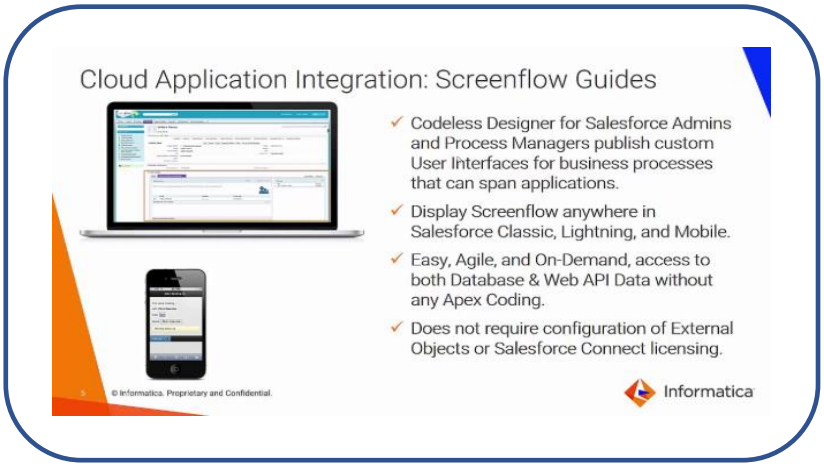
IMPLEMENTATION OF ACCESS CONTROL ON ASSETS USING GUIDES IN INFORMATICA CLOUD APPLICATION INTEGRATION

Guides are used to build user interactive integration applications for users with no or less access to code. With use of informatica integrated design environment guides can be implemented as set of screens to automate several processes and interfaces of applications such as Salesforce.

Guides Usage:

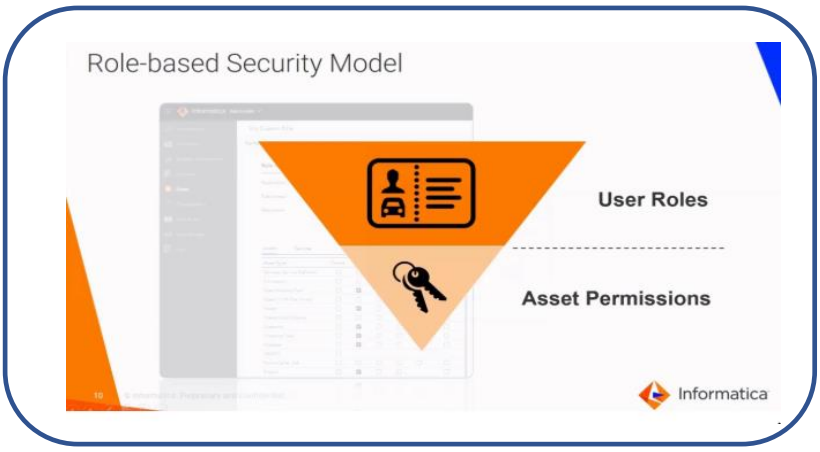
- Guides interact and prompt users to choose, enter and confirm data.
- Guides require minimal technical expertise and choose appropriate path based on the instruction given.
- They can be used in salesforce for easy access of interfaces and also can be accessed via mobile.



Source: www.Informatica.com

Informatica security model:

Informatica has incorporated the asset permission methodology to restrict the object access based on user role which is limited to specific role such as developer/service consumer etc.



Source: www.Informatica.com

The below scenario explains how the asset level security can be implemented using guides.

For example, User1 and User2 have the same User Roles as developer but they must be given access to their corresponding business processes/asset which is a limitation on the asset access.

This has been solved by the below approach.

Fig: Guide implantation depicting user authorization and activation for an asset/component

1. Login/Sign up:

Upon execution of guide, User is landed to a screen that allows him to choose Sign up or login.
Login: When User selected to Login, user will be directed to Login screen to fill the details to create his account.

1. Provide user name.
2. User name is validated against the user repository and if the user is not valid/not existing he will be prompted to Sign up or exit.
3. If the user name is correct, user is prompted to provide password, in case of wrong password which has restriction of 3 attempts limit.

Sign up: When user selects to sign up,

1. User is landed in sign up screen to provide user name, email and password.
2. Upon successful signup, admin will be notified via Email to authorize the user to activate.
3. Once the admin activates the URL, then only user will be able to use his credentials to access the process further.
4. Though the user registration/sign up is completed user will not be able to login till his account is activated.

2. Validation:

Once the user provides the details, user name, password and activation details will be validated against user repository.

3. Multiple Login attempts:

If the user details did not match with the user repository, user will be given 3 more attempts to try the username password combination.

4. Authorization & activation:

As soon as the registration/sign up is completed, admin gets an URL to activate the user. Once the admin approves the user, user gets activated and notified that his account is active. User will be allowed to login to the application.

Conclusion:

The above approach can be incorporated to any ICRT process so that the asset/object access can be restricted among users having similar role.

Contact us for further details

Leela Susmitha Valluri
Sr. Technology Specialist
leelasusmithav.in@mouritech.com

MOURI Tech
www.mouritech.com