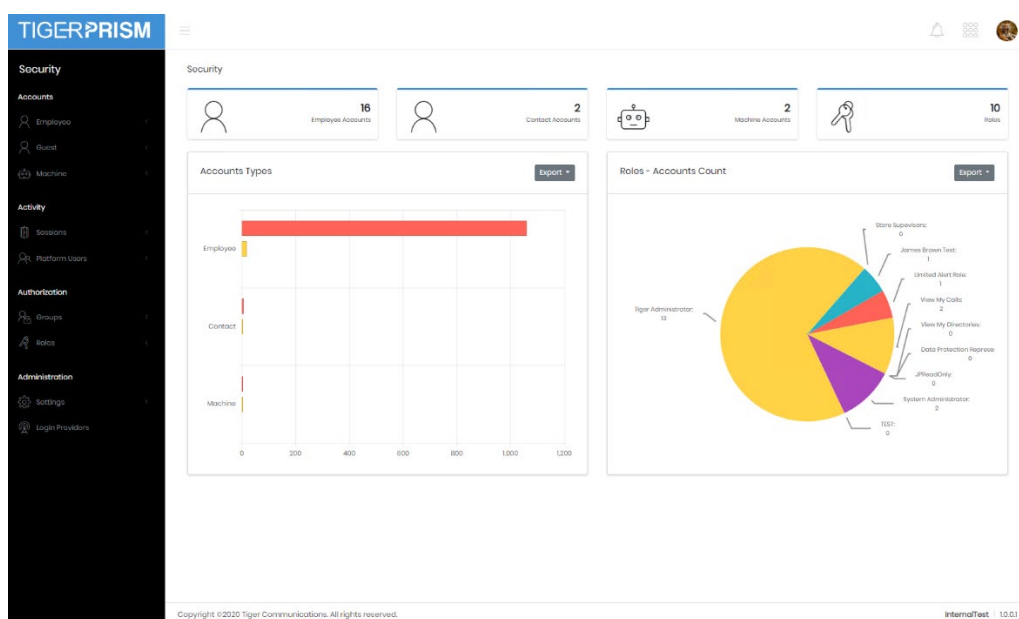


## Administrate \ Security

### Overview

The security module handles account setup and oversight, including any SAML login providers, the definition of the roles that are assigned to accounts and which data is available to users. User sessions can be monitored and terminated from security.

The landing page displays a summary of the accounts assigned by type, and the number of roles defined in Prism across the top, while the two graphs show the number of accounts by type (displaying potential account holders as actors) and the number of accounts each role is assigned to.



## Accounts

### Type of Account

There are three account types in Prism.

Employee accounts are created from people defined in the Enterprise Employee section.

Guest accounts are created from people defined in the Enterprise Contact section.

Machine accounts are created here, generally for specific tasks.

There is no difference in the function of employee, guest or machine accounts.

### Search

The search grid shows all employee/guest accounts or machines depending on the section. For standard grid controls see common features.

### Recycle Bin

When an account is deleted it goes into the recycle bin and can be restored if required again in the future. The recycle bin grid looks exactly like the search grid, but with an additional control on the right of each record to restore it.

Employee Accounts | Search

Filter

		Username	Display Name	Job Title	Last Sign In	Email Confirmed	Is Disabled
		ben.hegerl@tigerprism.com	Ben Hegerl	Senior Systems Engineer	15/05/2020 14:58:19	✓	×
		ben.hegerl@tigerprism.com	Ben Hegerl	Engineer	12/06/2020 13:10:45	✓	×
		ben.hegerl@tigerprism.com	Ben Hegerl	Systems Engineer	19/06/2020 12:57:09	✓	×
		ben.hegerl@tigerprism.com	Ben Hegerl		18/05/2020 12:43:30	✓	×
	JS	js@tigerprism.com	John Smith			×	×
		john.smith@tigerprism.com	John Smith	HR Manager	25/06/2020 10:45:21	✓	×
	JD	jd@tigerprism.com	John Doe			×	×
	JC	jc@tigerprism.com	John Doe		12/07/2020 19:29:37	✓	×
	KJ	kj@tigerprism.com	John Doe	Full Stack Developer	06/07/2020 14:27:04	✓	×
	LR	lr@tigerprism.com	John Doe			×	✓
		gmustarde@tigerprism.com	Gwendolin Mustarde	Systems Engineer	23/06/2020 14:58:03	✓	×
		ben.hegerl@tigerprism.com	Ben Hegerl	Senior Consultant Systems Engineer	30/06/2020 09:06:18	✓	×

50 Items Per Page 1 - 16 of 16 items

## Account Creation

### User Accounts

Employee and Guest account creation follow identical four step paths.

### User Selection

The first stage is to find an existing employee or contact to create the account against. The search box will display an incremental search as a name is typed in. Select the user once found. The lower part of the screen will then show preview information to help confirm that the correct user has been selected.

Employee Accounts | Create

1

2

3

✓

User Selection

Account Details

Roles

Completed

Employee

Gwendolin Mustarde

Type at least 2 characters to filter the results.

User Preview

Display Name

Gwendolin Mustarde

Job Title

Geological Engineer

Email

gmustarde@umich.edu

> Next

### Account Details

Once the correct user has been selected the second step is to configure some basic account information.

Employee Accounts | Create

Account Details

Username\*

gmustardo8s@umich.edu

Can Access Api: Off

View Digits: Off

Lockout Enabled: On

Do Not Sync: Off

Logins

Local: On

Windows: Off

Windows Username

< Previous

Next >

1. The username for the account. This defaults to the email address for the user.
2. Whether this account can make use of API functions.
3. Whether the account can see the called and calling numbers in Analyse modules. This affords digit privacy for all users while allowing the account to run reports.
4. If the account is to be locked out after a number of failed login attempts.
5. Should this this account be updated by directory integration. Most commonly this is set to On for most active accounts, but Off for accounts which have View My Activity access only.
6. Can the account log in using Prism local authentication or not?
7. Can the account log in with Windows authentication or not? If so the username to expect.

## Roles

The third step is to allocate one or more roles to the account. Each role will build up a little more of what the account is allowed to do or access. Roles are defined in the Authorization\Roles section.

Employee Accounts | Create

Roles

Filter

Selected Roles: 3

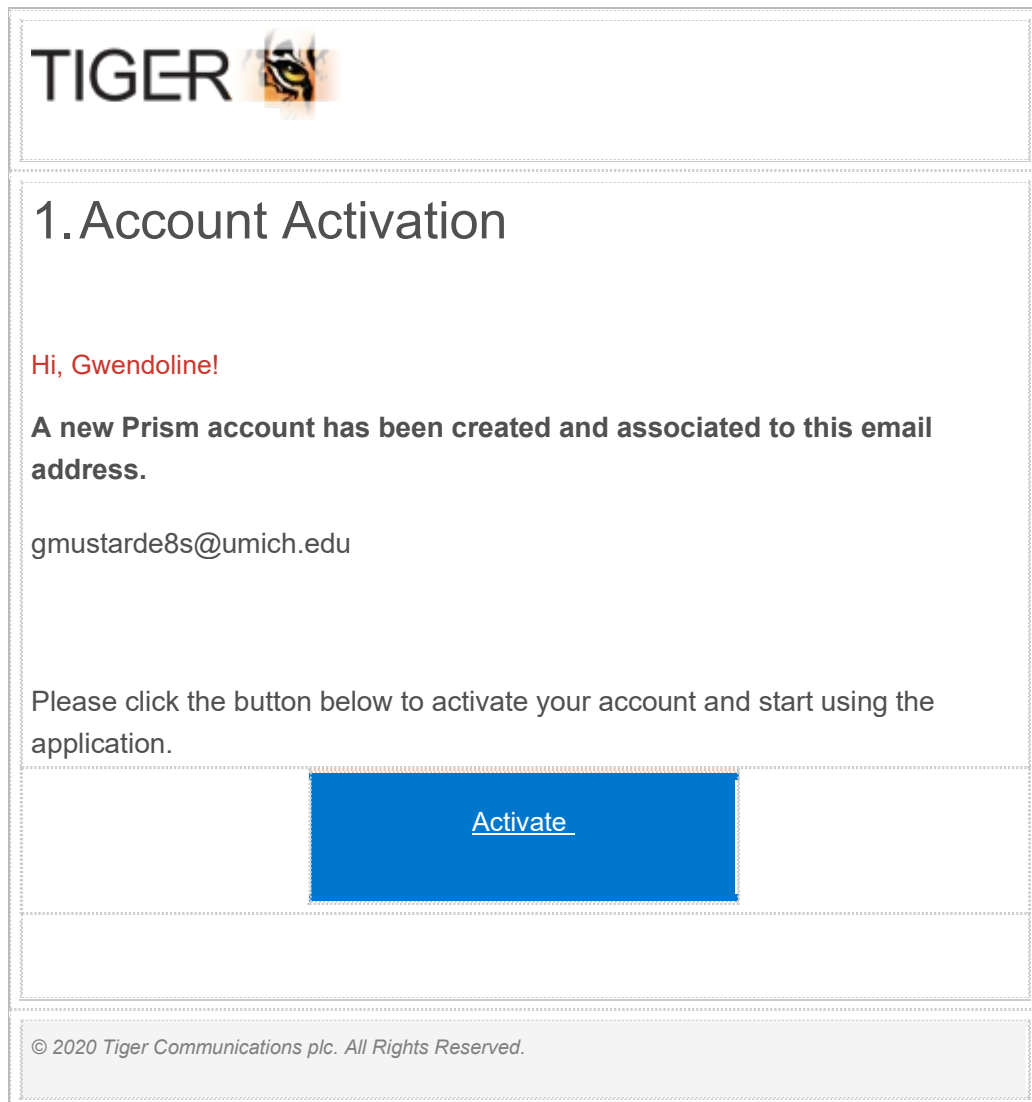
	Role Name	Role Description	Is User Defined
<input type="checkbox"/>	Tiger Administrator	Grant full access to the application (except Data Protection actions)	×
<input type="checkbox"/>	System Administrator	Grant full access to the application (except Data Protection actions)	×
<input checked="" type="checkbox"/>	View My Calls	Grant full access to the 'View My Call' module	×
<input checked="" type="checkbox"/>	View My Directories	When the 'View My Directories' role is assigned to a user, the visible tree nodes and the call data access are dynamically established based upon a user's position within a particular tree. A user will be able to see all calls made to or from the user's parent organization or any of its descendants. When viewing a tree, only parent organizations and the descendant organizations of the user's parent organization will be visible.	×
<input checked="" type="checkbox"/>	Store Supervisors	Store Supervisors Role for internal supervisors	✓

