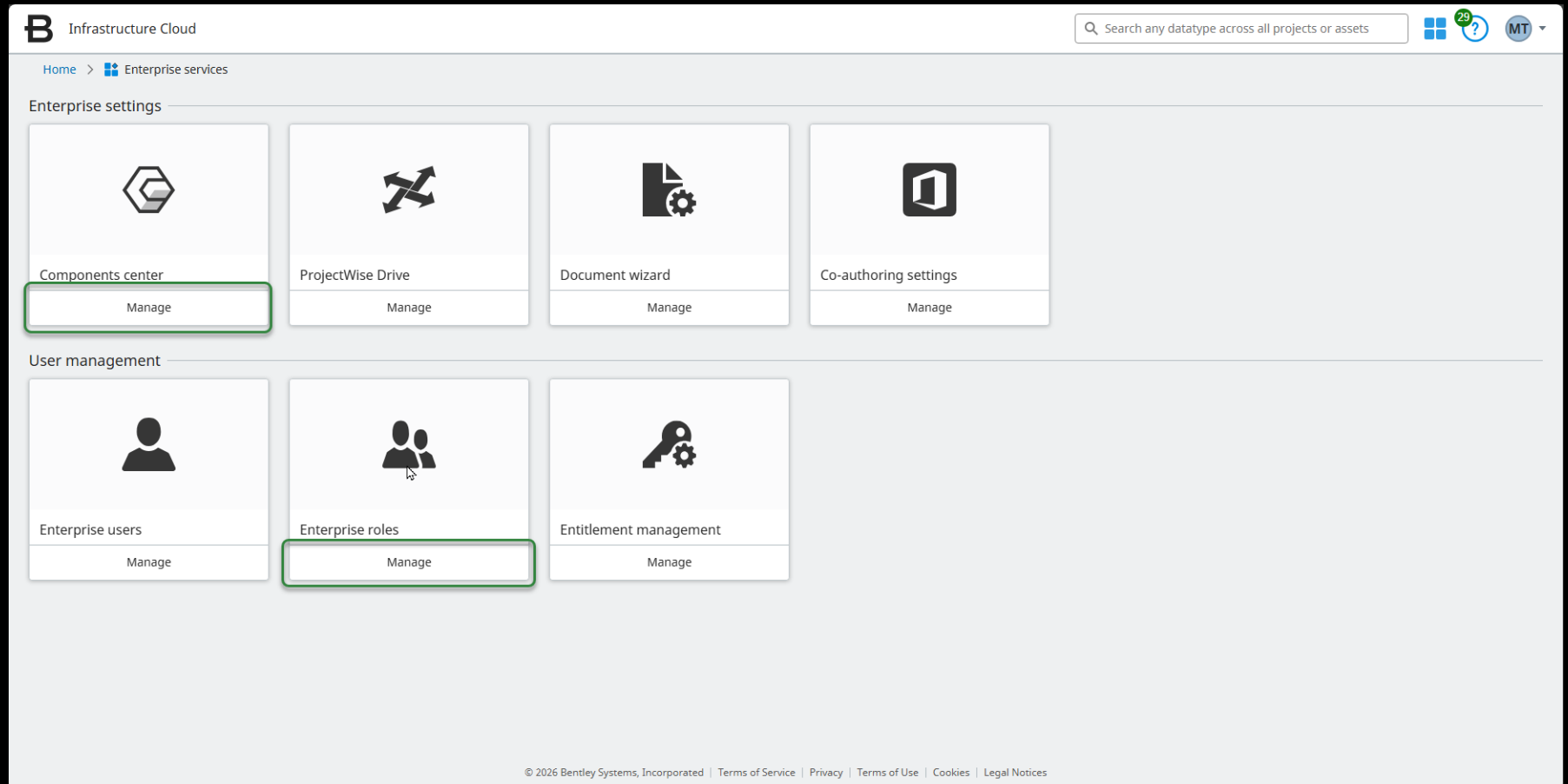


Getting Started - Online

The Bentley Infrastructure Cloud (BIC) start screen features two key links.

These apply to the entire enterprise.

