

Documentation

Agents

The following agents are configured under [Main Menu > Administration > Configuration > Integration engine > Agents](#):

1. IdP Agent

The IdP agent is responsible for managing user authentication and identity validation. It is integrated with the Identity Provider (IdP) and linked to it through its Public ID.

[Main Menu](#) > [Administration](#) > [Configuration](#) > [Integration engine](#) > [Agents](#) 1 / 3 ▶

Basics Attribute mapping Load triggers Massive actions Account metadata

Name	idp *	
Description	Soffid Identity Provider	
Usage	IAM ▼	
Type:	Soffid Identity Provider ▼ <small>Class:es.caib.seycon.idp.agent.IDPAgent</small>	
Server	Each main synchronization server ▼	▼
Shared Thread:	<input checked="" type="checkbox"/> No Dedicated threads: 1	
Task timeout (ms)		Long task timeout (ms):
Trust passwords	<input checked="" type="checkbox"/> No	
Read only	<input checked="" type="checkbox"/> No	
Pause tasks	<input checked="" type="checkbox"/> No	
Manual account creation	<input checked="" type="checkbox"/> No	
Role-based	<input checked="" type="checkbox"/> No	
Groups		
User domain	Default user domain ▼ *	
Passwords domain	Default password domain ▼ *	
User Type	<div><input checked="" type="checkbox"/> User Type</div> <div><input type="checkbox"/> External user</div> <div><input checked="" type="checkbox"/> Internal user</div> <div><input type="checkbox"/> SSO account</div>	

Connector parameters:

Public ID (Must match the public ID defined in Federation)

2. Source AD Agent

The Source AD Agent connects the Soffid console with the Active Directory (AD) to manage user data and synchronization, so we can carry out the authoritative load, to retrieve identities, and the reconciliation process, to request the accounts and ensure that all users are aligned with their

respective roles and responsibilities.

Main Menu > Administration > Configuration > Integration engine > Agents

2 / 3

BasicsAttribute mappingLoad triggersMassive actionsAccount metadata

NameSource AD: postbank.lpb.co.ls

DescriptionAuthoritative data source dc=postbank,dc=lpb,dc=co,dc=ls

UsageIAM

TypeActive Directory Only PasswordsClass:com. soffid. iam. sync. agent2. SSOActiveDirectoryAgent

ServerEach main synchronization server

Shared Thread:

No

Dedicated threads: 1

Task timeout (ms)Long task timeout (ms):

Trust passwordsYes

Authoritative identity sourceYes-

Read onlyNo

Pause tasksNo

Manual account creationNo

Role-basedNo

Groups

User domainDefault user domain *

Passwords domainDefault password domain *

User Type

User Type

External user

Internal user

SSO account

Connector parameters:

Hostname10.0.1.220

LDAP base DNdc=postbank,dc=lpb,dc=co,dc=ls

Principal namepostbank\soffid

Password

Enable debugNo

Accepted certificatesAny (insecure)

Follow referralsDon't

Manage child domainsNoDomains to ignore:

Create OUs when neededNo

Generate flat groupsNo

Undelete deleted usersNo

Real time load last login attributeNo

Real time load identity changesNo

3. SSO Agent

The SSO Agent is responsible for managing user login session across multiple applications. This agent serves as an auxiliary component that facilitates the registration of local accounts in the password vault. This capability allows for secure storage and management of user credentials.

Main Menu > Administration > Configuration > Integration engine > Agents 3 / 3

BasicsAttribute mappingLoad triggersMassive actionsAccount metadata

NameSSO

DescriptionExternal SSO accounts

UsageIAM

Type:External accountsClass:com.softid.iam.sync.sso.agent.SSOAgent

ServerEach main synchronization server

Shared Thread:

No

Dedicated threads: 1

Task timeout (ms)Long task timeout (ms):

Trust passwords

No

Read only

No

Pause tasks

No

Manual account creation

Yes

User domainDefault user domain

Passwords domainDefault password domain

Connector parameters:

AD user

AD Password

Native SMBNo

For more information, please refer to [Agents](#).

Web SSO

The following elements are required for the configuration of Web Single Sign-On (WSSO):

1. Attribute definition

In [Main Menu > Administration > Configuration > Web SSO > Attribute definition](#) , the auto-generated user attributes are stored. These attributes are sent from the IdP to the SP, based on the attribute sharing policies.

