

Introduction to Roles & Permissions



Table of Contents

Welcome to Roles and Permissions!

Chapter 1:	
Namely Roles	5
- Default roles	6
- Role management	7
- Permission descriptions	9
Chapter 2:	
Field Group Bundles	18
- Default bundles	19
- Bundle configuration	20
- Bundle and role assignment	21
Chapter 3:	
Administrator System Access	25
- User role management	26
- New profile fields	27
- Permission management	28

Roles & Permissions



	TEAMS COMPANY	Search Welcome to Namely's Roles and Permissions!
Company		
Reports Vitals Go	bals Settings	This course will provide you with extensive
General	Access Roles	knowledge in permission configuration and
Company Info	Administrator	management. We will cover the following topics
Invitations	HR admin- Rename- Edit- Clone	
Overhead	Payroll Admin- Rename- Edit- Clone	 Namely Roles
Import Data	Executive- Rename- Edit- Clone	- Default roles
Documents	Manager- Rename- Edit- Clone	- Role management
Home Page Updates	Employee- Rename- Edit- Clone	- Permission descriptions
Notifications	Manager - Approvals- Rename- Edit- Clone	
SAML	Employee - Approvals- Rename- Edit- Clone	 Field Group Bundles
Employee Data	Add Role	- Default bundles
Profile Fields		- Bundle configuration
Roles & Permissions		- Bundle and role assignment
Field Group Bundles		
		 Administrator System Access User role management

- New profile fields

- Permission management





Celebrate Ricky Thon's 10-year anniversary! Apr 1, 2015

Roles & Permissions:

Namely offers a robust, customizable framework for managing access roles and user permissions. Client access to roles and permission settings is initially disabled until administrative training is conducted.

When new Namely sites are created, four (4) default, staff access roles are added:

- Employee
- Manager
- Executive
- HR Support Admin

Each of the above roles may be adjusted and configured to the system administrators' specifications. Upon initial import, all employees are assigned the Employee access role, which is the most conservative and limited.

Namely System Administrators by default have access to view and manage all company and employee data settings. Administrators are the only users with unlimited access roles. As few individuals as possible should have this level of access to ensure system security.

Permission configurations are typically established during an organizations' initial implementation (prior to staff rollout), but may be maintained and updated on an ongoing basis.

Basic Navigation

Access role and permission settings directly from the Namely homepage. Select the **Company** tab from the upper, black ribbon dashboard.

Note:

Most individuals will not view or have access to the **Company** tab in Namely.



Employee - Approvals- Rename- Edit- Clone

Add Role

Access Roles

Roles & Permissions:

From the **Company** tab, select **Settings**. Under the **Employee Data** column, find the default user roles in the **Roles & Permissions** section.

Access Roles:

Any access role in this section is available for user assignment. Roles may be configured and managed by taking the following actions:

- Rename
- Edit
- Clone
- Delete
- Add Role

Rename Role:

Default role names may be changed to reflect an organizations' users. Select, **Rename** to update the title of an existing role's name.

Edit Role:

By selecting **Edit**, the permissions and settings behind each role will display. Administrators may adjust individual role permissions at any time. Updates become effective immediately after saving.

Clone Role:

Administrators may clone an existing role to efficiently create a new access role. When creating a new role, begin by cloning the existing **Employee** role, and then add or subtract permissions as appropriate.

Delete Role:

Administrators may delete superfluous access roles to avoid them being assigned to any users in the organization. Deleted roles may not be recovered. Ensure no user has a role assigned before deleting it.

Add Role:

An entirely new role, with no permissions prefilled or selected, may be added by selecting **Add Role**. Once added, select **Edit** to configure the role permissions and settings.

HOME PEOPLE	TEAMS COMP	ANY		۰ 🔝	Search	P
Company Reports Vitals Good	als Settings					
General	Role Emp	loyee				
Company Info		Global can log in	v			
Overhead		Global can import data				
Import Data Documents		Global can export data				
Home Page Updates		Ability: assume users				
SAML		Create announcements	v			
Employee Data		Destroy all announcements				
Roles & Permissions		Email all announcement	~			
Field Group Bundles		Create comments	~			
Change Reason Sets		Destroy all comments				
Termination Reasons		Send files to support				
organizational structure						

Ability: time off manage	P
- all	
- same departments	
- same profit center	
- same division	
- same	
- same country locations	
- same office locations	
- role under	
- same departments and role under	
- same profit center and role under	
- same division and role under	
- same and role under	
- same country locations and role under	

Permission Configuration

Access role settings are configured by selecting **Edit**, to the right of the appropriate role name.

