

Enterprise - Security Group Administration

Last Modified on 05/07/2020 8:39 am CDT

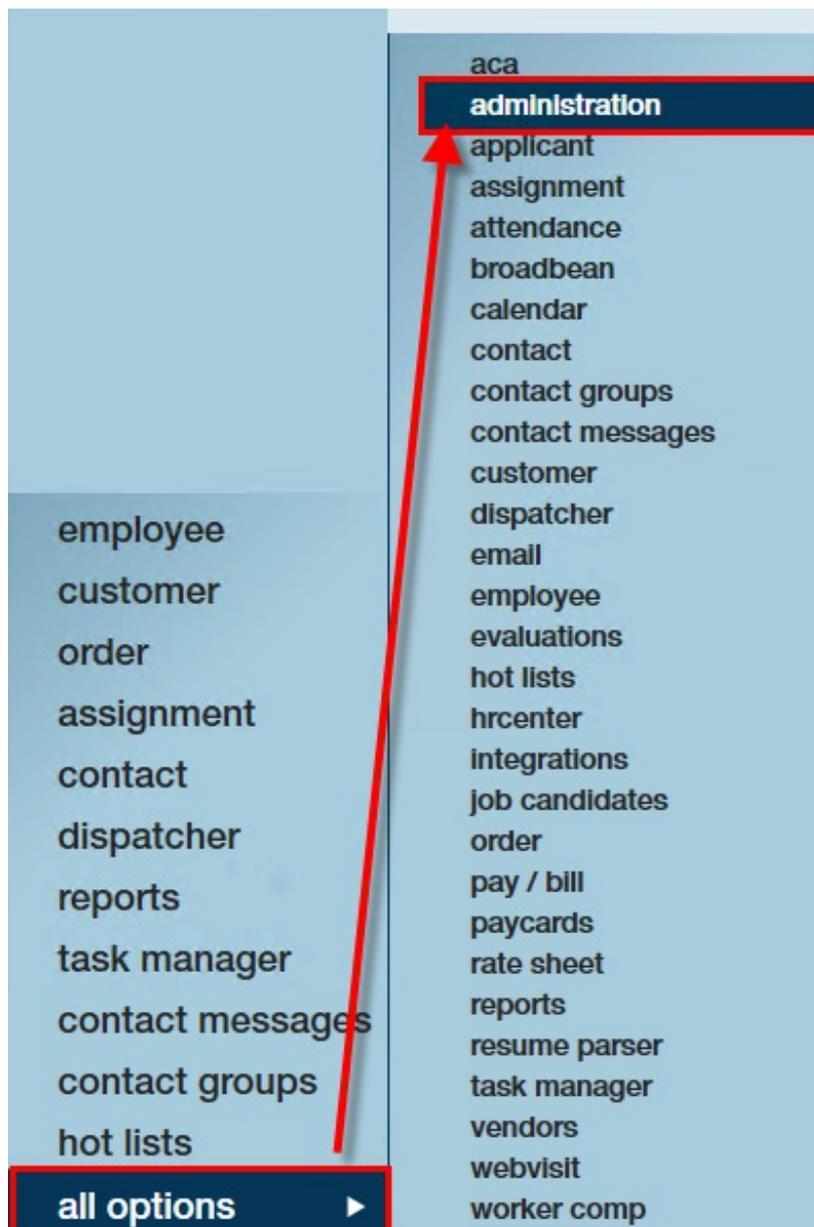
What are Security Groups?

Security groups are a new way in handling permissions and reports for our next generation products that make APIv3 calls, such as Beyond. This process is distinct and different from security roles and are not interchangeable. With security roles, users select individual roles that make up the permissions of the user. With security groups, users are only ever assigned one group per group type.

Note Security groups is for Beyond only. If you are looking to set up security from Beyond Administration, check out [Beyond - Managing Security Groups](#).