Main Menu > Administration > Configuration > Web SSO > Attribute definition

Name	ShortName	OID	OpenID name	RADIUS identifier	Value
Filter	Filter	Filter	Filter	Filter	Filter
<input type="checkbox"/> Accounts & Passwords	Secrets	urn:oid:1.3.6.1.4.1.22896.3.1.6			
<input type="checkbox"/> Email address	mail	urn:oid:0.9.2342.19200300.100.1.3	email		
<input type="checkbox"/> Full name	FullName	urn:oid:2.16.840.1.113730.3.1.241	full_name		
<input type="checkbox"/> Given Name	GivenName	urn:oid:2.5.4.42	given_name		
<input type="checkbox"/> Organizational unit	OU	urn:oid:2.5.4.11	ou		
<input type="checkbox"/> Phone	TelephoneNumber	urn:oid:2.5.4.20	phone		
<input type="checkbox"/> Role & group membership	memberOf	urn:oid:1.3.6.1.4.1.5923.1.5.1.1	meber_of		
<input type="checkbox"/> Session ID	SessionId	urn:oid:1.3.6.1.4.1.22896.3.1.1	session_id		
<input type="checkbox"/> Session key	SessionKey	urn:oid:1.3.6.1.4.1.22896.3.1.2			
<input type="checkbox"/> Surname	Surname	urn:oid:2.5.4.4	family_name		
<input type="checkbox"/> Surnames (all)	Surnames	urn:oid:1.3.6.1.4.1.22896.3.1.5	surnames		
<input type="checkbox"/> User ID	uid	urn:oid:0.9.2342.19200300.100.1.1	sub		
<input type="checkbox"/> User type	UserType	urn:oid:1.3.6.1.4.1.22896.3.1.4	user_type		

Displayed rows: 13

2. Attribute sharing policies

In [Main Menu > Administration > Configuration > Web SSO > Attribute sharing policies](#) the rules under which attributes are shared between the IdP and the SP can be defined. These policies ensure that only relevant and essential attributes are transmitted in a secure manner.

3. Identity & Service Providers

One Entity Group has been created (*Postbank*) in [Main Menu > Administration > Configuration > Web SSO > Identity & Service providers](#). The providers defined within this group are:

3.1. Identity Providers

The identity provider uses Soffid IdP for identity authentication. Adaptive authentication is configured, so if the name of the service provider requesting authentication begins with "Tacacs", it indicates that the service provider is utilizing the Terminal Access Controller Access-Control System (TACACS) and two-factor authentication (2FA) will be required, as shown below.

Description : Tacacs

Condition : `serviceProvider.startsWith("Tacacs");`

Always ask for credentials : ☒ Yes ☐ No

	First auth	Password	Kerberos	External	OTP	Email	SMS	PIN	Certificate	FIDO	Push
Password		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
OTP					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Email						<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SMS							<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PIN								<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Certificate									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FIDO										<input type="checkbox"/>	<input type="checkbox"/>
Push											<input type="checkbox"/>

Otherwise multi-factor authentication (MFA) will be required.

Authentication

Always ask for credentials : ☒ Yes ☐ No

Authentication methods

	First auth	Password	Kerberos	External	OTP	Email	SMS	PIN	Certificate	FIDO	Push
Password		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
OTP					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Email						<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SMS							<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PIN								<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Certificate									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FIDO										<input type="checkbox"/>	<input type="checkbox"/>
Push											<input checked="" type="checkbox"/>

Adaptive authentication...

Kerberos Domain

Kerberos Domain	Principal name	Description
Filter	Filter	Filter

Displayed rows: 0

Additionally, TLS and SAML can be configured uploading the PKCS12 files, which have already been uploaded.

Main Menu > Administration > Configuration > Web SSO > Identity & Service providers ◀ 4 / 15 ▶

Identification

IdP type : Soffid IdP
Identifier : https://soffid.postbank.lpb.co.ls:1443
Name : soffid.postbank.lpb.co.ls
Organization : Postbank
Contact : support@soffid.com

Network

Host Name : soffid.postbank.lpb.co.ls

	Behind proxy	Port	Encryption	Accept TLS Certificates
<input type="checkbox"/>	Filter	Filter	Filter	Filter
<input type="checkbox"/>	false	1443	TLSv1.3	true

Displayed rows: 1

TLS PublicKey : [Change public / private key](#) [Delete public / private key](#) [Generate PKCS10](#)