Permissions:

Role permissions are displayed in a vertical list with a series of checkboxes. Features and settings may be enabled by selecting the applicable checkbox.

Permission Scopes:

Certain permission settings may be scoped by different criteria to facilitate unique access restrictions. By double clicking on a permission lacking a checkbox, a series of additional scope options will appear in a vertical list. Permission scopes will be specific to each Namely platform's divisions, custom teams and user roles.

Permission Scopes:

- All
- Same department
- Same division
- Same profit center and same department
- Report under via team
- Report under via company
- Directly report under via company
- Directly dotted line under via company
- Self

Scopes help define the breadth of a user's management capability in Namely. One or more scopes may be selected and combined to expand or limit a user's access level. The amount of scopes will vary based on your organization's use of divisions and teams. Infinite scope combinations are possible. Layered permission scopes require a user to meet all requirements, i.e. the user must be a member of both the departments and divisions in the scope.

Exceptions:

Feature permissions with scopes accommodate access exceptions effortlessly. Exceptions may be defined by a division, access role or unique user name.

Whitelists:

Alternatively, feature scopes also support providing divisions, departments, access roles or unique user names with a particular permission privilege. The act of whitelisting allows for permission privileges to be granted on a selective basis.



Role Employee	
Global can log in	~
Global can import data	
Global can export data	
Ability: assume users	
Create announcements	
Destroy all announcements	
Email all announcement	~
Create comments	\checkmark
Destroy all comments	
Send files to support	
Company can view vitals	
Company can view reports	
Company settings info	

Permission Descriptions

Global can log in: Grants login access to Namely HRIS.

Global can import data:

Allows a user to import CSV files via Namely's import tool in Company Settings.

Global can export data:

Enables a user to be able to export data files.

Ability: assume users:

Only administrators are able to assume other users' profiles. This permission allows other access roles to view as the profile of another employee.

Create announcements:

Share an update in the organization's newsfeed on the Namely Homepage.

Destroy all announcements:

Allows the user to audit the organization's newsfeed, and delete inappropriate announcements shared by others.

Email all announcement:

Enables the checkbox "Email update to all" when sharing announcements in the newsfeed. Without this permission, users may only post directly to the newsfeed with no emails.

Create comments:

Permits users to comment on previously shared announcements, including activity posts from the Namely widgets (i.e. birthdays, new hires and work anniversaries).

Destroy all comments:

Allows the user to audit previously shared comments, and delete any comments that are inappropriate.

Send files to support:

Permits a user to access the Support File portal, through which confidential, proprietary data files may be sent to the Namely Support and Services teams. A user with this permission, may also access and view other previously sent support files. Password protect all sensitive files.



Company can view vitals	
Company can view reports	
Company settings info	
Company settings overhead	
Company settings team categories	
Company settings skill tags	
Company settings divisions	
Company settings performance review ratings	
Company settings job titles	
Company settings roles	

Permission Descriptions

Company can view vitals:

Allows the user access to the Company's Vitals dashboard, which displays utilization on custom teams, growth percentages, new hires and departures (within the last 30 days), and company-wide performance levels.

Company can view reports:

Allows the user to access a small library of standard reports viewable in the Company tab.

Company setting info:

Grants access to the company info tab within the Company Settings, under the General section.

Company settings overhead:

Allows a user to view and update the company overhead multiplier and annual billable hours per person.

Company settings team categories:

Opens the user to the Team Categories tab under Employee Data in Company Settings.

Company settings skill tags:

Allows the user to manage the company's list of skill tags, which once created may be assigned and searchable. Users may also create their own skill tags, if allowed.

Company settings divisions:

Allows a user to manage the divisions viewable on the Team page of Namely.

Company performance review ratings:

Permits the user access to manage the custom performance rating labels and colors in the Performance section of Company Settings.

