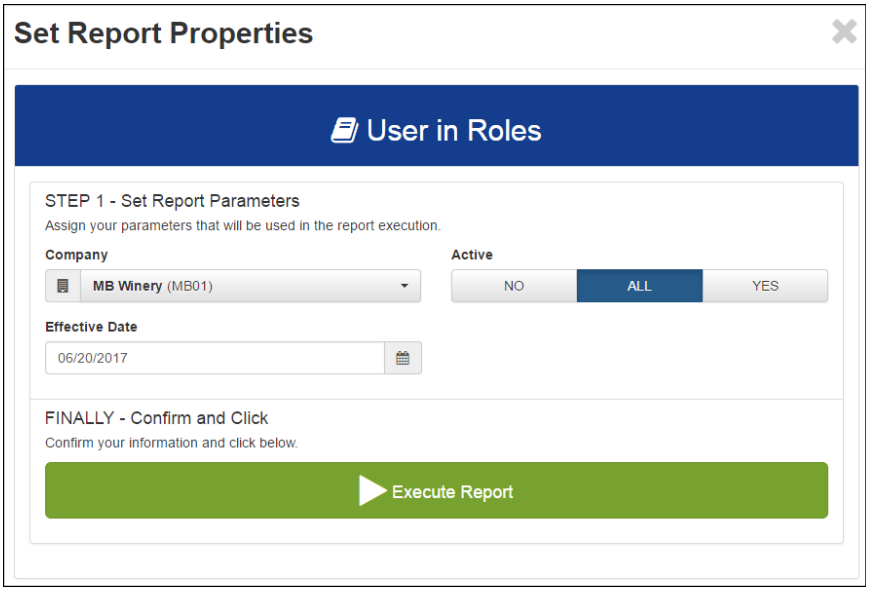


4. On the row for the **Users in Roles** report, click on the green arrow **Execute Report** icon. ▶



▶	User in Roles	Includes all user and role records for each user with the specified status. The columns include Usernam Employee Name(s), Employee ID, Company and Role Name
▶	User Integrations	All user in the specified status. The columns include User Name, HRAnswerLink User Name,NCS User Indicator,ThinkHR User Name, and Clock Number

5. The system displays the **Set Report Properties** screen.



Set Report Properties

User in Roles

STEP 1 - Set Report Parameters
Assign your parameters that will be used in the report execution.

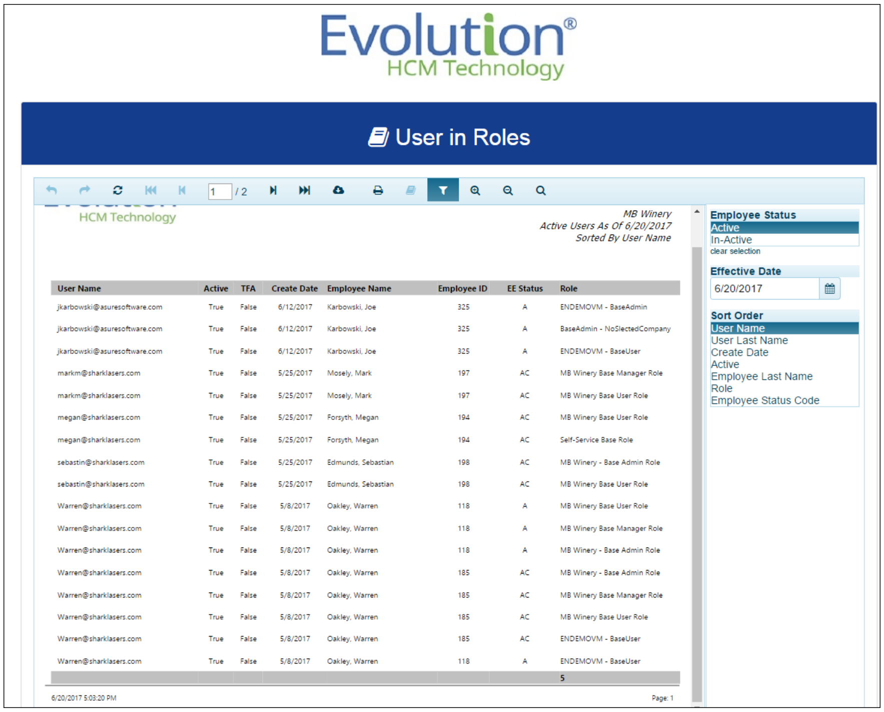
Company: MB Winery (MB01)