TLS Certificate chain : -----BEGIN CERTIFICATE-----
MIIG4DCCBcigAwIBAgIUlRl5tAa0pswDQYJKoZIhvcNAQELBQAwwgcYx CzAIBgNV

Service configuration

Metadata : <EntityDescriptor entityID="https://soffid.postbank.lpb.co.ls:1443" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">

SAML Security

PublicKey : [Change public / private key](#) [Delete public / private key](#) [Generate PKCS10](#)

Certificate chain : -----BEGIN CERTIFICATE-----
MIIDJjCCAfagAwIBAgIGAZEmIus3MA0GCgqGSIt3DQEBBQUAMEgxdjAgBgNVBAMM

3.2. Service Providers

Several service providers have been defined. Those that grant access to firewalls, routers and other systems, are prefixed with "Tacacs", thus 2FA will be required. For the remaining service providers, which allow access to proxies and other systems, MFA will be enforced, as stated previously. These providers allow users to connect to various systems directly, without initiating the connection through Soffid, while still ensuring identity authentication through the identity provider.

Main Menu > Administration > Configuration > Web SSO > Identity & Service providers ◀ 9 / 15 ▶

Identification

Type : Tacacs+
Identifier : Tacacs1.12
Name : Tacacs Active firewall

Tacacs+ configuration

Source IPs : 192.168.1.12
Tacacs+ secret :

	Authorization rules
<input type="checkbox"/>	Filter
<input type="checkbox"/>	always true

Displayed rows: 1

Login rules

Roles required to login : Roles required to login

System where an enabled account is required : Source AD: postbank.lpb.co.ls Authoritative data source dc=postbank,dc=lpb,dc=co,dc=ls

For more information, please refer to Web SSO.

XACML Policy Management

In [Main Menu > Administration > Configuration > Security Settings > XACML Policy Management](#) the policy set *PAMMFA* has been created, within which the policy *OTPAapprove* has been defined. It has the obligation to request an OTP with a timeout when launching a connection through PAM.

Policy

Identifier:

Version:

Description:

Rule Combining Algorithm:

Target

<input type="checkbox"/>	Subjects	Operator	Value	+	<input type="checkbox"/>	Resources	Operator	Value	+
Displayed rows: 0					Displayed rows: 0				
<input type="checkbox"/>	Actions	Operator	Value	+	<input type="checkbox"/>	Environments	Operator	Value	+
Displayed rows: 0					Displayed rows: 0				

Variables

<input type="checkbox"/>	Variable	Expression	+
			Displayed rows: 0

Rules

	Rule	Description	Effect	
<input type="checkbox"/>	Approve	Approve	Permit	
				Displayed rows: 1

Obligations

	Obligation	Full fill on	Attribute	Value	
<input type="checkbox"/>	urn:soffid:obligation:otp	Permit	timeout	30	
					Displayed rows: 1

[Undo](#) [Apply changes](#)

This policy is enabled through the Password vault Policy Enforcement Point in [Main Menu > Administration > Configuration > Security Settings > XACML PEP configuration](#), where the Policy Set Id must be specified.

Password vault Policy Enforcement Point (PEP)

Enable XACML Policy Enforcement Point : ☒ Yes ☐ No

Policy Set Id :

Policy Set Version :

Trace requests : ☒ Yes ☐ No

For more information, please refer to [XACML Policy Management](#) and [XACML PEP configuration](#).

Password Vault

As an example, in [Main Menu > Administration > Resources > Password vault](#) the *PAM Tests* folder has been created, within which two accounts have been created as well.

1. PAM TEST RDP

This account allows us to launch a connection to a machine through the PAM Launcher of Soffid. For this purpose, in "Basics", it is mandatory to indicate the login URL, where the network protocol must be specified (RDP in this case), together with the IP of the machine that we want to connect to. We also need to specify the Launch type, indicating it is a PAM Jump Server, and the Jump server group corresponding to the PAM Jump Server. Additionally, owners can be selected to handle privileged access.

