

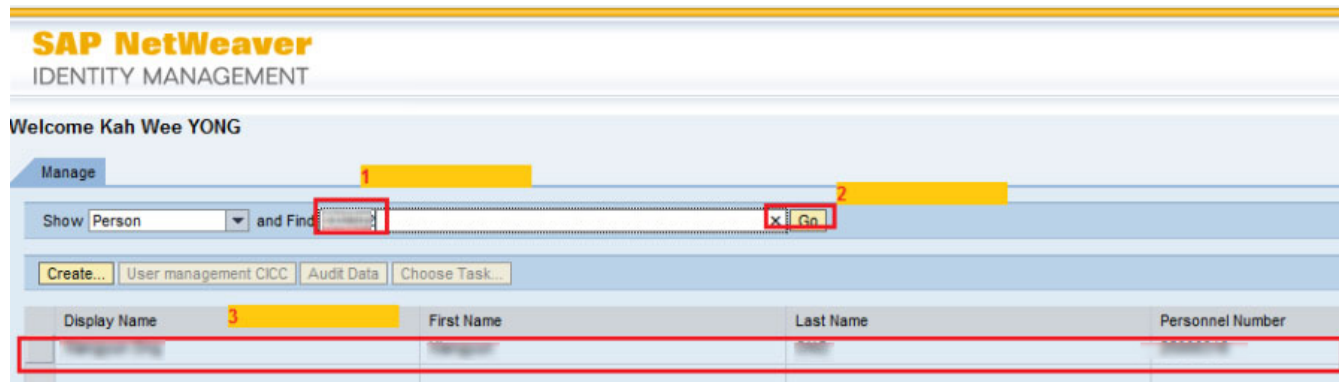
Terminating of PF1 users from Solvay Legacy

First – Go to IMD website link and login with your credentials
<http://pf7sapr3.ibm.be.solvay.com:51800/logon/logonServlet>



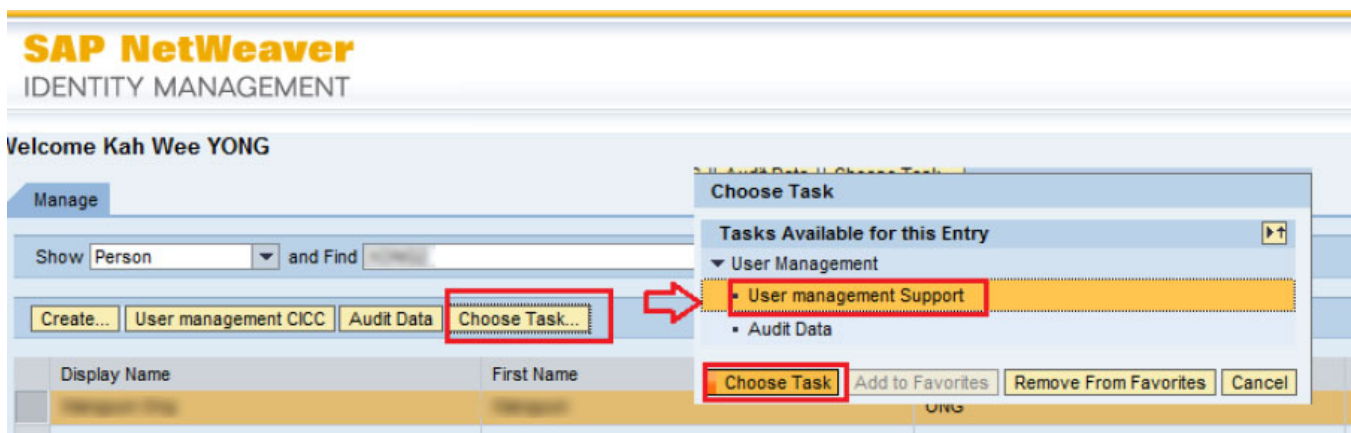
The image shows the SAP NetWeaver login page. On the left is a photograph of a man in a suit writing on a document. On the right, the text "SAP NetWeaver" is displayed in orange. Below it are two input fields: "User ID *" and "Password *", both highlighted with a red rectangular box. A "Log on" button is positioned to the right of the password field. At the bottom right is the SAP logo. At the bottom center, the text "© 2008 SAP AG. All rights reserved." is visible.