Active: NO [✓ ALL] YES

Effective Date: 06/20/2017

FINALLY - Confirm and Click
Confirm your information and click below.

6. Select the **Company**, change the **Effective Date**, if required, and select **Active** users: **No**, **All**, or **Yes**.
7. Click the **Execute Report** button. The Report that is generated will display a sortable Report that can be printed or exported as a CSV, PDF, Excel, RTF, TIFF, Web, or XPS document.
8. The system displays the **Users in Roles** report, a sample is shown below.



Evolution®
HCM Technology

User in Roles

HCM Technology

MB Winery
Active Users As Of 6/20/2017
Sorted By User Name

User Name	Active	TFA	Create Date	Employee Name	Employee ID	EE Status	Role
jkarbowski@asuresoftware.com	True	False	6/12/2017	Karbowski, Joe	325	A	ENDEMOVM - BaseAdmin
jkarbowski@asuresoftware.com	True	False	6/12/2017	Karbowski, Joe	325	A	BaseAdmin - NoSlectedCompany
jkarbowski@asuresoftware.com	True	False	6/12/2017	Karbowski, Joe	325	A	ENDEMOVM - BaseUser
markm@sharklasers.com	True	False	5/25/2017	Mosely, Mark	197	AC	MB Winery Base Manager Role
markm@sharklasers.com	True	False	5/25/2017	Mosely, Mark	197	AC	MB Winery Base User Role
megan@sharklasers.com	True	False	5/25/2017	Forsyth, Megan	194	AC	MB Winery Base User Role
megan@sharklasers.com	True	False	5/25/2017	Forsyth, Megan	194	AC	Self-Service Base Role
sebastin@sharklasers.com	True	False	5/25/2017	Edmunds, Sebastian	198	AC	MB Winery - Base Admin Role
sebastin@sharklasers.com	True	False	5/25/2017	Edmunds, Sebastian	198	AC	MB Winery Base User Role
Warren@sharklasers.com	True	False	5/8/2017	Oakley, Warren	118	A	MB Winery Base User Role
Warren@sharklasers.com	True	False	5/8/2017	Oakley, Warren	118	A	MB Winery Base Manager Role
Warren@sharklasers.com	True	False	5/8/2017	Oakley, Warren	118	A	MB Winery - Base Admin Role
Warren@sharklasers.com	True	False	5/8/2017	Oakley, Warren	185	AC	MB Winery - Base Admin Role
Warren@sharklasers.com	True	False	5/8/2017	Oakley, Warren	185	AC	MB Winery Base Manager Role
Warren@sharklasers.com	True	False	5/8/2017	Oakley, Warren	185	AC	MB Winery Base User Role
Warren@sharklasers.com	True	False	5/8/2017	Oakley, Warren	185	AC	ENDEMOVM - BaseUser
Warren@sharklasers.com	True	False	5/8/2017	Oakley, Warren	118	A	ENDEMOVM - BaseUser
							5

