IBM® Security Access Manager
for Versions 9.0.6.0

IBM Security Access Manager Multi-factor Authentication API

Version 1.0.0

Contents

Preface

Access to publications and terminology

The following publications complement the information contained in this document:

Publication Library

These publications complement the information that is contained in this publication:

Base Information

- *IBM® Tivoli® Access Manager Base Installation Guide*

  Explains how to install, configure, and upgrade Access Manager software, including the Web portal manager interface.

- *IBM Security Access Manager Base Administrator's Guide*

  Describes the concepts and procedures for using Access Manager services. Provides instructions for managing tasks from the Web portal manager interface and by using the pdadmin command.

WebSEAL Information

- *IBM Security Access Manager WebSEAL Installation Guide*

  Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.

- *IBM Security Access Manager WebSEAL Administrator's Guide*

  Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.

- *IBM Security Access Manager WebSEAL Developer's Reference*

  Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

Web Gateway Appliance Information

- *IBM Security Access Manager Web Gateway Appliance Administration Guide*

  Provides information about configuring and maintaining a Security Access Manager environment.

- *IBM Security Web Gateway Appliance Configuration Guide for Web Reverse Proxy*

  Provides configuration procedures and technical reference information for the Web Gateway Appliance.

- *IBM Security Web Gateway Appliance Web Reverse Proxy Stanza Reference*

  Provides a complete stanza reference for the Web Gateway Appliance Web Reverse Proxy.

Mobile Information

- *IBM Security Access Manager for Mobile Administration Guide*

  Describes how to manage, configure, and deploy an existing IBM Security Access Manager environment.

- *IBM Security Access Manager for Mobile Configuration Guide*

  Explains how to complete the initial configuration of IBM Security Access Manager for Mobile.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at `http://www.ibm.com/software/globalization/terminology`.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical Training

For technical training information, see the following IBM Education website at `http://www.ibm.com/software/tivoli/education`.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at `http://www.ibm.com/software/support/probsub.html`.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Introducing the Integration

Introduction

IBM Security Access Manager (ISAM) contains authentication mechanisms and policies that can be integrated into new or existing web applications to provide multi factor authentication. This integration provides a method that allows these strong authentication policies to be used to provide multi factor authentication to traditional mainframe style applications.

The strong authentication is implemented by creating an OAuth backchannel between the application and the ISAM appliance. A user will generate an expiring one time password (OTP) that they will use as the password to the application. The application must then use the OAuth backchannel to enable the ISAM appliance to validate the OTP and login the user.

You must have an ISAM environment with Advanced Access Control enabled to use this integration. The application must be configured to allow OAuth communication with the ISAM appliance.

The installer for this application will allow one or both of Mobile Multifactor authentication using IBM Verify or authentication using a FIDO U2F token. These are provided as an example of 2 common authentication mechanisms. Other mechanisms will also work but are not supported as part of the installer.

The installation has been tested against the following environments:

1. A clean ISAM appliance install with:
    a. Base and Advanced Access Control activated
    b. The runtime component configured against the embedded LDAP
    c. The required ACLs created
2. An ISAM appliance that has been setup following the IBM Verify Cookbook.

Although these were the main environments tested on. The installation script is flexible enough to work with most environments. Please see the list of parameters and their descriptions to plan the installation for any environment.

Integration Product Contents

The integration solution is packaged as a compressed file. The package contains the following files:

File Name	Description
`isam_apimfa_appx.pdf`	This integration guide.
`isam_apimfa_appx.zip`	Packaged ISAM App Exchange App for automated deployment, configuration and templating for use with the AppX Installer Python script. Extract this zip before executing the installer script.

Table 1: Integration Package contents

Before you start

This integration guide details the steps that are required to achieve this integration at a high level in your environment.

This guide does not cover the configuration of the entire environment. In particular, the following product installations and configurations must already be complete:

- IBM Security Access Manager
  - IBM Security Access Manager Web Reverse Proxy
  - IBM Security Access Manager Advanced Access Control

- IBM Security Appx Installer version 1.0.2
  - Download the appx installer from the App Exchange
  - Ensure that the prerequisites are met for the appx installer as per the documentation for that application

IBM Security Access Manager Configuration

Complete the following configuration steps on the IBM Security Access appliance prior to installing the integration.