Locating Security Groups

Security groups can be created by navigating to the 'administration' section in enterprise under 'all options':

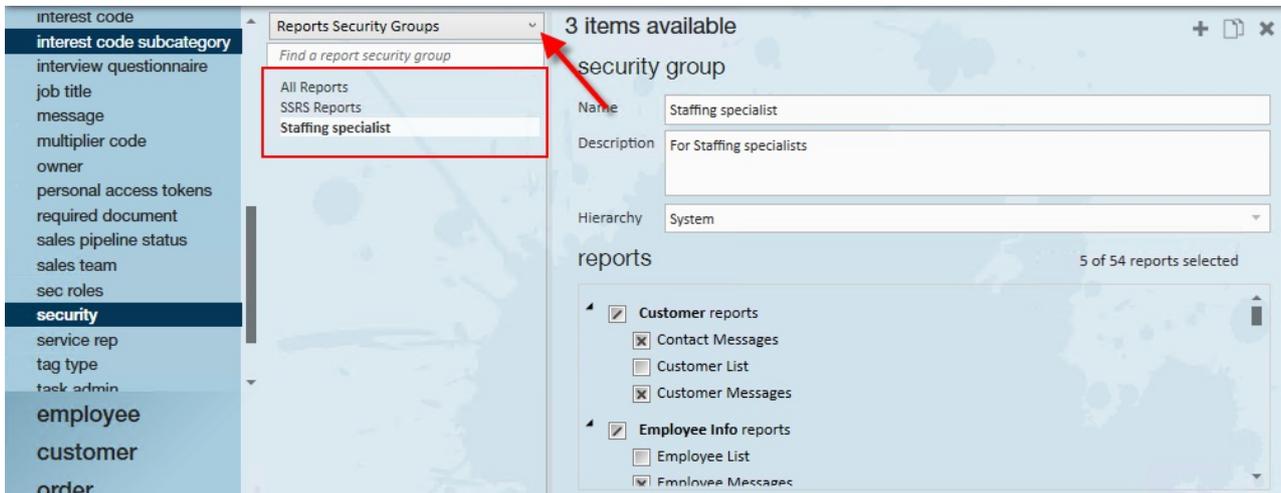


Navigate from here to the 'security' form. This is where security groups can be created, edited, and deleted. Each service rep can be allocated only one security group per security group types. Currently, five groups exist:

1. **Permission Security Groups**- a group that determines functionality a user can access.
2. **Reports Security Groups**- A group that determines the reports a user has access to.
3. **Custom Data Security Groups**- A group that determines the custom data fields a user can view/ and or edit.
4. **Customer Status Security Groups**- A group that governs the customer statuses that an individual service rep can change.

5. **Document Type Security Groups** - A group that governs the document types an individual service rep can view/print/or download.

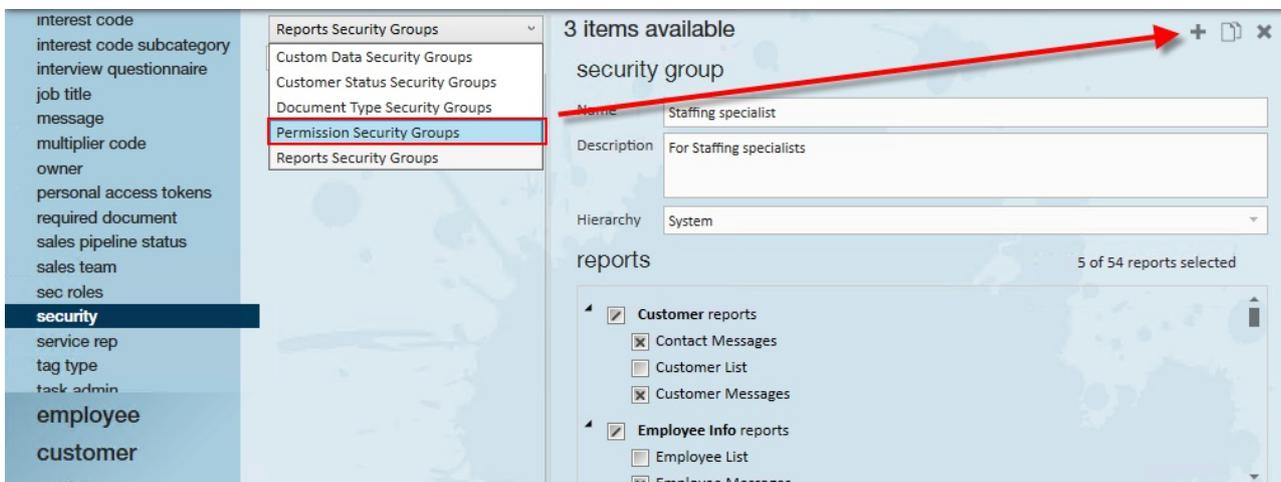
Select from the drop-down to preview any of the available security group types. After selecting a group type, the available groups will be displayed:



Creating Security Groups

Creating a new security group allows you to decide what that group is capable of. For example, if making a new report group, you may determine which reports are available to members of that group.