6/20/2017 5:03:20 PM

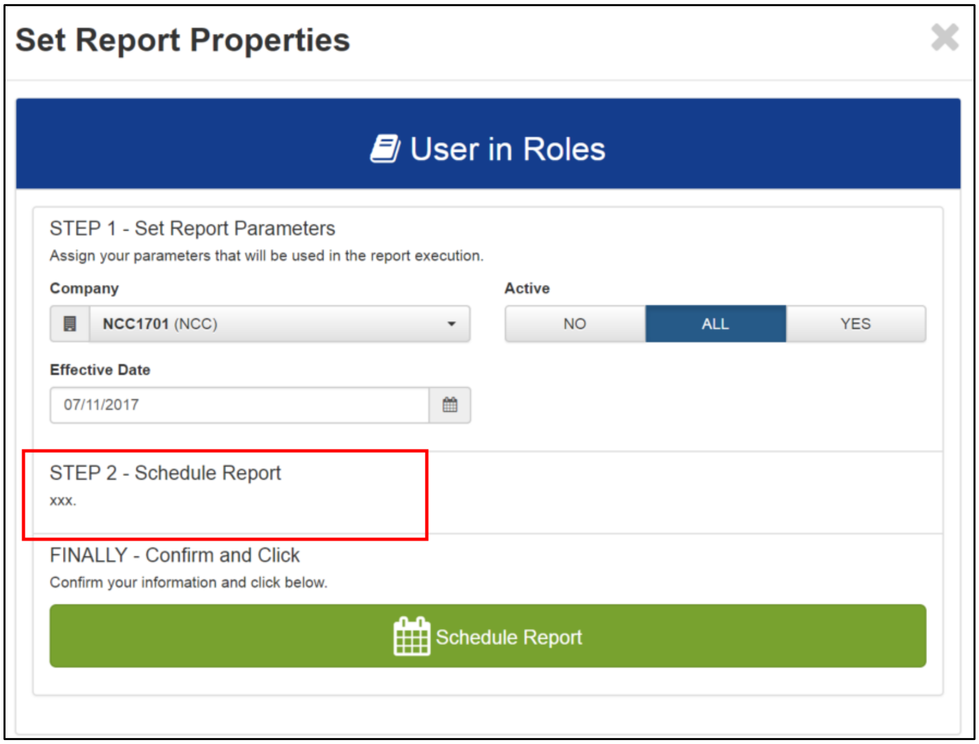
Page: 1

Employee Status
Active
In-Active
clear selection

Effective Date
6/20/2017

Sort Order
User Name
User Last Name
Create Date
Active
Employee Last Name
Role
Employee Status Code

Future functionality: To Schedule a Report, click on the **blue Calendar** icon. A pop up will be displayed that will allow you to set the Report parameters. Most importantly, a schedule date is displayed:



Set Report Properties

User in Roles

STEP 1 - Set Report Parameters
Assign your parameters that will be used in the report execution.

Company
NCC1701 (NCC)

Active
NO | ALL | YES

Effective Date
07/11/2017

STEP 2 - Schedule Report
xxx.

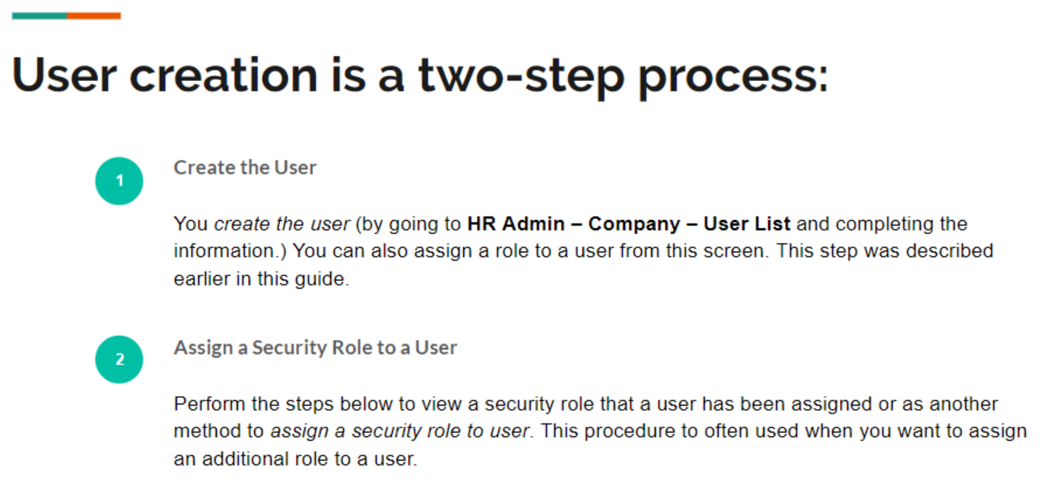
FINALLY - Confirm and Click
Confirm your information and click below.