Company settings job titles:

Grants the user access to manage job titles and tiers. Users with this permission may add, edit or delete job titles and tiers.

Company settings roles:

Enables the user to access and manage the platform's roles and permissions.

Company settings terminated reasons	
Company settings fields	
Company settings time off	
Company settings notifications	
Company settings documents	
Pay groups	
Company settings goals	
Company settings goals	
Company settings goals Company settings competencies Company settings holidays	

Permission Descriptions

Company settings terminated reasons:

Permits the user to manage the custom termination reasons that are tagged to departed employees' profiles.

Company settings fields:

Allows the user to manage the creation of custom profile fields, as well as the organization and layout of the profile field display to users.

Company setting time off:

Grants the user access to time off types, plans, settings and employee assignment in the Company Settings.

Company settings notifications:

Allows a user to manage the global time off notifications for all users on the platform.

Company settings documents:

Permits the user to upload, download and manage the company wide documents that are viewable in all employees' profiles.

Pay groups:

Grants the user access to manage a payroll client's pay groups. Initially pay groups are created and assigned by the Namely Implementation team.

Company settings goals:

Allows a user to view and update the organization's goals in the Company tab.

Company settings competencies:

Permits the user access to manage and assign employee competencies in the Performance section of Company Settings.

Company settings holidays:

Grants the user access to view, create and manage the company holiday plans.

Company settings workflow templates:

Enables the user to access and manage the organization's workflow templates for employee and manager change requests.



Reporting engine	
Integrations zenpayroll	
Integrations payroll admin	
Integrations payroll	
Integrations payroll timesheet always on	
Integrations payroll paystub always on	
Tasks manage all	
Tasks can create	~
Team add remove teams	
Team draft share	

Permission Descriptions

Reporting engine:

Permits the user to gain access to the reporting engine to create custom reports. Note a users' permissions will always be respected in the reporting engine; users are not able to report on data beyond their permission settings.

Integrations zenpayroll:

Deactivated permission.

Integrations payroll admin:

Grants the user access to Namely Payroll as an administrative user.

Payroll timesheet always on:

Enables an hourly user's ability to enter their time into time cards and against projects or jobs.

Payroll paystub always on:

Allows a user to access the Pay Stub tab in Namely Payroll to view their current and historical pay checks.

Tasks manage all:

Grants the user access to manage all task lists created on the platform. By default, users are only able to manage the task lists created by them or lists of which they are owners.

Tasks can create:

Enables the Tasks feature, accessible from the users' personal springboard on the Namely Homepage.

Team add remove teams:

Activates the Custom Team feature, accessible from the Team page. Users may add or delete teams.

Team draft share:

Grants the user access to view any Custom Team with a status of draft.



Team can view goals	
Ability: team read structure	- All
Ability: team read reports	- All
Ability: team modify structure	- All - Lead of teams
Ability: team modify settings	- All
Ability: team modify goals	
User create	
User delete	
Ability: user can view tier salaries	
Ability: user see	- All

Permission Descriptions

Team can view goals:

Permits the user to view the goals of Custom Teams. This does NOT allow users to view division or departmental goals.

Ability: team read structure:

Allows users to view the reporting relationships (org charts) within Custom Teams.

Ability: team read reports:

Grants the user access to the library of standard reports viewable within each Custom Team. Users lacking permission to view salary, experience or performance, will not view activity in the reports.

Ability: team modify structure:

Enables a team member (usually Lead of Team) to change reporting relationships within the Custom Team.

Ability: team modify settings:

Allows a user to access the Custom Team Settings, and make changes to all of the existing settings.

Ability: team modify goals:

Grants the user access to create, edit and delete Custom Team goals.

User create:

Enables the Add New Person tab viewable on the People page.

User delete:

Allows a user to delete an employee profile. Note this is not recommended. Profiles may be set as Inactive (user status) and archived. Deleted profiles are not recoverable or accessible.

Ability: user can view tier salaries:

Grants the user access to view tiered salary comparisons in the Compensation & Benefits tab of users' profiles.

Ability: user see:

Permits a user to see and be seen by other users in the platform.

