

Access Policies

Contents

- Access Policies..... 3**
 - Access Rules..... 3
 - View Access Policies..... 3
 - Create a New Access Policy..... 4
 - View Access Policy Information..... 6
 - Modify an Access Policy..... 7
 - Delete an Access Policy..... 9

Access Policies

An access policy is a set of logical rules that determines how users can consume data stored in the PHEMI system. Access policies can be optionally applied to data sources and datasets.

To create an access policy, you define one or more access rules. In each rule:

- The Subject specifies a set of the user authorizations.
- The Object specifies a set of data visibilities.
- The Action specifies the action to be taken if the rule is matched.

A rule is matched when the user making the request has an authorization matching at least one of those listed for Subject, and the data being requested has a visibility matching at least one of those listed for Object. When there is a match, the user may take the specified action(s) on the data.

If there is more than one access rule within a policy, the rules are related by OR logic.

The rules in a given access policy are intended to implement specific controls over a dataset. Depending on the number and kinds of datasets your organization works with, you may need just one access policy or multiple access policies.

If you have multiple access policies, it is possible for policies to conflict with one another and still represent a consistent governance policy, provided that each access policy is used to control different data sources or datasets. For example, one access policy may allow users with Researcher authority to read CONFIDENTIAL data while another access policy does not. This can be perfectly consistent, given the policies control different data.

Access Rules

Each access policy consists of one or more access rules.

Each rule has three parts. Together, the parts of the rule specify who (*subject*) can consume what data (*object*) and how (*action*).

- Subject. The subject specifies who may access the data, by listing the permitted user authorizations.
- Action. The action specifies how authorized users may consume the data.
- Object. The object specifies what data the permitted users are allowed to interact with, by listing the data visibilities.

View Access Policies

See what access policies have been configured on the **Access Policy Builder** page.

To view defined access policies:

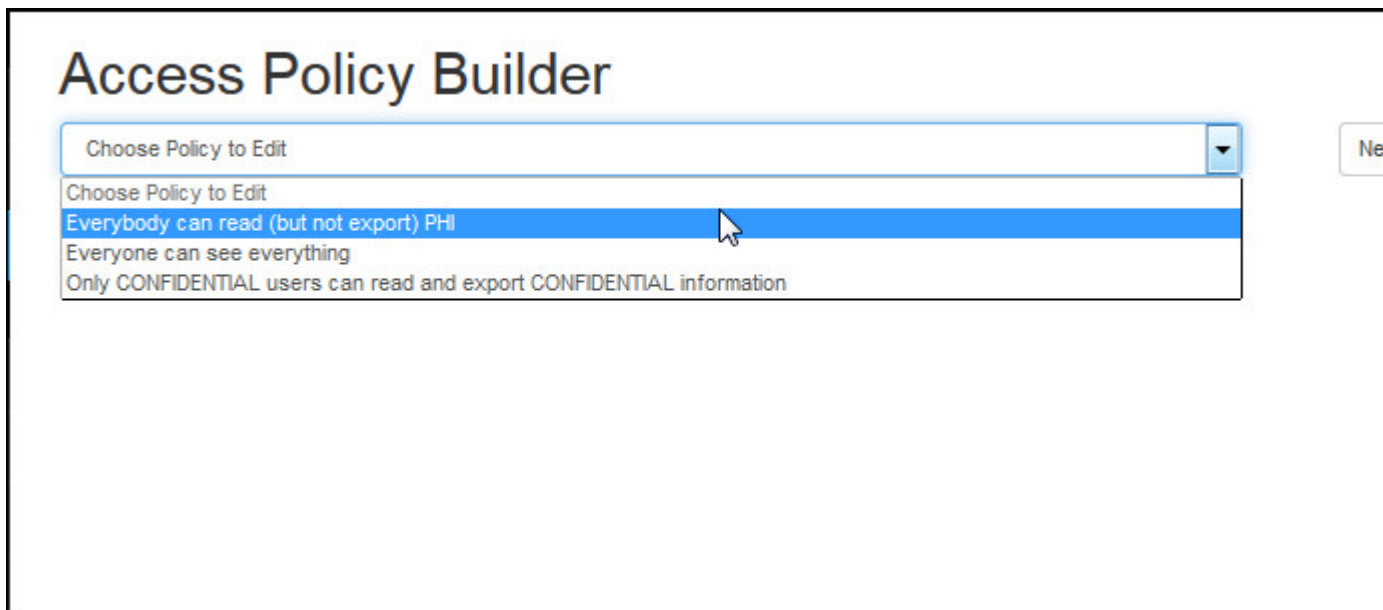
1.