1. ISAM Runtime Component Configuration
2. ISAM ACL creation

Note that if the ISAM appliance has been setup using the IBM Verify cookbook these tasks will have already been completed.

ISAM Runtime Component Configuration

The ISAM runtime component must be configured prior to the integration being installed.

To perform this configuration use the ISAM local management interface.

1. Using the menu select Secure Web Settings —> Runtime Component
2. Click the Configure button and follow the wizard steps

ISAM ACL Creation

The integration requires some existing ACL entries. Please ensure that the following ACLs exist prior to installing the integration and have the permissions shown.

- isam_mobile_anyauth
  - any-other Tr
  - User sec_master TcmdbsvaBRrxl
  - unauthenticated T
  - Group iv-admin TcmdbsvaBRrxl
  - Group webseal-servers Tgmdbsrxl
- isam_mobile_nobody
  - any-other T
  - User sec_master TcmdbsvaBRrxl
  - unauthenticated T
  - Group iv-admin TcmdbsvaBRrxl
  - Group webseal-servers Tgmdbsrxl
- isam_mobile_rest
  - any-other Tmdr
  - User sec_master TcmdbsvaBRrxl
  - unauthenticated T
  - Group iv-admin TcmdbsvaBRrxl
  - Group webseal-servers Tgmdbsrxl
- isam_mobile_unauth
  - any-other Tr
  - User sec_master TcmdbsvaBRrxl
  - Group iv-admin TcmdbsvaBRrxl
  - Group webseal-servers Tgmdbsrxl
  - unauthenticated Tr
- isam_mobile_rest_unauth
  - any-other Tmdrxl
  - User sec_master TcmdbsvaBRrxl
  - Group iv-admin TcmdbsvaBRrxl
  - Group webseal-servers Tgmdbsrxl
  - unauthenticated Tmdrxl

The attachment of these ACLs is listed later in this document.

Running the Installation Script

In this section the installation of the integration will be described.

Extracting the application and installer zip files

Having downloaded the IBM Security Multi-factor Authentication API application and the ISAM AppX Installer App, extract the isam_apimfa_appx.zip file into a new directory. Once this is complete the next step is to extract the isam_appx_installer.zip file into the same directory. Now amongst other files and directories the root of the new directory should contain

Filename	Description
`setup.sh`	The setup script used to install the application. Requires the appx_installer.py file.
`appx_installer.py`	The appx installer. This is not run directly to install the application but is rather called indirectly from the setup script.

Table 2: Directory files

Running the installer script

Having extracted the application and installer zip files into a new directory, execute the setup script to install the application by configuring the IBM Security Access Manager appliance.

For example:

```
[user@host ~]# ./setup.sh
```

The setup script can be run in 2 different ways:

1. Interactive mode. In this mode the user will be prompted to enter the required configuration options. Some of these have default values whilst others are mandatory.

   Example:

   ```
   ./setup.sh -I
   ```

2. Non interactive mode. In this mode all of the configuration options are specified up front. Some of these have default values whilst others are mandatory.

   Example:

   ```
   ./setup.sh --lmihost isam.test.ibm.com --lmipwd Passw0rd  --policypwd Passw0rd --proxyip 192.168.42.102 --rthost www.test.ibm.com --easuserpwd passw0rd --oauthclientsecret passw0rd --ldappwd Passw0rd
   ```

Example install on a clean environment

One of the tested environment mentioned above was a clean ISAM appliance with:

1. Base and Advanced Access Control activated
2. The runtime component configured against the embedded LDAP
3. The required ACLs created

In this environment all of the configuration tasks need to be performed. To setup both MMFA and FIDO U2F authentication the setup script command would be:

./setup.sh --lmihost isam.test.ibm.com --lmipwd passw0rd --policypwd passw0rd --proxyip 192.168.42.102 --rthost www.test.ibm.com --easuserpwd passw0rd --createdefault true --oauthclientsecret passw0rd --ldappwd Passw0rd

Example install on an IBM Verify environment

One of the tested environment mentioned above was an ISAM appliance that has been setup following the IBM Verify Cookbook.