When creating a security group, be sure to determine which group type you are creating. Service reps can belong to one of each type. When you have decided which group to create, select the '+' icon:



When creating a new security group, consider paralleling this with the real groups who

work for your company. Creating a group can provide clarity in what the user can do and what they can see. Once a new security group is created, a wizard opens. Enter the following information:

- **Security Group Type**- The current type of group you are creating. This is dependent upon which group you were in when the '+' icon was selected.
- **Hierarchy**- The hierarchy level/location this security role will be available at.
- **Name**- The title for your security group.
- **Description**- An explanation of this group that is a concise summary of the role.

The screenshot shows a 'create new security group' wizard. At the top, there's a blue header with a question mark and close icon. Below it, the title 'create new security group' is displayed. The main area is divided into two sections. The first section, 'Security Group Type', has a dropdown menu. Below it are three input fields: 'Hierarchy', 'Name', and 'Description'. Each field has a red exclamation mark icon to its left, indicating a required field. The second section, 'Select permissions to be included in the new security group', contains a list of permissions with checkboxes. The permissions listed are: 'employee-bankaccount-updatewhileinachrun' (Can update an employee bank account while in a staged ACH run), 'employee-eeo-create' (Can create employee EEO information), 'employee-eeo-read' (Can read employee EEO information), 'employee-eeo-update' (Can update employee EEO information), and 'employee-unmask-zpi'. At the bottom of the window, there's a red status bar with a '4' and a warning icon, and buttons for 'Cancel' and 'Save'.

Depending on the group created, you will be prompted to select the criteria that defines that group. For permissions, that means selecting permissions. For custom data, that may mean what fields are visible/editable to that rep.

Permission Security Groups

This group type governs specific functionality that can be set for a group. Select the permissions you wish to grant members of this group:

create new security group

Security Group Type **Permission**

Hierarchy: High Tech Staffing

Name: Branch Managers

Description: For branch managers.

Select permissions to be included in the new security group

- employee-bankaccount-updatewhileinachrun**
Can update an employee bank account while in a staged ACH run
- employee-eeo-create**
Can create employee EEO information
- employee-eeo-read**
Can read employee EEO information
- employee-eeo-update**
Can update employee EEO information
- employee-unmask-gpi**
Unmask Employee SSN
- everify-case-admin**
Can manage all E-Verifu cases regardless of owner

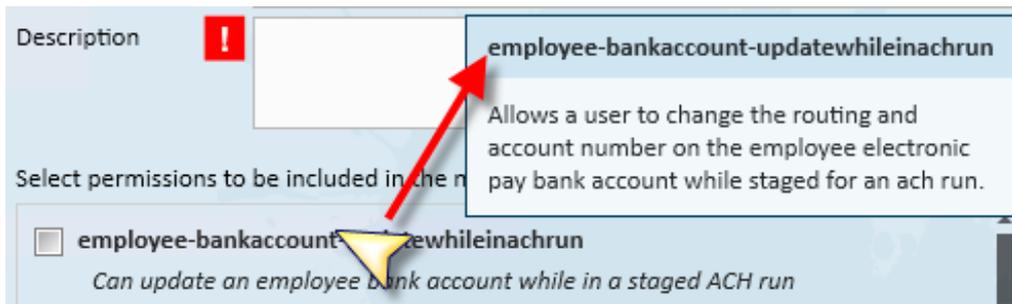
Cancel Save

If you don't have access to the 'admin' permission, some permissions may be grayed out:

permissions 11 of 11 permi

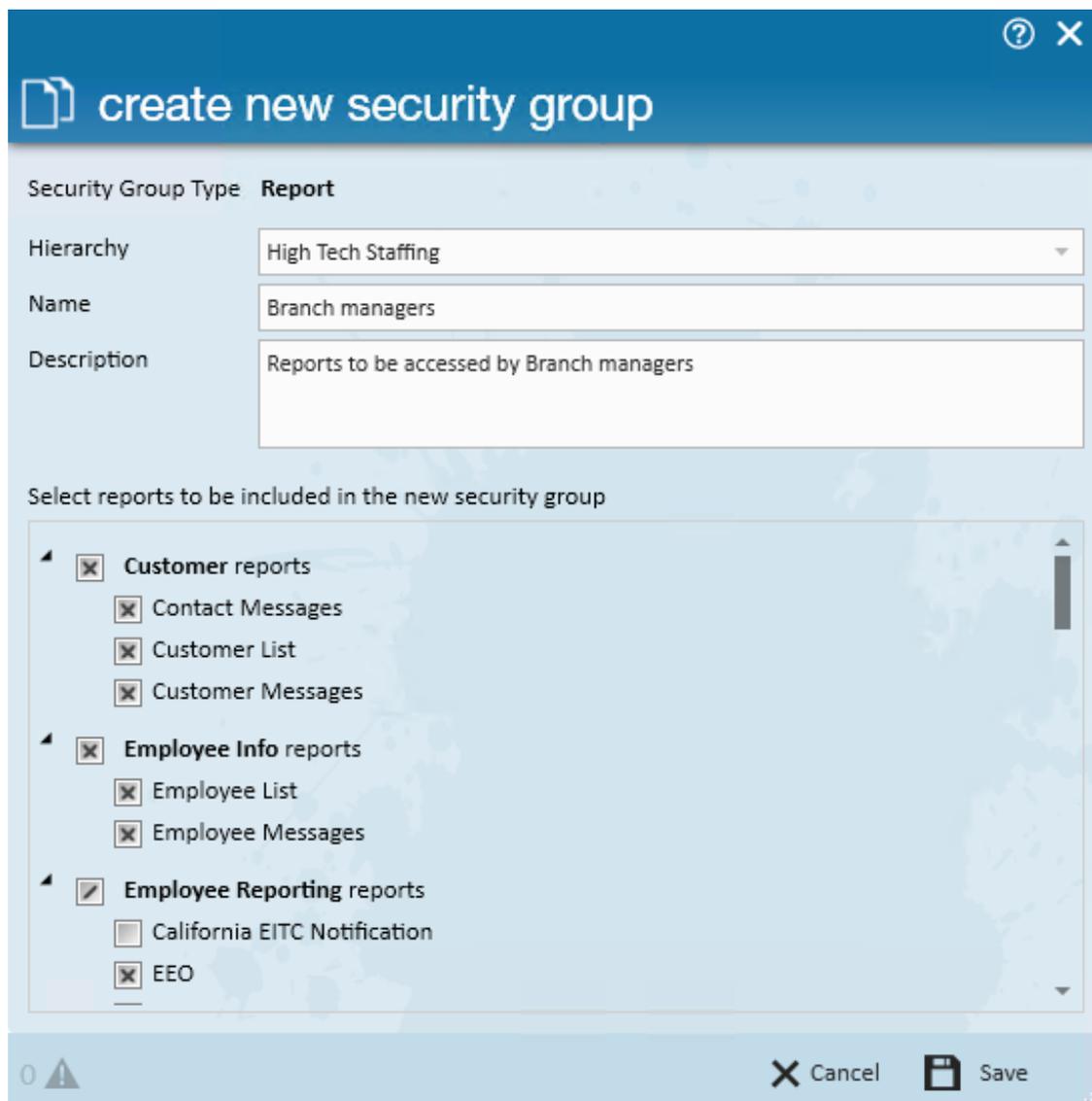
- admin**
Admin
- allow-full-access**
Full access
- employee-bankaccount-updatewhileinachrun**
Can update an employee bank account while in staged ACH run
- employee-eeo-create**

Note If you are unsure of what a specific permission does, hover your cursor over the permission for a quick tool tip on the functionality:



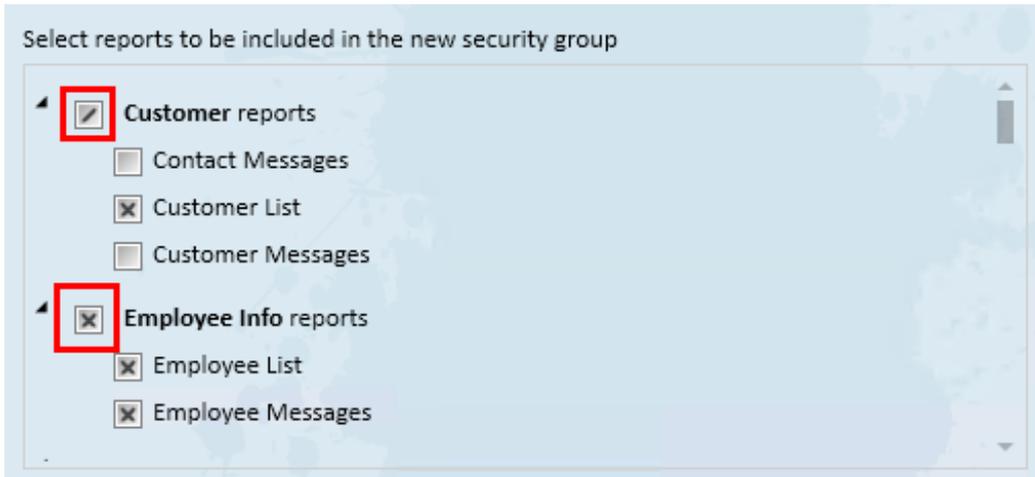
Reports Security Groups

This group type determines which reports the members of its group can run. Select the reports you wish to grant members of this group:

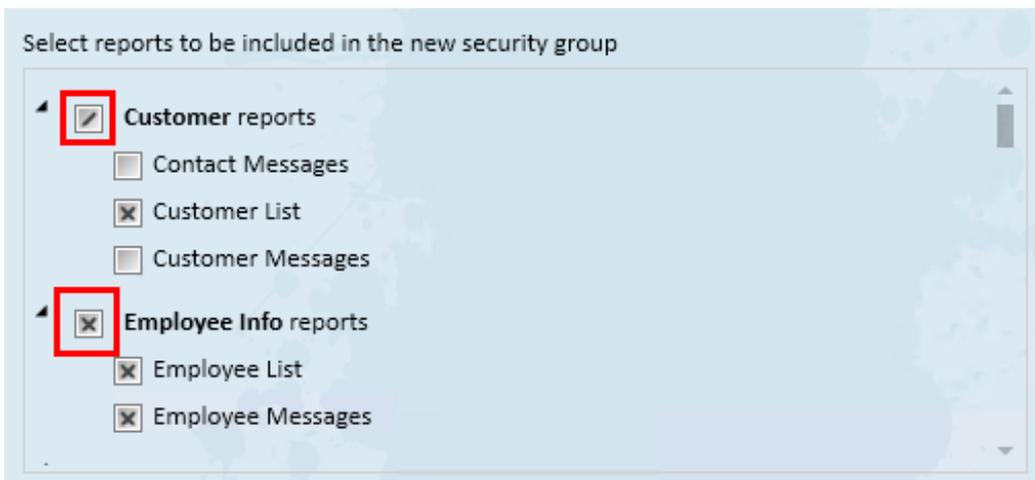


Note When selecting reports for a reports security group, you may choose to select

some or all of the reports in a given grouping. If only some reports are chosen, that group will have a '/' in the checkbox representing that group. If all the reports in a group are selected, this will be denoted by an 'x':



Note When selecting reports for a reports security group, you may choose to select some or all of the reports in a given grouping. If only some reports are chosen, that group will have a '/' in the checkbox representing that group. If all the reports in a group are selected, this will be denoted by an 'x':



Custom Data Property Security Groups

This group type determines what custom data fields can be viewed/created by a service rep. Select whether members of this group can write and/or read this custom data field. For more information on custom data fields: [How to Set up and Manage Custom Data:](#)

? X
create new security group

Security Group Type **Custom Data Property**

Hierarchy

Name

Description

Select custom data properties to be included in the new security group

Name	Origin Type	Hier	Deny Read	Deny Write
3rd	Assignment	High Tech Staffing	<input type="checkbox"/>	<input type="checkbox"/>
64bit int	Order	High Tech Staffing	<input type="checkbox"/>	<input type="checkbox"/>
ACA Safe Harbor Rate of Pay	Employee	System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Account Code	Assignment	System	<input type="checkbox"/>	<input type="checkbox"/>
acct code	Assignment	High Tech Staffing	<input type="checkbox"/>	<input type="checkbox"/>
Activation Date	Customer	High Tech Staffing	<input type="checkbox"/>	<input type="checkbox"/>
AFE - Authorization for Expenditur...	Customer	Memphis NE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Alternate Badge Number	Employee	High Tech Staffing	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Alternate Customer Number	Customer	High Tech Staffing	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Save

Once a custom data security group is created, the group will display every active custom data field that is in your system. Click on the column headers to reorganize the list of fields.

