Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Canada

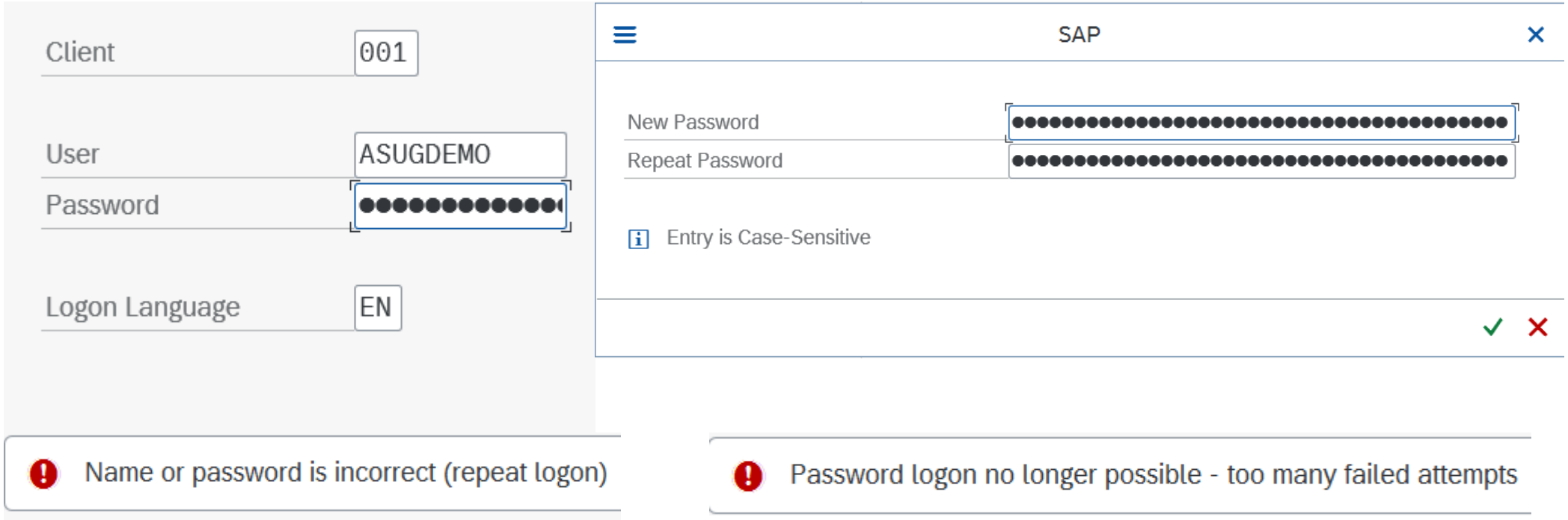
Single Sign On For All

February 2024

The Challenge

How could we provide a seamless user experience while reducing costs and improving security for 25 departments all leveraging a common SAP solution?

How do we get away from this?