In this environment the MMFA tasks and default instances are already setup and can be skipped. Also the OAuth backchannel will need to listen on a non default port. The script command would be:

./setup.sh --lmihost isam.test.ibm.com --lmipwd Passw0rd --policypwd Passw0rd --proxyip 192.168.42.102 --rthost www.test.ibm.com --easuserpwd Passw0rd --createdefault false --configdefault false --configscim false--oauthproxy backchannel --oauthhttpsport 445 --oauthlistport 7236 --oauthclientsecret passw0rd --enablemmfa true --mmfaproxy mobile --createmobile false --configmmfa false --configmmfaapimfa true

Note: This installation assumes that the environment has been setup by following the IBM Verify Cookbook. Please ensure that all of the steps in the cookbook have been completed prior to running the above installation script.

Verifying Output of the setup script

The setup script will update the configuration of the IBM Security Access Manager appliance for use with this application.

Ensure the script completes successfully and check for any errors or warnings in the output.

```
Starting App Deployment

2017-11-28 13:48:13,215 - AppX - INFO - replace_config_variables

2017-11-28 13:48:13,216 - AppX - INFO - App Name: <IBM Security App Exchange
Partner Application>

2017-11-28 13:48:13,216 - AppX - INFO - replace_original_manifest

...
```

```
2017-11-28 13:48:13,216 - AppX - INFO - Connecting to ISAM at
'https://isam903lmi.mysecure.org'

2017-11-28 13:48:13,903 - AppX - INFO -

2017-11-28 13:48:22,868 - AppX - INFO - Deploying changes

...

Complete
```

Usage and Advanced Configuration Options

The following table lists and describes all of the configuration parameters for running the installer script.

Parameter	Required	Default	Description
--lmihost	Yes		Security Access Manager Appliance Local Management Interface hostname.
--lmiport	No	443	Security Access Manager Appliance Local Management Interface port.
--lmipwd	Yes		Security Access Manager Appliance administrator password.
--policyadmin	No	sec_master	Security Access Manager administrator user ID.
--policypwd	Yes		Security Access Manager administrator password.
--domain	No	Default	Security Access Manager Domain Name.
--proxyip	Yes		Listening IP address of the reverse proxy instances.
--rthost	Yes		Advanced Access Control runtime listening interface hostname.
--easuserpwd	Yes		Advanced Access Control runtime easuser password.
--defaultproxy	No	default	The name of the default reverse proxy instance.
--createdefault	No	false	Boolean flag indicating whether or not to create the default reverse proxy instance. Only set this to true if the instance does not already exist.

Parameter	Required	Default	Description
--defaulthttpsport	No	443	HTTPS port of the default reverse proxy instance.
--defaultlistport	No	7234	Listening port of the default reverse proxy instance.
--overwritedefault	No	true	Boolean flag indicating whether or not to overwrite an existing default reverse proxy instance (if one already exists with the same name as listed in defaultproxy). If createdefault is set to false this will be ignored.
--configdefault	No	true	Boolean flag indicating whether or not to run the required configuration tasks on the default reverse proxy instance.
--overwritedefaultconf	No	true	Boolean flag indicating whether or not to overwrite the existing default reverse proxy instance configuration. If set to false, any existing configuration will remain unchanged but any new configuration will be set.
--configscim	No	true	Boolean flag indicating whether or not to configure the SCIM components. Set this to false if the SCIM components have already been configured.
--oauthproxy	No	backchannel	The name of the OAuth backchannel reverse proxy instance. This will be used for Oauth communication between the application and the ISAM appliance.
--oauthhttpsport	No	444	HTTPS port of the OAuth backchannel reverse proxy instance.
--oauthlistport	No	7235	Listening port of the OAuth backchannel reverse proxy instance.
--oauthclientsecret	Yes		Client secret for the OAuth backchannel API Client. This is the password/secret used to establish the Oauth channel.
--enablemmfa	No	true	Boolean flag indicating whether or not to enable Mobile Multifactor authentication (MMFA) as a source of 2nd factor authentication for the application.
--mmfaproxy	No	mobile	The name of the MMFA reverse proxy instance
--createmobile	No	true	Boolean flag indicating whether or not to create the MMFA reverse proxy instance. Only set this to true if the instance does not already exist.
--mmfahttpsport	No	445	HTTPS port of the MMFA reverse proxy instance.

