Monitoring UI

With the Monitoring UI, you can configure all errors that occur on the Bridge instance in regards of

- downtimes
- notification threshold
- notification patterns

All those adjustments can be made, if this error has occurred at least once. Once the error has occurred, it will be added to the database and can be configured. It is not possible to "create" errors within the UI.

On this Page:

Related Pages:

- Monitoring Base Service
- Deployment of xUML Services
- Deploying and Managing Resources

Installing the UI

The Monitoring UI is an add-on to the Monitoring Base service. Given the case that the Monitoring Base Service is already deployed and configured (see Monitoring Base Service), the UI can just be deployed without any other prerequisites.
For information on how to deploy services, refer to Deployment of xUML Services.

User Authentication and Authorization

The access to the Monitoring UI can be controlled via user authentication and authorization.

User Authentication

Set setting **Use User Authentication** to **true** to enable user authentication. User authentication can be controlled via

SmartCard login	To use SmartCard login, enable this via setting **Login With Smartcard supported and enabled**.
a **database** dedicated to identity access management	Configure database **IdentityAccessManagement.sqlite** with valid user data and deploy it to the E2E Bridge. Refer to Deploying and Managing Resources for information on how to deploy resources to an E2E Bridge.

User Authorization

An LDAP directory is used to check for authenticated users, if they are allowed to access the UI. Specify the corresponding LDAP settings as described in Changing the UI Settings below.

Changing the UI Settings

The E2E Monitoring UI can be configured via its service settings. For more information on how to access the settings of a service, refer to xUML Service Settings.

Setting Name	Description	Values / Examples	
User Authentication			
Use User Authentication	Specify whether user authentication should be used to control access to the UI.	**true** (default)	Use user authentication.
		false	Do not use user authentication.
TokenValidDurationDays	Specify the duration in **days** the user session will be valid.	`0` (default)	
TokenValidDurationHours	Specify the duration in **hours** the user session will be valid.	`0` (default)	
TokenValidDurationMinutes	Specify the duration in **minutes** the user session will be valid.	`15` (default)	
User Authorization (LDAP Configuration)			
getMethodFromAlias	Specify the LDAP access query method.	`GET` (default)	
getURLFrom Alias	Provide host and port for the LDAP access query.	`ldap://localhost:384`	

LDAP PW	Provide a password for LDAP authentication.		
LDAP User	Specify the user for LDAP authentication.	`CN=John Smith,ou=users, ou=staff,DC=e2e,DC=ch`	
ldapLink_1	Specify the LDAP link (1).		
ldapLink_2	Specify the LDAP link (2).		
Name of LDAP Group 1	Specify the group the UI user has to be member of (1).		
Name of LDAP Group 2	Specify the group the UI user has to be member of (2).		
ID Of Application	Specify the Application ID to check against.		
SmartCard Login			
Login With Smartcard supported and enabled	Enable/Disable SmartCard login.	**true** (default)	SmartCard login enabled.
		false	SmartCard login disabled.