## Completed

The final step is a summary of selections to confirm that everything is correct before account creation.

## User Account Activation

As soon as a user account is created Prism sends an email to the user for account activation. The template for these emails can be edited in Settings for Security.



Until the user has responded to this, their account page will show a banner message to advise that the account is not activated, with a button to resend the activation email.



## Machine Accounts


### Machine Creation

Machines differ from user accounts. They are created here without accounts (as employees or contacts are created in Enterprise). The machine can then be given an account and assigned roles through its [detail page](#) later.

### Machine Details

Choose a type for the machine, the types are functionally the same, but allow categorisation. Then enter a unique name.

Machines | Create



The progress bar shows four steps: 1. Machine Details (active), 2. Photo, 3. Notes, and 4. Completed.

**Machines Details**

Machine Type\*  
Bot


Machine Name\*  
Autoreporter

> Next

### Photo

A picture can be assigned to help differentiate machines.

Machines | Create

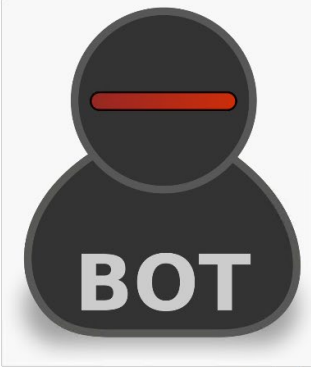


The progress bar shows four steps: 1. Machine Details, 2. Photo (active), 3. Notes, and 4. Completed.

**Photo**

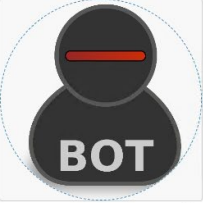
Browse | Gnome-stock\_person\_bot.svg.png

**Image**



A large preview of the selected image, which is a black silhouette of a person with a red horizontal bar across the face and the word 'BOT' in white.

**Thumbnail**



A smaller preview of the same image, showing the word 'BOT' more clearly.

< Previous

> Next

## Notes

Notes can be added against the machine if required.

Machines | Create

1 Machine Details

2 Photo

3 Notes

4 Completed

Notes

Paragraph B I U [Icons]

This machine runs reports with full dialled numbers showing.

< Previous

Next >

## Completed

Shows a summary of the information entered before creation.

## Machine Account Creation

Once the machine itself is created, an account can be added to it. Find the machine in the search grid and go to the detail page. The second tab is Machine Account, this will be empty for a new machine.

Machines | Autoreporter

Edit Photo

BOT

Autoreporter

Machine Details

Machine Account

Notes

Audit

+ Add Account

Click 'Add Account', this will start a new wizard with three steps.

## Account Details

All machine accounts are local login only, so this page is simpler than the user account equivalent.

Machines | Create - Autoreporter

1 Account Details

2 Roles

3 Completed

Account Details

Username\*

autoreporter ✓

Password\*

Confirm Password\*

Lockout Enabled ON

Can Access Api ON

Do Not Sync OFF

View Digits ON

Next >

## Roles

Roles are assigned in the same way as for [User accounts](#)

## Completed

Shows a summary of the information entered before creation.

## Detail Page

User account detail pages are the same for both employee and guest accounts. Contacts can be given exactly the same rights as employees.

Employee Accounts | James Halley

Account not activated. [Resend Activation Email](#)

**Account Details**

Username: james.halley@madcup.com

Language: English

Time Zone: (UTC+00:00) Dublin, Edinburgh, Lisbon, London

Theme: Default

Font Size: Small

**Statistics**

Total Sign Ins: 0

Last Sign In:

**Roles Authorization**

Permissions | Department - Access | Cost Centres - Access | Network Access | Reports Access | Dashboards Access

Permissions

Area Name	Module	Permission Name	Permission Description	Area Name	Module	Roles
Area Name: Analytics	Module: Telephony	Analytics Road	Grant VIEW access to the ANALYTICS management screens	Analytics	Telephony	Store Supervisors

There are four areas of the detail page.

1. The name and any picture for the employee record
2. Space for a banner message about the account
3. Details about the account itself
4. A breakdown of the exact access the roles assigned to the account have granted

## Account Details

The account details tab allows review and editing of the basic properties of the account. It has options for account lockout, API access, View Digits and Integration synchronization as well as some other user settings such as language, theme and font size. These can also be changed by the user in their own settings.

Lastly some login statistics are displayed, showing the number of time the account login has been used, and the date of the most recent login.

## Logins

The logins tab shows details of any configured login mechanisms for the account.

Account Details Logins Roles Audit

Login Providers

Windows ☐ OFF

Local ☒ ON

Windows Username

Last Local Password Change 13/07/2020 11:30:38

Last Sign In Attempt

Consecutive Failures 0

Login Providers

Login Provider Name	Login Provider Type	Login Name
No linked accounts configured		

Local, Windows and any configured SAML providers can be enabled or disabled for the user here.

## Roles

The roles tab lists all roles that have been assigned to the account.

Account Details Logins Roles Audit

Roles

Role Name	Role Description
View My Calls	Grant full access to the 'View My Call' module
Store Supervisors	Store Supervisors Role for internal supervisors

Editing the page allows additional roles to be added, or existing ones to be removed.

Account Details Logins Roles Audit

Roles

Role Name	Role Description	
Tiger Administrator	Grant full access to the application (except Data Protection actions)	<input type="checkbox"/> OFF
System Administrator	Grant full access to the application (except Data Protection actions)	<input type="checkbox"/> OFF
View My Calls	Grant full access to the 'View My Call' module	<input checked="" type="checkbox"/> ON
View My Directories	When the 'View My Directories' role is assigned to a user, the visible tree nodes and the call data access are dynamically established based upon a user's position within a particular tree. A user will be able to see all calls made to or from the user's parent organization or any of its descendants. When viewing a tree, only parent organizations and the descendant organizations of the user's parent organization will be visible.	<input type="checkbox"/> OFF
Store Supervisors	Store Supervisors Role for internal supervisors	<input checked="" type="checkbox"/> ON

## Audit

The audit tab shows the details for account creation and last modification.

## Roles Authorization

The lower part of the page shows the access available to the account based on the roles assigned.



## Activity Sessions

### Search

The search grid allows visibility over which user accounts have active, abandoned or ended sessions. For standard grid controls see common features.