Parameter	Required	Default	Description
--mmfalistport	No	7236	Listening port of the MMFA reverse proxy instance.
--overwritemobile	No	true	Boolean flag indicating whether or not to overwrite the MMFA reverse proxy instance (if one already exists with the same name as listed in mmfaproxy). If createmobile is set to false this will be ignored.
--configmmfa	No	true	Boolean flag indicating whether or not to run the required configuration tasks on the MMFA reverse proxy instance.
--overwritemmfa	No	true	Boolean flag indicating whether or not to overwrite the existing MMFA reverse proxy instance configuration. If set to false, any existing configuration will remain unchanged but any new configuration will be set.
--ldappwd	Yes (but only if configmmfa is set to true)		Embedded LDAP bind user password.
--configmmfaapimfa	No	true	Boolean flag indicating whether or not to configure the MMFA advanced access control components that are specific to this integration.
--overwritemmfaapimfa	No	true	Boolean flag indicating whether or not to overwrite the MMFA advanced access control configuration that is specific to this integration.
--publichostname	No	The value of rthost	Advanced Access Control runtime listening interface public hostname. This is the publicly accessible host that can be used to access the MMFA reverse proxy instance. It will be used in MMFA configuration and is ignored if configmmfa is set to false.
--publicport	No	The value of mmfahttpsport	Advanced Access Control runtime listening interface public port. This is the publicly accessible port that can be used to access the MMFA reverse proxy instance. It will be used in MMFA configuration and is ignored if configmmfa is set to false.
--enableu2f	No	true	Boolean flag indicating whether or not to enable FIDO U2F as a source of 2nd factor authentication for the application.

Table 3: Setup script parameters

Testing the installation

The application includes some additional resources that can be used to validate the installation of the application.

Filename	Description
`mainframe_demo.sh`	This is a simple script that simulates a mainframe login.
`apimfa.html` `apimfa_inner.html`	These 2 html files comprise a sample web page that will allow device registration and OTP generation to allow login to the mainframe_demo application

Table 4: Test resources

To test the application installation perform the following tasks:

1. Add the apimfa.html and apimfa_inner.html to the junction root of the default reverse proxy instance.
2. Update the mainframe_demo script.
    a. Set the BASEURL to the url of the backchannel reverse proxy instance. For example:
        i. https://www.test.ibm.com
    b. Set the PORT to the port of the backchannel reverse proxy instance. For example:
        i. 444
3. Access the sample web page
    a. https://www.test.ibm.com/apimfa.html
4. The browser should prompt to login
    a. Login using an existing user in ISAM. If not user exists then create a new user is ISAM. For example:
        i. user create testuser cn=testuser,dc=iswga Test User passw0rd
        ii. user modify testuser account-valid yes
5. Click on the link to Manage / Register IBM Verify and FIDO U2F
6. Register:
    a. A mobile device with IBM Verify installed (using the AuthenticatorClient); and/or
    b. A FIDO U2f token
7. Once registered click the Home button to return to the main page
8. Click on the link to Obtain Application OTP
9. Select the device to authenticate with
10. After successful authentication click Generate OTP for the mainframe_demo app
11. Run the mainframe_demo script
    a. Login with the ISAM user and the OTP
    b. Verify that the script prints the message “Authentication Success”

Adding a new Authentication Mechanism

The installer provides the ability to configure one or both of the FIDO U2F and Mobile Multi-factor authentication mechanisms as the source of the 2nd factor authentication. This does not mean that the application is limited to only these. If another mechanism is required, follow this process to add it into the list of available mechanisms.