Five columns will display on the custom data properties to define each field:

1. **Name**- The name of the custom field.
2. **Origin Type**- The record the field applies to.
3. **Hier**- The hierarchy in which the field exists.
4. **Deny Read**- When checked, the field **will not be viewed** by a member of this group.
5. **Deny Write** - When checked, the field **will not be editable** by a member of this group.

custom data properties 181 properties. Deny Read:49, Deny Write:51

Name	Origin Type	Hier	Deny Read	Deny Write
ACA Safe Harbor Rate of Pay	Employee	System	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Alternate Badge Number	Employee	High Tech Staffing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Attitude Rating	Employee	High Tech Staffing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Badge ID	Employee	High Tech Staffing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Badge ID ex	Employee	High Tech Staffing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
BADGE IDENTIFICATION	Employee	High Tech Staffing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Badge Issued	Employee	System	<input type="checkbox"/>	<input type="checkbox"/>
Badge Number	Employee	High Tech Staffing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Badge Number	Employee	High Tech Staffing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Badge Number	Employee	High Tech Staffing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Badge Number 12	Employee	System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Barbie Experience	Employee	High Tech Staffing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Belt Size	Employee	High Tech Staffing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Birthdate	Employee	High Tech Staffing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Note If a field is not checked, it will be visible to the user.

Note If a field is currently inactive in the administration section of Enterprise under custom data, it will not be viewable.

Customer Status Security Groups

This security group governs a service rep's ability to update customer statuses. Select statuses that members of this group should be able to change:

create new security group

Security Group Type: **Customer Status**

Hierarchy: High Tech Staffing

Name: Branch Managers

Description: For Branch Managers

Select customer status values to be included in the new security group

- A Active
- B Bid
- C Credit Check in Progress
- D Do Not Service
- H Hold for Credit Check
- I Inactive
- L Lost
- N No longer valid
- P Prospect

Cancel Save

In the example above, the users in this group will be able to change any customer record except a customer with the status of "No Longer Valid."

Note Service reps that do not belong to any customer status security groups will not be able to update customer records in Beyond.

Document Type Security Groups

This group governs the document types that are available so be seen/created/deleted by service reps. Select whether or not the members of this group may read/write/delete these document types:

? X

create new security group

Security Group Type: **Document Type**

Hierarchy: High Tech Staffing

Name: Branch Managers

Description: For Branch Managers

Select document types to be included in the new security group

Document Type	Can Read	Can Write	Can Delete
Applicant Portal Resume	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Background Check	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Care Now Report	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CIA Result	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer call	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Documentation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Federal 8850	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal 9061	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal 9062	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

X Cancel Save

Note It should be an exceptionally rare occurrence that any group be given the ability to delete documents.

Editing Existing Groups

An existing group may be edited by selecting/deselecting the check-boxes representing that group's permissions:

3 items available + [icon] x

security group

Name: All Permission

Description: All Permission

Hierarchy: High Tech Staffing

permissions 12 of 14 permissions selected

- employee-bankaccount-updatewhileinachrun**
Can update an employee bank account while in a staged ACH run
- employee-eeo-create**
Can create employee EEO information
- employee-eeo-read**
Can read employee EEO information
- employee-eeo-update**

members + x

Rep Full Name	Active	SrIdent
Darek.Wolke	<input checked="" type="checkbox"/>	23039