Sessions | Search

Session Id	Session Start	Session End	Schema	Display Name	User Type	Last Activity	Status
733F5F2-F8A5-D633-FE90-E2B4FE291394	16/07/2020 14:43:58		local		Employee	16/07/2020 14:51:19	Active
A9C8A762-6784-C882-6D77-D58853888D8A	16/07/2020 13:58:14		local		Employee	16/07/2020 13:58:14	Abandoned
9A9E0B3E-63CD-8E80-82D8-F829720FAB5	16/07/2020 13:21:06	16/07/2020 14:44:23	Windows		Employee	16/07/2020 13:45:09	Ended
AE209DE1-4F7E-86ED-3030-16B9EB44DFAB	16/07/2020 13:09:58		local		Employee	16/07/2020 13:36:21	Abandoned
312F4ED4-6A3D-792D-0312-4B9CF3E25C79	16/07/2020 12:52:24	16/07/2020 13:22:23	local		Employee	16/07/2020 12:52:27	Ended
9794A05C-F527-5FE3-W7B-59660F0B0FA6	16/07/2020 10:52:34		local		Employee	16/07/2020 12:13:33	Abandoned
F22A1ED9-501F-FACD-04B2-6B2DEB5A3A60	16/07/2020 10:19:01		local		Employee	16/07/2020 10:34:00	Abandoned
3F810FA0-83A0-D98E-3154-51BC042E2AEA	16/07/2020 10:12:51		Windows		Employee	16/07/2020 10:12:56	Abandoned
1C06F0AB-F476-DFC4-946E-1FDBA38D5A8F	16/07/2020 09:51:16	16/07/2020 09:51:21	Windows		Employee	16/07/2020 09:51:18	Ended
4A7EB39D-A95F-70AF-BC8E-829C37E916C	16/07/2020 09:39:39	16/07/2020 09:39:44	Windows		Employee	16/07/2020 09:39:39	Ended
90476BB8-E8A9-15C5-EC45-92A0D2D08379	16/07/2020 09:39:20	16/07/2020 09:39:24	Windows		Employee	16/07/2020 09:39:21	Ended
5EA5A0CA-12A4-9DF5-7D14-83A4742EE690	16/07/2020 09:38:07	16/07/2020 09:38:53	local		Employee	16/07/2020 09:38:48	Ended
E840E8C0-8E01-B3A3-4254-7D8EC5C4196A	16/07/2020 09:32:12	16/07/2020 09:36:45	local		Employee	16/07/2020 09:32:16	Ended
38464F37-357F-AC65-83B8-E80A1B1F532	16/07/2020 09:17:04		local		Employee	16/07/2020 10:20:28	Abandoned
4187F9F9-42BF-26F3-F4CA-287ACFF7EB40	16/07/2020 09:09:15	16/07/2020 09:27:42	local		Employee	16/07/2020 09:27:38	Ended
6E066C85-9A40-B1B8-2A1A-FF24195B43A3	16/07/2020 09:03:29	16/07/2020 09:05:07	local		Employee	16/07/2020 09:04:59	Ended
97916CD0-4A84-5DB7-A4FD-BE902FEB7FD	16/07/2020 07:29:32		local		Employee	16/07/2020 07:50:57	Abandoned
EEAE9892-8F13-A714-A7B1-896C4D037CB1	15/07/2020 13:57:18		local		Employee	15/07/2020 14:18:48	Abandoned
F5AFOEBA-3919-E4F2-BAFD-BA305938CF98	15/07/2020 12:02:08		local		Employee	15/07/2020 12:02:51	Abandoned
0480EB08-D1A3-48DF-8238-9EA0CB8E014	15/07/2020 10:31:07		local		Employee	15/07/2020 13:24:55	Abandoned
F86620B3-63CC-EE89-9A35-2D239D8DD42D	15/07/2020 09:08:15		local		Employee	15/07/2020 09:08:15	Abandoned
98E8D916-2885-415B-FE0D-65C789247FC4	14/07/2020 19:40:27		local		Employee	14/07/2020 19:41:26	Abandoned
B97C89C6-FAE1-FECA-8229-9742E08363CA	14/07/2020 18:39:25		local		Employee	14/07/2020 19:43:58	Abandoned
1289A5CC-C237-F6BA-981D-48FFE2DE42A	14/07/2020 16:07:08		local		Employee	14/07/2020 16:07:14	Abandoned
6C251955-E47F-196F-8105-EF2FA6D377C5	14/07/2020 16:06:12		local		Employee	14/07/2020 16:06:12	Abandoned
60B73901-A141-4CBA-174C-458BF2013892	14/07/2020 16:04:45	14/07/2020 16:04:57	local		Employee	14/07/2020 16:04:49	Ended
B0DFBF32-F7B0-4DBC-FAEF-7FA229807F04	14/07/2020 16:04:01	14/07/2020 16:04:22	local		Employee	14/07/2020 16:04:14	Ended

1 - 50 of 708 items

### Terminating sessions

From the grid active sessions can be terminated. You cannot end your own session, but any other active user should show a control on the right of the active session record.

Sessions | Search

Session Id	Session Start	Session End	Schema	Display Name	User Type	Last Activity	Status
FE903D7-38FF-4020-38D6FA781368	13/07/2020 08:40:03		local	John Doe	Employee	13/07/2020 08:40:28	Active
3D88349D-986A-F719-75E8-A33C7C7289F	13/07/2020 07:56:00		local	Philipp Smith	Employee	13/07/2020 08:30:26	Active
EB95ECB-FE95-0F44-C39B-8E8E76X00963	13/07/2020 07:01:04		local	Philipp Smith	Employee	13/07/2020 07:04:47	Abandoned

### Platform Users

Not implemented at this time.

## Authorization

### Overview

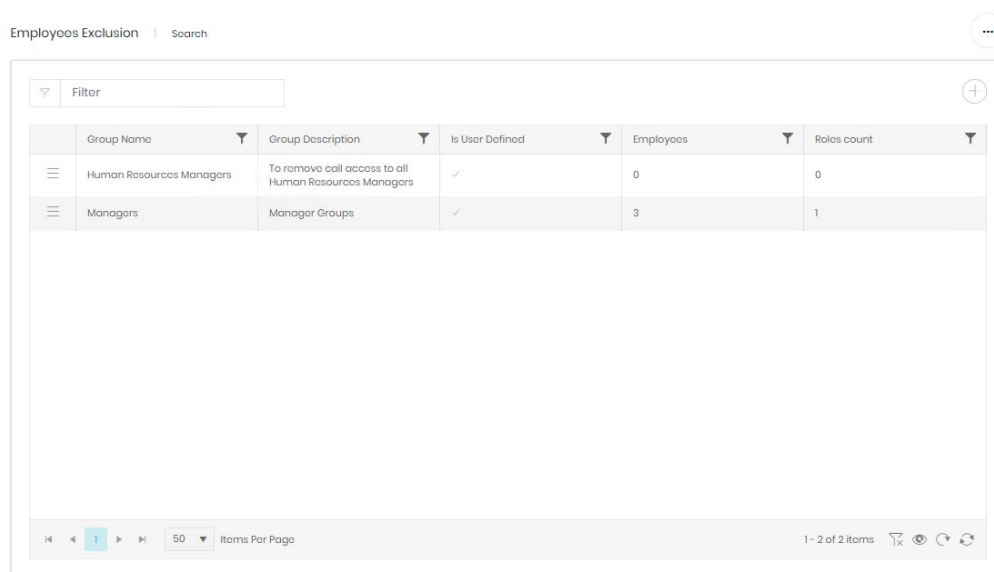
Users are authorised for access to the various functions and data in Prism by roles assigned to their account. Each role may have a set of permissions for system functions (e.g. Dashboards, or fixed charge read & write) and may have one or more Groups which convey access to specific parts of the system.

By defining groups and roles carefully, great flexibility can be given to which users are granted access to Prism's functions without having to configure users individually.

### Groups

There are 10 types of Group, although many are similar. When a group type is selected from the navigation menu it displays a management grid. For standard grid controls see common features.

Employees Exclusion | Search



	Group Name	Group Description	Is User Defined	Employees	Roles count
	Human Resources Managers	To remove call access to all Human Resources Managers	✓	0	0
	Managers	Manager Groups	✓	3	1

1 - 2 of 2 items

Each group type's grid will have slightly different columns relating to the counts of items included, and the number of roles to which the group is applied.