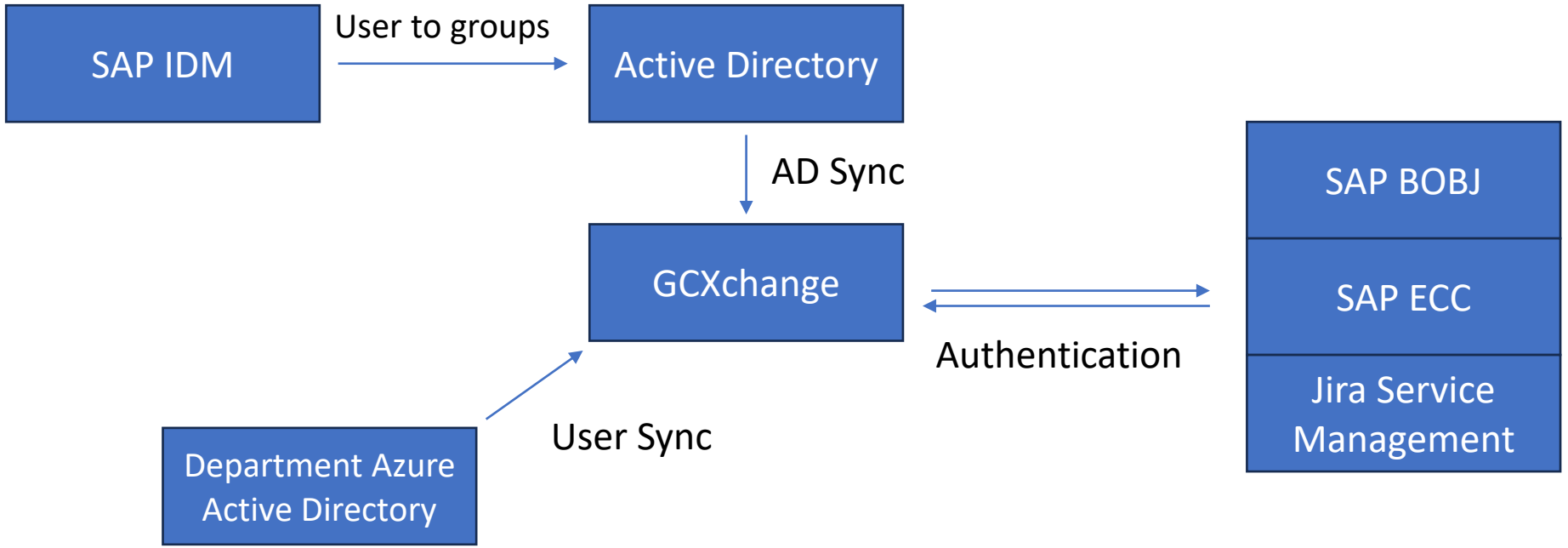
The Teams Involved

- TBS Cloud Infrastructure
- Departmental Cloud Infrastructure
- IT Security Coordinators
- SAP BASIS and Security
- Project and change managers
- Functional and testing team

Departmental Engagement

- Prerequisites
  - Azure Active Directory
  - Security survey to determine cloud guardrails
  - Security agreement between departments
- Azure configuration
  - Creation of a Service Principal in your tenants
  - Setting up cross-tenant access settings
  - Creation/Resuing of an “All Users” group

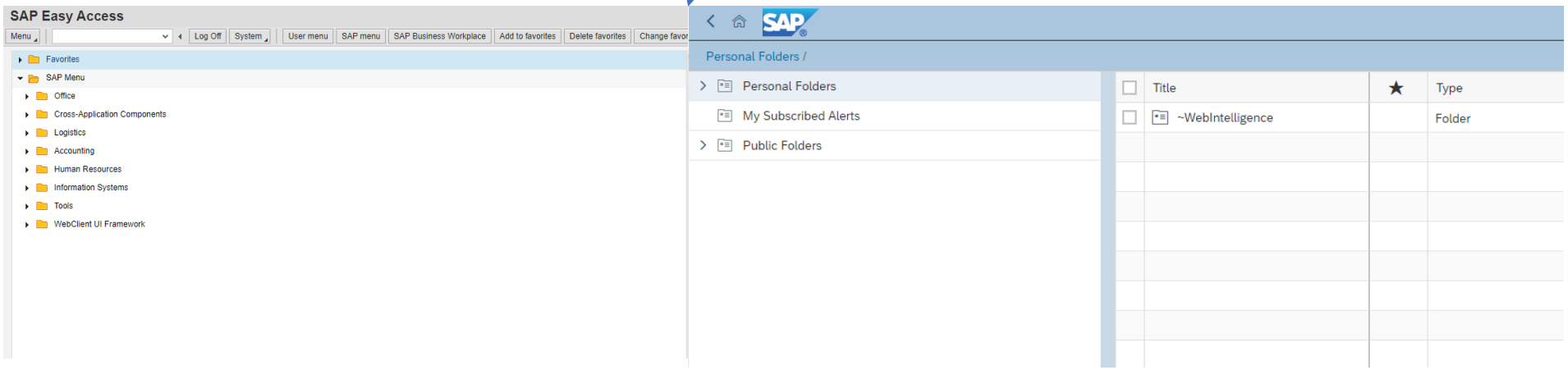
High Level Design



Login Process

Bob Theuser logs into their departmental network account

Bob opens Google chrome and selects the SAP system they would like to connect to



Bob is logged into to the SAP applications

Technical Implementation Steps

- Configured SAML in SAP ECC, SAP BOBJ, and JIRA Service Management
- Created relying parties for each system
- Created Active directory groups to restrict users to certain systems
- Provisioned users to new group structure
- Developed B2B Azure Active Directory sync scripts