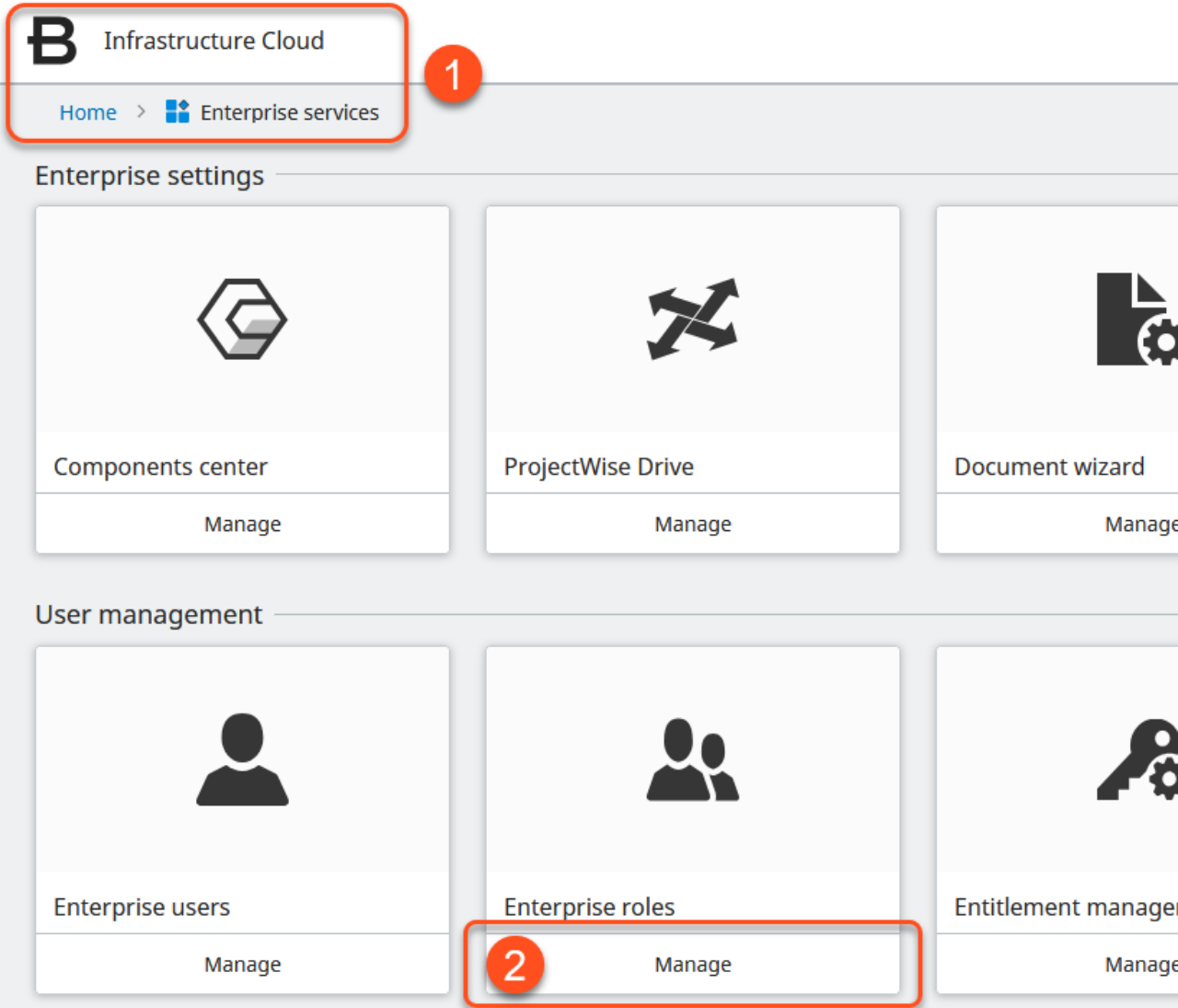
- **Components Center**
This launches the Components Center online portal where content can be created and managed.
- **Enterprise Roles**
This accesses user management for all Bentley online features.
The default Project Administrator Role includes access to all Components Center functions.
Other Enterprise Roles will need to be added or edited to deliver appropriate access for production use.



Access Control

The first point where access to Components Center is controlled is at the Enterprise level.

From the Infrastructure Cloud Enterprise Services page (1) go to Enterprise Roles and click Manage (2).



Access Control

The Account management page will open in either Users or Roles view.

In User view clicking + Add (1) allows individual users to be added, they can also be bulk uploaded (2).

If the account is federated with Bentley any registered user with the specified domain name will be added here automatically. Once federated, it should not be necessary to manually add new users.

Permission to access Components Center and other functions is most effectively managed by creating Enterprise Roles, then assigning those Roles to selected users.

The screenshot displays the 'Account management' interface. At the top, there are navigation tabs: 'Home', 'BAS Engineering' (selected), 'Assets', and 'Projects'. Below these, the 'Account management' section is visible. It has two sub-tabs: 'Users' (selected) and 'Roles'. In the 'Users' view, there is a '+ Add' button (labeled with a red circle '1') and a 'Bulk actions' dropdown menu (labeled with a red circle '2'). Below the buttons, there is a table with a header 'Name' and a list of users. The table has a checkbox column on the left and a 'Name' column. The users listed are: 'BAS Engineering', 'BAS Engineering', 'BAS Engineering', 'BAS Engineering', '(Unaffiliated)', 'BAS Engineering', 'BAS Engineering', 'BAS Engineering', and 'BAS Engineering'.