### Creating Groups

#### Department/Cost Centres/Projects

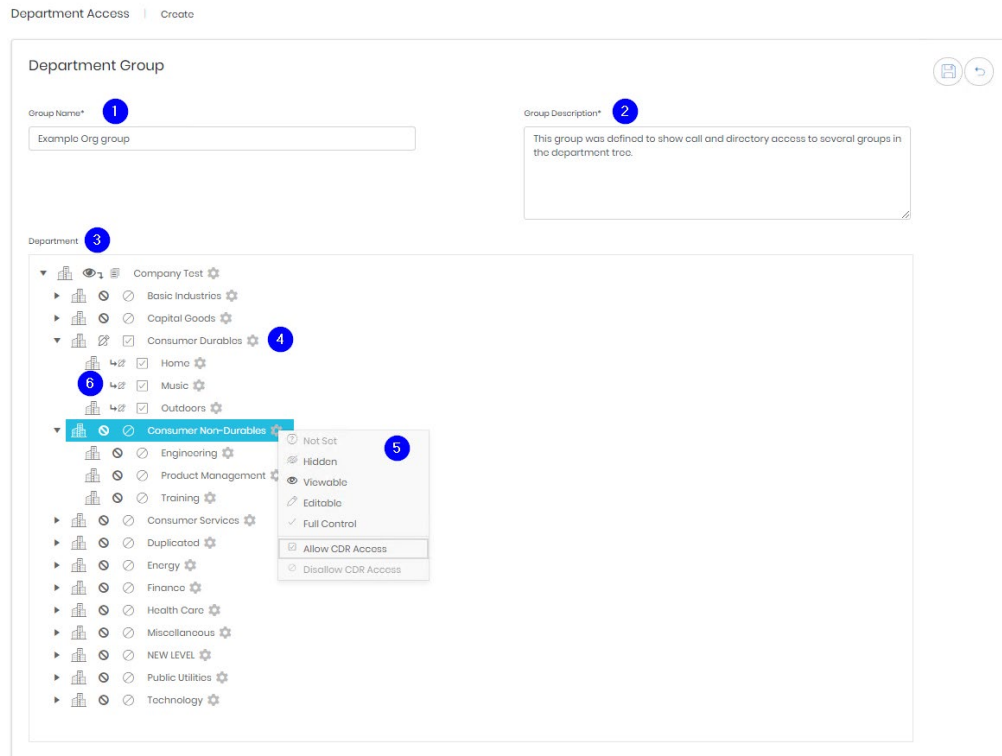
These three group types define specific access to each of the three directory trees.

There are two predefined groups in each type.

Tree Administrator gives the role access to the whole tree. Whether this is read only or not is determined by the role's permissions.

View My Directories is a special dynamic group which allows access to the organization which the current user is in, plus all descendant organizations. Whether this is read only or not is determined by the role's permissions.

Additional groups can be created for each of the three organization types and existing user defined ones can be viewed and edited from the management grid.



A new group requires a name and description (1 & 2). Below those is the tree showing the directory view chosen (3).

The organizations in the tree can be expanded to show their descendants. To the right of each organization name is a cog icon (4). When clicked this opens a menu with several controls (5). There are actually two aspects of access defined in this menu.

First is the management access level. This determines what the group allows a role to see and edit in the enterprise directory management screens. Icons corresponding to the chosen options are displayed to the left of the organization in the tree.

- Hidden – cannot be seen. This is the default state for all organisations when a group is created.
- Viewable – Can be seen in the directory, but no changes can be made.
- Editable – edits can be made to the organization's name and description. Fixed charges and tariffs assigned to it and any custom fields which have been enabled.
- Full control – All aspects of the organization can be changed, it can be moved, backdated, or deleted. New organizations can be created. This level is required to manage endpoint and authorization code assignments.

The second pair of controls govern whether or not the role can see call data for the organization.

Note that when an organization's access is changed, all descendant organizations inherit that change (6). This is shown with a slightly different icon. This inherited state can be overridden by setting the specific Management or CDR Access for the descendants.

When the access changes for the group are complete click save. The new group will now be listed and available for selection when customising a [role](#).

## Employee Exclusion

After defining access to a section of one of the directory trees there may be individual employees whose data should not be available for example higher level managers, or HR staff. These members can be added to exclusion groups which will remove them from any access granted by Department, Cost Centre or Project Groups.

Create a new group from the management grid or select an existing one.

Employees Exclusion | Create

Create Employee Group

Group Name\* **1**

Board

Group Description\* **2**

All top level management

Employees Exclusion

All Employees **3**

Filter

Display Name	Email	Job Title	
Adeline Brinson	abrinson2n@disqus.co	Quality Control Specialist	+
Adeline Brinson	abrinson2n@disqus.co		<b>5</b>
Adeline Wood	awoodqa@nih.gov	Systems Administrator IV	+
Adeline La Monnier	alamonnier6@cdc.gov	Software Test Engineer IV	+
Adana Rippingale	arippingale9@fema.gov	Developer I	+
Adorne Braawood	abroawoodr6@yale.edu	Professor	<b>7</b>
Adrien Longworthy	alongworthy2h@businesswire.com	Staff Accountant II	+
ads			+
Adriell Swin	aswinig@oracle.com	Health Coach II	+

Selected Employees **4**

Filter

Display Name	Email	Job Title	
Adorne Braawood	abroawoodr6@yale.edu	Professor	<b>6</b>
Aldon Magrannell	amagrannellat@hp.com	Professor	

A new group requires a name and description (1 & 2). Below those are two grids showing all employees (3) and selected employees (4). Both grids use the standard grid controls details in common features.

Against each employee who should be added to the group click the plus (5), this will add the employee to the selected grid. To remove them click the bin icon (6).

Employees who are already selected are greyed but remain in the All Employees grid.

When the employee selections for the group are complete click save. The new group will now be listed and available for selection when customising a [role](#).

## Network

Network groups allow CDR access for the CDR Source or channels specified in the group. This means that CDR access can be given or withheld on a geographical, or topological basis, in line with responsibilities.

## Reports

Report groups determine which specific reports are available to a role. There is a predefined group, Reports Administrator, which allows access to all reports, but groups can be set up to allow more restricted report types to users.

Create a new group from the management grid or select an existing one.

Reports Access | Create

### Create Report Group

Group Name\* **1**  
Incoming Reports

Group Description\* **2**  
All reports from the incoming category

**5**

Report Access

Report name	Access granted
Module: Microsoft Teams	
Module: Office 365	
Module: Telephony	
Report category: Detail	
Call Information	OFF
Report category: Incoming <b>3</b>	
Departmental Responses	<b>4</b> ON
Departmental Response Summary	ON
End Point Responses	ON
First Point of Answer Target Response Analysis	ON
Departmental Answer Performance	ON
End Point Answer Performance Report	ON
Customers First Point Of Answer	ON
Report category: Management	

A new group requires a name and description (1 & 2). The list (3) shows all reports from every licenced module and can be collapsed or expanded with the controls on the left. For each report that the group should allow access to set the slider to “On” (4). Two specific controls allow all sliders to be set on or off (5).

When the report selections for the group are complete click save. The new group will now be listed and available for selection when customising a [role](#).

## Exports

Export groups work in exactly the same way as [Report groups](#).

## Views

Views access groups control which elements of analytics are available to roles. There is a predefined group, Views Administrator, which allows access to all views in all modules.

Create a new group from the management grid or select an existing one.

Views Access | Create

### Create View Group

Group Name\* **1**  
Channel Group Solzura

Group Description\* **2**  
Channel Group Solzura from telephony module only

**5**

Views Access

View	Access granted
Module: Telephony	
View Category: Telephony	
Call Logs <b>3</b>	OFF
Calls	OFF
Solzuers	<b>4</b> ON

A new group requires a name and description (1 & 2). The list (3) shows all views from every licenced module and can be collapsed or expanded with the controls on the left. For each view that the group should allow access to set the slider to “On” (4). Two specific controls allow all sliders to be set on or off (5).

When the view selections for the group are complete click save. The new group will now be listed and available for selection when customising a [role](#).

## Widgets

Widget groups allow access to sets of saved analytics widgets. This allows a team to create and share widgets between them, or an administrator to create either one widget to distribute to many teams, or several widgets to deploy via a group to one or more roles.

Create a new group from the management grid or select an existing one.

Widgets Access | Create

### Create Widget Access Group

Group Name\* **1**  
Example widget group

Group Description\* **2**  
Group for the manual writing team to share widgets

Widgets **5**

Widget Name	Widget Type	View	Version	Access granted
Module: Telephony				
<b>3</b> Example Widget 1		Call Logs	1	<b>4</b> <input checked="" type="checkbox"/> ON

Full access No access

A new group requires a name and description (1 & 2). The list (3) shows all widgets from every licenced module and can be collapsed or expanded with the controls on the left. Each widget can be allocated to the group by setting the slider to “On” (4). Two specific controls allow all sliders to be set on or off (5).

When the widget selections for the group are complete click save. The new group will now be listed and available for selection when customising a [role](#).

Widget groups do not have to contain widgets on creation, they can be created empty for one or more roles to share. When a widget has been defined in analytics it can be saved to a widget group (or several groups) instead of privately.