When the Report parameters are set, click **Schedule Report**. The Report will be generated on the selected date as a sortable Report that can be printed or exported as a CSV, PDF, Excel, RTF, TIFF, Web, or XPS document.

Tip: Make sure that any pop-up blockers are turned off on your browser.

Appendix A: Viewing / Assigning a Role to a User with the Assign Users to Roles Screen

Users who are signed in as a Super Admin or a Service Bureau Admin user can view the security role(s) that a user has been assigned and they can also assign a security role to a user with the **Assign Users to Roles** screen. Note that users can have (and should be assigned to) multiple roles.



User creation is a two-step process:

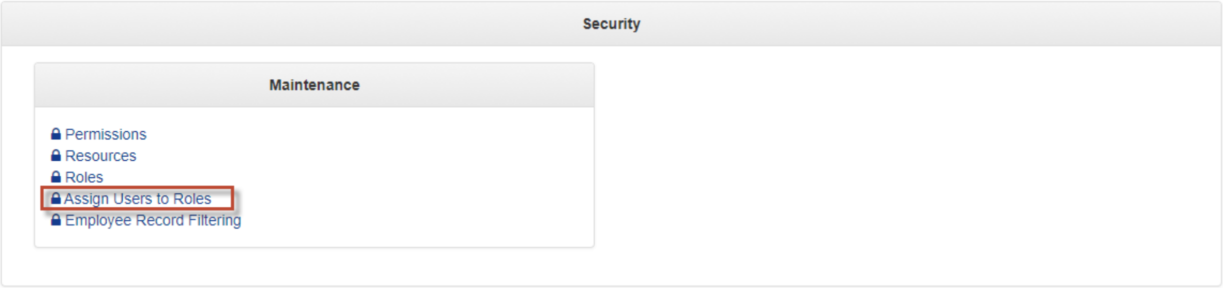
1 Create the User

You *create the user* (by going to **HR Admin – Company – User List** and completing the information.) You can also assign a role to a user from this screen. This step was described earlier in this guide.

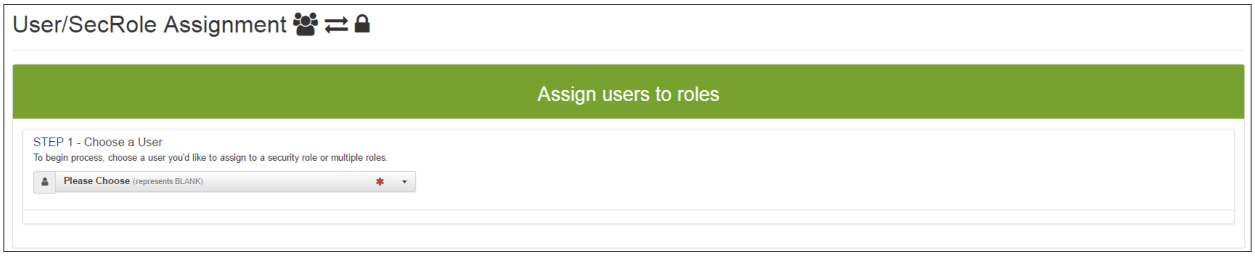
2 Assign a Security Role to a User

Perform the steps below to view a security role that a user has been assigned or as another method to *assign a security role to user*. This procedure to often used when you want to assign an additional role to a user.