1. Configure the required authentication policy.
2. Edit the mapping rule “select_2fa”
3. Search for the text “add more methods here if you have them”
4. Add in the details for the new method.
    a. For example: If the new method was for QRCode login:

```
// add more methods here if you have them
if (true) {
        // Can use QRCode login
        var method = {};
        method["type"] = "qrcode";
        method["policyURI"] = "urn:ibm:security:authentication:asf:qrcode_initiate";

        method["displayLabel"] = "QRCode Login";
        permittedMethods.push(method);
}
```

5. Now when Obtain Application OTP is clicked the new method should be available in the selection list.

Configuration Tasks

This section is a reference to the ISAM configuration tasks that are run during the installation. There are a number of subsections that relate to a separate part of the setup.

OAuth Backchannel

The installer will create and configure a number of components that will be used for Oauth communication between the application and the ISAM appliance.

1. Create a backchannel reverse proxy instance. The name, HTTPS port and listening port are configurable when running the setup script.
2. Load the ISAM appliance local runtime default certificate into the pdsrv CA signer certificates.
3. Create a junction on the backchannel reverse proxy instance “/mga”.
4. Update the backchannel reverse proxy instance configuration file with the required values for this integration.
5. Attach the required ACLs to the OAuth backchannel URLs:
    a. isam_mobile_unauth —> /mga/sps/oauth/oauth20/token
    b. isam_mobile_rest —> /mga/sps/apiauthsvc
    c. isam_mobile_nobody —> /mga

Default Reverse Proxy Instance

The installer may create and configure a default reverse proxy instance used as an interface to the management of the multi factor authentication mechanisms and generation of one time passwords for authentication to the application.

1. Create the default reverse proxy instance if required. The name, HTTPS port and listening port are configurable when running the setup script. If this instance already exists the creation can be skipped.
2. Create a junction on the default reverse proxy instance “/mga”.
3. Create a junction on the default reverse proxy instance “/scim”.
4. Update the default reverse proxy instance configuration file with the required values for this integration.

5. Attach the required ACLs to the default URLs:
    a. isam_mobile_anyauth —> /mga/sps/xauth
    b. isam_mobile_anyauth —> /mga/sps/mga/user/mgmt/html
    c. isam_mobile_anyauth —> /mga/sps/mmfa/user/mgmt/html
    d. isam_mobile_anyauth —> /mga/sps/oauth/oauth20/clients
    e. isam_mobile_anyauth —> /mga/sps/ac
    f. isam_mobile_anyauth —> /mga/sps/auth
    g. isam_mobile_anyauth —> /mga/sps/common/qr
    h. isam_mobile_anyauth —> /mga/sps/wssoi
    i. isam_mobile_nobody —> /mga
    j. isam_mobile_rest —> /mga/sps/mmfa/user/mgmt/auth_methods
    k. isam_mobile_rest —> /mga/sps/mmfa/user/mgmt/qr_code
    l. isam_mobile_rest —> /mga/sps/mmfa/user/mgmt/transactions
    m. isam_mobile_rest —> /scim
    n. isam_mobile_rest —> /mga/sps/mga/user/mgmt/otp
    o. isam_mobile_rest —> /mga/sps/mga/user/mgmt/device
    p. isam_mobile_rest —> /mga/sps/mmfa/user/mgmt/authenticators
    q. isam_mobile_rest —> /mga/sps/mga/user/mgmt/questions
    r. isam_mobile_rest —> /mga/sps/mga/user/mgmt/grant
    s. isam_mobile_rest_unauth —> /mga/websock/mmfa-wss
    t. isam_mobile_rest_unauth —> /mga/sps/apiauthsvc
    u. isam_mobile_unauth -> /mga/sps/authservice/authentication
    v. isam_mobile_unauth -> /mga/sps/oauth/oauth20/session
    w. isam_mobile_unauth -> /mga/sps/oauth/oauth20/token
    x. isam_mobile_unauth -> /mga/sps/static
    y. isam_mobile_unauth -> /mga/sps/oauth/oauth20/authorize
    z. isam_mobile_unauth -> /mga/sps/authsvc

SCIM Configuration

The installer may configure the required SCIM components.