Ability: user add to team	
Review create	
Review delete	
Review template create	
Ability: review view	- Self
Ability: review manage	
Review view all self reviewers	
Review batcher manage	
Ability: access hidden goals	- Report under via Company - Self

Ability: time off manage

Ability: user add to team:

Allows the user to add others to a Custom Team.

Review create:

Enables the user to utilize the Review Creation tool in Performance Management. This tool is not recommended.

Review delete:

Grants the user access to delete a performance review. Deleted reviews are not accessible or recoverable.

Review template create:

Enables a team member to access and manage performance review templates, including the template index page and folders. This permission must be combined with Review Create to allow a user to update templates.

Ability: review view:

Allows a user to view feedback shared with them in performance review cycles. Typically this is scoped to 'Self' for employees to access only their own information.

Ability: review manage:

Grants the user access to manage the reviews of others. Typically managers have this permission scoped to their direct reports' performance reviews.

Review view all self reviewers:

Enables the employee to view their previously provided feedback on other users' performance reviews. In other words, users are able to see all reviews that they have written.

Review batcher manage:

Allows a user to access and manage the performance review cycle wizard. Note with this access, users will be able to view and manage all performance review cycles.

Ability: access hidden goals:

Grants the user access to view goals in draft status.

Ability: time off manage:

Permits a user to approve and decline time off requests for others. Typically scoped to direct line employees.



- All	Ability: time off basic view
	Ability: division modify settings
- All	Ability: division read structure
	Ability: division modify goals
	Api permanent access token
	Api access
	Change requests manage all
	Company settings saml
	Edit onboarding templates
	Administer onboarding sessions

Permission Descriptions

Ability: time off basic view:

Allows the user a basic view of time usage in the Namely Calendar, not in the Time Off & Sick Leave section of profiles.

Ability: division modify settings:

Enables the user to modify the organization's division's settings, (e.g. divisions, departments etc.).

Ability: division read structure:

Grants the user access to view all division reporting relationships and org charts.

Ability: division modify goals:

Enables a team member to access and modify division goals.

API permanent access token:

Allows a user to have full and complete access to the platform, with the ability to manage the API access token and connection.

API access:

Grants the user access to manage and interact with the API on a limited basis, with permission scopes implemented.

Change requests manage all:

Allows a user to manage all submitted change requests company-wide. Typically users are only able to manage the requests submitted to them for approval.

Company settings SAML:

Permits a user access to setup and manage single sign-on (SSO) on the platform.

Edit onboarding templates:

Grants the user access to view, create, edit and delete onboarding templates used to induct new hires onto the platform.

Administer onboarding sessions:

Allows a user to administer and manage onboarding sessions for new hires.

Bundle: hr admin read		Role Field Gr
- user read		Beneath the p
- user edit		Field group bu
- user request		and modified.
Bundle: manager reports to edit		Once assigne the profile field
- user read		themselves, th
- user edit	- Directly Report under via Company	_
- user request		Save: After updating select Save ir
Bundle: manager reports to read		
- user read	- Report under via Company	
- user edit		
- user request		
_		

Permission Descriptions

Role Field Group Bundles:

Beneath the permission settings of every access role, a group of field group bundles will display. Field group bundles within the role, control the aspects of a users' profile that may be viewed and modified.

Once assigned, field group bundles determine the profile fields a user may view and edit of themselves, their peers, and their direct reports.

After updating a access role's permissions, select **Save** in the bottom left corner.

Activity 1:

Navigate to the Roles & Permissions section of Company. Name all of the existing roles displayed.

Activity 2:

Navigate to the Roles & Permissions section of Company. Select the Employee role, and clone it. Next rename the role 'IT - Asset & Equipment Management'.

Activity 3:

Navigate to the Roles & Permissions section of Company. Access the role titled, 'IT - Asset & Equipment Management' and select edit. Add the ability to run custom reports.



Notes:			



- user read	- user read
- user edit	- user edit
- user request	- user request
rts to edit	undle: manager reports to edit
- user read	- user read
- user edit - Directly Report under via Company	- user edit
- user request	- user request
rts to read	undle: manager reports to read
- user read - Report under via Company	- user read
- user edit	- user edit
- user request	- user request

Role Field Group Bundles:

Beneath the permission settings of every access role, a set of field group bundles will display. Field group bundles within the role control the aspects of a users' profile that may be viewed and modified.