Save As... ✕

Widget name\*  
Example widget 2 ✓

☐ Save widget just for me

☒ Save widget to the following widget groups:

☐ OFF Simple Widget Group

☒ ON Example widget group

Select All

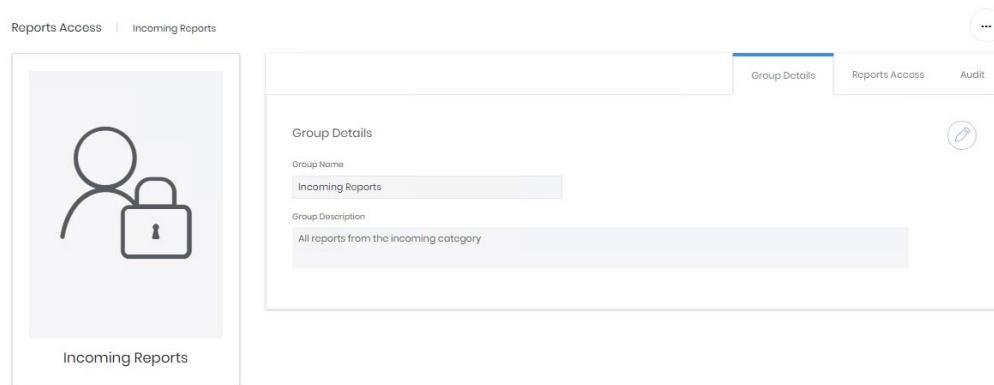
Save Cancel

## Dashboards

Dashboards groups work in exactly the same way as [Report groups](#).

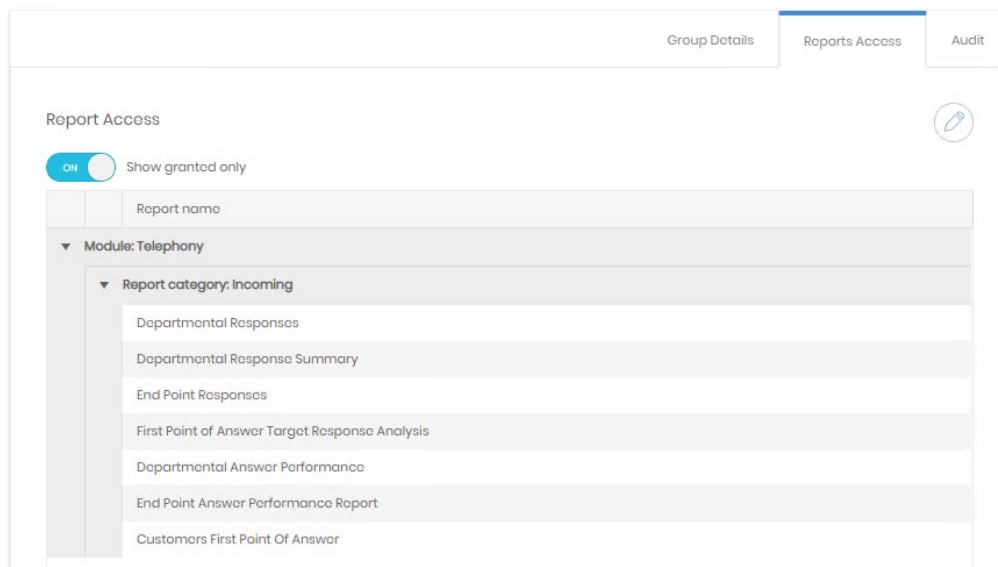
## Editing existing groups

Existing groups can be viewed in the management grid for each. The detail page for a group shows three tabs.

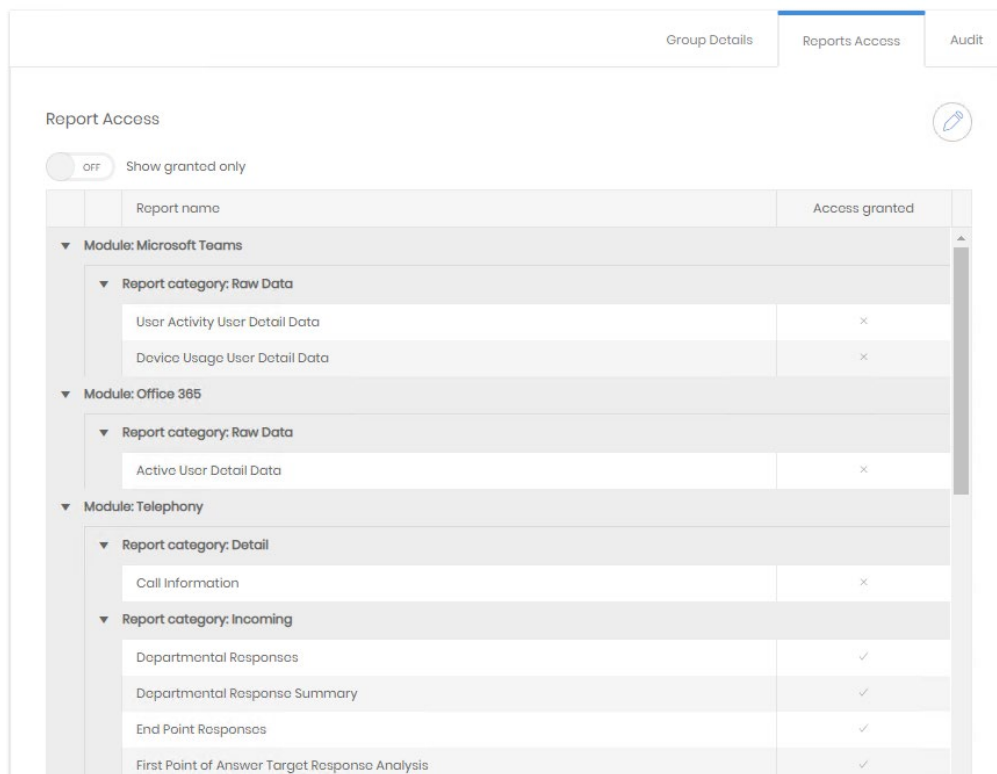


The first shows the name and description, both can be edited here

The second shows a version of the definition screen from group creation. Sometimes simplified to show only those items that have been selected.



Although the 'Show granted only' control can be switched off to show the other options available



Report name	Access granted
<b>Module: Microsoft Teams</b>	
<b>Report category: Raw Data</b>	
User Activity User Detail Data	×
Device Usage User Detail Data	×
<b>Module: Office 365</b>	
<b>Report category: Raw Data</b>	
Active User Detail Data	×
<b>Module: Telephony</b>	
<b>Report category: Detail</b>	
Call Information	×
<b>Report category: Incoming</b>	
Departmental Responses	✓
Departmental Response Summary	✓
End Point Responses	✓
First Point of Answer Target Response Analysis	✓

These options can be adjusted by editing this tab.

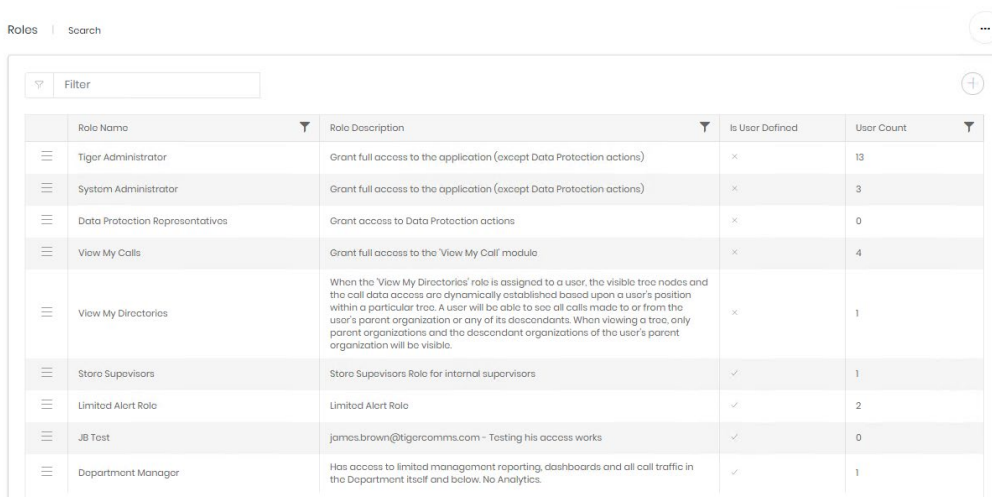
The Audit tab shows creation and last updated details.

## Roles

Each role can contain a set of permissions and one or more groups, although neither is required – a role can just supply group access or just permissions. A user account's functional and data access is defined by the sum of what is provided by the roles assigned to it. Excepting Employee Exclusion Groups roles only add levels of access.

## Search

The roles available can be found in the search grid. For standard controls see common features.