Adding Members/Service Reps to Security Groups

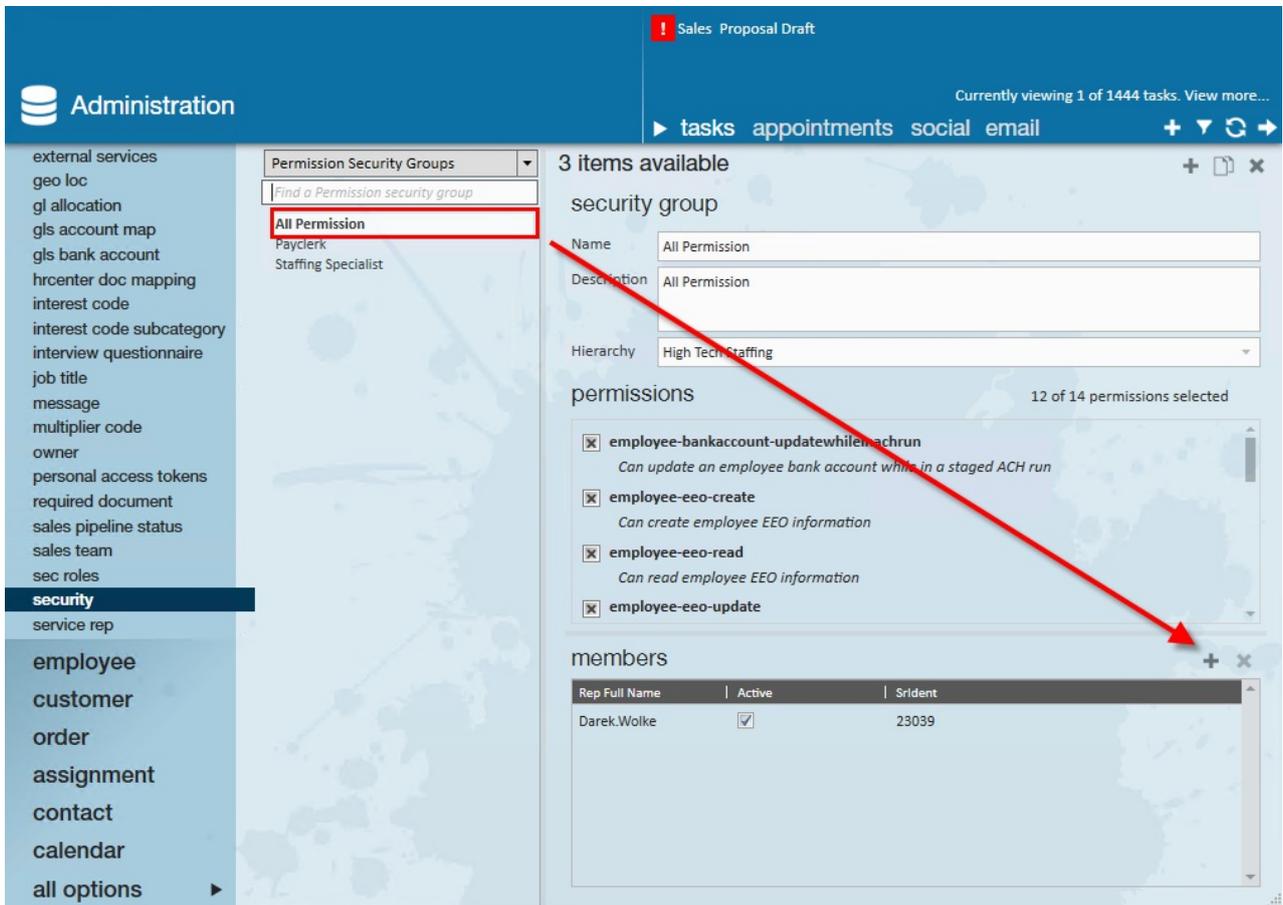
Members can be reviewed from the 'members' section on the security form:

members + x

Rep Full Name	Active	SrIdent
alexander.swanson	<input checked="" type="checkbox"/>	24213

There are two ways to add members/security reps to a security group:

1. From within the security form, simply select the group you wish to review the members of and select the '+' icon:



Here, a wizard will appear where a service rep can be selected.

Note If service rep already has a security group for the selected type, they will be deleted from that group and added to the new group.

add member to security group

Security Group Type: **Permission**

Name: **Staffing Specialist**

Description: **Standard Staffing specialist**

Select a service rep to add to this security group: alexander.swanson

Warning: The service rep that you selected is already a member of the [Payclerk] security group.

If you proceed, this service rep will be removed from that security group and added to the [Staffing Specialist] security group.