Once assigned, field group bundles determine the profile fields a user may view and edit of themselves, their peers, and their direct reports.

Manager reports to edit:

Refers to the profile fields a manager may edit in the profiles of their direct reports.

Manager reports to read:

Refers to the profile fields a manager may only view in the profiles of their direct reports.

Field Group Bundle Scopes:

Every field group bundle has a series of scopes by which users may read, edit and request information. By double clicking on the three options, (e.g. user read, edit and request), a series of additional scope options will appear in a vertical list. Permission scopes will be specific to each Namely platform's divisions, custom teams and user roles.

Permission Scopes:

- All
- Same department
- Same division
- Same office location
- Same profit center
- Same department and same office location
- Same department and same division
- Same division and office location
- Report under via team
- Report under via company
- Directly report under via company
- Directly dotted line under via company
- Self

Scopes help define the breadth of a user's management capability in Namely. One or more scopes may be selected and combined to expand or limit a user's access level. The amount of scopes will vary based on your organization's use of divisions and teams. Infinite scope combinations are possible. Layered permission scopes require a user to meet all requirements, i.e. the user must be a member of both the departments and divisions in the scope



Bundle: hr admin read	
- user read	
- user edit	
- user request	
Bundle: manager reports to edit	
- user read	
- user edit	- Directly Report under via Company
- user request	
Bundle: manager reports to read	
- user read	- Report under via Company
- user edit	
- user request	
Save	

Field Group Bundle Scopes

Scope types

- User read
- User edit
- User request

Exceptions:

Field group bundles with scopes accommodate access exceptions effortlessly. Exceptions may be defined by a division, department, access role or unique user name.

Exception Scenario:

The access role 'Regional Director (North America)' allows the user to view the compensation, time off, goals, and performance history for all staff ranked lower in the reporting tree EXCEPT for the users in Finance, Operations and Sales divisions for the Canada office location.

Whitelists:

Alternatively, feature scopes also support providing divisions, departments, access roles or unique user names with a particular permission privilege. The act of whitelisting allows for permission privileges to be granted on a selective basis.

Field Group Bundle Assignment:

By not selecting a scope type within the role's field group bundle, the permission is not granted to the user. All field group bundles created will display at the bottom of every role, but only those bundle rights relevant to the users' role should be assigned.

Save:

After updating a access role's permissions, select **Save** in the bottom left corner.

HOME PEOPLE TE		A 🔍 Search	P
Company Reports Vitals Goals	Settings		
General Company Info	Field Bundles View Grid		
Invitations	Approvals - Manager Edit - Rename - Edit		
Import Data	 Approvals -Self Edit - Rename - Edit Basic All - Rename - Edit 		
Documents Home Page Updates	 Basic Edit Self - Rename - Edit Basic Read Self - Rename - Edit 		
Notifications	 HR Admin Edit - Rename - Edit HR Admin Read - Rename - Edit 		
SAML Employee Data	 Manager Reports to Edit - Rename - Edit Manager Reports To Read - Rename - Edit 		
Profile Fields	Add Field 0	Sroup Bundle	
Field Group Bundles			

Field group bundles map to the unique field configuration in each Namely platform.

Add Field Group Bundle:

As your list of custom user roles grows, it may be necessary to create additional field group bundles. Create a new bundle by entering its name and selecting **Add Field Group Bundle**. After creation, the bundle may be customized and assigned in user access roles.

Rename Role:

Default bundle names may be changed to reflect an organizations' users. Select, **Rename** to update the title of an existing bundle's name.

Edit:

By selecting **Edit**, the permissions and settings behind each role will display. Administrators may adjust individual role permissions at any time. Updates become effective immediately after saving.

Delete Role:

Administrators may delete superfluous access roles to avoid them being assigned to any users in the organization. Deleted roles may not be recovered. Ensure no user has a role assigned before deleting it.

View Grid:

Select View Grid beneath Field Bundles to view all field bundles map to their respective profile fields with permission rights assigned according to each users' role.