Role Name	Role Description	Is User Defined	User Count
Tiger Administrator	Grant full access to the application (except Data Protection actions)	×	13
System Administrator	Grant full access to the application (except Data Protection actions)	×	3
Data Protection Representatives	Grant access to Data Protection actions	×	0
View My Calls	Grant full access to the 'View My Call' module	×	4
View My Directories	When the 'View My Directories' role is assigned to a user, the visible tree nodes and the call data access are dynamically established based upon a user's position within a particular tree. A user will be able to see all calls made to or from the user's parent organization or any of its descendants. When viewing a tree, only parent organizations and the descendant organizations of the user's parent organization will be visible.	×	1
Store Supervisors	Store Supervisors Role for internal supervisors	✓	1
Limited Alert Role	Limited Alert Role	✓	2
JB Test	james.brown@tigercomms.com - Testing his access works	✓	0
Department Manager	Has access to limited management reporting, dashboards and all call traffic in the Department itself and below. No Analytics.	✓	1

There are several pre-defined roles in Prism, these cannot be edited.



**Tiger Administrator** – Full access to all aspects of the system, except Data Privacy actions. A Tiger Administrator can appoint a Data Protection Agent but cannot perform the forget process.

**System Administrator** - Full access to all aspects of the system, except Data Privacy actions.

**Data Protection Representatives** – This role cannot be assigned in the usual way but is added to accounts via the Data Privacy module. It allows the forget actions required under EU and UK law.

**View My Calls** – Usually assigned by directory integration. This is a role that gives access to the simple View My Activity module, allowing users to see their own calls and maintain a phone book to define personal and business numbers.

**View My Directories** – A special role allowing access to the user's organization in the directory tree and all descendant organizations. Ideal for manager roles. Access granted by this role will adjust depending on the directory position of the user at the time.

## Create

Additional roles can be created for more specific access requirements. It is worth taking time to consider how to structure the roles in your system, especially if there are a large number of users with different requirements. Making several simpler roles instead of one or two complex ones might lead to an easier time when configuring accounts in the future. Providing a detailed explanatory description for each role is strongly recommended.

New roles are created with a five step wizard.

## Details

Roles | Create

1 Details 2 Permissions 3 Enterprise Groups 4 Data Access Groups 5 Completed

Roles Details

Role Name\*

Example Role

Role Description\*

Defining a role with many permissions and groups for the manual.

Next

Step 1 requires a name and description for the role. Tiger strongly advises that the description be complete so that a role can be chosen from the list when creating or updating an account, instead of needing to be opened to see what it grants.

## Permissions

Step 2 selects the permissions for the role. Permissions provide functional access to aspects of Prism. For example, the ability to see the Enterprise Directory management screens is needed in addition to groups defining access to parts of the directory.

Roles | Create

Permissions

Filter (2)

Selected Permissions 8 (3)

(4)	Permission Name	Permission Description
▶	Administration	
▶	Alerts	
▼	Charging	
(1) ▶	Charges	
▼	Fixed Charges	
<input checked="" type="checkbox"/>	Fixed Charges Read	Grant VIEW access to the FIXED CHARGES management screens
<input type="checkbox"/>	FixedCharges Write	Grant WRITE access to the FIXEDCHARGES management screens
▶	Tariffs	
▶	Taxation	
▼	Enterprise	
▶	Contact Management	
▶	Directory Search	
▼	Employees	
<input checked="" type="checkbox"/>	Employees Read	Grant VIEW access to the EMPLOYEE management screens
<input type="checkbox"/>	Employees Write	Grant WRITE access to the EMPLOYEE management screens
▶	Locations	
▼	Tree Nodes	
<input checked="" type="checkbox"/>	Departments Read	Grant VIEW access to the DEPARTMENTS management screens
<input type="checkbox"/>	Departments Write	Grant WRITE access to the DEPARTMENTS management screens

The permissions tree is grouped by module and can be expanded or collapsed with the controls on the left (1). The items displayed can also be filtered to find types of or specific permissions (2). The number of selections is displayed at the top (3) and these selections are retained through different filtering, expansion or collapsing operations. There is a select/deselect all box at the top of the tree (4) to reset selections, or to start with everything and reduce permissions if that is easier for the role.

## Enterprise Groups

The enterprise groups step will list all defined groups dealing with the Enterprise module. That includes all three directory trees, Network groups and employee exclusions. Each set of groups is listed individually, and each set has a select all box available.

Roles | Create

1 2 3 4

Details Permissions Enterprise Groups Data Access Groups Completed

### Enterprise Groups

#### Department - Access

Group Name	Group Description	
Tree Administrator	Grants full access to the current tree.	<input type="checkbox"/>
View My Directories	Visible tree nodes and the call data access are dynamically established based upon a user's position within a particular tree. A user will be able to see all calls made to or from the user's organization or any of its descendants. When viewing a tree, only the user's organization its descendant organizations will be visible.	<input checked="" type="checkbox"/>
Energy	Energy and sub departments	<input type="checkbox"/>
Finance	Finance	<input type="checkbox"/>

#### Cost Centres - Access

Group Name	Group Description	
Tree Administrator	Grants full access to the current tree.	<input type="checkbox"/>
View My Directories	Visible tree nodes and the call data access are dynamically established based upon a user's position within a particular tree. A user will be able to see all calls made to or from the user's organization or any of its descendants. When viewing a tree, only the user's organization its descendant organizations will be visible.	<input checked="" type="checkbox"/>
121-25-4308	121-25-4308	<input type="checkbox"/>

#### Projects - Access

Group Name	Group Description	
Tree Administrator	Grants full access to the current tree.	<input type="checkbox"/>
View My Directories	Visible tree nodes and the call data access are dynamically established based upon a user's position within a particular tree. A user will be able to see all calls made to or from the user's organization or any of its descendants. When viewing a tree, only the user's organization its descendant organizations will be visible.	<input type="checkbox"/>

#### Employees Exclusion

Group Name	Group Description	
Human Resources Managers	To remove call access to all Human Resources Managers	<input type="checkbox"/>
Managers	Manager Groups	<input checked="" type="checkbox"/>

#### Network Access

Group Name	Group Description	
Network Administrator	Grants full access to all network nodes.	<input type="checkbox"/>
Access to Trunk Group 001	Access to Trunk Group 001	<input type="checkbox"/>
Southwest Campus	PABX and Channel groups located on the SE Campus	<input checked="" type="checkbox"/>

## Data Access Groups

The next step is to assign data access to the role. The remaining types of group are listed in this stage. As with Enterprise groups the types are grouped together.

Roles | Create

1 2 3 4

Details Permissions Enterprise Groups Data Access Groups Completed

### Data Access Groups

#### Report Access

Group Name	Group Description	
Reports Administrator	Grants full access to all reports.	<input type="checkbox"/>
Basic Reports	Basic Reports	<input type="checkbox"/>
Outbound Reports	Outbound Reports	<input type="checkbox"/>
Department Management Reports	Department Management report set for managers	<input checked="" type="checkbox"/>
Incoming Reports	All reports from the incoming category	<input type="checkbox"/>

#### Exports Access

Group Name	Group Description	
Exports Administrator	Grants full access to all exports.	<input type="checkbox"/>
Simple Exports	Simple Exports	<input checked="" type="checkbox"/>

#### Dashboards Access

Group Name	Group Description	
Dashboards Administrator	Grants full access to all dashboards.	<input type="checkbox"/>
Basic Dashboards	Basic Dashboards	<input checked="" type="checkbox"/>

#### Widgets

Group Name	Group Description	
------------	-------------------	--

## Completed

Shows a summary of the information entered before creation.

Roles | Create

1

2

3

4

✓

Details Permissions Enterprise Groups Data Access Groups Completed

Summary Expand All

1. Roles Details

Role Name  
Example Role

Role Description  
Defining a role with many permissions and groups for the manual.

2. Permissions

Permission Name	Permission Description
Machines Road	Grant VIEW access to the MACHINE management screens
Fixed Charges Road	Grant VIEW access to the FIXED CHARGES management screens
Tariffs Road	Grant VIEW access to the TARIFFS management screens
Taxes Road	Grant VIEW access to the TAXES management screens
Contacts Road	Grant VIEW access to the CONTACT management screens
Employees Road	Grant VIEW access to the EMPLOYEE management screens
Locations Road	Grant VIEW access to the LOCATION management screens
Departments Road	Grant VIEW access to the DEPARTMENTS management screens
Cost Centres Road	Grant VIEW access to the COST CENTRES management screens

3. Enterprise Groups

Department Groups

Group Name	Group Description
View My Directories	Visible tree nodes and the call data access are dynamically established based upon a user's position within a particular tree. A user will be able to see all calls made to or from the user's organization or any of its descendants. When viewing a tree, only the user's organization its descendant organizations will be visible.

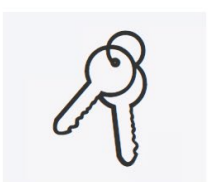
Cost Centre Groups

Group Name	Group Description
------------	-------------------

## Detail Page and Editing Roles

The details page for a role has two main sections. The top of the page shows three tabs. The first shows the name and description of the role.

Roles | Department Manager



Department Manager

Details Accounts Audit

Roles Details

Role Name  
Department Manager

Role Description  
Has access to limited management reporting, dashboards and all call traffic in the Department itself and below. No Analytics.