	Name
☐	BAS Engineering
☐	BAS Engineering
☐	BAS Engineering
☐	BAS Engineering
☐	(Unaffiliated)
☐	BAS Engineering
☐	BAS Engineering
☐	BAS Engineering
☐	BAS Engineering

Access Control

In Roles view clicking + Create allows new Enterprise Roles to be added at the Enterprise level.

These can include appropriate Components Center permissions.

Once Roles containing the appropriate Components Center permissions have been created or modified at the Enterprise level, end users who are members of these groups will be able to access the assigned Components Center functions.

Home

BAS Engineering

Assets

Account management

Users

Roles

+ Create

Edit

Delete

Name

☐

Project Administrator

☒

Team Member

☐

BIC0001 BIM Coordinator

☐

Component Center Approver

☐

Component Center Creator

☐

Components Center Administrator

☐

Components Center General

☐

iTwin Creator

☐

iTwinX

1 row selected

Description

Project Administrator

Team Member

BIC0001 BIM Coordinator

Read. Upload, Write, Approve

Can Read, Write, Upload

Admin

Read

Role to manage who can create new iTwins

This role equals ProjectWise Manage permissions.

Access Control

A new Enterprise will contain two default Roles:

1. Project Administrator
2. Team Member

These are good examples of how Enterprise Roles can be set up.

The Project Administrator includes the Components Center permissions shown on the right.

Two other available permissions are omitted; No Access obviously, and Access Control as that would limit the controls that can be applied within Components Center.

☒	Share Catalogs	i
☐	No Access	i
☐	Access Control	i
☐		i

The screenshot displays the 'BAS Engineering' interface. On the left, the 'Account management' panel shows a list of roles under the 'Roles' tab. The 'Project Administrator' role is selected and highlighted with a red box and a red circle with the number '1'. The 'Team Member' role is also visible, highlighted with a red box and a red circle with the number '2'. On the right, the 'Role details' panel for the 'Project Administrator' role is shown. It lists the role name, description, and selected permissions. The 'Components Center' permission group is expanded and highlighted with a red box, showing a list of permissions: Read, Upload, Write, Approve, View Analytics, Share Catalogs, Delete, and Edit. Each permission has an information icon. The 'Components Center' group shows 8/10 permissions are selected. Other permission groups like Administration (9/10), Project Activities (1/11), Construction Services (1/2), iModelHub (5/5), Project Insights Service (2/2), ProjectWise Deliverables Management (5/5), ProjectWise Forms (10/10), and Reality data and geospatial features (4/4) are also listed.

Home BAS Engineering User One UO

Account management

Users Roles

+ Create Edit Delete

Name

☒	Project Administrator	1
☐	Team Member	2
☐		
☐		
☐		
☐		
☐		
☐		
☐		
☐		

1 row selected

Role details

Role name
Project Administrator

Role description
Project Administrator

Selected permissions [Expand all](#)

Permission groups

> Administration	9/10	i
> Project Activities	1/11	i
☒ Components Center	8/10	i
Read		i
Upload		i
Write		i
Approve		i
View Analytics		i
Share Catalogs		i
Delete		i
Edit		i
> Construction Services	1/2	i
> iModelHub	5/5	i
> Project Insights Service	2/2	i
> ProjectWise Deliverables Management	5/5	i
> ProjectWise Forms	10/10	i
> Reality data and geospatial features	4/4	i