1. Create 2 new server connections
    a. A connection to the embedded LDAP (localldap). This should be modified post install if the embedded LDAP is not being used but rather an external LDAP is in use.
    b. A web service connection to the local SCIM endpoint.
2. Update the SCIM Endpoint Configuration authentication mechanism. Set the connection to be the new SCIM web service server connection.
3. Configure SCIM
    a. Set readwrite mode for urn:ietf:params:scim:schemas:extension:isam:1.0:MMFA:Transaction:transactionsPending
    b. Set readwrite mode for urn:ietf:params:scim:schemas:extension:isam:1.0:MMFA:Transaction:transactionsPending:txnStatus
    c. Set the LDAP connection to be the new embedded LDAP server connection
    d. Enable ISAM integration

Mobile Multi-factor Authentication (MMFA)

The installer may configure MMFA as a source of multi factor authentication.

4. Create the mobile reverse proxy instance if required. The name, HTTPS port and listening port are configurable when running the setup script. If this instance already exists the creation can be skipped.

5. Create a junction on the mobile reverse proxy instance “/mga”.
6. Create a junction on the mobile reverse proxy instance “/scim”.
7. Update the mobile reverse proxy instance configuration file with the required values for this integration.
8. Create a new mapping rule BuildMMFAStepupLoginPrompt.
9. Create new template files:
    a. C/mmfa/user/mgmt/mmfa/usc/transactions.html
    b. C/mmfa/user/mgmt/mmfa/metadata/AuthenticatorClient/metadata.json
10. Create 2 new push notification providers. These are not setup with proper keys, ids and secrets and should be modified post install.
    a. apple —> verifypushcreds.mybluemix.net
    b. android —> verifypushcreds.mybluemix.net
11. Create a new authentication mechanism
    a. BuildMMFAStepupLoginPrompt
12. Create 2 new authentication policies
    a. MMFA User Presence Response. To allow user presence verification from the mobile device.
    b. MMFA Fingerprint Response. To allow fingerprint verification from the mobile device.
13. Create a new API definition
    a. AuthenticatorDef
14. Create a new API client
    a. Authenticator Client
15. Set the advanced tuning parameter
    a. runtime_profile.jvm_option —> -Dhttps.protocols=TLSv1.2,TLSv1.1,TLSv1
16. Set the advanced configuration item
    a. .httpClient.defaultSSLProtocol —> TLSv1.2
17. Load the IBM IMC API Gateway default certificate into the rt_profile_keys CA signer certificates (api8.silverpop.com:443).
18. Load the Push Notification Bluemix Proxy default certificate into the rt_profile_keys CA signer certificates (verifypushcreds.mybluemix.net:443).
19. Run the MMFA config
    a. Client ID —> AuthenticatorClient
    b. Endpoints all use the prefix https://public_host:public_port (as defined in the setup script)
    c. Discovery mechanisms
    d. Fingerprint
    e. User presence
    f. Custom QR Code Options —> ignoreSslCerts == true
20. Attach the required ACLs to the mobile URLs:
    a. isam_mobile_anyauth —> /mga/sps/oauth/oauth20/logout
    b. isam_mobile_nobody —> /mga
    c. isam_mobile_rest —> /mga/sps/mga/user/mgmt/questions
    d. isam_mobile_rest —> /mga/sps/mmfa/user/mgmt/auth_methods
    e. isam_mobile_rest —> /mga/sps/mmfa/user/mgmt/qr_code
    f. isam_mobile_rest —> /mga/sps/mga/user/mgmt/grant
    g. isam_mobile_rest —> /mga/sps/mmfa/user/mgmt/transactions
    h. isam_mobile_rest —> /scim
    i. isam_mobile_rest —> /mga/sps/mmfa/user/mgmt/authenticators
    j. isam_mobile_rest —> /mga/sps/mga/user/mgmt/device
    k. isam_mobile_rest —> /mga/sps/mga/user/mgmt/otp
    l. isam_mobile_unauth —> /mga/sps/oauth/oauth20/token
    m. isam_mobile_unauth —> /mga/sps/mmfa/user/mgmt/details
    n. isam_mobile_rest_unauth —> /mga/sps/apiauthsvc

Mobile Multi-factor Authentication (MMFA) for APIMFA

The installer may configure additional components that will allow MMFA to act as a source of multi factor authentication.