The second tab lists the accounts which are using the role.

Roles Accounts

Filter

	Username	Display Name	User Type	Last Sign In	Is Disabled
JH	james.halley@madoup...	James Halley	Employee		x

The audit tab shows the details for role creation and last modification.

The bottom part of the page shows the results of the various groups and permissions applied to the role. Tabs will only show on the display if an appropriate group is applied. In the example below there is no Projects access granted to the role, so there is no 'Project – Access' tab.

Roles Authorization | (+)

Permissions | Department - Access | Cost Centres - Access | Network Access | Report Access | Dashboards Access

Permissions

☒ Show granted only

Area Name	Permission Name	Permission Description	Is Granted
Area Name: Dashboards	Dashboards View	Grant VIEW access to the DASHBOARDS management screens	✓
Area Name: Employees	Employees Read	Grant VIEW access to the EMPLOYEE management screens	✓
Area Name: Reports	Reports View	Grant VIEW access to the REPORTS management screens	✓
Area Name: Tree Nodes	Departments Read	Grant VIEW access to the DEPARTMENTS management screens	✓
	Cost Centres Read	Grant VIEW access to the COST CENTRES management screens	✓

Otherwise each tab shows the sum of the groups applied. If two permissions groups are applied the permissions tab will list all granted permissions from both. The directory tree for Department/Cost Centre/Projects Access shows the resulting access form all groups applied. The role below has two department access groups applied, so shows access (of different types) applied to organizations in the view.

Roles Authorization | (+)

Permissions | Department - Access | Cost Centres - Access | Network Access | Report Access | Dashboards Access

Department

Group Name	Group Description	Is User Defined
Energy	Energy and sub departments	✓
Finance	Finance	✓

Company Test

- Basic Industries
- Capital Goods
- Consumer Durables
- Consumer Non-Durables
- Consumer Services
- Duplicated
- Energy
  - Accounting
  - Legal
  - Marketing
- Finance
  - Business Development
  - Human Resources
  - Music
  - Sales
  - Services
- Health Care

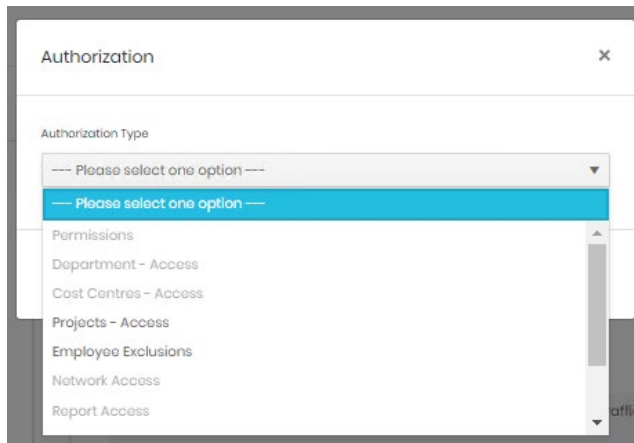
The method to add additional groups to a role depends on what group types are applied already. In the above examples there are permission groups, department and cost centres, and network enterprise groups, and report and dashboard Data Access groups. To add further groups of any of these types, navigate to the appropriate tab and edit the tab. This will show the group list for the type and allow selection or deselection of individual groups.

Roles Authorization | (+)

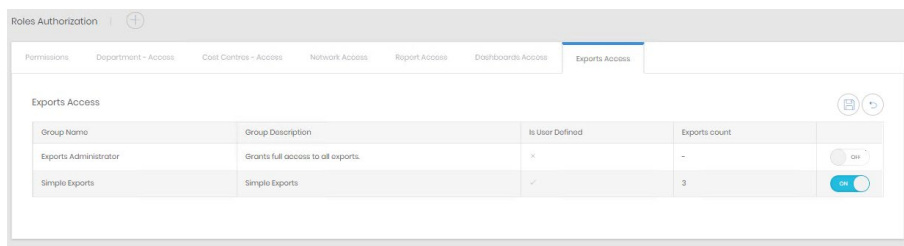
Permissions | Department - Access | Cost Centres - Access | Network Access | Report Access | Dashboards Access

Group Name	Group Description	Is User Defined	
Tree Administrator	Grants full access to the current tree.	×	OFF
View My Directories	Visible tree nodes and the call data access are dynamically established based upon a user's position within a particular tree. A user will be able to see all calls made to or from the user's organization or any of its descendants. When viewing a tree, only the user's organization its descendant organizations will be visible.	×	OFF
Energy	Energy and sub departments	✓	ON
Finance	Finance	✓	ON

If there is not a group of that type already then click the + next to Roles Authorization to add a new type of authorization. A list will display, with existing types greyed out.



Select the new group type and confirm. The tab will be added, and a list of available groups shows for selection. Remember that additional permissions may be required if new Enterprise or Data Access tabs are added.

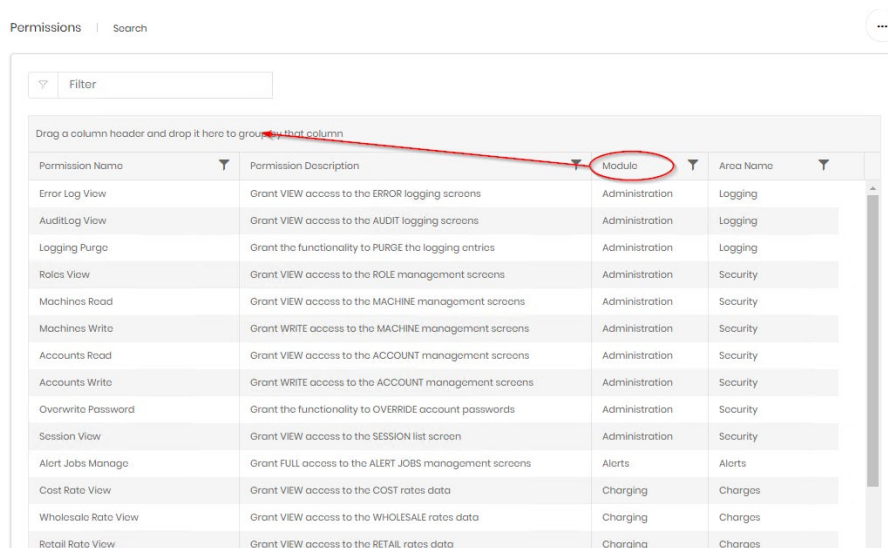


Once saved the role is updated. The effect is immediate and all accounts with that role will have the revised access levels.

## Permissions

The permissions section has a full list of available permissions for reference. The permissions are presented in a grid and there is a general filter as well as the normal column filters. However, the permissions grid has one additional feature. Each of the column headings can be dragged above the header bar to form a group.

For example, here is the default display,



By dragging the module header up, all permissions are grouped by their module

Permissions | Search

Filter

↑ Module X

Permission Name	Permission Description	Module	Area Name
▼ Module: Administration			
Error Log View	Grant VIEW access to the ERROR logging screens	Administration	Logging
AuditLog View	Grant VIEW access to the AUDIT logging screens	Administration	Logging
Logging Purge	Grant the functionality to PURGE the logging entries	Administration	Logging
Roles View	Grant VIEW access to the ROLE management screens	Administration	Security
Machines Read	Grant VIEW access to the MACHINE management screens	Administration	Security
Machines Write	Grant WRITE access to the MACHINE management screens	Administration	Security
Accounts Read	Grant VIEW access to the ACCOUNT management screens	Administration	Security
Accounts Write	Grant WRITE access to the ACCOUNT management screens	Administration	Security
Overwrite Password	Grant the functionality to OVERRIDE account passwords	Administration	Security
Session View	Grant VIEW access to the SESSION list screen	Administration	Security
▼ Module: Alerts			
Alert Jobs Manage	Grant FULL access to the ALERT JOBS management screens	Alerts	Alerts
▼ Module: Charging			
Cost Rate View	Grant VIEW access to the COST rates data	Charging	Charges

Additional fields can be used to group further, a grouping level can be removed by clicking the 'X' in the grouping bar.

The same functionality is available when viewing and editing permissions on a role's [detail page](#).