Search for the user ID of the person who has left the company



The image shows the SAP NetWeaver Identity Management user search interface. At the top, it says "SAP NetWeaver IDENTITY MANAGEMENT". Below that, it says "Welcome Kah Wee YONG". There is a "Manage" button. A search bar contains the text "Show Person" and "and Find", with a red box around the search input field. To the right of the search bar is a "Go" button. Below the search bar are buttons for "Create...", "User management CICC", "Audit Data", and "Choose Task...". At the bottom, there is a table with columns: "Display Name", "First Name", "Last Name", and "Personnel Number". The first row of the table is highlighted with a red rectangular box.

Select the user name line and click choose task. In the popup box select user management support and click choose task as shown below



In the logon data tab, tick ALL those boxes in white to lock their account in respective environment (Solvay Leagacy systems). Boxes in white means the user have valid account in that environment.

Next scroll further down to the user group(blue systems) and key in ZZZ:DELETE as shown

User management Support

Display Name: Xiangyun Ong First Name: Xiangyun Last Name: ONG Personnel Number: 25000316 User ID: XONG2

Save Modify Refresh

Address Logon data Permissions HCM data

User ID Alias:

User Type: Dialog

Encrypted Password:

System specific locking automatically set if last role is removed (local locking is not retrieved)

System specific unlock automatically set if a role is assigned

Global locked is set as soon as the global valid to date is reached

Locked: ☒

Locked (DE2_020): ☐

Locked (DE2_021): ☐

Locked (DE2_040): ☐

Locked (DE2_050): ☐

Locked (DE2_110): ☐

Locked (DQ1_020): ☐

Locked (SF1_020): ☒

Locked (PF1_020): ☒

Locked (SF1_050): ☒

Locked (PF1_050): ☒

Locked (SQ1_020): ☒

Locked (PQ1_020): ☒

Locked (SI1_020): ☐

Locked (WAD_110): ☐

Locked (WAO_250): ☐

Locked (WAV_400): ☐

Locked (WAP_400): ☐

Locked (WBD_110): ☐

Locked (WBQ_400): ☐

Locked (WBP_400): ☐

Locked (WD1_110): ☐

Locked (WGD_110): ☐

Locked (WGV_400): ☐

Locked (WGO_260): ☐

Locked (WGP_400): ☐

Locked (WQ1_260): ☐

Locked (WV1_400): ☐

Locked (WPI_400): ☐

Locked (PP2_020): ☐

Locked (PQ2_020): ☐

Locked (SQ2_020): ☐

Locked (SP2_020): ☐

Locked (DQ2_020): ☐

Locked (DP2_020): ☐

User Group for Authorization Check

User Group:

User group (blue system): ZZZ:DELETE

User group (green system): ISAAPHDA

Scroll down further and input the expiry date for each available environment.

System specific valid to is leading if set (automatically if last role is removed)

Valid From:

Valid Through:

Valid to (DE2_020):

Valid to (DE2_021):

Valid to (DE2_040):

Valid to (DE2_050):

Valid to (DE2_110):

Valid to (DQ1_020):

Valid to (SF1_020):

Valid to (PF1_020):

Valid to (SF1_050):

Valid to (PF1_050):

Valid to (SQ1_020):

Valid to (PQ1_020):

Valid to (S11_020):

Valid to (WAD_110):

Valid to (WAQ_250):

Valid to (WAV_400):

Valid to (WAP_400):

Valid to (WBD_110):

Valid to (WBQ_400):

Valid to (WBP_400):

Valid to (WD1_110):

Valid to (WGD_110):

Valid to (WGV_400):

Valid to (WGQ_260):

Valid to (WGP_400):

Valid to (WQ1_260):

Valid to (WV1_400):

Valid to (WP1_400):

Valid to (PP2_020):

Valid to (PQ2_020):

Valid to (SP2_020):

Valid to (SQ2_020):

Valid to (DQ2_020):

Valid to (DP2_020):

Other Data

Account Number:

Cost Center:

Once the above is done, proceed to click save to confirm. After saving, the user accounts will be locked and expired in the respective environments after IMD server is refreshed in a few minutes time.

User management Support

Display Name Xiangyun Ong First Name Xiangyun Last Name ONG Personnel Number 25000316 User ID XONG2

Save **Modify** **Refresh**

Address **Logon data** **Permissions** **HCM data**

User ID Alias:

User Type:

Encrypted Password:

System specific locking automatically set if last role is removed (local locking is not retrieved)

System specific unlock automatically set if a role is assigned

Global locked is set as soon as the global valid to date is reached

NOTE: There's no need to set the role expiry date or remove the roles, just lock the user account in their respective environment, set user group to ZZZ:DELETE and then set the expiry date will suffice.