🧳 н	ome pe	OPLE	TEAMS	COMPANY									٩	R -	Search	
Comp	any															
Reports	Vitals	Goals	Settin	gs												
Conoral			Field	Crid												
Company I	nfo		Field	Ghà												
Invitations																
Overhead					ţ								p			
Import Data	a				ger Edi	ij						to Edit	To Rea			
Document	S				- Mana	-Self E		Self	I Self	Edit	Read	eports	leports			
Home Page	e Updates				Irovals	rovals	ic All	ic Edit	ic Read	Admin	Admin	ager R	lager R			
Notification	ns				i)App	i)App	i)Bas	i)Bas	i)Bas	i)HR	i)HR	i)Mar	i.) Mar			
SAML			Gener	ral))))))	0)	0			
Employee	Data		Pro	ofile Photo (HR appropriate,			¥	•								
Profile Fiel	ds			GUID												
Roles & Pe	rmissions			Eirst name												
Field Group	p Bundles	>		Prist name			×.						-			
Workflow E	ditor			Preferred name				×								
Change Re	ason Sets			Middle name			2									
Terminatio	n Reasons			Last name			2									
Organizati	onal Structur	70		Access role						Ø						
organizau		e	Core	User status Performance Competencies						•						
			Coun	seling Documentation Form												
			Per	formance Improvement Plan												
			Fm	ployee Company Handbook												
				Travel Expense Policy												
			Em	Personal & Contact												
			Ell	List												
			Sexu	al & Substance Abuse Policy												
				Offer Letter				¥	ø							
				NDA												
				W-2												
				Incident Report												
				I-9 Form												
				Performance Review Report												
				New Hire Package												
				Visa Documentation				Ø	ø							
				Passport												
			Othe	r												
			Com	petencies												
				Competency			V									
			Sa	10												

Field group bundles map to the unique field configuration in each Namely platform.

View Grid:

2

Select **View Grid** beneath **Field Bundles** to view all field bundles map to their respective profile fields with permission rights assigned according to each users' role.

Field Group Bundle Grid:

The Field Group Bundle Grid depicts how field group bundle permissions are assigned to user profile fields.

Profile Fields:

Standard and custom profile fields list in the left vertical column. Profile section headers (e.g. General, Skills & Experience, Compensation, Teams & Allocations, Performance, Goals etc.) display in bold. As new custom profile fields are created, they will display in this list.

Group Bundles:

Group bundles display across the top of the grid. View the role assignments by selecting the letter (i) for information. Field group bundles unassigned to roles will be blank.

Save:

After updating field group bundle permissions, select **Save** in the bottom left corner.

Activity 1:

Navigate to the Field Group Bundles section of permissions. List all of the existing Field Group Bundles.

Activity 2:

Navigate to the Field Group Bundles section of permissions. Add a new field group titled, 'IT - Edit / Read'

Activity 3:

Navigate to the Field Group Bundles section of permissions. Select View Grid. In the vertical profile field list, select the asset and equipment management fields in the 'IT - Edit / Read' column. Next, return to the role 'IT - Asset & Equipment Management' and assign 'User Read - All' and 'User Edit - All' in the new Field Group Bundle 'IT - Edit / Read'.



Notes:	

Administrator System Access

omp	anv													
eports	Vitals	Goals	Setting	S										
			F 1-1-1	0.14										
eneral	ofo		Field	Grid										
ultations	110													
workoad													_	
aport Data					er Edit	t						o Edit	o Read	
ocuments					Manag	Self Edi		elf	Self	諎	ead	ports t	ports 1	
ome Page	Undates				- slavo	S- slevo	AII	Edit Se	Read S	dmin Ec	dmin Re	ger Re	ger Re	
otification	is) Appro) Appro) Basic) Basic) Basic) HR Ac) HR Ad) Mana) Mana	
AML			Genera	al	į)	Ĺ.	i)	i)	(i	Ĺ.	(i	Ĺ)	(i	
			Prot	ïle Photo (HR appropriate,			V	V						
mployee I	Data			please)										
offie Field	as			GUID										
oles & Per	missions Duadlas	~		First name			Ø						8	
ela Group	Bundles	1		Preferred name			Ø	Ø						
orkflow E	ditor			Middle name			ø						•	
nange ke	ason Sets			Last name			•						0	
ermination	n keasons			Access role						¥				
rganizatio	onal Structur	е		User status	Ø					Ø				
			Core P	erformance Competencies				۷						
			Couns	eling Documentation Form				Ø						
			Perfo	rmance Improvement Plan				Ø						
			Emp	loyee Company Handbook			ø							
				Travel Expense Policy										
			Eme	ergency Protocol & Contact List										
			Sexua	& Substance Abuse Policy									0	
				Offer Letter				¥	¥				2	
				NDA									0	
				W-2										
				Incident Report										
				I-9 Form										
			P	erformance Review Report										
				New Hire Package										
				Visa Documentation				¥						
				Passport										
			Other		_	_	_		_					
			Comp	etencies										