Roles Authorization | +

Permissions | Department - Access | Cost Centres - Access | Network Access | Report Access | Dashboards Access

Permissions

ON Show granted only

↑ Module X

Permission Name	Permission Description	Module	Is Granted
▼ Module: Enterprise			
Employees Read	Grant VIEW access to the EMPLOYEE management screens	Enterprise	✓
Departments Read	Grant VIEW access to the DEPARTMENTS management screens	Enterprise	✓
Cost Centres Read	Grant VIEW access to the COST CENTRES management screens	Enterprise	✓
▼ Module: Telephony			
Dashboards View	Grant VIEW access to the DASHBOARDS management screens	Telephony	✓
Reports View	Grant VIEW access to the REPORTS management screens	Telephony	✓

## Administration

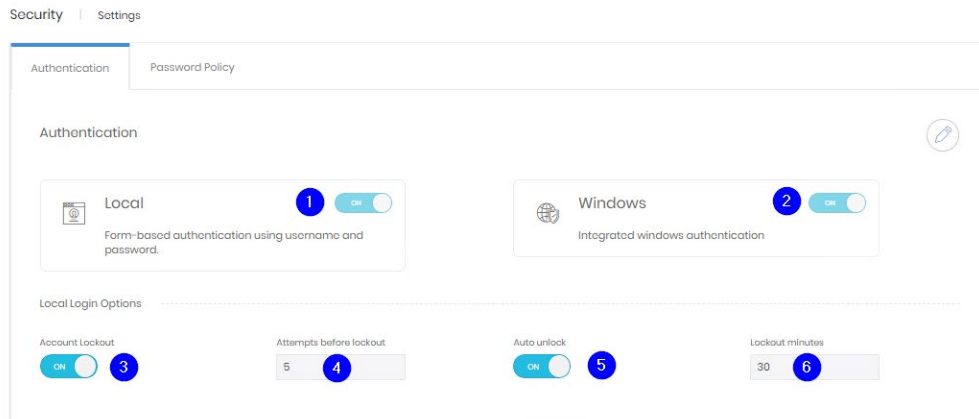
### Settings

#### General

General security settings are broken into two sections.

#### Authentication

The authentication tab covers settings relating to local and windows authentication.



The controls govern whether local or windows authentication is allowed for Prism (1 & 2). If accounts are locked after incorrect attempts (3), how many attempts cause a lockout (4), whether account unlock with or without intervention (5), and after how long if automatic unlocking is permitted.

#### Password Policy

Prism's password policy governs the passwords for local accounts. There are three basic areas within the policy section.

The top part covers expiration. Controls are given to enable expiration and to set the expiration period



The second section relates to passwords' required complexity.



The last section has some more specific requirements. Passwords can be forced to not include the company or user's names. Reuse of previous passwords can be prevented, either just the last one, or several.



Finally, there is a space to input blocked passwords. These may be blocked by the organization or may simply be a list of common passwords sourced from elsewhere. Passwords to be blocked should be entered, comma-separated into the box. The drop-down menu above the box contains some template lists to start with.

Other Requirements

Do not include personal data  
☐ OFF

Do not include organisation name  
☐ OFF

Prevent reuse  
☒ ON

Reuse previous count  
1

Passwords to Block --- Please select or ▼

123456, password, 12345678, qwerty, 12345, 123456789, letmein, 1234567, football, iloveyou, admin, welcome, monkey, login, abc123, starwars, 123123, dragon, password, master, hello, freedom, whatever, qazwsx, trustno1

Define here all the passwords to be blocked by the system (pre-defined templates are provided using the select box above)

## Email Templates


Prism uses templates to send out messages for new account activation, and for when users request a password reset.

These templates can be viewed here.

Email Templates | Manage

Template: Account Activation ▼

Subject: Account Activation

**TIGER** 

**Account Activation**

Hi, {{DisplayName}}!

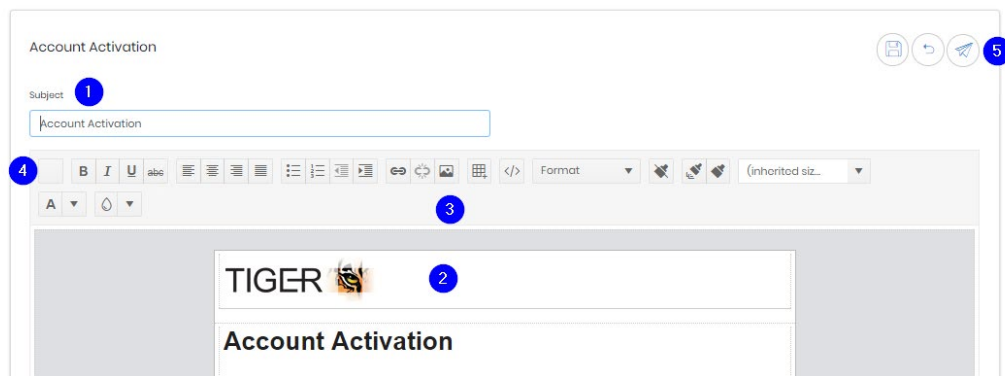
A new Prism account has been created and associated to this email address.  
{{Email}}

Please click the button below to activate your account and start using the application.

[Activate](#)

© {{Year}} Tiger Communications plc. All Rights Reserved.

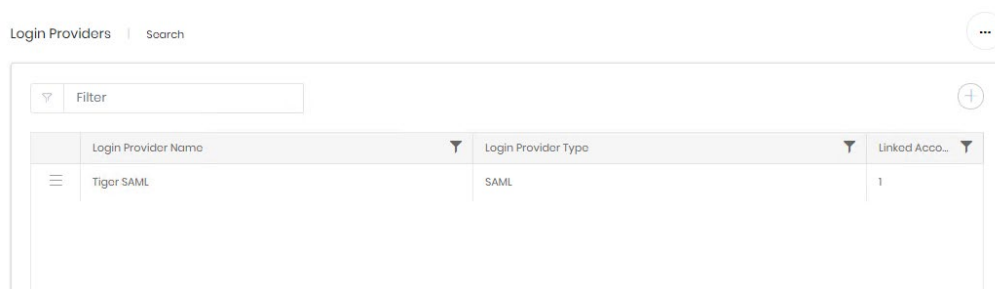
The templates can also be edited



The subject can be altered (1) and the body (2) edited with some formatting options (3). The top left button (4) allows selection and insertion of available merge fields. A test email can be sent during the editing stage (5).

## Login Providers

Prism can be configured to allow authorisation via additional SAML providers. Initially displayed is a grid containing currently configured providers

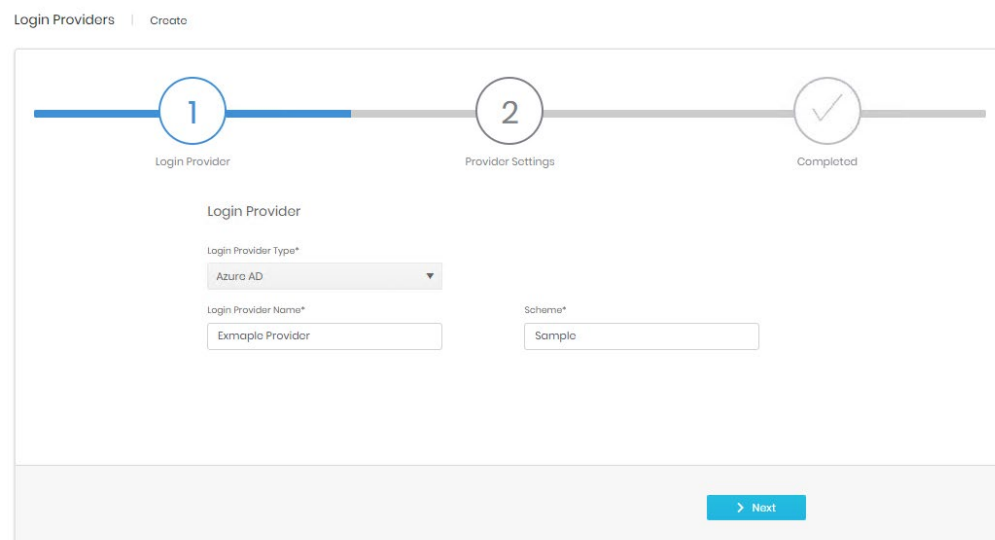


## Create

Adding a new provider starts a three step wizard.

## Login Provider

Select the provider type and enter a name and scheme for the entry.



Step 2 will vary depending on the provider type selected.

For Azure AD type the Tenant id and Client id are required

Login Providers | Create

1 Login Provider

2 Provider Settings

Completed

Provider Settings

Tenant id\*

Client id\*

< Previous

Next >

For OpenIdConnect type Authority, Response Type, and Client id are needed.

Login Providers | Create

1 Login Provider

2 Provider Settings

Completed

Provider Settings

Authority\*

Response type\*

Client id\*

< Previous

Next >

### Completed

Shows a summary of the information entered before creation.

### Detail Page

The detail for a provider has three tabs. The first two reflect the details entered at creation and can be edited if necessary.

Login Providers | Tiger SAML

Tiger SAML

Login Provider

Provider Settings

Audit

Login Provider Type

SAML

Scheme

Saml2

Login Provider Name

Tiger SAML

The audit tab shows the details for account creation and last modification.