ISAM Password-callout Configuration Guide

IBM Security Identity Governance and Intelligence version 5.2.5.1 adds support for reverse password synchronization (RPS) from ISAM Password-callout. When you set up the ISAM connector in Identity Governance and Intelligence and run ‘Change Password’ from ISAM, Identity Governance and Intelligence synchronizes the password for all the other accounts (WinAd, Linux, etc.) that are in the same ‘Password Sync Group’.

To enable the RPS functionality, you need to run the following configuration steps in the ISAM VA:

1) Import the IGI VA certificate into the ISAM VA. Follow these steps:

   a. In the ISAM Virtual Appliance, select **Manage system settings** -> **Secure Settings** -> **SSL Certificates**.

   b. In the SSL Certificates table, select the **pdsrv** (Certificate Database Name) row. Then, select **Manage** -> **Edit SSL Certificate Data**.

   c. In the pop up window, choose **Signer Certificates**. Select **Manag**e -> i**mport**.

   d. In the ‘Import Signer Certificate’ pop up window, select the IGI certificate that you want to import.

   e. After the certificate is imported, close the ‘Edit SSL Certificate Database’ window. The following info message is displayed:
   ‘There is currently one undeployed change. <link>Click here to review the changes or apply them to the system.’ Click the link to deploy the changes. After the deployment completes, ignore the warning message to restart reverse proxy at this time.

2) Customize the ‘Reverse Proxy’ configuration file. Follow these steps:

   a. Back in ‘Home Appliance Dashboard’, select **Secure Web Settings** -> **Manage** -> **Reverse Proxy**.

   b. In the ‘Reverse Proxy’ table, select **default**. Select **Manage** -> **Configuration** -> **Edit Configuration File**. The ‘Advanced Configuration File Editor’ opens.

   d. Search the configuration file and find the **[password-callouts]** section. Configure the required attributes that are listed in the following table:

Attribute Name	Attribute Value (i. e.)	Description	Required
proxy	http[s]://<address>:<port>	The proxy, if any, which is used to reach the various end-points. The configuration entry should be in URL format	Optional
authentication-endpoint	https://{host}:{port}/igi/v2/security/token	This is the endpoint which will be called to obtain an access token which can then be used in the subsequent password update callouts. If no endpoint is specified a BA header, constructed from the client-id and client-secret configuration entries, will be used. The endpoint should conform to the OAuth client credential flow (OAuth 2.0 RFC 6749, section 4.4). OAuth 2.0 RFC 6749, section 4.4	Required
client-id	admin	The client identifier, which is used when authenticating to the callout services. (IGI's Admin's Username)	Required

search-endpoint	https://{host}:{port}/igi/v2/agc/users/accounts/.search	The endpoint which will be called to map the ISAM user identity into an identity which is known to the callout services. This endpoint should conform to the System for Cross-domain Identity Management RFC 7644 # (section 3.4.2). System for Cross-domain Identity Management: Protocol (section 3.4.2) If no endpoint is specified the ISAM user identity, as # provided in the password change request, will be used in the callout # to the pre/post update services.	Required

search-filter	userName eq "{username}" Note: userName is the one logged in ISAM pwdcfg_name eq "ISAM" Note: “ISAM” is account configuration name in IGI for ISAM connector and it must be registered in IGI urn:ibm:params:scim:schemas:resource:bean:agc:2.0:Account:code eq "{username}" and urn:ibm:params:scim:schemas:resource:bean:agc:2.0:Account:pwdcfg_name eq "ISAM"	The search filter which is used when mapping the ISAM user identity into an identity which is known to the callout services. This search filter should conform to the System for Cross-domain Identity Management # RFC 7644 (section 3.4.2.2). The '{username}' macro can be used in the filter to indicate the user identity which has been provided in the password change request.	Required (At least one filter need to be applied to locate the account)
pre-update-endpoint	https://{host}:{port}/igi/v2/agc/users/accounts/PasswordValidateRequests	The endpoint which will be called to perform any password pre-update processing. This endpoint should conform to the draft-hunt-scim-password-mgmt-00 RFC (section 2.5). draft-hunt-scim-password-mgmt-00 (section 2.5)	Required
pre-update-user-prefix	/Users/accounts/	The prefix which is used when building the user identity to be included in the password pre-update callout.	Required

post-update-endpoint	https://{host}:{port}/igi/v2/agc/users/accounts/	The endpoint which will be called to perform any password post-update processing. This endpoint should conform to the System for Cross-domain dentity Management: Protocol RFC 7644 (section 3.5.2) [System for Cross-domain dentity Management: Protocol RFC 7644 (section 3.5.2)]	Required
static-header	realm:IDEAS # Any static headers which should be added to the callout requests. The # format of the configuration entry will be: 'header name: header value', # for example: # static-header = realm:IDEAS	The configuration entry may be specified multiple times, one for each header that needs to be added to the callout requests. The value of realm in static-header must be IDEAS for “search-endpoint”, “pre-update-endpoint”, “post-updated-endopoint”	Required (realm is required in IGI)
static-header	password-callout:true # The value of password-callout must be “True”	Required for reverse password synchronization	Required
authentication-static-header	realm:ADMIN # The value of realm in authentication-static-header must be ADMIN for “authentication-endpoint”	Added it only for authentication-endpoint use	Required
client-secret	IGI’s Admin’s password	The following configuration item is contained within the obfuscated	Required

		database and as such is obfuscated within this file. If the value is modified within this configuration file the corresponding change will be applied to the obfuscated database.	

3) After you filled in all required fields in the configuration file, select **Save**. The system then asks you to deploy the changes and to restart Reverse Proxy to make them effective.