Main Menu > Administration > Resources > Password vault < 3 / 4 >

Actions Basics

Common attributes

System :SSO⌵⚡ External SSO accounts

Name :2

Login name :dmokopotsa

Description :PAM TEST RDP

Type :Unmanaged⌵

Status :Enabled⌵

Credential type :Password

Password policy :SSO account⌵

Managers

Manager groups :Manager groups👤

Manager users :Manager users👤

Manager roles :Manager roles👤

Password synchronization

Server type :⌵

Server name :Server name

Launch properties

Login url :rdp://10.0.1.62

Launch type :PAM Jump server⌵

Jump server group :Postbank-PAM-Jump-Server - Postbank PAM Jump Server⌵

Owners

Owner groups :Owner groups👤

Owner users :dmokopotsa👤 Motseki Mokopotsa ⌵
admin👤 Soffid Administrator ⌵
Owner users :SOFFID_ADMIN@soffid👤 SOFFID Administrator ⌵
Owner roles :Owner roles👤

SSO Users

Granted groups :Granted groups👤

Granted users :Granted users👤

Granted roles :Granted roles👤

Password vault

Vault folder :PAM Tests

Inherit new permissions :III No

Audit information

Created :13/8/2024 16:12

Last login :

Last change :9/9/2024 18:00

Last updated :

Last password set :13/8/2024 16:29

Password expiration :13/8/2025 16:29

In use by :

Consequently, in "Actions", a password must be set in the "Set now" option, so we can launch the connection and unlock the use of the account. Have in mind that we can change the password policies in Main Menu > Administration > Configuration > Security Settings > Password Policies.

Main Menu > Administration > Resources > Password vault < 3 / 4 >

Actions Basics

Name :2

Description :PAM TEST RDP

System :SSOExternal SSO accounts

Login name :dmokopotsa

Login url :rdp://10.0.1.62

Credential type :Password

In use by :

Launch

View password

Set now

However, when launching the connection an OTP will be requested, due to the Password vault policy previously explained.

Actions Basics

Name : 2

Description : PAM TEST RDP

System : SSO

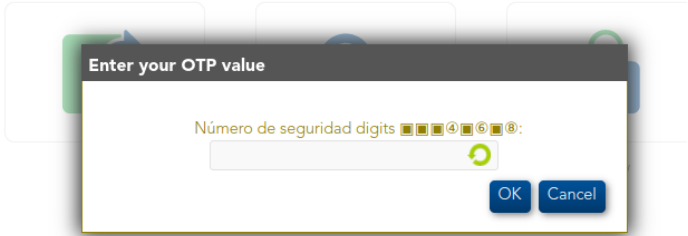
Login name : dmokopotsa

Login url : rdp://10.0.1.62

Credential type : Password

In use by :

External SSO accounts



2. PAM TEST SSH

Another account has been defined for launching a connection through SSH. The concepts explained in the previous account extend to this one.

For more information, please refer to [Password vault](#).

Connectors

The plugins required for the connectors are stored in [Main Menu > Administration > Configuration > Global Settings > Plugins](#) , where the addon files can be uploaded.

Main Menu > Administration > Configuration > Global Settings > Plugins

Plugin	Version	Deployed by	Date
Filter	Filter	Filter	Filter
<input type="checkbox"/> Default plugin	3.6.4		26/8/2024 14:57
<input type="checkbox"/> External accounts plugin	1.0.2		25/6/2024 10:49
<input type="checkbox"/> Mariadb plugin	1.0.3		25/6/2024 10:49
<input type="checkbox"/> Oracle plugin	2.2.4		25/6/2024 10:49
<input type="checkbox"/> REST Web service plugin	1.2.14		25/6/2024 10:50
<input type="checkbox"/> SQL Server plugin	1.0.1		25/6/2024 10:49
<input type="checkbox"/> SQL plugin	1.7.10		25/6/2024 10:50
<input type="checkbox"/> Shell plugins	1.4.16		26/8/2024 14:58
<input type="checkbox"/> Soffid Admin addon	3.1.18	admin	1/8/2024 14:59
<input type="checkbox"/> Soffid Identity Federation	3.6.21-2024.08.24.17.02	admin	24/8/2024 17:02
<input type="checkbox"/> Soffid Identity XACML	3.0.18	admin	19/8/2024 09:57
<input type="checkbox"/> Soffid OTP addon	2.2.20	admin	1/8/2024 14:59
<input type="checkbox"/> Windows plugin	5.4.22		26/8/2024 14:57

Displayed rows: 13

These tools help manage external accounts, databases like MariaDB, Oracle, and SQL Server, and interact with REST web services. They also provide SQL execution capabilities, shell scripting, and seamless integration with Windows environments. On the security and identity management side, we have connectors that handle identity federation, XACML and multi-factor authentication via OTP.

For more information, please refer to [Connectors](#).

Revision #49

Created 8 October 2024 12:45:29 by araja@soffid.com

Updated 24 October 2024 08:57:37 by araja@soffid.com