1. Go to **HR Admin** – **Security** – **Maintenance** – **Assign Users to Roles**.



2. The system displays the **Assign users to roles** screen.



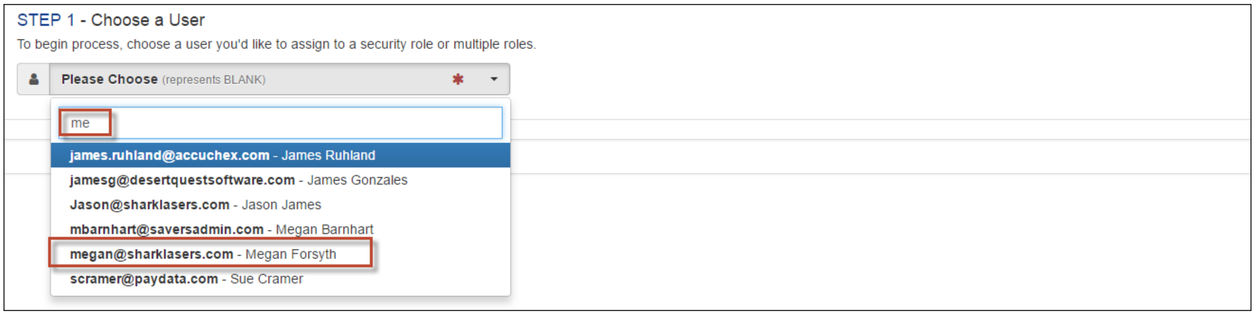
STEP 1 - Choose a User

To begin process, choose a user you'd like to assign to a security role or multiple roles.

Please Choose (represents BLANK) *

3. In the **Step 1 – Choose a User** section of the screen, use the dropdown menu to select the user to which you want to assign a role. You can select from the dropdown or enter in the first few characters of the user name to narrow the search list. In the following example, we entered '**me**' to quickly find **Megan Forsyth**.

   It's important to remember that unless you are signed in as a **Super Admin**, or a **SB Admin**, you won't be able to use this feature



STEP 1 - Choose a User

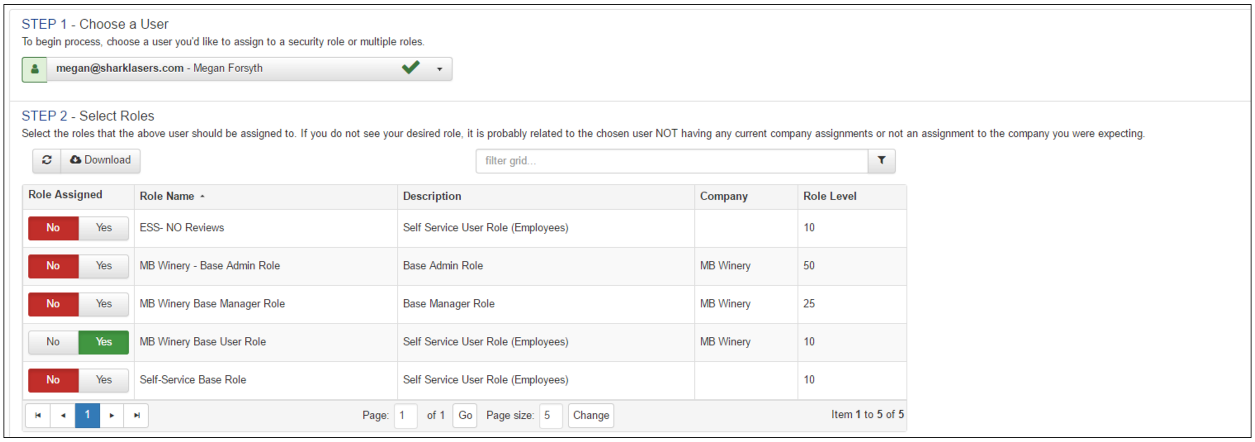
To begin process, choose a user you'd like to assign to a security role or multiple roles.

Please Choose (represents BLANK)

me

- james.ruhland@accuchex.com - James Ruhland
- jamesg@desertquestsoftware.com - James Gonzales
- Jason@sharklasers.com - Jason James
- mbarnhart@saversadmin.com - Megan Barnhart
- megan@sharklasers.com - Megan Forsyth
- scramer@paydata.com - Sue Cramer

4. The system displays the **Step 2 – Select Roles** section of the screen. It shows a list of the user roles currently available for the user and the company.



