Group Roles

E2E Bridge user access for groups is based on roles **ADMIN**, **MODELER**, and **USER**.
The user access rights are based on the group the user is assigned to. Depending on the group's role, the user has full or restricted access to the functions of the E2E Bridge.

All user access rights are summarized on page Summary of Default User Access Rights.

On this Page:

Related Pages:

- Summary of Default User Access Rights

Role ADMIN

Users belonging to a group with role **ADMIN** may invoke any function of the Bridge.
The Bridge has one pre-defined user **Administrator** (user id **admin**) that is member of the pre-defined group **Administrators** (group id **admin**). The role **ADMIN** has been assigned to this group.

Role MODELER

The role **MODELER** enables a user to perform the most important actions, but limits access to certain features:

Feature	Rights / Restrictions
Navigation	• In the **Domain** section of the navigation, the user only sees the navigation items **Users** and **Deployment**. • The user has no access to the management functions of a domain (import and removal of node instances). • He is not allowed to manage groups.
User management	• The user is not allowed to view or manage groups. • He may only change his own password. • He may not create and delete users. • He is not allowed to change his group assignment.
Management of a Bridge node instance	• Selecting a node instance in the navigation, the user may see the node instance preferences, logging data, and firmware information. • He is not allowed to update the preferences or upload firmware packages.
Management of the Bridge	Selecting **Bridge Server** in the sub-navigation of a node instance, the user may only see the deployed services, ports, Bridge preferences, licensing information, resources, and the add-on tabs java and XSLT. He is not allowed to take any action.
Management of services	• The user may deploy services, but may only delete, replace, start, and stop one, if he himself or a member of the same group deployed it. • He may modify all preferences of a service but the owner and the automatic startup, if he himself or a member of the same group deployed the service. • Access is granted to the history, logging and version information of a service. • He may only view the error dumps, if he himself or a member of the same group deployed the service. • He may only modify the configuration settings (key-value pairs), if he himself or a member of the same group deployed the service. • He may view the persistent state information and change it, if he himself or a member of the same group deployed the service.
Management of proxies	• The user may see all proxy related information. • He is not allowed to create or delete proxy nodes. • He is not allowed to start and stop proxy services. • He is not allowed to edit proxy configuration files and templates • He cannot manage E2E Proxy Server certificates.

Role USER

Users belonging to the role **USER** may invoke only read-only actions, with the exception of changing his user name and password.

Feature	Rights / Restrictions
Navigation	• In the **Domain** section of the navigation on the left, the user only sees the entry **Users**. • No access is granted to the management functions of a domain (import and removal of node instances). • He may not deploy, delete, replace, start, and stop services. • Furthermore, he is not allowed to manage groups.
User management	• The user is not allowed to view or manage groups. • He may only change his own password. • He may not create and delete users. • He is not allowed to change his group assignment.
Management of a Bridge node instance	• Selecting a node instance in the navigation, the user may see the node instance preferences, logging data, and firmware information. • He is not allowed to update the preferences or upload firmware packages.
Management of the Bridge	Selecting **Bridge Server** in the sub-navigation of a node instance, the user may only see the deployed services, ports, Bridge preferences, licensing information, resources, and the add-on tabs java and XSLT. He is not allowed to take any action.
Management of services	The user may see all service related information, but may not deploy, start, stop, modify, or delete a service.
Management of proxies	• The user may see all proxy related information. • He is not allowed to create or delete proxy nodes. • He is not allowed to start and stop proxy services. • He is not allowed to edit proxy configuration files and templates. • He cannot manage E2E Proxy Server certificates.