Open the **Access Policy Builder** page, by clicking the **Access Policy Builder** icon.  in the left navigation bar.

The **Access Policy Builder** page opens.



2. At the right of the **Choose Policy to Edit** field, click the drop-down arrow to see the list of configured access policies.



Create a New Access Policy


Create a new access policy on the **Access Policy Builder** page.

Before you can define an access policy you must configure the following:

- User authorities
- Data visibilities
- Environments (access networks)

To create a new access policy, define one or more access rules:

- 1.

Open the **Access Policy Builder** page, by clicking the **Access Policy Builder** icon  in the left navigation bar.

The **Access Policy Builder** page opens.

Access Policy Builder

Choose Policy to Edit

New Policy

- Click the **New Policy** button.

The form for the new access policy opens, with Rule 1 ready for you to edit.

Access Policy Builder

Choose Policy to Edit

New Policy

Name (New policy)

Rule 1

Subject

None

Action

CAN

None

Object

None

Environmental

WHEN

None

Add Rule

Save Access Policy

- Enter the access rule information.

Option

Subject

Action

Description

Mandatory. The user authorizations allowed to perform the action on the data. User authorizations are configured for the system by the administrator.

Mandatory. The action(s) an authorized user may take on the data. Supported actions are as follows:

- Read. The user may view the data.
- Export. The user may export the data to a destination, such as a SAP system.

Option
Object

Description

Mandatory. The data visibilities authorized users are allowed to access. Data visibilities are configured by the administrator.


4. Add another rule by clicking the **Add Rule** button. Or, save the access policy by clicking the **Save Access Policy** button. The system confirms when the access policy has been successfully saved.

View Access Policy Information

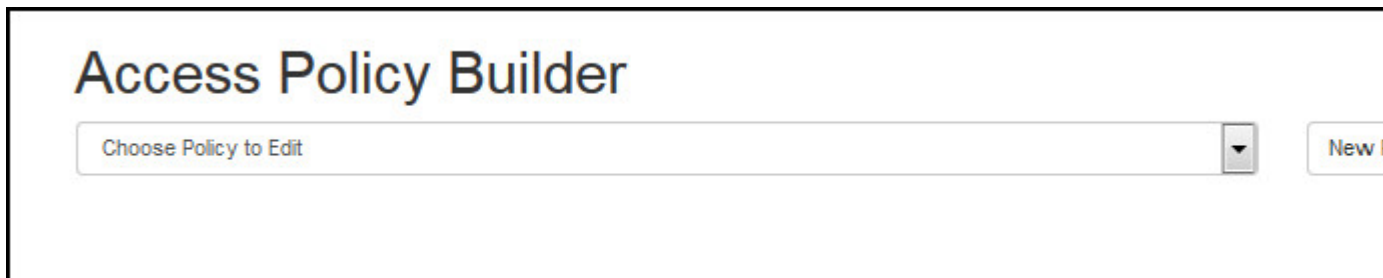
View the information configured for a given access policy on the **Access Policy Builder** page.

To view information for an access policy:

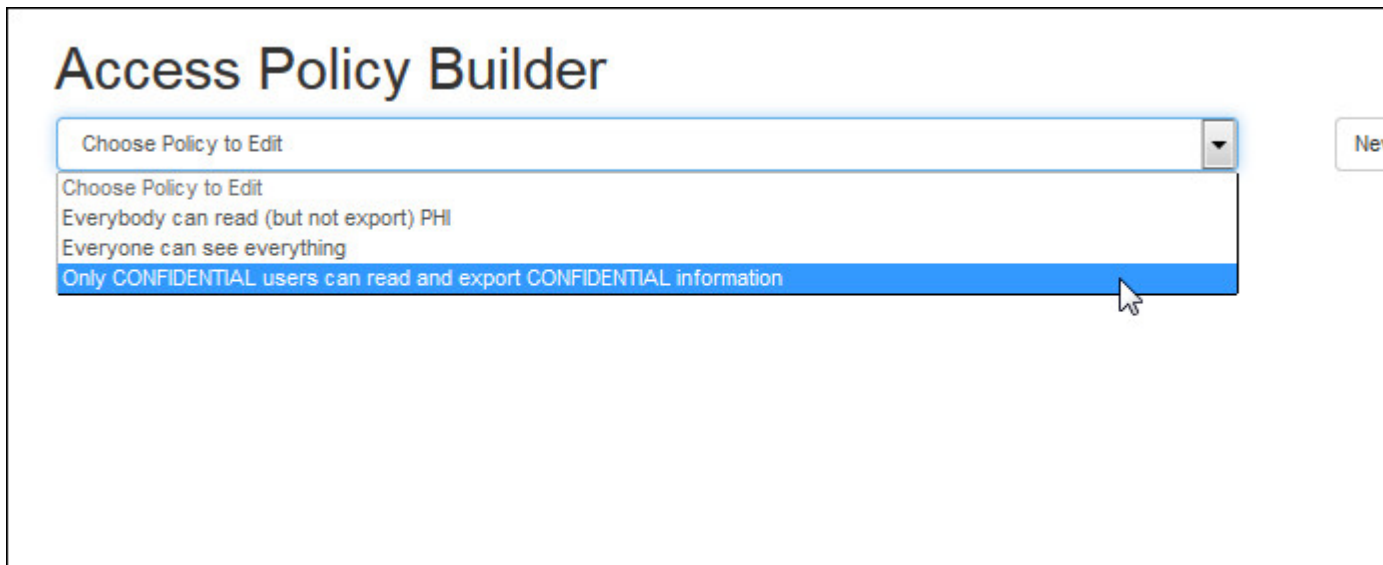
1.

Open the **Access Policy Builder** page, by clicking the **Access Policy Builder** icon.  in the left navigation bar.

The **Access Policy Builder** page opens.



2. At the right of the **Choose Policy to Edit** field, click the drop-down arrow to see configured access policies. Select the policy you want to view.



The screen for the selected access policy opens, showing the information configured for it.

Access Policy Builder

Only CONFIDENTIAL users can read and export CONFIDENTIAL information

Name

Only CONFIDENTIAL users can read and export CONFIDENTIAL information

Rule 1

Subject

CONFIDENTIAL

Object

CONFIDENTIAL

CAN

Action

Read, Export

Delete Access Policy


Save Access Policy

Modify an Access Policy

Modify an access policy on the **Access Policy Builder** page.

To modify an access policy:

1.

Open the **Access Policy Builder** page, by clicking the **Access Policy Builder** icon.  in the left navigation bar.

The **Access Policy Builder** page opens.

Access Policy Builder

Choose Policy to Edit

New

2. At the right of the **Choose Policy to Edit** field, click the drop-down arrow to see configured access policies. Select the policy you want to modify.

Access Policy Builder

Choose Policy to Edit
Everybody can read (but not export) PHI
Everyone can see everything
Only CONFIDENTIAL users can read and export CONFIDENTIAL information

The screen for the selected access policy opens, showing the information configured for it.

Access Policy Builder

Name

Rule 1


Subject		Action
<input type="text" value="CONFIDENTIAL"/>	CAN	<input type="text" value="Read, Export"/>

Object

3. Do any of the following.

- Modify an existing rule by editing values for Subject, Action, or Object.
- Add a new rule by clicking the **Add Rule** button and populating the fields. *What do the fields mean?*

•

Delete a rule by clicking the trash can icon.  to the right of the rule.

