Password provisioning

Purpose

The purpose of this page is to clarify the understanding of the system logic and requirements in relation to password provisioning of IDM system.

Overview

IDM system (with SAP provisioning framework) is able to do password provisioning, which means you can ensure that the user has the same password in all managed application systems. Before doing this, you need to consider the security policy of your organization, and also the requirement from relevant application systems (for example, password policy). Then, you may consider setting initial or productive password during provisioning.

Enable password provisioning

There are two attributes relevant here: MX_PASSWORD and MX_ENCRYPTED_PASSWORD. MX_PASSWORD is stored as hash value for the password, while MX_ENCRYPTED_PASSWORD is encrypted (two-way encryption). So SAP provisioning framework’s password provisioning is based on attribute MX_ENCRYPTED_PASSWORD, which means, it must exist for the relevant MX_PERSON entry so that password provisioning function can work. When choosing “Enable password provisioning” in Password policy tab of your identity store, this will ensure that when storing MX_PASSWORD from web UI, attribute MX_ENCRYPTED_PASSWORD will also be stored separately. But if you want to set these attributes via some job, MX_ENCRYPTED_PASSWORD still need to be set separately although you may have set MX_PASSWORD already. Besides, you also need to set hash/encrypted value explicitly via some script for them. Following internal functions should be helpful here: uGenHash, uEncrypt and uDecrypt.

Setting initial password

By default, SAP provisioning framework sets initial password to the application systems (AS ABAP, AS Java and SAP HANA) if you are using password provisioning, which means end users need to change their password when they firstly logon to these application systems after provisioning from IDM. But if password is already stored centrally in IDM, it may not make sense that end users change it again in application systems. Then you can consider configuring the connector tasks to set productive password as below.

Setting productive password

Both AS ABAP and AS Java system API here allow to set productive password when secure communication channel is fulfilled. For ABAP system, SNC (Secure Network Communication) is required. For AS Java, SSL (Secure Socket Layer) is required. Then, you also need to set the relevant flag (attribute) for the relevant connector pass. For AS ABAP, it is ProductivePwd (set to X), and for AS Java, it is passwordchangerequired (set to false). You can find more information for this in the Related Content section below.

Related Content

Related Documents

SAP NetWeaver Identity Management for SAP System Landscapes: Configuration Guide

Related SAP Notes/KBAs

1602902  Password Not Set to Productive on User Creation
1575445  Setting productive password in ABAP Systems