1. Create new mapping rule
    a. reformat_totp_response
2. Update existing mapping rules
    a. AuthenticatorPreTokenGeneration
    b. AuthenticatorPostTokenGeneration
3. Create a new authentication mechanism
    a. Reformat TOTP Response
4. Create new authentication policies
    a. APIMFA Backchannel TOTP Validation Policy
    b. MMFA Stepup Login

FIDO U2F Authentication

The installer may configure FIDO U2F as a source of multi factor authentication.

1. Update template files:
    a. C/authsvc/authenticator/u2f/register.html
2. Update the FIDO U2F Universal 2nd Factor authentication mechanism
    a. Set the application ID to https://<rthost>
    b. Set attestationEnforcement to Optional

Common Components

The installer will create and configure a number of components that are common to the OAuth backchannel, MMFA and FIDO U2F.

1. Create new mapping rules
    a. MMFASCIMHelper
    b. backchannel_infomap
    c. browser_infomap
    d. pre_2fa
    e. require_2fa
    f. require_apiclient
    g. select_2fa
2. Create new template files
    a. C/authsvc/authenticator/apimfa/browser.html
    b. C/authsvc/authenticator/apimfa/redirect.html
    c. C/authsvc/authenticator/apimfa/browsercomplete.html
    d. C/authsvc/authenticator/apimfa/backchannelcomplete.json
    e. C/authsvc/authenticator/apimfa/selection.html
    f. C/authsvc/authenticator/apimfa/backchannelerror.json
    g. C/authsvc/authenticator/apimfa/browsererror.html
    h. C/authsvc/authenticator/apimfa/backchannelerror.html
    i. C/authsvc/authenticator/apimfa/backchannelcomplete.html
3. Create new authentication mechanisms
    a. APIMFA Browser
    b. Require API Client
    c. APIMFA Backchannel

   d. Require 2FA
   e. Select 2FA

4. Create new authentication policies
   a. APIMFA Browser Policy
   b. APIMFA Backchannel Policy
   c. Select 2FA Policy

Error Message Reference

Common errors encountered during the AppX installer are included below. Ensure that the appx installer prerequisites have been installed as per the appx installer documentation.

Python 2.7 errors

The AppX installer requires Python 3.
When attempting to install a Partner app using Python 2.7 or below the `TemporaryDirectory` package is not available.

```
Starting App Deployment
Traceback (most recent call last):
  File "appx-installer.py", line 2074, in <module>
    open_archive()
  File "appx-installer.py", line 94, in open_archive
    temporary_directory = tempfile.TemporaryDirectory()
AttributeError: 'module' object has no attribute 'TemporaryDirectory'
```

Installing `backports.tempfile` is not sufficient as other Python 3 packages are required.

Checking your Python version

Ensure you have Python 3 installed and your environment variables correctly referencing the python3 binary

```
[user@host ~]# which python
/usr/bin/python
[user@host ~]# /usr/bin/python --version
Python 2.7.10
```

If you have Python 3 installed, you can execute the setup script which calls the appx installer using the python3 command.

For example:
`python3 appx-installer.py backchannel_instance/`

Security Access Manager Appliance Connectivity

The system executing the AppX Installer to install the Partner app must have connectivity to the Security Access Manager appliance.

```
IO Error
```

```
2017-12-07 11:53:32,969 - AppX - INFO - Connecting to ISAM at
'https://isam903lmi.mysecure.org'
Traceback (most recent call last):
  File "appx-installer.py", line 2079, in <module>
    connect_isam()
…
requests.exceptions.ConnectionError:
HTTPSConnectionPool(host='isam903lmi.mysecure.org', port=443): Max retries exceeded
with url: /core/sys/versions (Caused by
NewConnectionError('<urllib3.connection.VerifiedHTTPSConnection object at
0x10cd98450>: Failed to establish a new connection: [Errno 8] nodename nor servname
provided, or not known',))
```

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.