New Profile Field Permissions:

Q

Administrators may create new custom profile fields in the Profile Field section of Company Settings. Once created, administrators are the only ones to view and edit these fields until permissions are assigned to other access roles.

New Fields in the Field Group Bundle Grid:

Depending on the type of profile field created, administrators may navigate to the Field Group Bundle section of Employee Data in Company Settings. In the vertical column, apply the appropriate check marks to allow for view and edit rights for the applicable access roles.

Profile Field Permission Confirmation:

Upon adjusting custom profile field permissions, assume the corresponding user profiles to confirm that they're able to view and edit the field data as intended.

	HOME	PEOPLE	TEAMS	COMF	PANY	۵.	- Search	Q
Pe	onle							Add New Person
Dire	ectory Org	g Chart						
Fi	nd Employees				Name	Title	Location	
5	Search name or	title 🔍			Marcie Aldridge	Chief Operations Officer	London	
E	By Team	_			Tess Anderson	VP, Marketing	New York	
E	an reams By Title	-		R	Chandra Ardis	Marketing Strategist	New York	
E	by Tier	-		P	Monica Asea	Director of Product	New York	
E	By Skill Tag	-			Darryl Brignac	Junior Account Executive	New York	
E	By Office Location	s ans		2	Nick Christman	Marketing Director		
E	By Country Location	ons tions		2	Tammy Coco	Sales Executive	New York	
E	by Division			2	Mark Copper	Account Exective		
E	By Profit Center	•		27	Kelly Dufner	Software Developer	London	
E	by Departments	•		•	Mel Dulle	Software Developer	New York	
E	ly Status	•		đ	Christian Elderkin	UX Designer	London	
E	By Performance	s 💌		ę	Annabelle Files	Regional Sales Manager	New York	
E	by Office	•		9	Julio Freeney	Business Development Manager	New York	
E	By Access Role All Access Roles	•		3	Sarah Fye	VP, Client Services	New York	
	Filter	42 Results		g.	Neil Gatson	VP, Finance	New York	
				G.	Tania Goodwyn	Co-Founder	London	
					By Access Role			
				1	All Access R Administrato	oles r		

User Role Management

Administrators may search and filter by **Access Role** on the People page. All access roles created in Namely will surface in the dropdown menu. Select, **Filter** to view the individuals with this access role assigned.

Before modifying or eliminating an access role, confirm the individuals with the role assigned. Access roles should not be deleted until they have been unassigned to all users. Upon selecting Delete, Namely will guide you in reassigning the users to a different access role.

Administrator HR admin Payroll Admin Executive Manager Employee Manager - Approvals Employee - Approvals





💉 HOME PEOPLE	TEAMS	COMPANY		🔺 🛄 -	Search 🔎
Create New Re	port				
Report Name		Available Profile Fie	lds		
Access Roles - Q2 2015					
Select Type		Guid First name Preferred name	Departure date (days since Departure date Reason for termination	 e) Office company mo Mobile phone Office address 1 	bile
Profile		Middle name Last name	Eligible for rehire Employee	Office address 2 Office city	
Document		Job tier Start date (years since)	Company email Office main number	Office state Office zip	
Team Position		Start date (days since) Start date	Office direct dial Office phone	Office country id Office country nam	e
Team		Departure date (years sinc	e) Office fax	My bio	
Bonus		Best happy hour spot Favorite food	Date of birth (days Date of birth	since) Home country Home phone	name
Salary History		Favorite lunch spot (near t Shirt size	he office) Marital status Social security num	Personal email	ntact
Job Title		Favorite pet My one wish	Home address 1 Home address 2	Emergency co Laptop serial n	ntact phone
Time Off Request		Your sign Linkedin url	Home city Home state	Laptop Company cell	phone
Time Off Usage		Gender Date of birth (years since)	Home zip Home country id	Additional assi	gned equipment
Goal		Company credit card	Checking muting number	Posumo	Montoo notos
Review Answer		Key tag number	Checking account number	Role description	Certifications
Reviewer		Location	Savings routing number I Savings account number J	lob description	Certificate number
Performance		Banking documentation	Federal exemptions	Succession strategy	Certificate expiration date
Competency		Direct deposit information	State ming status S State exemptions S	Succession level	License name License number
Create		Direct deposit	T shirt size	experience gaps Mentor notes	License institution License expiration date
		Transcripts	Dontal amount	Healthcare coupra	e level