Change Management

- Worked with departments to review the future state login options
  - Presented proof of concept
- Determined impact to existing access management processes
- Communicated the new login process
- Welcome email when new users are onboarded or when access changes
- Updated Training Documentation

Testing and Rollout

- Worked with departmental representatives to perform testing in nonproduction environments
- Performed production cutover activities and testing over two days
- Departmental client testing in production
- Hypercare support for two weeks post go-live

Challenges and Lessons Learned

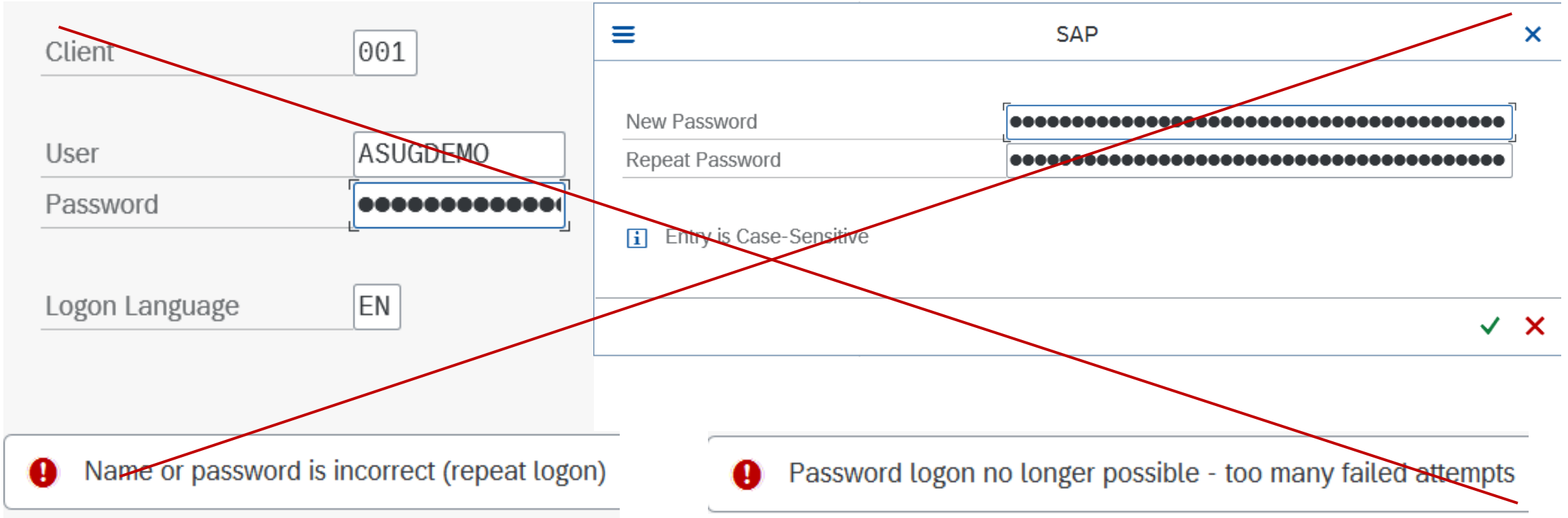
TIMEOUT ISSUES

SYSTEM SPECIFIC CONFIGURATION

USER DATA QUALITY

ALLOCATE MORE TIME FOR TESTING

The Result


Client
001
User
ASUGDEMO
Password
Logon Language
EN
SAP
New Password
Repeat Password
Entry is Case-Sensitive
Name or password is incorrect (repeat logon)
Password logon no longer possible - too many failed attempts

Questions