Cancel Save

2. This can also be achieved from the 'service rep' form. Here, the service rep may be selected and their security group may be determined or changed per type listed:

Administration

! Sales Proposal Draft

Currently viewing 1 of 1444 tasks. View more...

tasks appointments social email

Find a service rep 233 items available

Active

Rep Full Name

- Adam Helgeson
- Administrator
- Alec Wojciechowski
- Alex Binstock
- alexander.swanson**
- Asif Irani
- Aliesch Sutton
- Alissa Anundson
- Allison Giese
- Amanda LeBrun
- andrew
- Andrew Larson
- ben
- Brad Cox
- Brandon Johnson
- brianr
- Casey Kraus
- Claudette Jaswa
- colin

Reps Hierarchy

- Hier ID Allowed System
- Hier ID High Tech Staffing
- Branch ID Memphis SE

Main Rep Info

- SRIdent 24213
- Active
- Rep Name alexander.swanson
- Rep Full Name alexander.swanson
- Initials AS
- EINC 0
- Email alexander.swanson@tempworks.com
- Phone Number (651)452-0366
- Order Type Temp
- Sales Team ID AJ & Sarah
- Time Zone Central Standard Time
- Use Daylight Savings
- Web Portal System

Security Groups

Select security groups that service rep belongs to.

Permission Reports

Staffing Specialist

6 of 14 permissions in security group

- employee-bankaccount-updatewhileir
Can update an employee bank account while in a staged ACH run
- employee-eeo-create
Can create employee EEO information
- employee-eeo-read
Can read employee EEO information
- employee-eeo-update
Can update employee EEO information
- employee-unmask-gpi
Unmask Employee SSN
- verify-case-admin
Can manage all E-Verify cases regardless of owner.
- verify-case-edit
Can create and edit E-Verify Cases

Note If you have changed a user's permissions, we recommend having the user

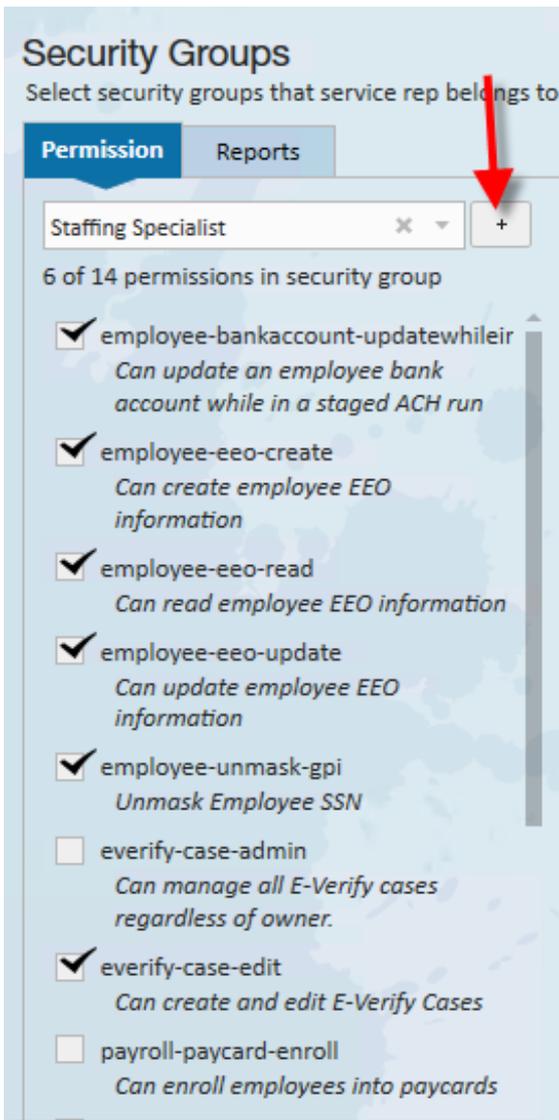
clear their system cache by either navigating to the  menu > User Settings > Clear Data Cache or by clearing the browser cache. This will ensure the permission changes are made instantly.

Data Cache

In order to provide you with the fastest possible experience, Beyond keeps some of your data on or close to your device. However, this can sometimes result in out-of-date data being displayed on the screen. If you believe this to be the case, you can clear the cache and start fresh.

CLEAR CACHE

A new security group may even be created using the '+' icon:



Note Security groups can be used to further limit what service reps are allowed to view or edit through property permissions. If you have more questions or want additional options limited, contact our support team.

Related Articles