STEP 1 - Choose a User

To begin process, choose a user you'd like to assign to a security role or multiple roles.

megan@sharklasers.com - Megan Forsyth ✓

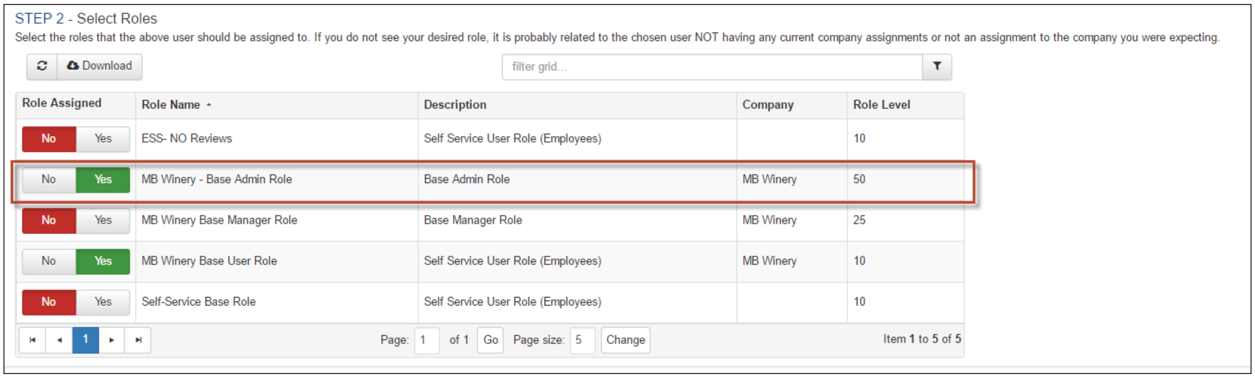
STEP 2 - Select Roles

Select the roles that the above user should be assigned to. If you do not see your desired role, it is probably related to the chosen user NOT having any current company assignments or not an assignment to the company you were expecting.

Role Assigned	Role Name	Description	Company	Role Level
[✓ No] Yes	ESS- NO Reviews	Self Service User Role (Employees)		10
[✓ No] Yes	MB Winery - Base Admin Role	Base Admin Role	MB Winery	50
[✓ No] Yes	MB Winery Base Manager Role	Base Manager Role	MB Winery	25
No [✓ Yes]	MB Winery Base User Role	Self Service User Role (Employees)	MB Winery	10
[✓ No] Yes	Self-Service Base Role	Self Service User Role (Employees)		10

Note: If you do not see the role you want to assign, most likely it is due to the selected user not having any current company assignments and/or not an assignment to the company you were viewing.

5. In the **Role Assigned** column on the left, use the **Yes/No** toggles to assign a role(s) to the user. For example, assume Megan Forsyth has already been assigned the Base User Role (for the MB Winery company). To assign Megan the Base Admin Role also, you would toggle the **MB Winery – Base Admin Role** from **No** to **Yes** as shown below.



STEP 2 - Select Roles

Select the roles that the above user should be assigned to. If you do not see your desired role, it is probably related to the chosen user NOT having any current company assignments or not an assignment to the company you were expecting.

Role Assigned	Role Name	Description	Company	Role Level
[✓ No] Yes	ESS- NO Reviews	Self Service User Role (Employees)		10
No [✓ Yes]	MB Winery - Base Admin Role	Base Admin Role	MB Winery	50
[✓ No] Yes	MB Winery Base Manager Role	Base Manager Role	MB Winery	25
No [✓ Yes]	MB Winery Base User Role	Self Service User Role (Employees)	MB Winery	10
[✓ No] Yes	Self-Service Base Role	Self Service User Role (Employees)		10

Note: Users can – any should be - assigned to multiple roles.

6. You’re done, Megan now has been assigned both the **Base User** Role and the **Base Admin** Role for the **MB Winery** company.