Permission Management:

Administrators may also access the Reporting Engine to monitor and manage access role assignment.

Reporting Engine:

Any Profile type report will include Access Role as an additional column. Select Profile as the Type of report. Once created, select Access Role in the Add Column task bar on the left side.

Apply Filters:

Apply Access Role filters to quickly view all users with an assigned access role. Print, save or download the report as needed.

HOME PEOPLE TE	AMS COMPANY	Search	P
Clinton Ton		Cancel	Save
	First Name		
30	Clinton		
10	Preferred Name		
1 Replace X Remove	Middle Name		
General	Last Name		
Skills & Experience	Ton		
Compensation & Benefits	Access Role		
Teams & Allocations	Administrator 🔹		
Performance	Leas Status		
Time Off & Sick Leave	Active Employee		
Documents			
Competencies	Employee Type Full Time		

User Role Management

Upon creating a new profile, the Access Role must be assigned to employees by an administrator with role management permissions.

HOME PEOPLE T	TEAMS COMPANY
Clinton Ton	
6-	First Name Clinton
1 Replace X Remove	Preferred Name Middle Name
General >	Last Name
Compensation & Benefits	Ion
Teams & Allocations	✓ Administrator
Performance	HR admin Payroll Admin
Time Off & Sick Leave	Manager
Documents Competencies	Manager - Approvals Employee - Approvals
	Full Time
	Job Title
	Edit History
	Start Date
	2011-04-12

Assign Access Role:

In edit mode, select the **Access Role** field. A dropdown menu of active access roles will display. Assign the appropriate role and select **Save** in the top right corner.

Administrator System Access

HOME PEOPLE	TEAMS COMPANY		- 🔍	Search	P
Vew As	Clinton Ton relative Full Profile VP, Business Development Departments Sales & Business Development Division Sales Office Locations New York City - HO Profit Center New York City - HO Profit Center New York City London Office	ths)		Email OFFICE DIRECT DIAL OFFICE DIRECT OFFICE DIRECT OFFICE DIRECT OFFICE DIRECT OFFICE DIRECT OFFICE OFF	
General >	First Name				
Compensation & Benefits	Last Name				
Teams & Allocations	Lon Access Role				
Performance	Administrator				
Goals	Active Employee				
Time Off & Sick Leave	Request: Termination Employee Type				
Documents	Full Time				
Competencies	Job Tele Executive / VP Job Titles VP. Business Development (01/25/2014 - Present)				

View As Profiles:

After updating employees' access roles, administrators may confirm their permissions by viewing as the profile of the employee.

View As:

Beneath every employees' profile, displays a blue ribbon titled 'View As'. Select this tab to assume the user's profile and confirm their permission settings.

Stop View As:

Stop viewing as a user by selecting the orange text 'Stop Viewing as...." at the top center of the Namely ribbon dashboard.



Activity 1:

Navigate to the People page of Namely. Select an individual and assign the new access role 'IT - Asset & Equipment Management'.

Activity 2:

View as the individual assigned the 'IT - Asset & Equipment Management' access role in Activity 1.

Activity 3:

After assuming the above user's profile in Activity 2, navigate to the Asset & Equipment section of a different employee's profile. Confirm that this role allows the IT user to view and edit the appropriate asset and equipment fields.

Notes:	

Notes:			

Notes:	

Thank You For Attending!