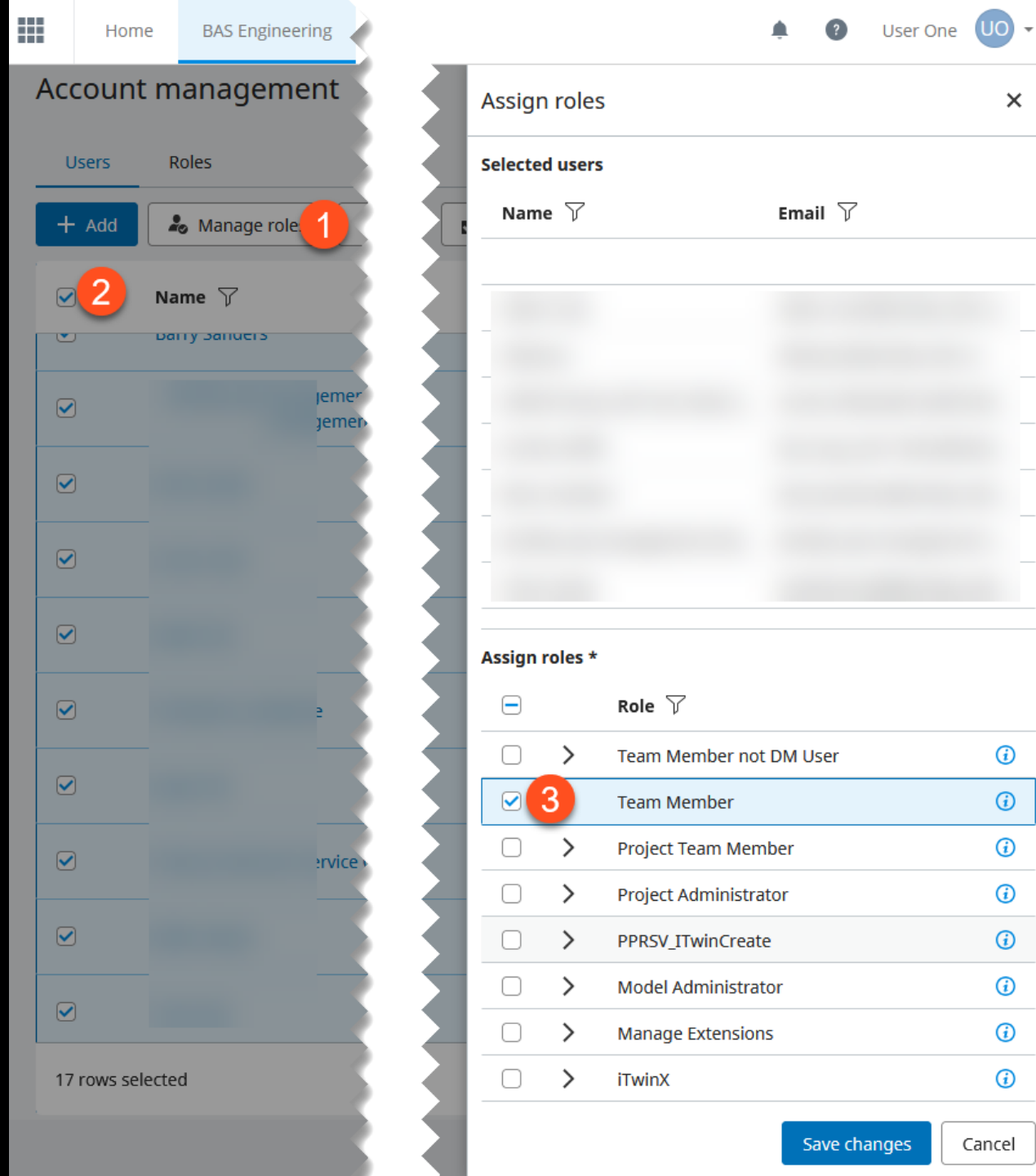
The default Team Member has far more limited permissions.

The Team Member is an example of a clear and useful multi-purpose Role to work with.

Adding Components Center > Read permission would enable all users assigned the Team Member Role to see and place content from Components Center.

Click Manage Role (1), select one or more Users (2) and assign Roles from those available (3).

Role name	Team Member
Role description	Team Member
Selected permissions	Expand all
Permission groups 	
> iModelHub	2/5 
> Reality data and geospatial features	1/4 
> Share	2/4 



Access Control

One approach to Components Center permissions would be to have explicit Roles for the various levels of access required as shown alongside.

The downside of this is that if specific Roles are created for the many services available in BIC the list of available Roles and their management could become cumbersome. Applying permissions to Roles that have wider application may be more manageable.

For example, Components Center General only contains the Components Center > Read permission. This could simply be added to Team member.

Role name	
Components Center General	
Role description	
Read	
Permission groups	
▼ Components Center	1/10 ⓘ
Read	ⓘ



Account management

[Users](#)[Roles](#)[+ Create](#)[Edit](#)[Delete](#)**Name** [Project Administrator](#)[Team Member](#)[BIC0001 BIM Coordinator](#)[Component Center Approver](#)[Component Center Creator](#)[Components Center Administrator](#)[Components Center General](#)[iTwin Creator](#)[iTwinX](#)

Access Control

Components Center access can also be managed on a per Catalog basis, covered later.

These Catalog specific Roles are hardcoded in Components Center. Enterprise level Roles should therefore reflect the behaviours of these internal Components Center Roles.

There may be wider Enterprise Roles that are a good match for Designer, Creator and Approver. If not, then there is reason to include Components Center specific Enterprise Roles.

Once all five of the Components Center Role equivalent permissions have been applied to Enterprise Roles and end users have been added to those roles, Components Center will be fully available for production use.

Catalog level security is largely optional. It is only required when it is necessary to apply further granularity for particular projects or other functional grouping within the Components Center.

Role						
Role	Read	Upload	Write	Approve	Share Catalog	Access Control
General	☒					
Designer	☒	☒				
Creator	☒	☒	☒			
Approver	☒	☒	☒	☒	☒	
Admin	☒	☒	☒	☒	☒	☒
No access						
Cancel						