4. Click the **Save Access Policy** button to save the changes.

Delete an Access Policy

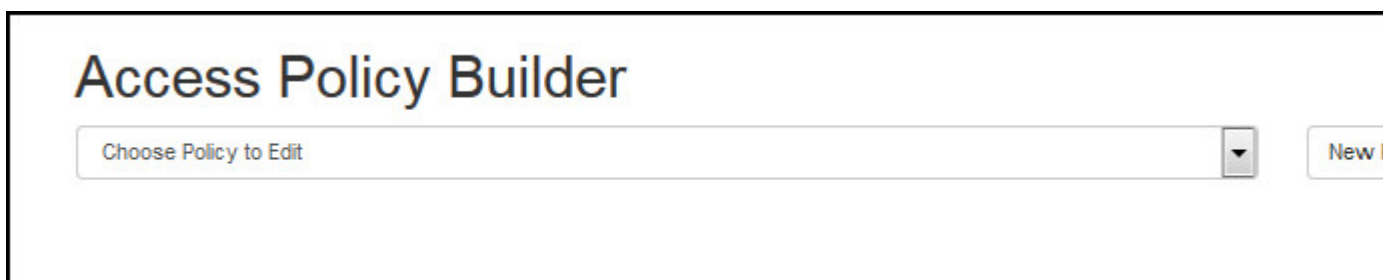
Delete an access policy on the **Access Policy Builder** page.

To delete an access policy:

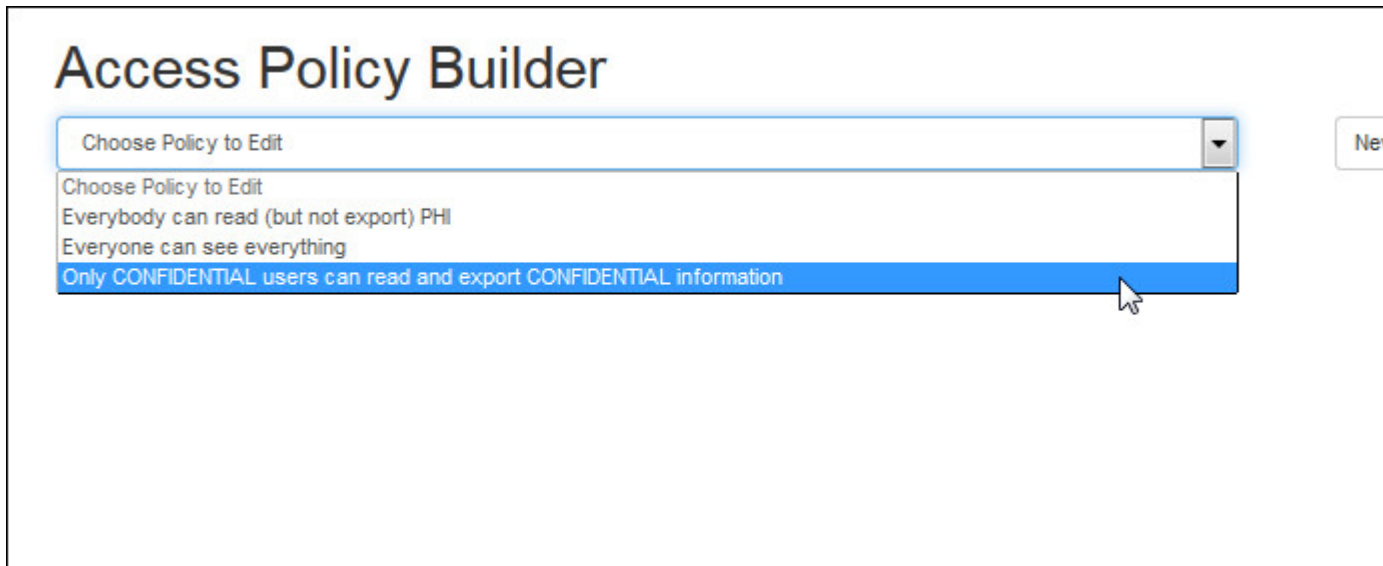
- 1.

Open the **Access Policy Builder** page, by clicking the **Access Policy Builder** icon.  in the left navigation bar.

The **Access Policy Builder** page opens.



2. At the right of the **Choose Policy to Edit** field, click the drop-down arrow to see configured access policies. Select the policy you want to modify.



The screen for the selected access policy opens, showing the information configured for it.

Access Policy Builder

Only CONFIDENTIAL users can read and export CONFIDENTIAL information ▼

Name Only CONFIDENTIAL users can read and export CONFIDENTIAL information

Rule 1

Subject		Action
CONFIDENTIAL ▼	CAN	Read, Export ▼

Object

CONFIDENTIAL ▼

Delete Access Policy Save Access Policy

3. Click the **Delete Access Policy** button. The system asks you to confirm deletion; click **Delete**.